Adaptive Defense 360

Guía para el administrador de redes

Tabla de contenidos

1. Prólogo

¿A quién está dedicada esta guía?

Iconos

1.1. Introducción

Esta guía contiene información y procedimientos de uso para obtener el máximo beneficio del producto **Adaptive Defense 360**.

1.2. ¿A quién está dirigida esta guía?

Esta documentación está dirigida a administradores de red que necesitan proteger los equipos informáticos y dispositivos móviles de la empresa, determinar el alcance de los problemas de seguridad detectadas y establecer planes de respuesta y prevención frente a las amenazas y ataques dirigidos avanzados (APTs).

Aunque **Adaptive Defense 360** es un servicio gestionado que ofrece seguridad garantizada sin intervención del administrador de la red, también provee información muy detallada y de fácil comprensión sobre los procesos y programas ejecutados por los usuarios en los equipos de la empresa, ya sean amenazas conocidas o desconocidas como programas legítimos.

Para que el administrador de la red pueda interpretar correctamente la información ofrecida son necesarios conocimientos técnicos de entornos Windows a nivel de procesos, sistema de ficheros y registro, así como entender los protocolos de red utilizados con mayor frecuencia.

1.3. Iconos

En esta guía se utilizan los siguientes iconos:

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consejo importante de cara a un uso correcto de las opciones de **Adaptive Defense 360**.

Consulta en otro capítulo o punto del manual

2. Introducción

2.1. Introducción

Adaptive Defense 360 es una solución basada en múltiples tecnologías de protección, que permite sustituir el producto de antivirus tradicional instalado en la empresa por un servicio mucho más completo de seguridad gestionada.

Adaptive Defense 360 protege los equipos informáticos permitiendo ejecutar únicamente el software lícito, mientras supervisa y clasifica todos los procesos ejecutados en el parque informático del cliente en base a su comportamiento y naturaleza. Además, completa su oferta de seguridad ofreciendo herramientas monitorización, análisis forense y resolución para poder determinar el alcance de los problemas detectados y solucionarlos.

A diferencia de los antivirus tradicionales, **Adaptive Defense 360** utiliza un nuevo concepto de seguridad que le permite adaptarse al entorno particular de cada empresa, supervisando la ejecución de todas las aplicaciones y aprendiendo constantemente de las acciones desencadenadas por cada uno de los procesos.

Tras un breve periodo de aprendizaje, **Adaptive Defense 360** es capaz de ofrecer un nivel de protección muy superior al de un antivirus tradicional, al tiempo que proporciona una información valiosa sobre el contexto en el que se sucedieron los problemas de seguridad con el objetivo de determinar su alcance e implantar las medidas necesarias para evitar que se vuelvan a suceder.

Adaptive Defense 360 es un servicio multiplataforma compatible con Windows, Linux, Mac OS X, Android y alojado en la nube; por lo tanto, no requiere de nueva infraestructura de control en la empresa, manteniendo de esta manera un TCO bajo.

2.2. Características principales de Adaptive Defense 360.

Adaptive Defense 360 ofrece un servicio de seguridad garantizada frente a amenazas y ataques avanzados y dirigidos a las empresas a través de cuatro pilares:

- **Visibilidad**: Trazabilidad de cada acción realizada por las aplicaciones en ejecución.
- **Detección**: monitorización constante de los procesos en ejecución y bloqueo en tiempo real de exploits conocidos, Zero-day y otras amenazas avanzadas diseñadas para pasar desapercibidas a los antivirus tradicionales.
- **Resolución y Respuesta:** Información forense para investigar en profundidad cada intento de ataque, y herramientas de resolución.
- **Prevención**: Evita futuros ataques bloqueando aquellas aplicaciones maliciosas y fortaleciendo la seguridad del parque informático.

*Figura 1: Los cuatro pilares de la protección avanzada de **Adaptive Defense 360***

2.3. Perfil de Usuario de Adaptive Defense 360

Aunque **Adaptive Defense 360** es un servicio gestionado que ofrece seguridad sin intervención del administrador de la red, también provee información muy detallada y comprensible sobre la actividad de los procesos ejecutados por los usuarios en toda la infraestructura de IT de la empresa. Esta información puede ser utilizada por el administrador para delimitar claramente el impacto de posibles problemas y adaptar sus protocolos de seguridad, evitando así situaciones equivalentes en el futuro.

Todos los usuarios con un agente **Adaptive Defense 360** instalado en su equipo disfrutarán de un servicio de seguridad con garantías, impidiendo la ejecución de programas que supongan una amenaza para el desarrollo de la empresa.

2.4. Componentes principales de la arquitectura Adaptive Defense 360

Adaptive Defense 360 se apoya en la monitorización del comportamiento de los procesos ejecutados en el parque de cada cliente. Esta información se analiza mediante técnicas de Machine Learning en infraestructuras Big Data alojadas en la nube; de esta forma el cliente no tiene que instalar hardware ni recursos adicionales en sus oficinas.

A continuación, se muestra el esquema general de **Adaptive Defense 360** y los componentes que lo forman:

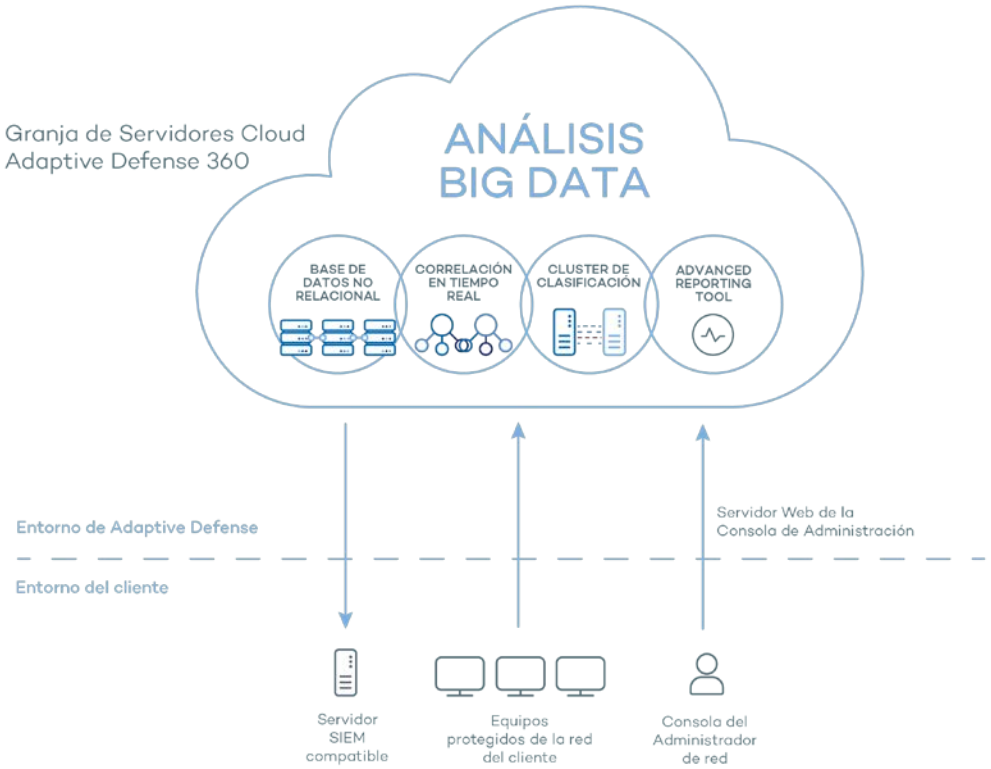


*Figura 2: Esquema general **Adaptive Defense 360***

Adaptive Defense 360 está formado por los elementos siguientes:

- Granja de servidores Cloud
- Servidor Web de la consola de administración
- Equipos protegidos con **Adaptive Defense 360** mediante el software instalado
- Equipo del administrador de red que accede a la consola Web
- Servidor de informes avanzados ART (Advanced Reporting Tool)
- Servidor SIEM compatible
- Módulo de protección instalado en los equipos de la red

A continuación, se detallan los diferentes roles de la arquitectura mostrada.

2.4.1 Granja de servidores Cloud Adaptive Defense 360

El clúster de servidores en la nube de **Adaptive Defense 360** recopila todas las acciones realizadas por los procesos de usuario y enviadas desde los agentes instalados en los equipos del cliente. Mediante técnicas de inteligencia artificial, evalúa su comportamiento y dicta una clasificación por cada proceso en ejecución, que es devuelta al agente para tomar una decisión y mantener protegidos los equipos de la empresa.

El clúster de servidores **Adaptive Defense 360** está formado por una granja de servidores alojada en la nube que configura un entorno de explotación Big Data donde se aplican los algoritmos Machine Learning de forma continuada para clasificar cada proceso ejecutado.

Las ventajas de este nuevo modelo de análisis de procesos en la nube frente al adoptado por los antivirus tradicionales basados en el envío de muestras al proveedor y análisis manual son varias:

- El porcentaje de error al clasificar un proceso ejecutado en multitud de equipos a lo largo del tiempo es del 99'9991% (menos de 1 error cada 100.000 ficheros analizados) con lo que el número de falsos positivos y falsos negativos es cercano a cero.
- Todos los procesos de los equipos protegidos por **Adaptive Defense 360** son monitorizados y analizados con lo que se elimina la incertidumbre de los antivirus tradicionales, que únicamente reconocen lo que es malware y desconocen el resto de aplicaciones.
- El retraso en la clasificación de los procesos vistos por primera (ventana de oportunidad) vez es mínimo ya que el agente **Adaptive Defense 360** envía las acciones que desencadena cada proceso en tiempo real, disminuyendo de manera drástica el tiempo de exposición a las amenazas. Adicionalmente, los ficheros ejecutables encontrados en el equipo del usuario desconocidos para la plataforma **Adaptive Defense 360** serán enviados a la granja de servidores de Panda Security para su análisis.

El impacto en el rendimiento de la red del cliente debido al envío de los ejecutables desconocidos está configurado para pasar desapercibido. Un fichero desconocido se envía una sola vez para todos los clientes que usan Adaptive Defense 360. Además, se han implementado mecanismos de gestión del ancho de banda y limites por equipo y hora, con el objetivo de minimizar el impacto en la red del cliente.

- La monitorización continúa de cada proceso permite a **Adaptive Defense 360** clasificar como malware elementos que inicialmente tenían un comportamiento de goodware. Este patrón de actuación es muy habitual en los ataques dirigidos y otras amenazas avanzadas diseñadas para operar por debajo del radar.
- El análisis en la nube libera al cliente de instalar y mantener infraestructuras de hardware y software junto al pago de licencias y la gestión de garantías de hardware, con lo que el TCO desciende significativamente.

2.4.2 Servidor Web de la consola de administración

Toda la gestión de **Adaptive Defense 360** se realiza a través de la consola Web accesible para el administrador desde la URL https://www.pandacloudsecurity.com/PandaLogin/

La consola Web es compatible con los navegadores más comunes y es accesible desde cualquier lugar y en cualquier momento utilizando cualquier dispositivo que tenga instalado un navegador compatible.

La consola Web es "responsive", de modo que es accesible desde móviles y tablets en cualquier momento y lugar.

2.4.3 Equipos protegidos con Adaptive Defense 360

Adaptive Defense 360 requiere de la instalación de un componente software y que tiene que estar instalado en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad.

Este componente está formado por dos módulos: el agente de comunicaciones y el módulo de la protección.

Aunque en este capítulo se diferencia entre "agente" y "protección", son dos módulos que se instalan a la vez y son necesarios para la correcta gestión de la seguridad del equipo a proteger. De esta forma, "agente" y "protección" son utilizados de forma indistinta para referirse al componente software instalando en el equipo de cada usuario.

- **Agente de comunicaciones**

El agente se encarga tanto de gestionar las comunicaciones entre los equipos administrados y el servidor de **Adaptive Defense 360** como de establecer un diálogo entre los equipos que pertenecen a una misma red del cliente.

Este módulo, además de la gestión de los procesos locales, es el encargado de recoger los cambios de configuración que el administrador haya realizado a través de la consola Web, y de aplicarlos sobre el módulo de Protección.

Para comprobar si el administrador ha realizado cambios de configuración se utiliza la siguiente lógica:

- El administrador modifica la configuración en la consola Web.
- El servidor envía una notificación para indicar a los equipos afectados la existencia de cambios de configuración que les afectan.
- Los equipos comprueban cada 15 minutos si hay alguna notificación para ellos. Si la hay:
  - El equipo solicita al servidor de **Adaptive Defense 360** las nuevas políticas de configuración que tiene disponibles.
  - El servidor se las entrega y el equipo aplica los cambios.

El agente también se coordina con otros agentes de diferentes equipos en su mismo grupo mediante la funcionalidad Peer to Peer o "rumor" para centralizar y gestionar las descargas de los ficheros de firmas y actualizaciones desde Internet. Consulta el capítulo 10 Actualización de la protección para más información.

Proxy dinámico

El agente guarda una lista con información de los equipos en la red que tengan otros agentes instalados, y sean capaces de enviar mensajes a Internet. Estos agentes se denominan Proxys.

Para poder actuar como proxy para otros agentes, una máquina debe cumplir los siguientes requisitos: disponer de conexión directa a Internet, y disponer al menos de 256 MB de RAM. Además, el equipo debe de haber concluido completamente la secuencia de instalación.

Cuando la lista de proxys está vacía o ninguno de los agentes que están en ella responde (Disponibilidad = 0), el agente envía un mensaje por broadcast a la subred preguntando ¿quién es Proxy? para que estos le respondan y pueda mandar mensajes a Internet a través de ellos.

Mientras realiza la espera por datos de la lista de proxys válidos, el módulo del Proxy no atenderá peticiones de otros mensajes.

La lista de proxys tendrá un valor asociado para cada Proxy con el número de intentos que se permiten fallar en la comunicación con otro agente antes de invalidar ese agente como proxy.

Por defecto el número de veces será 3, y cuando este valor alcance 0 se entenderá que ese agente no es válido como proxy. Si en algún momento todos los proxys de la lista son inválidos se entiende que la lista es no válida en su conjunto y se comenzará la búsqueda de proxys, lanzando un mensaje "¿quién es proxy?".

Puede ocurrir que el mensaje se envíe correctamente a un proxy de la lista, pero que éste al intentar mandar el mensaje a Internet descubra que ya no tiene conexión.

En ese caso el agente remoto repetirá la secuencia aquí descrita reenviando el mensaje a un proxy de su lista, pero además enviará por TCP al agente del que le llegó el mensaje otro de tipo "Yo no soy Proxy", para indicarle que lo borre de su lista porque ya no tiene conexión a Internet.

Este proceso se repetirá hasta que el mensaje se envíe correctamente a Internet o hasta que pase por un número máximo de proxy sin conseguir enviarse, en cuyo caso se perderá.

Se puede configurar el número de proxys por los que puede pasar un mensaje. Por defecto sólo se enviará a 1, y si falla el envío desde ése se perderá el mensaje.

Dentro del mensaje se guarda la lista de proxys por los que ha pasado, de modo que no se envíe dos veces al mismo proxy sin conexión a Internet.

Proxy estático

Si se desea que todos los accesos a Internet se hagan a través de un equipo concreto decidido por el administrador, en lugar de por equipos determinados de forma dinámica, el agente de comunicaciones admite la posibilidad de especificar qué máquina deseamos que actué como Proxy.

La máquina que actúe como 'Proxy estático' debe cumplir los siguientes requisitos:

- Debe tener un agente instalado
- Debe tener acceso directo a Internet
- Disponer de al menos 256 MB de memoria.
- Debe haber comunicado con el servidor en las últimas 72 horas

Si en algún momento el equipo que se estableció para que actúe como proxy estático deja de cumplir alguno de los requisitos necesarios para ejercer como tal, se desactivará en la consola Web la configuración del proxy estático, desapareciendo el nombre del equipo que estaba configurado y se mostrará un mensaje indicándole cuál de dichos requisitos se incumple.

El administrador podrá seleccionar otro equipo para que realice las funciones de proxy estático. Si un equipo deja de ser proxy estático por haber sido incluido en la lista negra, una vez que deje de pertenecer a dicha lista, si se desea que actúe de proxy estático será necesario configurarlo de nuevo para que transiten por él todas las comunicaciones con el servidor.

Cuando el agente tenga que realizar un acceso a Internet en primer lugar intentará comunicarse utilizando el 'proxy estático'.

Si la comunicación con el Proxy estático no es posible, se intentará llevar a cabo el acceso a internet siguiendo la secuencia de comunicaciones habitual.

Si tiene una configuración válida almacenada, intentará la comunicación utilizando dicha configuración.

En caso contrario, intentará comunicarse mediante conexión directa a Internet.

Si tampoco consigue la conexión directa, lo intentará a través de otro equipo 'proxy dinámico', cuyo funcionamiento se ha detallado en el apartado anterior.

Cuando el equipo que está actuando como proxy recibe una petición de acceso a Internet intentará realizar la conexión de forma directa. Si la conexión se realiza con éxito enviará la respuesta obtenida al agente que solicitó la conexión.

La configuración del proxy estático se realiza editando las propiedades del perfil al que pertenecen los agentes instalados. Para ello en la ventana Configuración elija el perfil a modificar en el panel de la derecha y allí, en el menú Windows y Linux haz clic en la pestaña **Opciones avanzadas** y activa la casilla **Centralizar todas las conexiones con el servidor a través del siguiente equipo**.

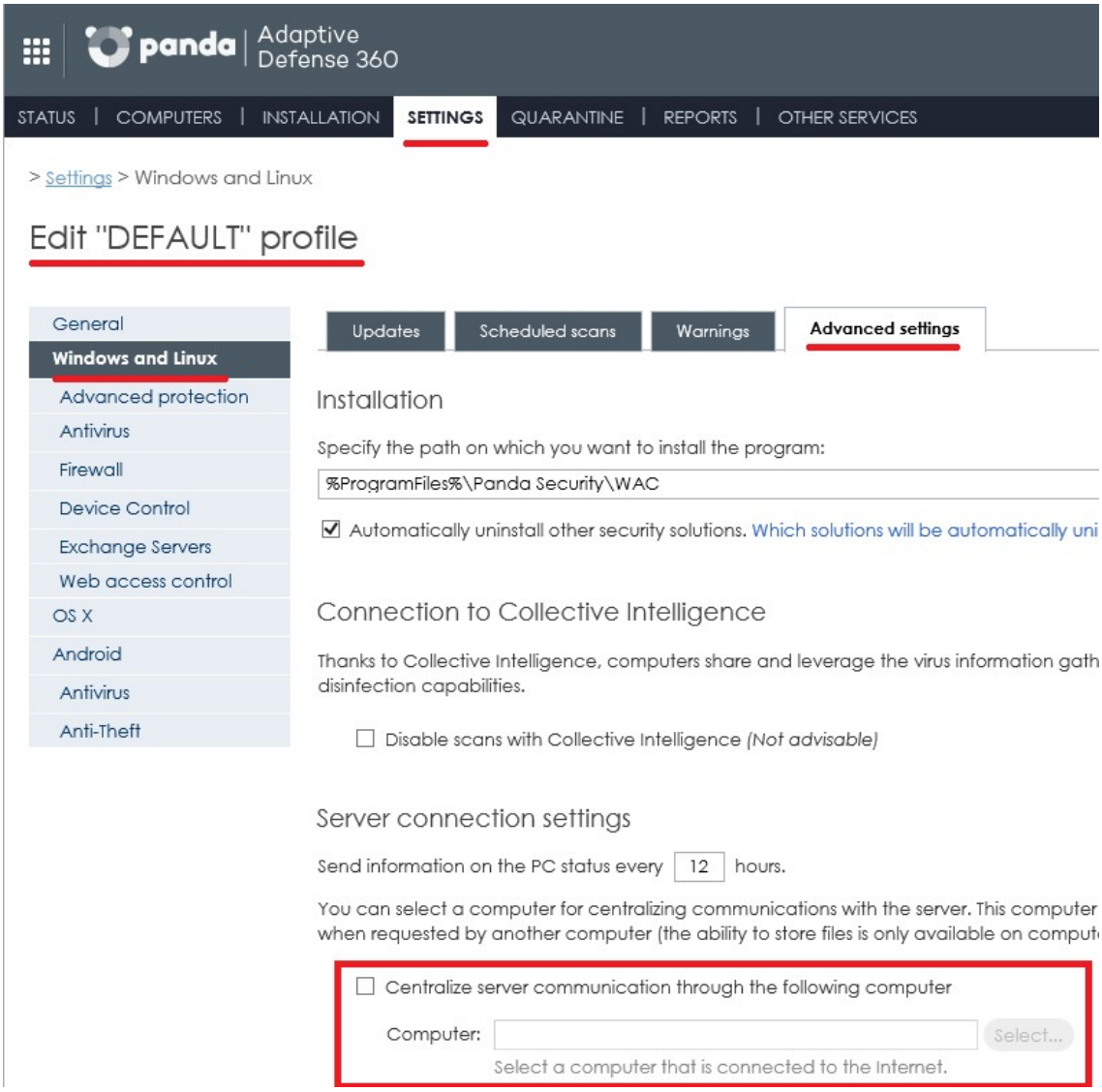


Figura 3: Configuración de un equipo de la red

- **Módulo de Protección**

Este módulo contiene las tecnologías encargadas de proteger los equipos del cliente. **Adaptive Defense 360** reúne en un mismo producto todos los recursos necesarios para detectar el malware de nueva generación y dirigido (APT) al tiempo que incorpora herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

El agente Adaptive Defense 360 se instala sin problemas en máquinas con otras soluciones de seguridad de la competencia.

2.5. Servicios Adaptive Defense 360

Panda Security ofrece otros servicios de carácter opcional que le permiten al cliente integrar la

solución con su infraestructura IT ya desplegada y obtener de forma directa inteligencia de seguridad desarrolla en los laboratorios de Panda Security.

2.5.1 Servicio Advanced Reporting Tool

Adaptive Defense 360 permite el envío automático y transparente de toda la información recogida de los equipos de usuario al servicio **Advanced Reporting Tool**, un sistema de almacenamiento y explotación del conocimiento generado en la red del cliente.

Las acciones de los procesos ejecutados en el parque de IT son enviadas a **Advanced Reporting Tool** para relacionarlos de forma flexible y visual, con el objetivo de extraer inteligencia de seguridad y conseguir información adicional sobre las amenazas y sobre el uso que los usuarios están dando a los equipos de la empresa.

El servicio **Advanced Reporting Tool** es accesible directamente desde el panel de control de la propia consola Web de **Adaptive Defense 360**.

Consulta la Guía de usuario Advanced Reporting Tool accesible desde la web de producto para configurar y sacar provecho del servicio de análisis de conocimiento y búsquedas avanzadas.

2.5.2 Servicio SIEMFeeder: Integración con el servidor SIEM del cliente

Adaptive Defense 360 se integra con las soluciones SIEM de proveedores externos implementadas por los clientes en sus infraestructuras de IT, enviando los datos recogidos sobre la actividad de las aplicaciones ejecutadas en sus equipos. Esta información se entregará al SIEM, ampliada con todo el conocimiento de la plataforma **Adaptive Defense 360,** y podrá ser explotada por los sistemas de que disponga el cliente.

A continuación, se listan los sistemas SIEM compatibles con **Adaptive Defense 360**:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora

Consulta la Guía de usuario SIEMFeeder para una descripción detallada de la información recogida por Adaptive Defense 360 y enviada al sistema SIEM del cliente.

2.5.3 Samples Feed

Este servicio está diseñado para servir como complemento indispensable en aquellas empresas que tengan su propio laboratorio para el estudio de malware.

Mediante una API REST Panda Security entrega ejemplares del malware normalizado para su estudio, así como de las aplicaciones goodware encontradas en la red del cliente.

También se entregan automatizaciones del malware encontrado, que constan de un completo informe de ejecución en los entornos sandbox, formados por máquinas reales en la infraestructura de Panda Security.

2.5.4 IP Feeds

Se trata de un servicio de suscripción donde el cliente recibe bloques de direcciones IP utilizadas por las redes de bots detectadas y analizadas por Panda Security.

Este flujo de información se entrega de diariamente y puede ser aprovechado por los dispositivos de seguridad del cliente, incrementando así el nivel de protección de toda la red.

2.5.5 Módulo Remote control

Para facilitar la resolución remota de problemas, **Adaptive Defense 360** pone a disposición de los clientes el módulo de control remoto desde la nube **Remote Control**. De esta forma, el administrador de la red dispondrá de varias herramientas, tales como el escritorio remoto o la línea de comandos remota entre otros, para realizar labores de limpieza de malware y comprobar el buen funcionamiento del equipo.

Todas las herramientas ofrecidas en el módulo Remote Control son ejecutadas desde la nube, en cualquier momento y en cualquier lugar, desde la consola de **Adaptive Defense 360** y con el único requisito de utilizar un navegador web compatible.

Consulta la Guía para el administrador de Remote control para una descripción detallada sobre este módulo.

2.6. Dispositivos soportados en Adaptive Defense 360

Adaptive Defense 360 es compatible con los siguientes sistemas operativos:

- Windows Workstation
- Windows Server
- Mac OS X
- Linux
- Tablets y móviles Android

La consola de administración es compatible con los navegadores mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge (se recomienda desactivar el filtro SmartScreen)
- Firefox

2.7. Recursos y documentación disponible

A continuación, se detalla una relación de recursos disponibles sobre **Adaptive Defense 360.**

Guía para administradores de red

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADAPTIVEDEFENSE360-manual-ES.pdf

Guía de Advanced Reporting Tool

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-Guia-ES.pdf

Guía de SIEMFeeder

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-ES.PDF

Página de soporte de producto.

http://www.pandasecurity.com/spain/support/adaptive-defense-360.htm

Página de producto

http://www.pandasecurity.com/spain/intelligence-platform/solutions.htm

3. El ciclo completo de protección adaptativa

3.1. Introducción

Este capítulo ofrece una visión de la estrategia general adoptada por **Adaptive Defense 360** para gestionar la seguridad de la red de la empresa.

Más de 200.000 nuevos virus son generados diariamente y una parte muy sustancial de este nuevo malware está diseñado para ejecutarse en los equipos de los usuarios durante largos periodos de tiempo y en segundo plano, sin dar muestras de su existencia.

Por esta razón, el enfoque tradicional de protección mediante archivos de identificadores locales o en la nube ha demostrado ser progresivamente ineficiente: debido al creciente número de malware desarrollado, su ventana de oportunidad es cada vez mayor, entendida ésta como el tiempo que transcurre desde que el primer equipo es infectado a nivel mundial, hasta que los proveedores de seguridad identifican ese nuevo malware y alimentan sus archivos de identificadores con la información necesaria para detectarlo.

De esta manera, toda estrategia de seguridad pasa por minimizar el tiempo de exposición al malware, siendo éste el tiempo que transcurre desde que una amenaza desconocida entra en la red del cliente hasta que es reconocida como malware. En la actualidad el tiempo de exposición estimada es de 259 días para ataques dirigidos, un tipo de amenazas cada vez más frecuente y que tiene como principales objetivos el robo de datos y el espionaje industrial.

Debido a este cambio drástico en el panorama del malware **Adaptive Defense 360** propone un nuevo enfoque de seguridad basado en el **ciclo de protección adaptativa**: un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos integrados y centralizadas en una única consola Web de administración. Gracias a este enfoque es posible mostrar el ciclo completo de la seguridad de la red en tiempo real.

El ciclo de protección adaptativa permite evitar o minimizar las brechas de seguridad, reduciendo de forma drástica las pérdidas de productividad y el riesgo de robo de información confidencial en la empresa; el administrador es liberando de la compleja tarea de determinar qué es peligroso y por qué razón, recuperando espacio y tiempo para gestionar y vigilar el estado de la seguridad de los recursos que administra.

El departamento de IT será capaz de tomar decisiones que permitan adaptar la política de seguridad de la empresa con la misma agilidad que mutan los patrones de ataque del malware avanzado.

3.2. El ciclo de protección adaptativa

El objetivo de **Adaptive Defense 360** es el de facilitar al departamento de IT la creación de un espacio donde poder definir y establecer las políticas de seguridad de empresa que respondan rápida y adecuadamente a los nuevos tipos de amenazas que emergen de forma constante. Este espacio es producto, por una parte, de la liberación de responsabilidades del equipo técnico en la

compañía a la hora de decidir qué ficheros son seguros y cuales son peligrosos, y por qué motivo: con **Adaptive Defense 360** el departamento técnico de la empresa recibirá una clasificación sin ambigüedades de absolutamente todos los programas ejecutados en el parque informático gestionado.

Por otra parte, el departamento de IT también recibirá un conjunto de herramientas para la visualización del estado de la seguridad, la resolución de los problemas ocasionados por el malware avanzado y el análisis forense, que permite estudiar de forma detallada el comportamiento de APTs y otras amenazas.

Con toda esta información y herramientas, el administrador podrá cerrar el ciclo completo de la seguridad en la empresa: monitorizar el estado del parque informático gestionado, revertir el sistema a la situación previa a las brechas de seguridad en caso de producirse, y conocer su alcance para poder implementar las medidas de contingencia apropiadas. Todo este ciclo se encaja dentro de un proceso de refinamiento contante, que resultará en un entorno informático seguro, flexible y productivo para los usuarios de la empresa.

Este ciclo constante de protección adaptativa implementado por las empresas con ayuda de **Adaptive Defense 360** se puede resumir en la Figura 4.

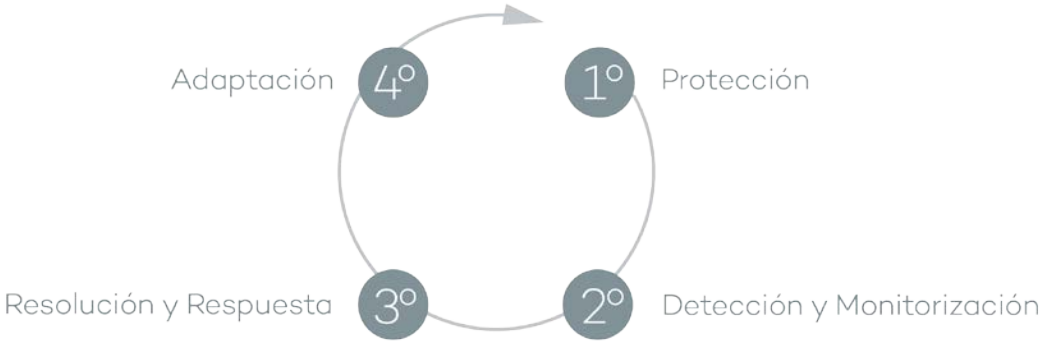


Figura 4: El ciclo de protección adaptativa

3.3. Fase I: Protección completa del parque informático

> ***Consulta los capítulos 13,14 y 15 Perfiles de protección Windows, Perfiles de protección Linux y Perfiles de protección Mac OS X para más información sobre las funcionalidades de protección de Adaptive Defense 360 tratadas en esta sección***

La primera fase del ciclo de protección adaptativa incluye las herramientas necesarias para proteger y defender de forma efectiva el parque informático de posibles ataques e intentos de infección. **Adaptive Defense 360** es compatible con estaciones de trabajo y servidores Windows, Linux y Mac OS X, así como con tablets y teléfonos móviles Android.

3.3.1 Protección contra exploits

Adaptive Defense 360 implementa tecnologías para proteger los equipos de la red frente a amenazas que aprovechan bugs en el software instalado (exploits). Estos bugs provocan comportamientos anómalos de aquellas aplicaciones comprometidas, que desembocan en fallos de seguridad en el parque informático del cliente.

Las amenazas de tipo exploit utilizan tanto vulnerabilidades conocidas como de día cero (0-day) o desconocidas, en una cadena de eventos (CKC, Cyber Kill Chain), que han de completar para comprometer los equipos de la red. **Adaptive Defense 360** bloquea de forma efectiva y en tiempo real esta cadena de eventos para impedir que los ataques de tipo exploit prosperen, dejándolos sin efecto.

Para conseguir este nivel de protección y respuesta inmediata ante todo tipo de exploits, **Adaptive Defense 360** implementa nuevos hooks en el sistema operativo, que utiliza para monitorizar localmente y de forma constante las acciones de los procesos ejecutados en el equipo del usuario.

De esta forma, **Adaptive Defense 360** detecta las técnicas usadas por los hackers para la explotación de vulnerabilidades, y se aleja del esquema tradicional de búsqueda de patrones y detecciones estáticas de pares CVE - payload mediante ficheros de firmas, implementados por otros productos de seguridad.

Adaptive Defense 360 ofrece una protección anti exploit generalista, fruto de algoritmos en constante adaptación por el equipo de expertos en ciberataques de Panda Security frente a técnicas de explotación de vulnerabilidades como Head Spraying, Anti ROP, desactivación de DEP y ASLR entre otras.

3.3.2 Protección antivirus permanente e inteligencia colectiva

La protección antivirus permanente es el módulo de seguridad tradicional que cubre los vectores de infección más utilizados por los hackers. Este módulo se alimenta del archivo de identificadores publicado por Panda Security para su descarga en local y del acceso en tiempo real a la Inteligencia Colectiva.

En el contexto actual de crecimiento continuo del malware, los servicios alojados en la nube han cobrado especial importancia frente a las actualizaciones del fichero de firmas local, para gestionar con éxito la enorme cantidad de amenazas que surgen de forma continuada. Por esta razón la protección de antivirus de **Adaptive Defense 360** se basa fundamentalmente en la Inteligencia Colectiva, una plataforma de conocimiento en la nube que aumenta exponencialmente la capacidad de detección.

Esta plataforma consta de servidores que clasifican y procesan de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones que se han producido en sus equipos. **Adaptive Defense 360** realiza consultas a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos de los equipos.

Cuando un nuevo ejemplar de malware es detectado en el equipo de un miembro de la comunidad de usuarios, **Adaptive Defense 360** se encarga de enviar la información necesaria a los servidores de Inteligencia Colectiva alojados en la nube, de forma totalmente automática y anónima. La información es procesada por dichos servidores, entregando una solución no sólo al usuario afectado, sino también al resto de usuarios de la comunidad, en tiempo real.

Adaptive Defense 360 se sirve de la Inteligencia Colectiva para aumentar la capacidad de detección y evitar penalizaciones en el rendimiento del equipo del cliente. Ahora todo el conocimiento está en la nube y, gracias a **Adaptive Defense 360**, todos los usuarios pueden beneficiarse de ello.

3.3.3 Protección contra técnicas avanzadas de ocultación y virus de macro

Al margen de la tradicional estrategia de detección contrastando el payload del fichero objeto de estudio con el fichero de firmas, **Adaptive Defense 360** implementa tecnologías que permiten analizar el comportamiento de los procesos de forma local.

De esta manera se detectan comportamientos extraños en los principales motores de scripting (Visual basic Script, Javascript y Powershell) incorporados en todos los sistemas Windows actuales y utilizados como extensión de la línea de comandos. También se detectan macros maliciosas embebidas en ficheros ofimáticos como Word, Excel, PowerPoint etc.

También son detectadas las últimas técnicas de ejecución de malware sin fichero (los llamados FileLess Malware) que inyectan el payload del virus directamente en el proceso utilizado para la explotación de la vulnerabilidad. En estos casos, al no escribir ningún fichero en el disco duro se reducen significativamente las probabilidades de detección en las soluciones de seguridad tradicionales.

Como complemento se incorporan además los habituales motores heurísticos y de detección de ficheros maliciosos por características estáticas.

3.3.4 Protección del correo y la Web

Adaptive Defense 360 evita el habitual enfoque de seguridad de correo y Web basado en plugins que añaden la funcionalidad de protección a determinados clientes de correo y navegadores. En su lugar, el funcionamiento de la protección consiste en una interceptación a bajo nivel de todas las comunicaciones que usan protocolos comunes como HTTP, HTTPS o POP3. De esta manera, se ofrece una protección homogénea y permanente para todas las aplicaciones de correo y Web pasadas presentes y futuras, sin necesidad de configuraciones específicas ni de actualizaciones de plugins cuando los proveedores de los programas de correo y navegación publiquen nuevas versiones de su software.

3.3.5 Protección de la red por cortafuegos y sistema de detección de intrusos (IDS)

Adaptive Defense 360 ofrece tres herramientas básicas a la hora de filtrar el tráfico de red que recibe

o envía el equipo protegido:

- Protección mediante reglas de sistema: se trata de las tradicionales reglas que describen las características de la comunicación: puertos, IPs, protocolos etc. con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas establecidas
- Protección de programas: establece un conjunto de reglas que permitan o denieguen la comunicación a determinados programas instalados en el equipo de usuario
- Sistema de detección de intrusos: permite detectar patrones de tráfico malformado que afecten a la seguridad o al rendimiento del equipo protegido, rechazando dichos patrones.

3.3.6 Control de dispositivos

Los dispositivos de uso común como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles pueden ser utilizados como vía de infección. **Adaptive Defense 360** permite determinar cuál será el comportamiento del dispositivo en los equipos protegidos, bloqueando su acceso o permitiendo su uso de forma parcial (solo lectura) o completa.

3.3.7 Filtrado de Spam, Virus y contenidos en servidores Exchange

Adaptive Defense 360 analiza los correos con destino a buzones situados en el servidor Exchange en busca de spam, virus, herramientas de hacking y programas potencialmente no deseados sospechosos.

Para ello implementa una protección antivirus y anti-spam para servidores Exchange. De esta forma se consigue optimizar el tiempo de trabajo de los usuarios y aumentar la seguridad de los equipos de la red.

Adaptive Defense 360 protege los servidores de correo Exchange mediante dos tecnologías distintas:

- **Protección de buzones**

Se utiliza en los servidores Exchange con el rol de Mailbox y permite analizar las carpetas / buzones en backgroud o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones admite la manipulación de los diferentes elementos del cuerpo del mensaje analizado, lo que permite sustituir los elementos peligrosos encontrados por otros limpios, introducir únicamente los elementos peligrosos en cuarentena etc.

La protección de buzones optimiza el funcionamiento del servidor Exchange al recibir un nuevo fichero de firmas, realizando el análisis de todo el servidor en segundo plano, y aprovechando los tiempos de menor carga del servidor. El algoritmo de análisis es inteligente, y evita volver a examinar los mensajes ya analizados previamente.

- **Protección de transporte**

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Mailbox y permite analizar el tráfico que es atravesado por el servidor Exchange.

En la protección de transporte no se permite la manipulación del cuerpo de los mensajes. De esta forma, el cuerpo de un mensaje peligroso es tratado como un solo bloque y las acciones que **Adaptive Defense 360** permite ejecutar aplican al mensaje por completo: borrar el mensaje, meterlo en cuarentena, dejar pasar sin modificar etc.

3.3.8 Control de acceso a páginas Web

Restringe el acceso a determinadas categorías Web y permite configurar URLs individuales a las que se autorizará o restringirá el acceso. Esta herramienta permite optimizar el ancho de banda de la red e incrementar la productividad del negocio.

Las páginas Web se agrupan en 59 categorías y tan solo es necesario seleccionar aquellas a las que se desea denegar el acceso.

Además, **Adaptive Defense 360** permite definir configuración de horarios, con la que podrás restringir el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorizarlo en el horario no laborable o en el fin de semana

3.3.9 Protección de sistemas vulnerables

Adaptive Defense 360 también protege a aquellos sistemas que son reconocidos por la industria como vulnerables, debido a que han alcanzado su etapa de EOL (End Of Life), como Windows XP. Estos sistemas ya no reciben parches de seguridad y los fallos encontrados pueden ser aprovechados por el malware en forma de exploits.

3.4. Fase II: Detección y monitorización

La segunda fase del ciclo de protección adaptativa asume que el malware o el ataque dirigido consiguió sortear las barreras establecidas en la fase de Protección e infectó con éxito una o varias máquinas de la red, pasando esta infección desapercibida para el usuario del equipo

En esta fase **Adaptive Defense 360** implementa una serie de tecnologías novedosas que permiten al administrador de la red localizar el problema.

3.4.1 Protección permanente avanzada

La protección avanzada de **Adaptive Defense 360** es una tecnología innovadora que monitoriza de forma continuada todos los procesos que se ejecutan en los equipos Windows de la red del cliente. **Adaptive Defense 360** recoge todas las acciones desencadenadas por los procesos del usuario y los envía a la nube de Panda Security, donde se examinan mediante técnicas automáticas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o

malware) con un 99'9991 (menos de 1 error cada 100.000 ficheros analizados) de precisión, evitando de esta manera falsos positivos.

Para los casos más complicados Panda Security cuenta con un laboratorio de expertos especialistas en diseccionar malware, con el único objetivo de clasificar todos los ejecutables localizados en el menor tiempo posible desde la primera vez que fueron vistos en la red del cliente.

Adaptive Defense 360 admite tres modos de bloqueo para los procesos que todavía no han sido clasificados (desconocidos) y para los ya clasificados como malware:

- **Audit**

En el modo Audit **Adaptive Defense 360** solo informa de las amenazas detectadas, pero no bloquea ni desinfecta el malware encontrado. Este modo es útil para probar la solución de seguridad o para comprobar que la instalación del producto no comprometa el buen funcionamiento del equipo.

- **Hardening**

En aquellos entornos donde se producen cambios constantes del software instalado en los equipos de los usuarios o se ejecutan muchos programas desconocidos, como por ejemplo programas de creación propia, puede no ser viable esperar a que **Adaptive Defense 360** aprenda de ellos para clasificarlos.

El comportamiento del modo Hardening consiste en balancear el riesgo de infección de los equipos y la productividad de los usuarios, limitando el bloqueo de los programas desconocidos a aquellos que se consideran peligrosos a priori. De esta forma se distinguen cuatro escenarios:

- Ficheros ya clasificados por **Adaptive Defense 360** como goodware: se permite su ejecución.
- Ficheros ya clasificados por **Adaptive Defense 360** como malware: son enviados a cuarentena o desinfectados.
- Ficheros sin clasificar que vienen del exterior (Internet, correo y otros): se bloquea su ejecución hasta que el sistema emita una clasificación. En función de la clasificación se permitirá su ejecución (goodware) o serán movidos a cuarentena (malware).

En muchas ocasiones la clasificación es casi inmediata de forma que un programa descargado de internet y desconocido para Adaptive Defense 360 será bloqueado en un primer momento, pero minutos después podrá ser ejecutado si resulto ser goodware.

- Ficheros sin clasificar ya instalados en el equipo del usuario antes de la implantación de **Adaptive Defense 360**: se permite su ejecución, aunque sus acciones se monitorizan y serán enviadas al servidor para su estudio. Una vez clasificados se permitirá su ejecución (goodware) o serán movidos a cuarentena (malware)

- **Lock**

En entornos donde la seguridad sea la máxima prioridad, y con el objetivo de ofrecer una protección de máximas garantías **Adaptive Defense 360** deberá ser configurado en modo Lock. En este modo la ejecución del software en proceso de clasificación será bloqueada y se podrá garantizar la ejecución únicamente del software lícito.

De la misma forma que en el modo Hardening, los programas clasificados como maliciosos serán enviados a cuarentena, mientras que para los programas desconocidos se bloqueará su ejecución hasta ser clasificado como goodware o malware.

Más del 99% de los programas encontrados en los equipos de los usuarios están ya clasificados en los sistemas de Adaptive Defense 360. Los bloqueos afectarán a una minoría de programas

3.4.2 Monitorización de ficheros de datos

Adaptive Defense 360 registra todos los accesos a ficheros de datos del usuario por parte de los procesos ejecutados en el equipo. De esta manera, aunque el malware consiga infectar el equipo, será posible precisar con exactitud qué ficheros fueron modificados y en qué momento. También será posible determinar si los ficheros fueron enviados fuera de la empresa a través de Internet, las direcciones IP de destino y otra valiosa información que facilitará tanto el análisis forense posterior como las acciones de resolución. A continuación, se muestran los tipos de ficheros de datos que se monitorizan:

- Documentos de suites ofimáticas.
- Documentos en formato PDF.
- Documentos de aplicaciones CAD.
- BBDD de escritorio.
- Almacenes de contraseñas de navegadores.
- Almacenes de contraseñas de clientes de correo.
- Almacenes de contraseñas de clientes de FTP.
- Almacenes de contraseñas de Directorio Activo.
- Almacenes de certificados y certificados de usuario.
- Almacenes de Digital Wallet.
- Configuración de navegadores.
- Configuración de firewall.
- Configuración de GPO.

3.4.3 Visibilidad del estado de la red

Adaptive Defense 360 ofrece una serie de recursos para poder valorar el estado de la seguridad de la red en un solo vistazo, a través de un panel de control formado por paneles de Actividad.

Algunas de estas herramientas, como los informes, son ya conocidas; sin embargo, lo importante en

este punto no solo es determinar si la red del cliente está siendo atacada y en qué grado o forma sino contar con la información necesaria para poder valorar una probabilidad de infección.

En los paneles de **Adaptive Defense 360** se puede encontrar información clave en este sentido:

- Cuáles son los procesos desconocidos para **Adaptive Defense 360** encontrados en los equipos de la red, y que están siendo investigados para su posterior clasificación en Panda Security, junto con una valoración preliminar de su peligrosidad.
- Actividad detallada en forma de listados de acciones de aquellos programas desconocidos que finalmente resultaron ser malware.
- Detecciones realizadas en los diferentes vectores de infección protegidos.

Con este módulo el administrador tiene una visión global de los procesos que se ejecutan en su red, tanto del malware reconocido que intenta entrar y es detenido en el módulo de protección, como del malware desconocido y diseñado para pasar inadvertido por las tecnologías de detección tradicionales y que consiguió sortear los sistemas de detección configurados.

El administrador finalmente tendrá la posibilidad de reforzar la seguridad de su red impidiendo toda ejecución de software desconocido o, por el contrario, balancear de forma muy sencilla el nivel de bloqueo en favor de una mayor flexibilidad a la hora de ejecutar ciertos programas no conocidos.

Consulta el capítulo 17 Visibilidad y monitorización del malware para más información

3.5. Fase III: Resolución y respuesta

En caso de infección el administrador tiene que ser capaz de actuar en dos líneas: revertir de forma rápida el estado de los equipos afectados previo a la infección y poder calcular el impacto de la 1infección: si hubo fuga de datos, hasta donde consiguió penetrar el ataque, qué equipos resultaron comprometidos etc. La fase Resolución y respuesta ofrece herramientas para estos dos escenarios

- **Respuesta**

El administrador cuenta con la herramienta de Análisis Forense: todas las acciones ejecutadas por el malware son mostradas para su evaluación, incluyendo el vector de infección (cómo llegó el malware a la red), los intentos de propagación a otros equipos o los accesos al disco duro del usuario para obtener información confidencial y conexiones a equipos externos para su extracción.

Consulta el capítulo 22 Análisis forense para más información sobre el uso de esta herramienta

- **Resolución**

Adaptive Defense 360 cuenta con varias herramientas de resolución, unas manuales y otras automáticas.

Entre las automáticas se encuentra el tradicional módulo de desinfección propio de un antivirus junto a la cuarentena que almacena los elementos sospechosos o eliminados.

Para casos de infecciones debidas a malware avanzado o desinfecciones muy complejas, el administrador podrá utilizar desde la misma consola Web de administración la herramienta independiente especializada en desinfección de Panda Security: **Cloud Cleaner**.

También dispondrá de herramientas de acceso remoto para conectarse a los equipos y realizar cualquier proceso manual que se pueda requerir, en función de las acciones ejecutadas por el malware incluidas en el análisis forense.

Consulta el capítulo 20 Herramientas de resolución para más información

3.6. Fase IV: Adaptación

Una vez realizado el estudio con las herramientas de Resolución y respuesta de la fase anterior y localizadas las causas que propiciaron la infección, el administrador deberá de ajustar la política de seguridad de la empresa para que situaciones equivalentes no vuelvan a producirse.

La fase de Adaptación puede reunir una gran cantidad de iniciativas en función de los resultados revelados por el análisis forense: desde cursos de educación y sensibilización en el correcto uso de Internet para los empleados de la empresa hasta la reconfiguración de los routers corporativos o de los permisos de los usuarios en sus máquinas personales.

Desde el punto de vista del equipo, **Adaptive Defense 360** puede reforzar la seguridad de múltiples maneras:

- **Cambiando la configuración de la protección avanzada.**

Si los usuarios de la empresa tienden a utilizar siempre el mismo software, o algunos de ellos suelen instalar programas de dudosa procedencia, una opción para minimizar el riesgo de estos equipos es implementar el modo Lock de la protección avanzada. De esta forma se limita la exposición al malware en los equipos más problemáticos impidiendo la ejecución de los programas que no sean legítimos.

- **Cambiando de la configuración de la protección antivirus**

Programar un mayor número de análisis o activar la protección de vectores de infección como Web o correo ayudará a proteger los equipos que reciban malware por estas dos vías.

- **Limitando la navegación Web a categorías concretas**

Reconfigurar las categorías accesibles a la navegación limita el acceso a páginas de origen dudoso, cargadas de publicidad y propensas a ofrecer descargas en apariencia inocentes (descarga de libros, programas piratas etc) pero que pueden infectar de malware los equipos.

- **Filtrando la llegada de correo con Phising o Spam**

Un vector muy utilizado para ataques de tipo phising es el correo. Reforzando la configuración del filtrado de contenidos y del filtro antiSpam se limita la cantidad de correo no solicitado que llega a los buzones de los usuarios, reduciendo la superficie de ataque.

- **Bloqueando parcial o totalmente pen drives y otros dispositivos externos**

Otro de los vectores de infección más típicos son las memorias y los módems USB que los usuarios se traen de casa. Limitando o bloqueando completamente su uso evitará la infección por estas vías.

- **Limitando la comunicación de los programas instalados con el Firewall y el Sistema de detección de intrusos (IDS)**

El firewall es una herramienta orientada a reducir la superficie de exposición de los equipos, evitando la comunicación de programas que de por si no son malware pero que pueden suponer una ventana abierta a la entrada del mismo. Si se ha detectado una entrada de malware por programas de tipo chat o P2P, una correcta configuración de las reglas del firewall evitará la comunicación de estos programas con el exterior.

El firewall y el IDS también puede ser utilizado para minimizar la propagación del malware una vez ha infectado el primero de los equipos de la red. Examinando las acciones que desencadenó con la herramienta de Análisis forense se podrán generar nuevas reglas de cortafuegos que limiten la comunicación entre equipos o los protejan de ataques de red.

4. Creación de cuentas Panda

Creación de una cuenta Panda
Activación de la cuenta Panda

4.1. Introducción

La Cuenta Panda ofrece al administrador un mecanismo de creación y acceso seguro a los servicios contratados con Panda Security, frente al método estándar de recepción de credenciales por correo electrónico.

Con una Cuenta panda es el propio administrador quien crea y activa el método de acceso a la consola Web de **Adaptive Defense 360**.

4.2. Creación de una Cuenta Panda

Para crear una nueva Cuenta Panda es necesario seguir el procedimiento descrito a continuación

Recepción del mensaje de correo

- Al adquirir **Adaptive Defense 360** recibirás un mensaje de correo electrónico procedente de Panda Security.
- Haz clic en el vínculo que contiene el mensaje para acceder a la Web desde la que podrás crear la Cuenta Panda.

Figura 5: Creación de una Cuenta Panda

Rellena el formulario

- Rellena con tus datos el formulario mostrado.
- Utiliza el desplegable situado en la esquina inferior derecha si deseas que la página se muestre en otro idioma.
- Accede al acuerdo de licencia y la política de privacidad haciendo clic en el vínculo correspondiente.
- Haz clic en **Crear** cuando hayas terminado para recibir un mensaje de correo electrónico en la dirección especificada en el formulario. Utilizando ese mensaje podrás activar la cuenta.

4.3. Activación de la Cuenta Panda

Una vez creada la Cuenta Panda es necesario activarla. Para ello hay que utilizar el mensaje de correo electrónico que has recibido en la bandeja de entrada de la dirección mail utilizada para crear la Cuenta Panda.

- Ve a la bandeja de entrada y localiza el mensaje.
- Haz clic en el botón de activación. Al hacerlo, se confirmará como válida la dirección proporcionada al crear la Cuenta Panda. En caso de que el botón no funcione, copia en el navegador el enlace que se muestra en el mensaje.
- La primera vez que se acceda a la Cuenta Panda se solicitará una confirmación de contraseña. Después, haz clic en el botón **Activar cuenta**.
- Introduce los datos necesarios y haz clic en **Guardar datos**. Si prefieres facilitar los datos en otra ocasión, utiliza la opción **Ahora no**.
- Acepta el acuerdo de licencias y haz clic en **Aceptar**.

Una vez finalizado con éxito el proceso de activación de la Cuenta Panda te encontrarás en la página principal de Panda Cloud. Desde aquí puedes acceder a la consola Web de **Adaptive Defense 360**. Para ello, utiliza el icono de acceso directo que encontrarás en **Mis servicios**.

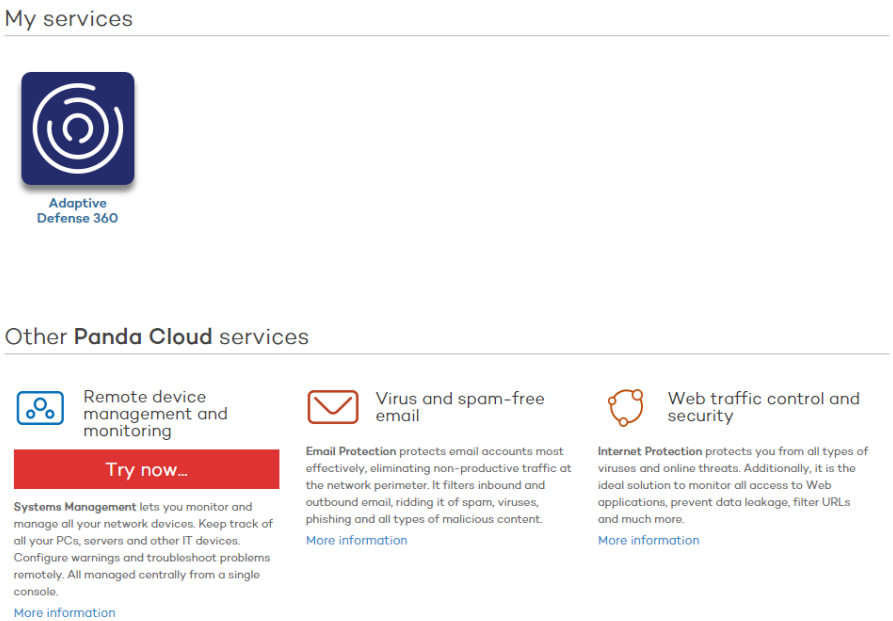


Figura 6: Pantalla de Panda Cloud mostrando los servicios disponibles para la cuenta creada

5. La consola de administración

Estructura general de la consola Web de administración

5.1. Introducción

La consola Web es la herramienta principal del administrador para la gestión de la seguridad. Al tratarse de un servicio Web centralizado posee una serie de características que influirán de forma positiva en la forma de trabajo del departamento de IT:

- **Única herramienta para la gestión completa de la seguridad.**

Con la consola Web el administrador podrá distribuir el software de protección en los equipos de la red, establecer las configuraciones de seguridad, monitorizar el estado de la protección de los equipos y disponer de herramientas de resolución y análisis forense en caso de problemas. Toda la funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y minimizando la complejidad de utilizar varios productos de distintos proveedores.

- **Gestión centralizada de la seguridad para todas las oficinas y usuarios desplazados**

La consola Web está alojada en la nube de forma que no es necesario instalar nueva infraestructura en las oficinas del cliente ni configuraciones de VPNs o redirecciones de puertos en los routers corporativos. Tampoco serán necesarias inversiones en hardware, licencias de sistemas operativos o bases de datos, ni gestión de mantenimientos / garantías para asegurar la operatividad del servicio.

- **Gestión de la seguridad desde cualquier lugar y en cualquier momento**

La consola Web de administración es de tipo responsive / adaptable con lo que se ajusta al tamaño del dispositivo utilizado para la gestión de la seguridad. De esta manera el administrador de la red podrá gestionar la seguridad desde cualquier lugar y en cualquier momento mediante un smartphone, un notebook o un PC de escritorio.

5.1.1 Requisitos de la consola Web

La consola Web es accesible a través de la siguiente URL:

https://www.pandacloudsecurity.com/PandaLogin/

Para acceder a la consola Web de administración es necesario cumplir con el siguiente listado de requisitos:

- Contar con unas credenciales validas (usuario y contraseña).

Consulta el capítulo 4 Creación de cuentas Panda para más información de cómo crear una Cuenta Panda de acceso a la consola Web.

- La última versión de un navegador web compatible:
  - Chrome
  - Internet Explorer
  - Microsoft Edge
  - Firefox
- Conexión a internet y comunicación por el puerto 443

5.1.2 Federación con IDP

Adaptive Defense 360 delega la gestión de las credenciales en un Proveedor de Identidades (Identity Provider, IDP), una aplicación centralizada responsable de gestionar las identidades de los usuarios.

De esta forma con una única Cuenta Panda el administrador de la red tendrá acceso a todos los productos contratados con Panda Security de forma segura y sencilla.

Consulta la ayuda online del producto para obtener más información sobre IdP

5.2. Estructura general de la consola Web de administración

La consola Web de administración cuenta con recursos que facilitan al administrador una experiencia de gestión homogénea y coherente, tanto en la administración de la seguridad de la red como en las tareas de resolución y análisis forense.

El objetivo es entregar una herramienta sencilla, pero a la vez flexible y potente, que permita empezar a gestionar la seguridad de la red de forma productiva en el menor período de tiempo posible.

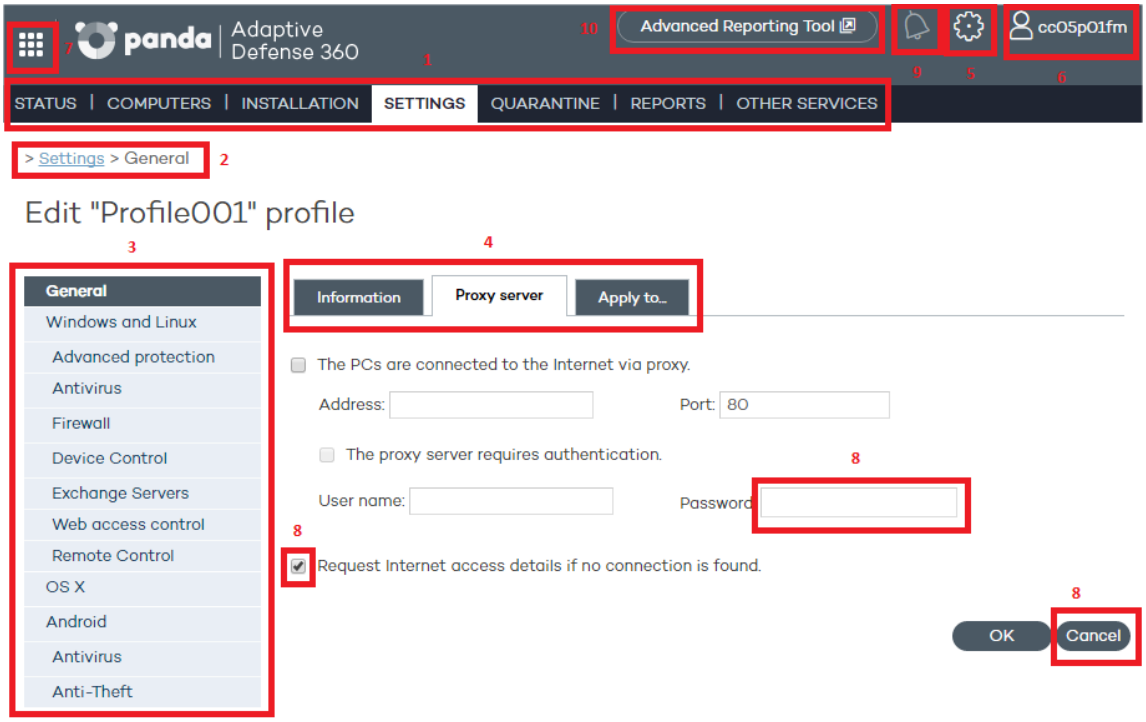


Figura 7: Estructura general de la consola de administración

5.2.1 Menú superior (1)

El menú superior está formado por 7 ventanas, cada una de ellas agrupa recursos y herramientas relacionadas:

- Estado
- Equipos
- Instalación
- Configuración
- Cuarentena
- Informes
- Otros servicios

Ventana Estado

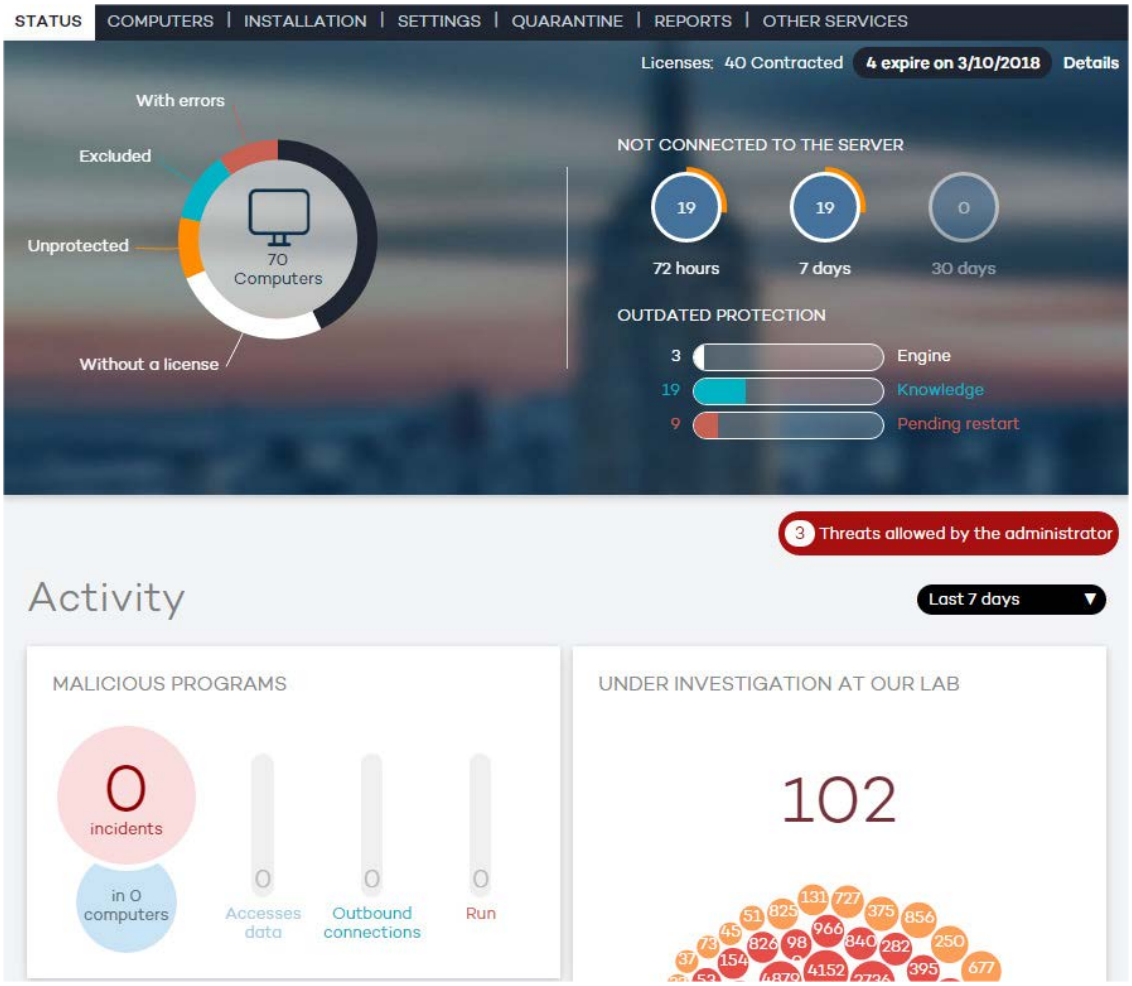


*Figura 8: Ventana **Estado***

La ventana **Estado** es la primera que se muestra una vez que se accede a la consola Web. En ella se detalla información sobre el estado de la protección y sus licencias, utilizando para ello unos contadores que permiten determinar de un vistazo el estado de la seguridad del parque informático.

Si aún no se ha instalado la protección en ningún equipo, se mostrará la ventana **Equipos** con un mensaje invitando a hacerlo y las indicaciones necesarias para ello.

La ventana **Estado** está compuesta por paneles con información gráfica que describe el estado de la seguridad de la red y de licenciamiento de **Adaptive Defense 360**.

Consulta el capítulo 6 Licencias para más información acerca de la gestión de licencias en Adaptive Defense 360. Consulta el capítulo 17 Visibilidad y monitorización del malware y el capítulo 19 Informes para más información acerca del estado de la seguridad de la red en tiempo real y de los informes consolidados

Ventana Equipos

Contiene la información de estado de los equipos de la red. La ventana **Equipos** mostrará un asistente de instalación en caso de que todavía no haya ningún equipo con un agente instalado en la red.

Desde la ventana **Equipos** es también posible agregar agentes, aunque esta tarea se aborda de forma completa en la ventana **Instalación**.

Ventana Instalación

Contiene todas las herramientas necesarias para el despliegue de agentes **Adaptive Defense 360** en la red.

Consulta el capítulo 9 Instalación de la protección para obtener más información acerca del proceso de instalación de los agentes Adaptive Defense 360 en los equipos de la red

Ventana Configuración

Permite la gestión de grupos y perfiles de protección, así como su configuración.

Consulta los capítulos 11 Grupos y 12 Perfiles de para más información sobre la creación de perfiles y grupos, y los capítulos 13, 14 y 15 para la configuración de los perfiles de protección dependiendo de la plataforma a proteger (Windows, Linux, Mac OS X y Android)

Ventana Cuarentena

Contiene un listado de todos los elementos encontrados en la red que **Adaptive Defense 360** ha considerado sospechosos y/o han sido borrados para evitar peligros de infección.

Consulta el capítulo 21Cuarentena para obtener más información

Ventana Informes

Los informes permiten obtener y enviar por correo documentos estáticos consolidados en diversos formatos sobre áreas concretas del servicio de seguridad.

Consulta el capítulo19 Informes para más información

Ventana Otros servicios

Permite ponerse en contacto con el departamento técnico de Panda Security, así como enviar comentarios y sugerencias de mejora del servicio.

5.2.2 Ruta de navegación (2)

La ruta de navegación muestra en todo momento el camino completo de la ventana donde se encuentra el administrador.

