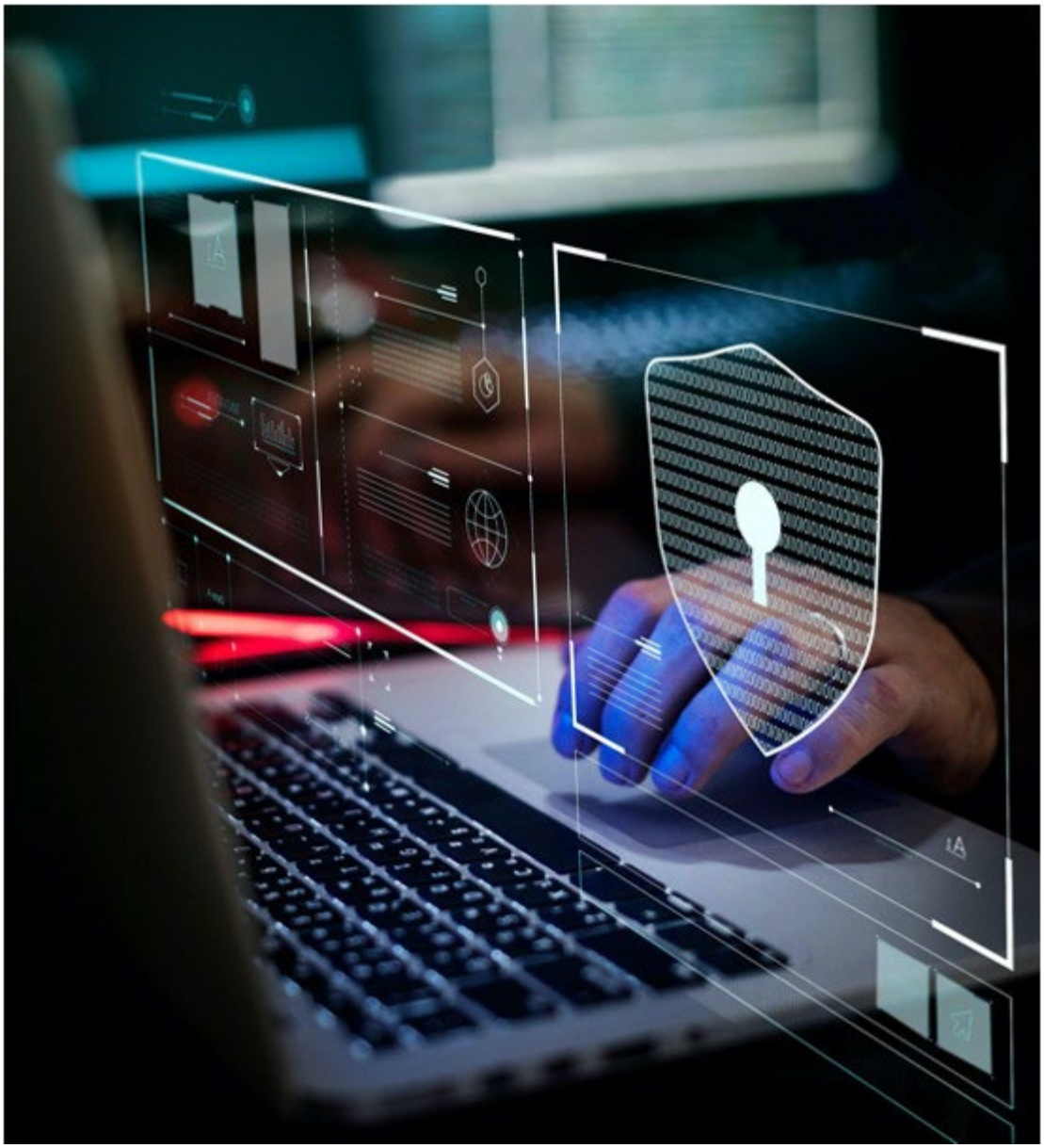


Seguridad de nueva generación de Xerox: En colaboración con Trellix[1]

Informe

[1]Trellix, conocido anteriormente como McAfee Enterprise business

xerox™

Antecedentes

Los equipos multifunción (MFP) de hoy en día son sistemas integrados complejos. Contienen, entre otras cosas, sistemas operativos a gran escala, servidores web integrados, compatibilidad con múltiples pilas de protocolos, interfaces de hardware y software externos e interfaces de programación de aplicaciones (API) para interactuar con los sistemas empresariales. Debido a la gran capacidad y potencia de estos dispositivos multifunción, pueden representar un grave riesgo para su red y sus sistemas corporativos si no están debidamente protegidos.