Este camino está formado por los nombres de ventanas recorridos hasta llegar a la actual, separadas por el símbolo “>”.

Se utilizan hipervínculos para poder retroceder de forma directa a cualquier punto del camino explorado, sin tener que iniciar el recorrido desde el menú de ventanas superior.

5.2.3 Menú lateral (3)

El menú lateral se muestra en varias ventanas como **Instalación** o **Configuración**. Contiene una serie de entradas que el administrador puede seleccionar para mostrar paneles de configuración adicionales. Al hacer clic sobre estas entradas son agregadas de forma normal a la ruta de navegación tratado en el apartado anterior.

5.2.4 Pestañas (4)

Se utilizan para agrupar elementos comunes de configuración en muchas ventanas de la consola Web. Al hacer clic sobre las pestañas no se añaden a la ruta de navegación.

5.2.5 Botón de configuración general (5)

Muestra un menú desplegable con varias opciones de configuración de carácter general mostradas a continuación:

Usuarios

Permite crear nuevos usuarios de acceso a la consola Web de administración con diferentes niveles de acceso.

Consulta el capítulo 8 Usuarios para más información sobre usuarios y permisos

Preferencias

Agrupa múltiples configuraciones que afectan al comportamiento general de la consola Web:

- **Lenguaje**: permite seleccionar el idioma utilizado en la consola Web de entre los 13 disponibles.
- **Alertas por correo**: permite al administrador recibir alertas por correo directamente desde la plataforma **Adaptive Defense 360** con las detecciones y bloqueos que se producen en cada equipo Windows. Para prevenir aquellos casos en los que el servidor de correo interno de la organización este caído, sea inaccesible por el equipo o simplemente el cliente no disponga de un servidor de correo SMTP, la plataforma **Adaptive Defense** enviará también alertas por correo directamente a la cuenta del administrador sin pasar por el servidor de correo interno de la empresa

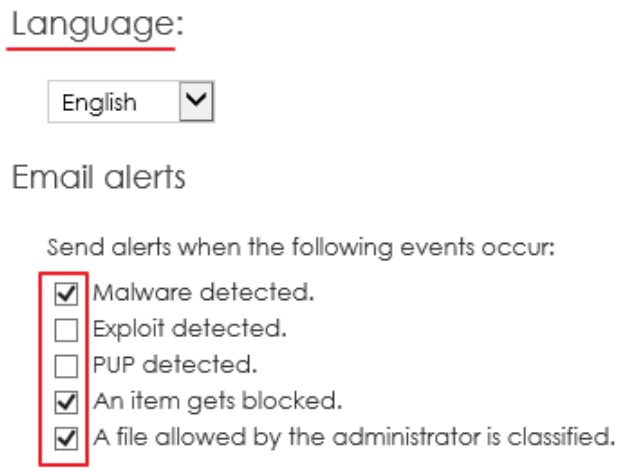


Figura 9: Ventana de configuración de alertas

Las opciones de configuración permiten indicar las condiciones de envío de una alerta por correo:

- **Malware o PUP detectado**: se enviarán como máximo 2 emails por fichero, máquina y día para evitar el bloqueo del buzón del administrador. El envío de mails por malware o PUP detectado se encuentra activado por defecto.
- **Exploit detectado**: se enviarán tantas alertas por correo como detecciones se produzcan, sin limitaciones. El envío de mails por exploit detectado se encuentra activado por defecto
- **Elemento bloqueado**: se enviará 1 email por fichero, máquina y día para evitar el bloqueo del buzón del administrador. El envío de mails por elementos bloqueados se encuentra desactivado por defecto.
- **Clasificación de archivos permitidos por el administrador**: esta alerta aplica únicamente en el caso de que el administrador haya excluido un elemento bloqueado, bien por estar sin clasificar en el momento de la ejecución, bien por estar clasificado como malware. Dado que ésta es una situación de potencial peligro, el sistema enviará una alerta al administrador cuando se haya producido un cambio en la clasificación del elemento excluido. El caso más frecuente es el de una exclusión de un elemento desconocido y bloqueado que **Adaptive Defense** clasifica como malware.

- **Vista por defecto**: determina la forma en que se mostraran los equipos en la consola Web: por su nombre o por su dirección IP.
- **Restricciones de grupo**: permite establecer el número máximo de equipos que pertenecerán a un grupo determinado.
- **Acceso remoto**: permite configurar las credenciales de acceso a los equipos administrados por **Adaptive Defense 360** que tengan alguno de los productos de escritorio remoto soportados instalados (LogMeIn, TeamViewer y VNC). También permite compartir este acceso con el proveedor de servicios para poder delegar la gestión de los equipos.

Acceso remoto permite configurar la integración de Adaptive Defense 360 con herramientas de acceso remoto de terceros compatibles. Adicionalmente Adaptive Defense 360 ofrece el módulo Remote Control como herramienta de resolución que no requiere productos de terceros ni configuración especifica. Consulta con tu comercial para contratar el módulo Remote control de Adaptive Defense 3650. Consulta el documento Remote control Guía para el administrador, para más información

- **Gestión automática de archivos sospechosos**: permite enviar de forma transparente al laboratorio de Panda Security los archivos clasificados como sospechosos para su estudio.

- **Gestión de cuentas**: permite fusionar cuentas y delegar la administración de los equipos.

Consulta el capítulo 7 Gestión de cuentas para más información

Ayuda

Contiene la ayuda contextual de la consola Web. Pulsa F1 para acceder a la ayuda asociada a la pantalla mostrada en la consola Web.

Guía avanzada de administración

Contiene la guía avanzada de administración para su descarga.

Soporte técnico

Permite ponerse en contacto con el departamento técnico de Panda Security para realizar consultas o reportar incidencias.

Buzón de sugerencias

Permite ponerse en contacto con el departamento de producto de Panda Security para enviar comentarios y sugerencias de mejora del servicio.

Acuerdo de licencia

Muestra el EULA del producto

Acerca de

Muestra las versiones de los diversos componentes del servicio.

5.2.6 Usuario logeado (6)

Permite hacer un log out de la consola Web, mostrando la pantalla de IDP (Identity Provider) para hacer login en la consola Web de administración

5.2.7 Botón Panda Cloud (7)

Al pulsar sobre este botón el administrador tendrá acceso a la página de Panda Cloud, donde se muestran de forma rápida todos los servicios que tiene contratados con Panda Security.

5.2.8 Elementos de configuración (8)

La consola Web **Adaptive Defense 360** utiliza controles estándar para introducir configuraciones, como son:

- Desplegables de selección
- Combos de selección

- Botones
- Casillas de activación y desactivación.
- Cuadros de texto

En muchos casos la consola Web realiza un análisis del texto introducido para comprobar que los datos sean correctos (existencia del carácter "@" en cuadros de texto para la introducción de direcciones de correo, comprobación de datos numéricos etc)

Para la navegación de listados **Adaptive Defense 360** utiliza tablas. Todas las tablas tienen una cabecera que permite establecer un criterio de ordenación. Haciendo clic sobre una cabecera se selecciona esa columna como referente ascendente de ordenación de la tabla. Volviendo a hacer clic la ordenación será descendente.

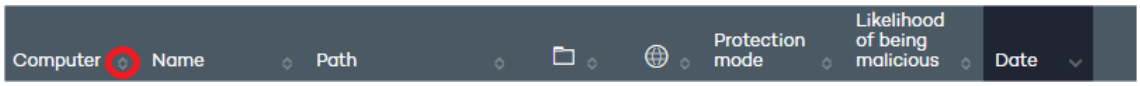


Figura 10: Cabecera de la tabla mostrando los controles de ordenación

La dirección de la flecha indica la dirección aplicada.

En la parte inferior de las tablas se encuentra la herramienta de paginación. Dependiendo del tipo de tabla la funcionalidad de esta herramienta varía:

- Selector del número de líneas por página
- Acceso directo a páginas específicas
- Avance de una página
- Retroceso de una página
- Avance hasta la última página
- Retroceso hasta la primera página

Figura 11: Pie de tabla mostrando los controles de paginación

5.2.9 Notificaciones (9)

El icono de notificaciones incluye un número marcado en rojo con los mensajes urgentes que el sistema necesita entregar al administrador.

Las notificaciones utilizan un código de colores Azul, Naranja y Rojo para indicar la importancia de las mismas.

5.2.10 Acceso al servicio Advanced Reporting Tool (10)

Mediante este botón se accede a la consola Web de administración de Advanced Reporting Tool, un servicio que permite obtener reportes detallados y realizar búsquedas avanzadas sobre las

aplicaciones del parque y la actividad de las mismas.

Consulta la Guía de usuario Advanced Reportingf Tool para más información

6. Licencias

Contratación y renovación de licencias
Estado de las licencias
Asignación y liberación de licencias
Notificaciones por fecha de caducidad de licencias contratas

6.1. Introducción

Para beneficiarse de los servicios de seguridad avanzada es necesario adquirir licencias de **Adaptive Defense 360** para Windows /Linux / Android o de **Adaptive Defense 360** para OS X en caso de requerir protección para equipos de esta plataforma. De acuerdo con las necesidades del parque informático a proteger será necesario instalar las protecciones en equipos, desinstalarlas, eliminar equipos de la lista de equipos protegidos, añadir nuevos equipos a dicha lista, etc.

La utilización que se haga de las licencias tiene su reflejo en el número de licencias disponibles

Las licencias de Adaptive Defense 360 para Windows/Linux/Android pueden ser utilizadas indistintamente en equipos con sistema operativo Windows, Linux o Android.

Si deseas proteger equipos y servidores OS X, deberás adquirir licencias específicas para ello, ya que son independientes de las que se adquieren para equipos con sistema operativo Linux/Windows/Android.

6.2. Contratación y renovación de licencias

Para la puesta en marcha del servicio es necesaria la contratación de licencias en un número igual o superior a los equipos que queramos proteger. Una licencia de **Adaptive Defense 360** es asignada a un único equipo (estación de trabajo o servidor).

Para contratar y/o renovar licencias consulta con tu partner asignado

6.2.1 Mantenimientos

Las licencias se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con las características mostradas a continuación:

- **Producto**: **Adaptive Defense 360**, **Adaptive Defense 360** + Advanced Reporting, Panda Remote Control
- **Contratadas**: número de licencias contratadas en el mantenimiento
- **Tipo:** Trial para licencias de prueba (30 días), o Release
- **Caducidad**: Fecha en la que las licencias caducan y los equipos dejarán de estar protegidos.

Según la plataforma a proteger se generan dos mantenimientos diferentes:

- **Mantenimientos para Windows / Linux / Android**: las licencias contratadas para estas plataformas son intercambiables y pueden ser usadas en cualquiera de ellas
- **Mantenimientos para Mac OS X**: son licencias específicas de equipos OS X

En la parte superior de la consola Web se muestra el número total de licencias contratadas en todos los mantenimientos activos junto con la fecha de caducidad del mantenimiento más próximo en el tiempo y el número de licencias asociadas.

Para visualizar el detalle de los mantenimientos contratados haz clic en la ventana **Estado** y en **Detalles.**

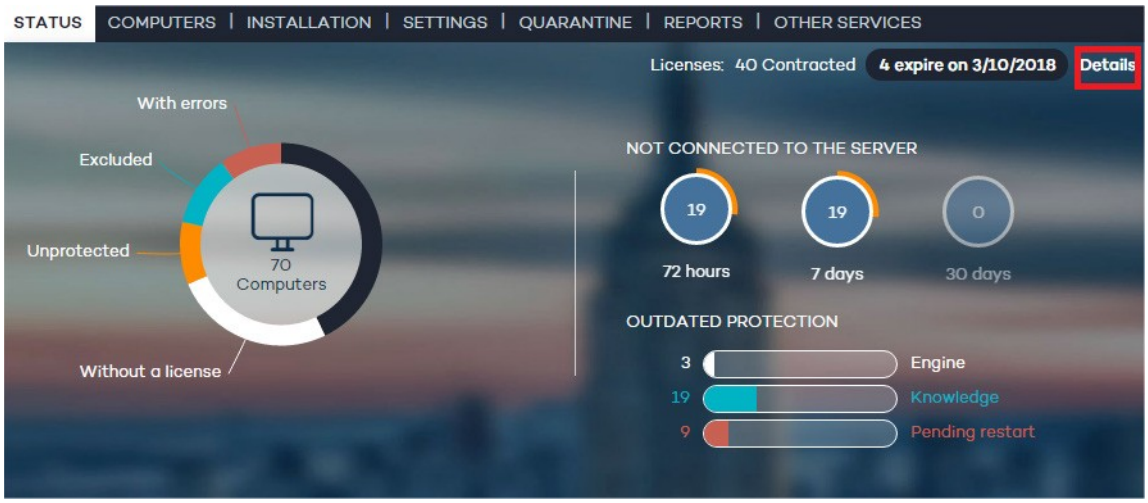


Figura 12: Acceso a la pantalla de Detalles

Se mostrará la ventana Listado de licencias formada por un listado de mantenimientos e información adicional.

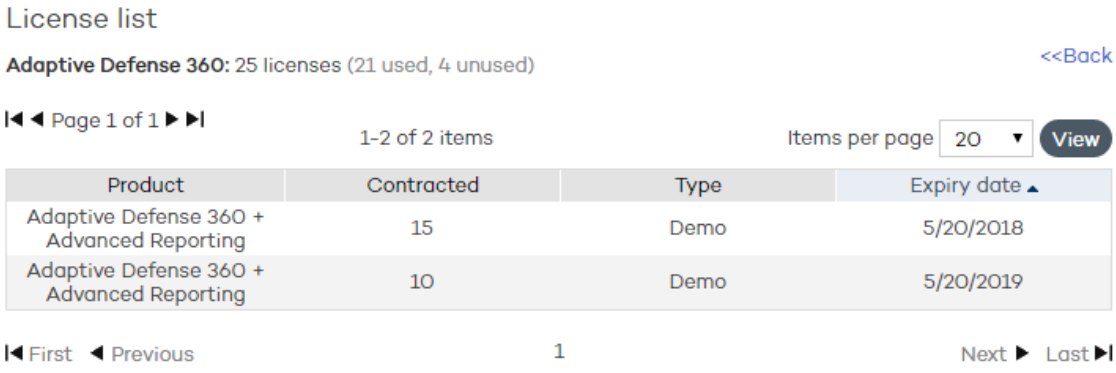


Figura 13: Listado de mantenimientos contratados

En la parte superior se muestra el estado de las licencias repartido en 2 grupos según el tipo:

- **Adaptive Defense 360**: número de licencias contratadas (número de licencias usadas, número de licencias sin usar) número de equipos sin licencia
- **Endpoint Protection for OS X**: número de licencias contratadas (número de licencias usadas, número de licencias sin usar) número de equipos sin licencia

En la parte central se listan los diferentes mantenimientos con sus características. Pasando el puntero

del ratón por encima se mostrará información extendida sobre las características del mantenimiento.

6.3. Estado de la protección

En la ventana **Estado** se incluye el panel de control de **Adaptive Defense 360** donde se refleja el estado actual de los equipos de la red, representado mediante un círculo con distintos colores y contadores asociados.

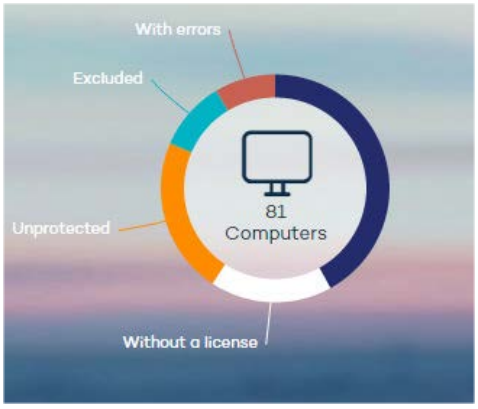


Figura 14: Panel con la distribución por porcentajes del estado de la protección del parque informático

Al pasar el puntero del ratón por encima de cada color se mostrará un tooltip con el número de equipos que coincidan con el criterio mostrado en la leyenda en el gráfico.

Haz clic en las diferentes zonas del panel para mostrar información extendida del estado de las licencias.

Equipos de la red

En la parte central del panel se muestran todos los equipos encontrados en la red del cliente, independientemente de su estado (con licencia válida asignada o no, con errores etc). Este contador incluye también los equipos localizados por la herramienta de descubrimiento.

Haz clic en el contador para mostrar la ventana **Equipos**

Equipos ok

La franja azul del círculo se corresponde con aquellos equipos protegidos, es decir, equipos con una licencia de **Adaptive Defense 360** válida y que no presenten errores en sus protecciones.

Estos equipos consumen licencia

Equipos sin licencia

Los equipos sin licencia son aquellos a los que no se les está aplicando la protección debido a que no se dispone de licencias suficientes para protegerlos, o bien son equipos que pertenecen a un

grupo con una restricción máxima configurada por el administrador.

Haz clic en la zona blanca para mostrar la ventana **Equipos**, pestaña **Sin licencia** con un listado de los equipos que no tienen licencia asignada.

Estos equipos no consumen licencia

Equipos con errores

La franja roja representa a los equipos con errores, equipos con una licencia asignada que completaron la instalación del agente con éxito pero que alguna o todas sus protecciones han dado error.

Estos equipos consumen licencia.

Equipos excluidos

La franja azul representa a los equipos excluidos. En caso de tener un número de licencias contratadas menor que el número total de equipos a proteger, puedes priorizar la asignación de unos equipos frente a otros excluyendo equipos.

Los equipos excluidos son aquellos equipos que el administrador ha determinado que no serán protegidos temporalmente. Los equipos excluidos no compiten por obtener una licencia libre, no se actualizan ni reportan su estado al servidor **Adaptive Defense 360**.

Estos equipos no consumen licencia.

Equipos desprotegidos

Representados por la franja amarilla, son equipos desprotegidos debido a que el proceso de instalación del agente no ha sido completado con éxito, son equipos descubiertos en la red mediante la herramienta de descubrimiento o son equipos cuyo agente ha sido desinstalado.

Estos equipos no consumen licencia.

6.4. Asignación y liberación de licencias

Al Instalar el agente en un equipo, del total de licencias disponibles se restará una licencia de **Adaptive Defense 360** para Windows/Linux/Android o de **Adaptive Defense 360** para OS X, en función del sistema operativo en el que instale la protección de forma automática.

Al eliminar un equipo de la lista de equipos protegidos, al total de licencias disponibles se sumará una licencia de **Adaptive Defense 360** para Windows/Linux/Android o de **Adaptive Defense 360** para OS X, en función del sistema operativo del equipo eliminado y de forma automática.

Al disminuir en X unidades el número de licencias contratadas por caducidad pasarán al estado

Sin licencia tantos equipos Windows/Linux/Android u OS X como licencias del sistema operativo en cuestión hayan disminuido.

Reasignar licencias

En los casos en los que el número de licencias contratadas sea menor que el número de equipos a proteger en la red, este excedente de equipos pasará a formar parte de la pestaña **Sin licencia**. Estos equipos competirán por cualquier incremento de licencias disponibles que se produzca, tal y como se explica en el apartado Contratación y renovación de licencias.

Para evitar que un equipo sin licencia compita por las nuevas licencias contratadas es necesario borrarlo de la consola Web. Para ello, en la ventana **Equipos**, pestaña **Sin licencia** selecciona los equipos y haz clic en el desplegable **Eliminar los equipos seleccionados**.

En el caso de querer liberar la licencia de un equipo correctamente licenciado es necesario excluir el equipo con licencia. En este momento esa licencia quedará libre y será asignada a un equipo de la lista **Sin licencia**.

No se puede utilizar el borrado de un equipo con licencia ya que, en la siguiente comunicación con el servidor, Adaptive Defense 360 volverá a dar de alta al equipo en la consola

6.5. Notificaciones por fecha de caducidad de licencias contratadas

En el área de **Notificaciones** aparecerán diferentes avisos en función de la proximidad de la fecha de caducidad (menos de 60 días); también si se ha superado dicha fecha o si las caducidades dejarían menos licencias disponibles de las usadas actualmente.

Estas notificaciones son independientes en función del sistema operativo que tengan los equipos afectados por la caducidad de la licencia, es decir, se mostrarán por una parte las notificaciones de caducidad de licencias **Adaptive Defense 360** para Windows/Linux/Android, y, por otra, de las de **Adaptive Defense 360** para OS X.

En ambos casos podrás renovar la licencia poniéndote en contacto con el distribuidor habitual o comercial. **Adaptive Defense 360** te lo recordará mediante un mensaje en la ventana **Estado**.

7. Gestión de cuentas

Delegar la gestión de la cuenta
Unificar cuentas

7.1. Introducción

Los usuarios de la consola con permisos de control total pueden acceder a las funcionalidades de gestión de cuentas que **Adaptive Defense 360** pone a su disposición: delegar la gestión de una cuenta y unificar cuentas.

> *Consulta el capítulo 8 Usuarios para obtener información sobre los diferentes tipos de permisos*

Ambas opciones están accesibles en la ventana **Gestión de cuentas**, desde el menú **Preferencias** y haciendo clic en **Gestionar cuentas**.

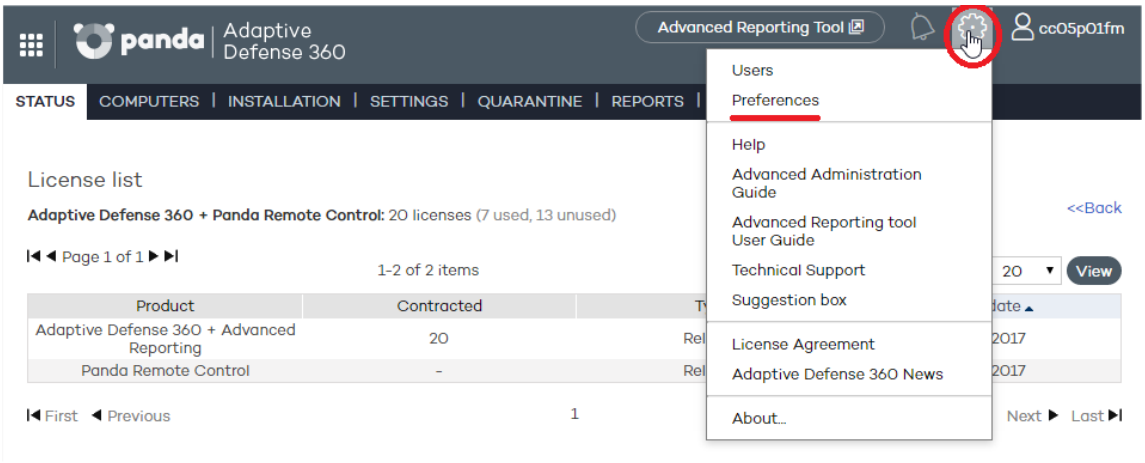


Figura 15: Acceso a la ventana preferencias

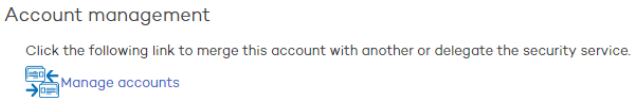


Figura 16: Acceso a la gestión de cuentas

7.2. Delegar la gestión de una cuenta

Esta opción permite que la seguridad de los equipos sea gestionada por un proveedor de servicio (partner) o también modificar el proveedor al que desea encomendar la gestión de la seguridad.

> *Para delegar la gestión de su cuenta en un partner necesitarás el identificador de Panda Security de dicho partner.*

Para ello en el apartado **Delegar seguridad a su proveedor de servicio** introduce el identificador del proveedor que gestionará la seguridad de los equipos.

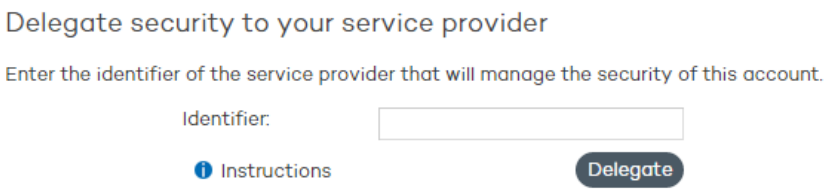


Figura 17: Ventana para introducir el identificador del proveedor de servicios a delegar

7.2.1 Errores posibles al delegar la gestión de una cuenta

Al tratar de activar la funcionalidad de delegación del servicio, pueden aparecer los siguientes errores:

- **El identificador introducido no es válido**. Por favor, revíselo e introdúzcalo de nuevo. Por favor, asegúrate de haber introducido correctamente todos los dígitos del identificador del partner.
- **No dispone de licencias para realizar esta operación**. Contacta con tu distribuidor o comercial habitual para renovarlas. Si las licencias han caducado no podrás acceder a la funcionalidad de delegación de servicio. Por favor, contacta con tu distribuidor o comercial habitual para renovar las licencias.
- **No puede realizar esta operación**. Consulte con su distribuidor o comercial habitual. Es posible que las características de los servicios/licencias que se contrataron no permitan la utilización de la funcionalidad de delegación de servicio. Por favor, consulta al distribuidor o comercial habitual.
- **Ha ocurrido un error y no se ha podido dar de alta la solicitud**. Por favor, inténtelo de nuevo. Este error tiene lugar cuando el proceso falla por un motivo desconocido. Por favor, vuelve a intentarlo y si no consigues realizar la activación del servicio, contacta con el soporte técnico de Panda Security.

7.3. Unificar cuentas

Cuando un cliente tiene productos contratados en varias cuentas, es posible unificarlos en una sola y posibilitar así la gestión centralizada de la seguridad de los equipos. El proceso de unificación o fusión de cuentas consiste en traspasar todos los datos de una cuenta-origen a una cuenta-destino y eliminar la cuenta-origen.

> ***El proceso de traspaso de datos no es inmediato, por lo que puede que transcurra un tiempo hasta que pueda comprobarlo en la consola Web de su cuenta-destino.***

7.3.1 Implicaciones de la unificación de cuentas

Antes de proceder a la unificación de cuentas, es MUY IMPORTANTE tener en cuenta las consecuencias que ello conlleva:

- Los servicios asociados a la cuenta-origen se migrarán a la cuenta-destino y dejarán de estar activos en la cuenta-origen. La cuenta será eliminada y el acceso a la consola Web

de la cuenta-origen será denegado.

- En la consola Web de la cuenta-destino, se mostrarán los datos e informaciones sobre los equipos gestionados desde la cuenta-origen. Para comprobarlo, tan sólo tiene que acceder a la consola Web de la cuenta-destino.
- Se producirá la reasignación automática de las protecciones instaladas en los equipos gestionados desde la cuenta-origen, pasando a ser gestionados desde la cuenta- destino. No será necesario reinstalar las protecciones.

7.3.2 Requisitos para unificar cuentas

A continuación, se muestran los requisitos que han de cumplirse para que el proceso de unificación de cuentas se complete con éxito. Si cualquiera de los requisitos enumerados no se cumpliera el proceso será interrumpido y se mostrará un mensaje de error en la consola.

- La cuenta-origen y la cuenta-destino tienen que tener el mismo producto **Adaptive Defense 360**
- La cuenta-origen y la cuenta-destino tienen que tener la misma versión de **Adaptive Defense 360**
- Ni la cuenta-origen ni la cuenta-destino pueden tener licencias que hayan expirado
- La cuenta-origen y la cuenta-destino tienen que pertenecer al mismo partner
- La cuenta-origen tiene que tener menos de 10.000 licencias. La cuenta-destino sí podrá tener más de 10.000 licencias.
- La cuenta-origen y la cuenta-destino tienen que tener los mismos servicios adicionales contratados.

7.3.3 Pasos para unificar las cuentas

- Accede a la consola Web de la cuenta-origen, la que será dada de baja.
- Haz clic en **Gestionar cuentas** en la ventana **Preferencias**. Se mostrará la ventana **Gestión de cuentas**.
- Selecciona **Unificar**.
- Introduce el Login Email de un usuario que disponga de permiso de control total sobre la cuenta a la que desea traspasar los datos y el número de cliente (identificador) que fue enviado en el mensaje de bienvenida.
- Si estás seguro de que deseas unificar las cuentas, haz clic en **Unificar**.

7.3.4 Efectos de la unificación de cuentas en la configuración del servicio

La unificación de cuentas implica el traslado de información de configuración y datos sobre los equipos gestionados desde la cuenta-origen a la cuenta-destino. A continuación, se muestran los cambios y la información que se añade o se pierde en la cuenta-destino:

- **Licencias**: Se añaden todos los mantenimientos activos y no caducados o en periodo de gracia de la cuenta-origen, es decir, la información sobre las licencias activas, sus fechas de inicio y caducidad, tipo de licencia, etc.
- **Perfiles de configuración**: Se añaden todos los perfiles de configuración de las protecciones de la cuenta-origen. En el caso de que en la cuenta-destino exista un perfil con el mismo nombre (por ejemplo, Perfil Comercial), el perfil procedente de la cuenta- origen será

"renombrado" mediante un sufijo numérico (Perfil Comercial-1).

El perfil por defecto -perfil Default- de la cuenta-origen se traspasará a la cuenta-destino, pero será considerado como un perfil más y perderá la marca de perfil por defecto.

- **Grupos de equipos**: Se añaden todos los grupos de equipos. En el caso de grupos de igual nombre, el funcionamiento será similar al aplicado para los perfiles en el punto anterior.
- **Protección**: Se añade toda la información de las protecciones activas y de las correspondientes a equipos excluidos o sin licencia.
- **Informes**: No se añade a la cuenta-destino la configuración de los informes generados en la cuenta-origen.
- **Estadísticas**: Se incorpora toda la información de detecciones de la cuenta-origen en la cuenta-destino.
- **Cuarentena**: Se pierden todos los elementos en la cuarentena de la cuenta-origen, así como los elementos excluidos de cuarentena y los restaurados.
- **Usuarios**: Se añaden todos los usuarios de la consola Web de la cuenta-origen (con sus correspondientes permisos), excepto el usuario por defecto -Default-.

7.3.5 Posibles mensajes de error al unificar cuentas

Al tratar de unificar dos cuentas, pueden aparecer los siguientes mensajes de error:

- No podemos realizar la operación de unificación porque las cuentas a unificar son de distintos distribuidores. Por favor, contacte con su distribuidor o comercial de Panda Security
- No podemos realizar la operación de unificación porque ambos clientes deben de estar en la misma versión del producto. Por favor, verifique si no tiene pendiente de ejecutar una actualización de versión, si el problema persiste contacte con su distribuidor o comercial de Panda Security para ambos clientes tengan la misma versión
- No podemos realizar la operación de unificación porque ambos clientes no disponen de licencias del mismo producto y/o servicio. Por favor, contacte con su distribuidor o comercial de Panda Security para que ambas cuentas tengas licencias de los mismos productos y/o servicios
- Error, las licencias del cliente origen de la fusión han caducado. Por favor, contacte con su distribuidor o comercial de Panda Security
- No podemos realizar la operación de unificación al tratarse de una operación en la que se ven involucrados un gran número de equipos, sin embargo, la unificación podrá realizarse en Panda Security. Por favor, contacte con el soporte técnico de su distribuidor o de Panda Security.

En el caso de que un cliente tenga varios errores se mostrará únicamente el primer error encontrado. Cuando éste se solucione se mostrará el siguiente error y así sucesivamente hasta que todos los errores hayan sido corregidos.

8. Usuarios

8.1. Introducción

En este capítulo el término "usuario" se refiere a las diferentes cuentas creadas para acceder a la consola Web, y no a los usuarios de la red que trabajan con equipos protegidos por Adaptive Defense 360

La creación de usuarios junto a la asignación de permisos permite repartir las tareas de gestión del servicio **Adaptive Defense 360** entre varios administradores con distintos niveles de acceso según el perfil técnico y responsabilidad que tengan en la empresa.

Toda la configuración de usuarios y permisos se realiza en el menú **Usuarios**

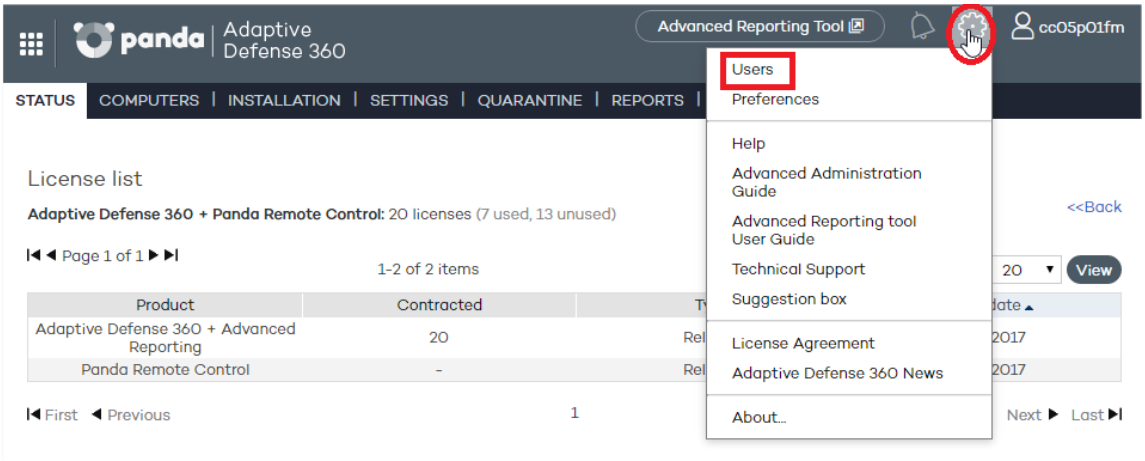


Figura 18: Acceso a la ventana Usuarios

El menú **Usuarios** distribuye la información en tres columnas: **Login Email**, **Nombre** y **Permisos**. A medida que se vayan creando usuarios, éstos aparecerán en el listado, junto al tipo de permisos que les haya otorgado.

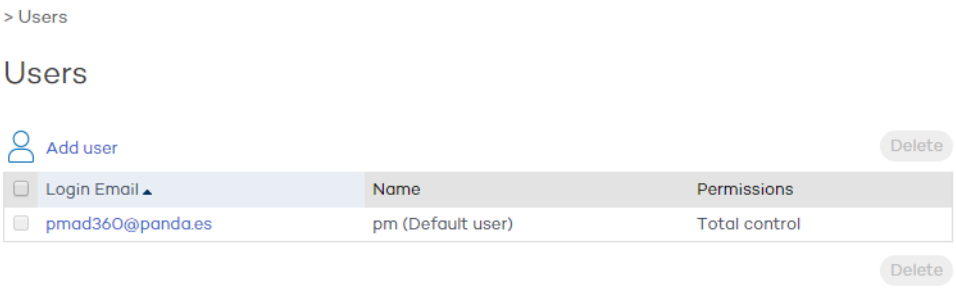


Figura 19: Ventana Usuarios

8.2. Creación de usuarios

Para crear un usuario:

- En el menú **Usuarios**, haz clic en **Añadir usuario**.
- Introduce el **Login Email** y confírmalo.
- Es posible añadir información adicional si así lo deseas, utilizando para ello la caja de texto

Comentarios.

- Selecciona el permiso que deseas asignar al usuario. Para más información consulta el apartado **Tipos de permisos**.
- En **Grupos** selecciona el grupo/subgrupo o grupos/subgrupos sobre los que el usuario podrá actuar, de acuerdo con los permisos asignados. El usuario con permiso de control total podrá actuar sobre todos los grupos.
- Haz clic en **Añadir**. A continuación, se mostrará un mensaje informando del envío de un correo electrónico a la dirección que se ha especificado al crear el usuario.
- Una vez creado el usuario, se mostrará en el listado de la ventana **Usuarios**.

8.3. Modificar los datos del usuario

En el menú **Usuarios**, haz clic en la dirección de correo electrónico del usuario para acceder a la ventana **Edición de usuario**.

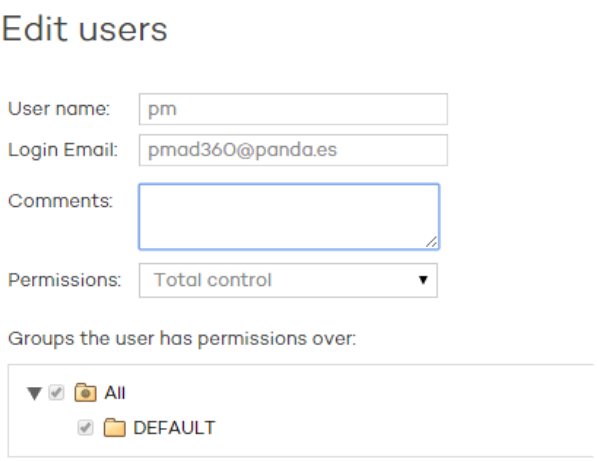


Figura 20: Ventana Edicion de usuario

En esta ventana podrás modificar los comentarios, el permiso y los grupos de equipos a los que tiene acceso, pero no se podrá modificar el Login Email ni el nombre de usuario.

En el caso del usuario por defecto, solo se podrá modificar el campo Comentarios.

Modificar el nombre del usuario

Para cambiar el nombre de un usuario, accede a la consola Panda

Cloud mediante el icono situado en la parte superior izquierda o introduce las credenciales del usuario en la pantalla de login de la consola y haz clic en el nombre del usuario. A continuación, selecciona **Modificar cuenta**.

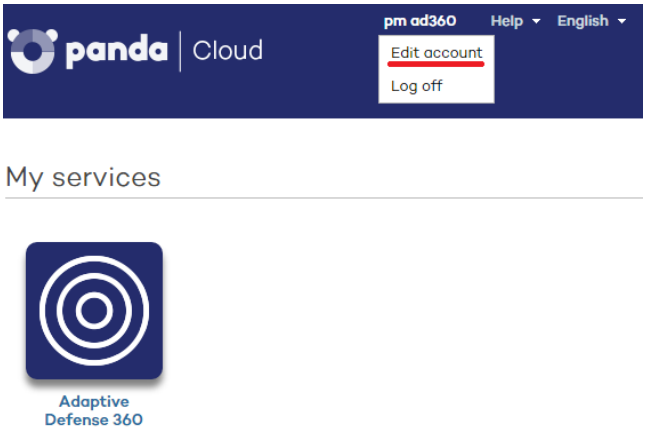


Figura 21: Acceso a la ventana de Edición de la Cuenta Panda

De este modo accederás a la ventana de gestión de la Cuenta Panda, donde puedes modificar los datos de ese usuario y cambiar la contraseña. A continuación, haz clic en **Actualizar**.

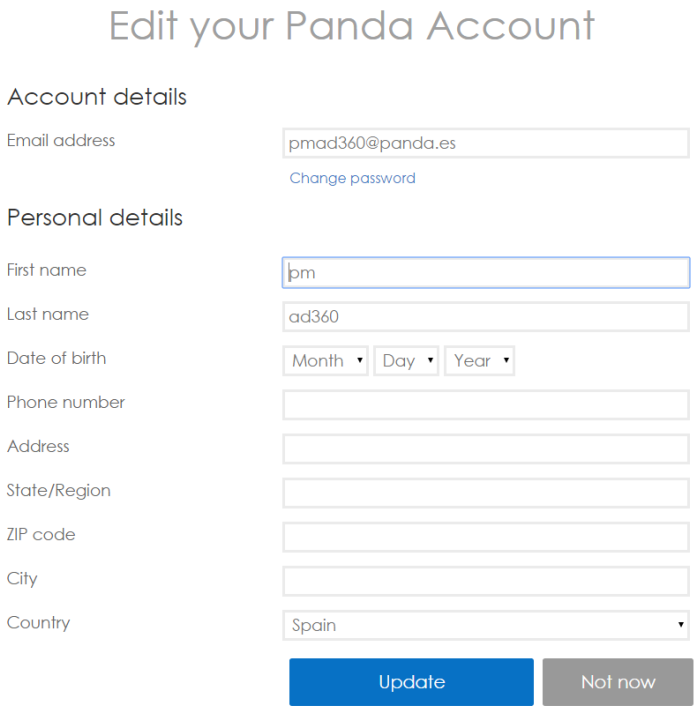


Figura 22: Ventana de Edición de la Cuenta panda

Una vez terminado el proceso ambas consolas Web (**Panda Cloud** y **Adaptive Defense 360**) mostrarán el nuevo nombre del usuario.

8.4. Borrar un usuario

Para eliminar un usuario desde el menú **Usuarios** selecciona en el listado el usuario a borrar y marca la casilla correspondiente que está situada junto al **Login Email** del usuario. A continuación, haz clic en el botón **Borrar**.

8.5. Asignación de permisos a usuarios / grupos

Adaptive Defense 360 permite asignar distintos tipos de acceso para un usuario concreto de la consola sobre uno o más grupos de equipos. De esta forma un usuario únicamente podrá gestionar la seguridad de los equipos que forman parte de los grupos a los que tiene acceso.

Para asignar permisos a grupos edita el usuario y selecciona los grupos a los que pertenecen los equipos que el usuario podrá gestionar su seguridad.

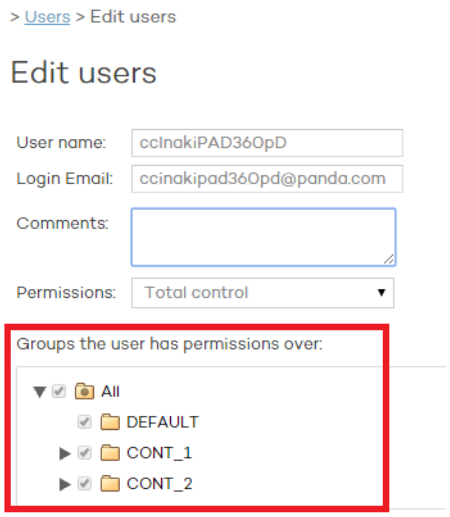


Figura 23: Edición de los grupos accesibles al usuario

8.5.1 Herencia de los permisos aplicados

Al aplicar permisos sobre un grupo específico, todos sus subgrupos heredarán los permisos asignados. Desde ese momento, todos los subgrupos de nueva creación que dependan de ese grupo heredarán de forma automática los permisos asignados al grupo padre.

Si, por el contrario, se asignan permisos a un grupo padre y a algunos de sus subgrupos, pero no a todos, la cadena de herencia se rompe de forma que futuros subgrupos que podamos añadir no heredarán los permisos asignados al grupo padre.

8.6. Tipos de permisos

En **Adaptive Defense 360** se establecen tres tipos de permisos. En función del permiso que se asigne a un usuario, éste podrá realizar mayor o menor número de acciones que afectarán o bien a todos o a algunos equipos y grupos.

Las acciones que el usuario podrá llevar a cabo afectan a diferentes aspectos de configuración básica y avanzada de la protección, y van desde la creación y modificación de sus propias credenciales de usuario y la configuración y asignación de perfiles a grupos y equipos, hasta la generación y obtención de diferentes tipos de informes, entre otros.

Los permisos existentes son:

- Permiso de control total
- Permiso de administrador
- Permiso de monitorización

8.6.1 Permiso de control total

Gestión de usuarios

El usuario puede:

- Ver todos los usuarios creados en el sistema.
- Crear usuarios
- Modificar usuarios
- Eliminar usuarios.

Gestión de grupos y equipos

El usuario puede:

- Crear y eliminar grupos/subgrupos.
  - El permiso de control total sobre un grupo es extensible a todos sus subgrupos.
  - En el caso de que se creen nuevos subgrupos sobre un grupo para el que esté autorizado un usuario con control total, dicho usuario tendrá automáticamente permiso sobre el nuevo subgrupo creado.
- Gestionar la configuración de los perfiles de protección de todos los grupos.
- Asignar equipos a todos los grupos/subgrupos.
- Mover equipos de un grupo/subgrupo a otro.
- Editar el campo **Comentarios** en la pantalla **Detalle de equipos**.
- Acceso remoto a cualquier equipo.

Gestión de perfiles e informes

El usuario puede:

- Copiar perfiles y ver todas las copias realizadas de todos los perfiles.
- Configurar análisis programados de rutas específicas para cualquier perfil.
- Visualizar informes (informes inmediatos, no programados), de cualquier grupo.
- Crear tareas de envío de informes programados sobre cualquier grupo
- Visualizar todas las tareas de envío de informes.

Búsqueda de equipos desprotegidos.

El usuario puede:

- Configurar tareas de búsqueda de equipos desprotegidos.
- Visualizar y/o eliminar cualquiera de las tareas creadas.

Desinstalación de la protección

El usuario puede:

- Configurar tareas de desinstalación de protecciones.
- Visualizar y/o eliminar cualquiera de todas las tareas creadas.

Gestión de licencias y cuentas

El usuario puede:

- Utilizar la opción de Ampliar licencias mediante código de activación.
- Utilizar la opción de Unificar cuentas.
- Delegar la gestión de su cuenta en un partner.

8.6.2 Permiso de administrador

Las acciones que el usuario con permiso de administrador puede llevar a cabo y que tienen que ver con gestión de usuarios, equipos, grupos, configuración y desinstalación de la protección, sólo son aplicables a equipos o grupos sobre los que el usuario administrador tenga permiso o que hayan sido creados por él.

Gestión de usuarios

El usuario puede:

- Crear usuarios
- Eliminar los usuarios que ha creado
- Modificar los usuarios que ha creado
- Ver los usuarios que ha creado.

Búsqueda de equipos desprotegidos

El usuario puede:

- Crear tareas de búsqueda para que equipos de los grupos sobre los que se tienen permisos realicen la búsqueda.
- Visualizar y/o eliminar cualquiera de las tareas de búsqueda de equipos creadas, pero sólo desde equipos pertenecientes a grupos sobre los que tenga permiso.

Gestión de grupos y equipos

El usuario puede:

- Crear grupos/subgrupos, ya sean manuales o automáticos por dirección IP, y gestionar la configuración de los perfiles de los grupos sobre los que tiene permiso. Su permiso es efectivo sobre todos los grupos existentes hasta el grupo hijo seleccionado, es decir, el

usuario administrador no podrá tener acceso a un grupo hijo sin tenerlo también al grupo padre.

- Eliminar los grupos sobre los que tiene permisos. Sólo se podrán eliminar grupos que no tengan equipos, por lo que antes de eliminar un grupo/subgrupo es necesario asignar o mover sus equipos a otro grupo/subgrupo. Una vez "vaciado" el grupo/subgrupo se podrá proceder a la eliminación.
- Editar el campo **Comentarios** de los equipos sobre los que tenga permisos, en la pantalla **Detalle de equipos**.
- Acceso remoto a aquellos equipos que pertenezcan a grupos/subgrupos sobre los que tenga permiso.

Desinstalación de protecciones

El usuario puede:

- Configurar tareas de desinstalación de protecciones en equipos o grupos sobre los que tenga permiso.
- Visualizar y/o eliminar tareas de desinstalación, pero sólo en equipos pertenecientes a grupos sobre los que tenga permiso.

Gestión de perfiles e informes

El usuario puede:

- Crear perfiles nuevos y visualizarlos.
- Crear copias de perfiles sobre los que tiene permiso y visualizarlos.
- Configurar análisis programados de rutas específicas para perfiles sobre los que tenga permiso o hayan sido creados por él.
- Visualizar informes (informes inmediatos, no programados) que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe.
- Crear tareas de envío de informes programados sobre grupos sobre los que tenga permisos
- Visualizar las tareas de envío de informes que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe. En caso contrario no podrá visualizar la tarea de envío de informes.

8.6.3 Permiso de monitorización

El usuario puede:

- Modificar sus propias credenciales.
- Ver y monitorizar la protección de los grupos/subgrupos que se le asignen.
  - El permiso de monitorización sobre un grupo es extensible a todos sus subgrupos.
  - En el caso de que se creen nuevos subgrupos sobre un grupo para el que esté autorizado un usuario con permiso de monitorización, éste tendrá automáticamente permiso sobre el nuevo subgrupo creado.
- Visualizar los perfiles asignados a grupos/subgrupos sobre los que tenga permiso.
- Visualizar las tareas de búsqueda de equipos protegidos realizadas desde equipos pertenecientes a grupos/subgrupos sobre los que tenga permiso.

- Visualizar las tareas de desinstalación de los grupos/subgrupos sobre los que tenga permiso.
- Visualizar informes (informes inmediatos) de grupos/subgrupos sobre los que tenga permisos.
- Visualizar las tareas de envío de informes que incluyan grupos/subgrupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos/subgrupos que aparezcan en el informe. En caso contrario no podrá visualizar la tarea de envío de informes.

9. Instalación de la protección

9.1. Introducción

La instalación es el proceso que distribuye en los equipos el software necesario para activar el servicio de protección avanzado, la monitorización y la visibilidad del estado de la seguridad de la red.

Es importante instalar la protección en todos los equipos de la red del cliente para evitar brechas de seguridad que más tarde puedan ser aprovechadas por los atacantes mediante malware dirigido específicamente a los equipos vulnerables.

Adaptive Defense 360 ofrece varias herramientas que facilitan la instalación de la protección, estas herramientas están disponibles o no dependiendo de la plataforma destino de la protección.

A continuación, se muestra una tabla con las herramientas incorporadas en **Adaptive Defense 360** y su disponibilidad según la plataforma de destino.

Herramienta	Plataforma			
	Windows	Linux	Mac OS X	Android
Descarga del agente desde la consola	SI	SI	SI	SI
Generación de URL de descarga	SI	SI	SI	SI
Herramienta de distribución centralizada	SI	No	No	No
Búsqueda de equipos desprotegidos	SI	No	No	No

*Tabla 1: Métodos de despliegue de **Adaptive Defense 360** según la plataforma*

9.1.1 Descarga del agente desde la consola Web

Consiste en descargar el paquete de instalación directamente desde la consola de administración. Para ello en la ventana **Instalación** elige la plataforma a proteger: Windows Linux, Android y Mac OS X.

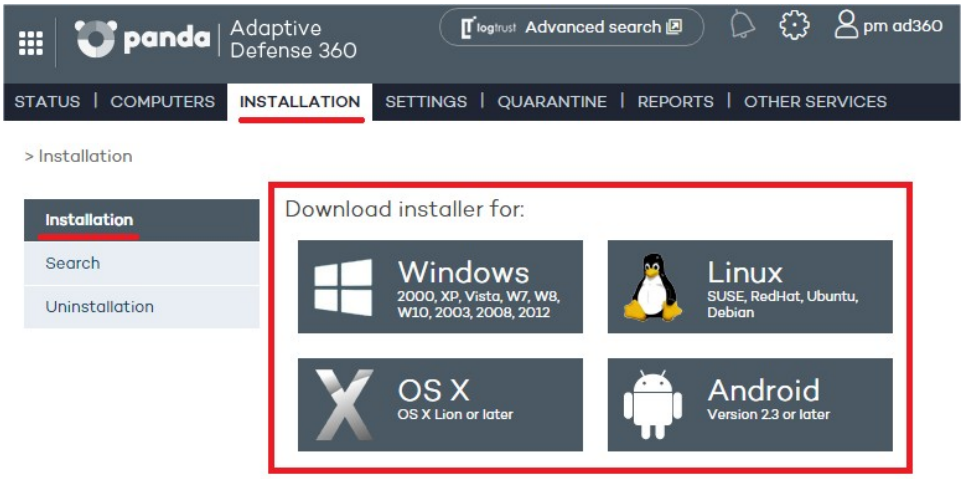


Figura 24: Ventana de selección de agente por plataforma

Haz clic en el icono apropiado para iniciar la descarga del paquete. Aunque este método de instalación es similar para todos los sistemas operativos (Windows, Linux, OS X, Android), consulta más adelante en este mismo capítulo el apartado de instalación correspondiente a cada plataforma, con el fin de conocer a fondo las peculiaridades del proceso de instalación.

Tanto en Linux como en Windows el instalador es el mismo para plataformas de 32 y de 64 bits. Consulta los requisitos que los equipos y dispositivos deben cumplir antes de descargar el instalador.

9.1.2 Generación de URL de descarga

Este método permite la creación de una URL de descarga que podrá ser enviada por correo a los usuarios para iniciar una instalación manual en cada equipo.

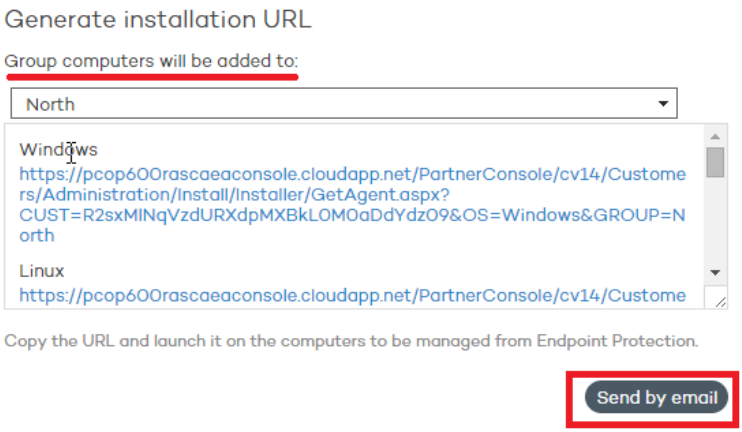


Figura 25: Ventana de URL de descargas

El método de distribución de la URL de descarga es mediante correo con el botón **Enviar por email**.

Para establecer la pertenencia del equipo instalado a un grupo determinado de forma automática en el momento de la instalación selecciona en el desplegable el grupo apropiado. Por defecto la pertenencia estará establecida en el grupo DEFAULT

Automáticamente los usuarios recibirán un correo electrónico con el enlace de descarga

correspondiente a su sistema operativo. Al hacer clic en el enlace, se iniciará la descarga del instalador.

9.1.3 Herramienta de distribución centralizada

La herramienta de distribución permite instalar y desinstalar la protección de forma centralizada en los equipos de la red con sistema operativo Windows, evitando así la intervención manual de los usuarios a lo largo del proceso.

En la ventana **Instalación** haz clic en **Descargar herramienta de distribución remota**. En el cuadro de diálogo de descarga de archivo selecciona **Guardar**, y cuando la descarga haya finalizado ejecuta el archivo desde el directorio en el que se haya guardado. El asistente te guiará a lo largo del proceso de instalación.

Adaptive Defense 360 es compatible además con la instalación centralizada mediante herramientas de terceros como por ejemplo Active Directory de Microsoft.

El funcionamiento de la herramienta de distribución centralizada y la instalación con herramientas de terceros se detallan en el Apéndice I: Herramientas de instalación centralizada

9.1.4 Búsqueda de equipos desprotegidos

Adaptive Defense 360 dispone de un sistema de descubrimiento de equipos que permite que el administrador pueda tener una visión general de cuáles son los equipos de su red que no se encuentran protegidos.

Este sistema se basa en la configuración y ejecución de tareas de búsqueda, que se llevan a cabo desde un "equipo descubridor", que ha de reunir una serie de requisitos para poder actuar como tal:

- Tener instalado el agente y la protección, y estar integrado correctamente en el servidor de **Adaptive Defense 360**
- No deberá de estar en la pestaña de **Equipos excluidos**, en la ventana **Equipos**
- Deberá haberse conectado durante las últimas 72 horas con el servidor de **Adaptive Defense 360**.
- No deberá estar realizando una tarea de desinstalación. El equipo no podrá estar en ninguno de los siguientes estados en una tarea de desinstalación:
  - **En espera**
  - **Iniciando**
  - **Desinstalando**
- Debe disponer de conexión a Internet, ya sea directamente, o a través de otros equipos (funcionalidad 'proxy')

La configuración de las tareas de búsqueda se realiza desde la ventana de **Instalación**, en el menú **Búsqueda**

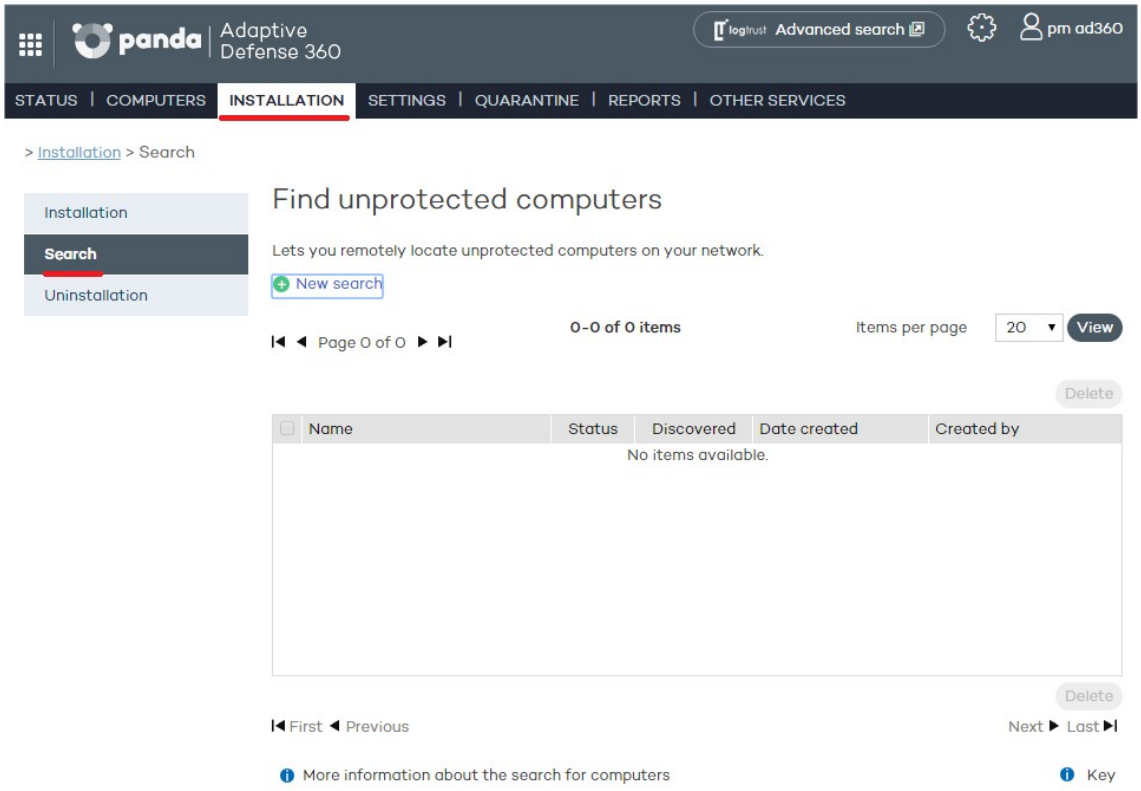


*Figura 26: Ventana de **Búsqueda de equipos sin proteger***

En esta pantalla se muestra un listado de las búsquedas anteriores, editables haciendo clic en cada una de ellas. Haz clic en el botón **Nueva búsqueda** para acceder a una nueva pantalla de configuración de búsquedas.

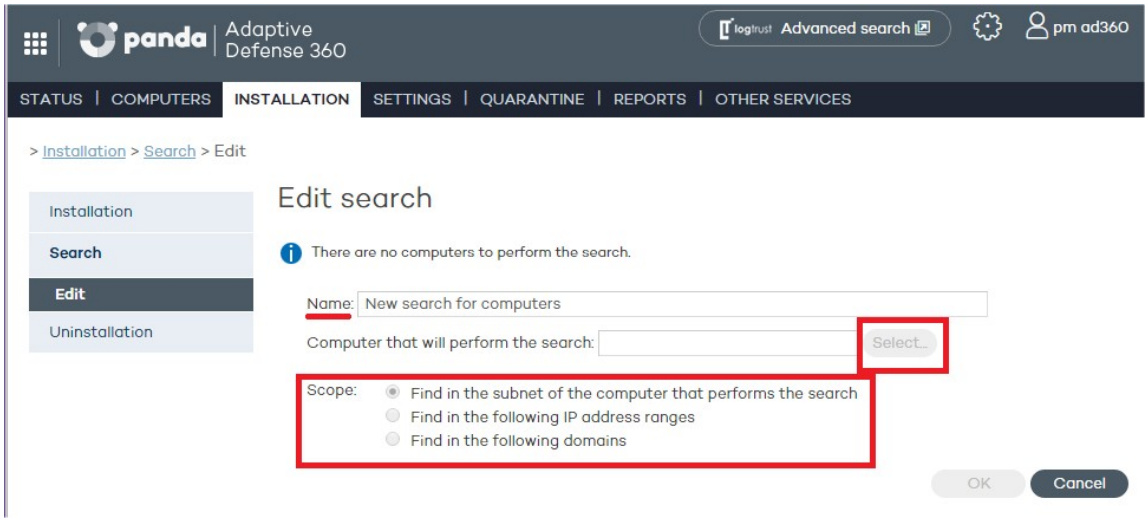


Figura 27: Configuración de una nueva búsqueda de equipos en la red

Proporciona la información para configurar la tarea de búsqueda:

- Nombre de la tarea (de 50 caracteres como máximo)
- No se permite crear tareas con el mismo nombre dentro del mismo cliente
- No se permite la introducción de los siguientes caracteres en el nombre de las tareas <,
- >, “, ‘, &
- Equipo desde donde se lanzará la tarea de descubrimiento de equipos ('equipo

descubridor"), seleccionándolo de la lista de equipos protegidos.

Tipos de búsqueda

Para limitar el alcance del barrido de la red, elige una de las siguientes opciones:

- **La subred del equipo que realiza el descubrimiento (opción seleccionada por defecto)**

Esta opción utiliza la máscara de subred de la configuración TCP/IP del equipo que realiza el barrido para limitar el rango de dispositivos a buscar.

Las búsquedas por subred muestran todos dispositivos encontrados en la red, no solo equipos Windows

- **Uno o varios rangos de direcciones IP (IPv4) introducidos por el usuario**

Si se introducen rangos con direcciones IP en común se realizará el descubrimiento una única vez.

Las búsquedas por rangos de direcciones IP muestran todos dispositivos encontrados en la red, no solo equipos Windows

- **Uno o varios dominios introducidos por el usuario**

La enumeración de equipos pertenecientes a un dominio **Adaptive Defense 360** requiere que el servicio Examinador de equipos de Windows esté funcionando en el equipo que realiza la búsqueda. El servicio localizará al equipo en su segmento de red que tenga el rol de Examinador Principal.

Dependiendo de si la red es un grupo de trabajo o un dominio se distinguen dos escenarios posibles:

- Red con Primary Domain Controller (PDC / BDC) o Active Directory (AD) instalado

El servidor PDC o AD toma el rol de Domain Master Browser y genera una única la lista completa que obtiene de cada Examinador Principal con los equipos encontrados en cada segmento de red. El administrador podrá ver un único listado en la consola **Adaptive Defense 360** con todos los equipos de la red.

- Red sin Primary Domain Controller (PDC / BDC) ni Active Directory (AD) instalado.

Al no existir un equipo que haga las veces de Domain Master Browser el Examinador Principal de cada segmento de red solo contiene la lista de los equipos que pertenecen a ese segmento. El equipo **Adaptive Defense 360** que realiza la búsqueda únicamente obtendrá la lista del segmento al que pertenece.

Para obtener un resultado completo será necesario programar desde la consola Adaptive Defense 360 una búsqueda independiente para cada segmento de red.

Estados de la tarea de búsqueda

- **En espera**: El 'Equipo descubridor' se descargará la orden de descubrimiento del servidor. El servidor tendrá constancia de esta acción y modificará el estado de la tarea.
- **Iniciando**:
  - El 'Equipo descubridor' recalculará la prioridad de la nueva tarea, junto con las tareas que ya estuviesen a la espera de ser ejecutadas. Esperará a que le llegue el turno, según la lógica de prioridades.
  - El 'Equipo descubridor' comprobará que cumple con los requisitos para poder ejecutar la tarea.
  - Se enviará un mensaje al servidor indicando el comienzo de la ejecución de la tarea.
- **En curso**
  - El 'Equipo descubridor' realizará el barrido de la red, en busca de equipos.

Secuencia de la tarea de búsqueda

La secuencia de acciones según el tipo de barrido elegido es la siguiente:

- Por IP (Rangos de IP y Subred)
  - Se hace un ping a cada IP mediante el protocolo ICMP
  - Se espera la respuesta al ping
  - Se intenta resolver el nombre de las IPs que responden
- Por dominio
  - Se enumeran los equipos pertenecientes al dominio
  - Determinar si las máquinas que tenemos en la lista tienen el agente instalado
  - Se envía un mensaje al agente
  - Se espera respuesta

Resultados de la tarea de búsqueda

El equipo descubridor enviará siempre al servidor el listado completo de equipos no protegidos descubiertos, aunque no haya sufrido modificación con respecto al listado enviado anteriormente por el mismo equipo.

El listado de equipos descubiertos contendrá:

- Equipos sin agente instalado.
- Equipos integrados en otra Cuenta Panda: al no ser posible la comunicación con agentes de otras Cuentas Panda no se recibirá respuesta y por lo tanto se asumirá que el equipo no está protegido.

El tiempo de espera de la respuesta será= 3 seg * Número de equipos que han respondido a petición del protocolo ICMP (ping) + 30 seg (margen de seguridad).

Los equipos excluidos no se considerarán equipos no protegidos descubiertos, y por lo tanto NO se incluirán en el listado de equipos descubiertos.

Detalle de los equipos no protegidos

De cada 'Equipo descubierto', se obtendrá:

- Dirección IP, siempre.
- Nombre de equipo, si el 'Equipo Descubridor' fue capaz de resolverlo.

9.2. Visión general del despliegue de la protección

El proceso de instalación comprende una serie de pasos a seguir dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger. Para desarrollar un despliegue con garantías de éxito es necesario elaborar una plantificación que comprenda los puntos enumerados a continuación:

1 Localiza y determina las características y el número de dispositivos desprotegidos en la red

Localiza los equipos Windows que no tienen instalada protección en la red del cliente con la herramienta de **Búsqueda de equipos desprotegidos**.

2 Determina si dispones del número de licencias suficiente para el despliegue

Compara el resultado de la búsqueda, al cual se añadirán todos los dispositivos de plataformas no compatibles con la herramienta de búsqueda (Android, Mac OS X y Linux) que quieras proteger, con el número de licencias libres, teniendo en cuenta las particularidades descritas en el capítulo Licencias.

3 Determina el procedimiento de instalación

Dependiendo del número total de equipos Windows será preferible realizar una instalación con la Herramienta de distribución centralizada o con herramientas de terceros, o por el contrario utilizar la herramienta Generación de URL de descarga para su envío por email al usuario y así efectuar una instalación manual.

4 Verifica si los equipos tienen otro antivirus ya instalado

Para instalar **Adaptive Defense 360** en un equipo en el que ya se encuentra instalada alguna otra solución de seguridad ajena a Panda Security, elige entre instalarlo sin desinstalar la otra protección, de tal manera que ambas soluciones de seguridad convivan en el mismo equipo o, por el contrario, desinstala la otra solución de seguridad y funciona exclusivamente con **Adaptive Defense 360**.

En función del tipo de versión de **Adaptive Defense 360** instalada, el comportamiento por defecto

varía.

Versiones Trials

En versiones de evaluación por defecto **Adaptive Defense 360** se instalará en un equipo que ya dispone de otra solución ajena a Panda Security. De esta forma podrás evaluar **Adaptive Defense 360** comprobando cómo registra amenazas avanzadas que pasan inadvertidas para el antivirus tradicional instalado.

Versiones comerciales

Adaptive Defense 360 no se instalará en un equipo que ya dispone de otra solución ajena a Panda Security. Si **Adaptive Defense 360** dispone del desinstalador de dicho producto, lo desinstalará y a continuación se lanzará la instalación de **Adaptive Defense 360**. En caso contrario, se detendrá la instalación.

> *Consulta la lista de los antivirus que Adaptive Defense 360 desinstala automáticamente en el Apéndice III: Listado de desinstaladores. Si la solución a desinstalar no está en la lista, será necesaria su desinstalación manual.*

Este comportamiento por defecto es configurable tanto en versiones trials como en versiones comerciales desde la ventana de **Configuración / (pulsar sobre el perfil a editar) / Windows y Linux / Opciones Avanzadas**.

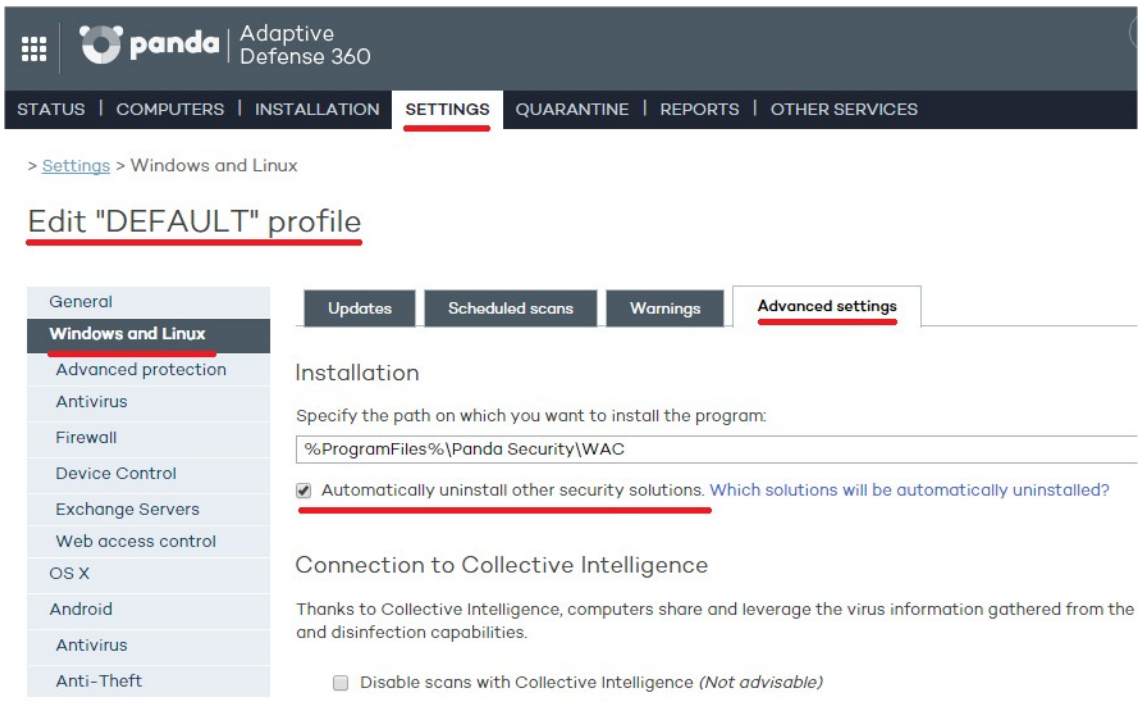


Figura 28: Opción de desinstalación automática de productos de seguridad externos

Productos de protección antivirus de Panda Security

Si el equipo está protegido previamente con Endpoint Protection, Endpoint Protection Plus o Panda

Fusion la protección es actualizada sin necesidad de desinstalar ni reinstalarla.

Si el equipo está protegido previamente con Admin Secure (Panda Security for Business) las reglas a aplicar son las mismas que si se tratara de un antivirus de la competencia.

5 Determina si se cumplen los requisitos mínimos de la plataforma destino

Los requisitos mínimos de cada plataforma se describen más adelante en este capítulo, en la sección correspondiente a cada plataforma.

6 Determina si será necesario el reinicio del equipo para finalizar la instalación

Todos los servicios de protección de **Adaptive Defense 360** excepto el cortafuegos y el sistema de prevención de intrusos (IDS) en plataformas Windows comenzarán a funcionar sin necesidad de reiniciar los equipos. Si se requiere el funcionamiento del cortafuegos será necesario programar una ventana reinicio en los equipos de la red.

Es posible que se requiera un reinicio del cliente o se produzca un pequeño micro corte en la conexión con algunas versiones anteriores de Citrix.

7 Establece si es necesario la instalación en horario no laboral

La instalación de **Adaptive Defense 360** provoca un micro corte de menos de 4 segundos de duración sobre las conexiones establecidas por los programas en funcionamiento en el equipo. Las aplicaciones que no implementen mecanismos para detectar cortes de conexión requerirán un reinicio. Si no es posible este reinicio y además la aplicación no se comporta adecuadamente tras el micro corte, se recomienda la instalación del agente **Adaptive Defense 360** fuera del horario laboral.

Para obtener un despliegue completo es necesario programar desde la consola Adaptive Defense 360 una búsqueda independiente para cada segmento de red.

9.3. Instalación en equipos Windows

La instalación de **Adaptive Defense 360** en dispositivos Windows puede realizarse de forma manual descargando el instalador desde la consola Web o enviado la URL de descarga por correo al usuario, o de forma automática con la herramienta de distribución centralizada, explicada en el Apéndice I: Herramientas de instalación centralizada.

9.3.1 Requisitos de acceso a Internet

Para la correcta instalación y funcionamiento de **Adaptive Defense 360** es necesario permitir el acceso a una serie de URLs desde los equipos donde se instalará el agente de protección.

En caso de que se disponga de un firewall, proxy, o cualquier tipo de restricción en la red, es necesario permitir el acceso a las URLs mencionadas a continuación para el correcto funcionamiento de **Adaptive Defense 360**.

El proceso de instalación clasifica de forma automática las aplicaciones más utilizadas por el usuario en su equipo, sin necesidad de esperar a que sean ejecutadas. El objetivo es agilizar el proceso de clasificación y evitar el bloqueo de aplicaciones en el proceso de arranque del equipo, cuando la red puede no estar disponible. Por esta razón es muy importante que en el proceso de instalación del software Adaptive Defense 360 se satisfagan todos los requisitos de acceso a internet descritos a continuación

Consola Web de administración

- https://www.pandacloudsecurity.com/
- https://managedprotection.pandasecurity.com/
- https://pandasecurity.logtrust.com

Actualizaciones

- http://acs.pandasoftware.com/member/installers/
- http://acs.pandasoftware.com/member/uninstallers/
- http://enterprise.updates.pandasoftware.com/pcop/pavsig/
- http://enterprise.updates.pandasoftware.com/pcop/files/
- http://enterprise.updates.pandasoftware.com/pcop/nano
- http://enterprise.updates.pandasoftware.com/pcop/sigfiles/sigs
- http://acs.pandasoftware.com/free/
- http://acs.pandasoftware.com/sigfiles
- http://acs.pandasoftware.com/pcop/uacat
- http://enterprise.updates.pandasoftware.com/pcop/uacat/
- http://enterprise.updates.pandasoftware.com/updates_ent/
- https://pcopsupport.pandasecurity.com
- http://pcoplinux.updates.pandasecurity.com/updates/nanoupdate.phtml (Linux systems)
- http://pcoplinux.downloads.pandasecurity.com/nano/pavsignano/nano_1/ (Linux systems)
- http://www.intego.com (OS X systems)

Comunicaciones con el servidor

- https://mp-agents-inst.pandasecurity.com
- http://mp-agents-inst.pandasecurity.com/Agents/Service.svc
- https://mp-agents-inst.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-sync.pandasecurity.com/Agents/Service.svc
- https://mp-agents-sync.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-async.pandasecurity.com/Agents/Service.svc
- https://agentscomp.pandasecurity.com/AgentsSecure/Service.svc

- https://pac100pacprodpcop.table.core.windows.net
- https://storage.accesscontrol.pandasecurity.com
- https://prws.pandasecurity.com
- http://beaglecommunity.appspot.com (Panda Cloud Cleaner)
- http://waspproxy.googlemail.com (Panda Cloud Cleaner)

Comunicaciones con los servidores de Inteligencia Colectiva

- http://proinfo.pandasoftware.com
- http://proinfo.pandasoftware.com/connectiontest.html

  Si la conexión con las URLs arriba indicadas no es posible, el producto intentará conectarse a http://www.iana.org.
- https://euws.pandasecurity.com
- https://rpuws.pandasecurity.com
- https://rpkws.pandasecurity.com/kdws/sigs
- https://rpkws.pandasecurity.com/kdws/files
- https://cpg-kw.pandasecurity.com
- https://cpp-kw.pandasecurity.com
- https://cpg-fulg.pandasecurity.com
- https://cpp-fulg.pandasecurity.com
- https://cpg-fusm.pandasecurity.com
- https://cpp-fusm.pandasecurity.com
- https://cpg-fuo.pandasecurity.com
- https://cpp-fuo.pandasecurity.com
- https://ows.pandasecurity.com

Comunicaciones con plataforma Cloud Cleaner

- https://sm.pandasecurity.com/csm/profile/downloadAgent/

Antispam y URL Filtering

- http://*.pand.ctmail.com
- http://download.ctmail.com

Habilita los puertos (intranet del cliente) TCP 18226 y UDP 21226 para una correcta comunicación entre los agentes de comunicaciones de **Adaptive Defense 360**, así como los puertos 443 y 80 en el proxy.

En dispositivos de tipo perimetral, tales como cortafuegos avanzados, que inspeccionan y bloquean comunicaciones en función de su contenido se recomienda agregar reglas adicionales que permitan el tráfico libre a las URLs mencionadas

9.3.2 Requisitos hardware y software

- Procesador: Pentium 1 Ghz
- Memoria RAM: 1 Gbyte
- Espacio para la instalación: 650 MB

- **Estaciones:**

- Sistemas operativos: Windows 10, Windows 8.1, Windows 8, Windows 7 (32 y 64-bit), Windows Vista (32 y 64-bit), Windows XP (32 y 64-bit) SP2 y superior.

- **Servidores**

- Sistemas operativos: Windows Server 2003 (32 y 64 bits) SP1 y superior, Windows Server 2008 (32 y 64 bits)*, Windows Server 2008 R2*, Windows Server 2012 y Windows Server 2012 R2, Windows Multipoint Server 2012.
- Sistemas operativos Windows Core: Windows Server Core 2008, 2008 R2 y 2012 R2

En sistemas operativos Windows Server Core no es necesaria la instalación del GUI para el buen funcionamiento de Adaptive Defense 360. Consulta el capítulo 10 Actualización de la protección para conocer las recomendaciones de actualización relativas a esta familia de sistemas operativos

- Memoria RAM: 1 Gbyte

- **Otras aplicaciones compatibles:**

- VMWare ESX 3.x,4.x, , 5,x y 6.x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x, 9.x, 10.x, 11.x y 12.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008, 2008R2, 2012, 2012R2 y 2016 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer y XenApp 5.x y 6.x

Para distribuir desde la herramienta de distribución a máquinas con Windows server 2008 R2, activa la opción de "Activar la gestión remota del servidor desde otro ordenador" según las instrucciones de Microsoft especificadas en el siguiente artículo: http://support.microsoft.com/kb/976839.

9.4. Instalación en equipos Windows con Microsoft Exchange

9.4.1 Requisitos de acceso a Internet

Los requisitos de acceso a Internet del agente para Windows con Microsoft Exchange son los mismos que los del agente para Windows.

9.4.2 Requisitos hardware y software

Los requisitos de hardware para instalar la protección de Servidores Exchange son los que marca el propio Exchange Server:

- Exchange 2003:

http://technet.microsoft.com/es-es/library/cc164322(v=exchg.65).aspx

- Exchange 2007:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.80).aspx

- Exchange 2010:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.141).aspx

- Exchange 2013

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.150).aspx

- Exchange 2016

https://technet.microsoft.com/es-es/library/aa996719(v=exchg.160).aspx

Las versiones de Microsoft Exchange Server soportadas por **Adaptive Defense 360** son:

- Microsoft Exchange Server 2003 Standard (SP1 / SP2)
- Microsoft Exchange Server 2003 Enterprise (SP1 / SP2)
- Microsoft Exchange Server 2007 Standard (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 Enterprise (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 included in Windows SBS 2008
- Microsoft Exchange Server 2010 Standard (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 included in Windows SBS 2011
- Microsoft Exchange Server 2013 Standard
- Microsoft Exchange Server 2013 Enterprise
- Microsoft Exchange Server 2016 Standard
- Microsoft Exchange Server 2016 Enterprise

Los roles en los que se instala la protección Servidores Exchange en Exchange 2007 y Exchange 2010 son:

- Mailbox
- Hub Transport
- Edge Transport

Los roles en los que se instala la protección Servidores Exchange en Exchange 2013 son:

- Mailbox

Sistemas operativos soportados:

- Exchange 2003: Windows Server 2003 32 bits SP1+ y Windows Server 2003 R2 32 bits
- Exchange 2007: Windows Server 2003 64 bits SP1+, Windows Server 2003 R2 64 bits, Windows 2008 64 bits y Windows 2008 R2
- Exchange 2010: Windows 2008 64 bits y Windows 2008 R2
- Exchange 2013: Windows Server 2012 y Windows Server 2012 R2
- Exchange 2016: Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

9.5. Instalación en equipos Linux

La instalación de **Adaptive Defense 360** en dispositivos Linux se realiza de forma manual descargando el instalador desde la consola Web o enviado la URL de descarga por correo al usuario.

9.5.1 Requisitos de acceso a Internet

Además de las URLs listadas en el apartado Windows, las URLs listadas a continuación deben de ser accesibles desde el agente Linux:

- http://pcoplinux.updates.pandasecurity.com/updates/nanoupdate.phtml
- http://pcoplinux.downloads.pandasecurity.com/nano/pavsignano/nano_1/

9.5.2 Requisitos hardware y software

Distribuciones soportadas

- Ubuntu (32/64 bits) versión 12 o superior
- Red Hat Enterprise (64 bits) versión 6.0 o superior
- Debian Squeeze (32/64 bits)
- OpenSuse (32/64 bits) versión 12 o superior
- Suse Enterprise Server de 64 bits versión 11SP2 o superior
- CentOS 6.x o superior

Prerrequisitos

Para que el producto funcione correctamente el sistema debe cumplir los siguientes requisitos:

- Debe estar instalada la utilidad lsb_release (en RedHat y Debian).
  - En Debian se debe descargar e instalar el paquete:

`lsb-release_3.2-23.2squeeze1_all.deb`

- En RedHat se debe descargar e instalar el paquete:
  `redhat-lsb.i686`

- Dependencias de la protección PavSL (todas las distribuciones). La protección PavSL necesita de la instalación de las siguientes librerías:
  - `libsoup-2.4.so.1` (Librería cliente / servidor HTTP para GNOME)
  - `libgthread-2.0`
  - `libmcrypt.so.4` (Funciones de encriptacion MCrypt)
  - `libz.so.1` (librería de compresión y descompresión zlib)
- Comprobar que en el directorio `/opt/PCOPAgent/PCOPScheduler/pavsl-bin/` se encuentran todas las dependencias de la proteccion PavSL
- AT/CRON se encuentra correctamente instalado y habilitado (en todas las distribuciones). Verifica que los servicios de AT y CRON se encuentran correctamente instalados y activados en los servicios del sistema.
- Es necesario que esté disponible el comando `whiptail` para ejecutar el script de configuración del proxy.

9.6. Instalación en equipos Mac OS X

La instalación de **Adaptive Defense 360** en dispositivos Mac OS X se realiza de forma manual descargando el instalador desde la consola Web o enviado la URL de descarga por correo al usuario.

9.6.1 Requisitos de acceso a Internet

Además de las URLs listadas en el apartado Windows, las URLs listadas a continuación deben de ser accesibles desde el agente Linux:

- mp-agents-inst.pandasecurity.com (OS X systems)
- mp-agents-sync.pandasecurity.com (OS X systems)
- mp-agents-async.pandasecurity.com (OS X systems)
- http://www.intego.com (OS X systems)
- http://www.integodownload.com (OS X systems)
- http://www.netupdate2.intego.com (OS X systems)
- https://www.netupdate2.intego.com (OS X systems)

9.6.2 Requisitos hardware y software

Sistemas operativos soportados

Adaptive Defense 360 soporta los siguientes sistemas OS X:

- Mac OS X 10.6 Snow leopard (Procesador Intel Core 2 Duo o superior)

- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite
- Mac OS X 10.11 El Capitan
- MacOS 10.12 Sierra

Hardware

- Procesador: Intel® Core 2 Duo
- Disco duro: 1.5 GB espacio libre en disco

9.7. Instalación en dispositivos Android

La instalación de **Adaptive Defense 360** en dispositivos Android se realiza de forma manual descargando el instalador desde la consola Web, enviando la URL de descarga por correo al usuario, o mediante un sistema EMM compatible con Android for Work.

La instalación de forma manual y mediante la URL de descarga tienen la particularidad de que, una vez instalado Adaptive Defense en el dispositivo Android, es necesario realizar una tarea adicional para vincular el dispositivo Android con el grupo de equipos en el que se integrará en la consola Web de **Adaptive Defense 360**. De esta forma, la consola Web detecta la existencia del dispositivo y lo reconoce como tal dentro del listado de equipos protegidos.

Instalación enviando la URL de descarga

La instalación se realiza desde el dispositivo Android, mediante una URL de instalación que se envía por correo electrónico.

En la consola Web de **Adaptive Defense 360**, selecciona el grupo en el que desees integrar el dispositivo (por defecto está seleccionado el grupo Default) y haz clic en **Enviar por correo**.

Automáticamente los usuarios recibirán un correo electrónico que contiene dos URL. La primera de ellas es la de instalación. Al hacer clic en ella se muestra la página de **Adaptive Defense 360** de Google Play desde donde podrá realizar la instalación.

Una vez instalada la protección, abre **Adaptive Defense 360** desde el dispositivo y haz clic en la segunda URL que contiene el correo recibido anteriormente.

Instalación desde la consola Web

Se requiere que el usuario acceda a la consola de **Adaptive Defense 360** desde el dispositivo Android y haga clic en el icono de Android del menú Instalación. Una vez allí podrá elegir entre la instalación mediante un código QR o desde la Play Store.

Para leer el código QR es necesaria la instalación de un programa de tipo scanner de códigos QR como por ejemplo Barcode Scanner.

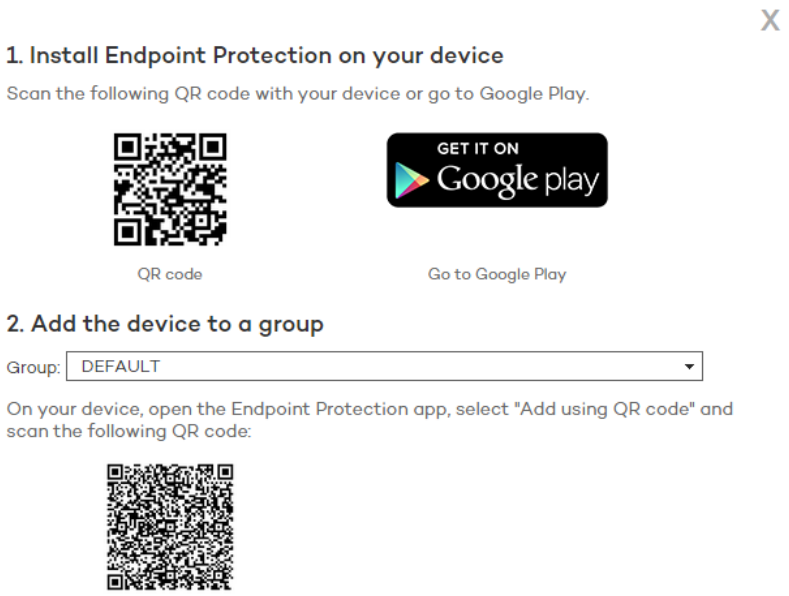


Figura 29: Ventana de instalación para el agente Android

Una vez instalado el agente **Adaptive Defense 360** en el dispositivo Android es necesaria su vinculación a un grupo concreto. Selecciona en la consola el grupo apropiado en el desplegable Grupo y haz clic en **Añadir este dispositivo** al grupo en el dispositivo Android para escanear el segundo código QR mostrado.

Instalación desde un sistema EMM compatible con Android for Work

Un EMM (Enterprise Mobility Management) es un software que, entre otras funcionalidades, permite instalar aplicaciones, localizar y rastrear equipos, administrar dispositivos móviles y sincronizar los archivos de los dispositivos con los de un servidor.

Todas las operaciones se llevan a cabo de forma remota e independientemente de la operadora de telefonía de que se trate o de quién sea el proveedor de servicios.

En el caso de **Adaptive Defense 360**, puedes utilizar un EMM compatible con Android for Work para instalar e integrar la app en los dispositivos Android que deseas proteger.

Para ello, configura dos parámetros en tu EMM:

- **URL de integración**

Introducir la URL que aparece en la pantalla de instalación, dentro de **Generar URL de instalación**, una vez has seleccionado el grupo en el que quieres integrar el dispositivo

- **Nombre automático**

Dependiendo de la selección que hagas (True o False) el nombre que se asignará al dispositivo será diferente. La opción por defecto es False.

- True

Se asignará automáticamente un nombre al dispositivo. Este nombre será el que se mostrará en la consola Web de **Adaptive Defense 360**, y tendrá el siguiente formato:

```
<Modelo de dispositivo>_<identificador único>
```

- False

Introduce el nombre que deseas asignar al dispositivo.

- **Descarga de la app de Adaptive Defense 360**

La app puedes descargarla desde aquí:

https://play.google.com/store/apps/details?id=com.pandasecurity.pcop

9.7.1 Requisitos de acceso a Internet

Además de las URLs listadas en el apartado Windows, las URLs listadas a continuación deben de ser accesibles desde el agente Android:

- https://dmp.devicesmc.pandasecurity.com
- https://pcopsupport.pandasecurity.com
- https://rpuws.pandasecurity.com
- https://rpkws.pandasecurity.com/kdws/sigs
- http://iext.pandasecurity.com/ProyIEXT/ServletIExt

Para que las notificaciones push funcionen correctamente desde la red de la empresa abre los puertos 5228, 5229 y 5230 a todo el bloque ASN 15169 de IPs correspondientes a Google

9.7.2 Requisitos hardware y software

Adaptive Defense 360 es compatible con todos los terminales Android con versión 2.3 Gingerbread y superiores. Se requieren 15 megabytes de espacio en la memoria interna para su funcionamiento.

9.8. Introducción a la instalación mediante generación de imágenes

En redes formadas por equipos muy homogéneos o equipos virtuales, el procedimiento de instalación del sistema operativo y de las herramientas que lo acompañan puede automatizarse.

Esta automatización consiste en generar una imagen base (también conocida como master, imagen gold o imagen "plataforma") instalando en un equipo virtual o físico el sistema operativo ya actualizado, así como todo el software que el usuario vaya a necesitar, incluyendo las herramientas de seguridad. Una vez preparado para funcionar el equipo se extrae una copia del disco duro que se vuelca en el resto de equipos de la red, reduciendo el tiempo de despliegue de forma muy sustancial.

Si el administrador sigue este procedimiento de despliegue automatizado y **Adaptive Defense 360** forma parte de la imagen base, serán necesarios algunos pasos adicionales sobre el procedimiento mostrado para su correcto funcionamiento.

La instalación del software **Adaptive Defense 360** en cualquier equipo lleva asociada la asignación automática de un identificador único que es utilizado por Panda Security para referenciar al equipo en la consola de administración. Si posteriormente se genera una imagen gold con el software **Adaptive Defense 360** ya instalado y se clona en otros equipos, todos los equipos que reciban esa imagen heredarán el mismo identificador de **Adaptive Defense 360**, de forma que la consola únicamente mostrará un equipo.

Para evitar esta situación borra el identificador generado con el programa `reintegra.zip`, descargable de la página de soporte de la web de Panda Security

http://www.pandasecurity.com/spain/support/card?id=500201

En esta página encontrarás instrucciones precisas sobre el procedimiento de instalación del agente **Adaptive Defense 360** en una imagen gold o master.

9.9. Desinstalación de la protección

Adaptive Defense 360 ofrece tres herramientas para la desinstalación de las protecciones instaladas. A continuación, se muestra una tabla con la disponibilidad de cada método según la plataforma a desinstalar.

Herramienta	Plataforma			
	Windows	Linux	Mac OS X	Android
Desinstalación local	SI	SI	SI	SI
Desinstalación con herramienta de distribución centralizada	SI	No	No	No
Desinstalación desde la consola de	SI	No	No	No

administración

*Tabla 2: Métodos de desinstalación de **Adaptive Defense 360** según la plataforma*

9.9.1 Desinstalación local

La desinstalación de **Adaptive Defense 360** se realiza de forma manual desde el panel de control del sistema operativo, siempre y cuando el administrador de la protección no haya establecido una contraseña de desinstalación al configurar el perfil de la protección para su PC. Si lo ha hecho, necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

Consulta el capítulo 13 Perfiles de protección Windows para más información acerca de la contraseña de administrador

En Windows 8 o superior:

- P*anel de Control* > *Programas* > *Desinstalar un programa*.
- También puedes realizar la desinstalación tecleando, en el menú Metro: "desinstalar un programa".

En Windows Vista, Windows 7, Windows Server 2003 y superiores:

- *Panel de Control* > *Programas y características* > *Desinstalar o cambiar*.

En Windows XP

- *Panel de Control* > *Agregar o quitar programas*.

En OS X

- *Finder* > *Aplicaciones* > Arrastre el icono de la aplicación que desea desinstalar a la papelera.

En dispositivos Android:

- Accede a Configuración de Android. *Seguridad* > *Administradores de dispositivos*.
- Desactiva la casilla correspondiente a **Adaptive Defense 360**. A continuación, *Desactivar* > *Aceptar*.
- De nuevo en la pantalla de Configuración de Android selecciona Aplicaciones instaladas. Haz clic en **Adaptive Defense 360** > Desinstalar > Aceptar.

9.9.2 Desinstalación con la herramienta de distribución centralizada

La desinstalación mediante la herramienta de distribución centralizada solo está disponible para equipos Windows.

En la ventana principal de la consola Web, haz clic en **Instalación** y después **Desinstalación centralizada**.

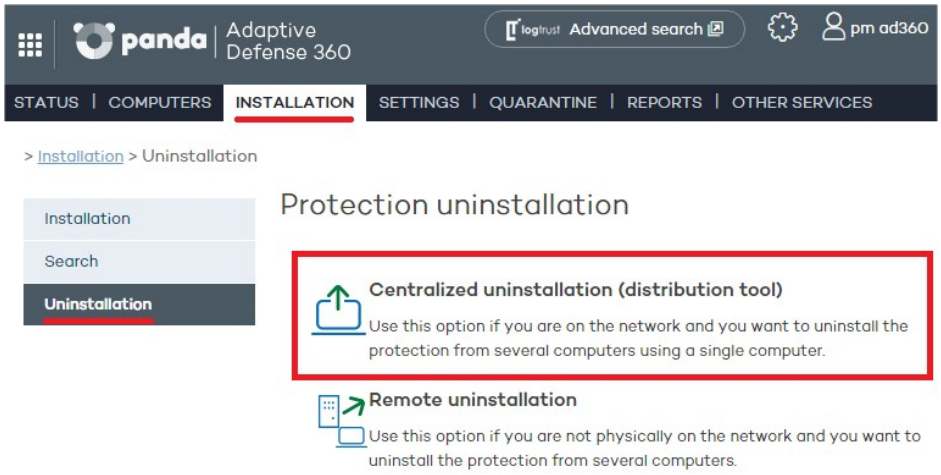


Figura 30: Acceso a la herramienta de desinstalación centralizada

> *Consulta el Apéndice I: Herramientas de instalación centralizada para más información*

9.9.3 Desinstalación desde la consola Web de administración

> *La desinstalación desde la consola de administración solo está disponible para equipos Windows*

Con la desinstalación remota es posible desinstalar la protección desde la consola Web de forma sencilla y eficaz, y sin necesidad de desplazarse hasta el lugar donde se encuentran los equipos. Este tipo de desinstalación supone, por tanto, un abaratamiento en costes y desplazamientos.

El proceso se inicia con la creación y configuración de tareas de desinstalación. Para ello selecciona el grupo y los equipos del grupo a los que afectará la desinstalación, y comprueba cuáles han sido los resultados del proceso de desinstalación accediendo a detalles sobre cada uno de ellos.

Creación de tareas de desinstalación remota

- En la ventana principal de la consola Web, haz clic en **Instalación** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana.
- Selecciona Desinstalación remota.

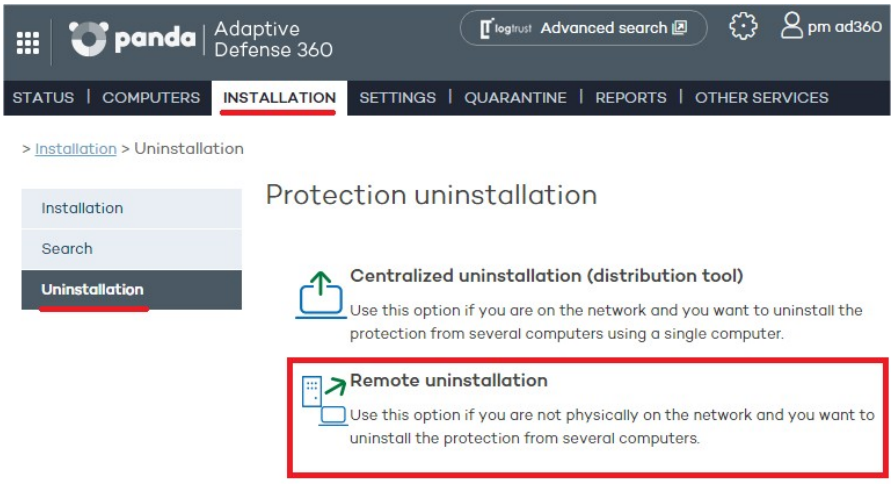


Figura 31: Ventana de desinstalación remota

Para establecer tareas de desinstalación el usuario que accede a la consola de administración debe poseer permiso de control total o administrador. Para más información, consulta el capítulo 8: Usuarios.

- Para establecer una tarea de desinstalación, haz clic en **Nueva desinstalación**. A continuación, en la pantalla **Edición de desinstalación** nombra la tarea y selecciona el grupo en el que están los equipos cuya protección quieres desinstalar. Los grupos mostrados serán aquellos sobre los que el administrador tenga permisos.
- Si el grupo seleccionado tiene aplicado un perfil de configuración que incluye una contraseña de desinstalación, introdúcela en la caja de texto **Contraseña**.
- Selecciona los equipos en el listado de equipos que se muestran en la **pestaña Equipos disponibles,** y haz clic en **Agregar**. Al seleccionarlos, se mostrarán en la pestaña **Equipos seleccionados.**

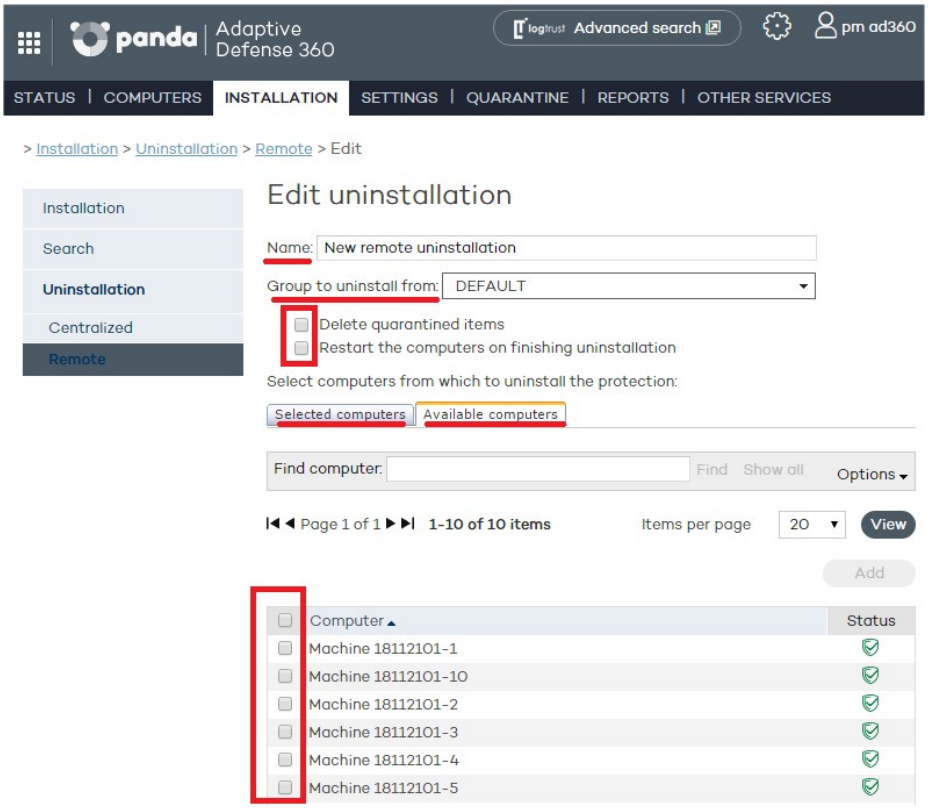


Figura 32: Ventana de selección de equipos para desinstalar

Visualización del desarrollo de la instalación remota.

Las tareas de desinstalación aparecerán listadas en la pantalla **Desinstalación remota.** Para eliminarlas haz clic en **Eliminar**.

En esta pantalla la información se organiza en las siguientes columnas:

- **Nombre**: muestra el nombre que se ha dado a la tarea de desinstalación cuando se ha creado.
- **Estado**: indica mediante iconos el estado en que se encuentra la tarea de desinstalación.
- **Protecciones desinstaladas**: detalla el número de protecciones desinstaladas.
- **Fecha creación**: fecha en que se creó la tarea de desinstalación. Creado por: usuario que creó la tarea de desinstalación.

Según el tipo de permiso del que disponga el usuario de la consola, se podrán crear, visualizar o eliminar tareas de desinstalación de protecciones.

Para ver los detalles de alguna de las desinstalaciones, haz clic sobre el nombre de la desinstalación y accederás a la pantalla **Resultado de la desinstalación**.

Resultado de la desinstalación remota

Al hacer clic en nombre de una tarea de desinstalación accederás a la pantalla **Resultado de la desinstalación**. Además del nombre y las fechas de comienzo y final de la desinstalación, esta pantalla también proporcionará información sobre los equipos afectados por la desinstalación y el

estado en el que ésta se encuentra.

En el caso de que la tarea esté en estado **En espera**, la fecha de inicio mostrará un guión (-). Lo mismo sucederá con la fecha de fin si la tarea no ha finalizado.

Para consultar la configuración de la tarea de desinstalación haz clic en el vínculo **Ver configuración**.

Incompatibilidad entre tareas de búsqueda de equipos desprotegidos y desinstalación remota

Si un equipo está involucrado en una tarea de desinstalación (**En espera**, **Iniciando**, o **En curso**), no es posible crear otra tarea de desinstalación sobre él ni seleccionarlo como equipo desde el que lanzar búsquedas de equipos desprotegidos.

Si un equipo está ejecutando una tarea de descubrimiento de equipos desprotegidos, no es posible crear una tarea de desinstalación sobre él

10. Actualización de la protección

Actualización de sistemas Windows
Actualización de sistemas Linux
Actualización de sistemas Mac OS X
Actualización de sistemas Android

10.1. Introducción

Adaptive Defense 360 es un servicio cloud gestionado que no requiere por parte del administrador la ejecución de taras relativas a la actualización de los servidores o de la infraestructura de back-end encargada de soportar el servicio de protección; sin embargo, sí es necesaria la actualización de los agentes instalados en los equipos de la red del cliente.

Los elementos instalados en el equipo del usuario son dos:

- Agente de comunicaciones
- Motor de la protección
- Archivo de identificadores

Dependiendo de la plataforma a actualizar el procedimiento y las posibilidades de configuración varían como se indica en la tabla mostrada a continuación:

Módulo	Plataforma			
	Windows	Linux	Mac OS X	Android
Agente de comunicaciones	Bajo demanda			
Protección	Automático y configurable	Local	Automático	Automático
Archivo de identificadores	Automático y configurable	Automático	Automático	Automático

Tabla 3: Tipos de actualización en función de la plataforma

- **Automático y configurable**: la actualización es configurable mediante la consola y el despliegue es remoto.
- **Automático**: la actualización no es configurable pero el despliegue es remoto
- **Local**: la actualización se realiza de forma manual o mediante herramientas de distribución centralizada de terceros.
- **Bajo demanda**: el administrador puede iniciar la actualización cuando esté disponible, pudiendo de esta forma retrasarla hasta el momento que considere oportuno

10.2. Actualización del agente de comunicaciones

La actualización del agente de comunicaciones es común para todas las plataformas y se realiza desde el área **Notificaciones** de la consola de administración.

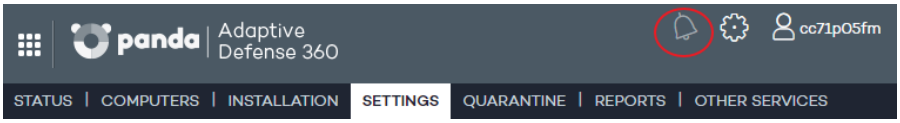


*Figura 33: Acceso al **Area de notificaciones***

Cuando esté disponible una nueva versión se mostrará una notificación invitando al administrador a actualizar el módulo del agente en todos los equipos de la red con **Adaptive Defese 360** instalado.

10.3. Actualización de sistemas Windows

La configuración de las actualizaciones forma parte del perfil de protección asignado al equipo. Para acceder a la configuración haz clic en la ventana **Configuración** y elige un perfil a editar. Después haz clic en **Windows y Linux** y elige la pestaña **Actualizaciones**

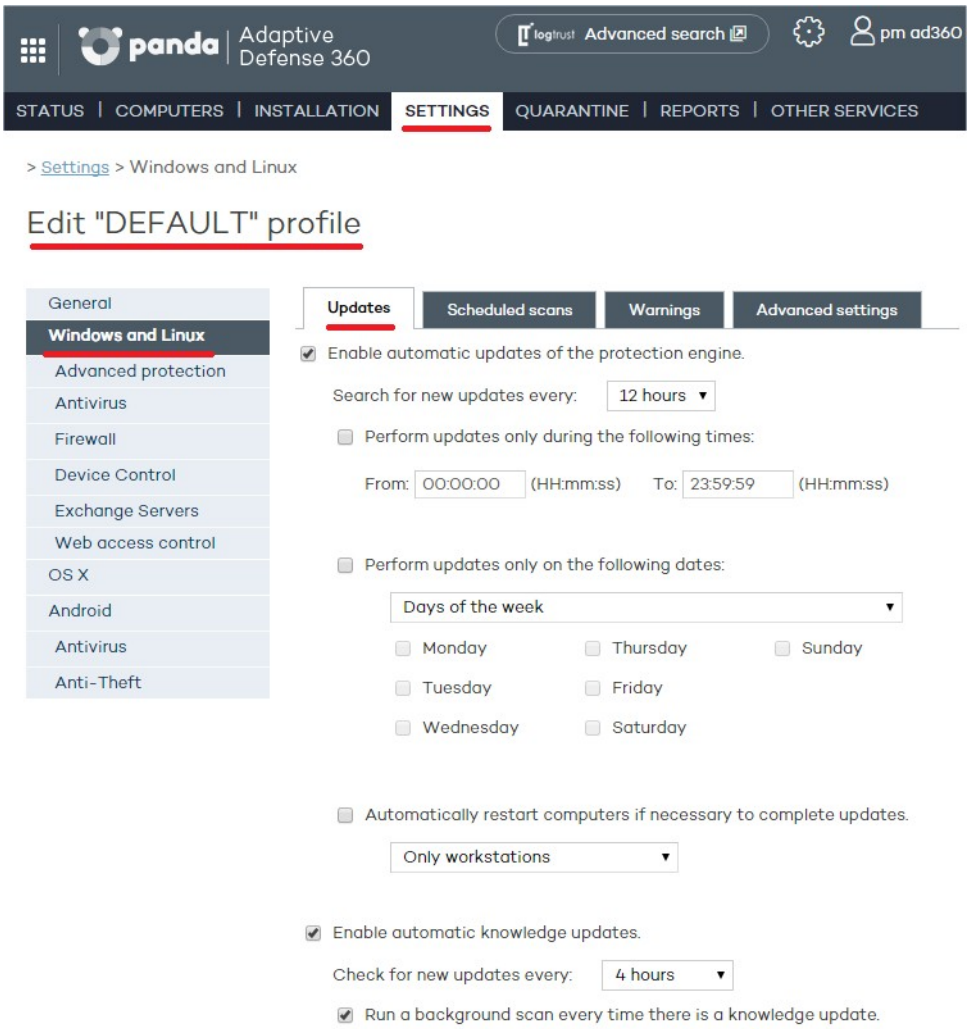


Figura 34: Acceso a la ventana de actualización

10.3.1 Actualización de la protección

- Marca la casilla de activación de las actualizaciones.
- Utiliza el desplegable para establecer cada cuánto tiempo deseas que se busquen nuevas actualizaciones.

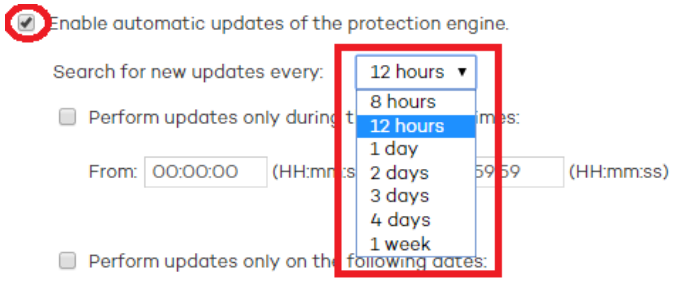


Figura 35: Configuración de la frecuencia de actualización de la protección

- Se puede establecer la fecha en la que tendrán lugar las actualizaciones automáticas y la franja horaria. Selecciona el día o los días de la semana en los que quieres realizar la actualización.

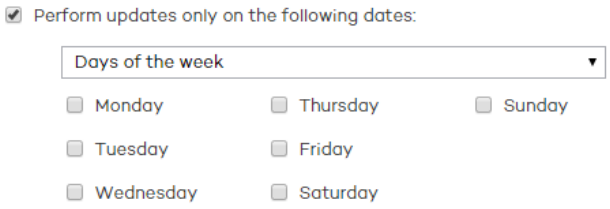


Figura 36: Configuración de la frecuencia de actualización según el día de la semana

- El intervalo de días del mes en los que se realizará la actualización.

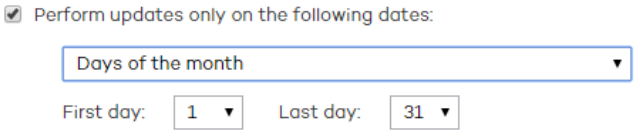


Figura 37: Configuración de la frecuencia de actualización según el mes

- El intervalo de fechas en los que se realizará la actualización.

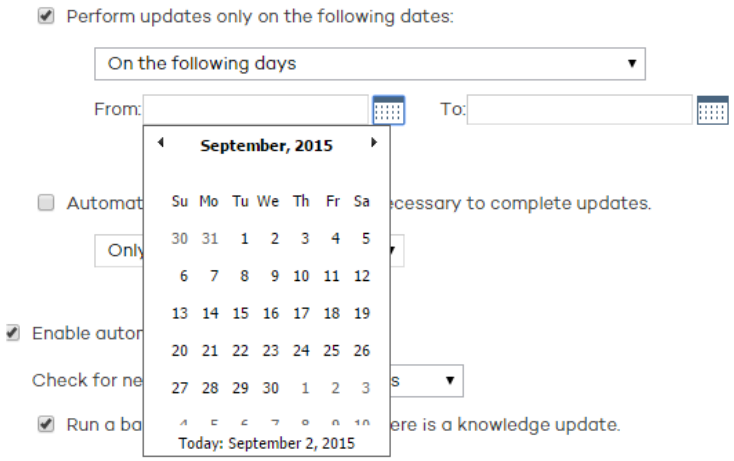


Figura 38: Configuración de la frecuencia de actualización para un intervalo de días

> ***La actualización no se aplicará hasta el reinicio del equipo. Si no se activa la casilla de reinicio automático y el equipo no se reinicia de forma manual pasados 15 días, el agente empezará a mostrar mensajes al usuario para que reinicie el equipo.***

- Indica qué familias de equipos se reiniciarán de forma automática después de aplicar

una actualización.

- Define la franja horaria en la que se realizará la actualización

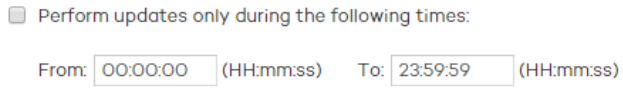


Figura 39: Configuracóon de la franja horaria de actualización

10.3.2 Actualización del archivo de identificadores

- Marca la casilla para activar la actualización automática.
- Selecciona en el desplegable la periodicidad con la que deseas que se realice la búsqueda de actualizaciones.

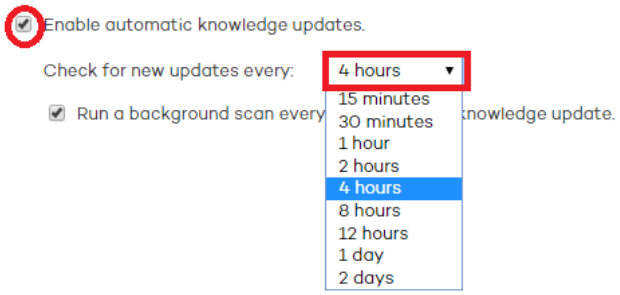


Figura 40: Configuración de la frecuencia de consulta a la nube para buscar un nuevo fichero de firmas

Se recomienda deshabilitar esta opción en entornos virtuales ya que al existir varias máquinas compitiendo por el mismo hardware físico, al actualizarse las firmas en todas ellos se podrían llegar a dar problemas de rendimiento

- Selecciona si es necesario ejecutar un análisis en segundo plano cada vez que el archivo de identificadores se haya actualizado.

10.3.3 Funcionalidad Peer to Peer o Rumor

La tecnología Peer to Peer, también conocida como "rumor", consiste en una funcionalidad de tipo P2P que reduce el consumo de ancho de banda de la conexión a Internet, dando prioridad a que los equipos que ya han actualizado un archivo desde Internet lo compartan con otros que también necesitan actualizarlo. Así se evitan los accesos masivos a Internet y los consiguientes colapsos.

La funcionalidad P2P es de gran utilidad en el despliegue de **Adaptive Defense 360** a la hora de descargarse el programa de instalación. Cuando una de las máquinas ha descargado de Internet el programa de instalación, las otras tienen conocimiento de ello por medio de sus respectivos agentes de comunicación, que han sido activados y han puesto en marcha el proceso de instalación de **Adaptive Defense 360**.

En lugar de acceder a Internet acceden a la máquina que posee el programa de instalación y lo cogen directamente de ella. A continuación, se realiza la instalación.

Esta funcionalidad es también muy útil en el caso de actualizaciones del motor de la protección y del archivo de identificadores, y se implementa en los dos procesos locales que necesitan descargar ficheros de Internet: `WalUpd` y `WalUpg`.

La activación se hace en los ficheros de configuración walupd.ini y walupg.ini, situados en la carpeta `InstallDir` del directorio de instalación de **Adaptive Defense 360**:

```
WALUPD.ini
[GENERAL]
UPDATE_FROM_LOCAL_NETWORK=1
WALUPG.ini
[GENERAL]
UPGRADE_FROM_LOCAL_NETWORK=1
```

La funcionalidad P2P funciona de forma independiente en cada uno de estos procesos locales, pudiendo estar activo únicamente en uno de ellos.

- **Funcionamiento**

Cuando una máquina termina de actualizar los ficheros de firmas o alguna protección (o el propio agente) envía por broadcast la información de los ficheros que tiene disponibles al resto de máquinas de la red.

En cuanto al envío de la información para WALUpg, en caso de ser necesario algún reinicio después de la instalación/actualización de las protecciones, si el usuario opta por no reiniciar el equipo inmediatamente sino más tarde, la información de la funcionalidad P2P se enviará de forma inmediata en lugar de esperar al reinicio.

El funcionamiento se muestra en el siguiente diagrama:

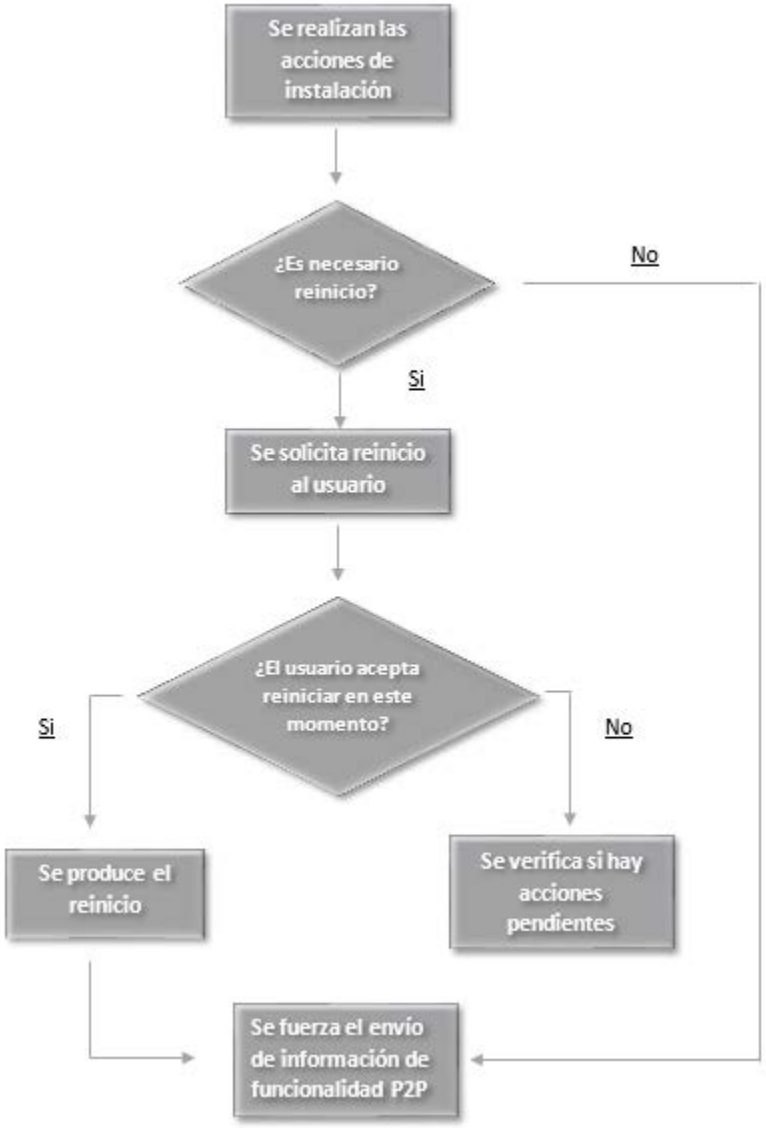


Figura 41: Esquema de funcionamiento de la tecnología rumor

Las máquinas que reciben el mensaje guardarán la información que han recibido para utilizarla cuando la necesiten.

Si una máquina necesita algún fichero, antes de intentar descargarlo de Internet comprobará si puede obtenerlo de otra máquina. Si es así enviará un mensaje a la máquina que lo tiene disponible para solicitárselo. El fichero se recibirá de forma asíncrona y se esperará un tiempo máximo a recibirlo antes de reintentar.

La máquina que tiene el fichero recibirá un mensaje de solicitud y como respuesta enviará un mensaje con el fichero.

La máquina que pidió el fichero lo recibirá y podrá proseguir con la actualización o upgrade.

10.4. Actualización de sistemas Windows Core

Debido a la ausencia de entorno gráfico en los sistemas Windows Server Core, se recomienda realizar la actualización de **Adaptive Defense 360** de forma programada. En el momento de terminar la actualización es necesario el reinicio del servidor para poder completar el proceso, pero como esta petición se realiza mediante la consola local y requiere un entorno gráfico instalado y funcionando, el mensaje no se mostrará y la actualización no se podrá completar.

Una vez programada la actualización se recomienda atender a la consola de administración para comprobar que realmente el servidor se reinició y que la actualización está correctamente instalada.

10.5. Actualización de sistemas Linux

10.5.1 Actualización de la protección

En equipos con sistema operativo Linux no es posible realizar una actualización remota, por lo que cuando exista una nueva versión de la protección ésta deberá instalarse de nuevo en los equipos.

Cuando transcurran 7 días desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos con sistema operativo Linux aparecerán como "desactualizados" en la ventana **Estado**.

10.5.2 Actualización del archivo de identificadores

En equipos con sistema operativo Linux, no es posible configurar la periodicidad de la actualización automática del archivo de identificadores. Se hará siempre cada 4 horas.

10.6. Actualización de sistemas Mac OS X

10.6.1 Actualización de la protección

En equipos con sistema operativo OS X la actualización de la protección se realiza de forma automática, aunque es posible desactivarla desde la consola de administración.

Transcurridas 72 horas desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos se mostrarán como desactualizados en la ventana **Estado**.

10.6.2 Actualización del archivo de identificadores

En el caso de los equipos con sistema operativo OS X, no es posible configurar la periodicidad de la actualización automática del archivo de identificadores, por lo que se realizará cada hora.

Transcurridas 48 horas desde que exista una versión del archivo de identificadores superior a la que los equipos tienen instalada, los equipos se mostrarán como desactualizados en la ventana **Estado**.

10.7. Actualización de sistemas Android

10.7.1 Actualización de la protección

La actualización de la protección Android se publicará en la Google Play y el agente mostrará un aviso de forma automática para que el usuario acepte a la actualización desde el propio terminal.

10.7.2 Actualización del archivo de identificadores

Las actualizaciones del archivo de identificadores se pueden realizar de forma automática. Además, también se puede elegir que estas actualizaciones se realicen exclusivamente por medio de redes Wi-Fi.

11. Grupos

11.1. Introducción

Adaptive Defense 360 permite organizar mediante agrupaciones los equipos de la red con características de protección y seguridad comunes.

De esta forma, en redes de más de 10 PCs es usual crear varios grupos que contengan a todos los equipos con requisitos de seguridad similares, como por ejemplo los PCs de un departamento, los equipos manejados por usuarios de una misma categoría en la empresa o con conocimientos informáticos equivalentes etc.

La creación y gestión de grupos se realiza desde la ventana **Equipos** o desde la ventana **Configuración** mediante los tres iconos situados en la parte inferior del árbol de grupos.

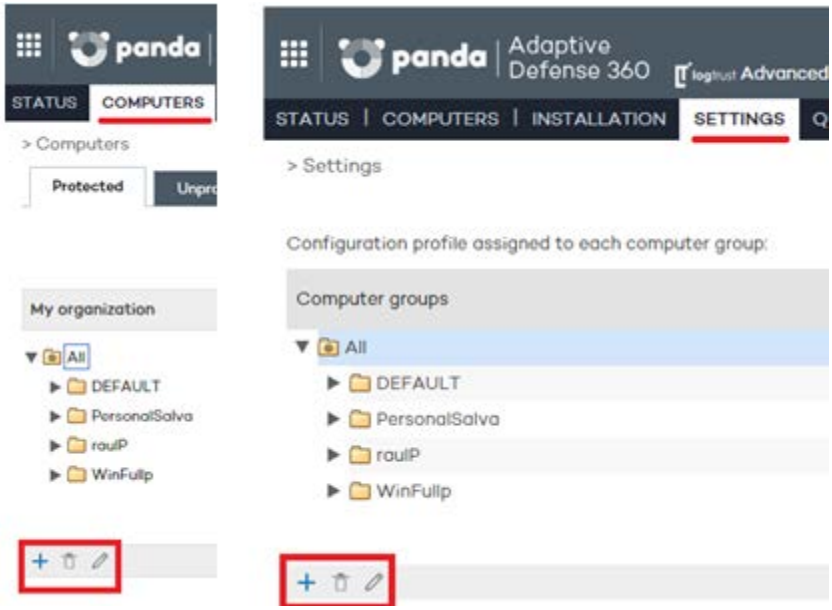


*Figura 42: Creación de grupos desde la ventana **Equipos** y **Configuración***

11.1.1 Pertenencia de un equipo a un grupo

En **Adaptive Defense 360** un equipo únicamente puede pertenecer a un grupo en un momento concreto. La pertenencia de un equipo a un grupo u otro se establece de varias formas:

- En el momento de la instalación del agente en el equipo tal y como se indica en el capítulo 9 Instalación de la protección
- Moviendo de forma manual los equipos desde la consola de administración. Consulta el apartado **Mover equipos de forma manual a un grupo** en este mismo capítulo.
- Moviendo de forma automática los equipos que pertenecen a grupos de tipo automático. Consulta el apartado **Creación de grupos automáticos por IP** y el apartado **Creación de grupos automáticos por Directorio Activo** en este mismo capítulo para configurar reglas que permitan definir de forma automática la pertenencia de los equipos a grupos.

11.2. Árbol de grupos

El árbol de grupos es un recurso accesible desde la ventana **Equipos** y desde la ventana

Configuración y permite observar la jerarquía de grupos y subgrupos creada hasta el momento.

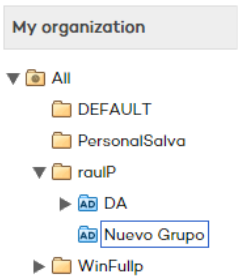


Figura 43: El Árbol de grupos

El nodo padre está situado en la parte superior y de él cuelgan todos los grupos y subgrupos definidos por el administrador. **Adaptive Defense 360** se entrega con un grupo DEFAUL pre generado que, por defecto agrupará a todos los dispositivos con un agente instalado.

El nodo padre recibe el nombre de **Todos** y está representado por el icono .

No se podrá modificar, borrar ni asignar perfiles de protección al nodo padre

Cada nodo del árbol de grupos cuenta con una flecha situada a la izquierda que permite desplegarlo en caso de que contenga subgrupos.

11.3. Tipos de grupos

Grupo manual

Se identifican en la consola Web con el icono

Son grupos de tipo estático: la pertenencia de los equipos a este tipo de grupo no varía a lo largo del tiempo a no ser que el administrador los mueva de forma manual mediante la herramienta **Mover**. Consulta más adelante el apartado **Mover equipos de forma manual**.

Grupo automático por direcciones IP

Se identifican en la consola Web con el icono

Este tipo de grupo está formado por subgrupos y cada uno de ellos lleva asociadas reglas configuradas por el administrador que describen los rangos de IPs de los equipos que contienen. De esta forma, al mover un equipo a un grupo de tipo **Automático por direcciones IP Adaptive Defense 360** consulta la IP del equipo y mueve el equipo de forma automática al subgrupo que concuerde con las reglas definidas en él.

Grupo automático basado en Directorio Activo

Se identifican en la consola Web con el icono

Este tipo de grupo está diseñado para replicar la estructura del Directorio Activo de la organización. Al añadir un equipo a un grupo automático basado en Directorio Activo, **Adaptive Defense 360** creará en la consola Web de forma automática la estructura de subgrupos necesaria para poder mover el equipo al grupo al que pertenece en el Directorio Activo.

11.4. Creación de grupos de tipo manual

- Haz clic en la pestaña **Configuración**.
- Si se quiere crear un subgrupo, selecciona primero el grupo padre en el árbol de grupos.
- Si se quiere crear un grupo de primer nivel, selecciona el grupo padre Todos
- Haz clic en el icono Se mostrará una ventana con los parámetros a configurar

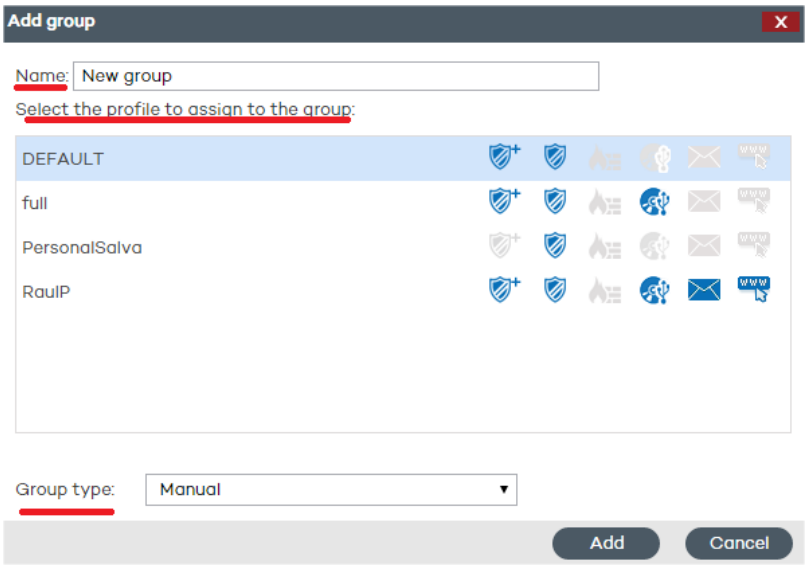


Figura 44: Ventana de creación de grupos

- Introduce el nombre del grupo y selecciona el perfil de protección que deseas asignar al grupo añadido. Para obtener más información sobre perfiles de protección consulta el capítulo 12 Perfiles de protección.

No es posible crear grupos cuyo nombre coincida con el de otro grupo del mismo nivel

- Selecciona el **Tipo de grupo: Manual**.

Haz clic en **Añadir**. El grupo creado se añadirá en el árbol de grupos.

11.5. Creación de grupos automáticos por direcciones IP

El proceso de creación de estos grupos es el mismo que los grupos manuales, pero seleccionando

Automático por direcciones IP en **Tipo de grupo**.

Una vez creado el grupo se mostrará la ventana de edición. Desde esta ventana se podrán crear y configurar las reglas automáticas para el grupo que se acaba de crear.

Figura 45: Controles para la edición de un grupo automático por direcciones IP

Haciendo clic en el icono  se mostrará la pantalla de creación de reglas.

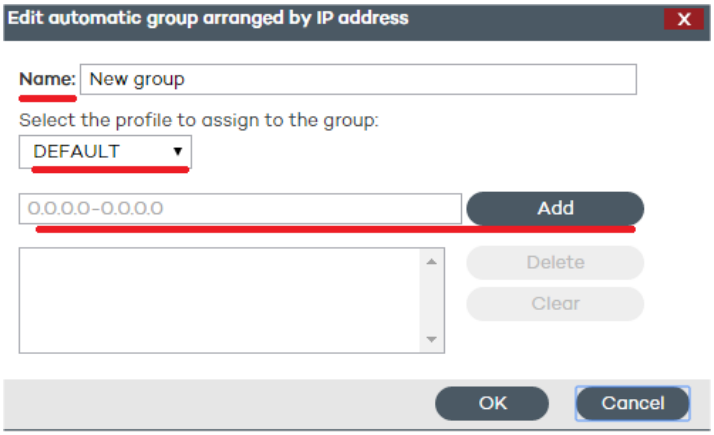


Figura 46: Ventana de edición de grupos

En la pantalla de creación de reglas será necesario especificar:

- El nombre de la regla
- El perfil de protección que se asignará a la regla
- El o los rangos de IPs que forman la regla.

Una vez terminada la configuración haz clic en **Ok**. Cada una de las reglas así creadas genera automáticamente un subgrupo dentro del grupo de tipo **Automático por direcciones IP** creado en el paso previo. Los equipos que pertenezcan a un grupo de tipo **Automático por direcciones IP** se moverán automáticamente al subgrupo apropiado en función de su dirección IP.

11.5.1 Importación desde archivos .csv

A la hora de establecer las reglas automáticas para el grupo, éstas pueden ser importadas desde un archivo .csv. Haz clic en **Importar y Seleccionar** para localizar el archivo .csv en tu disco duro.

Formato del archivo .csv que se desea importar

En cada línea se podrán mostrar de una a tres cadenas de datos separadas por tabulador, en el siguiente orden:

- Ruta del grupo a crear (desde el origen de la importación sin incluir el grupo Todos), por ejemplo: `\Justicia, palacio\sala1`

- Rango de IP, con dos posibilidades: IP-IP o IP-máscara (este campo es opcional)
- Perfil (este campo es opcional)

En el caso de no especificar rango de IP pero sí perfil, habrá que utilizar doble tabulador entre los dos campos visibles (ruta del grupo y perfil):

```
\PalacioJusticia  PJusticia
```

Otros ejemplos:

```
\Hospital\Urgencias\Ambu1     10.10.10.10-10.10.10.19
\Hospital\Urgencias
\Hospital\Urgencias\Ambu2     10.10.10.20-10.10.10.29  PAmbulancia
\Hospital\AmbulatorioAreilza   10.10.20.10/22  PerfilAmbulatorio
\Justicia,Palacio\Segunda Instancia  10.10.50.10/12   Justicia 2
```

Si al importar grupos mediante un archivo .csv la información de alguna de las líneas del fichero no es correcta, se mostrará un error especificando la línea y cadena cuyo formato no es válido. En caso de error en al menos una de las líneas ningún grupo del archivo .csv será importado.

Una vez se hayan importado satisfactoriamente grupos mediante un archivo .csv dentro de un grupo automático por IP, ya no será posible volver a repetir esta acción para ese mismo grupo

11.5.2 Funcionamiento de los grupos automáticos por IP

La clasificación de un equipo que pertenece a un grupo automático por IP y posterior movimiento al subgrupo apropiado según su IP se produce en el momento de la instalación del agente en el equipo. Si posteriormente ese equipo es movido a otro grupo no se realizará una reclasificación.