Los fabricantes de equipos multifunción han aumentado significativamente sus esfuerzos de ingeniería para ajustar los controles de seguridad de estos dispositivos introduciendo mejoras de protección, entre las que se incluyen:

- Cifrado de disco y sobrescritura de disco para proteger los datos del usuario final
- Habilitación de protocolos cifrados como Seguridad del nivel de transporte (TLS), Seguridad de protocolo de Internet (IPsec) y Protocolo simple de gestión de red versión 3 (SNMPv3) para proteger los datos transmitidos desde y hacia el dispositivo
- Autenticación de usuario para la mayoría de las tareas
- Control de acceso mediante la adición de cortafuegos y roles basados en grupos de Directorio activo (AD)
- Registros de auditoría para su seguimiento
- Programas de evaluación de seguridad como la Certificación de criterios comunes

¿Son los equipos multifunción sistemas integrados o abiertos? ¿Necesitan estos dispositivos un nivel adicional de seguridad? En ese caso, ¿cuál es la solución adecuada para proteger los servidores, los equipos de sobremesa y las redes frente a las amenazas actuales y futuras? Esta es una pregunta que los expertos de las comunidades de seguridad intentan responder constantemente.

Sabemos que las tecnologías de seguridad tradicionales, como los antivirus, tienen una eficacia limitada contra las amenazas actuales, como las amenazas persistentes avanzadas (APT) y las redes de bots.

La realidad es que, a pesar de la protección adicional que han añadido los proveedores de equipos multifunción, los incidentes de seguridad siguen produciéndose. El tema común entre estos incidentes de seguridad es que los clientes solo se dan cuenta después de que se produce la infracción. Entonces, el proveedor y el cliente no consiguen evitar daños, proponer soluciones e implementar una solución. Es el equivalente a evaluar los restos y realizar la reparación después de que hayan asaltado la cámara acorazada del banco y robado el dinero.

[1]Trellix, conocido anteriormente como McAfee Enterprise business

DISPOSITIVOS INTEGRADOS

Un sistema integrado es un sistema informático diseñado para funciones determinadas. Los sistemas integrados abarcan todos los aspectos de la vida moderna: cajeros automáticos, dispositivos médicos, impresoras, dispositivos de puntos de venta, quioscos, etc.

Sin embargo, los equipos multifunción actuales realizan algo más que una única función concreta: son un híbrido entre una función concreta y un servidor informático en red. Ambos tienen discos duros, sistemas operativos, servidores web, múltiples conexiones de entrada y salida e interfaces, y procesan distintos tipos de información. ¿Necesitan estos dispositivos un nivel adicional de seguridad? ¿Cuál es la solución adecuada que puede proteger a los servidores, los equipos de sobremesa y las redes frente a amenazas actuales y futuras? Esta es una pregunta que los expertos de las comunidades de seguridad intentan responder constantemente.

Sabemos que las tecnologías de seguridad tradicionales, como el software antivirus, no son capaces de combatir las amenazas actuales, como las amenazas persistentes avanzadas (APT) y las redes de bots, y cada vez se reconoce más que la tecnología de listas blancas y listas permitidas puede ser la respuesta para combatir estas amenazas.

Empecemos por lo que son las listas blancas/listas permitidas y las listas negras/listas de bloqueo.

LISTAS NEGRAS/LISTAS DE BLOQUEO

Para luchar contra los accesos no autorizados, el uso indebido de la información y los programas maliciosos, los administradores de seguridad informática suelen recurrir a herramientas como programas antivirus, antimalware y supervisión de accesos y contenidos de la red. La mayoría de las herramientas pueden dividirse en dos modelos: listas negras/listas de bloqueo y listas blancas/listas permitidas.