Los grupos automáticos por IP tienen en cuenta todas las IPs del equipo (equipos con alias de red o varias tarjetas de red físicas), quedándose con la primera coincidencia que se encuentre

La búsqueda de grupo se realiza por nivel y después por orden de creación de grupo. La navegación de los grupos es siempre descendente, si no se encuentra un subgrupo que coincida con ningún criterio definido, el equipo será movido al grupo padre

11.6. Creación de grupos automáticos por Directorio Activo

El proceso de creación de estos grupos es el mismo que los grupos manuales, pero seleccionando **Automático por Directorio Activo** en **Tipo de grupo**.

11.6.1 Replicación de la estructura del Directorio Activo automática

El proceso de generación y actualización de los subgrupos dentro de un **grupo automático por Directorio Activo** en la consola Web se produce de forma automática para cada equipo que pertenezca a este tipo de grupo. La cadena de eventos que se ejecuta es la siguiente:

- El administrador mueve de forma manual el equipo al grupo automático por directorio activo o la pertenencia del equipo a este tipo de grupo queda determinada en su instalación.
- El agente **Adaptive Defense 360** recupera la información de Directorio activo al que pertenece el equipo: Unidad Organizativa, nombre del PC etc.
- Esta información es enviada al servidor **Adaptive Defense 360**. En el servidor se comprueba si el subgrupo equivalente a la Unidad Organizativa existe en la consola:
  - Si no existe se crea de forma automática y se mueve el equipo al subgrupo recién creado. Se le asigna el perfil de protección Default por defecto.
  - Si ya existe el equipo se mueve al subgrupo apropiado.

El árbol de subgrupos que cuelga de un grupo automático por directorio activo se actualiza de forma automática en el caso de que equipos que ya pertenecían al mismo se muevan otras Unidades Organizativas del Directorio Activo: **Adaptive Defense 360** creará de forma automática el nuevo subgrupo si fuera necesario y moverá el equipo.

No se requiere ninguna configuración particular en el Directorio Activo, ni en los agentes **Adaptive Defense 360** instalados ni en la consola de administración. Cada agente recupera la información del Directorio Activo al que pertenece y la envía de forma automática al servidor **Adaptive Defense 360**, actualizando el árbol mostrado en la consola Web.

El envío de los cambios desde el agente Adaptive Defense 360 al servidor se realiza según lo configurado en el apartado Opciones de conexión con el servidor del perfil de protección asignado al equipo.

11.6.2 Replicación de la estructura del Directorio Activo manual

La importación manual de la estructura del Directorio Activo obedece a uno de los dos escenarios mostrados a continuación:

- No todos los equipos de la red tienen un agente **Adaptive Defense 360** instalado que pueda reportar la Unidad Organizativa a la que pertenece, pero el administrador desea disponer de la estructura del Directorio Activo completa en la consola Web de administración.
- El administrador quiere disponer de la estructura completa de grupos y subgrupos desde el principio y sin necesidad de comenzar el despliegue de los agentes de **Adaptive Defense 360**.

Una vez creado el grupo se presentará la pantalla de edición.

Figura 47: Ventana de edición de grupos basados en Active Directory

Para precargar la estructura del Directorio Activo previamente exportada en formato csv haz clic en el botón **Importar**.

El archivo a importar debe tener el siguiente formato:

- Ser un archivo con extensión .csv
- Cada línea del archivo debe incluir la ruta del grupo, y si se desea el perfil asociado a ese grupo. Ambos datos deberán estar separados por tabulador, es decir: "Group Path" tabulador "Nombre del Perfil" [Opcional]

Ejemplo de fichero .CSV:

```
activedirectory.org           ProfileName
activedirectory.org\Domain Controllers ProfileName
activedirectory.org\Computers ProfileName
activedirectory.org\OrganizationUnit1     ProfileName
activedirectory.org\OrganizationUnit1\Departament1    ProfileName
activedirectory.org\OrganizationUnit1\Departament2    ProfileName
```

A la hora de realizar la importación, se visualiza un enlace que mostrará ayuda sobre cómo generar el archivo csv para la importación

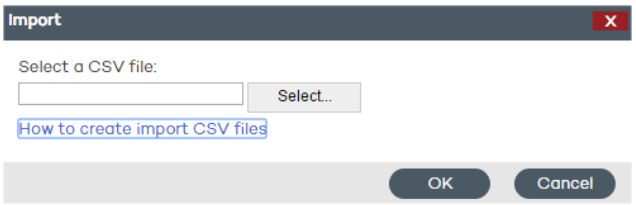


Figura 48: Ventana de selección de fichero csv

11.6.3 Visualización de la ruta del Directorio activo al que pertenece el equipo

En la ventana **Equipos**, selecciona el equipo que quieres ver en la ventana **Detalles.** El apartado Ruta del Directorio activo contiene la información solicitada

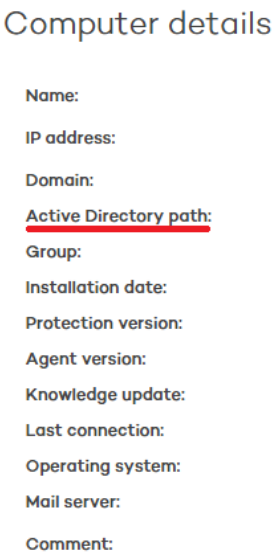


Figura 49: Ventana de detalles del equipo

11.7. Integración de equipos en un grupo

11.7.1 Integración manual

Un equipo o grupo de equipos siempre se puede mover a cualquier grupo de forma manual, ya sea el grupo de tipo manual, Automático por IP o Automático por Directorio Activo.

- En la ventana **Equipos**, dentro de la pestaña **Protegidos**, selecciona en el listado el/los equipos que deseas asignar.
- Haz clic en el botón **Mover**.

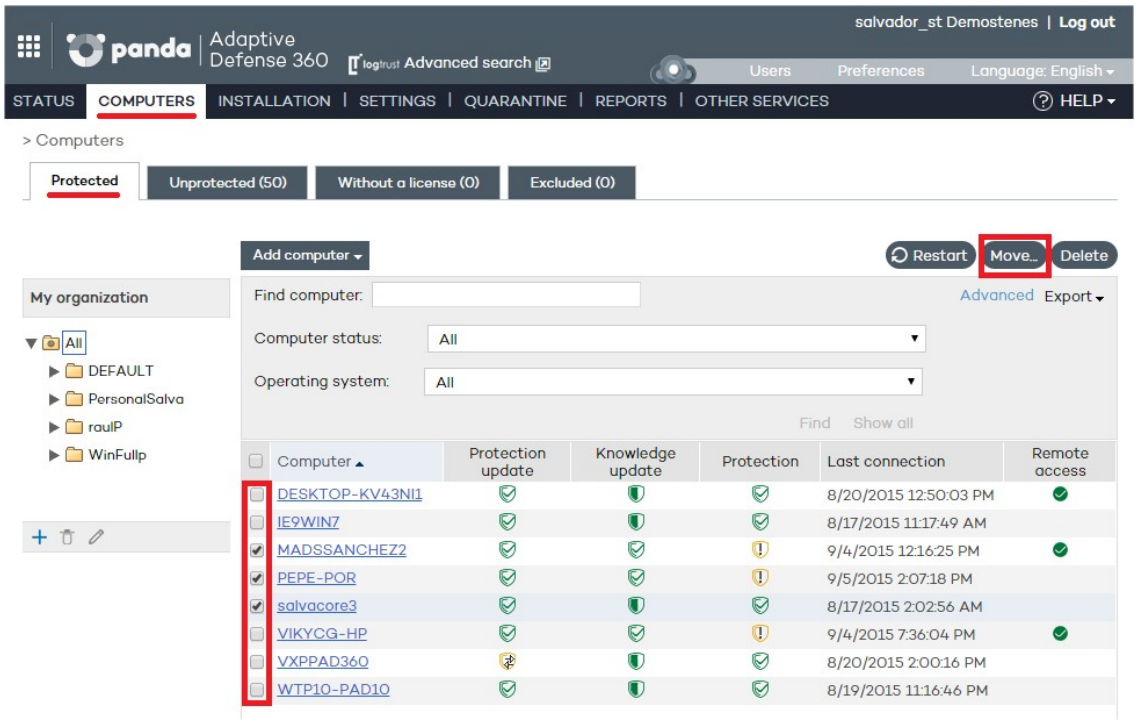


Figura 50: Selección de equipos a mover

- En la ventana **Mover equipos** selecciona el grupo/subgrupo en el que desea incluir el/los equipos.

- Haz clic en el botón **Mover**.

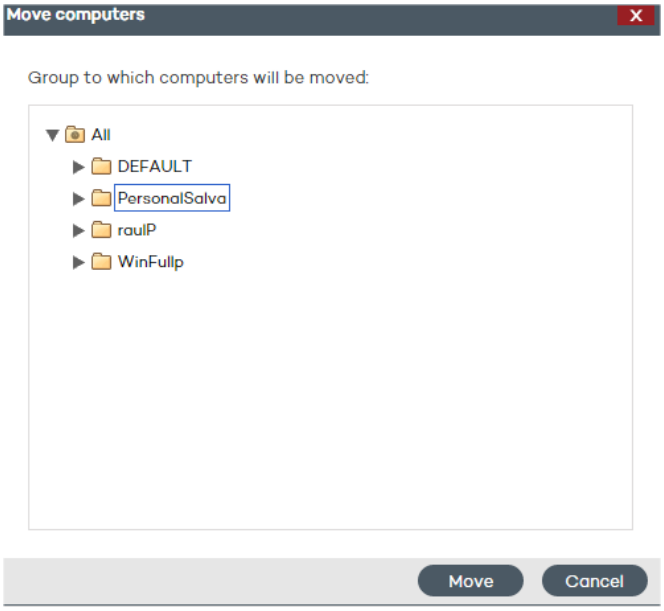


Figura 51: Ventana de selección de destino

La asignación de equipos no es posible realizarla si el permiso del usuario utilizado en la consola es el de monitorización. Para conocer más sobre permisos de usuario, consulta el capítulo 8 Usuarios.

En caso de intentar mover equipos a un grupo que haya alcanzado su número máximo de instalaciones, se mostrará un mensaje advirtiendo de la imposibilidad de realizar la acción. Consulta Restricciones de grupos más adelante en este capítulo.

11.7.2 Integración en la instalación

Al iniciar el proceso de instalación de la protección en un equipo mediante la descarga del instalador selecciona el grupo en el que se integrará el equipo una vez terminada la instalación.

Si el equipo se integra en un subgrupo automático por direcciones IP, **Adaptive Defense 360** moverá el grupo al subgrupo apropiado. Si el equipo no encaja con ningún subgrupo definido será colocado en el grupo padre.

11.8. Editar y eliminar grupos

Crea, elimina y edita grupos desde la ventana **Equipos** y **Configuración**.

Editar un grupo manual

Para editar un grupo manual selecciónalo en el árbol y haz clic en el icono 

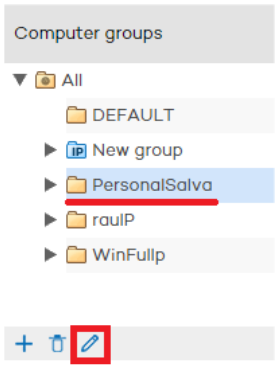


Figura 52: Edición de grupos

A continuación, edita el nombre del grupo y asigna el perfil de la protección que desees, elegido de entre la lista de perfiles que se mostrarán.

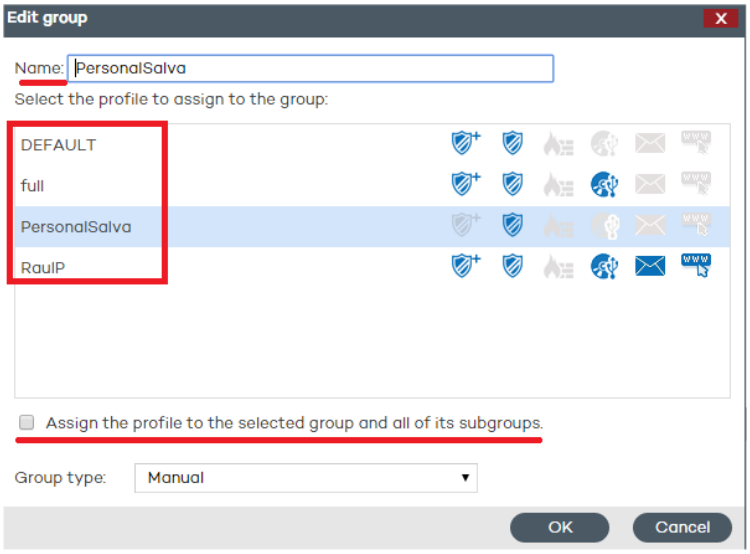


Figura 53: Ventana de edición de grupos

En el caso de que el grupo posea subgrupos, podrás aplicar a todos ellos el perfil seleccionado. Para ello, marca la casilla **Asignar el perfil al grupo seleccionado y a todos sus subgrupos** y haz clic en **Aceptar**.

Editar un grupo automático por direcciones IP

En este tipo de grupo se distinguen dos casos: la edición del grupo padre y la edición de subgrupos con reglas de IP asociadas.

El caso de la edición del grupo padre es idéntico al caso de un grupo manual, si bien desde la ventana **Configuración** es posible acceder a la edición de los subgrupos mediante el botón **Editar grupo.** Haz clic en este botón para acceder a la ventana de edición donde se mostrarán las reglas de IPs y subgrupos asociados al grupo automático por IP.

Editar un grupo automático por Directorio activo

En este tipo de grupo se distinguen dos casos: la edición del grupo padre y la edición de subgrupos con la estructura del Directorio activo de la empresa.

El caso de la edición del grupo padre es idéntico al caso de un grupo manual, si bien desde la ventana **Configuración** es posible acceder a la edición de los subgrupos mediante el botón **Editar grupo**.

No se podrá cambiar el nombre de los subgrupos de un grupo automático por Directorio activo ya que cualquier modificación dejaría desalineada la estructura generada en la consola de Adaptive Defense con respecto a la estructura del Directorio activo de la empresa. En este escenario cualquier modificación sería revertida en la consola de administración creando de nuevo el subgrupo que cambió de nombre y moviendo a éste los equipos.

Eliminar un grupo

Para eliminar un grupo, selecciónalo en el árbol de grupos y a continuación haz clic en el icono

 .

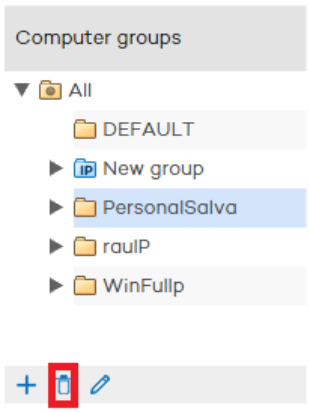


Figura 54: Borrado de grupos

No es posible eliminar un grupo si contiene grupos o subgrupos. Antes de eliminar un grupo es necesario asignar los equipos que lo integran a otro grupo/subgrupo.

11.9. Restricciones de grupo

Las restricciones de grupo sirven para controlar el número de equipos que pueden pertenecer a un determinado grupo y es especialmente útil para partners que desean asignar un determinado grupo a un cliente concreto. Para ello el administrador puede establecer el número total de equipos que pueden pertenecer a un grupo de forma simultánea y la duración de esta pertenencia.

Se recomienda el uso del producto gratuito para partners Panda Partner Center para la gestión completa del ciclo de vida del cliente. Consulta a tu comercial para habilitar el acceso al servicio.

Para activar las restricciones de grupo, en el menú **Preferencias** activa la casilla **Permitir asignar restricciones a los grupos** en la zona **Restricciones de grupo**.

Una vez activada, en las ventanas de creación de grupo se añadirán dos configuraciones adicionales:

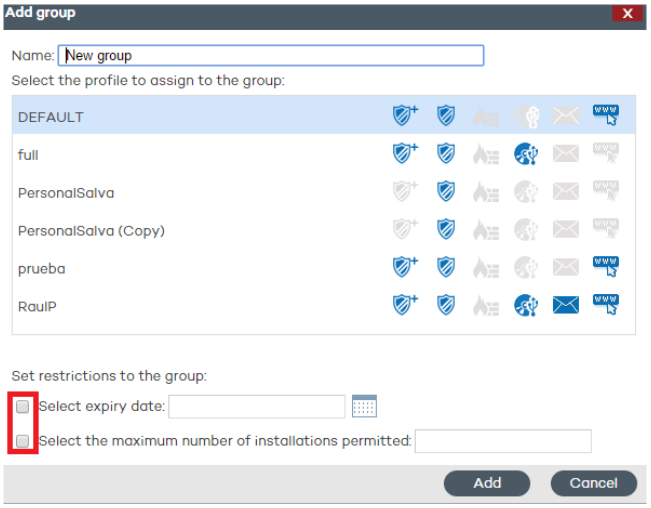


*Figura 55: Nuevas configuraciones al activar **Restricciones de grupo***

- **Selecciona fecha de caducidad**: establece la fecha máxima de pertenencia de un equipo al grupo. Una vez pasada esa fecha el equipo pasará a estado **Sin licencia**.
- **Selecciona número máximo de instalaciones**: determina el número máximo de equipos que pertenecen al grupo.
  - Si se intenta mover un equipo a un grupo que ya alcanzó el número máximo de instalaciones se visualizará un error en la consola Web de administración.
  - Si se intenta instalar un equipo en un grupo que ya alcanzó el número máximo de instalaciones se mostrará un error en el agente local del equipo.

12. Perfiles de protección

Visión general y planificación de la protección del parque informático
Creación y gestión de perfiles de protección
Configuración general de perfiles de protección

12.1. Introducción

Este capítulo sirve de introducción a la configuración de los perfiles de seguridad, también llamados perfiles de protección, o simplemente perfiles.

El perfil de protección es la herramienta principal utilizada en **Adaptive Defense 360** para distribuir la política de seguridad definida por el administrador entre los equipos de la red que ya cuenten con un agente instalado.

Un perfil de seguridad es una configuración específica de los módulos de protección, que se aplica a uno o varios grupos de dispositivos.

Un perfil de seguridad puede contener configuraciones que afecten a plataformas de distinto tipo, como por ejemplo Windows y Mac OS X. De esta manera, con un único perfil de seguridad es posible dar una configuración de la protección a todos los dispositivos de la red, independientemente del tipo del dispositivo que la reciba.

12.2. Visión general y planificación de la protección del parque informático

Para desplegar la configuración de la seguridad de forma eficiente, es recomendable que el administrador siga una serie de pasos generales que facilitarán la implementación de la política de seguridad definida en la empresa, al tiempo que se minimizan posibles fallos y brechas de seguridad:

1 Definir la política de seguridad de empresa

El primero paso que debe de afrontar el equipo responsable de la seguridad en la empresa es la creación de una serie de documentos que establezcan el marco de seguridad requerido por la compañía.

Este marco o política de seguridad deberá ser compatible con las necesidades de acceso a la información de los usuarios de la red y contemplará el uso de las herramientas requeridas por los trabajadores para desempeñar sus tareas sin problemas.

El objetivo final es describir un entorno productivo y seguro para los equipos de la red y para la integridad de los datos manejados por la compañía, protegiendo sus activos informáticos de accesos no autorizados y evitando las fugas de información que puedan dañar su imagen y causar graves perjuicios económicos.

Para la elaboración de este documento el equipo encargado de la seguridad necesita conocer las características de seguridad y detección de comportamientos sospechosos implementadas en las herramientas de protección que utilizará para garantizar un entorno confiable y productivo; a continuación, se muestra una tabla de las funcionalidades asociadas a la seguridad de **Adaptive Defense 360** y su disponibilidad en las diferentes plataformas para dispositivos de usuario.

Características / plataforma mínima	Windows	Linux	Mac OS X	Android
Protección avanzada permanente (Audit, Hardening, Lock)	X			
Detección de robo de datos	X			
Protección ante sistemas vulnerables	X			
Protección contra virus permanente	X		X	X
Protección contra virus bajo demanda	X	X	X	X
Programación de tareas de análisis	X	X	X	X
Protección del correo	X			
Protección Web	X			
Cortafuegos de red	X			
Cortafuegos de aplicaciones	X			
Sistema de detección de intrusos	X			
Filtrado de URL por categorías	X			
Control de dispositivos	X			
Protección antirrobo				X

Tabla 4:Características de protección por plataforma de usuario soportada

Para servidores de ficheros y correo **Adaptive Defense 360** ofrece las siguientes características:

Características / plataforma mínima	Windows Server	Microsoft Exchange	Mac OS X	Linux
Protección avanzada permanente (Audit, Hardening, Lock)	X*	X*		
Detección de robo de datos	X*	X*		
Protección ante sistemas vulnerables	X*	X*		
Protección contra virus permanente	X	X	X	
Protección contra virus bajo demanda	X	X	X	X
Programación de tareas de análisis	X	X	X	X
Protección de buzones del correo		X		
Protección del tráfico entre servidores de correo (transporte)		X		
Protección antispam		X		
Filtrado de contenidos		X		
Cortafuegos de red	X	X		
Cortafuegos de aplicaciones	X	X		
Sistema de detección de intrusos	X	X		
Filtrado de URL por categorías	X	X		
Control de dispositivos	x	X		

Tabla 5: Características de protección por plataforma de servidor soportada

(*) Tecnología compatible con plataformas Windows Server, Workstation y Exchange. Requiere de la ejecución del PEs sospechoso para su funcionamiento.

2 Generar un listado con todos los dispositivos de la empresa a proteger

El objetivo de este punto es determinar los dispositivos de la empresa que recibirán una configuración de seguridad de **Adaptive Defense 360**. Para ello es necesario conocer el sistema operativo del dispositivo, su rol dentro del parque informático (servidor, puesto de trabajo, dispositivo móvil) y el perfil del usuario que lo utilizará, así como el departamento al que pertenece.

3 Verificar que todos los dispositivos listados tienen un agente Adaptive Defense 360 instalado

Para que los equipos queden integrados en la consola de **Adaptive Defense 360** y protegidos es

necesario que tengan instalado un agente y posean una licencia válida asignada. Consulta el capítulo 9 Instalación de la protección para verificar los procedimientos de instalación. Consulta el capítulo 7 Gestión de cuentas para comprobar el estado de las licencias de **Adaptive Defense 360**.

4 Agrupar los dispositivos según sus características de seguridad comunes

Desarrollar una estrategia clara de agrupación de dispositivos es un factor clave a la hora de gestionar la seguridad de la red; una configuración de seguridad se aplicará a uno o más grupos de equipos, es por lo tanto necesario localizar y reunir a aquellos dispositivos que tengan idénticos requisitos de seguridad.

Para poder segmentar la red en diferentes grupos es necesario establecer los criterios de agrupación que se utilizarán; para ello será necesario tener en cuenta la información del equipo y del usuario que lo utiliza obtenida en el segundo punto, perfil del usuario que lo utilizará, plataforma utilizada etc.

5 Creación de perfiles de seguridad

Un perfil de seguridad es una plantilla de configuración que se asigna a uno o varios grupos de dispositivos y define el comportamiento de la protección.

Algunas características configurables dentro de un perfil de seguridad son por ejemplo el tipo de análisis que se realizará y sobre qué elementos, nivel de acceso del usuario a los dispositivos conectados en su equipo, cada cuánto tiempo se actualizará la protección y otra serie de parámetros.

El administrador necesitará crear tantos perfiles de seguridad como comportamientos de seguridad distintos requiera la distribución de equipos en grupos realizada en el punto anterior.

6 Asignación de perfiles de seguridad a grupos

A la hora de asignar perfiles a los grupos creados, las opciones son varias dependiendo del tamaño de la red de la empresa: un mismo perfil se puede aplicar a varios grupos, cada grupo creado puede tener un perfil diferente o se puede dar el caso de que sólo se necesiten un único perfil y un único grupo para redes pequeñas o muy homogéneas.

Una vez aplicado el perfil de seguridad los dispositivos que forman el grupo quedarán protegidos según el comportamiento de la protección descrito en el perfil de seguridad asignado.

12.3. Creación y gestión de perfiles de protección

Toda la gestión de perfiles de protección se realiza desde la ventana **Configuración**

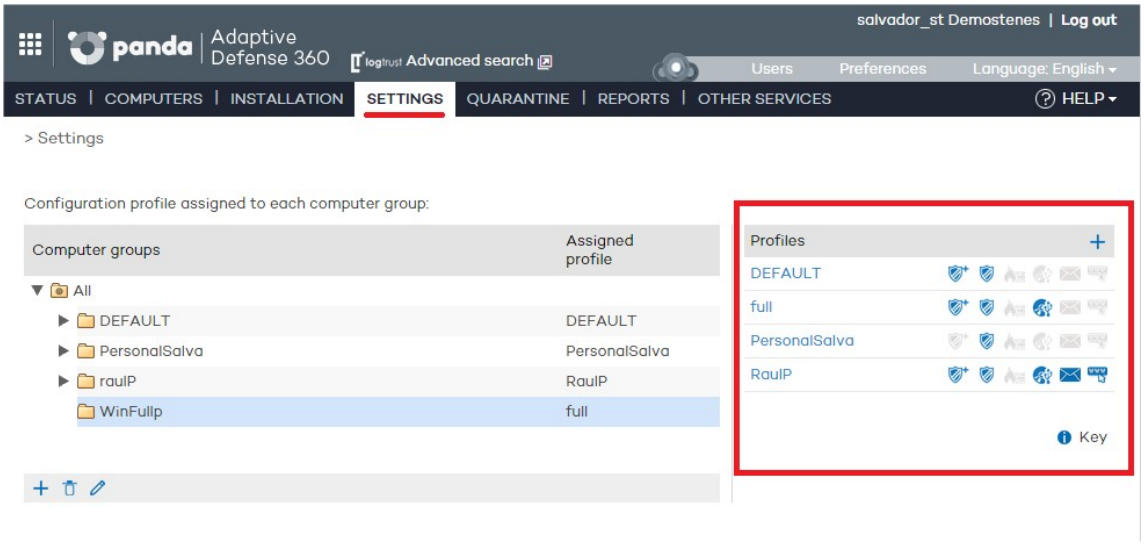


Figura 56: Acceso a los perfiles de protección

12.3.1 Creación de perfiles de seguridad

Si es necesario crear perfiles nuevos, a medida que se creen se mostrarán en la ventana **Configuración** junto al perfil Default ya existente, acompañados de información sobre las protecciones que incluyen.

Después podrás modificar en cualquier momento la configuración de un perfil haciendo clic sobre su nombre y accediendo a la ventana **Editar perfil**.

Si se intenta asignar a un perfil un nombre ya utilizado para otro, se mostrará un mensaje de error.

Si no es posible visualizar un perfil que ya existe probablemente no se disponga de permisos para ello. Consulta el capítulo 8 Usuarios para más información.

Para crear un perfil haz clic en el icono en la ventana **Configuración** y accederás a la ventana **Editar perfil**. Desde aquí podrás configurar el perfil nuevo.

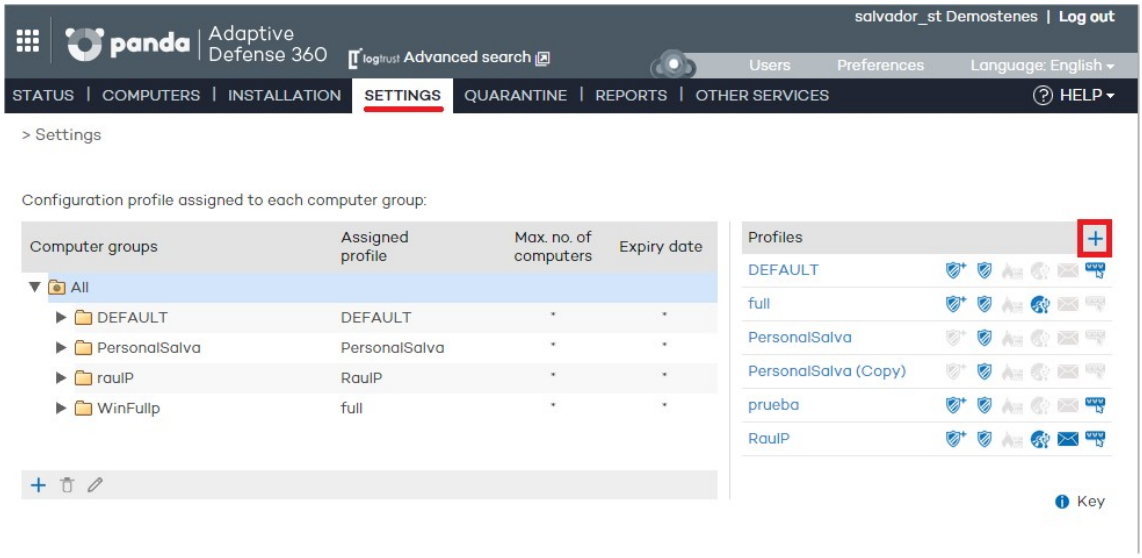


Figura 57: Acceso a la ventana de creación de perfiles de seguridad

La configuración de la protección de un perfil de protección se trata de forma general más adelante en este capítulo.

12.3.2 Copia de perfiles de protección

Adaptive Defense 360 ofrece la posibilidad de realizar copias de perfiles existentes. Esto resulta útil cuando se prevea que la configuración básica de un perfil que ya está creado es susceptible de ser aplicada a otros grupos de equipos con cambios en la política de protección.

De esta manera en lugar de crear dicha configuración básica cada vez, podrá copiar el perfil para después personalizarlo y adaptarlo a las circunstancias concretas de protección que necesite.

En la pantalla **Configuración**, posiciona el cursor sobre los iconos que muestran las protecciones activas del perfil que deseas copiar, y haz clic en el icono  .

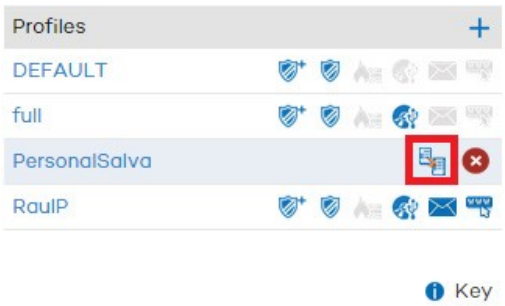


Figura 58: Copia de perfiles de seguridad

Una vez copiado el perfil, éste se mostrará en la lista bajo el perfil original con el mismo nombre que tiene el perfil original, añadiendo el texto (copia) al final.

En el caso del perfil **DEFAULT**, es posible hacer una copia, pero el perfil copiado no tendrá la condición de perfil por defecto ni será asignado automáticamente a ningún equipo. El perfil **DEFAULT** original será siendo el predeterminado.

La copia de perfil será posible en función del tipo de permiso del que se disponga.

12.3.3 Borrado de perfiles de protección

Para borrar el perfil seleccionado haz clic en el icono .

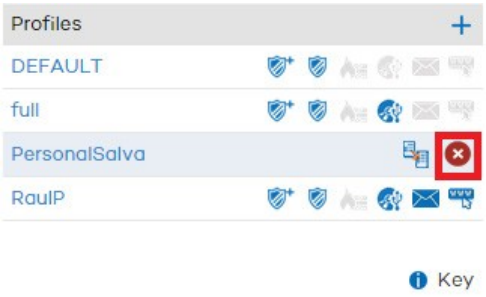


Figura 59: Borrado de perfiles de seguridad

El borrado de un perfil de protección solo es posible si se cumplen todas las condiciones mostradas a continuación:

- El perfil de protección no es el perfil DEFAULT.
- El usuario que accede a la consola Web de administración para borrar el perfil de protección tiene permisos suficientes
- El perfil de protección no está asignado a ningún grupo de equipos.

Si alguno de los puntos anteriores no se cumple el borrado del perfil de protección fallará y se mostrará un error en la consola Web de administración.

12.4. Configuración general de perfiles de protección

Para configurar el perfil creado haz clic en el mismo. Se mostrará una nueva ventana con un menú lateral de dos niveles donde se agrupan las características, distribuidas según la plataforma del equipo a proteger (Windows, Linux, Mac OS X y Android)

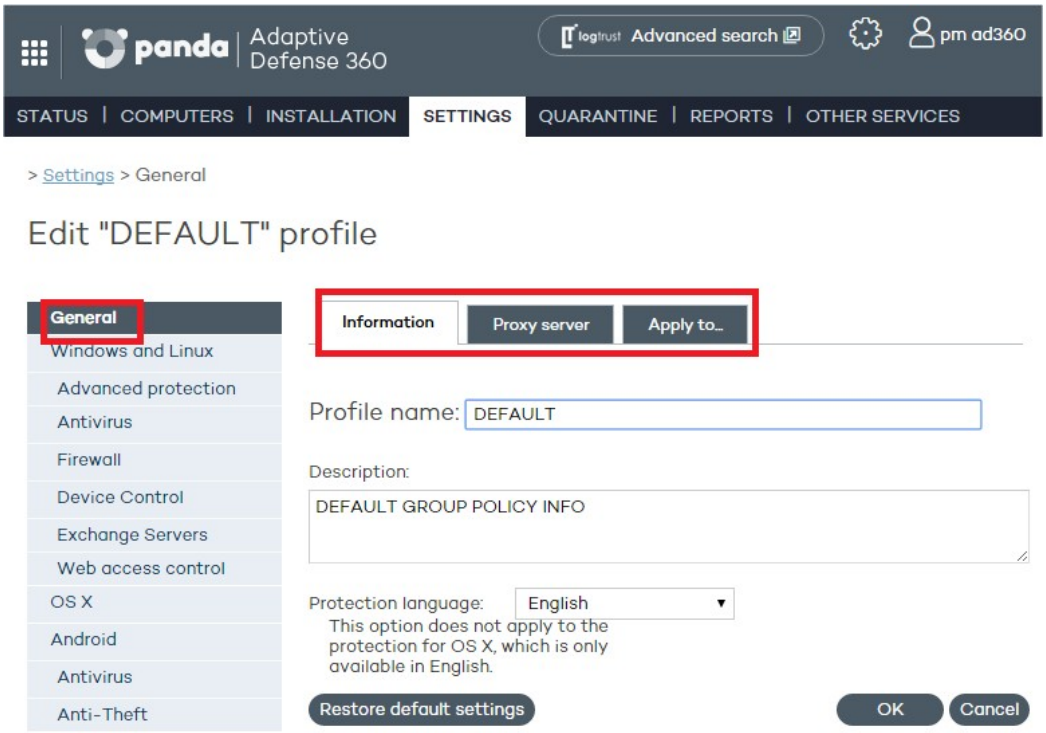


Figura 60: Acceso a la configuración general de un perfil de protección

La configuración general se distribuye en tres pestañas

Pestaña Información

Asigna un nombre al perfil y añade una descripción adicional que sirva para identificar el perfil y seleccionar el idioma en el que se instalará la protección.

La configuración del idioma por defecto de la protección sólo afectará a los equipos Windows, ya que la protección de **Adaptive Defense 360** para OS X se instala siempre en inglés. En el caso de los dispositivos Android, la protección se instalará en el idioma del dispositivo y, si no está soportada, en inglés.

Pestaña Proxy

Establece cuál es la conexión a Internet del equipo, si ésta se realiza a través de proxy y si se requiere una autenticación para ello.

> *Para equipos en roaming con proxy configurado en el perfil de protección aplicado, o para aquellos casos en los que el proxy deje de estar accesible debido a un fallo temporal, el agente intentará conectarse a Internet por otros medios disponibles.*

En el caso de los equipos con sistema operativo Linux, esta configuración de la conexión a Internet es necesario hacerla desde el equipo mediante la línea de comandos.

Selecciona la casilla **Solicitar datos de acceso a Internet.** En caso de no detectarse conexión, si el agente no consigue acceder a Internet mostrará una ventana al usuario para que introduzca los

datos de conexión.

Pestaña Aplica a

Lista los grupos asignados al perfil

13. Perfiles de protección Windows

13.1. Introducción

La configuración de un perfil de seguridad para equipos Windows se realiza desde la ventana **Configuración.** Selecciona el perfil a configurar en el panel de Perfiles y después el menú lateral **Windows y Linux**.

Cada uno de los módulos de protección Windows cuenta con una entrada propia en el menú lateral.

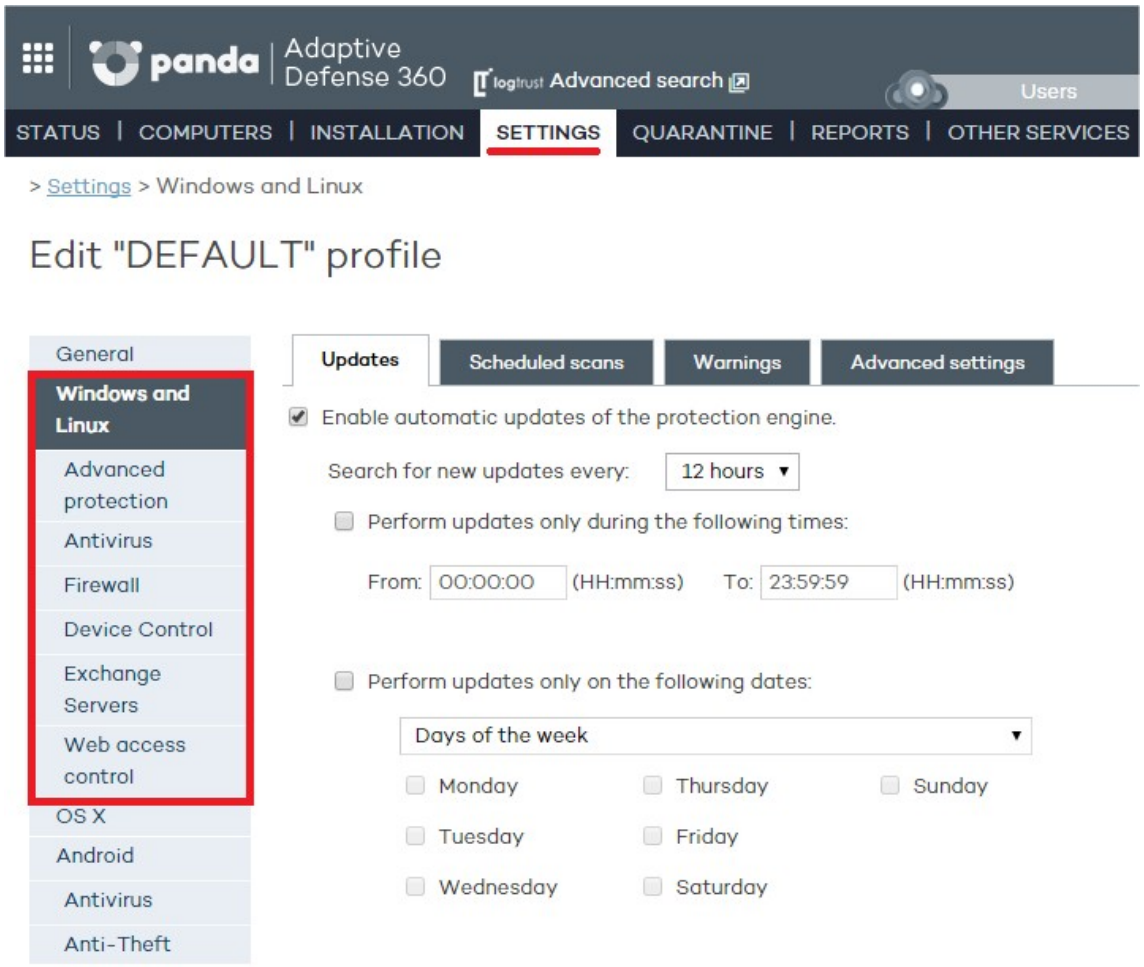


Figura 61: Acceso a las diferentes secciones de configuración en un perfil de protección

13.2. Configuración general

Para mostrar las cuatro pestañas de configuración que permiten determinar el comportamiento de las actualizaciones, análisis programados, alertas y configuraciones avanzadas de instalación y conectividad haz clic en la entrada **Windows y Linux** del menú lateral.

Actualizaciones

Consulta el capítulo 10 Actualización de la protección para obtener información sobre las actualizaciones

Análisis programados

Utiliza las opciones que se muestran en la pestaña **Análisis programados** para crear tareas de análisis, periódicas, puntuales o inmediatas y determinar si afectarán a todo el PC o a determinados elementos del mismo.

Puedes programar análisis exclusivos de los discos duros o especificar las rutas concretas en las que se encuentran las carpetas o archivos a analizar.

Las tareas de análisis se añaden en el listado principal de la pestaña **Análisis programados** de la ventana **Editar perfil**, desde donde puedes editarlas o eliminarlas.

A continuación, se indican los pasos necesarios para configurar una nueva tarea de análisis:

- Haz clic en el botón **Nuevo** para acceder a la ventana **Edición de perfil** – **Nueva tarea de análisis**.

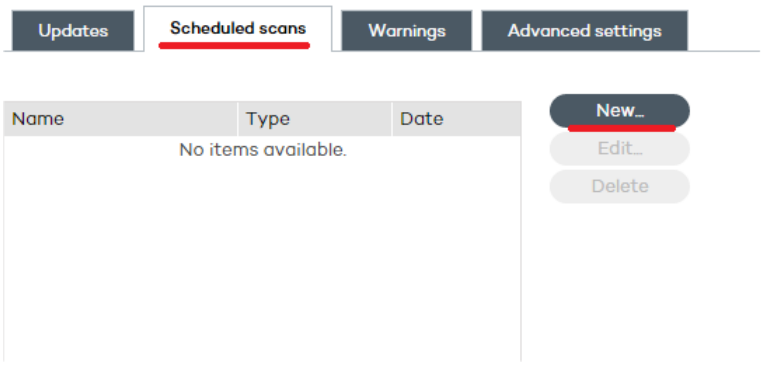


Figura 62: creación de un nuevo análisis programdo

- En la nueva ventana introduce la siguiente información:
  - **Nombre**: indica el nombre con el que quieres identificar el análisis que va a programar.
  - **Tipo de análisis**: selecciona el tipo de análisis que vas a crear:
    - **Análisis inmediato**: Una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de **Adaptive Defense 360** y se constate que se ha producido alguna modificación en la configuración de la protección.
    - **Análisis programado**: el análisis tendrá lugar en la hora y fecha que se determine en **Fecha de comienzo** y **Hora de comienzo**. Mediante el desplegable es posible determinar si la hora de comienzo configurada está referida al servidor **Adaptive Defense 360** o es tomada del equipo del usuario.
    - **Análisis periódico**: determina la fecha y hora de comienzo, y selecciona en el desplegable **Repetición** la periodicidad que deseas adjudicar al análisis.
  - **Analizar**: selecciona la opción que deseas:
    - **Todo el PC**: este tipo de análisis incluye los discos duros y unidades USB
    - **Discos duros**

- **Otros elementos**: Utiliza esta opción para analizar elementos concretos almacenados (archivos, carpetas,...). Será necesario introducir la ruta en la que se encuentra el elemento a analizar. El formato de la ruta ha de empezar por \\equipo, \\IP o (letra de unidad):\

  Ejemplos:

  ```
  \\equipo\carpeta
  c:\carpeta1\carpeta2
  ```

  El número máximo de rutas a analizar que podrás introducir por cada perfil es 10. En función del permiso que se posea se podrán establecer rutas específicas de análisis.

- Para configurar aspectos complementarios de los análisis programados haz clic en el link **Opciones avanzadas de análisis**:
  - Para activar el análisis de archivos comprimidos, marca la casilla correspondiente.
  - Selecciona el software malintencionado que deseas analizar. **Virus** siempre estará activo.
  - Analiza todo por defecto o excluye del análisis determinadas extensiones, carpetas o archivos. En este caso utiliza los botones **Añadir**, **Vaciar** y **Eliminar** para conformar la lista de exclusiones.

Alertas

Aquí puedes configurar los dos tipos de alertas generadas por el software **Adaptive Defense 360**:

- **Alertas locales**: son las alertas que mostrará el agente en el equipo del usuario cuando se detecte malware en los equipos, intentos de intrusión o dispositivos no permitidos

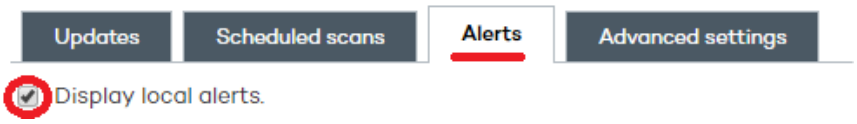


Figura 63: acceso a la configuracion de alertas locales

- **Alertas por correo**: son las alertas que enviará al administrador el agente **Adaptive Defense 360** por correo, alertando del malware encontrado en los equipos y de las violaciones de las políticas definidas en el módulo de **Control de Dispositivos**.

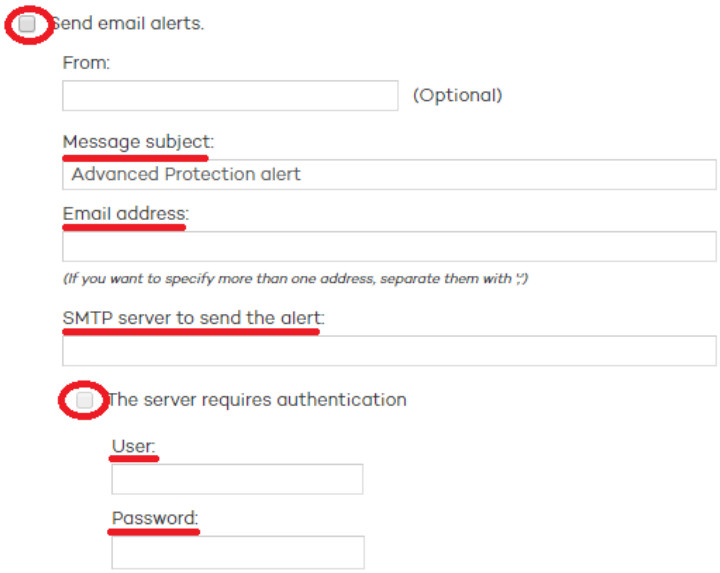


Figura 64: Ventana de configuración de envío de alertas por correo desde el equipo del cliente

Para configurar el correo electrónico que contendrá la alerta, activa la casilla **Enviar alertas por correo**:

- **Desde**: indica la dirección de correo origen de la alerta. Esta dirección deberá de corresponder a un buzón gestionado por el servidor de correo indicado más adelante, o al menos ser aceptada por el servidor de correo configurado para su reenvío. En caso de no indicar una dirección de correo la alerta se enviará con el campo origen `nombre_equipo@panda.local`
- **Asunto del mensaje**: añade un asunto al mensaje para que el administrador pueda añadir filtros a su cliente de correo que le permitan ordenar los mensajes de alertas recibidos.
- **Dirección de correo**: añade varias direcciones de correo separadas por el carácter ";"
- **Servidor SMTP que enviará la alerta**: dirección IP del servidor de correo de la empresa. Deberá ser accesible desde el software **Adaptive Defense 360**
- **El servidor requiere autenticación**: si el servidor de correo no es open relay para las direcciones IP internas de la empresa, será necesario suministrar credenciales para el envío del correo. El envío de las credenciales es compatible con el protocolo ESMTP extensión `AUTH LOGIN`.

El equipo enviará un correo al administrador con información básica de la alerta:

- **Tipo de malware**: especifica la categoría del malware detectado
- **Equipo afectado**: nombre del equipo donde se ha producido la alerta
- **Ruta** (si aplica)
- **Fichero** (si aplica): nombre del fichero donde se detectó la amenaza
- **Acción aplicada**: medida de resolución automática realizada por el equipo

Se enviará una alerta cada vez que se realice una de las siguientes acciones:

- Detección de malware
- Detección de operación no autorizada sobre un dispositivo por el módulo de Control de dispositivos

Para evitar el bloqueo del buzón de correo del administrador, **Adaptive Defense 360** entrará en "modo epidemia" cuando se detecten más de 20 eventos del mismo malware o del mismo dispositivo en menos de un minuto. A partir de este momento enviará un único correo cada cinco minutos con un resumen del número de sucesos detectados. Para salir del "modo epidemia" es necesario que en el último minuto no se hayan producido dos o más sucesos de ese tipo.

Opciones avanzadas

Aquí se podrán especificar aspectos que tienen que ver con la instalación de la protección en los equipos, así como con la conexión de éstos a Internet y a los servidores de **Adaptive Defense 360**.

También se podrán configurar opciones relacionadas con la cuarentena de los archivos sospechosos.

- **Instalación**: Especifica en qué directorio quieres instalar la protección.
- **Desinstalar automáticamente otras protecciones**: especifica si **Adaptive Defense 360** desinstalará productos de la competencia instalados previamente en el equipo o si, por el contrario, ambos productos podrán convivir. Consulta el capítulo 9 Instalación de la protección para más información.
- **Conexión con la Inteligencia Colectiva**: desactiva los análisis con la Inteligencia Colectiva. Es recomendable mantener activa esta opción para disfrutar de toda la protección que la Inteligencia Colectiva proporciona.
- **Conexión con el servidor**: Determina cada cuánto tiempo el equipo envía información a los servidores de **Adaptive Defense 360** acerca del estado de la protección instalada. El intervalo debe de estar entre 12 y 24
  - **Centralizar todas las conexiones con el servidor a través del siguiente equipo**: Especifica el equipo a través del cual desea que se centralicen las conexiones con el servidor de **Adaptive Defense 360**. Para ello, marca la casilla y haz clic en el botón **Seleccionar**. En la pantalla **Selección de equipo** elije el equipo o búscalo mediante el botón **Buscar**. A continuación, haz clic en **Aceptar**.
- **Opciones de cuarentena**: establece la ruta dentro del equipo del usuario donde se depositarán los elementos restaurados de la cuarentena.
- **Contraseña de administración**: La contraseña de administración te permite realizar tareas de desinstalación y configuración de la protección local en modo administrador. Es decir, con la misma contraseña podrás desinstalar **Adaptive Defense 360** de los equipos en los que está ha instalado o permitir que sea el usuario de dichos equipos quien active o desactive las protecciones desde la consola local de **Adaptive Defense 360**. No se trata de opciones excluyentes, por lo que se puede optar por seleccionar ambas a la vez.

13.3. Configuración de la protección avanzada

La protección avanzada establece los diferentes modos de bloqueo frente al malware

desconocido y protege al equipo de APTs, amenazas avanzadas y programas maliciosos que utilizan vulnerabilidades (exploits) para infectar el equipo del usuario.

13.3.1 Comportamiento

- **Auditoria**: En el modo auditoria **Adaptive Defense 360** solo informa de las amenazas detectadas, pero no bloquea ni desinfecta el malware encontrado.
- **Hardening**: permite la ejecución de los programas desconocidos ya instalados en el equipo del usuario. Los programas desconocidos que vienen del exterior (Internet, correo y otros) serán bloqueados hasta su clasificación. Los programas clasificados como malware serán movidos a cuarentena.
  - **No informar del bloqueo al usuario del equipo**: las notificaciones del agente generadas por el bloqueo de programas desconocidos y origen externo no se muestran al usuario.
  - **Informar del bloqueo al usuario del equipo**: **Adaptive Defense 360** mostrará un mensaje en el equipo del usuario cada vez que se bloquee la ejecución de un programa.
- **Lock**: Bloquea la ejecución de todos los programas desconocidos hasta que estén clasificados.
  - **No informar del bloqueo al usuario del equipo**
  - **Informar del bloqueo al usuario del equipo**: el usuario recibe un aviso del agente instalado explicando la razón del bloqueo
  - **Dar la opción de ejecutar**: muestra al usuario una ventana en su equipo durante 1 minuto que le permitirá elegir si el elemento desconocido se ejecutará bajo su responsabilidad o no. Esta exclusión es permanente hasta que el administrador modifique su configuración desde la consola Web.

13.3.2 Anti-exploit

La protección anti exploit bloquea de forma automática y sin intervención del usuario en la mayor parte de los casos los intentos de explotación de vulnerabilidades de procesos con fallos de programación instalados en el equipo del usuario.

Funcionamiento de la protección anti-exploits

Los equipos de la red contienen algunos procesos con fallos de programación. Estos procesos son conocidos como “procesos vulnerables” y, aunque sean programas legítimos, no interpretan correctamente ciertas secuencias de datos que recogen del exterior.

Cuando un proceso vulnerable recibe información con determinados patrones conocidos por los hackers, se produce un mal funcionamiento que termina con una inyección de fragmentos de código específicamente preparados por el hacker en las regiones de memoria gestionadas por el proceso vulnerable. Estos procesos reciben el nombre de “procesos comprometidos”.

La inyección de código provoca que el proceso comprometido ejecute acciones para las que no fue programado, generalmente peligrosas para el equipo del usuario. La protección anti-exploit de **Adaptive Defense 360** detecta esta inyección de código malicioso en los procesos vulnerables ejecutados por el usuario.

Adaptive Defense 360 bloquea los ataques de tipo exploit mediante dos cursos de acción

diferentes, dependiendo del exploit encontrado:

- **Bloqueo del exploit**

Adaptive Defense 360 detecta la inyección de código en el proceso vulnerable cuando todavía no se ha completado. El proceso no llega a comprometerse y el riesgo del equipo es nulo, con lo que no se requiere reinicio del proceso afectado ni del equipo de usuario, ni implica pérdida de información por parte del proceso afectado.

El usuario puede recibir una notificación del bloqueo dependiendo de la configuración establecida por el administrador.

- **Detección del exploit**

Adaptive Defense 360 detecta la inyección de código en el proceso vulnerable cuando ya se ha producido. Debido a que el proceso vulnerable ya contiene el código malicioso, el proceso está comprometido y es imperativo reiniciarlo antes de que ejecute acciones que puedan poner en peligro la seguridad del equipo.

Independientemente del tiempo transcurrido desde la detección hasta el reinicio del proceso **Adaptive Defense 360** considera en riesgo el equipo, aunque es evidente que el riesgo es directamente proporcional al tiempo que se tarde en reiniciar el proceso afectado. **Adaptive Defense 360** puede reiniciar el proceso de forma automática para minimizar los efectos adversos, o delegar en el usuario la decisión, pidiéndole permiso de forma explícita para reiniciarlo.

En el caso de que el administrador haya configurado un reinicio automático para minimizar la posibilidad de efectos adversos, el usuario puede sufrir la perdida de información gestionada por el proceso afectado. En el caso de que el administrador haya delegado en el usuario la decisión, el usuario podrá salvar la información, minimizando la posibilidad de pérdida de información.

Se recomienda establecer el reinicio automático de procesos para minimizar la posibilidad de efectos adversos del exploit

En los casos en que no sea posible reiniciar el proceso afectado se pedirá permiso al usuario para reiniciar el equipo completo.

Configuración de la detección anti - exploits

- **Detectar exploits**: habilita la protección contra exploits
  - **Auditar**: se notificará en la consola Web la detección del exploit, pero no se tomarán acciones contra él ni se informará al usuario del equipo. La notificación también puede producirse vía correo electrónico según la configuración que el administrador haga de las alertas por correo electrónico a través de la opción **Preferencias** del botón de configuración general.

- **Bloquear**: bloquea los ataques de tipo exploit. Puede requerir el reinicio o el cierre del proceso afectado por el exploit.
  - **Informar del bloqueo al usuario del equipo:** el usuario recibe una notificación, pero el proceso comprometido se reinicia de forma automática si es necesario.
  - **Pedir permiso al usuario**: el usuario recibe una petición de autorización para el cierre del proceso comprometido por el exploit en caso de ser necesario. Esta opción resulta útil para que el usuario pueda salvar la información crítica antes de que se produzca el cierre del proceso. Si se requiere el reinicio del equipo se pedirá confirmación al usuario, independientemente de la configuración **Pedir permiso al usuario**.

Dado que muchos exploits continúan ejecutando código malicioso, hasta que no se produzca el reinicio o el cierre del proceso la incidencia no se marcará como resuelta en el panel de elementos maliciosos y exploit de la consola Web

13.3.3 Exclusiones

Esta configuración afecta tanto a la protección antivirus como a la protección avanzada.

Permite configurar elementos en los equipos de la red que no serán analizados por la protección **Adaptive Defense 360**

- **Extensiones**: permite especificar extensiones de ficheros que no serán analizadas.
- **Carpetas**: permite especificar carpetas cuyo contenido no será analizado.
- **Ficheros**: permite especificar ficheros concretos que no serán analizados.

13.3.4 Uso de la red

Para los ficheros ejecutables encontrados en el equipo del usuario y que sean desconocidos para la plataforma **Adaptive Defense 360** el agente enviará el fichero al servidor para su análisis. El impacto en el rendimiento de la red del cliente debido al envío de los ejecutables desconocidos está configurado de forma predeterminada (máximo de 50 Mbytes por hora y agente) para pasar completamente desapercibido. Un fichero desconocido se envía una sola vez para todos los clientes que usan **Adaptive Defense 360**. Además, se han implementado mecanismos de gestión del ancho de banda con el objetivo de minimizar el impacto en la red del cliente.

Para configurar el número máximo de megas que un agente podrá enviar en una hora introduce el valor y haz clic en **Ok**. Para establecer transferencias ilimitadas deja el valor a 0.

13.3.5 Privacidad

Para que **Adaptive Defense 360** pueda incluir el nombre y la ruta completo de los ficheros enviados para su posterior visualización en los informes y en las herramientas de análisis forense, activa la casilla apropiada en la pestaña **Privacidad**.

13.4. Configuración de la protección antivirus

Para configurar el comportamiento general de la protección antivirus en el perfil que estás creando haz clic en las pestañas **Archivos**, **Correo** y **Web**.

La acción a ejecutar por **Adaptive Defense 360** ante un fichero de tipo malware o sospechoso queda definida en los laboratorios de Panda Security y sigue las siguientes pautas:

- **Ficheros conocidos como malware – desinfectables**

Se desinfectan y se elimina el fichero original quedando sustituido por una copia desinfectada y sin peligro para el usuario.

- **Ficheros conocidos como malware no desinfectable**

Para los casos en los que no sea posible una desinfección el fichero será movido a cuarentena

Archivos

Configurar el comportamiento básico de la protección antivirus relativa al sistema de ficheros

- Selecciona la casilla **Activar protección permanente de archivos**.
- Marca la casilla correspondiente para analizar archivos comprimidos.
- Selecciona los tipos de malware a detectar por la protección.
  - **Virus**: protección contra programas que se pueden introducir en los ordenadores produciendo efectos nocivos e incluso destructivos e irreparables
  - **Herramientas de hacking y PUPs**: protección contra programas que puede ser utilizados por un hacker para causar perjuicios a los usuarios de un ordenador y protección contra Programas potencialmente no deseados

Si la protección permanente de archivos esta activada la detección de Virus no se podrá desactivar.

A continuación, selecciona las tecnologías de detección por comportamiento:

- **Bloquear acciones maliciosas**: activa tecnologías anti exploit que analizan localmente el comportamiento de los procesos buscando actividad sospechosa.

Para definir exclusiones haz clic en **Opciones avanzadas** donde se mostrará la pestaña **Exclusiones** explicadas en el apartado anterior **Configuración de la protección avanzada**

Correo

Configura el comportamiento de la protección antivirus del perfil creando para el correo electrónico.

- Activa la protección permanente de correo y la de archivos comprimidos
- Marca la casilla correspondiente para seleccionar el tipo de malware a detectar.
  - **Virus**
  - **Hacking tools y PUPs**
  - **Sospechosos**
  - **Phishing**: programas que intentan conseguir información confidencial de un usuario de forma fraudulenta. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

Para definir las extensiones de ficheros adjuntos que no serán tratadas por la protección haz clic en **Opciones avanzadas.** Se mostrará la ventana de exclusiones.

Para acceder a opciones avanzadas de protección de correo consulta el apartado dedicado a Exchange Server más adelante en este mismo capítulo.

Web

En esta pestaña se podrá configurar el funcionamiento de la protección para la navegación Web. De esta manera el administrador evitará que los usuarios se vean afectados por malware o phishing procedente de páginas Web.

Esta protección va desactivada por defecto. Para activarla, sigue los siguientes pasos:

- Marca la casilla para activar la protección permanente para navegación Web en estaciones y/o servidores Windows.

La detección de virus se encuentra siempre activada.

- Para activar detección de phishing en las páginas Web, marca la casilla correspondiente.

13.5. Configuración de la protección Firewall y detección de intrusos

Adaptive Defense 360 ofrece tres herramientas básicas a la hora de filtrar el tráfico de red que recibe o envía el equipo protegido:

- **Protección mediante reglas de sistema**: se trata de las tradicionales reglas que describen las características de la comunicación: puertos, IPs, protocolos etc. con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas establecidas.
- **Protección de programas**: establece un conjunto de reglas que permitan o denieguen la comunicación a determinados programas instalados en el equipo de usuario
- **Sistema de detección de intrusos**: permite detectar patrones de tráfico malformado que

afecten a la seguridad o al rendimiento del equipo protegido, rechazando dichos patrones.

Para configurar la protección del firewall decide si los usuarios configurarán el firewall desde sus equipos (firewall en modo usuario) o si será el administrador quien se encargue de ello (firewall en modo administrador).

- **Firewall en modo usuario**

Selecciona la opción que permite que la configuración del firewall la establezca el usuario de cada equipo.

En este caso el usuario podrá acceder a la configuración del firewall desde el agente de su equipo.

- **Firewall en modo administrador**

Mantén la opción por defecto **Aplicar la siguiente configuración al firewall** para configurar el cortafuegos de forma centralizada desde la consola Web, indicando si la configuración de la protección firewall se aplicará a servidores y/o estaciones Windows mediante las casillas correspondientes.

General

Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso, según se trate de accesos públicos, como pueden ser las redes wifi de un cibercafé, o redes gestionadas o de acceso limitado como la red de la empresa. Para ajustar el comportamiento por defecto del cortafuegos el administrador de la red selecciona el tipo de red al que se conectan usualmente los equipos del perfil configurado.

- **Red pública**: Una red de este tipo es propia de cibercafé, aeropuertos, etc. Conlleva limitación de su nivel de visibilidad y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios
- **Red de confianza**: Este tipo de red generalmente es de oficina o casera. El equipo es perfectamente visible para el resto de equipos de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios

La variación del comportamiento del software **Adaptive Defense 360** según la red seleccionada se refleja en la consola en el número de reglas añadidas de forma automática. Estas reglas se pueden ver en la pestaña **Programas** y **Sistema** como **reglas de Panda**

Programas

En esta pestaña se establecen qué programas del usuario se podrán comunicar con la red y cuáles no.

Para desarrollar una correcta estrategia de protección sigue los pasos mostrados a continuación

en el orden indicado:

1 **Establece la acción por defecto en Acción por defecto.**

- **Permitir acceso** establece la estrategia de permitir las conexiones de los programas que no haya sido definido su comportamiento mediante una regla en el siguiente paso. Este es el modo por defecto y considerado básico.
- **Denegar acceso** establece la estrategia de denegar las conexiones de los programas que no haya sido definido su comportamiento mediante una regla en el siguiente paso. Este es el modo avanzado ya que requiere añadir reglas con todos los programas que los usuarios utilizan de forma habitual; de otro modo las comunicaciones de esos programas serán denegadas, afectando probablemente a su buen funcionamiento.

2 **Haz clic en el botón Añadir para definir el comportamiento específico de una aplicación concreta:**

- **Permitir entrantes y salientes**: El programa se podrá conectar a la red (Internet y redes locales) y también permitirá que otros programas o usuarios se conecten con él. Existen ciertos tipos de programas que requieren este tipo de permisos para funcionar correctamente: programas de intercambio de archivos, aplicaciones de chat, navegadores de Internet, etc.
- **Permitir salientes**: El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.
- **Permitir entrantes**: El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos de salida.
- **No permitir ninguna conexión**: El programa no podrá acceder a la red.

Prevención de intrusiones

La prevención de intrusiones permite detectar y rechazar tráfico mal formado y preparado para impactar en el rendimiento o la seguridad del equipo a proteger. Este tipo de tráfico puede provocar un mal funcionamiento de los programas del usuario que lo reciben y puede derivar en problemas serios de seguridad, permitiendo la ejecución de aplicaciones del usuario de forma remota por parte del hacker, extracción y robo de información etc.

Adaptive Defense 360 identifica 15 tipos de patrones genéricos que pueden ser activados o desactivados haciendo clic en la casilla apropiada. A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

- **IP explicit path**: Se rechazan los paquetes IP que tengan la opción de "explicit route". Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.
- **Land Attack**: Comprueba intentos de denegación de servicios mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.
- **SYN flood** lanza inicios de conexión TCP de forma masiva para obligar al equipo a comprometer recursos para cada una de esas conexiones. Se establece un límite máximo de conexiones TCP abiertas para evitar una sobrecarga del equipo atacado.
- **TCP Port Scan**: detecta si un equipo intenta conectarse a varios puertos del equipo protegido en un tiempo determinado. Detiene el ataque denegando las respuestas al equipo sospechoso. Adicionalmente filtra las respuestas para que el origen del tráfico de scaneo ni siquiera obtenga respuesta de puerto cerrado

- **TCP Flags Check**: Detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de "Port Scanning" al detener ataques de este tipocomo "SYN & FIN" y "NULL FLAGS" y a la de "OS identification" ya que muchas de estas pruebas se basan en respuestas a paquetes TCP inválidos
- **Header lengths**
  - **IP**: Se rechazan los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos.
  - **TCP**: Se rechazan los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos.
  - **Fragmentation** control: Realiza comprobaciones sobre el estado de los fragmentos de un paquete a reensamblar, protegiendo de ataques de agotamiento de memoria por ausencia de fragmentos, redireccionado de ICMP disfrazado de UDP y scanning de máquina disponible.
- **UDP Flood**: Se rechazan los paquetes UDP que llegan a un determinado puerto si exceden en cantidad a un número determinado en un periodo determinado.
- **UDP Port Scan**: Protección contra escaneo de puertos UDP.
- **Smart WINS**: Se rechazan las respuestas WINS que no se corresponden con peticiones que el equipo haya enviado
- **Smart DNS**: Se rechazan las respuestas DNS que no se corresponden con peticiones que el equipo haya enviado
- **Smart DHCP**: Se rechazan las respuestas DHCP que no se corresponden con peticiones que el equipo haya enviado
- **ICMP Attack**: Este filtro implementa varias comprobaciones:
  - **SmallPMTU**: Mediante la inspección de los paquetes ICMP se detectan valores inválidos en el tamaño del paquete utilizados para generar una denegación de servicio o ralentizar el tráfico saliente.
  - **SMURF**: Envío de grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando el tráfico por cada equipo de la subred. Se rechazan las respuestas ICMP no solicitadas si estás superan una determinada cantidad en un segundo.
  - **Drop unsolicited ICMP replies**: Se rechazan todas las respuestas ICMP no solicitadas o que hayan expirado por el timeout establecido.
- **ICMP Filter echo request**: se rechazan las peticiones de Echo request.
- **Smart ARP**: Se rechazan las respuestas ARP que no se corresponden con peticiones que el equipo protegido haya enviado para evitar escenarios de tipo ARP cache poison.
- **OS Detection**: Falsea datos en respuestas al remitente para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos a aprovechar las vulnerabilidades asociadas al sistema operativo detectado. Esta defensa se complementa con la de "TCP Flags Check".