Un antivirus se basa en códigos hash de malware conocido. Una vez aislada una variante particular del virus, su hash se añade a la lista negra/lista de bloqueo, que toma la forma de los archivos .dat que se deben descargar a diario. El problema es que los proveedores de antivirus tardan una media de cuatro días en aislar el virus y publicar una actualización de los archivos .dat. Durante ese tiempo, cualquier ordenador que dependa exclusivamente del antivirus es vulnerable.

La mayor desventaja de este enfoque es que siempre está un paso por detrás de la amenaza. Y lo más importante, las herramientas basadas en listas negras/listas de bloqueo son totalmente ineficaces frente a un evento como un ataque de día cero.

Ataques de día cero

Un ataque de día cero aprovecha las vulnerabilidades de los dispositivos que no cuentan actualmente con una solución. Por lo general, cuando una empresa de software detecta un error o problema con un software después de su lanzamiento, desarrollará y ofrecerá un parche para solucionar el problema. Un ataque de día cero aprovechará ese problema antes de que se haya creado un parche. Al encontrar estas vulnerabilidades antes de que los desarrolladores de software las encuentren, un programador malicioso puede crear un virus o gusano que las explote y dañar el sistema de diversas maneras.

[1]Trellix, conocido anteriormente como McAfee Enterprise business

LISTAS BLANCAS/LISTAS PERMITIDAS

El enfoque de listas blancas/listas permitidas se basa fundamentalmente en la identificación de archivos para un entorno de TI y permite que solo estos archivos se ejecuten en el sistema. Básicamente, es permitir solo lo que se sabe que es bueno y detener todo lo que es desconocido. La política prefijada es denegar la ejecución a menos que se haya añadido explícitamente un programa de software a la lista blanca/lista permitida. Muchas de las herramientas de supervisión utilizadas en la actualidad están bajo listas blancas/listas permitidas, ya que "solo permiten" que pasen por el sistema los usuarios designados, direcciones de IP específicas o tipos predefinidos de servicios. ¡Con esto, puede tener la seguridad de que una red de bots no puede reclutar sus equipos multifunción para lanzar ataques!

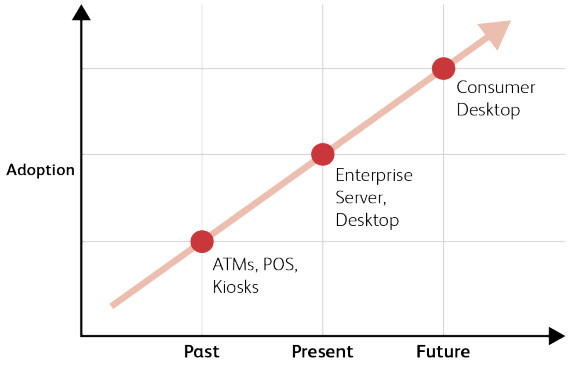
Se sabe que las redes de bots están formadas por miles de ordenadores infectados. Una red de bots es una colección de ordenadores infectados por malware que incluye al ordenador bajo el comando central y el control de un botmaster. A cada ordenador infectado se le denomina "zombie". El malware de la red de bots reside en el ordenador infectado, a menudo sin el conocimiento del propietario del ordenador y sin interferir en su funcionamiento. El botmaster vende los servicios de la red de bots a un cliente con el fin de enviar spam publicitario por correo electrónico o provocar un ataque de denegación de servicio distribuido (DDOS). En un ataque DDOS, todos los zombies intentan acceder simultáneamente a un sitio web concreto, saturándolo de tráfico y provocando su caída. Piense en términos de "Anonymous" atacando a un sitio web gubernamental o de un medio de comunicación que no les guste. El software Control integrado de Trellix[1] de los dispositivos Xerox® impedirá que el malware infeccioso llegue a introducirse en el dispositivo, protegiéndolo así de ser asimilado por la red de bots.

Piense en la diferencia entre listas blancas/listas permitidas en un ordenador de sobremesa frente a un sistema integrado. En un ordenador de propósito general, el usuario puede cargar cualquier software arbitrario, lo que puede ser totalmente legítimo. A continuación, el software de listas blancas del escritorio debe preguntar al usuario si debería permitirse el nuevo software. Esto contrasta con un sistema integrado, en el que el desarrollador de software sabe exactamente qué debe ejecutarse en ese sistema y puede bloquear todo lo demás.