Sistema

En esta pestaña se definen las reglas tradicionales de filtrado de tráfico TCP/IP. **Adaptive Defense 360** extrae el valor de ciertos campos de las cabeceras de cada paquete que reciben o envían los equipos protegidos y explora el listado de reglas introducido por el administrador. Si alguna regla coincide con el tráfico examinado se ejecuta la acción asociada.

Mediante las reglas de sistema se establecen reglas de conexión que afectarán a todo el sistema, independientemente del proceso que las gestione, y son prioritarias con respecto a las reglas configuradas anteriormente para la conexión de los programas a la red.

Para desarrollar una correcta estrategia de protección frente a tráfico no deseado o peligroso sigue los pasos mostrados a continuación, en el orden que se indica:

1 **Establece la acción por defecto del cortafuegos en Acción por defecto, situada en la pestaña Programas.**

- **Permitir acceso** establece la estrategia de permitir las conexiones que no hayan sido definido su comportamiento mediante reglas en el siguiente paso. Por la misma razón expuesta anteriormente en la pestaña **Programas**, este es el modo básico de configuración: todas las conexiones no descritas mediante reglas vistas más adelante en el paso 2 serán aceptadas.
- **Denegar acceso** establece la estrategia de denegar las conexiones que no haya sido definido su comportamiento mediante reglas en el siguiente paso. Por la misma razón expuesta anteriormente en la pestaña **Programas**, este es el modo avanzado de configuración: todas las conexiones no descritas mediante reglas vistas más adelante en el paso 2 serán automáticamente denegadas.

2 **Haz clic en el botón Añadir para agregar reglas que describen conexiones de forma específica junto a una acción asociada.**

El orden de las reglas en la lista no es aleatorio, su aplicación se evalúa en orden descendente y, por lo tanto, al desplazar una regla hacia arriba o abajo en la lista, se modificará la prioridad en su aplicación.

A continuación, se describen los campos que forman una regla de sistema:

- **Nombre de regla**: nombre de la regla. No se admiten repetidas
- **Acción a realizar**: Establece la acción que ejecutará **Adaptive Defense 360** si la regla coincide con el tráfico examinado.
  - **Permitir**: permite el tráfico
  - **Denegar**: bloquea el tráfico. Se hace un Drop de la conexión
- **Sentido**: establece la dirección del tráfico para protocolo orientados a conexión como TCP
  - **Salientes**: tráfico saliente
  - **Entrantes**: tráfico entrante
- **Zona**
- **Protocolo**: permite especificar el protocolo de la regla. Según el protocolo elegido el campo local ports cambiará para ajustarse a sus características
  - **TCP**
  - **UDP**
  - **ICMP**
  - **IP Types**
- **Puertos locales / Servicios / Protocolos**: dependiendo del tipo de protocolo elegido se mostrará un campo u otro:

- **Puertos locales**: permite especificar los puertos locales de TCP y UDP. Se muestra un desplegable con los puertos más comunes y un campo personalizado para agregar cualquier puerto entre el rango 0-65535. Para introducir varios puertos independientes es necesario separarlos por comas. En caso de querer utilizar rangos es necesario utilizar el guion. (Ej: 80, 25, 120-134)
- **Servicios**: permite especificar el subtipo de mensaje ICMP
- **Protocolos**: permite especificar el protocolo de nivel superior que viajará en el paquete IP examinado.

13.6. Configuración del control de dispositivos

Dispositivos de uso común como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles también pueden constituir una vía de infección para los equipos.

La opción de configuración del control de dispositivos permite determinar el comportamiento de este tipo de dispositivos autorizando y asignando un nivel de utilización.

Para activar el control de dispositivos sigue los pasos mostrados a continuación:

- Marca la casilla **Activar el control de dispositivos**.
- Elige en el desplegable correspondiente el nivel de autorización del dispositivo
  - En el caso de las llaves USB y las unidades CD/DVD elige entre **bloquear**, **Permitir lectura** o **Permitir lectura y escritura**.
  - Para Bluetooth, dispositivos de imágenes, modems USB y teléfono móviles las opciones son **Permitir y Bloquear**.

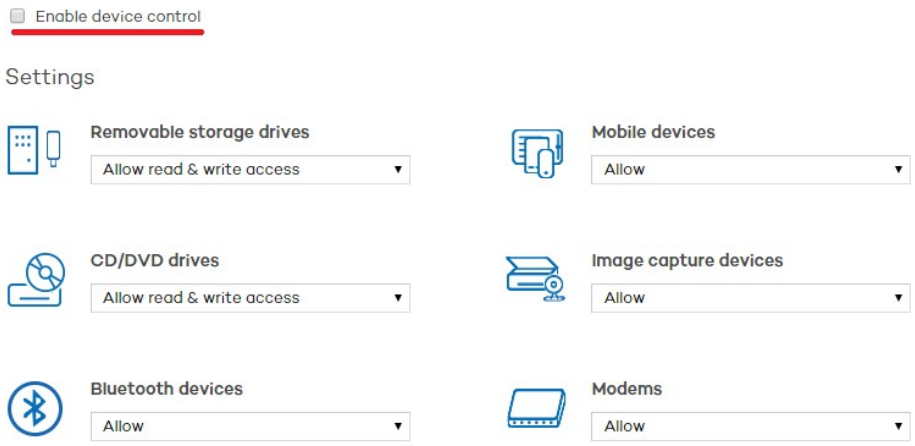


*Figura 65: Habilitar **Control de dispositivos** y vista de las categorías de dispositivos soportadas*

13.6.1 Exclusiones de dispositivos

En algunos casos pueden no permitirse determinado tipo de dispositivos, pero tener que autorizar el uso de un dispositivo en particular de ese tipo concreto.

Esta situación se implementa mediante una "lista blanca": una lista de dispositivos cuyo uso se permite, aunque pertenezcan a grupos de dispositivos que se hayan marcado como no

autorizados.

Para ello **Adaptive Defense 360** elabora un listado de dispositivos conectados por cada equipo. Haz clic en **Añadir** dentro de **Dispositivos permitidos** para mostrar un listado del cual puedes elegir los dispositivos que quieras excluir del bloqueo general configurado.

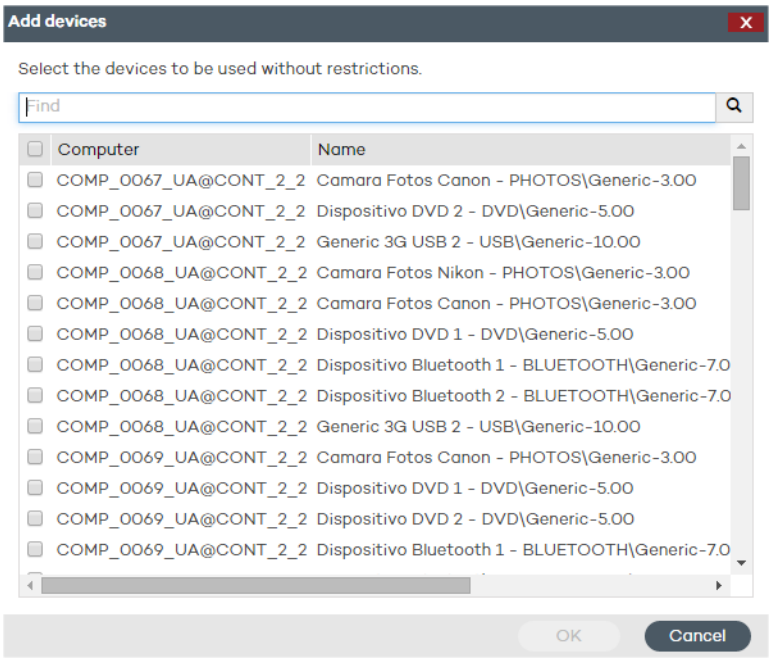


Figura 66: Listado de identificadores de dispositivos encontrados en la red

13.6.2 Exportar e importar listas de dispositivos permitidos

La lista de dispositivos permitidos se puede exportar a un archivo de texto. Esta operación también puede realizarse a la inversa, configurando en un archivo de texto la lista con los datos de los dispositivos que se desean permitir y a continuación importar esa lista desde la consola Web de **Adaptive Defense 360**.

Para exportar e importar listados de exclusiones ya configurados utiliza los botones **Exportar** e **Importar**

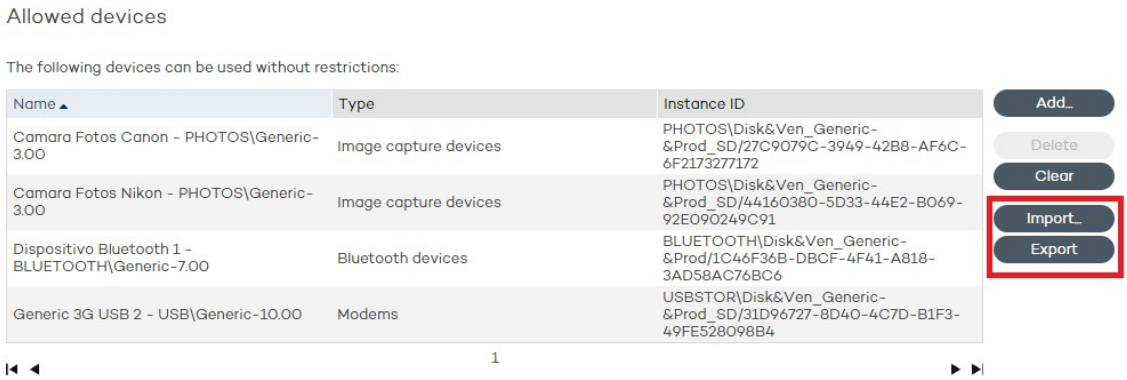


*Figura 67: Botones de **Importar** y **Exportar** listados de exclusiones*

13.6.3 Autorizar dispositivos una vez bloqueados

Cada vez que un dispositivo no autorizado intenta conectarse al equipo, **Adaptive Defense 360**

toma nota de ello y lo refleja en el **Detalle de detecciones**.

Este listado de detecciones está disponible desde el panel de control en la ventana **Estado** > **Origen de las detecciones** > **Dispositivos bloqueados**.

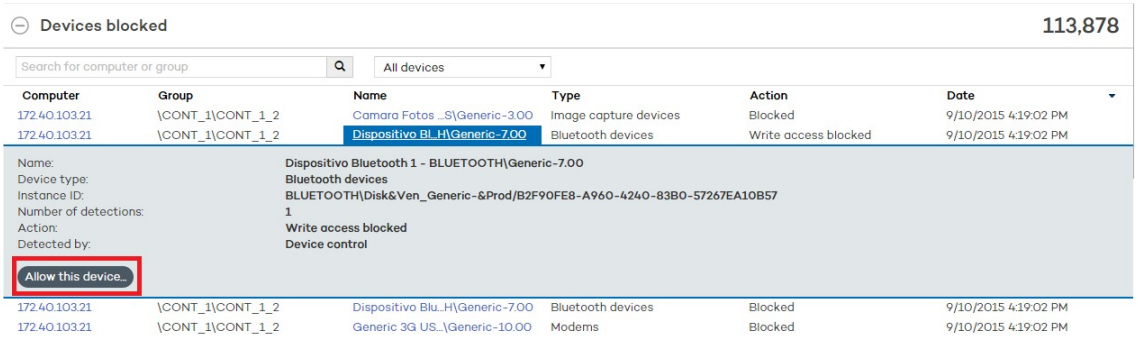


*Figura 68: Botón de **Permitir dispositivo** en los listados **Detalle de detecciones***

Dentro del detalle de la detección haz clic en el botón **Permitir este dispositivo** para seleccionar los perfiles afectados por la protección del dispositivo. De esta manera el dispositivo se incluirá en la lista de **Dispositivos permitidos** para los perfiles seleccionados.

13.6.4 Obtención del identificador único del dispositivo

Puedes obtener el identificador de dispositivos para utilizar dispositivos sin restricciones y sin esperar a que el usuario conecte los dispositivos en su equipo y excluirlos de forma manual. Para ello sigue los pasos siguientes:

- En el Administrador de dispositivos de Windows, accede a las propiedades del dispositivo USB que quieres identificar de forma única para excluirlo
- Accede a la pestaña **Detalles** y selecciona la propiedad **Recursos** en el desplegable **Propiedad**. A continuación, debería mostrarse un valor llamado `CM_DEVCAP_UNIQUEID`
- De nuevo en el desplegable Propiedad, selecciona Ruta de acceso a instancia del dispositivo y copia el identificador único de dispositivo

En el supuesto de que no se nombre ningún valor denominado `CM_DEVCAP_UNIQUEID` no será posible realizar la identificación del dispositivo de forma única. En este caso se puede utilizar como identificador el correspondiente al hardware del dispositivo.

En el desplegable Propiedad selecciona Identificador de hardware y se mostrará el identificador correspondiente, que será el que podrás utilizar. En este caso al usar este identificador se excluirá del control de dispositivos a todos los productos USB de la gama que posean ese identificador, ya que no habrá manera de diferenciar a unos de otros.

Con los identificadores únicos puedes elaborar una lista blanca e importarla tal y como se ha mostrado en el punto anterior.

13.6.5 Alertas

Se mostrarán al usuario avisos en su equipo con información de advertencia.

- Dispositivos no permitidos

Cuando la protección detecte que se ha conectado al equipo un dispositivo cuyo uso no esté permitido por el perfil de seguridad que se ha aplicado para ese equipo, se mostrará un aviso al respecto advirtiendo al usuario que no tiene permiso para acceder a dicho dispositivo.

- Dispositivos con permiso de solo lectura

El dispositivo conectado se mostrará con normalidad en el directorio Mi PC del equipo. Al hacer doble clic sobre la unidad, se mostrará un aviso advirtiendo de que el usuario no tiene permiso para escribir en el dispositivo.

13.7. Configuración de la protección para servidores Exchange

Si se disponen de las licencias apropiadas, desde la consola Web podrás activar la protección para servidores Exchange y aplicarla a cualquier servidor Exchange administrando.

La protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013 y 2016

La protección para servidores Exchange está compuesta por los módulos Antivirus, Anti-spam y Filtrado de contenidos.

Además, según el momento de análisis de **Adaptive Defense 360** en el flujo de correo, se distinguen dos formas de protección: protección de buzones y protección de transporte.

Como los modos de protección no están disponibles para todos los módulos de protección ni para todas las versiones de Exchange, la tabla mostrada a continuación muestra las combinaciones admitidas.

Módulo / modo	Antivirus	AntiSpam	Filtrado de contenidos
Buzón	2003, 2007, 2010		
Transporte	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016

Tabla 6:Modo de funcionamiento soportado según la versión de Exchange instalada

- **Protección de buzones**

Se utiliza en los servidores Exchange con el rol de Mailbox y permite analizar las carpetas / buzones en backgroud o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones solo se ofrece para el módulo Antivirus en los servidores Exchange 2003, 2007 y 2010

- **Protección de transporte**

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Mailbox y permite analizar el tráfico que es atravesado por el servidor Exchange.

13.7.1 Antivirus

Analiza en busca de virus, herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange

Para activar o desactivar la protección de buzones y/o de transporte haz clic en la casilla apropiada.

- **Protección de los buzones**

El comportamiento de la protección de los buzones es ligeramente diferente según se trate de Exchange 2013 / 2016 y el resto.

- En Exchange 2013 y 2016 no se permite manipular el mensaje; si contiene un elemento peligroso se introduce íntegro en cuarentena. El usuario protegido con **Adaptive Defense 360** recibirá un mensaje con el asunto original, pero con el cuerpo sustituido por un mensaje de advertencia, indicando que en caso de querer recuperar el mensaje original contacte con el administrador de la red.
- En el resto de versiones de Exchange se realiza la acción programada por Panda Security ante la detección de un elemento clasificado como malware: desinfectar el adjunto si es posible o introducirlo en cuarentena si no es posible. El usuario protegido con **Adaptive Defense 360** recibirá el mensaje con los adjuntos desinfectados o, en caso de que no fuera posible su desinfección, contendrán un fichero "`security_alert.txt`" de sustitución describiendo el motivo de la detección.

13.7.2 Anti-spam

Para activar o desactivar esta protección, utiliza la casilla de verificación **Detectar spam**

Acción para mensajes de spam

- **Dejar pasar el mensaje**: Añade la etiqueta Spam al Asunto de los mensajes. Esta será la opción configurada por defecto.
- **Mover el mensaje a...** especifica la dirección de correo electrónico a la que se moverá el mensaje, con la etiqueta Spam añadida en el Asunto.
- **Borrar el mensaje**
- **Marcar con SCL** (Spam Confidence Level).

SCL

SCL -Spam Confidence Level- es una escala de valores comprendidos entre el 0 y el 9 que se aplican a los mensajes de correo electrónico susceptibles de ser spam. El valor 9 se asigna a los mensajes que con total probabilidad son spam. El 0 es el valor que se aplica a los mensajes que no son spam. Este valor SCL se puede utilizar para marcar los mensajes que posteriormente serán tratados en función de un umbral configurable en el Directorio Activo: la protección adjudica al mensaje el valor SCL correspondiente y le permite pasar.

A continuación, será el administrador, en función del umbral determinado en el Directorio Activo, quien seleccione la acción que finalmente se realizará con el mensaje.

Direcciones y dominios permitidos y denegados

Configura listas de direcciones y dominios cuyos mensajes no serán analizados por la protección anti-spam (lista blanca) o listas de dominios y direcciones cuyos mensajes serán interceptados por la protección y eliminados (lista negra) con los botones **Añadir**, **Eliminar** y **Vaciar**

Las listas blancas y negras se rigen por las reglas siguientes:

- Si un dominio se encuentra en la lista negra y una dirección perteneciente a dicho dominio se encuentra en la lista blanca, se permitirá dicha dirección, pero no el resto de direcciones del dominio.
- Si un dominio se encuentra en la lista blanca y una dirección perteneciente a dicho dominio se encuentra en la lista negra, dicha dirección no será aceptada, pero sí el resto de direcciones de dicho dominio.
- Si un dominio (por ejemplo: domain.com) se encuentra en la lista negra y un subdominio de este (ej: mail1.domain.com) se encuentra en la lista blanca, se permitirán direcciones de dicho subdominio, pero no el resto de direcciones del dominio o de otros subdominios diferentes.
- Si un dominio se encuentra en la lista blanca también se considerarán incluidos en la lista blanca todos sus subdominios.

Filtrado de contenidos

Permite filtrar los mensajes de correo electrónico en función de la extensión de los archivos adjuntos incluidos en ellos.

Para ello se establece una lista de mensajes que pueden tener adjuntos sospechosos e indica la acción a realizar con dichos mensajes.

También se puede aplicar el filtrado de contenidos a mensajes que incluyan adjuntos con dobles extensiones

- **Considerar archivos adjuntos peligrosos los que tienen las siguientes extensiones**: Marca esta casilla para considerar como peligrosos los archivos adjuntos con alguna extensión determinada. Una vez marcada la casilla, configura la lista de extensiones a bloquear con los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar**.
- **Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto en**

los siguientes casos: el filtrado de contenidos impedirá la entrada de todos los mensajes de correo electrónico con adjuntos de doble extensión, excepto aquellos cuyos adjuntos tengan las extensiones seleccionadas. Para configurar la lista de dobles extensiones que sí se permitirá utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar**.

- **Acción a realizar**: selecciona si deseas que los mensajes se borren o si prefieres desviarlos a otra dirección de correo electrónico. Esto puede resultar útil para analizar a posteriori los adjuntos recibidos y modificar la lista de extensiones seleccionadas como peligrosas

Registro de detecciones

Todas las detecciones producidas en un servidor Exchange son almacenadas localmente en un archivo CSV. De esta forma se ofrece información adicional acerca de la imposibilidad de entrega de los mensajes a sus destinatarios.

El fichero recibe el nombre `ExchangeLogDetections.csv` y se almacena en la carpeta

`%AllUsersProfile%\Panda Security\Panda Cloud Office Protection\Exchange`

El contenido del fichero se dispone en formato tabular con la siguiente distribución de campos:

- **Date**: fecha de la llegada del correo al servidor Exchange
- **From**: remitente del correo
- **To**: destinatario del correo.
- **Subjet**: asunto del correo.
- **Attachments**: listado con los ficheros adjuntos al correo.
- **Protection**
- **Action**

13.8. Configuración del control de acceso a las páginas Web

Restringe el acceso a determinadas categorías Web y permite configurar URLs individuales a las que se permitirá o restringirá el acceso. Esto contribuirá a la optimización del ancho de banda de la red y a la productividad del negocio.

Denegar el acceso a páginas Web

Las páginas Web se agrupan en 59 categorías. Selecciona aquellas categorías a denegar el acceso. Puedes modificar las categorías seleccionadas siempre que sea necesario.

Para activar el control de acceso a páginas Web para estaciones Windows, servidores Windows o ambos marca la casilla correspondiente y selecciona las categorías a denegar el acceso.

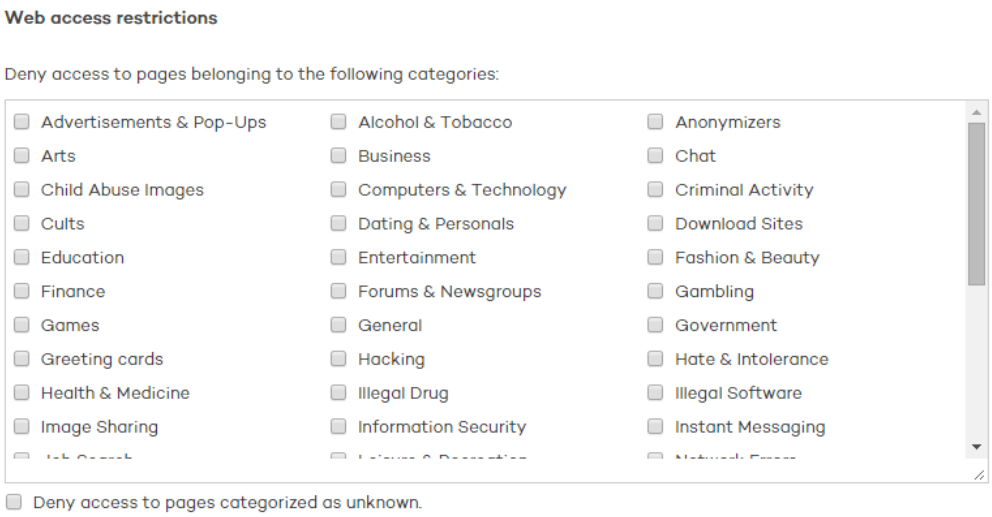


Figura 69: Listado de categorías de URLs

Cuando desde el equipo se intente acceder a una página Web que pertenece a una categoría de las anteriores, se mostrará un aviso en el navegador del usuario indicando el motivo de la denegación de acceso.

Cuando se modifiquen las categorías a las que se desea restringir o permitir el acceso, transcurrirá un plazo máximo de 15 minutos hasta que los equipos recojan la nueva configuración. Durante este intervalo de tiempo el comportamiento del control de acceso a páginas Web será el anterior a la modificación

Denegar el acceso a páginas de categoría desconocida

Para denegar el acceso a páginas no categorizadas activan la casilla **Denegar acceso a las páginas cuya categoría sea desconocida**

En Intranets o Webs de tipo interno que se conectan a través de los puertos 80 u 8080 puede suceder que se clasifiquen como pertenecientes a una categoría desconocida y, por tanto, se deniegue el acceso a ellas con el consiguiente perjuicio para los usuarios. Para mitigar esta situación añade las páginas Web desconocidas que sean necesarias a la lista blanca de exclusiones

Lista de direcciones y dominios permitidos o denegados

La lista blanca (acceso permitido) o lista negra (acceso denegado) especifica listas de páginas Web a las que siempre se permitirá o siempre se denegará el acceso.

Para modificar ambas listas:

- Introduce en la caja de texto la URL del dominio o dirección.
- Haz clic en **Añadir**.
- Utiliza los botones **Eliminar** y **Vaciar** para modificar la lista.
- Finalmente, haz clic en **Aceptar** para guardar la configuración.

Base de datos de URLs accedidas desde los equipos

Cada uno de los equipos recopila en una base de datos información sobre las URL a las que se ha accedido desde él. Esta base de datos solo se puede consultar en local, es decir, desde el propio equipo, durante un plazo de 30 días.

Los datos almacenados en la base de datos son:

- Identificador del usuario.
- Protocolo (http o https).
- Dominio.
- URL
- Categorías devueltas.
- Acción (Permitir/denegar).
- Fecha de acceso.
- Contador acumulado de accesos por categoría y dominio.

13.9. Configurar horarios del control de accesos a páginas Web

Puedes restringir dentro de la semana el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorizarlo en el horario no laborable o en el fin de semana.

Para activar el control horario de accesos a páginas Web elige la opción **Activar solo durante las siguientes horas.**

A continuación, selecciona las horas en las que quieras que el control horario esté activado. Para activarlo sólo en un horario determinado, marca la casilla correspondiente y utiliza la cuadrícula para señalar las horas en las que se activará.

- Para seleccionar días completos haz clic en el día de la semana indicado.
- Para seleccionar una misma hora en todos los días de la semana haz clic en la hora indicada

Se usará la hora local de cada equipo y no la hora del servidor Adaptive Defense 360

14. Perfiles de protección Linux

Configuración general
Configuración de la protección antivirus

14.1. Introducción

La configuración de un perfil de seguridad que aplique a equipos Linux se realiza desde la ventana **Configuración**, seleccionando el perfil a configurar en el panel de **Perfiles** y después el menú lateral **Windows** y **Linux**.

En este capítulo únicamente se detallarán las configuraciones soportadas por los sistemas Linux

14.2. Configuración general

Actualizaciones

En el caso de los equipos con sistema operativo Linux no es posible realizar una actualización automática, por lo que cuando exista una nueva versión de la protección ésta deberá instalarse de nuevo en los equipos.

Cuando transcurran 7 días desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos con sistema operativo Linux aparecerán como "desactualizados" en la ventana **Estado**, momento en el que el administrador podrá proceder a instalar la versión superior en los equipos.

En el caso de los equipos con sistema operativo Linux, no es posible configurar la periodicidad de la actualización automática del archivo de identificadores., se hará siempre cada 4 horas.

Análisis programados

A continuación, se indican los pasos necesarios para configurar una nueva tarea de análisis:

- Haz clic en el botón **Nuevo** para acceder a la ventana **Edición de perfil – Nueva tarea de análisis**.
- En la nueva ventana introduce la siguiente información:
  - **Nombre**: indica el nombre con el que quieres identificar el análisis que se va a programar.
  - **Tipo de análisis**: selecciona el tipo de análisis que se va a crear:
    - **Análisis inmediato**: Una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de **Adaptive Defense 360** y se constate que se ha producido alguna modificación en la configuración de la protección.
    - **Análisis programado**: el análisis tendrá lugar en la hora y fecha que se determine en Fecha de comienzo y Hora de comienzo. Mediante el desplegable es posible determinar si la hora de comienzo está referida al servidor **Adaptive Defense 360** o es tomada del equipo del usuario.
    - **Análisis periódico**: determina la fecha y hora de comienzo, y selecciona en el desplegable **Repetición** la periodicidad que desea adjudicar al análisis.
  - **Analizar**: selecciona el alcance del análisis
    - **Todo el PC**: incluye los discos duros y unidades USB

  - **Discos duros**
  - **Otros elementos**: analizar elementos concretos almacenados (archivos, carpetas...). Introduce la ruta en la que se encuentra el elemento a analizar. El formato de la ruta ha de empezar por /

    Ejemplo: `/root/documents`

- Haz clic en el link **Opciones avanzadas de análisis** para configurar aspectos complementarios de los análisis programados:
  - Activar el análisis de archivos comprimidos.
  - Seleccionar el software malintencionado que desea analizar: **Hacking tools y PUPs y Virus** siempre están activos.
  - Analizar todo por defecto o excluir del análisis determinadas extensiones, carpetas o archivos. Para conformar la lista de exclusiones utiliza los botones **Añadir, Vaciar y Eliminar**.

Alertas

Las alertas no están soportadas en Linux

Opciones avanzadas

- **Instalación**: La ruta de instalación no es configurable.
- **Conexión a la inteligencia colectiva**: no es posible desactivar la conexión con la Inteligencia Colectiva, por lo que siempre que los equipos estén conectados a Internet la protección instalada en ellos se alimentará de ella.
- **Opciones de conexión con el servidor**: esta opción no está disponible en Linux
- **Opciones de cuarentena**: la cuarentena no está soportada en Linux
- **Contraseña de administrador**: esta opción no está disponible en Linux

14.3. Configuración de la protección antivirus

En equipos Linux no existe protección permanente de ficheros. De esta forma el método para proteger los equipos pasa por la realización de análisis bajo demanda o la programación de análisis periódicos explicados en el apartado anterior.

15. Perfiles de protección Mac OS X

Características particulares de la protección para Mac OS X

Configuración general de la protección para OS X

Configuración de la protección antivirus

15.1. Introducción

La configuración de un perfil de seguridad para equipos Mac OS X se realiza en la ventana **Configuración.** Selecciona el perfil a configurar en el panel de **Perfiles** y haz clic en el menú lateral **OS X.**

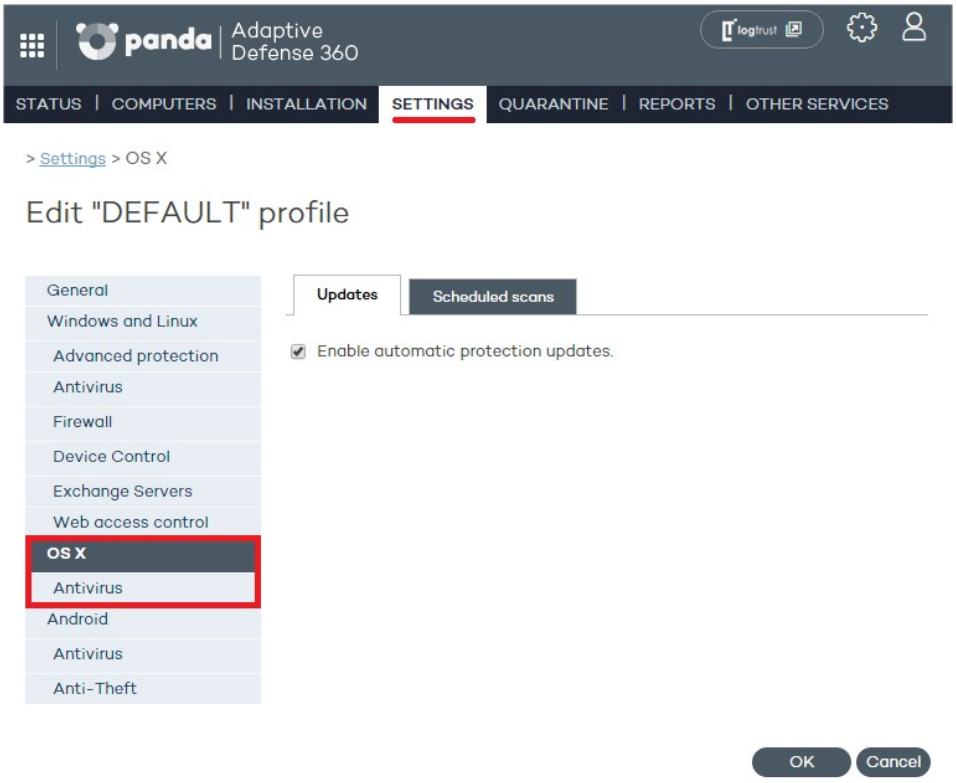


Figura 70: Acceso a la configuración de un perfil Mac OS X

15.2. Características particulares de la protección para Mac OS X

La protección para OS X reúne una serie de características propias que la diferencian de la protección para equipos con sistema operativo Windows/Linux.

Configuración de las actualizaciones en equipos con sistema operativo OS X

En equipos con sistema operativo OS X no es posible configurar la periodicidad de la actualización automática del archivo de identificadores, por lo que se realizará cada hora.

Transcurridas 48 horas desde que exista una versión del archivo de identificadores superior a la que los equipos tienen instalada, los equipos se mostrarán como desactualizados en la ventana **Estado**.

Frecuencias de las actualizaciones de la protección para equipos con OS X

Las frecuencias con que se realizan las actualizaciones de la protección para los equipos con sistema operativo OS X, son las siguientes:

- Actualización del fichero de firmas: Cada hora

- Cambios en la configuración de la protección: Cada 4 horas
- Actualización de la información de detecciones: Cada 6 horas
- Actualización de la información del estado de los equipos: Cada 12 horas

Actualización automática del motor de la protección

En equipos con sistema operativo OS X la actualización de la protección se realiza de forma automática, aunque es posible desactivarla desde la consola Web de administración. Transcurridas 72 horas desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos se mostrarán como desactualizados en la ventana **Estado**. Durante la instalación se procederá a desinstalar la versión anterior y a instalar la nueva.

15.3. Configuración general de la protección para OS X

Haciendo clic en el menú lateral **OS X** se accede a la configuración general de la protección

Análisis programados

Utiliza las opciones que se muestran en la pestaña **Análisis programados** para crear tareas de análisis, periódicas, puntuales o inmediatas y determinar si afectarán a todo el Mac o a determinados elementos del mismo.

También podrás optar por programar análisis exclusivos de los discos duros o especificar las rutas concretas en las que se encuentran las carpetas o archivos que deseas analizar.

A medida que se vayan creando tareas de análisis, éstas se irán añadiendo en el listado principal de la pestaña **Análisis programados** de la ventana **Editar perfil**, desde donde podrá editarlas o eliminarlas.

A continuación, se indican los pasos necesarios para configurar una nueva tarea de análisis:

- Haz clic en el botón **Nuevo** para acceder a la ventana **Edición de perfil** – **Nueva tarea de análisis**.
- En la nueva ventana introduce la siguiente información:
  - **Nombre**: indica el nombre con el que quieres identificar el análisis que va a programar.
  - **Tipo de análisis**: selecciona el tipo de análisis que vas a crear:
    - **Análisis inmediato**: Una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de **Adaptive Defense 360** y se constate que se ha producido alguna modificación en la configuración de la protección.
    - **Análisis programado**: el análisis tendrá lugar en la hora y fecha que se determine en Fecha de comienzo y Hora de comienzo. Mediante el desplegable es posible determinar si la hora de comienzo está referida al servidor **Adaptive Defense 360** o es tomada del equipo del usuario.
    - **Análisis periódico**: determina la fecha y hora de comienzo, y selecciona en el desplegable **Repetición** la periodicidad que desea adjudicar al análisis.

- **Analizar**: selecciona el alcance del análisis:
  - **Discos duros**
  - **Otros elementos**: analiza elementos concretos almacenados (archivos, carpetas...). Será necesario introducir la ruta en la que se encuentra el elemento a analizar.

    El formato de la ruta ha de tener el formato Linux.

    Ejemplo:

    ```
    /root/documents
    ```

    El número máximo de rutas a analizar que podrás introducir por cada perfil es 10. En función del permiso que se posea se podrán establecer rutas específicas de análisis.

- Haz clic en el link **Opciones avanzadas de análisis** para configurar aspectos complementarios de los análisis programados:
  - Análisis de archivos comprimidos.
  - Software malintencionado a analizar. **Virus** siempre estará activo.
  - Analizar todo o excluir del análisis determinadas carpetas. Utiliza los botones **Añadir**, **Vaciar** y **Eliminar** para conformar la lista de exclusiones.

15.4. Configuración de la protección antivirus

Selecciona la casilla **Activar protección permanente de archivos** proteger el sistema de ficheros de los equipos Mac OS X.

Exclusiones

Permite configurar elementos carpetas en los equipos Mac OS X de la red que no serán analizados por la protección **Adaptive Defense 360.**

16. Perfiles de protección Android

Configuración de la protección antivirus
Configuración de la protección antirrobo

16.1. Introducción

El módulo de protección para dispositivos Android consta de dos apartados: antivirus y protección contra el robo.

Para configurar la protección que aplica a tablets y smartphones Android haz clic ventana **Configuración**, selecciona el perfil a configurar en el panel de **Perfiles** y haz clic en el menú lateral **Android**.

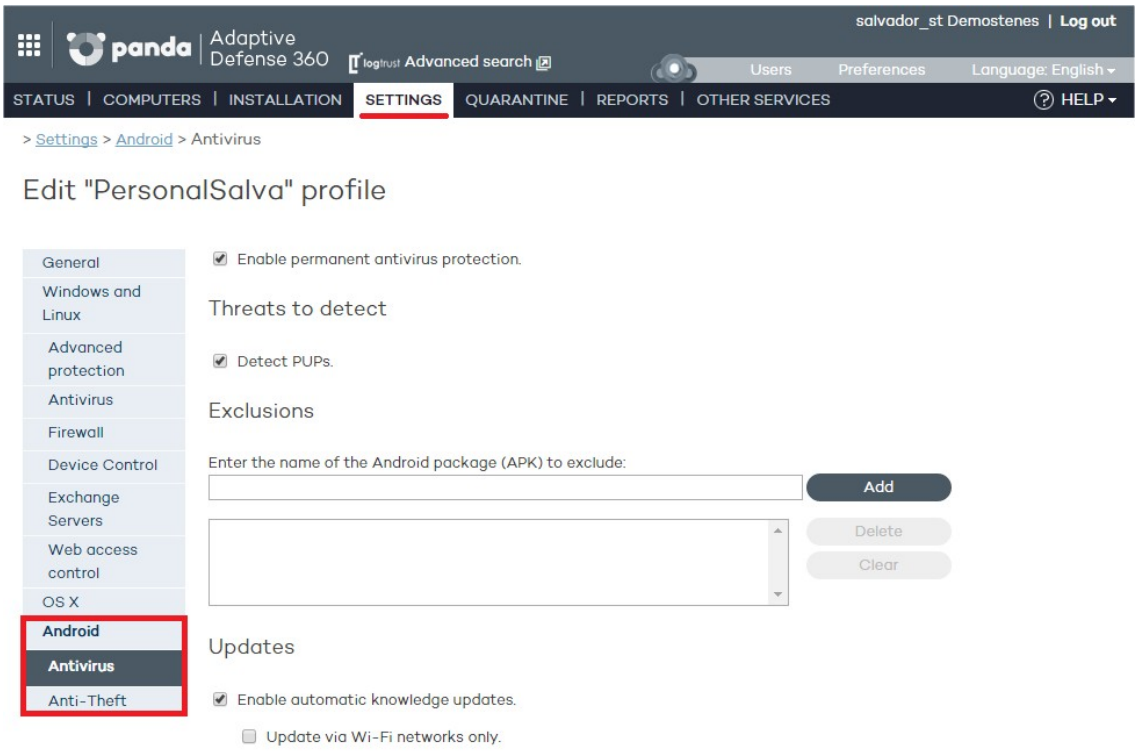


Figura 71: Acceso a la configuración de un perfil de proteccion Android

16.2. Configuración de la protección antivirus

La protección antivirus para smartphones Android protege los dispositivos frente a la instalación de aplicaciones con malware y PUPs analizando bajo demanda o de forma permanente el dispositivo móvil y las tarjetas de memoria SD conectadas.

Marca la casilla **Activar protección permanente antivirus** para activar la detección frente al malware. Selecciona la casilla **Detectar PUPs** para detectar programas potencialmente no deseados.

Exclusiones

La protección para Android permite realizar exclusiones de cualquiera de las aplicaciones instaladas, en su totalidad. Para ello, sigue los siguientes pasos:

- Introduce el nombre del paquete de Android (apk) que deseas excluir de los análisis y haz clic en **Añadir**.

- Utiliza los botones **Eliminar** y **Vaciar** si necesitas limpiar o modificar la lista de exclusiones.

Actualizaciones

Para actualizar el archivo de identificadores de forma automática marca la casilla **Activar actualización automática del conocimiento**. Además, también se pueden limitar las actualizaciones únicamente a aquellos momentos en que el usuario esté conectado a una red Wi-Fi para evitar cargos en la tarifa de datos contratada.

Análisis programados

Para programar un análisis, haz clic en el botón **Nuevo**.

Para crear tareas de análisis, que podrán ser inmediatas, programadas o periódicas utiliza las opciones que se muestran en la ventana **Nueva tarea de análisis**.

A medida que se vayan creando tareas de análisis, éstas se mostrarán en el listado de análisis programados del perfil para el que está configurando la protección antivirus. Desde allí se podrán editar o eliminar.

- **Análisis inmediato**: una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de **Adaptive Defense 360**.
- **Análisis programado**: el análisis tendrá lugar en la hora y fecha determinadas en la configuración. Para ello es necesario que la configuración de la programación se realice con la antelación suficiente. En caso de no disponer de conexión con el servidor de **Adaptive Defense 360** en la fecha y hora programadas, el análisis se realizará en el momento en que se establezca la conexión.
- **Análisis periódico**: el análisis tendrá lugar en la hora y fecha que se determine y se repetirá con la periodicidad elegida. Es recomendable realizar la programación del análisis con antelación suficiente para garantizar la existencia de conexión con el servidor de **Adaptive Defense 360**. En caso contrario, el análisis se realizará en el momento en que se establezca la conexión.

16.3. Configuración de la protección antirrobo

La protección antirrobo de **Adaptive Defense 360** permite controlar en todo momento los dispositivos Android de la empresa y determinar cuál será su comportamiento en el caso de robo o pérdida.

Al configurar esta protección desde la consola Web **Adaptive Defense 360** podrás localizar los dispositivos, borrarlos, bloquearlos, sacar una fotografía al ladrón y enviarla por correo electrónico a una dirección concreta.

Para activar esta funcionalidad marca la casilla **Activar protección antirrobo**

- **Informar de la localización del dispositivo**: marca esta casilla si se requiere información sobre la localización del dispositivo automáticamente.
- **Sacar una foto al tercer intento de desbloqueo del dispositivo y enviarla por correo a las**

siguientes direcciones: marca esta casilla para recibir un correo electrónico cuando se detecte actividad en un dispositivo robado. A continuación, introduce la dirección o direcciones de correo electrónico a las que se enviará la fotografía. Separa las direcciones utilizando punto y coma (;). si además de la opción de envío de foto del ladrón, se ha seleccionado previamente la de localización del dispositivo, junto con la foto del ladrón se recibirá el mapa detallando la localización del dispositivo.

Una vez realizada esta configuración, desde la ventana **Detalles de equipo** podrás ver en todo momento dónde se encuentra el dispositivo, bloquearlo mediante una clave y modificar la dirección de correo electrónico para recibir la fotografía.

Privacidad (Modo privado)

Como administrador puedes conceder permiso al usuario de un dispositivo determinado para que lo utilice en modo privado. Esto permitirá al usuario desactivar las opciones automáticas de localización del dispositivo y de foto al ladrón

Al activar el modo privado el agente de **Adaptive Defense 360** solicitará al usuario el establecimiento de un código personal de 4 dígitos. Este código le será requerido al administrador en la consola Web de administración cuando decida utilizar las funciones de localización automática del dispositivo y de foto al ladrón.

17. Visibilidad y monitorización del malware

Panel de control
Detecciones de malware
Listados de incidencias y malware detectado

17.1. Introducción

Adaptive Defense 360 ofrece cuatro grandes grupos de herramientas para visualizar el estado de la seguridad del parque informático:

- Panel de control de información actualizada en tiempo real
- Listados de incidencias y malware detectado
- Listados de equipos y dispositivos de la red
- Informes consolidados con información recogida a lo largo del tiempo

Consulta el capítulo 18 y 19 para obtener más información acerca del listado de equipos y dispositivos de la red y de los informes consolidados

Con estas cuatro herramientas podrás valorar en todo momento y de forma muy precisa el potencial riesgo de infección de tus equipos gestionados.

El objetivo final de las herramientas de visualización y monitorización es el de poder determinar el impacto de las brechas de seguridad y tomar las medidas apropiadas, tanto para mitigar su efecto como para evitar situaciones equivalentes en el futuro.

17.2. Panel de control

El panel de control de **Adaptive Defense 360** es accesible desde la ventana **Estado** y está distribuido en dos grandes secciones: **Actividad y Detecciones**. Cada sección contiene diversos paneles que muestran toda la información necesaria para determinar el estado de la seguridad de un solo vistazo.

Los paneles se generan en tiempo real y son interactivos: pasando el ratón por encima de los elementos se muestran tooltips con información extendida, y haciendo clic en los elementos se abrirán ventanas con listados de información detallada.

El panel de control muestra la información relevante en intervalo de tiempo fijado por el administrador mediante la herramienta situada arriba a la derecha de la ventana Estado. Los intervalos disponibles son:

- Últimas 24 h
- Últimos 7 días
- Último mes
- Último año

A continuación, se describe el contenido de los distintos paneles y su objetivo.

17.3. Sección Actividad

La sección **Actividad** muestra la clasificación de los programas ejecutados y analizados en los equipos Windows de la red, las incidencias de seguridad detectadas y un acumulado de los elementos bloqueados desconocidos que están siendo clasificados por el sistema

Adaptive Defense 360 genera una incidencia en el panel **Actividad** por cada pareja equipo – amenaza – tipo de amenaza (malware o PUP) distinta encontrada. Si la causa original del aviso no es resuelta se generarán un máximo de 2 incidencias cada 24 horas por cada equipo – amenaza encontrada que requiera la atención del administrador.

Para los ataques de tipo exploit, se generará una alerta cada vez que **Adaptive Defense 360** detecte un intento de explotación de vulnerabilidad en el equipo del usuario, independientemente del tipo de explotación y del proceso afectado.

El panel de **Actividad** se divide en cuatro zonas:

- Clasificación de todos los programas ejecutados y analizados
- Programas maliciosos y exploits
- Programas potencialmente no deseados
- Elementos actualmente bloqueados en clasificación

Clasificación de todos los programas ejecutados y analizados

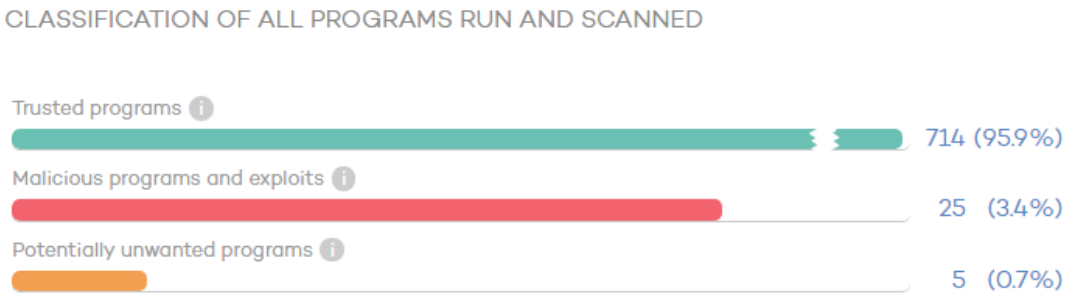


Figura 72: Panel de clasificación de los programas ejecutados y analizados

El objetivo de este panel es determinar de forma rápida el porcentaje de aplicaciones goodware y malware vistos y clasificados en la red del cliente, para el intervalo establecido por el administrador. El panel consta de tres barras horizontales junto al número de eventos asociado y el porcentaje sobre el total.

Este panel muestra datos de elementos clasificados para todo el parque informático, y no solo de aquellos equipos sobre los cuales el administrador tenga permisos según sus credenciales de acceso a la consola. Los elementos no clasificados no se muestran en este panel.

- **Aplicaciones confiables**: aplicaciones vistas en el parque del cliente que han sido analizadas y su clasificación ha sido goodware.

- **Aplicaciones maliciosas y exploits**: programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware, exploit, zero-day o ataques dirigidos.
- **Aplicaciones potencialmente no deseadas**: aplicaciones vistas en el parque del cliente que han sido analizadas su clasificación ha sido malware de tipo PUP

Haz clic en cada barra (exceptuando aplicaciones confiables) para abrir las ventanas de Listado MW o Listado PUP.

Programas maliciosos, exploits y programas potencialmente no deseados

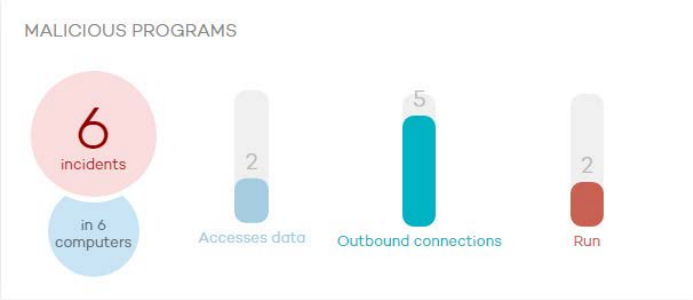


Figura 73: Panel de amenazas detectadas

La información presentada para el intervalo de tiempo fijado incluye datos de aquellos equipos sobre los cuales el administrador tiene acceso, determinado éste por las credenciales de acceso a la consola. Si el administrador no tiene permisos sobre todos los equipos de la red se mostrará un texto explicativo en la parte superior del panel.

- **Número de incidencias / avisos detectados**
- **Número de equipos con incidencias detectadas**
- **Acceden a datos**: Número de avisos que incluyen uno o varios accesos a información del usuario contenida en el disco duro de su equipo.
- **Conexiones exteriores**: número de avisos que establecieron conexiones con otros equipos.
- **Ejecutados**: Número de muestras malware que se llegaron a ejecutar

> *Programas maliciosos y exploits y programas potencialmente no deseados muestran datos con un intervalo como máximo de 1 mes. En el caso de que el administrador establezca un periodo de tiempo mayor se mostrara un texto explicativo en la parte superior del panel.*

Haz clic en cada uno de los elementos para mostrar la ventana de **Programas maliciosos y exploits** o **PUP**.

Elementos actualmente bloqueados en clasificación

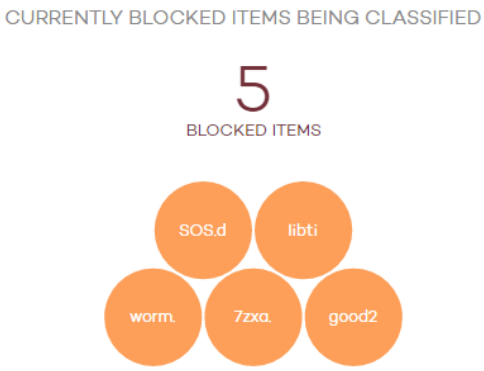


Figura 74: Panel de programas bloqueados en clasificación

En este panel se reflejan aquellos procesos desconocidos, detectados en la red del cliente y que requieren de una investigación en los laboratorios de Panda Security para poder ser clasificados como goodware o malware. Durante el tiempo que se emplea en su clasificación, los elementos pueden ser bloqueados en función del modo de configuración de la protección (Lock, Hardening o Audit).

La información mostrada en **Elementos Actualmente bloqueados en clasificación** es un histórico de los elementos bloqueados que aún no han sido clasificados. De esta forma, abarca desde la puesta en marcha del servicio en el cliente hasta el momento actual, y no se verá afectada por la selección del intervalo de tiempo establecida por el administrador.

El número total de elementos bloqueados en clasificación representa las aplicaciones diferentes (distinto MD5) que están siendo bloqueadas. Este número es independiente de la cantidad de intentos de ejecución que cada aplicación bloqueada ha llevado a cabo en cada equipo. Es posible que diferentes burbujas tengan en mismo nombre de malware. Este es un comportamiento típico en malware que utiliza técnicas de polimorfismo para evitar la detección de antivirus tradicionales basados en ficheros de firmas. Cada versión encontrada del malware (distinto MD5) será mostrada de forma independiente

Cada aplicación se contabiliza una única vez; esto quiere decir que, si una aplicación intenta ejecutarse en varias ocasiones en un mismo equipo, solo se contabilizará una vez.

El tamaño de las burbujas irá en función del número de equipos donde se encontró el malware y fue bloqueado.

Ejemplo:

En el panel de control se muestra un total de 8 elementos bloqueados en clasificación. Se trata de 8 aplicaciones que han sido bloqueadas y se están investigando. Cada una de ellas se representa con un círculo.

Supongamos que una de estas aplicaciones ha intentado ejecutarse en un equipo en treinta ocasiones durante un mismo día. Estas treinta ocasiones, al haberse dado en un mismo equipo y día, contabilizarán como una de las 8 detecciones que se muestran en el panel.

En el panel de control, las aplicaciones bloqueadas se muestran con un código de colores:

- **Naranja**: para las aplicaciones con probabilidad media de ser malware.
- **Naranja oscuro**: para las aplicaciones con probabilidad alta de ser malware.
- **Rojo**: para las aplicaciones con probabilidad muy alta de ser malware.

Al pasar el ratón por encima cada círculo se despliega mostrando su nombre completo y una serie de iconos que representan acciones clave:

Figura 75: Información de las acciones realizadas por los programas bloqueados

- **Carpeta**: el programa ha leído datos del disco duro del usuario.
- **Bola del mundo**: el programa estableció una conexión con otro equipo.

Para acceder al detalle de los elementos bloqueados actualmente en clasificación haz clic en el número de elementos bloqueados en clasificación o en alguno de los círculos

17.4. Sección Detecciones

La sección **Detecciones** consolida todos los intentos de intrusión que **Adaptive Defense 360** gestionó en el periodo de tiempo establecido.

Los datos reflejados abarcan todos los vectores de infección y todas las plataformas soportadas, de manera que el administrador pueda disponer de datos concretos (volumen, tipo, forma de ataque) relativos a la llegada a su red de malware que se ha desarrollado en un periodo de tiempo concreto.

Amenazas detectadas

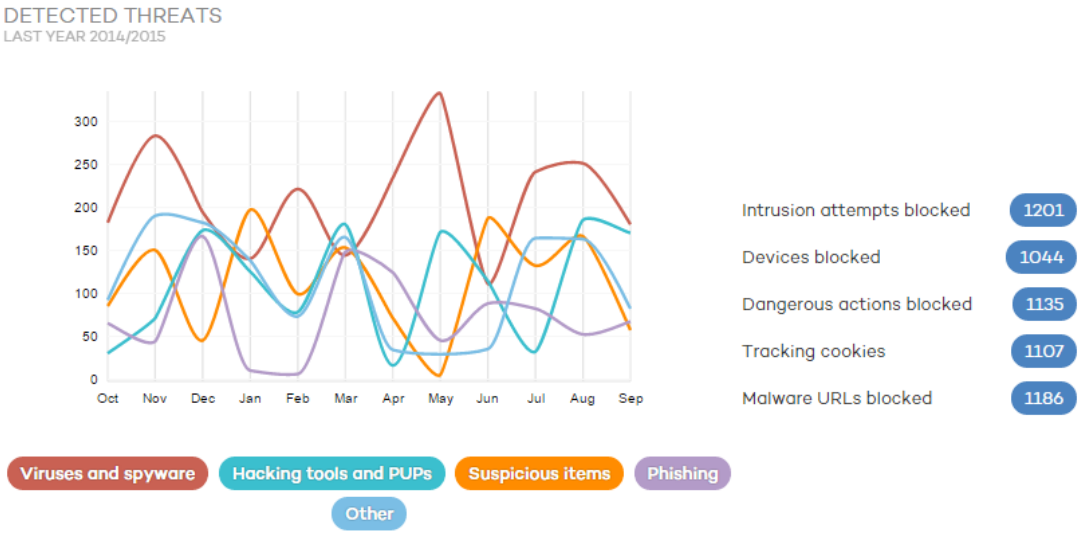


Figura 76: Panel de actividad consolidado

Este panel tiene dos secciones: un gráfico de líneas y un listado.

El diagrama de líneas es un evolutivo de las detecciones encontradas en el parque informático separadas por tipo de malware:

- Virus y spyware
- Herramientas de hacking y PUPs
- Sospechosos
- Phising
- Otros

En el eje de las Ys se muestran el número de ocurrencias y en el de las Xs la fecha.

Para simplificar el contenido del panel se puede pasar el puntero del ratón por encima de las leyendas mostradas en la parte inferior de la gráfica; de esta forma el resto de líneas desaparecerá.

El listado de la derecha muestra acciones no directamente relacionadas con malware encontrado pero importantes para que el administrador pueda revisarlas en busca de síntomas o situaciones potenciales de peligro.

- **Intentos de intrusión bloqueados**: son ataques detenidos por el Cortafuegos y el Sistema de prevención de intrusos
- **Dispositivos bloqueados**: periféricos bloqueados por el módulo de Control de dispositivos
- **Operaciones peligrosas bloqueadas**: detecciones realizadas por análisis del comportamiento local
- **Tracking cookies**: cookies detectadas para registrar la navegación de los usuarios
- **URL con malware bloqueadas**: direcciones Web que apuntaban a páginas con malware

Origen de las detecciones

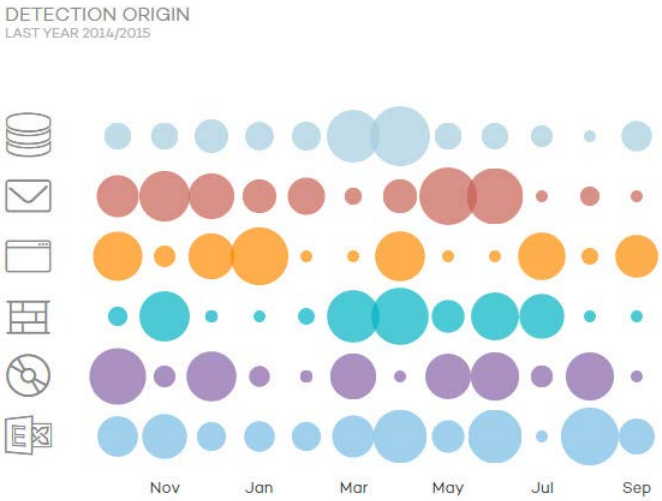


Figura 77: Panel de Actividad por vector de infección

Este panel muestra de forma gráfica los vectores de infección utilizados por el malware encontrado en la red.

En el eje de las Y se muestran diversos iconos que representan el vector de infección:

- Sistema de ficheros
- Correo local
- Navegación Web
- Firewall / Sistema de detección de intrusos
- Control de dispositivos
- Servidor Exchange

En el eje de las X se indica la fecha del intervalo seleccionado.

El contenido de la gráfica está formado por una serie de círculos de diferentes tamaños y colores. El tamaño del círculo refleja la proporción de ocurrencias encontradas y pasando el puntero del ratón por un círculo concreto se mostrará un tooltip con la suma de ocurrencias para una fecha y vector de infección determinado.

Spam Detectado

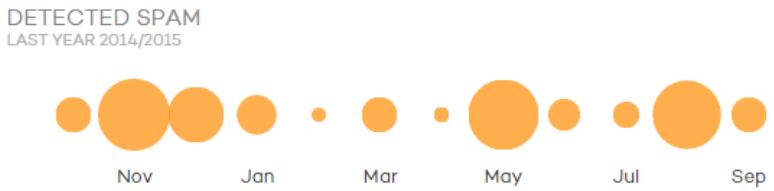


Figura 78: Panel de detección de spam consolidado por mes

Este panel muestra la cantidad de spam detectado en el servidor Exchange. En el eje de las X se indica las fechas del intervalo seleccionado.

El contenido de la gráfica está formado por una serie de círculos de diferentes tamaños. El tamaño del círculo refleja la proporción de ocurrencias encontradas y pasando el puntero del ratón por un círculo se mostrará un tooltip con la suma de ocurrencias para una fecha determinada.

Mensajes filtrados

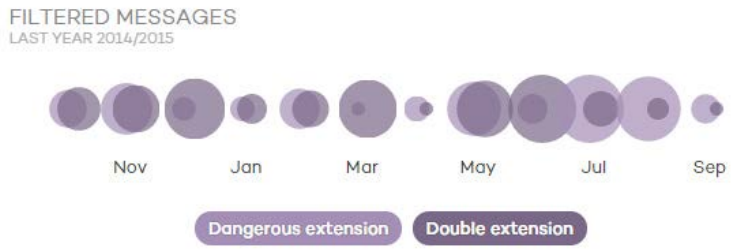


Figura 79: Panel de mensajes de correo filtrados por extensión peligrosa y doble extensión, consolidado por mes

Este panel muestra la cantidad de mensajes que fueron filtrados por el filtro de contenidos del servidor Exchange.

En el eje de las X se indica las fechas del intervalo seleccionado.

El contenido de la gráfica está formado por una serie de círculos de diferentes tamaños. El tamaño del círculo refleja la proporción de ocurrencias encontradas y pasando el puntero del ratón por un círculo se mostrará un tooltip con la suma de ocurrencias para una fecha.

Accesos a páginas Web

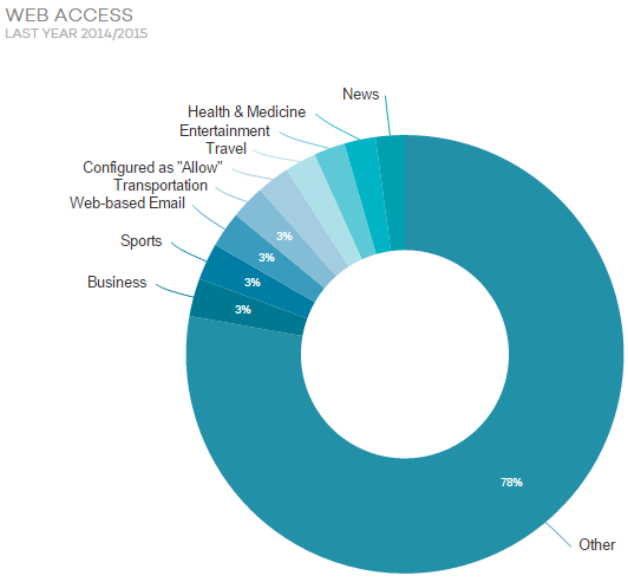


Figura 80: Panel de accesos web por categoría

Este panel muestra mediante un gráfico de tarta la distribución de categorías Web solicitadas por los usuarios de la red. Pasando el puntero del ratón por encima de los distintos segmentos se mostrará un tooltip con el total de peticiones registradas.

17.5. Listados de la sección Actividad

El objetivo de los listados es mostrar al administrador el detalle necesario para poder localizar el origen los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Para visualizar informes y listados detallados del malware o del software en estudio encontrado en la red del cliente haz clic en los diferentes paneles de la sección **Actividad**.

Desde los listados de Actividad también es posible añadir exclusiones y desbloquear elementos bloqueados en investigación

Las ventanas de listados tienen una estructura común mostrada a continuación:

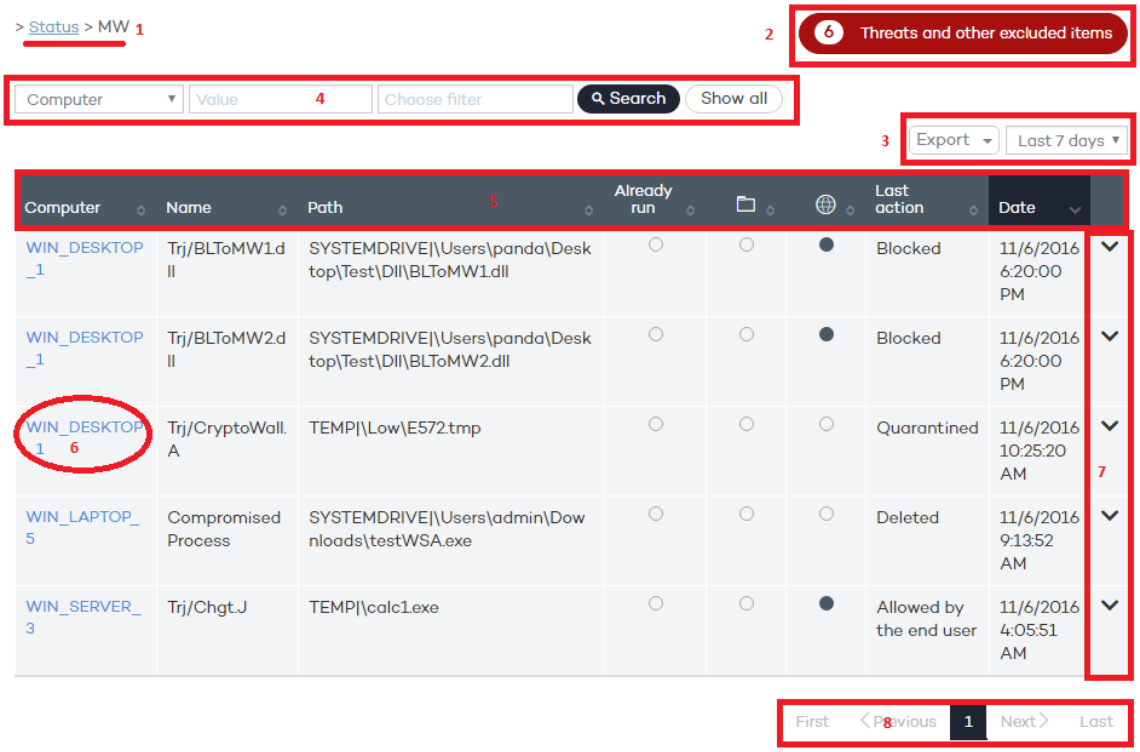


Figura 81: Estructura de un listado de Actividad

- Nombre del listado mostrado **(1)**
- Aviso de la existencia de ficheros clasificados como malware por **Adaptive Defense 360** que el administrador ha permitido su ejecución. **(2)**
- **Intervalo de datos mostrados y herramienta de exportación de listados**: permite al administrador aplicar los siguientes filtros de tiempo al listado:
  - Últimas 24 horas
  - Último día
  - Último mes.

  La herramienta de exportación permite salvar los listados mostrados en un fichero Excel o en formato CSV. **(3)**
- **Herramienta de filtrado**. Cada listado incorpora sus propios filtros en función de los datos presentados, explicados en cada apartado correspondiente. **(4)**
- El contenido de todas las tablas mostradas se puede ordenar haciendo clic en los campos cabecera. **(5)**
- Al hacer clic en el nombre del equipo se muestra información extendida: **(6)**
  - **Dirección IP:** dirección IP del equipo
  - **Fecha de instalación**: fecha en la que el agente fue instalado en el equipo
  - **Última conexión**: fecha en la que el equipo se conectó con el servidor **Adaptive Defense 360**
  - **Sistema operativo**
  - **Alertas disparadas**: número de alertas generadas en el intervalo seleccionado
  - **Grupo**: grupo al que pertenece el equipo
  - **Modo de protección**: modo de protección avanzada configurada para el equipo actualmente (Audit, Hardening, Lock).

- Desplegable con información de las acciones del malware. Consulta el capítulo 22 Análisis forense para más información sobre las acciones del malware detectado. Consulta el capítulo 20 Herramientas de resolución para más información sobre las herramientas incorporadas en **Adaptive Defense 360** para solucionar problemas.
- Sistema de paginación para una navegación más cómoda.

17.5.1 Listado Programas maliciosos y exploits

Para mostrar el listado de las amenazas encontradas en los equipos protegidos con **Adaptive Defense 360 haz** clic en los distintos elementos del panel **Programas maliciosos y exploits** o en **Programas maliciosos y exploits** dentro del panel **Clasificación de todos los programas ejecutados y analizados**.

Este listado se divide en dos secciones, accesibles mediante el selector situado en la parte superior del listado. Cada sección muestra un tipo de malware: programas maliciosos y exploits

Figura 82: Selector del tipo de malware

Programas maliciosos

Muestra los programas que muestran un comportamiento peligroso para el equipo del usuario.

En la parte superior se encuentra la herramienta de búsqueda:

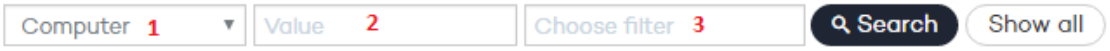


Figura 83: Herramienta de filtrado

El filtro **(1)** restringe la búsqueda indicada en la caja de texto **(2):**

- **Equipo**: la cadena de búsqueda se aplicará sobre el nombre del equipo
- **Nombre**: la cadena de búsqueda se aplicará sobre el nombre del malware
- **Fecha**: la cadena de búsqueda se aplicará sobre la fecha de la detección
- **MD5**: Digest de identificación del archivo
- **Origen de la infección**: la cadena de búsqueda se aplicará sobre la dirección IP del equipo de la red del cliente que inició el intento de infección.

El filtro **(3)** muestra las amenazas que satisfagan los criterios seleccionados

- **No Ejecutado**: malware detectado por la protección contra vulnerabilidades
- **Ejecutado**: el malware se llegó a ejecutar y equipo está infectado
- **Acceso a ficheros de datos**: el malware realizó accesos a disco para recoger información del equipo o para crear ficheros y los recursos necesarios para su ejecución
- **Comunicaciones**: el malware abrió sockets de comunicación con cualquier máquina, incluido localhost

- **Bloqueado**: malware conocido por **Adaptive Defense 360** y bloqueada su ejecución
- **Enviado a cuarentena**: el fichero no es desinfectable y se envió a cuarentena
- **Eliminado**
- **Desinfectado**: el fichero fue desinfectado por el antivirus
- **Permitido por el usuario final**: malware conocido por **Adaptive Defense 360** pero su ejecución fue permitida por el usuario.

Los campos de la tabla son los siguientes:

- **Equipo**: dispositivo donde se realizó la detección
- **Nombre**: nombre del malware
- **Ruta**: ruta completa donde reside el fichero infectado
- **Ejecutado alguna vez**: el malware se llegó a ejecutar
- **Ha accedido a datos**: amenaza ha accedido a ficheros que residen en el equipo del usuario.
- **Se ha comunicado con equipos externos**: la amenaza se comunica con equipos remotos para enviar o recibir datos.
- **Última acción**: acción aplicada sobre el malware (bloquear, permitir, enviar a cuarentena, eliminar, desinfectar, permitir por el usuario
- **Fecha**: fecha de la detección del malware en el equipo

Exploits

Muestra los programas que han recibido un intento de explotación.

En la parte superior se encuentra la herramienta de búsqueda:

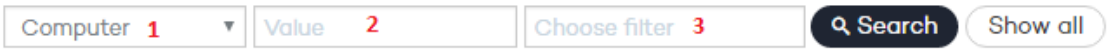


Figura 84: Herramienta de filtrado del listado de exploits detectados

El filtro **(1)** restringe la búsqueda indicada en la caja de texto **(2):**

- **Equipo**: la cadena de búsqueda se aplicará sobre el nombre del equipo
- **Programa comprometido**: la cadena de búsqueda se aplicará sobre la ruta y nombre del fichero comprometido por el exploit
- **Fecha**: la cadena de búsqueda se aplicará sobre la fecha de la detección
- **MD5**: la cadena de búsqueda se aplicará sobre el hash del fichero comprometido

El filtro **(3)** muestra las amenazas que satisfagan los criterios seleccionados

- **Riesgo SI**: busca los equipos que están o han estado en situación riesgo
- **Riesgo NO**: busca los equipos que no están en situación de riesgo
- **Permitido por el usuario:** busca los equipos donde el usuario ha rechazado la petición de

reinicio del proceso comprometido o del equipo.

- **Permitido por el administrador**: busca los equipos con programas comprometidos pero el administrador configuró la política de seguridad en modo auditoria.
- **Bloqueo inmediato**: busca los equipos con exploits bloqueados antes de su ejecución, sin requerir reinicio del programa objetivo de la amenaza.
- **Bloqueo tras finalizar proceso**: busca equipos con procesos comprometidos y reiniciados para bloquear el exploit.
- **Detectado. Pendiente de reinicio**: busca los equipos con procesos comprometidos que requieren un reinicio del proceso y todavía no se ha producido.

Los campos de la tabla son los siguientes:

- **Equipo**: dispositivo donde se detectó el intento de exploit
- **Programa comprometido**: ruta y nombre del fichero que ha recibido un ataque de tipo exploit.
- **Acción**: acción emprendida por **Adaptive Defense 360** en función de la política de seguridad asignada.
  - **Permitido por el usuario**: detección de exploit que requiere un reinicio del proceso o del equipo para ser bloqueado, en un equipo con una configuración de seguridad **Bloquear**, **Pedir permiso al usuario**, donde el usuario rechazó el reinicio del proceso comprometido.
  - **Permitido por el administrador**: detección de exploit en un equipo con una configuración de seguridad **Auditar** asignada.
  - **Bloqueo inmediato**: detección de exploit en un equipo con una configuración de seguridad **Bloquear** asignada, donde no fue necesario el reinicio del proceso ni del equipo.
  - **Bloqueo tras finalizar proceso**: detección de exploit en un equipo con una configuración de seguridad **Bloquear** asignada, donde fue necesario el reinicio del proceso o del equipo para completar el bloqueo.
  - **Detectado. Pendiente de reinicio**: detección de exploit en un equipo con una configuración de seguridad **Bloquear** asignada, donde es necesario el reinicio del proceso o del equipo para completar el bloqueo, pero todavía no se ha producido.
- **Riesgo**: indica si el equipo está o estuvo en riesgo por ataques de tipo exploit
  - **SI:** son los equipos que recibieron un ataque de tipo exploit bajo las circunstancias siguientes:
    - Tenían asignada una configuración de seguridad de tipo **Auditar**
    - El exploit requería el reinicio del proceso o del equipo para ser bloqueado, independientemente de cuando se haya producido o de si se ha producido o no.
  - **NO:** son los equipos que recibieron un ataque de tipo exploit y que no requieren un reinicio del proceso comprometido o del equipo para bloquearlo.
- **Fecha**: fecha de la detección del malware en el equipo

17.5.2 Elementos actualmente bloqueados en clasificación

En este listado se muestra una tabla con aquellos ficheros que, sin haber sido completada su clasificación, de una forma preliminar **Adaptive Defense 360** ha detectado algún riego en su

ejecución. Estos ficheros son bloqueados durante el tiempo empleado en su clasificación.

En la parte superior se encuentra la herramienta de búsqueda, que permite elegir entre los elementos bloqueados en el momento actual y un histórico de todos los elementos bloqueados hasta la fecha:

Figura 85: Selector de elementos actualmente bloqueados y listado histórico de elementos bloqueados desde la instalacion ***de Adaptive Defense 360***

Bloqueados actualmente

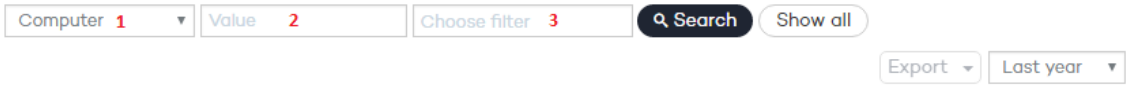


Figura 86: Herramienta de filtrado del listado de elementos bloqueados actualmente

El control **(1)** restringe la búsqueda indicada en la caja de texto **(2)** al campo seleccionado:

- **Equipo**: la cadena de búsqueda se aplicará sobre el nombre del equipo
- **Nombre**: la cadena de búsqueda se aplicará sobre el nombre del fichero bloqueado
- **Fecha**: la cadena de búsqueda se aplicará sobre la fecha del bloqueo
- **MD5**: la cadena de búsqueda se aplicará sobre el digest que representa al fichero bloqueado

El control **(3)** permite filtrar el listado por el modo de protección de **Adaptive Defense 360** que provocó el bloqueo (Lock o Hardening), y por el comportamiento mostrado por el proceso (Acceso a ficheros de datos, Comunicaciones), solo para aquellos elementos que haya sido permitida su ejecución con anterioridad y sus acciones hayan quedado registradas en el sistema.

Los campos de la pestaña Bloqueados actualmente son los siguientes:

- **Equipo**: Nombre del equipo donde se encontró el fichero desconocido
- **Nombre**: nombre del fichero desconocido.
- **Ruta**: indica dónde se ha detectado el fichero desconocido.
- **Ha accedido a datos**: el fichero desconocido ha accedido a ficheros que residen en el equipo del usuario.
- **Se ha comunicado con equipos externos**: el fichero desconocido se comunica con equipos remotos para enviar o recibir datos.
- **Modo de protección**: especifica el modo en el que se encontraba la protección en el momento de la detección del fichero desconocido.
- **Probabilidad de que sea malicioso**: Media, Alta, Muy Alta
- **Fecha**: fecha en la que se detectó por primera vez el fichero desconocido.

Historial

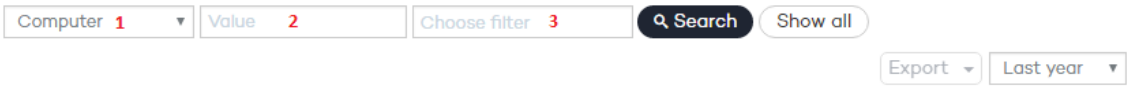


Figura 87: Herramienta de filtrado del historial de bloqueados

El control **(1)** restringe la búsqueda indicada en la caja de texto **(2)** al campo seleccionado:

- **Equipo**: la cadena de búsqueda se aplicará sobre el nombre del equipo
- **Nombre**: la cadena de búsqueda se aplicará sobre el nombre del fichero bloqueado
- **Fecha**: la cadena de búsqueda se aplicará sobre la fecha del bloqueo
- **MD5**: la cadena de búsqueda se aplicará sobre el digest que representa al fichero bloqueado

El control **(3)** permite filtrar el listado por diversos criterios, mostrados a continuación

- **Lock**: modo de protección avanzada cuando se produjo el bloqueo
- **Hardening**: modo de protección avanzada cuando se produjo el bloqueo
- **Acceso a ficheros de datos**: el fichero desconocido accedió a ficheros que residen en el equipo del usuario
- **Comunicaciones**: el fichero desconocido se comunicó con equipos remotos para enviar o recibir datos
- **Bloqueado**: el fichero desconocido fue bloqueado
- **Reclasificado a GW**: el fichero desconocido fue reclasificado como Goodware
- **Reclasificado a MW**: el fichero desconocido fue reclasificado como Malware
- **Reclasificado a PUP**: el fichero desconocido fue reclasificado como PUP
- **Excluido**: el fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución
- **No excluido**: el fichero desconocido no ha sido desbloqueado / excluido por el administrador

Los campos de la pestaña **Historial** son los siguientes:

- **Equipo**: nombre del equipo donde se encontró el fichero desconocido
- **Nombre**: nombre del fichero desconocido.
- **Ruta**: indica dónde se ha detectado el fichero desconocido.
- **Acción**: acción ejecutada
  - **Bloqueado**: el fichero desconocido fue bloqueado
  - **Reclasificado a GW**: el fichero desconocido fue reclasificado como Goodware
  - **Reclasificado a MW**: el fichero desconocido fue reclasificado como Malware
  - **Reclasificado a PUP**: el fichero desconocido fue reclasificado como PUP
- **Ha accedido a datos**: amenaza ha accedido a ficheros que residen en el equipo del usuario.

- **Se ha comunicado con equipos externos**: la amenaza se comunica con equipos remotos para enviar o recibir datos.
- **Modo de protección**: especifica el modo en el que se encontraba la protección en el momento del blqueo.
- **Excluido**: Se indica si el elemento fue excluido o no de la monitorización.
- **Probabilidad de que sea malicioso**: Media, Alta, Muy Alta
- **Fecha**.

17.5.3 Listado PUP

Para mostrar el listado de las amenazas encontradas en los equipos protegidos con **Adaptive Defense 360 haz** clic en los distintos elementos del panel **Programas potencialmente no deseados** .

Sobre el listado se aplicarán de forma automática diversos filtros en función de la zona del panel seleccionada.

En la parte superior se encuentra la herramienta de búsqueda equivalente a la de **Programas Maliciosos**:

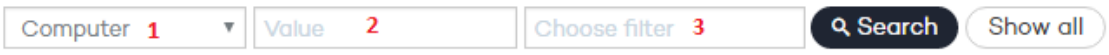


Figura 88: Herramienta de filtrado del listado PUP

El filtro **(1)** restringe la búsqueda indicada en la caja de texto **(2)** de escritura situado a la derecha al campo seleccionado:

- **Equipo**: la cadena de búsqueda se aplicará sobre el nombre del equipo
- **Nombre**: la cadena de búsqueda se aplicará sobre el nombre del PUP
- **Fecha**: la cadena de búsqueda se aplicará sobre la fecha de la detección
- **MD5**: Digest de identificación del archivo

El filtro **(3)** muestra los programas potencialmente no deseados que satisfagan los criterios seleccionados

- **No Ejecutado**: PUP detectado por la protección contra vulnerabilidades
- **Ejecutado**: el PUP se llegó a ejecutar y equipo está infectado
- **Acceso a ficheros de datos**: el PUP realizó accesos a disco para recoger información del equipo o para crear ficheros y los recursos necesarios para su ejecución
- **Comunicaciones**: el PUP abrió sockets de comunicación con cualquier máquina, incluido localhost
- **Bloqueado**: PUP conocido por **Adaptive Defense 360** y bloqueada su ejecución
- **Enviado a cuarentena**: el PUP no es desinfectable y se envió a cuarentena
- **Eliminado**
- **Desinfectado**: el PUP fue desinfectado por el antivirus
- **Permitido por el usuario**: PUP conocido por **Adaptive Defense 360** pero su ejecución fue

permitida por el usuario.

Los campos de la tabla son los siguientes:

- **Equipo**: dispositivo donde se realizó la detección
- **Nombre**: nombre del PUP
- **Ruta**: ruta completa donde reside el fichero infectado
- **Ejecutado alguna vez**: el PUP se llegó a ejecutar
- **Ha accedido a datos**: el PUP ha accedido a ficheros que residen en el equipo del usuario.
- **Se ha comunicado con equipos externos**: el PUP se comunica con equipos remotos para enviar o recibir datos.
- **Última acción**: acción aplicada sobre el PUP (bloquear, permitir, enviar a cuarentena, eliminar, desinfectar, permitir por el usuario
- **Fecha**: fecha de la detección del malware en el equipo

17.5.4 Listado detalle de detecciones

El listado de detecciones ofrece información consolidada y completa de todas las detecciones hechas en todas las plataformas y desde todos los vectores de infección soportados que los hackers han utilizado.

Para mostrar este listado haz clic en los paneles de **Amenazas detectadas** o en **Origen de las detecciones**, en la sección **Detecciones** del panel de control. La información se divide en tres listados:

- **Amenazas detectadas**
- **Equipos con más amenazas**
- **Malware más detectado.**

En la barra de herramientas situada en la parte superior es posible elegir el listado a mostrar, acotar el intervalo de tiempo mostrado y exportar los datos a un fichero. Haz clic en el botón **Exportar** para mostrar una ventana donde se pueden elegir los parámetros:

- Tipo de evento a exportar
- Formato del fichero exportado (Excel, csv)
- Intervalo de los datos exportados (últimas 24 horas, último mes, último año)

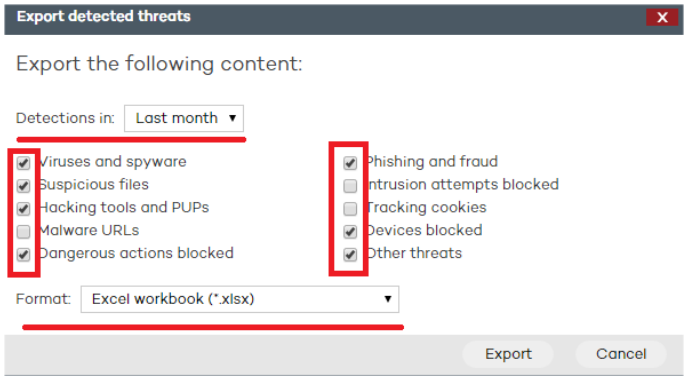


Figura 89: Configuración de la exportación del listado de detecciones

Listado de Amenazas detectadas

Muestra un listado de amenazas y eventos peligrosos vistos en la red, agrupados por su tipo.

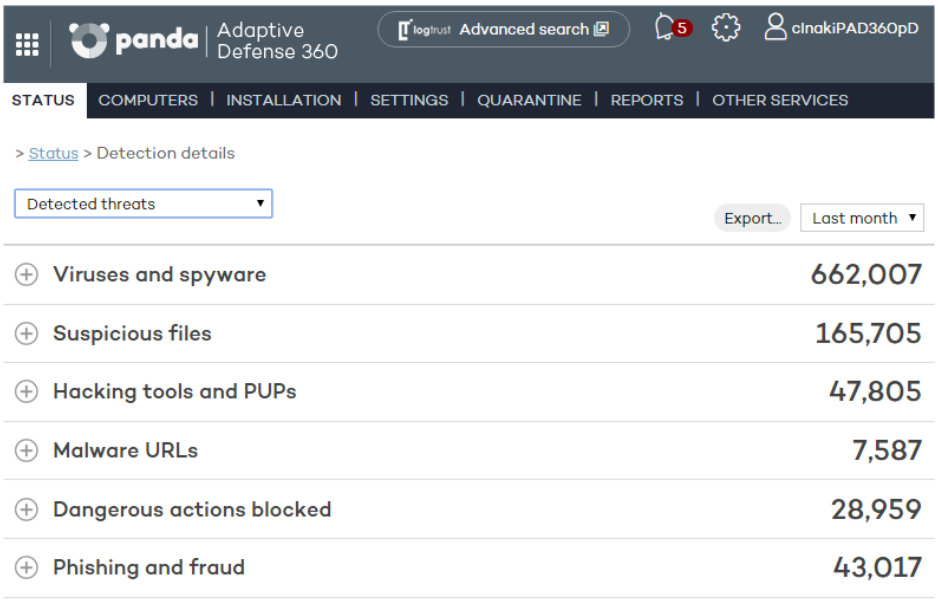


Figura 90: Tipos de amenazas y eventos detectados

Los grupos incluidos se muestran a continuación:

- **Virus y spyware**
- **Archivos sospechosos**: muestra los ficheros clasificados como sospechosos por el análisis heurístico de **Adaptive Defense 360**
- **Herramientas de hacking y PUPs**
- **URLs con malware**: URL que apuntan a páginas Web que contienen malware.
- **Acciones peligrosas bloqueadas**: muestra los ficheros clasificados como sospechosos debido a las técnicas de análisis de comportamiento
- **Phishing y fraude**
- **Intentos de intrusión bloqueados**: detecciones de tráfico malformado
- **Tracking cookies**: muestra las cookies utilizadas para espiar la navegación de los usuarios
- **Dispositivos bloqueados**: periféricos conectados al equipo del usuario que fueron bloqueados por el administrador.

- **Otras amenazas**: detección de malware con otras clasificaciones no cubiertas en los apartados anteriores (Jokes etc…)

Por cada grupo se incluye un contador con el número de ocurrencias encontradas para el intervalo de tiempo fijado y el tipo de malware elegido.

Pinchando en el icono  de un grupo concreto se desplegará su contenido, estructurado como se muestra a continuación.

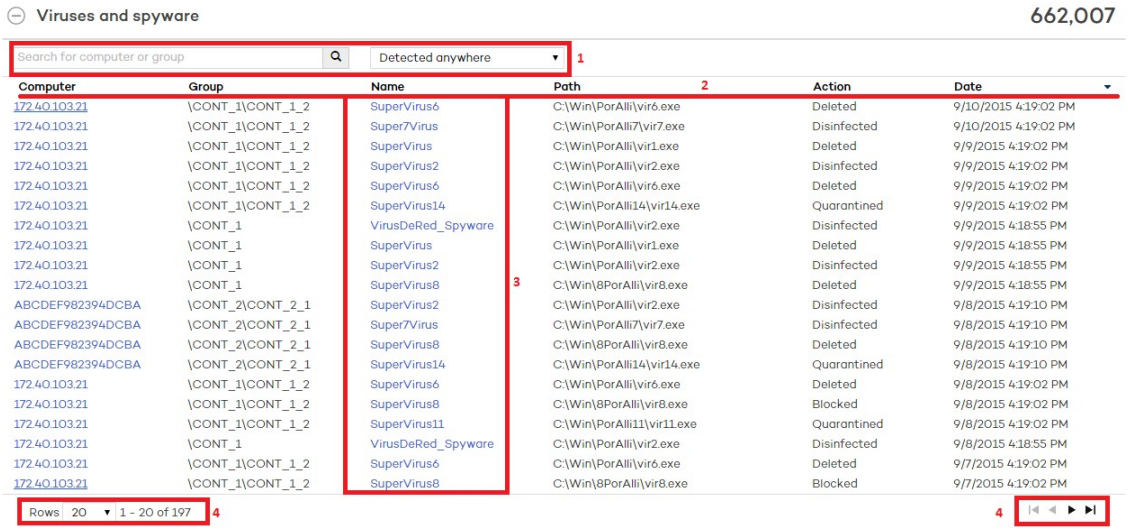


Figura 91:Estructura de un listado de amenazas detectadas

- **Herramientas para filtrar la información dentro del grupo (1)**

Dependiendo del grupo desplegado se mostrarán unos controles u otros:

- **Búsqueda de equipo o grupo**
- **Lugar de la detección**:
  - En cualquier sitio
  - En el sistema de archivos
  - En el servidor Exchange
  - En el correo
- **Tipo de dispositivo**:
  - Todos los dispositivos
  - Unidades de almacenamiento extraíbles
  - Dispositivos de captura de imágenes
  - Unidades de CD/DVD
  - Dispositivos Bluetooth
  - Módems
  - Dispositivos móviles

- **Número de filas a mostrar**
- **Herramientas de paginación**

- **Información de los elementos detectados (2)**

Dependiendo del grupo desplegado se mostrarán unas columnas u otras

- **Equipo**: nombre del equipo donde se realizó la detección.
- **Grupo**: grupo al que pertenece el equipo
- **Nombre**: nombre de la amenaza detectada
- **Ruta**: Ruta del sistema de ficheros donde reside la amenaza
- **Acción**: acción desencadenada por **Adaptive Defense 360**
  - **Borrado**: el malware no se pudo desinfectar y ha sido borrado
  - **Desinfectado**
  - **En cuarentena**
  - **Bloqueado**: la ejecución del malware se impidió mediante su bloqueo
  - **Proceso terminado**: el malware se estaba ejecutando y **Adaptive Defense 360** mató el proceso

- **Información de elementos específicos (3)**

Haz clic sobre algunos elementos para mostrar información extendida del elemento

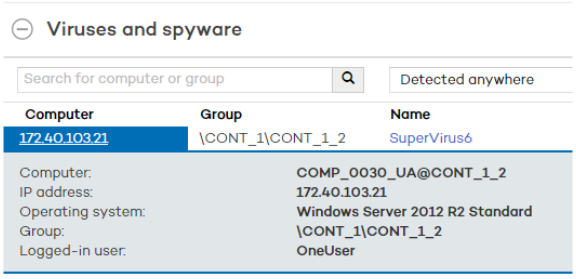


Figura 92: Información extendida de elementos

- **Herramientas de paginación (4)**

Permite especificar el número de filas que se mostrará en el grupo y moverse entre páginas.

Equipos con más amenazas

Este listado añade un nivel de agrupación con respecto al listado de **Amenazas detectadas** de forma que en primer lugar se muestran los equipos con más detecciones. Haz clic en cada equipo para mostrar un listado desglosado por tipo de detección, de la misma manera que en el listado **Amenazas detectadas**.

- **Información de los elementos detectados**

- **Equipo**
- **Grupo**
- **Detecciones**
- **Primera detección**: fecha de la primera detección encontrada en el intervalo fijado
- **Ultima detección**: fecha de la última detección encontrada en el intervalo fijado

Malware más detectado

Muestra un listado con las muestras del malware que más veces fueron vistos en la red del cliente.

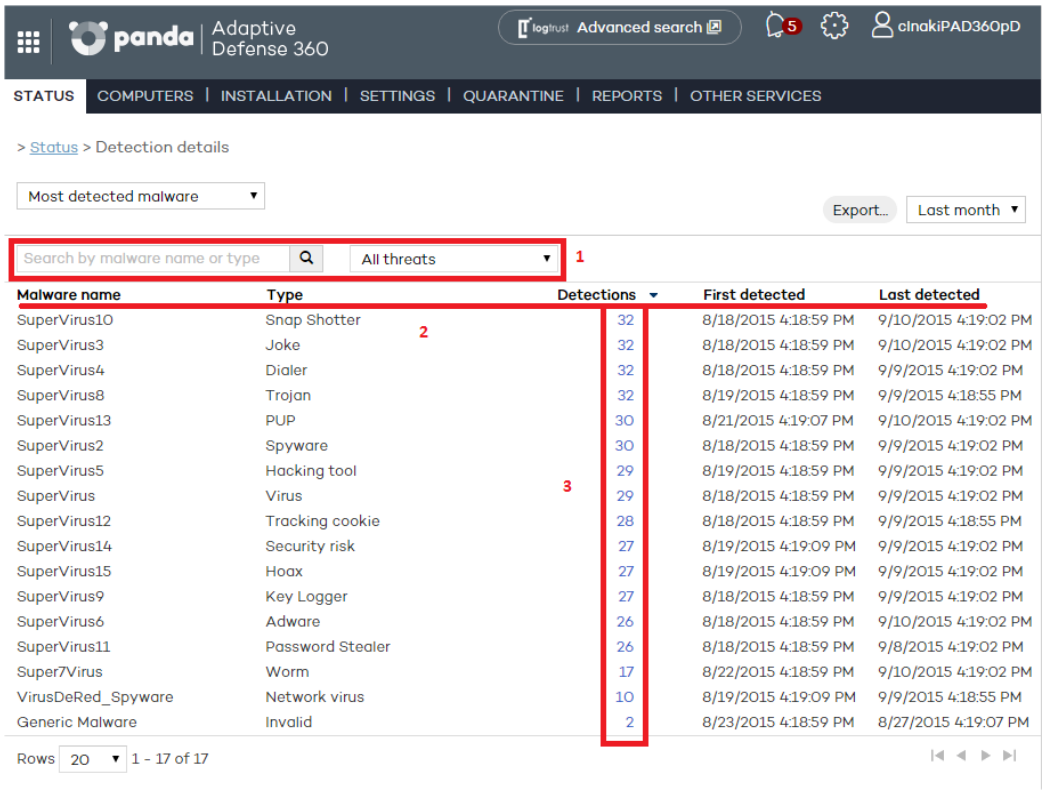


Figura 93: Listado con las amenazas más detectadas en el parque

- **Herramientas para filtrar la información del listado (1)**

- **Nombre de la amenaza o tipo**: permite realizar una búsqueda libre indicando el nombre de la amenaza o su tipo
- **Tipo de amenaza**: permite seleccionar el tipo de amenazas a mostrar
  - **Virus y Spayware**
  - **Herramientas de hacking y PUPs**
  - **Tracking cookies**
  - **Otras amenazas**

- **Información de los elementos detectados (2)**

- **Nombre del malware**

- **Tipo**
- **Detecciones**
- **Primera detección**
- **Ultima detección**

- **Información de elementos específicos (3)**

Haz clic sobre el número de detecciones de una amenaza concreta para mostrar el listado de **Amenazas detectadas**

Listado Accesos a páginas Web

Haz clic en el panel **Accesos a páginas Web**. El listado de accesos a páginas Web ofrece información consolidada y completa de las categorías de navegación Web de los usuarios.

Se divide en cuatro paneles:

- Categorías más accedidas (top 10)
- Equipos que más acceden (top 10)
- Categorías más bloqueadas (top 10)
- Equipos con más accesos bloqueados (top 10)

Cada panel cuenta con un link **Ver listado completo** que muestra una ventana con el listado de accesos íntegro para cada categoría.

17.6. Gestión de bloqueados y exclusiones

Adaptive Defense 360 bloquea por defecto todos los programas clasificados como malware y, adicionalmente, dependiendo de la configuración de la protección avanzada, también bloqueará los programas no vistos anteriormente hasta que sean analizados y emitida una clasificación sobre su seguridad.

En el caso de que un usuario no pueda esperar a que se emita una clasificación, o el administrador quiera permitir la ejecución de un elemento clasificado como malware, **Adaptive Defense 360** implementa recursos para evitar estos bloqueos de ejecución

De forma general se desaconseja el desbloqueo de elementos. Los elementos bloqueados por estar clasificados como peligrosos representan un riesgo cierto para la integridad de los sistemas de IT de la empresa y los datos almacenados en los mismos. Adaptive Defense 360 emite clasificaciones con un 99'999% de precisión. Para los elementos bloqueados por ser desconocidos existe una probabilidad alta de que terminen siendo clasificados como peligrosos. Por estas razones se recomienda evitar a toda costa el desbloqueo de elementos desconocidos o clasificados como malware / PUP

El acto por parte del administrador de la red de retirar el bloqueo impuesto por **Adaptive Defense 360** sobre la ejecución de un proceso del usuario recibe el nombre de Desbloquear un elemento si el elemento fue bloqueado por ser desconocido para **Adaptive Defense 360**, o Excluir un elemento (también Añadir una exclusión sobre un elemento) si el elemento fue bloqueado por haber sido clasificado como peligroso para el cliente (Malware o PUP).

- **Esquema general**

A continuación, se muestra un diagrama de estados donde se reflejan las diferentes situaciones por las que pasa un proceso analizado por **Adaptive Defense 360**, en función de la configuración de la protección avanzada, de la lista de exclusiones creada por el administrador y de los cambios de estado internos que se produzca a lo largo del tiempo. El diagrama se descompone en dos ramas presentadas por separado por razones de claridad: una rama para los ficheros conocidos y otra para los ficheros desconocidos.

17.6.1 Ficheros conocidos

*Figura 94: Diagrama de estados para ficheros conocidos por **Adaptive Defense 360***

En el caso de un fichero clasificado por **Adaptive Defense 360** como Malware y una política de protección avanzada distinta de Audit, los ficheros serán bloqueados a no ser que el administrador genere una exclusión que permita su ejecución.

17.6.2 Ficheros desconocidos

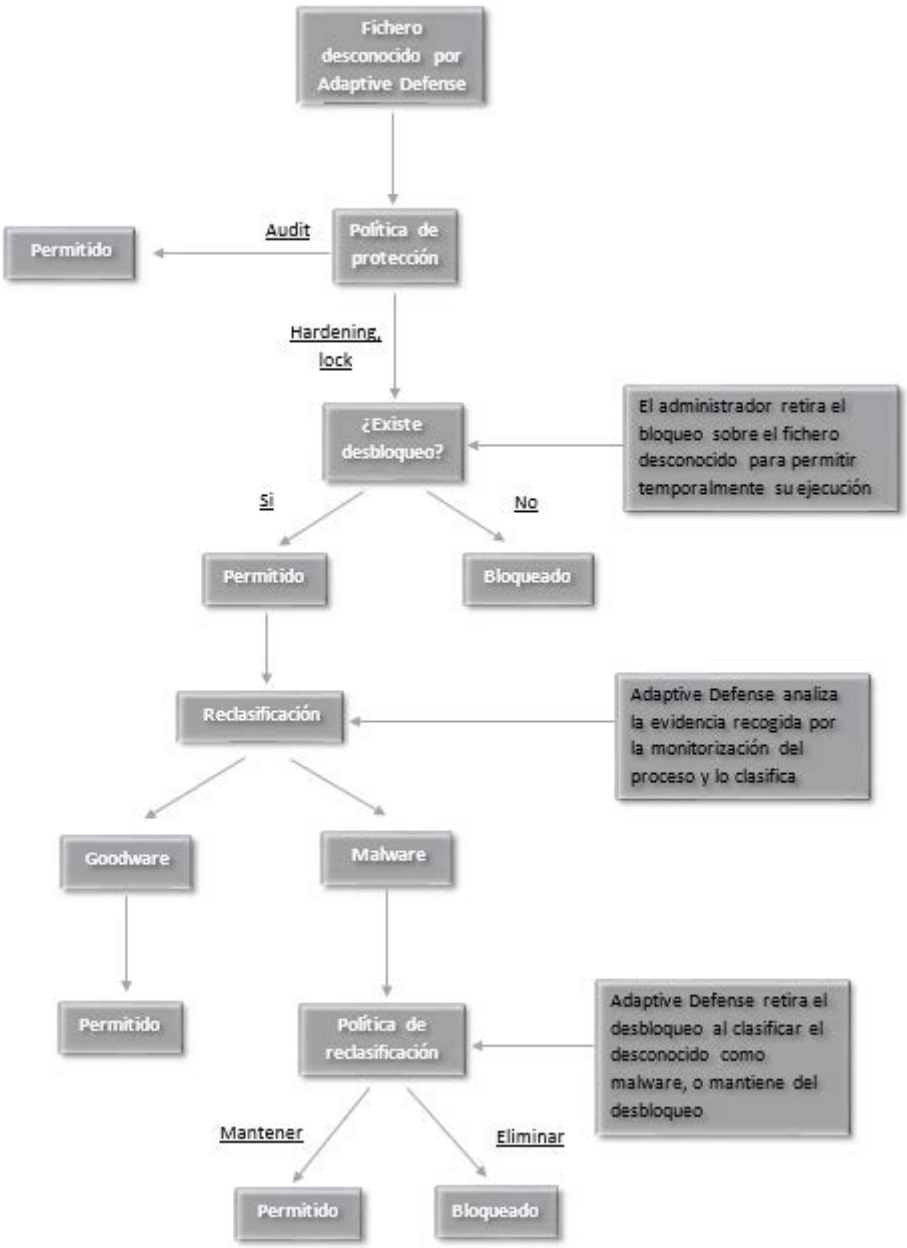


*Figura 95: Diagrama de estados para ficheros conocidos por **Adaptive Defense 360***

En el caso de los ficheros desconocidos (sin clasificar) y una política de protección avanzada distinta de Audit, los ficheros se bloquearán a no ser que el administrador de la red genere un desbloqueo. Independientemente del desbloqueo, **Adaptive Defense 360** clasificará el fichero y, dependiendo del resultado y de la política de reclasificación elegida, el fichero se bloqueará o se seguirá ejecutando.

17.6.3 Desbloquear elementos desconocidos pendientes de clasificación

Si los usuarios no pueden esperar a que el sistema haya completado la clasificación para liberar el bloqueo de forma automática, el administrador puede utilizar el botón **No volver a bloquear** en el listado de **Elementos actualmente bloqueados en clasificación**, accesible desde el panel de control **Actividad**.

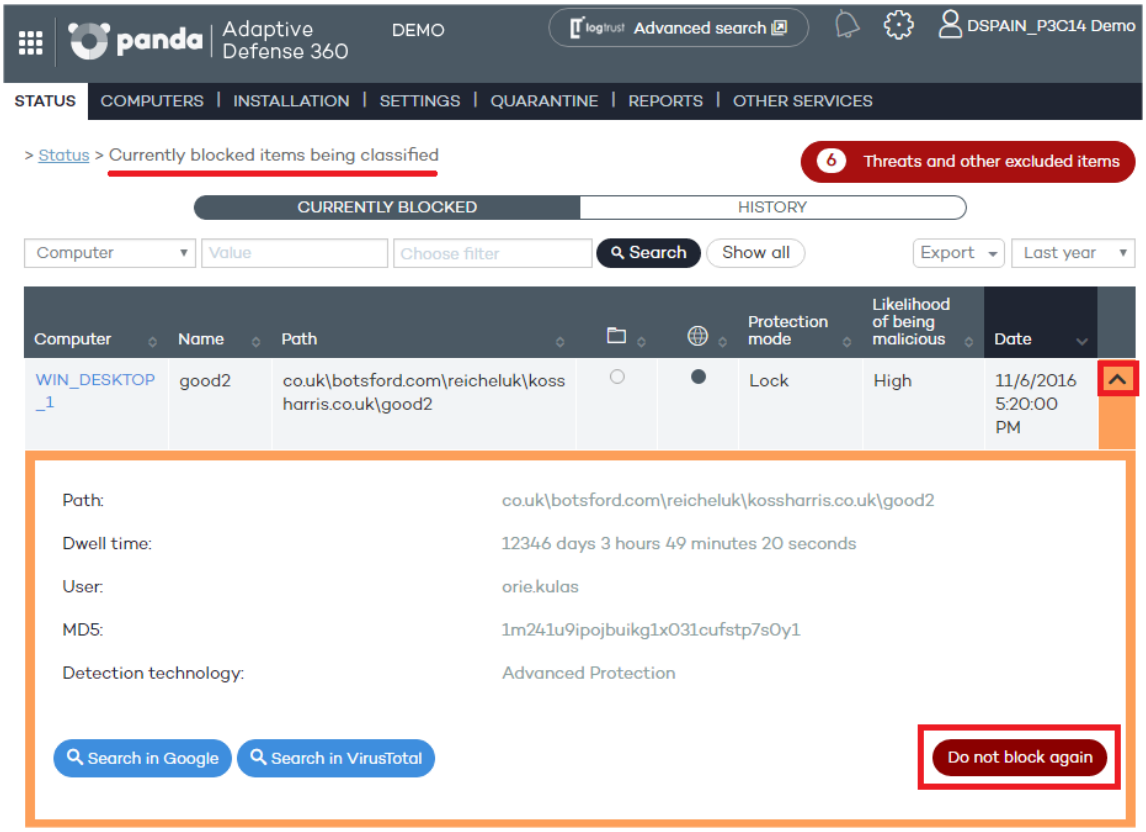


Figura 96: Botón de desbloquear elementos en clasificación

Una vez desbloqueado el elemento desaparecerá de la pestaña **Bloqueados actualmente** en el listado **Elementos actualmente bloqueados en clasificación** ya que el administrador asume el riesgo de su ejecución y por lo tanto el sistema no lo bloqueará. No obstante, **Adaptive Defense 360** continuará analizando el proceso hasta completar su clasificación. El elemento desbloqueado aparecerá en el listado de **Amenazas y otros elementos excluidos**.

17.6.4 Exclusiones de elementos clasificados como malware o PUP

Excluir un elemento clasificado como malware es la operación equivalente a desbloquear un elemento bloqueado sin clasificar, si bien en este caso se está permitiendo la ejecución de un programa que **Adaptive Defense 360** ya ha clasificado de forma efectiva como dañino o peligroso para el sistema.

Para excluir un elemento clasificado como malware o PUP haz clic en el botón **No volver a detectar** en los listados **Programas maliciosos** y **Programas potencialmente no deseados**, accesibles desde el panel de control **Actividad**.

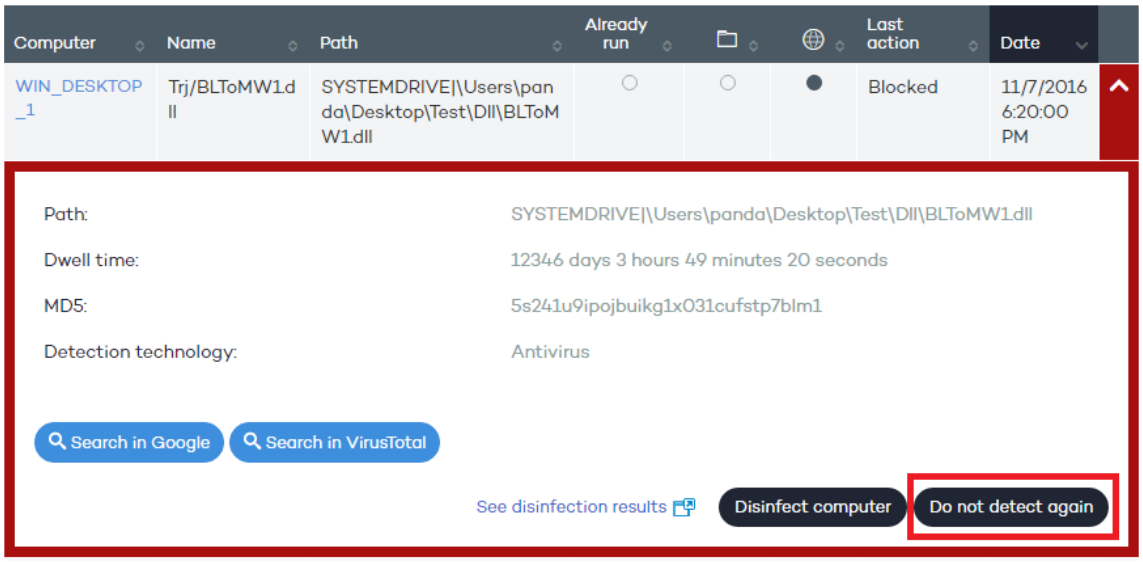


Figura 97: Botón no volver a detectar elementos clasificados como amenaza

Una vez excluido el elemento dejará de generar incidentes en los paneles de **Actividad** apropiados (Malware o PUP) y se añadirá al listado de **Amenazas y otros elementos excluidos**.

17.6.5 Acceso a la pantalla de gestión de los elementos excluidos

Para la gestión de los elementos excluidos y la gestión del comportamiento del sistema ante reclasificaciones de procesos conocidos o desconocidos haz clic en el botón **Amenazas y otros elementos excluidos** en la ventana **Estado,** o haz clic en un panel de la sección **Actividad** del dashboard, en la parte superior de los listados de malware/pup/bloqueados.

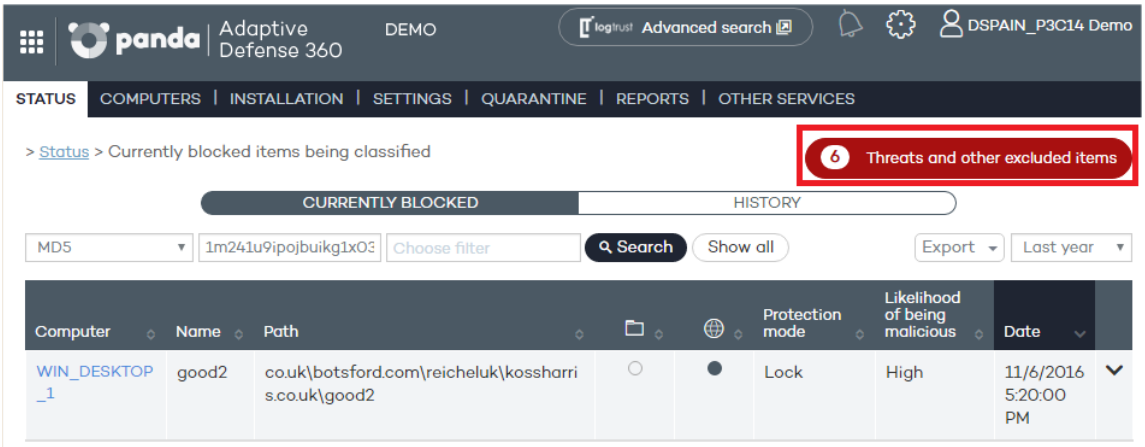


Figura 98: Acceso a los elementos excluidos del analisis por el administrador desde el listado de amenazas bloqueadas

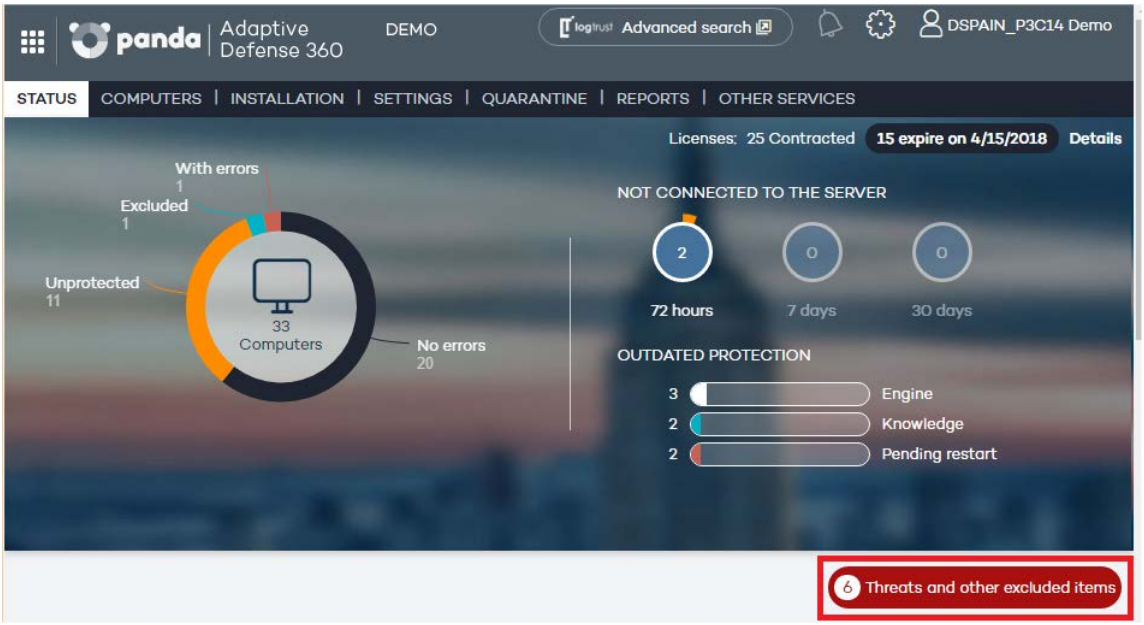


Figura 99: Acceso a los elementos excluidos del análisis por el administrador desde la ventana ***Estado***

La ventana **Amenazas y otros elementos excluidos** consta de un control de tipo selección que permite gestionar los ficheros actualmente permitidos o un histórico. Seleccionando una u otra opción la ventana cambiará para ajustar su contenido y opciones

17.6.6 Elementos permitidos actualmente

Muestra los elementos que tienen una exclusión activa. Todos los elementos que aparecen listados tienen permitida su ejecución.

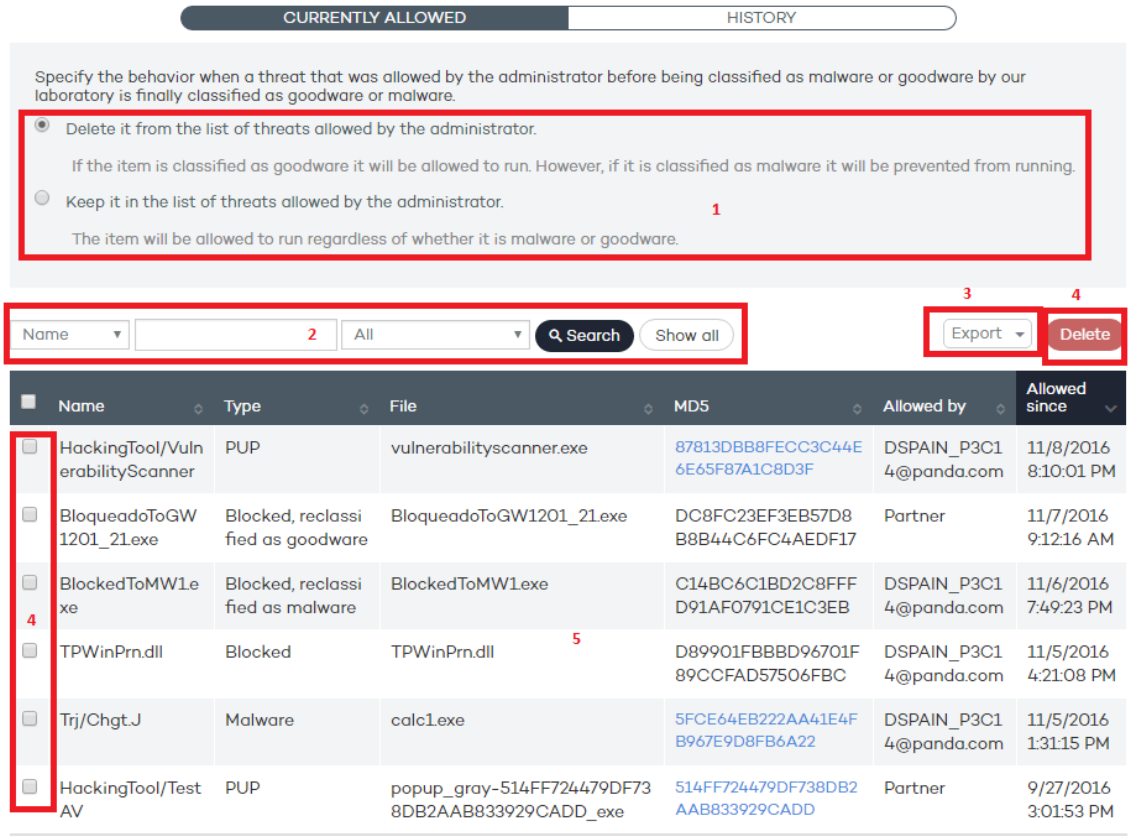


Figura 100: Estructura del listado ***Elementos permitidos actualmente***

La ventana **Permitidos** actualmente contiene las siguientes herramientas:

- Política de reclasificación (1)
- Filtrado de listados (2)
- Exportación de listados (3)
- Borrado de exclusiones (4)
- Listado de elementos excluidos actualmente (5)

Política de reclasificación (1)

La política de reclasificación permite determinar el comportamiento automático del sistema cuando un elemento desbloqueado por el administrador cambia su estado interno y es necesario tomar una nueva decisión de bloqueo / desbloqueo.

En los casos en los que el administrador desbloquea un elemento desconocido bloqueado, lo normal es que con el tiempo el elemento pase a ser conocido y clasificado como Malware o Goodware. Si el elemento anteriormente desconocido es clasificado como Goodware no requiere ningún tipo de acción ya que el sistema continuara permitiendo su ejecución. Por el contrario, si el elemento es clasificado como Malware, la política de reclasificación entra en juego, permitiendo al administrador definir el comportamiento de **Adaptive Defense 360**:

- **Eliminar de la lista de amenazas permitidas por el administrador**: si el fichero desconocido se ha clasificado como Goodware se seguirá ejecutando de forma normal, si es clasificado como Malware la exclusión se eliminará de forma automática y el fichero quedará bloqueado, a no ser que el administrador genere una nueva excepción manual para ese

fichero.

- **Mantener en la lista de amenazas permitidas por el administrador**: tanto si el fichero desconocido se ha clasificado como Goodware o Malware la exclusión se mantiene y el fichero seguirá ejecutándose.

En caso de seleccionar **Mantener en la lista de amenazas permitidas por el administrador**, se mostrará una ventana solicitando conformación ya que esta elección puede dar lugar a situaciones potencialmente peligrosas. Un escenario típico es el de un elemento desconocido originalmente, desbloqueado por el administrador para poder ser ejecutado mientras se clasifica y que, una vez analizado resulta ser peligroso. En este caso se continuaría su ejecución por no eliminarse la exclusión de forma automática debido a la política de reclasificación **Mantener en la lista de amenazas permitidas por el administrador** elegida.

Filtrado de listado (2)

El desplegable de la izquierda restringe la búsqueda indicada en la caja de texto al campo seleccionado:

- **Nombre**: nombre del malware o PUP
- **Archivo**: Nombre del fichero desconocido o que contiene la amenaza
- **MD5**: digest que identifica de forma única al fichero
- **Permitido por**: usuario de la consola que creó la exclusión.
- **Malware**: elemento clasificado como Malware
- **PUP**: elemento clasificado como PUP
- **Desconocido (Bloqueado)**: elemento sin clasificar hasta el momento
- **Bloqueado reclasificado a Malware / PUP**: elemento que fue bloqueado por ser desconocido y que posteriormente el sistema ha clasificado como peligroso.
- **Bloqueado reclasificado a Goodware**: elemento que fue bloqueado por ser desconocido y que posteriormente el sistema ha clasificado como seguro.

Una vez definido el filtro haz clic en el botón **Búsqueda** para aplicarlo, o en el botón **Mostrar todos** para mostrar todas las entradas y limpiar el filtro.

Exportación de listado (3)

Para exportar el listado haz clic en el botón **Exportar** y selecciona el formato del fichero exportado (xls o csv)

Borrado de entradas (4)

Para que **Adaptive Defense 360** recupere el comportamiento normal sobre un elemento previamente excluido o desbloqueado, selecciónalo en el listado y pulsar el botón **Eliminar**. Una vez eliminada la entrada el elemento se bloqueará o no dependiendo de su clasificación y del modo de protección avanzada seleccionado.

Listado (5)

- **Nombre**: nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar.
- **Tipo**: tipo del fichero bloqueado
  - **Malware**: elemento clasificado como Malware
  - **PUP**: elemento clasificado como PUP
  - **Bloqueado**: elemento sin clasificar hasta el momento
  - **Bloqueado reclasificado a Malware / PUP**: elemento que fue bloqueado por ser desconocido y que posteriormente el sistema ha clasificado como peligroso.
  - **Bloqueado reclasificado a Goodware**: elemento que fue bloqueado por ser desconocido y que posteriormente el sistema ha clasificado como seguro.
- **Archivo**: Nombre del fichero desconocido o que contiene la amenaza
- **MD5**: digest que identifica de forma única al fichero
- **Permitido por**: usuario de la consola que creó la exclusión
- **Permitida desde:** fecha en la que se permitió por primera vez la ejecución del elemento.

17.6.7 Historial

En esta ventana podrás visualizar el histórico de cambios realizado sobre los ficheros excluidos en **Adaptive Defense 360**. El listado permite ver el ciclo de estados completo de un fichero, desde que entra en el listado de excluidos o desbloqueados hasta que sale, pasando por los cambios de estado intermedios que el sistema o el administrador pueda haberle aplicado.

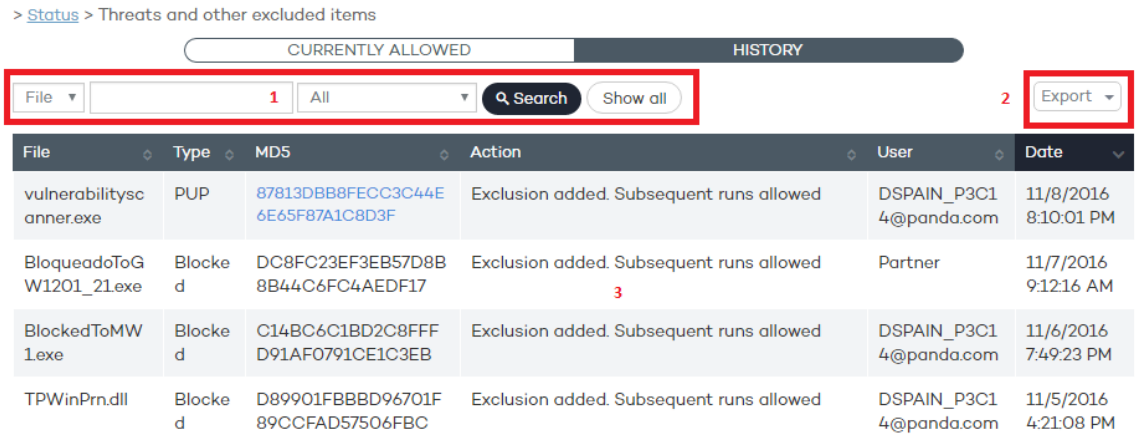


*Figura 101: Estructura del listado **Historial***

Filtrado de listado (1)

El desplegable de la izquierda restringe la búsqueda indicada en la caja de texto al campo seleccionado:

- **Archivo**: Nombre del fichero desconocido o que contiene la amenaza
- **MD5**: digest que identifica de forma única al fichero
- **Usuario**: login del usuario que inicio el cambio de estado

Exportación de listado (2)

Para exportar el listado haz clic en el botón **Exportar** y selecciona el formato del fichero exportado (xls o csv)

Listado (3)

- **Archivo**: Nombre del fichero desconocido o que contiene la amenaza
- **Tipo**: tipo del fichero bloqueado
  - **Malware**: elemento clasificado como Malware
  - **PUP**: elemento clasificado como Malware
  - **Bloqueado**: elemento sin clasificar
- **MD5**: digest que identifica de forma única al fichero
- **Acción**: indica el cambio de estado del fichero
  - **Añadida exclusión**. Permitidas ejecuciones posteriores: el administrador permite la ejecución del proceso y el fichero entra en el listado de elementos excluidos
  - **Eliminado de la lista de excluidos**: el administrador elimina la exclusión y el fichero sale del listado de elementos excluidos. El sistema recupera el comportamiento normal con respecto al fichero.
  - **Reclasificado a PUP / Malware**. Se elimina la exclusión: el fichero era desconocido cuando se excluyó y el sistema posteriormente lo ha clasificado como peligroso. El sistema ha retirado la exclusión de forma automática porque la política de exclusiones es **Eliminar de la lista de amenazas permitidas por el administrador** y por lo tanto se empieza a bloquear.
  - **Reclasificado a Goodware**. Se elimina la exclusión: el fichero era desconocido cuando se excluyó y el sistema lo ha clasificado como seguro. El sistema ha retirado la exclusión de forma automática porque la política de exclusiones es **Eliminar de la lista de amenazas permitidas por el administrador**. El fichero se sigue ejecutando.
  - **Excluido reclasificado a Goodware**. La exclusión se mantiene: el fichero era desconocido cuando se excluyó y el sistema lo ha clasificado como seguro. El sistema mantiene la exclusión de forma automática porque la política de exclusiones es **Mantener en la lista de amenazas permitidas por el administrador**. El fichero se sigue ejecutando y la exclusión deja de tener efecto.
  - **Excluido reclasificado a Malware / PUP**. La exclusión se mantiene: el fichero era desconocido cuando se excluyó y el sistema lo ha clasificado como peligroso. El sistema mantiene la exclusión de forma automática porque la política de exclusiones es **Mantener en la lista de amenazas permitidas por el administrador**. El fichero se sigue ejecutando.
  - **Configuración cambiada a "Borrar los programas reclasificados de la lista de amenazas permitidas"**: el administrador ha cambiado la política de exclusión
  - **Configuración cambiada a "Mantener los programas reclasificados de la lista de amenazas permitidas**: el administrador ha cambiado la política de exclusión."
- **Usuario**: cuenta de usuario que inició el cambio de estado o Automático si el cambio de estado fue una reclasificación interna del fichero
- **Fecha**: fecha del cambio

18. Visibilidad y monitorización de los equipos

Estado de los equipos en la red
Visibilidad de los equipos

18.1. Introducción

En este capítulo se describen los recursos implementados en **Adaptive Defense 360** que permiten controlar el estado de los equipos en la red

18.2. Estado de los equipos en la red

Un resumen rápido del estado de la protección se ofrece directamente desde el panel de control, en el menú **Estado**.

Figura 102: Panel de control de estado de los equipos

En esta sección del panel de control se muestran los equipos que requieren de la atención del administrador:

- Equipos que no han conectado con el servidor en las últimas 72 horas, 7 días y 30 días
- Equipos que tienen la protección sin actualizar: el motor, el archivo de identificadores y los que requieren un reinicio para aplicar la actualización del nuevo motor de protección descargado.

Haz clic en los distintos elementos del panel para mostrar la pestaña **Protegidos** de la ventana **Equipos,** con información más detallada.

18.3. Visibilidad de los equipos

La ventana **Equipos** muestra todos los elementos necesarios para facilitar la supervisión del parque informático y la búsqueda de los dispositivos:

- El árbol de grupos
- Pestañas de estado
- Herramientas de búsqueda
- Ventana de **Detalles de equipo** o dispositivo

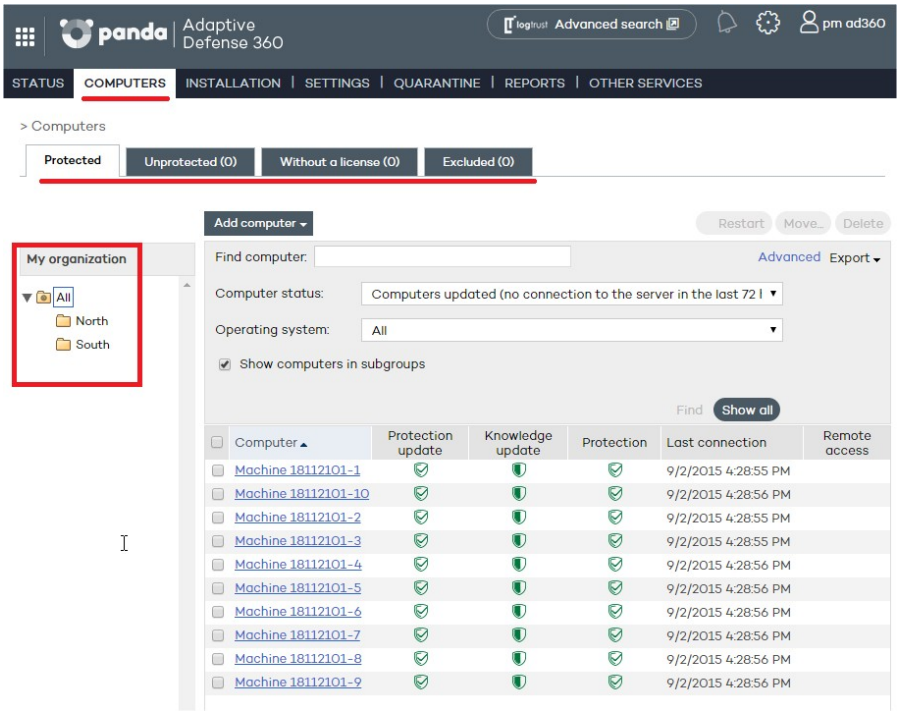


*Figura 103: Ventana de **Equipos***

Árbol de grupos

En la parte izquierda de la pantalla se encuentra el árbol de grupos, que permite desplazarse a través de los diferentes niveles y ver los equipos que contiene cada grupo. Para listar todos los equipos de la red haz clic en el nodo **Todos**.

Pestañas

Se ofrecen 4 agrupaciones en función del estado de la protección:

- Lista de equipos protegidos.
- Lista de equipos desprotegidos.
- Lista de equipos sin licencia.
- Lista de equipos excluidos.

Protegidos

Son equipos con el agente **Adaptive Defense 360** instalado de forma correcta y con una licencia válida asignada, aunque puedan estar desactualizados o con alguna protección en estado erróneo

Desprotegidos

Son equipos con el agente en proceso de instalación o desinstalación, equipos con la protección ya desinstalada y equipos descubiertos con la herramienta de descubrimiento

Sin licencia

Son equipos que tuvieron en el pasado una licencia válida asignada pero su mantenimiento ha

caducado de forma que ya no están protegidos. También son equipos que pertenecen a un grupo con restricciones de número máximo o por fecha y alguna de estas condiciones no se está cumpliendo para el equipo.

Excluidos

Son equipos que tienen un agente **Adaptive Defense 360** instalado pero que no compiten por obtener una licencia válida. El administrador puede excluir equipos de forma manual cuando el número de licencias válidas contratadas es inferior al número de equipos de la red a proteger.

18.3.1 Herramientas de búsqueda

Se puede filtrar el listado de equipos aplicando diversos criterios en función de la pestaña seleccionada.

Además, en algunas pestañas se incluye el botón **Avanzado**. Al pulsar se muestran / ocultan ciertos controles de búsqueda.

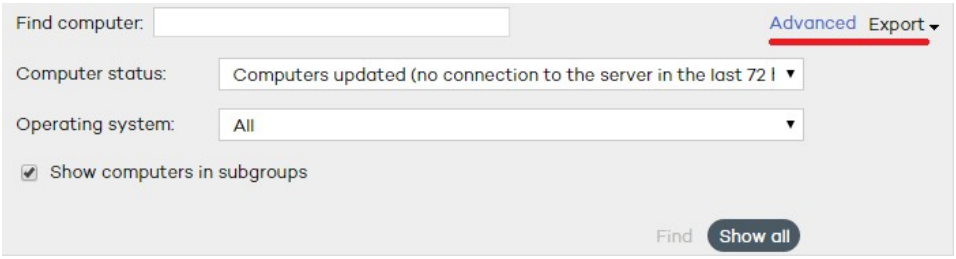


Figura 104: Herramientas de búsqueda de equipos

También se incluye un botón **Mostrar todos** que invalidad el criterio de búsqueda y lista todos los equipos dentro de la pestaña seleccionada.

A continuación, se muestra una relación de los controles y los criterios de búsqueda que permiten establecer por cada una de las pestañas.

Pestaña Protegidos

- **Buscar equipo**: permite realizar búsquedas libres por subcadenas sobre los campos que describen a los equipos: nombre y comentarios
- **Estado del equipo**:
  - **Todos**
  - **Equipos con protección activada**
  - **Equipos con todas las protecciones desactivadas**
  - **Equipos con protección actualizada**
  - **Equipos con protección desactualizada**
  - **Equipos con protección parcialmente activada**: equipos que tienen alguna de los módulos de protección desactivados
  - **Equipos con error en la protección**
  - **Equipos pendientes de reinicio**

- **Equipos con conocimiento actualizado**
- **Equipos con conocimiento desactualizado**
- **Equipos actualizados (sin conexión desde hace más de 72 horas)**
- **Equipos actualizados (sin conexión desde hace más de 7 días)**
- **Equipos actualizados (sin conexión desde hace más de 30 días)**

- **Sistema operativo**:
  - **Todos**
  - **Windows**
  - **Linux**
  - **Mac OS X**
  - **Android**
- **Mostrar equipos de los subgrupos**: busca en el grupo seleccionado en el árbol de grupos y en todos los grupos que cuelgan de él.