Utilizando una lista blanca/lista permitida, definimos lo que debería y no debería suceder. El caos comienza cuando es posible algo que no debería ocurrir, como que una aplicación Adobe® Flash® Player acceda a un sistema central. Con la tecnología de listas blancas/listas permitidas, puede impedir que una aplicación autorizada de otro modo acceda a archivos principales a los que no debería tener derechos.

Adopción de listas blancas/listas permitidas

Es un hecho ampliamente reconocido que la tecnología de listas blancas/listas permitidas es una forma eficaz de frustrar las amenazas de día cero.



¿CÓMO PUEDE AYUDARLE XEROX?

Entonces, ¿cuál es el paso siguiente en la evolución de la seguridad para mitigar los ataques a su red a través de los equipos multifunción? Xerox siempre ha sido líder del mercado en lo referente a la seguridad de sus impresoras y equipos multifunción.

En consonancia con nuestro continuo énfasis en la seguridad, Xerox se ha asociado con Trellix[1] para ir un paso por delante de las crecientes amenazas a los sistemas integrados. Juntos, hemos incorporado la supervisión automática y la autoprotección que cada unidad individual necesita para protegerse contra ataques malintencionados. Además, el Trellix[1] Agent que se ejecuta en el dispositivo es capaz de comunicarse directamente con la consola central de gestión de seguridad (Trellix[1] ePolicy Orchestrator) para permitir que las impresoras y los equipos multifunción se gestionen de la misma forma en que los clientes gestionan sus ordenadores de sobremesa.

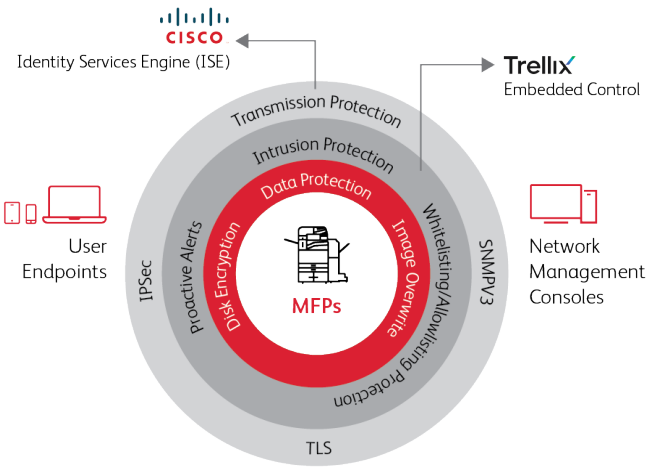
Los eventos de seguridad de Trellix[1] generados en cualquier equipo multifunción aprovisionado se comunican con Trellix[1] ePolicy Orchestrator configurado. Esto ayuda a simplificar la supervisión de todos los MFP aprovisionados desde Trellix[1] ePolicy Orchestrator.

Echemos un vistazo a lo que Trellix[1] está introduciendo para garantizar la mejor seguridad posible para los equipos multifunción Xerox®.

[1]Trellix, conocido anteriormente como McAfee Enterprise business

TECNOLOGÍA DE CONTROL INTEGRADO DE TRELLIX[1]

Con la tecnología de Control integrado de Trellix[1] en los dispositivos Xerox®, los clientes de todos los tamaños, desde pequeñas y medianas empresas (PYMES) con recursos informáticos limitados hasta empresas globales, pueden estar tranquilos sabiendo que sus equipos multifunción están seguros desde el primer momento.



El Control integrado de Trellix[1] utiliza la tecnología de listas blancas/listas permitidas para proteger sus dispositivos Xerox® de los ataques. Esto bloquea los sistemas críticos y previene eventos de cambios no autorizados para que solo se puedan ejecutar los programas de la lista blanca/lista permitida creada por Xerox. Otros programas, como .exe, .ppt y script, se consideran no autorizados. Se impiden los intentos de escribir en un archivo de solo lectura, o de leer desde un archivo o directorio de solo escritura, y se crea y registra un evento en el registro de auditoría del dispositivo. Si se configura SIEM (de forma nativa en AltaLink® Serie 8100, o a través del Administrador de dispositivos Xerox® para VersaLink®), todos los eventos del registro de auditoría se reenvían a un servidor SIEM para su registro y análisis. Además, si se configuran alertas por correo electrónico en el dispositivo Xerox®, se envía un correo electrónico a la dirección designada con los detalles del evento.