Pestaña Desprotegidos

- **Buscar equipo**: permite realizar búsquedas libres por subcadenas sobre los campos que describen a los equipos: **nombre** y **comentarios**
- **Estado del equipo**:
  - **Todos**
  - **Equipos sin protección**
  - **Equipos no administrados**: equipos en la red sin un agente instalado, encontrados mediante la herramienta de búsqueda
  - **Equipos instalando la protección**
  - **Equipos desinstalando la protección**
  - **Equipos con error en la protección**
  - **Equipos con error en la desinstalación**
  - **Equipos con nombre desconocido**
- **Sistema operativo:**
  - **Todos**
  - **Windows**
  - **Linux**
  - **Mac OS X**
  - **Android**
- **Mostrar equipos de los subgrupos**: busca en el grupo seleccionado en el árbol de grupos y en todos los grupos que cuelgan de él.

Pestaña Sin licencia

- **Buscar equipo**: permite realizar búsquedas libres por subcadenas sobre los campos que describen a los equipos: nombre y comentarios

Pestaña Excluidos

- **Buscar equipo**: permite realizar búsquedas libres por subcadenas sobre los campos que describen a los equipos: nombre y comentarios

18.3.2 Listados de equipos

Una vez establecidos los criterios de filtrado se mostrará el listado de equipos que los satisfacen.

La presentación del listado se realiza en una tabla con una serie de columnas que describen el estado del equipo y que varían en función de la pestaña elegida.

Los equipos con igual nombre y dirección IP se mostrarán como equipos diferenciados en la consola Web siempre y cuando tanto su dirección MAC como su identificador del agente de administración sean diferentes. Si deseas cambiar el modo en el que se nombran, puedes hacerlo seleccionando el icono situado en la cabecera de la consola Web. Consulta el capítulo 5 La consola de administración para más información

Pestaña Protegidos

- **Equipo**: muestra el listado de los equipos protegidos, denominándolos por su nombre o por su IP.
- **Actualización protección**: indica el estado de la protección. Al pasar el ratón por encima del icono se muestra el significado del icono y la versión de la protección instalada
  - Actualizado
  - No actualizado
  - Pendiente de reinicio
- **Actualización conocimiento**: indica el estado del fichero de identificadores. Al pasar el ratón por encima del icono se muestra el significado del icono y la fecha de actualización
  - Actualizado
  - No se conectó en las últimas 72 horas
  - No actualizado
- **Protecciones**: indica el grado de protección del equipo. Al pasar el ratón por encima del icono se muestran las protecciones activadas.
  - Todas las protecciones disponibles están activadas
  - Algunas de las protecciones disponibles están deshabilitadas
  - Sistemas con protecciones bajo demanda o programadas.
  - Alguna protección ha entrado en estado de error
- **Última conexión**: fecha en la que el equipo se conectó por última vez al servidor **Adaptive Defense 360**
- **Acceso remoto**: indica si el equipo es accesible mediante herramientas de control remoto.
  - El equipo es accesible mediante la herramienta Remote Control de Panda

Security. Consulta la guía para el administrador de Remote control para más información sobre esta herramienta.

-  El equipo tiene instalada alguna herramienta de acceso remoto de terceros fabricantes. Si solo es una, haciendo clic sobre el icono se mostrará un popup pidiendo las credenciales para acceder al equipo. Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrá elegir cuál de ellas desea utilizar para acceder al equipo. Consulta el capítulo 20 Herramientas de resolución para más información.

Pestaña Desprotegidos

- **Equipo**: muestra el listado de los equipos protegidos, denominándolos por su nombre o por su IP.
- **Estado**: muestra cuál es la situación de la protección. Para ello utiliza una serie de iconos
  -  Instalando
  -  Desinstalando
  -  Error en la desinstalación
  -  Error en la instalación
  -  Protección desinstalada con éxito.
- **Detalles:** se especifica el motivo por el cual el equipo se encuentra en determinado estado. Por ejemplo, si muestra el estado **Error instalando**, en **Detalle** se puede mostrar el código del error producido. Si, por el contrario, la columna **Estado** muestra **Sin protección**, **Detalle** mostrará la explicación **Protección desinstalada**
- **Ultima conexión**: muestra la fecha y hora en que tuvo lugar la última conexión con el equipo
- **Acceso remoto**: si esta columna muestra un icono, indica que el equipo tiene instalada alguna herramienta de acceso remoto. Si solo es una, haciendo clic sobre el icono podrá acceder a la herramienta y, una vez introducidas las credenciales correspondientes, acceder al equipo

Pestaña Sin licencia

- **Equipo**: muestra el listado de los equipos protegidos, denominándolos por su nombre o por su IP.
- **S.O.**: se muestra la versión del sistema operativo y nivel de Service pack en el caso de sistemas operativos Windows
- **Motivo**: muestra la razón por la cual el equipo no tiene licencia: no hay licencias validas suficientes o el equipo pertenece a un grupo con restricciones y estas no se cumplen.

Pestaña Excluidos

- **Equipo**: muestra el listado de los equipos protegidos, denominándolos por su nombre o por su IP. Si hay diferentes equipos con igual nombre y dirección IP, se mostrarán como equipos diferenciados en la consola Web siempre y cuando tanto su dirección MAC como su identificador del agente de administración sean diferentes. Si deseas cambiar el modo en el que se nombran, puedes hacerlo seleccionando el icono  situado en la cabecera de la consola Web. Consulta el capítulo 5 La consola de administración para más

información

- **Grupo**: Grupo al que pertenece el equipo excluido

18.3.3 Acciones sobre equipos seleccionados

Todas las tablas de listados cuentan con una primera columna de selección. Haciendo clic en la casilla de la cabecera seleccionará o deseleccionará todos los equipos de la lista

Además, a pie de tabla se encuentra la herramienta de paginación que permite el desplazamiento con mayor velocidad entre páginas.

Al seleccionar uno o más equipos de la tabla, y dependiendo de la pestaña elegida se podrán ejecutar unas acciones u otras.

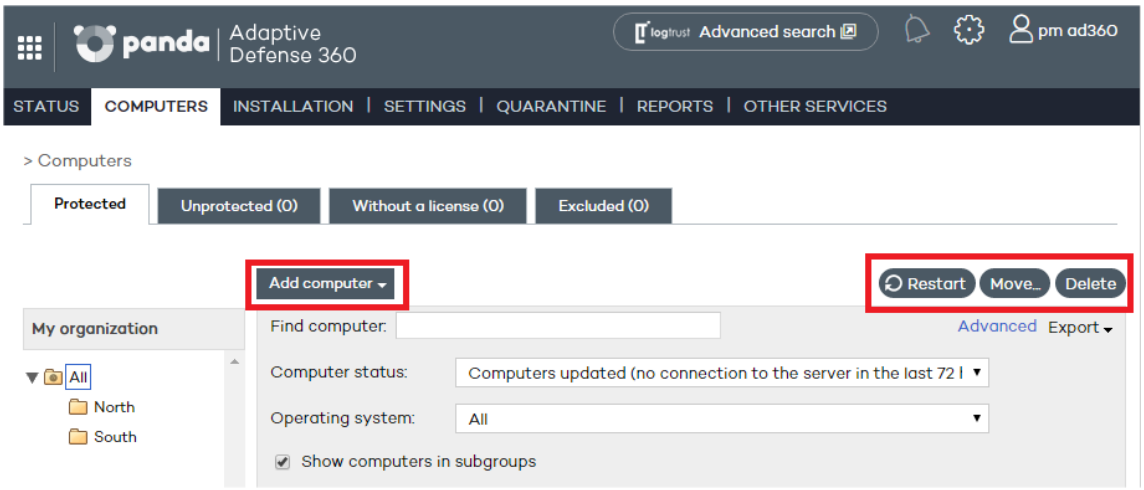


Figura 105: Botones para la gestión de equipos

Pestaña Protegidos

- **Añadir equipo**: muestra el asistente de instalación del agente **Adaptive Defense 360** para agregar nuevos equipos a la consola Web de administración.
- **Reiniciar**: reinicia los equipos seleccionados.
- **Mover**: permite cambiar de grupo a los equipos seleccionados.
- **Eliminar**: El equipo se elimina de la base de datos de **Adaptive Defense 360** aunque si no se ha desinstalado el agente del equipo volverá a aparecer en la consola en la siguiente conexión.
- **Acceso remoto**: indica que el equipo tiene instalada alguna herramienta de acceso remoto. Si solo es una, haz clic sobre el icono para acceder a la herramienta. Una vez introducidas las credenciales correspondientes, accederás al equipo. Si el equipo tiene instaladas varias herramientas de acceso remoto, sitúa el cursor sobre el icono para mostrar dichas herramientas y elegir cuál de ellas deseas utilizar para acceder al equipo.

Pestaña Desprotegidos

- **Eliminar los equipos seleccionados**: Los equipos seleccionados se eliminan de la base de datos de **Adaptive Defense 360**.
- **Eliminar todos los equipos**
- **Excluir los equipos seleccionados**

Pestaña Sin licencia

- **Eliminar los equipos seleccionados**
- **Eliminar todos los equipos**
- **Excluir los equipos seleccionados**

Pestaña Excluidos

- **Eliminar los equipos seleccionados**
- **Eliminar todos los equipos**

18.3.4 Detalle de equipos Windows, Linux y Mac OS X

Para acceder a los detalles de un equipo concreto haz clic en dicho equipo. A continuación, se mostrará la ventana **Detalles de equipo**, con información sobre el estado del equipo, independientemente de que esté protegido o no.

Detalles del equipo

- **Nombre**
- **Dirección IP**
- **Dominio**: solo se muestra en equipos Windows
- **Ruta Directorio Activo**: solo se muestra si el equipo pertenece a un Directorio Activo
- **Grupo**
- **Fecha de instalación**
- **Versión de la protección**
- **Versión del agente**
- **Actualización del conocimiento**: fecha del archivo de identificadores
- **Ultima conexión**
- **Sistema operativo**
- **Servidor de correo**
- **Campo comentarios**: Utiliza el campo **Comentario** si deseas añadir información adicional que pueda ayudar a identificar un equipo. Si el usuario que accede a la consola tiene permisos de monitorización no podrá modificar este campo.

Protecciones

Muestra el estado de los módulos de protección (activado, desactivado, no aplica)

- **Protección avanzada**. Indica el modo de la protección configurada: monitor, Hardening, Lock. Aplica a equipos Windows XP SP2 y superiores y a servidores Windows 2003 Server SP1 o superiores.
- **Protección de archivos.**
- **Protección de correo.**
- **Protección de navegación Web.**
- **Protección Firewall.**

- **Control de dispositivos.**
- **Protección antivirus para Exchange server.**
- **Protección antispam para Exchange server.**
- **Filtrado de contenidos para Exchange server.**
- **Control de acceso a páginas Web.**

Herramientas disponibles

Consulta el capítulo 20 Herramientas de resolución para más información.

- **Desinfectar el equipo**: **Adaptive Defense 360** desinfecta de forma automática el malware encontrado. Para equipos comprometidos por malware avanzado donde una desinfección estándar no sea posible se ofrece la herramienta de desinfección **Panda Cloud Cleaner**. Haz clic en el botón **Desinfectar equipo** para utilizarla.
- **Notificar problemas en el equipo**: notifica los problemas del equipo y los envía al personal cualificado de Panda Security.
- **Reiniciar equipos**: reinicia los equipos, incluyendo los que figuran en el listado de equipos protegidos como pendientes de reinicio
- **Eliminar de la base de datos**: elimina equipos, incluyendo los que no se han conectado con el servidor desde hace tiempo con la opción **Eliminar de la base de datos**. Los datos del equipo dejarán de ser utilizables y por tanto tampoco se podrá acceder al mismo.
- **Excluir**: Los equipos excluidos se mostrarán en la lista de equipos excluidos de la ventana **Equipos**. Al excluir equipos no se mostrará información ni alertas referentes a ellos en ningún otro lugar de la consola. Podrá deshacer la exclusión en cualquier momento

18.3.5 Detalles de dispositivos Android

En el caso de los dispositivos Android, en la ventana **Detalles de equipo** se muestran los datos del dispositivo y el estado de las protecciones antivirus y antirrobo, según la configuración que se haya realizado.

Si la protección antirrobo está activada en el dispositivo, se mostrará un mapa con la localización del dispositivo y las opciones correspondientes de la protección antirrobo: borrar, bloquear el dispositivo, realizar fotografía al ladrón y localizar el dispositivo.

Si alguna de las protecciones muestra un estado de error, haz clic en el vínculo **¿Cómo solucionar errores?** y accederás a instrucciones de soporte técnico que resultarán útiles para resolver el problema.

Detalles del equipo

Los detalles incluidos son los mismos que los mostrados en equipos Windows excepto:

- **Dirección IP**: no se muestra
- **Dominio**: no se muestra

- **Ruta directorio Activo**: no se muestra
- **ID dispositivo**: cadena de caracteres que identifica al dispositivo en **Adaptive Defense 360**

Protecciones

Muestra los módulos de protección activados

- Protección antivirus
- Protección antirrobo

Herramientas disponibles

- **Borrar dispositivo**: utiliza el botón **Borrar** para eliminar la información que se muestra del dispositivo y restaurar la configuración de fábrica.
- **Bloquear dispositivo**: Utiliza el botón **Bloquear dispositivo** para introducir la clave de cuatro dígitos necesaria para realizar el bloqueo.
- **Foto al ladrón**: al solicitar esta acción, cuando se detecte actividad en el dispositivo robado se sacará automáticamente una fotografía al autor de la sustracción. Introduce en la casilla de texto la dirección de correo electrónico a la que se enviará la fotografía.
- **Modo privado**: si el administrador ha concedido permiso al usuario del dispositivo para que lo utilice en modo privado, y el usuario lo ha activado mediante una contraseña, las opciones automáticas de localizar el dispositivo o de sacar foto al ladrón no funcionarán.
- **Lista de tareas**: El dispositivo Android mostrará el registro de tareas con información sobre las tareas que se han configurado desde la consola Web para que sean ejecutadas en el dispositivo.

Lista de tareas

Las tareas de alertas de robo, borrado y localización del dispositivo Android que se solicitan desde la consola Web para que se ejecuten en el dispositivo, se muestran en el registro de tareas de la ventana **Detalles de equipo**.

El registro muestra una tarea por estado. Por ejemplo, si existen tres tareas de alertas de robo, se mostrará una de ellas **Ejecutada**, otra como **Recibida** y otra como **Pendiente**. En la medida en que la primera tarea finalice y desaparezca del listado, la que se encuentra como Recibida pasará a **Ejecutada** y la que está como **Pendiente** pasará a **Recibida**.

El estado de las tareas es el siguiente:

- **Pendiente**: Las tareas se encontrarán en estado pendiente durante el intervalo de tiempo que va desde la configuración de la tarea en la consola Web hasta su recepción en el dispositivo. Hay que tener en cuenta que puede darse el caso de que el dispositivo se encuentre apagado o sin acceso a red, tiempo éste durante el que la tarea figurará como pendiente.
- **Recibida**: En este caso, el dispositivo ha recibido la solicitud de realización de una tarea, pero aún no la ha ejecutado o está en plena ejecución, y, por tanto, no ha finalizado. Por ejemplo, cuando se trata de una tarea de localización del dispositivo, la tarea se mostrará como recibida hasta que la localización sea efectiva. En el caso de la tarea de foto al ladrón, la tarea también se mostrará como recibida en tanto en cuanto no se ejecute el acto de sacar la fotografía. Esto es debido a que desde que se envía la solicitud de tarea

transcurre el tiempo que el ladrón tarda en activar el dispositivo, es decir, en tocar la pantalla.

- **Ejecutada**: La tarea se mostrará como ejecutada una vez que el dispositivo informe de la finalización de la misma (ya sea correctamente o con error).

19. Informes

Tipos de informes soportados
Generación y envío de informes

19.1. Introducción

Adaptive Defense 360 genera informes sobre el estado de la seguridad en la red informática y sobre las detecciones realizadas en un determinado periodo de tiempo. Además, puedes seleccionar el contenido que aparecerá en el informe, nivel de detalle, e incluir o no gráficos.

Cada usuario sólo podrá ver los equipos que pertenezcan a grupos sobre los que tenga permiso

19.2. Tipos de informes incluidos

Adaptive Defense 360 ofrece 5 tipos de informes:

- Ejecutivo
- De estado
- De detección
- Amenazas
- Auditoría de acceso a la consola
- Estado de equipos

19.2.1 Informe Ejecutivo

Descripción

Reúne en un mismo documento un resumen de los tres aspectos principales de la seguridad de la red:

- Estado de las protecciones instaladas en los equipos de la red
- Detecciones e intentos de infección en los equipos protegidos
- Estado del servicio contratado

Información incluida

- Resumen del estado de las protecciones instaladas y las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.
- Listas top 10 de equipos con malware detectado y ataques bloqueados, respectivamente.
- Listas top 10 de equipos con dispositivos bloqueados.
- Información sobre el estado de las licencias contratadas.
- Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).
- Spam detectado
- Listas top 10 de Categorías Web más accedidas.

- Listas top 10 de Equipos que más acceden.
- Listas top 10 de Equipos que han accedido a categorías prohibidas y a los cuales se les han bloqueado el acceso a URLs.

Formatos soportados

- Xml
- Csv
- Tiff
- Pdf
- Web
- Excel

19.2.2 Informe de estado

Descripción

Proporciona una visión general del estado de las protecciones y sus actualizaciones en el momento de solicitar el informe y detalla del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).

Formatos soportados

- Xml
- Csv
- Tiff
- Pdf
- Web
- Excel

19.2.3 Informe de detección

Descripción

Este informe ofrece la evolución de las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes y detalla el equipo, grupo, tipo de detección, número de veces (ocurrencia) de la detección, acción realizada y la fecha en que se produjo la detección.

Formatos soportados

- Xml
- Csv
- Tiff
- Pdf

- Web
- Excel

19.2.4 Informe de Amenazas

Descripción

Muestra los avisos producidos por la protección avanzada en tiempo real en el parque informático para las fechas definidas.

Información incluida

- Tabla con las máquinas de mayor riesgo, es decir, aquellos equipos que hayan tenido un mayor número de infecciones debidas a software malicioso.
- Información detallada de cada amenaza detectada:
  - Programas maliciosos
  - Programas potencialmente no deseados (PUPs)
  - Programas en investigación en los laboratorios de Panda Security

Para cada uno de los riesgos se muestra el total de detecciones, el número de dispositivos en los que se ha detectado, si se ha ejecutado, si ha conectada con el exterior y si ha accedido a datos.

Formatos soportados

- Xml
- Csv
- Tiff
- Pdf
- Web
- Excel

19.2.5 Informe de auditoría de accesos a la consola

Descripción

Muestra los accesos realizados a la consola por parte de los administradores del servicio de protección.

Información incluida

Una línea por cada acceso a la consola, indicando la información mostrada a continuación:

- **Usuario**: login utilizado para acceder a la consola
- **Permisos**: permisos de la cuenta del administrador utilizada para acceder a la consola
- **Conexión**: fecha y hora de la conexión
- **Desconexión**: fecha y hora de la conexión

Formatos soportados

- Xml
- Csv
- Tiff
- Pdf
- Web
- Excel

19.2.6 Informe de Estado de equipos

Descripción

Profundiza en el nivel de información sobre los equipos, que te permitirá conocer al detalle su estado

Información incluida

- Por cada equipo:
  - Identificador
  - Dirección IP
  - Grupo al que pertenece
  - Sistema operativo instalado
- Protección instalada
  - Fecha de instalación
  - Versión del agente
  - Versión de la protección.
- Actualizaciones
  - Estado de la última actualización del motor de la protección.
  - Estado de la última actualización del conocimiento.
- Estado de activación de las diferentes protecciones (protección avanzada, firewall, antivirus, control de dispositivos...)

Formatos soportados

- Csv
- Excel

19.3. Generación y envío de informes

En la ventana principal de la consola Web, haz clic en **Informes**. Se abrirá una ventana estructurada en tres secciones:

- Nombre y contenido del informe
- Alcance del informe

- Programar envío por correo

19.3.1 Nombre y contenido del informe

Selecciona el nombre del informe, su tipo de entre los cuatro tipos explicados en el punto anterior y el periodo que cubrirá el informe (últimas 24 horas, última semana o último mes) para el informe Ejecutivo y para el informe Amenazas.

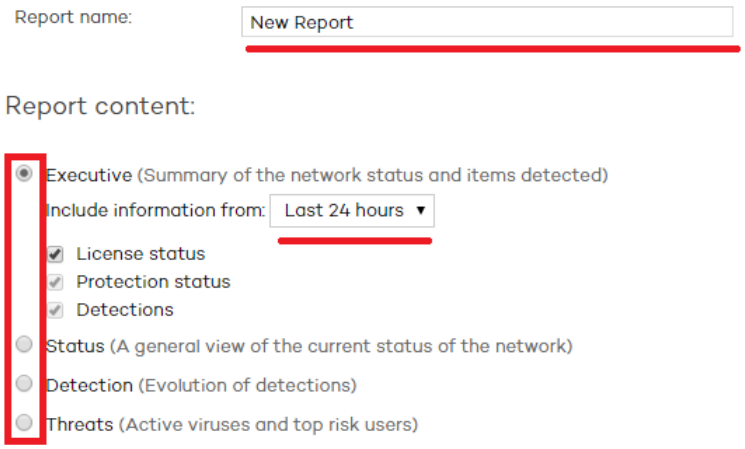


Figura 106: Configuración del nombre y tipo de informe

19.3.2 Alcance del informe

Define qué equipos de la red alimentarán con sus resultados el contenido del informe. La selección se realiza por grupos.

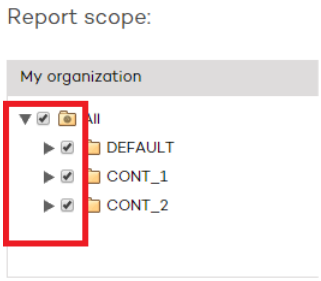


Figura 107: Selección de los grupos inlcuidos en el informe

19.3.3 Programar envío por correo

Si no necesitas programar el envío del informe haz clic en **Generar informe** dejando el campo **Periodicidad** en **No enviar**. El informe se generará al momento y aparecerá en la lista de informes de la parte izquierda de la pantalla.

El número de informes que podrás guardar es ilimitado. Para acceder de nuevo a un informe haz clic en el nombre del mismo en la lista que aparecerá en la parte izquierda de la ventana **Informes**.

Puedes programar el envío por correo del informe a los usuarios que el administrador de la red decida. Para ello es necesario definir los siguientes campos

- **Periodicidad**: frecuencia de envío. En función de la selección se podrá elegir día de la semana, la hora o el día del mes en que se producirá el envío:

  - Mensual
  - Semanal
  - Diaria
  - Primer día del mes.
- **Formato**: formato del informe a enviar
  - XML
  - CSV
  - IFF
  - PDF
  - Web
  - Excel
- **Para**: dirección de correo del destinatario del informe
- **Cc**: envió con copia
- **Asunto**: asunto del mensaje

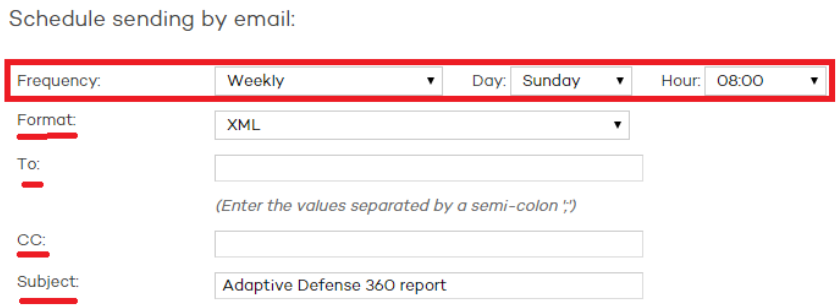


Figura 108: Programación del envío de informes

Puedes programar hasta 27 tareas de envío de informes. Una vez alcanzado dicho valor necesitarás eliminar alguna de ellas para crear más.

20. Herramientas de resolución

Desinfección automática de ficheros
Análisis y desinfección bajo demanda de ficheros
Desinfección avanzada de equipos
Reiniciar equipos
Acceso remoto al escritorio
Protección contra robo

20.1. Introducción

Adaptive Defense 360 cuenta con varias herramientas de resolución que permiten al administrador resolver los problemas encontrados en las fases de Protección, Detección y Monitorización del ciclo de protección adaptativa, presentado en el capítulo La protección adaptativa.

Algunas de estas herramientas son automáticas y no necesitan de la intervención del administrador, otras sin embargo requieren la ejecución de acciones concretas mediante la consola Web.

Todas las herramientas de resolución de **Adaptive Defense 360** se pueden utilizar desde la consola Web sin necesidad de desplazarse al equipo del usuario afectado, ahorrando costes en desplazamientos y tiempo del equipo técnico.

A continuación, se muestra una tabla de las herramientas disponibles por plataforma y su tipo (automático o manual).

Herramienta de resolución	Plataforma	Tipo	Objetivo
Desinfección automática de ficheros	Windows, Mac OS X, Android	Automático	Desinfectar o mover a cuarentena el malware encontrado en el momento de la infección de los equipos.
Bloqueo de exploits	Windows	Automático / Manual	Bloquea el intento de explotación de vulnerabilidades y la ejecución de código malicioso en procesos comprometidos
Análisis / Desinfección bajo demanda de ficheros	Windows, Mac OS X, Linux, Android	Automático (programado) / Manual	Analizar, desinfectar o mover a cuarentena el malware encontrado en los equipos protegidos en el momento que lo requiera el administrador o en franjas horarias concretas
Desinfección de equipos	Windows	Manual	Desinfección de los equipos afectados tanto por malware convencional como por el avanzado especialmente diseñado para dificultar su retirada
Reinicio bajo demanda	Windows	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección
Acceso remoto al escritorio	Windows	Manual	Herramientas de control remoto para acceder al escritorio de los equipos infectados
Protección contra robo	Android	Manual	Herramientas que ayudan a localizar dispositivos robados y determinar la identidad del ladrón

Tabla 7: Herramientas de resolución disponibles según la plataforma

Adicionalmente, Adaptive Defense 360 dispone del módulo Remote Control, que permite el acceso remoto a los dispositivos de los usuarios mediante herramientas de resolución avanzadas, sin necesidad de instalar productos de terceros.

20.2. Desinfección automática de ficheros

La desinfección automática es realizada por la Protección avanzada en tiempo real y por la Protección antivirus.

Ante una detección de malware **Adaptive Defense 360** desinfectará de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto el elemento se moverá a cuarentena.

La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Activar protección permanente de archivos** en **Antivirus**.

Consulta el capítulo 13 Perfiles de protección Windows para más información sobre los modos de bloqueo en Adaptive Defense 360 y configuraciones disponibles en el módulo antivirus.

Modo de protección avanzada	Protección antivirus	Comportamiento
Audit	Activado	Detección, Desinfección, Cuarentena
Hardening, Lock	Activado	Detección, Bloqueo de desconocidos, Desinfección, Cuarentena
Audit	Desactivado	Detección
Hardening, Lock	Desactivado	Detección, Bloqueo de desconocidos

Tabla 8: Comportamiento de Adaptive Defense 360 en función de la configuración de la protección avanzada y proteccion antivirus

20.3. Bloqueo de exploits

El bloqueo de exploits es realizado por la Protección avanzada.

Dependiendo de la configuración asignada al equipo y del tipo de exploit detectado, la resolución del problema (bloqueo del exploit) se llevará a cabo de forma automática o de forma manual.

Modo de protección avanzada	¿Requiere reinicio?	Comportamiento	Riesgo
Detectar, Bloquear	NO	Automático	NO
Detectar, Bloquear, pedir permiso	SI	Manual	SI
Detectar, Bloquear, no pedir permiso	SI	Automático	SI

Tabla 9: Comportamiento de Adaptive Defense 360 en función de la configuración de la protección avanzada y del tipo de exploit detectado

En los casos en los que no se pueda bloquear el exploit antes de su ejecución (Riesgo SI) será necesario comprobar las acciones ejecutadas por el programa comprometido. Consulta el capítulo 22 Análisis forense para obtener más información acerca del ciclo de vida de las amenazas detectadas por **Adaptive Defense 360.**

20.4. Análisis / Desinfección bajo demanda de ficheros

La desinfección bajo demanda de ficheros se realiza mediante la creación de tareas de análisis programadas o análisis puntuales bajo demanda.

20.5. Desinfección avanzada de equipos

En los equipos afectados por malware/PUP avanzado la desinfección automática puede llegar a fallar ya que este tipo de amenaza es mucho más difícil de resolver. Para identificar estos equipos consulta si se aprecian nuevas incidencias de forma constante y diaria en la sección de **Actividad** del panel de control. Solo en estos casos se requerirá una desinfección avanzada.

Una vez localizados los equipos infectados lanza de forma remota y desde la misma incidencia la herramienta de desinfección avanzada **Cloud Cleaner**. Para ello haz clic en los paneles de la sección **Actividad,** despliega la incidencia desde el panel de control en la ventana **Estado**, y haz clic en **Desinfectar Equipo**. También es posible desinfectar un equipo desde la en la ventana **Equipos**, pestaña **Protegidos** y haz clic en el equipo a desinfectar**,** accediendo a la ficha **Detalle** del equipo.

Cloud Cleaner es una herramienta especializada el desinfectar el malware avanzado. Para acceder a esta herramienta haz clic en cada equipo infectado de forma individual y elegir **Desinfectar Equipo**.

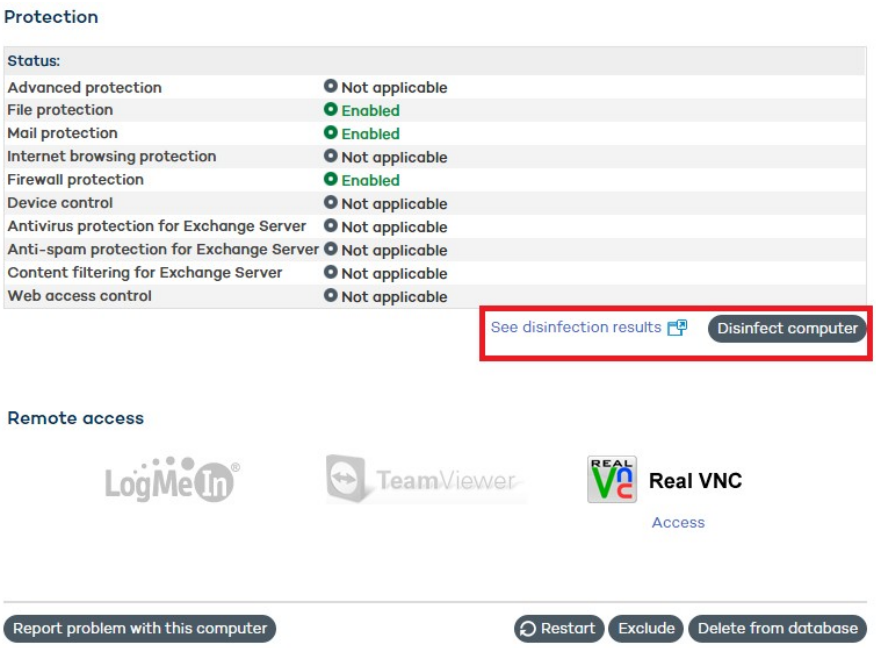


*Tabla 10: Acceso a la herramienta de desinfeccion avanzada **Cloud Cleaner***

Acto seguido se muestra una ventana de configuración rápida de la desinfección. Las opciones del menú de desinfección son las siguientes:

- **Eliminar Virus**: este check box siempre está habilitado y limpiar los virus encontrados en el equipo
- **Eliminar PUPs**: borra los programas potencialmente no deseados.
- **Limpiar cache del navegador**: limpia la cache del navegador instalado en el equipo (Internet Explorer, Firefox y Chrome)
- **Limpiar historial de navegación**: limpia el histórico de páginas Web del navegador
- **Eliminar cookies del navegador**: borra las cookies del navegador
- **Restaurar políticas del sistema que habitualmente son modificadas por el malware**: restaura el acceso al administrador de tareas, muestra archivos ocultos, muestra las extensiones de los archivos y en general restituye las políticas del sistema que el malware pueda haber cambiado impidiendo su restablecimiento a la configuración original elegida por el cliente
- **¿Quiere que se muestre la consola de desinfección en el equipo?**: muestra la consola de **Cloud Cleaner** con los resultados de la desinfección

Una vez configurada se creará una tarea de desinfección. Ejecutada la tarea se muestran los resultados haciendo clic en el link **Ver resultados de desinfecciones**.

Para más información sobre Cleaner Monitor consulta la ayuda Web del producto o en el enlace ***http://pcopdocuments.azureWebsites.net/Help/pccm/es-ES/index.htm***

En caso de encontrar dificultades al desinfectar un PC se recomienda descargar y ejecutar de forma manual la versión más actualizada de Panda Cloud Cleaner de ***http://pandacloudcleaner.pandasecurity.com***

20.6. Reiniciar equipos

Para actualizar los equipos a la última versión, o para corregir errores en la protección, reinicia los equipos de forma remota los dispositivos que figuren en el listado de equipos protegidos.

Para ello, en la ventana **Equipos** > **Protegidos** marca la casilla correspondiente al equipo o equipos que deseas reiniciar y haz clic en el botón **Reiniciar**.

Haz clic en el nombre del equipo para mostrar la ventana **Detalles** de equipo. Desde aquí también se puede ordenar el reinicio del equipo utilizando para ello el botón **Reiniciar**.

20.7. Acceso remoto al escritorio

Adaptive Defense 360 implementa dos formas de acceso al equipo remoto:

- Acceso mediante el módulo Remote Control de Panda Security
- Acceso mediante herramientas de acceso remoto de terceros fabricantes instaladas en el equipo.

En esta sección únicamente se tratan las herramientas de terceros fabricantes. Para obtener más información acerca del módulo Remote Control consulta la guía para el administrador de Remote control.

20.7.1 Visualizar equipos con acceso remoto

La funcionalidad de acceso remoto a los equipos resulta muy útil para acceder a los equipos de la red desde la consola de administración sin necesidad de trasladarse físicamente al lugar donde se encuentra el dispositivo.

Adaptive Defense 360 permite acceder a los equipos utilizando alguna de las herramientas de acceso remoto y versiones siguientes:

- TeamViewer: desde la 3.x a la 8.x
- RealVNC: 4.6.0, 4.5.4, 4.4.4, 4.3.2, 4.2.9 y VNC free 4.1.3
- UltraVNC: 1.0.9.5, 1.0.8.2, 1.0.6.5, 1.0.5.6 y 1.0.1.2
- TightVNC: 2.0.2, 2.0.1 y 2.0.0
- LogmeIn

En la ventana **Equipos** se mostrarán mediante un icono los equipos que tienen instalada alguna de estas herramientas de acceso remoto. Si solo es una, haz clic sobre el icono para acceder a la herramienta y, una vez introducidas las credenciales correspondientes, accede al equipo.

Se pueden introducir las credenciales desde la propia ventana **Equipos** o desde el menú

Preferencias haciendo clic en el icono  situado en la parte superior de la consola.

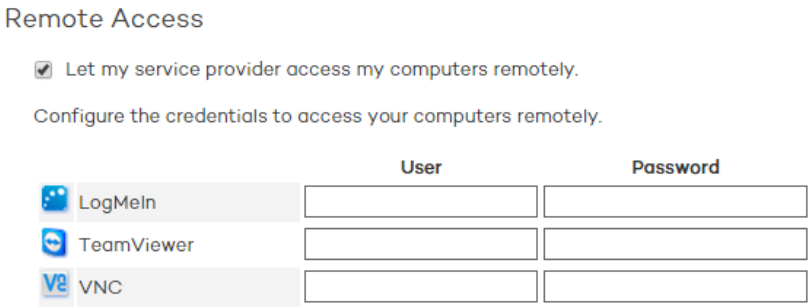


Figura 109: Ventana de confguracion de credenciales para las distintas herramientas de acceso remoto soportadas

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrás elegir cuál de ellas deseas utilizar para acceder al equipo.

Figura 110: Ventana de selección de la herramienta de acceso remoto

En el caso de que el equipo tenga más de una herramienta VNC instalada, solo se podrá acceder a través de una de ellas, siendo la prioridad de acceso la siguiente: 1-RealVNC, 2- UltraVNC, 3-TightVNC.

Dependiendo de si el usuario de la consola utilizado para acceder posee permiso de control total o de administrador, podrá utilizar el acceso remoto para acceder a más o menos equipos.

Si el permiso del usuario es de monitorización, no podrá acceder a ninguno y el icono de la columna Acceso remoto aparecerá deshabilitado

20.7.2 Cómo obtener acceso remoto

Acceso desde la ventana Equipos

La primera vez que se accede a la ventana **Equipos** se mostrará un aviso indicando que los equipos no disponen de acceso remoto instalado. Si deseas instalarlo utiliza el vínculo que se mostrará en el aviso.

Acceso desde la ventana Detalles de equipo

Desde la ventana **Detalles de equipo** también se podrá utilizar el acceso remoto, siempre y cuando

el equipo seleccionado tenga alguna de las herramientas de acceso remoto instalada. Si es así, Haz clic en el icono de la herramienta de acceso remoto a utilizar.

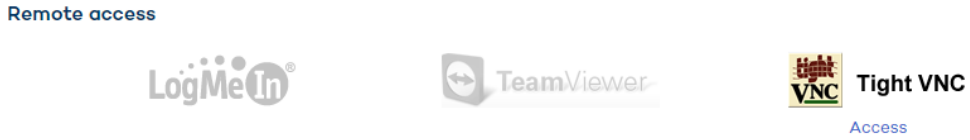


Figura 111: Iconos de la ventana Detalles de equipo indicando la instalación de la herramienta de acceso remoto Tight VNC en el equipo del usuario

Para poder tener acceso remoto, deberás instalar en las máquinas una de las soluciones de control remoto soportadas: TightVNC, UltraVNC, RealVNC, TeamViewer, LogMeIn.

En el caso de las herramientas VNC se seguirá la misma prioridad comentada anteriormente para el caso de que el equipo tenga instaladas más de una de estas herramientas.

20.7.3 Comportamiento de las herramientas de acceso remoto

Herramientas VNC

Estas herramientas sólo se podrán utilizar para acceder a equipos que estén en la misma red local que la del cliente.

Dependiendo de la configuración de autenticación de las herramientas, es posible que se pueda acceder a ellas sin necesidad de incluir credenciales de acceso remoto en la consola, o, por el contrario, tenga que configurar únicamente el password de acceso remoto o tanto el usuario como la password para poder conectar remotamente.

Para que al administrador pueda acceder a sus equipos a través de estas herramientas, debe permitir la ejecución del applet de Java en su propio equipo, en caso contrario, el acceso a los equipos, no funcionará correctamente.

TeamViewer

Esta herramienta se podrá utilizar para acceder a equipos que se encuentren fuera de la red local del cliente.

Para acceder a los equipos a través de TeamViewer solo será obligatorio introducir la password de los equipos, el campo “usuario” puede dejarse en blanco.

La password que hay que incluir para acceder a un equipo a través de TeamViewer, es la password de TeamViewer del equipo o la password configurada para el acceso no presencial, y no la password de la cuenta de cliente de TeamViewer.

Es recomendable disponer de la misma password de TeamViewer en todos los equipos, ya que cada usuario de la consola de **Adaptive Defense 360** sólo puede incluir una password para el acceso remoto a sus equipos a través de TeamViewer.

El equipo del administrador (equipos a través del cual se accede a la consola), deberá disponer de TeamViewer instalado (no es suficiente disponer de TeamViewer en modo ejecutor en dicho equipo).

LogMeIn

Esta herramienta se podrá utilizar para acceder a equipos que se encuentren fuera de la red local del cliente.

Para acceder a los equipos a través de LogMein, será necesario incluir el usuario y la password de la cuenta de LogMein.

20.8. Protección contra robo

La protección antirrobo de **Adaptive Defense 360** permite controlar en todo momento los dispositivos Android y determinar cuál será su comportamiento en el caso de robo.

Al configurar esta protección desde la consola Web podrás localizar los dispositivos, borrarlos, bloquearlos, sacar una fotografía al ladrón y enviarla por correo electrónico a una dirección concreta.

20.8.1 Activar la protección antirrobo

En la ventana principal de la consola haz clic en el menú **Configuración** y en el nombre del perfil para el que se desea configurar la protección antirrobo.

En la columna de la izquierda, haz clic en la opción **Antirrobo** que se muestra bajo Android.

Si deseas que **Adaptive Defense 360** te informe sobre la localización del dispositivo automáticamente, marca la casilla correspondiente.

Si deseas recibir un correo electrónico cuando se detecte actividad en un dispositivo robado, marca la casilla correspondiente. A continuación, introduce la dirección o direcciones de correo electrónico a las que se enviará la fotografía. Separe las direcciones utilizando punto y coma (;).

Si además de la opción de envío de foto del ladrón, has seleccionado previamente la de localización del dispositivo, junto con la foto del ladrón recibirás el mapa detallando la localización del dispositivo.

Una vez realizada esta configuración, desde la ventana **Detalles de equipo** podrás ver en todo momento dónde se encuentra el dispositivo, bloquearlo mediante una clave y modificar la dirección de correo electrónico para recibir la fotografía.

Privacidad (Modo privado)

El administrador puede conceder permiso al usuario de un dispositivo determinado para que lo

utilice en modo privado. Esto permitirá al usuario desactivar las opciones automáticas de localización del dispositivo y de foto al ladrón, utilizando para ello una contraseña.

Tanto la localización del dispositivo como la foto al ladrón bajo demanda seguirán siendo opciones disponibles siempre y cuando se disponga de la contraseña que el usuario ha introducido.

Para activar de nuevo la localización y la foto al ladrón automática, será imprescindible desactivar el modo privado.

21. Cuarentena

Comportamiento de la cuarentena y Malware Freezer

Gestión de la cuarentena

21.1. Introducción

Adaptive Defense 360 almacena en una zona reservada del disco duro del equipo aquellos contenidos sospechosos de ser maliciosos o no desinfectables, así como el spyware y herramientas de hacking detectadas.

Aunque el almacenamiento de los ficheros sospechosos es local a cada equipo, la cuarentena se gestiona de forma centralizada desde la consola Web de administración para todos los dispositivos Windows, permitiendo restaurar, buscar y eliminar elementos sin necesidad de desplazarse al puesto del usuario.

21.2. Cuarentena en equipos Linux y MacOS

En los equipos Linux y Android, ni los elementos sospechosos ni el malware detectado se envían a cuarentena. El malware detectado será desinfectado o eliminado y sobre los sospechosos se informa, peo no se realiza ninguna acción.

Los equipos OS X sólo disponen de cuarentena local. Una vez que los archivos son enviados a cuarentena, podrá optar por aplicar sobre ellos alguna de las opciones disponibles (marcar como no sospechosos, reparar o eliminar).

21.3. Comportamiento de la cuarentena y Malware Freezer

21.3.1 Almacenamiento de los ficheros sospechosos

El almacenamiento de los elementos en cuarenta se realiza en el directorio `%ProgramData%\Panda Security\Panda Security Protection\Quarantine`. Se trata de una carpeta inaccesible al resto de procesos del equipo y cifrada, de manera que no es posible el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la herramienta de restauración desde la consola Web.

21.3.2 Envío de elementos a cuarentena

El envío de elementos a cuarenta es automático y establecido por el departamento de Panda Labs en Panda Security, según sea su clasificación después de haber efectuado el análisis.

Una vez que los elementos sospechosos han sido enviados para su análisis, se pueden producir tres situaciones:

- Si los elementos son maliciosos: se desinfectados y posteriormente se restauran a su ubicación original, siempre y cuando exista desinfección para ello.
- -Si los elementos son maliciosos y no existe manera de desinfectarlos: permanecerán en la cuarentena durante 7 días.
- Si no se trata de elementos perjudiciales: se restauran directamente a su ubicación original.

- Si son elementos sospechosos: se almacenan durante 30 días como máximo. Si finalmente resultan ser goodware se restauran automáticamente

Al restaurar un elemento de la cuarentena no solo se restaura el fichero propiamente dicho sino también los permisos de Windows, propietario, entradas del registro referidas al fichero etc

21.4. Gestión de la cuarentena

En la ventana principal de la consola Web, haz clic en **Cuarentena**. La ventana mostrada se estructura en dos secciones: una zona de búsqueda y otra para mostrar el listado de elementos resultantes de dicha búsqueda.

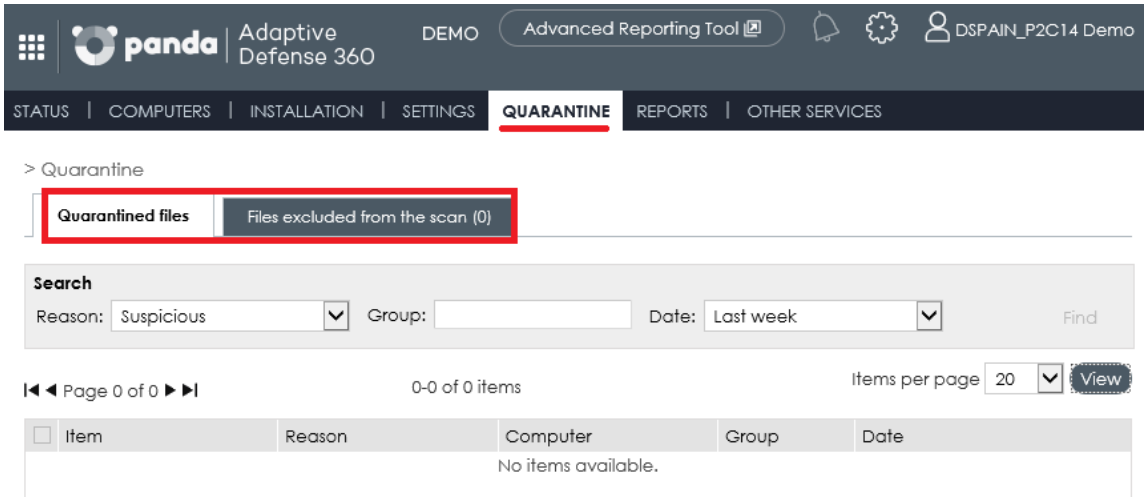


Figura 112: Ventana de cuarentena

21.4.1 Búsqueda de elementos en cuarentena

En la zona de búsqueda podrás filtrar los elementos que deseas visualizar en función de las características mostradas a continuación:

- **Motivo**: los archivos se clasifican en función de la razón o motivo por la que fueron puestos en cuarentena. Por defecto, se muestran los elementos que se han enviado a cuarentena por ser considerados sospechosos.
  - **Todos**
  - **Sospechosos**
  - **Infectados**
  - **PUP**: programas potencialmente no deseados
- **Grupo**. Una vez seleccionado el tipo de archivos que desea buscar, indica el grupo o subgrupo de equipos en que desea centrar la búsqueda.
- **Fecha**: Selecciona el periodo de tiempo que deseas.
  - **Todos**
  - **Ultimas 24h**
  - **Última semana**

- **Último mes**

21.4.2 Restauración de elementos en cuarentena

Si deseas restaurar algún elemento, marca la casilla correspondiente, haz clic en **Restaurar** y responde afirmativamente al mensaje de confirmación. A continuación, el elemento desaparecerá del listado de búsqueda y podrás encontrarlo en la pestaña **Archivos excluidos del análisis**.

Si quieres eliminar alguno de los elementos encontrados, selecciona la casilla correspondiente, haz clic en **Eliminar** y responde afirmativamente al mensaje de confirmación.

21.4.3 Listado de elementos en cuarentena

En el caso de que existan varios elementos que contengan el mismo tipo de malware, al restaurar o eliminar uno de ellos se restaurarán o eliminarán todos.

Si sitúas el cursor sobre cualquiera de los elementos del listado de búsqueda, aparecerá una etiqueta amarilla con información sobre dicho elemento.

- **Equipo**: muestra el nombre del equipo o su IP.
- **Grupo**: se detalla el nombre del grupo al que pertenece el equipo. La ruta completa del grupo sólo se muestra en el tooltip.

21.4.4 Archivos excluidos del análisis

Cuando un elemento de la ventana Cuarentena es seleccionado para restaurarlo, el elemento en cuestión desaparece de **Archivos en cuarentena** y pasa a figurar como archivo excluido del análisis **Archivos excluidos del análisis**.

De igual manera que se ha decidido excluir elementos de la cuarentena, se puede también devolverlos a dicha situación. Para ello, marca la casilla del elemento que deseas devolver y haz clic en **Deshacer exclusión**. A continuación, acepta el mensaje de confirmación.

El elemento seleccionado desaparecerá del listado de exclusiones, y volverá a aparecer en el listado de archivos en cuarentena cuando sea detectado de nuevo.

22. Análisis forense

Análisis forense mediante tablas de acciones
Análisis forense mediante grafos de ejecución
Interpretación de las tablas de acciones y grafos de actividad

22.1. Introducción

Cuando el panel de control de **Adaptive Defense 360** muestra un riesgo de infección es necesario determinar hasta qué punto ha sido comprometida la red y cuál fue el origen de la infección.

El malware de nueva generación se caracteriza por pasar inadvertido durante largos periodos de tiempo, que aprovecha para acceder a datos sensibles o a la propiedad intelectual generada por la empresa. Su objetivo es obtener una contrapartida económica, bien realizando chantaje cifrando los documentos de la empresa, bien vendiendo la información obtenida a la competencia, entre otras estrategias comunes a este tipo de ataques informáticos.

Sea cual sea el caso, se hace imprescindible determinar las acciones que desencadenó el malware en la red para poder tomar las medidas oportunas. **Adaptive Defense 360** es capaz de monitorizar de forma continuada todas las acciones ejecutadas por las amenazas, y almacenarlas para mostrar el recorrido de las mismas, desde su primera aparición en la red hasta su neutralización.

Adaptive Defense 360 presenta de forma visual este tipo de información de dos formas: a través de tablas de acciones y diagramas de grafos.

22.2. Análisis forense mediante las tablas de acciones

Desde la ventana **Estado** accede a los listados de amenazas detectadas seleccionando los paneles de la sección **Actividad** del panel de control.

Después, despliega cualquiera de ellas para obtener una tabla con información detallada de su actividad.

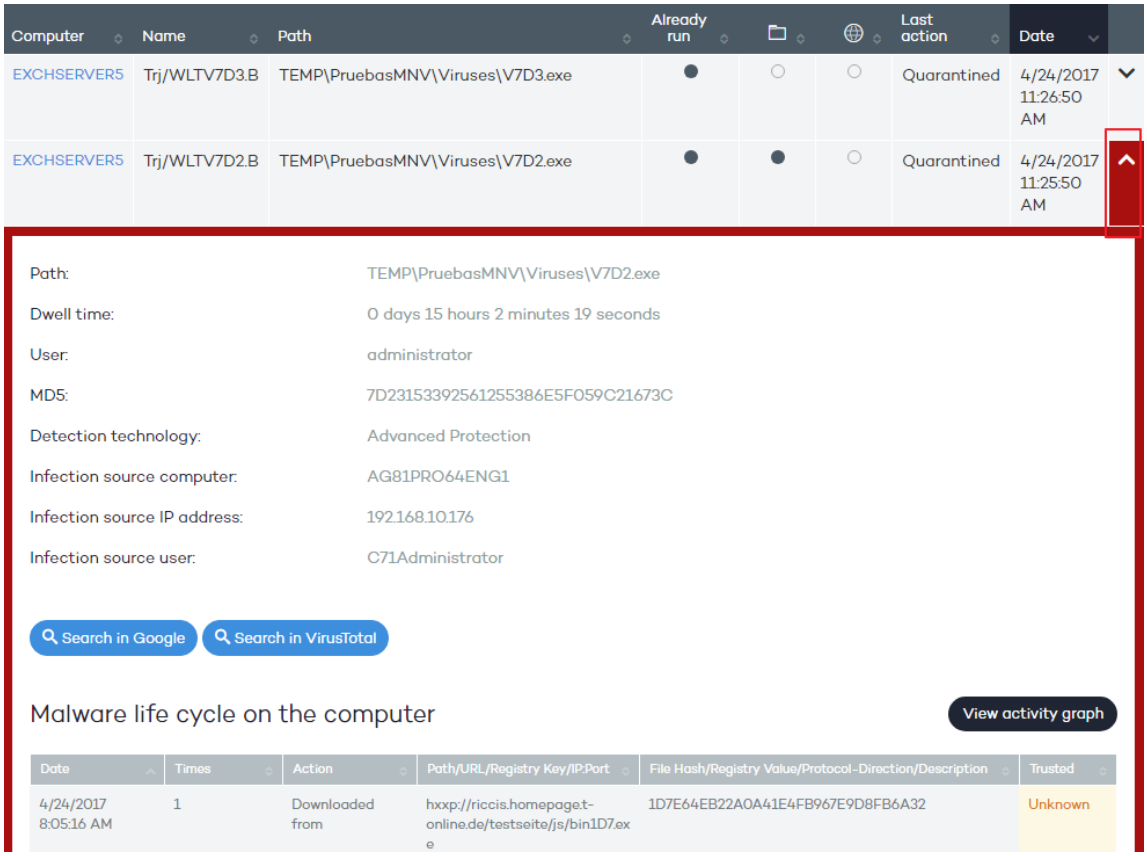


Figura 113: Acceso a las tablas de acciones / ciclo de vida de una amenaza

22.2.1 Información general de amenazas Malware

Los campos incluidos son:

- **Ruta**: Ruta del programa ejecutable que contiene el malware.
- **Tiempo de exposición**: Tiempo que la amenaza ha permanecido en el sistema sin clasificar.
- **Usuario**: usuario logeado en el sistema cuando se produjo el ataque.
- **MD5**: hash de la amenaza para su posterior consulta en VirusTotal o Google
- **Tecnología de detección**: muestra el motor que detectó la amenaza (**Protección avanzada** para detección por monitorización de las acciones del proceso, o **Antivirus** para la detección por fichero de firmas).
- **Equipo origen de la infección**: en el caso de que el intento de infección venga de un equipo de la red del cliente, indica el nombre del equipo.
- **IP origen de la infección**: en el caso de que el intento de infección venga de un equipo de la red del cliente, indica la dirección IP del equipo.
- **Usuario origen de la infección**: usuario logeado en la máquina origen de la infección
- **Ciclo de vida del malware en el equipo**: es una tabla con el detalle de cada una de las acciones desencadenadas por la amenaza.
- **Apariciones en el parque**: listado de los equipos de la red del cliente donde la amenaza fue vista, junto con la fecha de su primera aparición en cada equipo.

Se incluyen dos botones para profundizar la búsqueda en Internet mediante el buscador Google y en la web de Virustotal.

22.2.2 Información general de amenazas de tipo exploit

Los campos incluidos son:

- **Programa comprometido**: ruta del programa que recibió el intento de explotación.
- **Acción**: acción emprendida por **Adaptive Defense 360** en función de la política de seguridad asignada.
  - **Permitido por el usuario**: detección de exploit que requiere un reinicio del proceso o del equipo para ser bloqueado, en un equipo con una configuración de seguridad **Bloquear**, **Pedir permiso al usuario**, donde el usuario rechazó el reinicio del proceso comprometido.
  - **Permitido por el administrador**: detección de exploit en un equipo con una configuración de seguridad **Auditar** asignada.
  - **Bloqueo inmediato**: detección de exploit en un equipo con una configuración de seguridad **Bloquear** asignada, donde no fue necesario el reinicio del proceso ni del equipo.
  - **Bloqueo tras finalizar proceso**: detección de exploit en un equipo con una configuración de seguridad **Bloquear** asignada, donde fue necesario el reinicio del proceso o del equipo para completar el bloqueo.
  - **Detectado. Pendiente de reinicio**: detección de exploit en un equipo con una configuración de seguridad **Bloquear** asignada, donde es necesario el reinicio del proceso o del equipo para completar el bloqueo, pero todavía no se ha producido
- **Riesgo**:
  - **SI**: el equipo del usuario está en riesgo si el bloqueo del exploit ha requerido del reinicio del proceso comprometido o del sistema completo, independientemente de la política de configuración elegida por el administrador
  - **NO**: si el bloque del exploit es automático y no requiere del reinicio del proceso comprometido.
- **Usuario**: cuenta de usuario logeado en el equipo en el momento de producirse el exploit.
- **MD5**: hash del proceso comprometido
- **Tecnología de detección**: anti-exploit
- **Posible origen del exploit**: para exploits asociados a la web se mostrarán las URLs accedidas por el navegador en el momento del producirse el ataque. En otro tipo de exploit se mostrarán los ficheros accedidos por el proceso comprometido.
- **Versión del programa comprometido:** versión interna del programa comprometido que aparece en las cabeceras del ejecutable
- **Programa vulnerable**: el programa comprometido no está actualizado a la última versión y tiene vulnerabilidades conocidas y aprovechas por los atacantes
- **Ciclo de vida del malware en el equipo**: Es una tabla con el detalle de cada una de las acciones desencadenadas por el programa comprometido.
- **Apariciones en el parque**: listado de los equipos de los equipos de la red del cliente donde la amenaza fue vista junto con la fecha de su primera aparición en cada equipo

22.2.3 Tabla de acciones

En la tabla de acciones de la amenaza solo se incluyen aquellos eventos relevantes ya que la cantidad de acciones desencadenadas por un proceso es tan alta que impediría extraer información útil para realizar un análisis forense.

El contenido de la tabla se presenta inicialmente ordenado por fecha, de esta forma es más fácil seguir el curso de la amenaza.

A continuación, se detallan los campos incluidos en la tabla de acciones:

- **Fecha**: Fecha de la acción
- **Nº veces**: Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo **Nº veces** actualizado.
- **Acción**: acción realizada. A continuación, se indica una lista de las acciones que pueden aparecer en este campo:
  - Descargado de
  - Comunica con
  - Accede a datos
  - Es ejecutado por
  - Ejecuta
  - Es creado por
  - Crea
  - Es modificado por
  - Modifica
  - Es cargado por
  - Carga
  - Es borrado por
  - Borra
  - Es renombrado por
  - Renombra
  - Es matado por
  - Mata proceso
  - Crea hilo remoto
  - Hilo inyectado por
  - Es abierto por
  - Abre
  - Crea
  - Es creado por
  - Crea clave apuntando a Exe
  - Modifica clave apuntando a Exe
- **Path/URL/Clave de Registro /IP:Puerto**: es la entidad de la acción. Según sea el tipo de acción podrá contener:
  - **Clave del registro**: para todas las acciones que impliquen modificación del registro de Windows
  - **IP:Puerto**: para todas las acciones que impliquen una comunicación con un equipo

local o remoto

- **Path**: para todas las acciones que impliquen acceso al disco duro del equipo
- **URL**: para todas las acciones que impliquen el acceso a una URL

- **Hash del Fichero/Valor del Registro /Protocolo-Dirección/Descripción**: es un campo que complementa a la entidad. Según sea el tipo de acción podrá contener:
  - **Hash del Fichero**: para todas las acciones que impliquen acceso a un fichero
  - **Valor del Registro**: para todas las acciones que impliquen un acceso al registro
  - **Protocolo-Dirección**: para todas las acciones que impliquen una comunicación con un equipo local o remoto. Los valores posibles son:
    - TCP
    - UDP
    - Bidirectional
    - UnKnown
    - Descripción
- **Confiable**: El fichero está firmado digitalmente

Para localizar las acciones que más nos interesen del listado disponemos de una serie de filtros en la cabecera de la tabla.

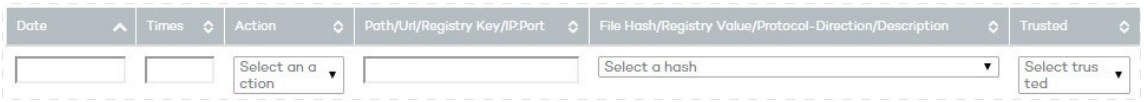


Figura 114: Herramienta de filtrado de la tabla acciones

Algunos de los campos son de tipo texto y otros son desplegables con todas las ocurrencias distintas dadas en la columna seleccionada. Las búsquedas textuales son flexibles y no requieren del uso de comodines para buscar dentro de cadenas de texto.

22.2.4 Sujeto y predicado en las acciones

Con el objeto de entender correctamente el formato utilizado para presentar la información en el listado de acciones es necesario establecer un paralelismo con el lenguaje natural:

- Todas las acciones tienen como sujeto el fichero clasificado como malware. Este sujeto no se indica en cada línea de la tabla de acciones porque es común para toda la tabla.
- Todas las acciones tienen un verbo que relaciona el sujeto (la amenaza clasificada) con un complemento, llamado entidad. La entidad se corresponde con el campo **Path/URL/Clave de Registro /IP:Puerto** de la tabla.
- La entidad se complementa con un segundo campo que añade información a la acción, que se corresponde con el campo **Hash del Fichero/Valor del Registro/Protocolo-Dirección/Descripción**.

A continuación, se muestran dos acciones de ejemplo de un mismo malware hipotético:

Fecha	Nº veces	Acción	Path/URL/Clave Registro/IP:Port	Hash del Fichero/Valor de Registro/Protocolo-Dirección/Descripción	Confiable
3/30/2015 4:38:40 PM	1	Comunica con	54.69.32.99:80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Carga	PROGRAM_FILES| \ MOVIES TOOLBAR\SAFETYN	9994BF035813FE8EB6BC98E CCBD5B0E1	NO

Tabla 11: Ejemplo de dos acciones activas ejecutadas por una amenaza

La primera acción indica que el malware (sujeto) se conecta (Acción Connects with) con la dirección IP `54.69.32.99:80` (entidad) mediante el protocolo TCP-Bidireccional.

La segunda acción indica que el malware (sujeto) carga (Acción Loads) la librería `PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL` con hash `9994BF035813FE8EB6BC98ECCBD5B0E1`

Al igual que en el lenguaje natural en **Adaptive Defense 360** se implementan dos tipos de oraciones:

- **Activa**: Son acciones predicativas (con un sujeto y un predicado) relacionados por un verbo en forma activa. En estas acciones el verbo de la acción relaciona el sujeto, que siempre es el proceso clasificado como amenaza y un complemento directo, la entidad, que puede ser de múltiples tipos según el tipo de acción.
- **Pasiva**: Son acciones donde el sujeto (el proceso clasificado como malware) pasa a ser sujeto paciente (que recibe la acción, no la ejecuta) y el verbo viene en forma pasiva (ser + participio). En este caso el verbo pasivo relaciona el sujeto pasivo que recibe la acción con la entidad, que es la que realiza la acción.

Ejemplos de acciones activas son los siguientes:

- Comunica con
- Carga
- Crea

Ejemplos de acciones pasivas son los siguientes:

- Es creado por
- Es descargado de

A continuación, se muestra una acción pasiva de ejemplo para un malware hipotético

Fecha	Nº veces	Acción	Path/URL/ Clave	Hash del Fichero/Valor de Registro/Protocolo-	Confiable

			Registro/ IP:Port	Dirección/Descripción	
3/30/2015 4:51:46 PM	1	Es ejecutado por	WINDOWS|\explorer.exe	7522F548A84ABAD8FA516DE5AB3931EF	NO

Tabla 12: Ejemplo de accion pasiva ejecutada por una amenaza

En esta acción el malware (sujeto pasivo) es ejecutado (acción pasiva Is executed by) por el programa `WINDOWS|\explorer.exe` (entidad) de hash `7522F548A84ABAD8FA516DE5AB3931EF`.

Las acciones de tipo Activo nos permiten inspeccionar en detalle los pasos que ha ejecutado el Malware. Por el contrario, las acciones de tipo pasivo suelen reflejar el vector de infección utilizado por el malware (qué proceso lo ejecutó, qué proceso lo copió al equipo del usuario etc.).

22.3. Análisis forense mediante grafos de ejecución

Los grafos de ejecución representan de forma visual la información mostrada en las tablas de acciones poniendo énfasis en el enfoque temporal.

Los grafos se utilizan inicialmente para tener, de un solo vistazo, una idea general de las acciones desencadenadas por la amenaza.

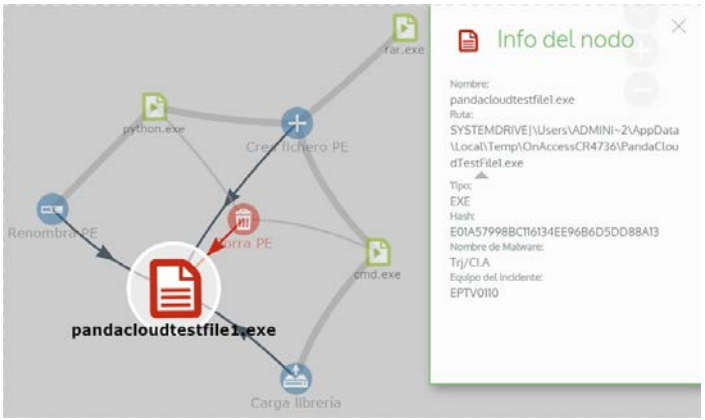


Figura 115: Información mostrada por un nodo en el diagrama de grafos

22.3.1 Diagramas

La cadena de acciones en la vista de grafos de ejecución queda representada por dos elementos:

- **Nodos**: representan acciones en su mayoría o elementos informativos
- **Líneas y flechas**: unen los nodos de acción e informativos para establecer un orden temporal y asignar a cada nodo el rol de "sujeto" o "predicado".

22.3.2 Nodos

Los nodos muestran la información mediante su icono asociado, color y un panel descriptivo que se muestra a la derecha de la pantalla cuando se seleccionan con el ratón.

El código de colores utilizado es el siguiente:

- **Rojo**: elemento no confiable, malware, amenaza.
- **Naranja**: elemento desconocido, no catalogado.
- **Verde**: elemento confiable, goodware.