El concepto de listas blancas/listas permitidas es sencillo: Xerox predefine una lista limitada de aplicaciones de confianza, y solo esas aplicaciones pueden ejecutarse. Es una solución ideal para dispositivos integrados de función fija. La misma tecnología se implementa en los cajeros automáticos.

Las funciones típicas, como la impresión, la copia, el escaneado y el fax, forman parte de una lista blanca/lista permitida de la aplicación de confianza. Además, las tareas administrativas, como las actualizaciones de firmware, las actualizaciones de software, la carga de formularios y fuentes, los cambios de atributos de configuración y los diagnósticos de los técnicos de Xerox, se incluyen como operaciones de confianza.

La intención del software Trellix[1] es evitar ataques que intenten corromper el software existente del dispositivo o instalar malware no autorizado. En el lenguaje de seguridad, se denominarían ataques de "inyección de código" o "ejecución de código remoto". A diferencia de lo que ocurre con otros programas informáticos que realizan escaneados periódicos para validar la integridad del conjunto de archivos del sistema operativo, cada intento de lectura, escritura y ejecución se comprueba en tiempo real. Además, el software Control integrado de Trellix[1] funciona "por debajo" del sistema operativo para que se detecte cualquier cosa, por ejemplo, un kit que ataca al sistema raíz (root kit), que intente iniciar una infección a ese nivel.

Ventajas que puede esperar en lo referente a la defensa ante amenazas:

- Eliminación de parches urgentes
- Reducción del número y la frecuencia de los ciclos de parches
- Disminución del riesgo de seguridad de día cero derivado de ataques polimórficos mediante malware, como gusanos, virus, troyanos e inyecciones de código, como desbordamiento de búfer, desbordamiento de heap (memoria dinámica) y desbordamiento de pila
- Confianza en la integridad de los archivos autorizados, garantizando que el sistema se encuentra en un estado conocido y verificado
- Reducción del coste de las operaciones relacionadas con los tiempos de inactividad no planificados para recuperación
- Aumento de la disponibilidad del sistema

El Control integrado de Trellix[1] detecta los cambios en tiempo real. Entre ellos se incluyen intentos de cambio de estado del sistema, incluido el código, la configuración y el registro. Todos los eventos de cambio se registran a medida que se producen y se envían al controlador del sistema.

SEGURIDAD MEJORADA DE TRELLIX[1]

La Seguridad mejorada de Trellix[1], de serie en equipos multifunción nuevos, está instalada y activada de forma predeterminada. Previene ataques generales como la lectura/escritura no autorizada de archivos y directorios protegidos y los agrega a directorios protegidos designados. Mantiene la integridad de la impresora multifunción ya que permite que solamente se ejecute el código autorizado y se efectúen los cambios autorizados. Con el sistema en funcionamiento, si se intenta cambiar las aplicaciones del sistema que operan el dispositivo, se avisa al administrador por correo electrónico. Además, esos intentos se guardan en los registros de auditoría y, en función de la configuración del cliente, se pueden notificar a través del software Xerox® CentreWare® Web o del Administrador de dispositivos Xerox® y, si está presente en el entorno, Trellix[1] ePolicy Orchestrator® (ePO). Si se configura SIEM (de forma nativa en AltaLink Serie 8100, o a través del Administrador de dispositivos Xerox para VersaLink), todos los eventos del registro de auditoría se reenvían a un servidor SIEM para su registro y análisis.

Xerox proporciona actualizaciones de listas blancas/listas permitidas, pero solo cuando se actualiza el software integrado. Por diseño, se confía en determinadas funciones del software, incluido el proceso de actualización de software. Se aplica una firma digital al software de Xerox® para garantizar su integridad y autenticidad. Si la firma es válida, el nuevo software se instala con una nueva lista blanca/lista permitida.

Independientemente de su proveedor de seguridad, seguirá beneficiándose de las funciones de seguridad integradas de Xerox y Trellix[1] sin necesidad de software adicional. La función de listas blancas/listas permitidas es independiente de cualquier software externo y está diseñada para funcionar sin interferir con el rendimiento del sistema.

[1]Trellix, conocido anteriormente como McAfee Enterprise business

La Seguridad mejorada de Trellix[1] está diseñada para eliminar los problemas relacionados con el aumento de los riesgos de seguridad asociados con la adopción de sistemas operativos comerciales en los sistemas integrados. Con sus dimensiones reducidas y sus bajos gastos generales, es una solución independiente de la aplicación que proporciona la seguridad sin mantenimiento que usted necesita.

Puede que se pregunte cómo se instala el nuevo software en la máquina, ya que la lista blanca/lista permitida solo permite el software que conoce. Todo el software autorizado está firmado digitalmente por Xerox. El proceso de instalación del software comprueba la firma digital antes de proceder a la instalación y, si la firma es correcta, informa a la Seguridad mejorada de Trellix[1] que el nuevo software se puede instalar con seguridad. Dado que Xerox define el conjunto de software permitido durante el desarrollo, cada conjunto de software lleva su lista blanca/lista permitida. Tras la instalación del software, la Seguridad mejorada de Trellix[1] utiliza la nueva lista blanca/lista permitida para determinar lo que está permitido.

Notificación de alertas de amenazas

Las alertas de amenazas pueden comunicarse de varias maneras dependiendo de su configuración concreta:

- **Registro de auditoría**: generado desde la interfaz de usuario en el equipo multifunción, activado de forma prefijada
- Si se configura SIEM (de forma nativa en AltaLink® Serie 8100, o a través del Administrador de dispositivos Xerox® para VersaLink®), todos los eventos del registro de auditoría se reenvían a un servidor SIEM para su registro y análisis
- **Alerta de correo electrónico desde el dispositivo**: configurado a través de la interfaz de usuario de Servicios de internet de Xerox® CentreWare®
- **Alertas e informes por correo electrónico a través del software Xerox® CentreWare Web y Administrador de dispositivos Xerox®**: se configuran mediante las interfaces de usuario del software Xerox® CentreWare® Web y el Administrador de dispositivos Xerox®
- **Alertas e informes por correo electrónico a través de Trellix[1] ePolicy Orchestrator**: se configuran a través del software de gestión de seguridad Trellix[1] ePolicy Orchestrator disponible en Trellix[1]
- Los eventos de seguridad de Trellix[1] generados en cualquier equipo multifunción aprovisionado se comunican con el ePolicy Orchestrator de Trellix[1] configurado. Esto ayuda a simplificar la supervisión de todos los MFP aprovisionados desde Trellix[1] ePolicy Orchestrator

CONTROL DE INTEGRIDAD DE TRELLIX[1]

El Control de integridad de Trellix[1] es un software comercial opcional que combina las funciones estándar de la Seguridad mejorada con la capacidad de supervisar y evitar ataques dirigidos y la ejecución no autorizada de archivos desde cualquier ubicación a través de sistemas que no son de confianza. Evita también la escritura de archivos ejecutables protegidos que no son parte del software del dispositivo Xerox® estándar. Es el nivel de seguridad superior, la mayor protección de la que puede disfrutar su equipo multifunción Xerox®.

El Control de integridad de Trellix[1] añade una capa de seguridad al impedir que se ejecuten nuevos archivos desde cualquier ubicación que no sea una fuente de confianza. Evita también la escritura de archivos ejecutables protegidos que, a su vez, previene la sobrescritura maliciosa de archivos ejecutables suministrados por Xerox. Detiene cualquier cambio o código no autorizado en el sistema en forma de malware, gusanos, troyanos, ataques de día cero e incluso ataques dirigidos. Solo se permite la ejecución de software aprobado, con lo que se evita un ataque para el que aún no existe una contramedida.

Xerox y Trellix[1] ofrecen una tecnología de listas blancas y listas permitidas que garantiza que solo el código correcto y ejecutable pueda ejecutarse en los sistemas protegidos. Garantiza que sus dispositivos presten solo los servicios que usted desea, al tiempo que impide que un atacante instale código malicioso. Esta tecnología se utiliza para proteger servidores, cajeros automáticos, terminales de puntos de venta y sistemas incorporados como impresoras y dispositivos móviles.