A continuación, se listan los nodos de tipo acción junto con una breve descripción:

Símbolo	Descripción
	Fichero descargado Fichero comprimido creado
	Socket / comunicación usada
	Comenzada la monitorización
	Proceso creado
	Fichero ejecutable creado Librería creada Clave en el registro creada
	Fichero ejecutable modificado Clave de registro modificada
	Fichero ejecutable mapeado para escritura
	Fichero ejecutable borrado
	Librería cargada
	Servicio instalado
	Fichero ejecutable renombrado
	Proceso detenido o cerrado

	Hilo creado remotamente
	Fichero comprimido abierto

Tabla 13: Nodos de tipo acción e información asociada

A continuación, se listan los nodos de tipo descriptivo junto con una breve descripción

Símbolo	Descripción
	Nombre de fichero y extensión **Verde**: Goodware **Naranja**: No catalogado **Rojo**: Malware/PUP
	Equipo interno (está en la red corporativa) **Verde**: Confiable **Naranja**: desconocido **Rojo**: No confiable
	Equipos externo **Verde**: Confiable **Naranja**: desconocido **Rojo**: No confiable
	País asociado a la IP de un equipo externo
	Fichero y extensión
	Clave del registro

Tabla 14: Tipos de nodo final e información asociada

22.3.3 Líneas y flechas

Las líneas del diagrama de grafos relacionan los diferentes nodos y ayudan a establecer el orden de ejecución de acciones de la amenaza de forma visual.

Los dos atributos de una línea son:

- **Grosor de la línea**: el grosor de una línea que une dos nodos indica el número de ocurrencias que esta relación ha tenido en el diagrama. A mayor número de ocurrencias mayor tamaño de la línea
- **Flecha**: marca la dirección de la relación entre los dos nodos.

22.3.4 La línea temporal

La línea temporal o Timeline permite controlar la visualización de la cadena de acciones realizada por la amenaza a lo largo del tiempo. Para visualizar el momento preciso en el que la amenaza

realizó cierta acción y recuperar información extendida que nos pueda ayudar en los procesos de análisis forense utiliza los botones situados en la parte inferior de la pantalla.

La línea temporal de los grafos de ejecución tiene este aspecto:

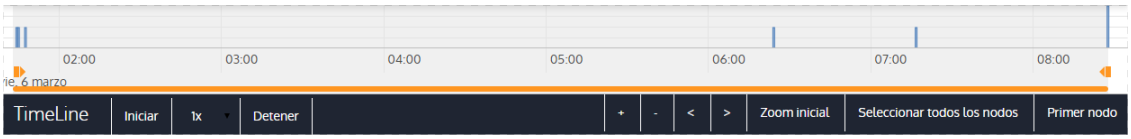


Figura 116: Línea temporal del ciclo de vida de una amenaza

Selecciona un intervalo concreto de la línea temporal arrastrando los selectores de intervalo hacia la izquierda o derecha para abarcar la franja temporal más interesante.

Figura 117: Seleccion de un intervalo en la linea temporal

Una vez seleccionada la franja temporal, el grafo mostrará únicamente las acciones y nodos que caigan dentro de ese intervalo. El resto de acciones y nodos quedará difuminado en el diagrama.

Las acciones de la amenaza quedan representadas en la línea temporal como barras verticales acompañadas del time stamp, que marca la hora y minuto donde ocurrieron.

Figura 118: Información temporal de las acciones de una amenaza

22.3.5 Zoom in y Zoom out

Para hacer zoom in o zoom out y ganar mayor resolución en el caso de que haya muchas acciones en un intervalo de tiempo corto utiliza los botones **+** y **–** de la barra temporal.

22.3.6 Timeline (línea temporal)

Para poder ver la ejecución completa de la amenaza y la cadena de acciones que ejecutó utiliza los siguientes controles:

- **Iniciar**: comienza la ejecución de la Timeline a velocidad constante de 1x. Los grafos y las líneas de acciones irán apareciendo según se vaya recorriendo la línea temporal.
- **1x**: establece la velocidad de recorrido de la línea temporal
- **Detener**: detiene la ejecución de la línea temporal
- **+ y -:** zoom in y zoom out de la línea temporal

- **< y >**: mueve la selección del nodo al inmediatamente anterior o posterior
- **Zoom inicial**: recupera el nivel de zoom inicial si se modificó con los botones + y –
- **Seleccionar todos los nodos**: mueve los selectores temporales para abarcar toda la línea tempora
- **Primer nodo**: Establece el intervalo temporal en el inicio, paso necesario para iniciar la visualización de la TimeLine completa

Para poder visualizar el recorrido completo de la Timeline primero seleccionar "Primer nodo" y después "Iniciar". Para ajustar la velocidad de recorrido seleccionar el botón 1x.

22.3.7 Filtros

En la parte superior del diagrama de grafos se encuentran los controles para filtrar la información mostrada.

Los criterios de filtrado disponibles son:

- **Acción**: desplegable que permite seleccionar un tipo de acción de entre todas las ejecutadas por la amenaza. De esta manera el diagrama solo muestra los nodos que coincidan con el tipo de acción seleccionada y aquellos nodos adyacentes relacionados con esta acción.
- **Entidad**: desplegable que permite elegir una entidad (contenido del campo Path/URL/Entrada de registro /IP:Puerto)

22.3.8 Movimiento de los nodos y zoom general del grafo

Para mover el grafo en las cuatro direcciones y hacer zoom in o zoom out utiliza los controles situados en la parte superior derecha del grafo.

Para hacer zoom in y zoom out más fácilmente se puede utilizar la rueda central del ratón.

El símbolo X permite salir de la vista de grafos.

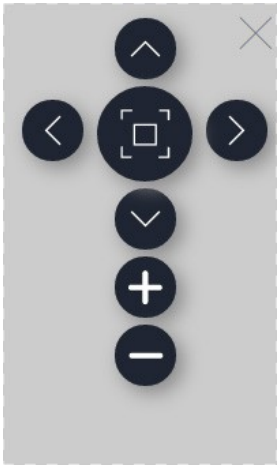


Figura 119: Controles para el manejo del diagrama de grafos

Si se prefiere ocultar la zona de botones Timeline para utilizar un mayor espacio de la pantalla para el grafo se puede seleccionar el símbolo  situado en la parte inferior derecha del grafo.

Finalmente, el comportamiento del grafo al ser representando en pantalla o arrastrado por alguno de sus nodos se configura mediante el panel mostrado a continuación, accesible al seleccionar el botón  situado a la izquierda arriba del grafo

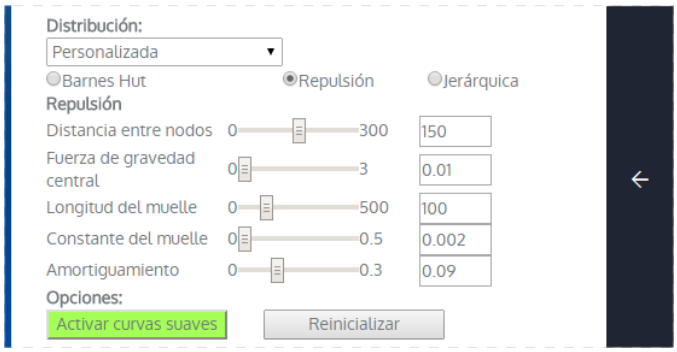


Figura 120: Configuración del comportamiento del diagrama de grafos

22.4. Interpretación de las tablas de acciones y grafos de actividad

Para interpretar correctamente las tablas de acciones y grafos de **Actividad** se requieren ciertos conocimientos técnicos ya que ambos recursos son representaciones de los volcados de evidencias recogidas, que deberán ser interpretadas por el propio administrador de red de la empresa.

En este capítulo se ofrecen unas directrices básicas de interpretación a través de varios ejemplos de malware real.

El nombre de las amenazas aquí indicadas puede variar entre diferentes proveedores de seguridad. Para identificar un malware concreto se recomienda utilizar el hash de identificación.

22.4.1 Ejemplo 1: Visualización de las acciones ejecutadas por el malware Trj/OCJ.A

En la cabecera de la tabla alertas se muestra la información fundamental del malware encontrado. En este caso los datos relevantes son los siguientes:

- **Fecha**: 06/04/2015 3:21:36
- **Equipo**: XP-BARCELONA1
- **Nombre**: Trj/OCJ.A
- **Tipo**: MW
- **Estado**: Ejecutado

- **Ruta del Malware**: TEMP | \Rar$EXa0.946\appnee.com.patch.exe

Estado del equipo

El estado del malware es Ejecutado debido a que el modo de **Adaptive Defense 360** configurado era Hardening: el malware ya residía en el equipo en el momento en que **Adaptive Defense 360** se instaló y era desconocido en el momento de su ejecución.

Hash

Con la cadena de hash se podrá obtener más información en sitios como Virus total para tener una idea general de la amenaza y su forma de funcionamiento.

Ruta del Malware

La ruta donde se detectó el malware por primera vez en el equipo pertenece a un directorio temporal y contiene la cadena RAR, de modo que procede de un fichero empaquetado que el programa WinRar descomprimió temporalmente en el directorio y dio como resultado el ejecutable `appnee.com.patch.exe`

Tabla de acciones

Paso	Fecha	Acción	Path
1	3:17:00	Es creado por	PROGRAM_FILES| \WinRAR\WinRAR.exe
2	3:17:01	Es ejecutado por	PROGRAM_FILES| \WinRAR\WinRAR.exe
3	3:17:13	Crea	TEMP| \bassmod.dll
4	3:17:34	Crea	PROGRAM_FILES| \Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifica	PROGRAM_FILES| \Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Borra	PROGRAM_FILES| \ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK
7	3:17:41	Crea	PROGRAM_FILES| \Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifica	PROGRAM_FILES| \Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll

9	3:17:59	Ejecuta	PROGRAM_FILES|\Google\Chrome\Application\chrome.exe

Tabla 15: Tabla de acciones ejemplo 1

Los pasos 1 y 2 indican que el malware fue descomprimido por el `WinRar.Exe` y ejecutado desde el mismo programa: el usuario abrió el fichero comprimido e hizo clic en el binario que contiene.

Una vez en ejecución en el paso 3 el malware crea una dll (`bassmod.dll`) en una carpeta temporal y otra (paso 4) en el directorio de instalación del programa Adobe Acrobat 11. En el paso 5 también modifica una dll de Adobe, quizá para aprovechar algún tipo de exploit del programa.

Después de modificar otras dlls lanza una instancia de Chrome y en ese momento termina la Timeline; **Adaptive Defense 360** catalogó el programa como amenaza después de esa cadena de acciones sospechosas y ha detenido su ejecución.

En la Timeline no aparecen acciones sobre el registro de modo que es muy probable que el malware no sea persistente o no haya podido ejecutarse hasta ese punto de lograr sobrevivir a un reinicio del equipo.

El programa Adobe Acrobat 11 ha resultado comprometido de modo que se recomienda su reinstalación, aunque gracias a que **Adaptive Defense 360** monitoriza ejecutables tanto si son goodware como malware, la ejecución de un programa comprometido será detectada en el momento en que desencadene acciones peligrosas, terminando en su bloqueo.

22.4.2 Ejemplo 2: Comunicación con equipos externos en BetterSurf

BetterSurf es un programa potencialmente no deseado que modifica el navegador instalado en el equipo del usuario e inyecta anuncios en las páginas Web que visite.

En la cabecera de la tabla alertas se muestra la información fundamental del malware encontrado. En este caso se cuenta con los siguientes datos:

- **Fecha**: 30/03/2015
- **Equipo**: MARTA-CAL
- **Nombre**: PUP/BetterSurf
- **Tipo**: MW
- **Ruta del Malware**: PROGRAM_FILES|\VER0BLOCKANDSURF\N4CD190.EXE
- **Tiempo de exposición**: 11 días 22 horas 9 minutos 46 segundos

Tiempo de exposición

En este caso el tiempo de exposición ha sido muy largo: durante casi 12 días el malware estuvo en estado latente en la red del cliente. Este comportamiento es cada vez más usual y puede deberse a varios motivos: puede ser que el malware no ha realizado ninguna acción sospechosa hasta muy tarde o que simplemente el usuario descargó el fichero, pero no lo ejecutó en el momento.

Tabla de acciones

Paso	Fecha	Acción	Path
1	08/03/2015 11:16	Es creado por	TEMP | \08c3b650-e9e14f.exe
2	18/03/2015 11:16	Es ejecutado por	SYSTEM | \services.exe
3	18/03/2015 11:16	Carga	PROGRAM_FILES | \VER0BLOF\N4Cd190.dll
4	18/03/2015 11:16	Carga	SYSTEM | \BDL.dll
5	18/03/2015 11:16	Comunica con	127.0.0.1:13879
6	18/03/2015 11:16	Comunica con	37.58.101.205:80
7	18/03/2015 11:17	Comunica con	5.153.39.133:80
8	18/03/2015 11:17	Comunica con	50.97.62.154:80
9	18/03/2015 11:17	Comunica con	50.19.102.217:80

Tabla 16: Tabla de acciones ejemplo 2

En este caso se puede apreciar como el malware establece comunicación con varias IPs. La primera de ellas (paso 5) es el propio equipo y el resto son IPs del exterior a las que se conecta por el puerto 80, de las cuales probablemente se descargue los contenidos de publicidad.

La principal medida de prevención en este caso será bloquear las IPs en el cortafuegos corporativo.

Antes de añadir reglas para el bloqueo de IPs en el cortafuegos corporativo se recomienda consultar las IPs a bloquear en el RIR asociado (RIPE, ARIN, APNIC etc.) para ver la red del proveedor al que pertenecen. En muchos casos la infraestructura remota utilizada por el malware es compartida con servicios legítimos alojados en proveedores como Amazon y similares de modo que bloquear IPs equivaldría a bloquear también el acceso a páginas Web normales.

22.4.3 Ejemplo 3: acceso al registro con PasswordStealer.BT

`PasswordStealer.BT` es un troyano que registra la actividad del usuario en el equipo y envía la información obtenida al exterior. Entre otras cosas es capaz de capturar la pantalla del usuario, registras las teclas pulsadas y enviar ficheros a un servidor C&C (Command & Control).

En la cabecera de la tabla alertas se muestra la información fundamental del Malware encontrado. En este caso se cuenta con los siguientes datos:

- **Ruta del Malware**: APPDATA | \microsoftupdates\micupdate.exe

Por el nombre y la localización del ejecutable el malware se hace pasar por una actualización de Microsoft. Este malware en concreto no tiene capacidad para contagiar equipos por sí mismo, requiere que el usuario ejecute de forma manual el virus.

Estado del equipo

El estado del malware es Ejecutado debido a que el modo de **Adaptive Defense 360** configurado era Hardening: el malware ya residía en el equipo en el momento en que **Adaptive Defense 360** se instaló y era desconocido en el momento de su ejecución.

Tabla de acciones

Paso	Fecha	Acción	Path
1	31/03/2015 23:29	Es ejecutado por	PROGRAM_FILESX86 | \internet explorer\iexplore.exe
2	31/03/2015 23:29	Es creado por	INTERNET_CACHE | \Content.IE5\ QGV8PV80\ index[1].php
3	31/03/2015 23:30	Crea clave apuntando a Exe	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Wind ows\ CurrentVersion\Run?MicUpdate
4	31/03/2015 23:30	Ejecuta	SYSTEMX86 | \notepad.exe
5	31/03/2015 23:30	Hilo inyectado por	SYSTEMX86 | \notepad.exe

Tabla 17: Tabla de acciones ejemplo 3

En este caso el malware es creado en el paso 2 por una página Web y ejecutado por el navegador Internet Explorer.

El orden de las acciones tiene una granularidad de 1 microsegundo. Por esta razón varias acciones ejecutadas dentro del mismo microsegundo pueden aparecer desordenadas en la Timeline, como sucede en el paso 1 y paso 2.

Una vez ejecutado el malware se hace persistente en el paso 3 añadiendo una rama en el registro que pertenece al usuario y que lanzará el programa en el inicio del sistema. Después comienza a ejecutar acciones propias del malware como arrancar un notepad e inyectar código en uno de sus hilos.

Como acción de resolución en este caso y en ausencia de un método de desinfección conocido

se puede minimizar el impacto de este malware borrando la entrada del registro. Es muy posible que en una máquina infectada el malware impida modificar dicha entrada; dependiendo del caso sería necesario arrancar el equipo en modo seguro o con un CD de arranque para borrar dicha entrada.

22.4.4 Ejemplo 4: Acceso a datos confidenciales en Trj/Chgt.F

`Trj/Chgt.F` fue publicado por wikileaks a finales de 2014 como herramienta utilizada por las agencias gubernamentales de algunos países para realizar espionaje selectivo.

En este ejemplo pasaremos directamente a la tabla de acciones para observar el comportamiento de esta amenaza avanzada.

Tabla de acciones

Paso	Fecha	Acción	Path
1	4/21/2015 2:17:47 PM	Es ejecutado por	SYSTEMDRIVE| \Python27\pythonw.exe
2	4/21/2015 2:18:01 PM	Accede a datos	#.XLS
3	4/21/2015 2:18:01 PM	Accede a datos	#.DOC
4	4/21/2015 2:18:03 PM	Crea	TEMP| \doc.scr
5	4/21/2015 2:18:06 PM	Ejecuta	TEMP| \doc.scr
6	4/21/2015 2:18:37 PM	Ejecuta	PROGRAM_FILES| \Microsoft Office\Office12\WI NWORD.EXE
7	4/21/2015 8:58:02 PM	Comunica con	192.168.0.1:2042

Tabla 18: Tabla de acciones ejemplo 4

Inicialmente el malware es ejecutado por el intérprete de Python (paso 1) para luego acceder a un documento de tipo Excel y otro de tipo Word (paso 2 y 3). En el paso 4 se ejecuta un fichero de extensión `scr`, probablemente un salvapantallas con algún tipo de fallo o error que provoque una situación anómala en el equipo y que pueda ser aprovechada por el malware.

En el paso 7 se produce una conexión de tipo TCP. La dirección IP es privada de modo que se estaría conectando a la red del propio cliente.

En este caso se deberá de comprobar el contenido de los ficheros accedidos para evaluar la pérdida de información, aunque viendo la Timeline la información accedida en principio no ha sido

extraída de la red del cliente.

Adaptive Defense 360 desinfectará por sí mismo la amenaza y bloqueará de forma automática posteriores ejecuciones del malware en este y en otros clientes.

23. Apéndice I: Herramientas de instalación centralizada

Instalación mediante Directorio Activo
Instalación mediante la herramienta de distribución

23.1. Introducción

Adaptive Defense 360 permite la instalación del agente Windows de forma centralizada en redes de tamaño medio o grande, mediante la herramienta de distribución centralizada incluida de forma gratuita o con herramientas de terceros.

En este capítulo se detalla la instalación del agente **Adaptive Defense 360** en una red Windows con Directorio Activo y con la herramienta de distribución incluida.

23.2. Instalación mediante Directorio Activo

A continuación, se muestran los pasos de una instalación mediante una GPO (Group Policy Object).

- Descarga del instalador **Adaptive Defense 360** y compartición: Coloca el instalador **Adaptive Defense 360** en una carpeta compartida que sea accesible por todos aquellos equipos que vayan a recibir el agente.
- Abre el applet "Active Directory Users and Computers" en el Directorio Activo de la red y crea una nueva OU (Organizational Unit) de nombre "Adaptive Defense".

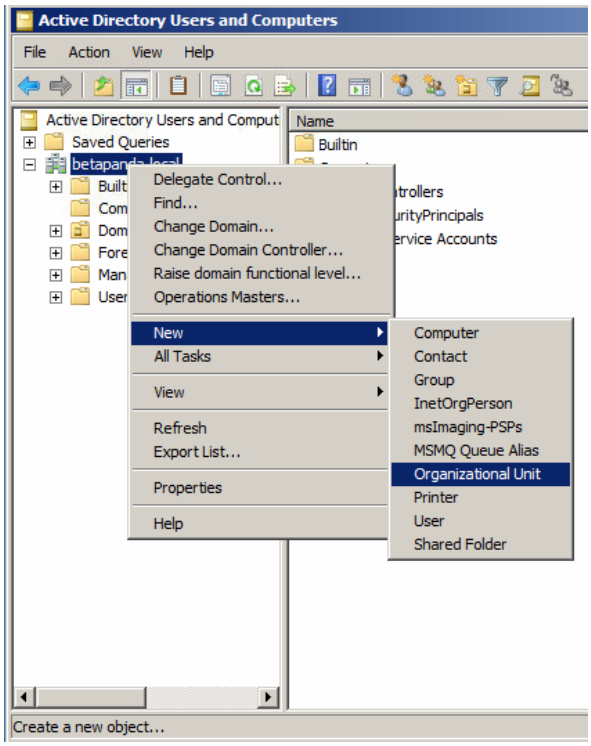


Figura 121: Creación de una nueva Unidad Organizativa

- Abre el snap-in Group Policy Management y en Domains selecciona la OU recién creada para bloquear la herencia.

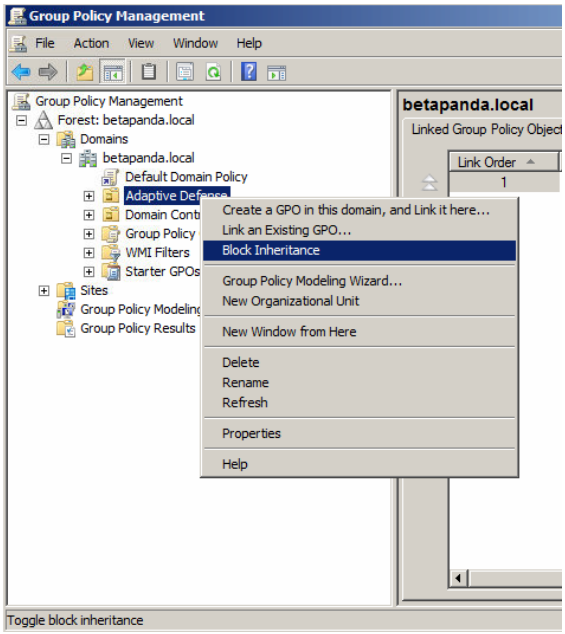
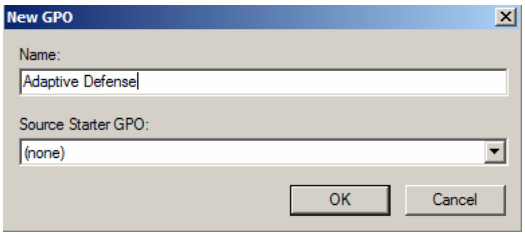


Figura 122: Bloqueo de la herencia

- Crea una nueva GPO en la OU "Adaptive Defense"



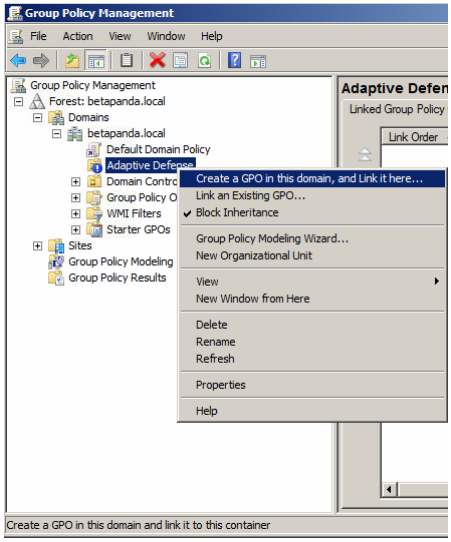


Figura 123: Creación de una nueva GPO

- Edita la GPO y añade un nuevo paquete de instalación que contendrá el agente **Adaptive Defense 360**. Para ello se nos pedirá que añadamos el instalador a la GPO.

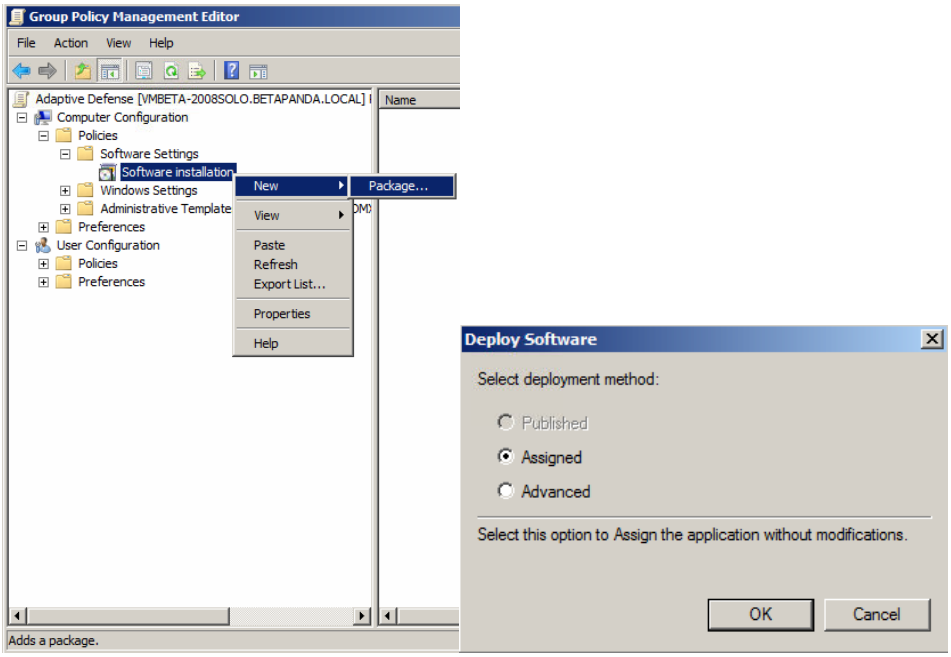


Figura 124: Creación de un nuevo paquete de instalación

- Una vez añadido mostramos las propiedades y en la pestaña Deployment, Advanced selecciona la casilla que evita la comprobación entre el sistema operativo de destino y el definido en el instalador.

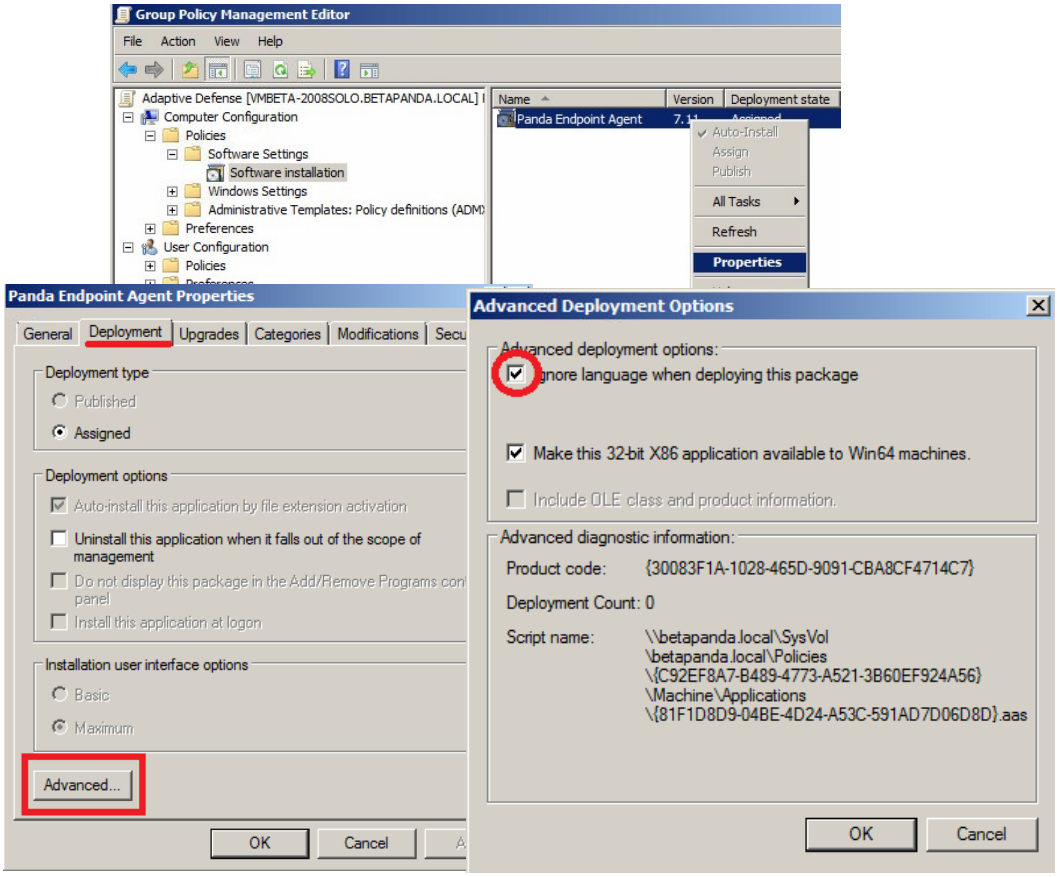


Figura 125: Configuración para ignorar el idioma definido en el instalador

- Finalmente añade en la OU Adaptive Defense creada anteriormente en Active Directory Users and Computers a todos los equipos de la red que se quiera enviar el agente.

23.3. Instalación mediante la herramienta de distribución

23.3.1 Requisitos mínimos

La instalación mediante la herramienta de distribución requiere de un equipo Windows con los requisitos mínimos mostrados a continuación:

- Sistema operativo: Windows, 10, Windows 8.1, Windows 8, Windows 7 (32 y 64 bits), Windows Vista (32 y 64 bits), Windows XP Professional (32 y 64 bits), Windows 2000 Professional, Windows Server 2000, Windows Server 2003 (32 y 64 bits), Windows Server 2008 (32 y 64 bits), Windows Server 2008 R2, Windows Home Server, Windows Server 2012 y Windows Server 2012 R2 (PCOP 6.70.20).
- Memoria: 64 MB
- Disco duro: 20 MB
- Procesador: Pentium II 300 MHz o equivalente
- Windows Installer 2.0 (aunque se recomienda Windows Installer 3.0 si se quiere poder desinstalar de forma remota)
- Navegador: Internet Explorer 6.0 o superior
- Otros:
  - Tener acceso al recurso Admin$ de los equipos en los que se va a distribuir la protección.
  - Disponer de un usuario con derechos de administrador sobre los equipos en los que se va a distribuir la protección.

Para que la herramienta funcione correctamente, en caso de utilizar Internet Explorer deberá desactivar en las **Opciones Avanzadas de Seguridad** el uso de SSL y activar el uso de TSL:

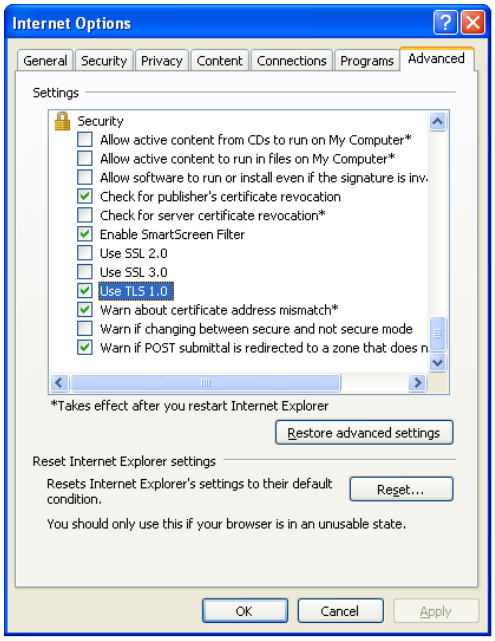


Figura 126: Activación de TLS en Internet Explorer

23.3.2 Pasos para el despliegue

A continuación, se muestran los pasos de una instalación mediante la herramienta de distribución de Panda Security.

Para descargar la herramienta de instalación haz clic en la ventana **Instalación** y luego **Descargar herramienta de distribución**

- Ejecuta el fichero `Distributiontool.msi` en el equipo que distribuirá el agente **Adaptive Defense 360** en la red.
- Una vez instalado ejecuta la herramienta desde el menú Inicio de Windows y se mostrará la pantalla de Instalación de protecciones, que permitirá distribuir la protección de dos modos:

Distribución por Dominios

- Introduce el grupo en el que se vayan a incluir los equipos a instalar. Esta selección marcará el perfil de protección que se va a aplicar a estos equipos.
- Dentro del árbol de red, selecciona los dominios o equipos sobre los que se quiere instalar.
- Utiliza un usuario y contraseña con permisos de administrador para realizar la instalación. El nombre de usuario deberá introducirse con formato dominio\usuario.
- Una vez introducidos los datos, pulsa la opción Instalar, para generar las tareas de instalación.

Distribución por direcciones IP o nombre de equipo

- Introduce el grupo en el que se vayan a incluir los equipos a instalar. Esta selección marcará el perfil de protección que se va a aplicar a estos equipos.
- En este paso, añade los nombres de los equipos a instalar, o las direcciones IP de los mismos, separadas por comas. También es posible seleccionar rangos de IPs (usar el símbolo "-" para los rangos (ej: `172.18.15.10 – 172.18.15.50`).
- Utiliza un usuario y contraseña con permisos de administrador para realizar la instalación. El nombre de usuario se deberá introducir con formato dominio\usuario
- Pulsa Instalar, para generar las tareas de instalación.
  - Verifica desde la consola que la tarea de instalación se ha completado con éxito.
  - A partir de entonces, comenzará la instalación de la protección, de forma completamente transparente.
  - Reinicia el equipo si así lo solicita.

23.3.3 Pasos para la desinstalación centralizada de Adaptive Defense 360

La herramienta de distribución de **Adaptive Defense 360** permite desinstalar la protección de una forma centralizada, evitando así la intervención manual de los usuarios a lo largo del proceso. Para ello sigue los pasos mostrados a continuación:

- Una vez en la consola de la herramienta, selecciona **Desinstalar protecciones**. Se abrirá la pantalla **Desinstalación de protecciones**, que permitirá desinstalar la protección de dos modos:

Desinstalación por Dominios

- Dentro del árbol de red, selecciona los dominios o equipos de los que quieres desinstalar.
- Introduce la contraseña de desinstalación que se utilizó para la instalación. En el caso de no haber utilizado contraseña, deja este campo en blanco.

- Utiliza un usuario y contraseña con permisos de administrador para realizar la desinstalación.
- El nombre de usuario deberá introducirse con formato dominio\usuario.
- Selecciona si deseas mantener los elementos en la cuarentena o no. En el caso de activar esta casilla, los elementos en cuarentena se eliminarán.
- Selecciona si deseas reiniciar los equipos tras la desinstalación. En este caso, los equipos se reiniciarán automáticamente una vez concluida la desinstalación.
- Una vez introducidos los datos, pulse la opción **Desinstalar**, para generar las tareas de desinstalación.

Desinstalación por direcciones IP o nombre de equipo

- Añade los nombres de los equipos a desinstalar, o las direcciones IP de los mismos, separadas por comas. También es posible seleccionar rangos de IPs (usar el símbolo "-" para los rangos (ej: `172.18.15.10 – 172.18.15.50`).
- Introduce la contraseña de desinstalación que se utilizó para la instalación. En el caso de no haber utilizado contraseña, deja este campo en blanco.
- Utiliza un usuario y contraseña con permisos de administrador para realizar la desinstalación.
- El nombre de usuario se deberá introducir con formato dominio\usuario
- Selecciona si deseas mantener los elementos en la cuarentena o no. En el caso de activar esta casilla, los elementos en cuarentena se eliminarán.
- Selecciona si deseas reiniciar los equipos tras la desinstalación. En este caso, los equipos se reiniciarán automáticamente una vez concluida la desinstalación.
- Pulse Desinstalar, para generar las tareas de desinstalación.
    - Verifica desde la consola que la tarea de desinstalación se ha completado con éxito.
    - A partir de ese momento, comenzará la desinstalación de las protecciones, de forma completamente transparente.
    - Reinicia los equipos cuando así se solicite.

24. Apéndice II: Comunicación con el equipo

Comunicación del equipo con Internet
Consumo de ancho de banda
Seguridad de las comunicaciones y de los datos almacenados

24.1. Introducción

En este apéndice se describen las comunicaciones entre los agentes y el servidor **Adaptive Defense 360**.

24.2. Comunicación del equipo con Internet

24.2.1 Intervalos de comunicación

Los agentes **Adaptive Defense 360** instalados en los equipos de la red se comunican con el servidor a intervalos regulares. Estos intervalos dependen del tipo de información que se transmita. Las cifras indicadas a continuación indican el tiempo transcurrido como máximo desde que se produce un evento que deba ser enviado al servidor, hasta que realmente se envía.

- **Comprobación de cambios de configuración en la consola**: cada 15 minutos
- **Cambios en la configuración del equipo (nombre, IP, Mac, versión del sistema operativo, Service pack etc)**: cada 12 horas.
- **Configuración del equipo (sin cambios)**: cada 24 horas
- **Comprobación de nuevo archivo de identificadores**: 4 horas por defecto.
- **Comprobación de actualización del motor de la protección**: 12 horas por defecto. Acceso a Internet

La siguiente tabla muestra de forma resumida cómo acceden a Internet los agentes de **Adaptive Defense 360** para las tareas que requieren comunicación a través de Internet.

Paso	Conecta do a Internet	No conecta do a Internet (al menos 1 agente en la red está conecta do)
Mensajes de comunicación con el servidor	Desde el puesto o también se pueden realizar desde un equipo especificado por configuración.	Desde el puesto que tenga conexión a Internet o desde el equipo que se haya especificado de forma explícita por configuración
Actualización de ficheros de firmas	Comparte las firmas descargadas por otros equipos de la red gracias a la tecnología P2P. Descarga los ficheros de firmas si otro equipo de la red no las ha descargado previamente. También se puede especificar por configuración un equipo del que realizar las descargas de las firmas. Este equipo actuará también como repositorio almacenando las firmas para que no sea necesario volver a descargarlas cuando las solicite otro equipo.	Actualización desde el puesto de la red que tenga conexión a Internet o desde el equipo que se haya especificado de forma explícita por configuración.
Instalación y actualizaciones del producto	Comparte los paquetes descargados por otros equipos de la red gracias a la tecnología P2P de **Adaptive Defense 360**. Descarga los paquetes si otro equipo de la red no los ha descargado previamente. También se puede especificar de forma explícita por configuración un equipo del	Actualización desde el puesto de la red que tenga conexión a Internet o desde el equipo que se haya especificado de forma explícita por configuración.

	que realizar la descarga del paquete del producto.	
Acceso a la Inteligencia colectiva	Las comunicaciones con la Inteligencia Colectiva son desde cada PC.*	No disponible aún el acceso a la Inteligencia Colectiva desde puestos sin conexión a Internet*.

Tabla 19: Secuencia de pasos para el acceso del equipo a Internet

*Si los PCs salen a Internet a través del proxy de la empresa, **Adaptive Defense 360** hará lo mismo. El proxy de la empresa a utilizar es parte de la configuración de **Adaptive Defense 360**.

24.3. Consumo de ancho de banda

La siguiente tabla muestra en forma de resumen el consume de ancho de banda de **Adaptive Defense 360** para los diferentes tipos de comunicación que se realizan.

Tipo de comunicación	Uso de ancho de banda aproximado
Instalación del producto	8.18 MB: Instalador y agente de comunicaciones 60.5 MB: Paquete del software de seguridad
Comunicaciones con el servidor	240 KB cada 12 horas (190KB en mensajes cada 15 minutos para ver si hay cambios de configuración y 50 KB en mensajes de estado, configuración y reportes)
Envío de las acciones realizadas por cada proceso en ejecución	1 MB al día por cada equipo
Actualización de los ficheros de conocimiento**	25 MB sólo la primera vez, tras instalar la protección 200 -300 KB cada 24 horas para las actualizaciones incrementales de conocimiento
Actualizaciones del producto**	8.18 MB: Agente de comunicaciones 60.5 MB: Paquete del software de seguridad Se realiza una actualización del producto cada 6 meses aproximadamente.
Consultas a la inteligencia Colectiva	Protección permanente en tiempo real 500 KB: Consumo el primer día cuando la cache está vacía. 35-100 KB: Consumo tras el primer día, una vez que la información está cacheada. Análisis de todo el PC 200-500 KB: Primer análisis de todo el PC. 50-200 KB: Sucesivos análisis de todo el PC.

Tabla 20: Consumos de ancho de banda unitarios según el tipo de operación efectuada en el equipo

*46,2 MB para el instalador de 64 bits

Las descargas para las actualizaciones de los ficheros de firmas y del producto son realizadas por 1 único equipo de la red, siempre y cuando los diferentes equipos requieran los mismos ficheros, gracias a la tecnología P2P de **Adaptive Defense 360.

Los ficheros de firmas incrementales son diferentes dependiendo del número de días que lleven desactualizados. Así, si un equipo tiene ficheros de firmas de hace 2 días y otro tiene ficheros de firmas de hace 1 día, los ficheros de firmas incrementales que se requieren descargar son diferentes.

Si se especifica de forma explícita que un equipo actúe como proxy / repositorio, todas las comunicaciones excepto las consultas a la Inteligencia Colectiva se harán a través de este equipo. Además, los ficheros de firmas se almacenarán en el equipo configurado como repositorio de forma que no será necesario descargarlas de nuevo cuando otro equipo de la red las requiera.

Cálculo del consumo de ancho de banda

Supongamos que tenemos una red de X PCs que están conectados entre sí en la red local y en los cuales vamos a instalar **Adaptive Defense 360**. El consumo de ancho de banda en esta red será aproximadamente el reflejado en la siguiente tabla.

Tipo de comunicación	Consumo de ancho de banda de acceso a Internet de X PCs	Consumo de ancho de banda en la en red local de X PCs
Instalación del producto (1 única vez)	8.18 MB del instalador y agente de comunicaciones X PCs + 60.5 MB del paquete del software de seguridad * X PCs	8.18 MB del instalador y agente de comunicaciones X PCs 60.5 MB del paquete del software de seguridad
Comunicaciones con el servidor	240 KB cada 12 horas * X PCs	240 KB cada 12 horas * X PCs
Envío de las acciones realizadas por cada proceso en ejecución	1 MB al día * X PCs	1 MB al día * X PCs
Actualización de los ficheros de conocimiento	25 MB sólo la primera vez, tras instalar la protección * X PCs + 160 KB cada 24 horas para las actualizaciones de conocimiento incremental * X PCs	25 MB sólo la primera vez, tras instalar la protección 160 KB cada 24 horas para las actualizaciones de conocimiento incremental
Actualizaciones del producto (cada 6 meses aproximadamente)	8.18 MB del instalador y agente de comunicaciones * X PCs + 60.5 * MB del paquete del software de seguridad * X PCs	8.18 MB del instalador y agente de comunicaciones + 60.5 * MB del paquete del software de seguridad
Consultas a la inteligencia Colectiva	500 KB la primera vez * X PCs + 35-100 KB cada día * X PCs	500 KB la primera vez * X PCs + 35-100 KB cada día * X PCs

Tabla 21: Cálculo del consumo de ancho de banda en grupos de PCs por tipo de operación

*46,2 MB para el instalador de 64 bits

24.4. Seguridad de las comunicaciones y de los datos almacenados

El nuevo modelo de protección de **Adaptive Defense 360** requiere obtener información de las acciones realizadas por las aplicaciones instaladas en los equipos del cliente.

La recogida de datos en **Adaptive Defense 360** sigue de forma estricta las directrices generales que se listan a continuación

- Se recoge únicamente información relativa a ficheros ejecutables de Windows, (ficheros .exe, .dll,...) que se ejecutan / cargan en el equipo del usuario. No se recoge ninguna información sobre ficheros de datos.
- Los atributos de los ficheros se envían normalizados retirando la información referente al usuario logueado. Así por ejemplo las rutas de ficheros se normaliza como `LOCALAPPDATA\nombre.exe` en lugar de `c:\Users\NOMBRE_DE_USUARIO\AppData\Local\nombre.exe`)
- Las URLS recogidas son únicamente las de descarga de ficheros ejecutables. No se recogen URLs de navegación de usuarios.
- No existe nunca la relación dato-usuario dentro de los datos recogidos.
- En ningún caso **Adaptive Defense 360** envía información personal a la nube.

Como información imprescindible para soportar el nuevo modelo de protección, **Adaptive Defense 360** envía información sobre las acciones que realizan las aplicaciones ejecutadas en cada equipo del usuario.

Atributo	Dato	Descripción	Ejemplo
Fichero	Hash	Hash del fichero al que hace referencia el evento	N/A
URL	Url	Dirección desde donde se ha descargado un ejecutable	http://www.malware.com/ejecutable.exe
Path	Ruta	Ruta normalizada en la que se encuentra el fichero al que hace referencia el evento	APPDATA\
Registro	Clave/Valor	Clave del registro de Windows y su contenido relacionado	HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\Panda Research\Minerva\Version = 3.2.21
Operación	Id Operación	Identificador de operación realizada en el evento (creación/modificación/carga/.. de ejecutable, descarga de ejecutable, comunicación,)	El evento de tipo 0 indica la ejecución de un ejecutable
Comunicación	Protocolo/Puerto/Dirección	Recoge el evento de comunicación de un proceso (no su contenido) junto con el protocolo y dirección	Malware.exe envía datos por UDP en el puerto 4865

Software	Software Instalado	Recoge la lista de software instalado en el equipo según el API de Windows	Office 2007, Firefox 25, IBM Client Access 1.0

Tabla 22: Información enviada a la nube

25. Apéndice III: Listado de desinstaladores

Si deseas instalar **Adaptive Defense 360** en un equipo en el que ya se encuentra instalada alguna otra solución de seguridad ajena a Panda Security, puedes elegir entre instalarlo sin desinstalar la otra protección, de tal manera que ambas soluciones de seguridad convivan en el mismo equipo o, por el contrario, desinstalar la otra solución de seguridad y funcionar exclusivamente con **Adaptive Defense 360**.

En función del tipo de versión de **Adaptive Defense 360** que desees instalar, el comportamiento por defecto varía.

Versiones Trials

En versiones de evaluación por defecto **Adaptive Defense 360** se instalará en un equipo que ya dispone de otra solución ajena a Panda Security. De esta forma podrás evaluar **Adaptive Defense 360** comprobando cómo registra amenazas avanzadas que pasan inadvertidas para el antivirus tradicional instalado.

Versiones comerciales

En este caso, por defecto **Adaptive Defense 360** no se instalará en un equipo que ya dispone de otra solución ajena a Panda Security. Si **Adaptive Defense 360** dispone del desinstalador de dicho producto, lo desinstalará y a continuación se lanzará la instalación de **Adaptive Defense 360**

360. En caso contrario, se detendrá la instalación.

Este comportamiento por defecto es configurable tanto en versiones trials como en versiones comerciales desde la ventana de Configuración / (pulsar sobre el perfil a editar) / Windows y Linux / Opciones Avanzadas.

Adaptive Defense 360 es capaz de desinstalar automáticamente los productos que aparecen en la siguiente tabla:

Fabricante	Nombre del producto
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32bit- Edition) AVG Internet Security 2013 (64bit- Edition) AVG AntiVirus Business Edition 2013 (32bit- Edition) AVG AntiVirus Business Edition 2013 (64bit- Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011

Fabricante	Nombre del producto
	AVG Internet Security Business Edition 2011 32bits* AVG Internet Security Business Edition 2011 64bits (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVGFree v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir PersonalEdition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x
CA	CA Total Defense for Business Client V14 (32bit- Edition) CA Total Defense for Business Client V14 (64bit- Edition) CA Total Defense R12 Client (32bit- Edition) CA Total Defense R12 Client (64bit- Edition)
Bitdefender	BitDefender Endpoint Protection 6.x BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32 bits) Check Point Endpoint Security 8.x (64 bits)
Eset	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32 bits) ESET NOD32 Antivirus 4.X (32 bits) ESET NOD32 Antivirus 4.X (64 bits) ESET NOD32 Antivirus 5 (32 bits) ESET NOD32 Antivirus 5 (64 bits) ESET NOD32 Antivirus 6 (32 bits) ESET NOD32 Antivirus 6 (64 bits) ESET NOD32 Antivirus 7 (32 bits) ESET NOD32 Antivirus 7 (64 bits)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
iSheriff	iSheriff Endpoint Security 5.x
Kaspersky	Kaspersky Endpoint Security 10 for Windows (32bit- Edition) Kaspersky Endpoint Security 10 for Windows (64bit- Edition) Kaspersky Endpoint Security 8 for Windows (32bit- Edition)

Fabricante	Nombre del producto
	Kaspersky Endpoint Security 8 for Windows (64bit- Edition) Kaspersky Anti-Virus 2010 9.0.0.459* Kaspersky® Business Space Security Kaspersky® Work Space Security Kaspersky Internet Security 8.0, 7.0, 6.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee LiveSafe 2016 x86 / x64 McAfee SaaS Endpoint Protection 6.x, 5.X McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0 McAfee Internet Security Suite 2007 McAfee Total Protection Service 4.7* McAfee Total Protection 2008
Norman	Norman Security Suite 10.x (32bit- Edition) Norman Security Suite 10.x (64bit- Edition) Norman Security Suite 9.x (32bit- Edition) Norman Security Suite 9.x (64bit- Edition) Norman Endpoint Protection 8.x/9.x Norman Virus Control v5.99
Norton	Norton Antivirus Internet Security 2008* Norton Antivirus Internet Security 2007 Norton Antivirus Internet Security 2006
Microsoft	Microsoft Security Essentials 1.x Microsoft Forefront EndPoint Protection 2010 Microsoft Security Essentials 4.x Microsoft Security Essentials 2.0 Microsoft Live OneCare Microsoft Live OneCare 2.5*
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205
PC Tools	Spyware Doctor with AntiVirus 9.x
Sophos	Sophos Anti-virus 9.5 Sophos Endpoint Security and Control 10.2 Sophos Endpoint Security and Control 9.5 Sophos Anti-virus 7.6 Sophos Anti-virus SBE 2.5* Sophos Security Suite
Symantec	Symantect.cloud - Endpoint Protection.cloud 22.x Symantec.cloud - Endpoint Protection.cloud 21.x (32bits) Symantec.cloud - Endpoint Protection.cloud 21.x (64bits) Symantec EndPoint Protection 12.x (32bits) Symantec EndPoint Protection 12.x (64bits) Symantec EndPoint Protection 11.x (32bits) Symantec EndPoint Protection 11.x (64bits) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
Trend Micro	Trend Micro Worry-Free Business Security 8.x (32bit- Edition) Trend Micro Worry-Free Business Security 8.x (64bit- Edition) Trend Micro Worry-Free Business Security 7.x (32bit- Edition) Trend Micro Worry-Free Business Security 7.x (64bit- Edition) Trend Micro Worry-Free Business Security 6.x (32bit- Edition) Trend Micro Worry-Free Business Security 6.x (64bit- Edition)

Fabricante	Nombre del producto
	Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x Trend Micro OfficeScan 11.x
Comodo AntiVirus	Comodo Antivirus V 4.1 32bits
Panda Security	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX y anteriores
	Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX y anteriores
	Panda Global Protection 2017* Panda Internet Security 2017* Panda Antivirus Pro 2017* Panda Gold Protection 2017*
	Panda Global Protection 2016* Panda Internet Security 2016* Panda Antivirus Pro 2016* Panda Gold Protection 2016*
	Panda Global Protection 2015* Panda Internet Security 2015* Panda Antivirus Pro 2015* Panda Gold Protection* Panda Free Antivirus
	Panda Global Protection 2014* Panda Internet Security 2014* Panda Antivirus Pro 2014* Panda Gold Protection*
	Panda Global Protection 2013* Panda Internet Security 2013* Panda Antivirus Pro 2013*
	Panda Global Protection 2012* Panda Internet Security 2012* Panda Antivirus Pro 2012*
	Panda Global Protection 2011* Panda Internet Security 2011* Panda Antivirus Pro 2011* Panda Antivirus for Netbooks (2011)*
	Panda Global Protection 2010 Panda Internet Security 2010 Panda Antivirus Pro 2010 Panda Antivirus for Netbooks

Fabricante	Nombre del producto
	Panda Global Protection 2009 Panda Internet Security 2009 Panda Antivirus Pro 2009
	Panda Internet Security 2008 Panda Antivirus+Firewall 2008 Panda Antivirus 2008
	Panda Internet Security 2007 Panda Antivirus + Firewall 2007 Panda Antivirus 2007

* Productos Panda 2017, 2016, 2015, 2014, 2013, 2012 necesitan un reinicio para completar la desinstalación.

* Comodo AntiVirus V 4.1 32 bits - En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción Permitir.

* F-Secure PSB for Workstations 9.00* - Durante el proceso de instalación del agente de **Adaptive Defense 360** en Windows 7 y Windows Vista, el usuario debe intervenir seleccionando la opción Permitir.

AVG Internet Security Business Edition 2011 32bits - Durante el proceso de instalación del agente de **Adaptive Defense 360**, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

** AVG Internet Security Business Edition 2011 64bits (10.0.1375) - Durante el proceso de instalación del agente de **Adaptive Defense 360**, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

* Kaspersky Anti-Virus 6.0 for Windows Workstations:

Durante el proceso de instalación del agente de **Adaptive Defense 360** en sistemas operativos de 64 bits el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

Para poder hacer la desinstalación, la protección de Kaspersky no debe tener password.

En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción Permitir.

* F-Secure PSB for Workstations 9.00 - Durante el proceso de instalación del agente de **Adaptive Defense 360**, el usuario debe intervenir seleccionando la opción Permitir en dos ventanas de F-Secure PSB for Workstations 9.00.

* AVG Anti-Virus Network Edition 8.5 - Durante el proceso de instalación del agente de **Adaptive Defense 360** el usuario debe intervenir seleccionando en dos ventanas de AVG Anti-Virus Network Edition 8.5 la opción Permitir.

* Productos Panda Antivirus 2011 - No se desinstalan en Windows Vista x64. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Panda Cloud Antivirus 1.4 Pro y Panda Cloud Antivirus 1.4 Free - En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Trend Micro - PC-Cillin Internet Security 2007 y 2008 no se puede desinstalar automáticamente en Windows Vista x64.

* Trend Micro - PC-Cillin Internet Security 2007 y 2008 no se pueden desinstalar automáticamente en Windows Vista x86 teniendo UAC activado.

* ESET NOD32 Antivirus 3.0.XX (2008) no se desinstala automáticamente en plataformas de 64 bits.

* ESET Smart Security 3.0 no se desinstala automáticamente en plataformas de 64 bits.

* ESET NOD32 Antivirus 2.7 tras la instalación del agente de **Adaptive Defense 360** el equipo se reiniciará automáticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* ESET NOD32 Antivirus 2.70.39 tras la instalación del agente de **Adaptive Defense 360** el equipo se reiniciará automáticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* Sophos Anti-virus SBE 2.5 no se desinstala correctamente en Windows 2008.

* eTrust Antivirus 7.1 no se desinstala en sistemas operativos de 64bits (Windows 2003 64bits y Windows XP 64bits).

* Norton Antivirus Internet Security 2008 no se puede desinstalar en Windows Vista con UAC activado.

* Kaspersky Anti-Virus 2010 9.0.0.459. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Kaspersky Anti-Virus 8. En Windows Vista con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* BitDefender Free Edition 2009 12.0.12.0. En Windows Vista con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* McAfee Total Protection Service 4.7. El desinstalador no funciona en sistemas con UAC activado. Además, en sistemas de 32 bits es necesaria la intervención del usuario.

* Microsoft Live OneCare 2.5. No desinstala en Windows Small Business Server 2008.

En caso de tener instalado un programa que no se encuentra incluido en el listado,

consulte con el proveedor correspondiente cómo desinstalarlo antes de instalar la protección de **Adaptive Defense 360**.

26. Apéndice IV: Conceptos clave

Acceso remoto

Tecnología que permite visualizar e interactuar con el escritorio de un dispositivo conectado a la red de forma remota.

Adaptador de red

El adaptador de red permite la comunicación entre los diferentes aparatos conectados entre sí y también permite compartir recursos entre dos o más equipos. Tienen un número de identificación único.

Adware

Programa que, una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente

El agente se encarga de las comunicaciones entre los equipos administrados y los servidores de **Adaptive Defense 360**, además de la gestión de los procesos locales.

Alerta

Mensaje relativo a la Actividad de protección de **Adaptive Defense 360** susceptible de requerir interacción. El administrador de la red recibe alertas mediante correo electrónico y el usuario las recibe mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

Análisis forense

Conjunto de técnicas y procesos ejecutados por el administrador de la red con herramientas especializadas que le permiten seguir la pista de un programa malicioso y determinar las consecuencias una vez el malware ha conseguido infectar un equipo de la red.

Análisis heurístico

El análisis heurístico analiza el software en base a cientos de características de cada archivo.

Así se determina el potencial que el software detectado tiene para llevar a cabo acciones maliciosas o dañinas cuando se ejecuta en un ordenador, y ello permite su clasificación como virus, spyware, troyano, gusano, etc.

Antivirus

Programas cuya función es detectar y eliminar virus informáticos y otras amenazas.

APT (Advanced Persistent Threat)

Conjunto de procesos dirigidos por hackers y orientados a infectar la red del cliente utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus

tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc).

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer. Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos. De esta forma, se dificulta la utilización ilegítima de llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

Archivo de identificadores

Es el fichero que permite a los antivirus detectar las amenazas. También es conocido con el nombre de fichero de firmas.

ARP (address Resolution Protocol)

Protocolo utilizado para resolver direcciones del nivel de red a direcciones del nivel de enlace. En redes IP traduce las direcciones IP a direcciones físicas MAC

Audit

Modo de configuración de **Adaptive Defense 360** que permite visualizar la actividad de los procesos ejecutados en los equipos protegidos de la red sin desencadenar ninguna acción de resolución (desinfección o bloqueo).

Avisos

También llamados Incidencias, es la forma de representar en la consola Web la actividad de los programas maliciosos detectados por la protección avanzada de **Adaptive Defense 360**.

Bloquear

Impedir la ejecución de los programas clasificados como malware o sin clasificar, dependiendo de la configuración de **Adaptive Defense 360** establecida por el administrador de la red.

Broadcast

Transmisión de paquetes en redes de datos por el método de difusión. Un mismo paquete de datos llegará a todos los equipos dentro de la misma subred. Los paquetes de broadcast no atraviesan encaminadores y utilizan un direccionamiento distinto para diferenciarlos de los paquetes unicast.

Ciclo de protección adaptativa

Nuevo enfoque de seguridad basado en la integración de un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos centralizados en una única consola de administración accesible desde cualquier lugar y en cualquier momento.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como malware y posterior desinfección.

Consola Web

Herramienta para configurar la protección, distribuir el agente a todos los equipos de la red y gestionarla. Desde la consola se puede conocer en todo el momento el estado de la protección instalada en su parque informático y extraer e imprimir los informes que sean necesarios.

Cuarentena

Repositorio de almacenamiento de contenidos sospechosos de ser maliciosos o no desinfectables, así como de spyware y herramientas de hacking detectadas.

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

Dialer

Se trata de un programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica a la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada interfaz de red tiene su propia identificación MAC determinada.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio ordenado y distribuido para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio o Directorio Activo.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

Equipos excluidos

Son aquellos equipos seleccionados por el usuario a los que no se les aplicará la protección. En calidad de excluidos, la consola Web no muestra ninguna información ni alerta sobre ellos. Tenga en cuenta que la exclusión puede deshacerse en cualquier momento.

Equipos sin licencia

Son aquellos equipos cuya licencia ha caducado o en los que ha superado el número máximo permitido de instalaciones de la protección. Estos equipos abandonan la lista de equipos sin licencia en el momento en que el usuario adquiere nuevas licencias.

Examinador principal

Rol del equipo dentro de una red Windows que mantiene un listado de todos los dispositivos conectados a su segmento de red.

Exploit

Fallo de software conocido y aprovechado por el malware, que provoca una cadena de errores controlada en provecho del propio malware que lo inicia.

Firewall

También conocido como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes como, por ejemplo, Internet.

Filtrado de URL por categoría

Control de las URLs solicitadas por los navegadores de la red con el objetivo de denegar o permitir su acceso, tomando como referencia una base de datos de URLs dividida en categorías o temas.

Fragmentación

En redes de transmisión de datos, cuando la MTU del protocolo subyacente es menor que el tamaño del paquete a transmitir, los encaminadores dividen el paquete en piezas más pequeñas (fragmentos) que se encaminan de forma independiente y se ensamblan en el destino en el orden apropiado.

Funcionalidad Peer To Peer (P2P)

La red Peer to Peer (P2P) es una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Es una forma legal de compartir archivos de forma similar a como se hace en el correo electrónico o mensajería instantánea, sólo que de una forma más eficiente.

En el caso de **Adaptive Defense 360**, la funcionalidad Peer To Peer reduce además el consumo de ancho de banda de la conexión a Internet, dando prioridad a que los equipos que ya han actualizado un archivo desde Internet lo compartan con otros que también necesitan actualizarlo. Así se evitan los accesos masivos a Internet y los consiguientes colapsos.

Funcionalidad Proxy

Esta funcionalidad permite el funcionamiento de **Adaptive Defense 360** en equipos sin acceso a Internet, realizándose los accesos a través de otro agente instalado en una máquina de su misma subred.

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grupo

En **Adaptive Defense 360**, un grupo es un conjunto de equipos informáticos a los que se aplica el mismo perfil de configuración de la protección. En **Adaptive Defense 360** existe un grupo inicial o grupo por defecto -Default- en el que se pueden incluir todos los ordenadores a proteger. También se pueden crear grupos nuevos.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

Hardening

Modo de configuración de **Adaptive Defense 360** que bloquea los programas desconocidos descargados de Internet, así como todos los ficheros clasificados como malware

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente.

Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido es un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso malicioso para ejecutar el ataque.

Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herramienta de distribución

Una vez descargada de Internet al PC administrador e instalada en éste, la herramienta de distribución permite instalar y desinstalar a distancia las protecciones en los equipos seleccionados. En **Adaptive Defense 360**, la herramienta de distribución solo se puede utilizar para desplegar la protección en equipos con sistema operativo Windows.

Herramienta de hacking

Programa que puede ser utilizado por un hacker para causar perjuicios a los usuarios de un ordenador (pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.).

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

ICMP (Internet Control Message Protocol)

Protocolo de control y notificación de errores utilizado por el protocolo IP en Internet.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

Joke

No es un virus, sino bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus.

Malware

Es un término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware tiene como objetivo infiltrarse en dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas.

Notificaciones

Avisos al administrador relativos a condiciones importantes de la plataforma **Adaptive Defense 360** tales como nuevas versiones del software, licencias a punto de caducar etc

Lock

Modo de configuración de **Adaptive Defense 360** que bloquea los programas desconocidos y clasificados como malware

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para crear programas capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

Malware freezer

Comportamiento de la cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la cuarentena,

evitando su borrado en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

MTU (Maximun transmission unit)

Tamaño máximo del paquete que el protocolo subyacente puede transportar.

Nube

La computación en la nube (Cloud Computing) es una tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios

Partner

Empresa que ofrece productos y servicios de Panda Security

Payload

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, metadatos, información de control y otros datos que son enviados para facilitar la entrega del mensaje.

En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil

Un perfil es una configuración específica de la protección. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que forman parte de dicho grupo o grupos.

Phishing

Intento de conseguir información confidencial de un usuario de forma fraudulenta. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.

Proceso local

Los procesos locales son los encargados de realizar tareas necesarias para la correcta implantación y administración de la protección en los equipos.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo del usuario.

Programas potencialmente no deseados

Son programas que se instalan en el equipo aprovechando la instalación de otro programa que es el que realmente se desea instalar.

Al finalizar la instalación del programa se muestran mensajes al usuario para que acepte la instalación de otros "programas" (PUPs) que aparentemente "forman parte" del que se quiere instalar y se presentan como necesarios para una correcta instalación. Al aceptar, se abre la puerta del equipo del usuario a estos programas potencialmente no deseados.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Un servidor proxy actúa como un intermediario entre una red interna (por ejemplo, una intranet) y una conexión externa a Internet. De esta forma, se puede compartir una conexión para recibir ficheros desde servidores Web.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

Red de confianza

Este tipo de red generalmente es de oficina o casera. El equipo es perfectamente visible para el resto de equipos de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

Red pública

Una red de este tipo es propia de cyberlocales, aeropuertos, etc. Conlleva limitación de su nivel de visibilidad y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

RIR (Regional Internet Registry)

Organización que supervisa la asignación y el registro de direcciones IP y de sistemas autónomos (AS, Autonomous System) dentro de una región particular del mundo.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los propios normalmente). Este tipo de software no es malicioso en sí mismo, pero es utilizado por los piratas informáticos para esconder evidencias y utilidades en los sistemas previamente comprometidos. Existen ejemplares de malware que emplean rootkits con la finalidad de ocultar su presencia en el sistema en el que se instalan.

ROP

ROP es una técnica de ejecución de exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR.

Los ataques tradicionales basados en desbordamiento de pila consistían en sobrescribir regiones de memoria enviando bloques de datos a la entrada de programas que no controlaban debidamente el tamaño de los datos recibidos. Estos ataques dejaron de funcionar cuando técnicas como DEP fueron implementadas de forma masiva en los sistemas operativos: en esta nueva situación el sistema operativo impide la ejecución del "código desbordado" ya que reside en regiones de

memoria marcadas como de no ejecución (datos). ROP sobrescribe la pila de llamadas (call stack) de un proceso para ejecutar zonas de código del propio proceso, conocidas como "gadgets". Así, el atacante puede "armar" un flujo de ejecución alternativo al del proceso original, formado por partes de código del proceso atacado.

SCL (Spam Confidence Level)

Valor normalizado asignado a un mensaje que refleja la probabilidad de que sea Spam, evaluando características tales como su contenido, cabeceras y otros.

Servidor Exchange

Es un servidor de correo de la compañía Microsoft. El servidor Exchange almacena los correos electrónicos entrantes y/o salientes y gestiona la distribución de los mismos en las bandejas de entrada configuradas para ello. Para conectarse al servidor y descargar el correo electrónico que haya llegado a su bandeja, los usuarios han de tener instalado en su equipo un agente de correo electrónico.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

SIEM (Security Information and Event Management)

Software que ofrece almacenamiento y análisis en tiempo real de las alertas generadas por los dispositivos de red y aplicaciones ejecutadas en el parque informático.

Sospechoso

Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por la protección de **Adaptive Defense 360**, tiene una alta probabilidad de ser considerado malware.

Spam

El término correo basura hace referencia a mensajes no solicitados, habitualmente de tipo publicitario y generalmente enviados en grandes cantidades, que perjudican de alguna o varias maneras al receptor.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

SYN

Bandera (flag) en el campo TOS de los paquetes TCP que los identifican como paquetes de inicio de conexión.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario.

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus sean conscientes de su existencia

Virus

Programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

Adaptive Defense 360