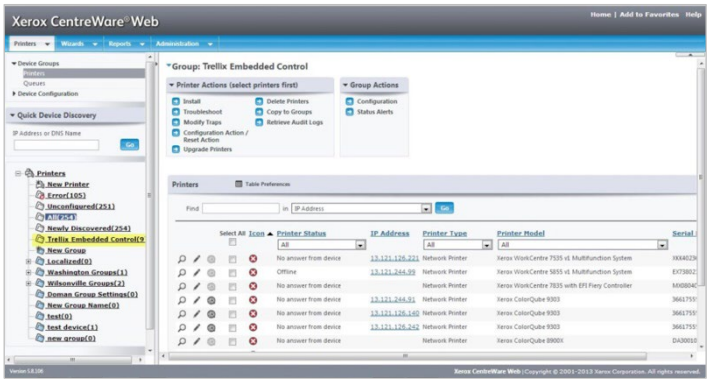
Como se ha mencionado anteriormente, la Seguridad mejorada de Trellix[1] se ofrece como una característica de serie, completamente instalada y habilitada, en ciertos modelos. En el caso del Control de integridad de Trellix[1] opcional, no se requiere ningún procedimiento de instalación para los clientes y la activación se basa en un proceso de clave de licencia.

GESTIÓN DE DISPOSITIVOS CON CONTROL INTEGRADO DE TRELLIX[1]

Existen varias opciones para gestionar los dispositivos con Control integrado de Trellix[1]:

Software Xerox® CentreWare® Web y Administrador de dispositivos Xerox®

El software Xerox® CentreWare® Web es un innovador programa basado en navegador que instala, configura, gestiona, supervisa y genera informes sobre las impresoras y equipos multifunción instalados en red en la empresa, independientemente de la marca. El Administrador de dispositivos Xerox® es una sola herramienta que instala colas de impresión y configura, gestiona, supervisa e informa sobre los equipos locales y conectados en red, de cualquier marca, de toda la empresa. Entre las funciones se incluyen la detección, configuración y gestión de dispositivos, seguimiento y visualización de trabajos, supervisión proactiva, diagnóstico remoto, solución de problemas e informes.



Trellix[1] ePolicy Orchestrator®

Este software permite a los administradores de TI unificar la gestión de la seguridad en puntos finales, redes, datos y soluciones de cumplimiento de Trellix[1] y de terceros.

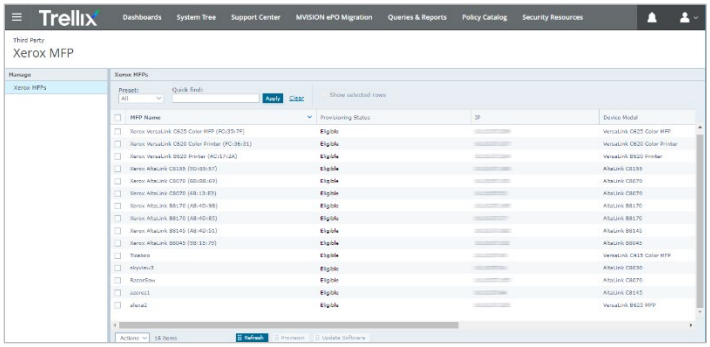
Trellix[1] ePolicy Orchestrator (ePO) es una herramienta de software de gestión de la seguridad que se puede adquirir y que facilita la gestión de los riesgos y el cumplimiento normativo a organizaciones de todos los tamaños. Ofrece a los usuarios paneles de arrastrar y colocar que proporcionan información de seguridad en todos los terminales (datos, dispositivos móviles y redes) para obtener información inmediata y tiempos de respuesta más rápidos. Trellix[1] ePO aprovecha las infraestructuras de TI existentes al conectar la gestión de Trellix[1] y las soluciones de seguridad de terceros al Protocolo ligero de acceso a directorios (LDAP), las operaciones de TI y las herramientas de gestión de la configuración.

[1]Trellix, conocido anteriormente como McAfee Enterprise business

Con visibilidad de extremo a extremo y potentes automatizaciones que reducen significativamente los tiempos de respuesta a incidencias, el software Trellix[1] ePO mejora la protección de los dispositivos integrados y reduce el coste y la complejidad de la gestión del riesgo y la seguridad.

El software Trellix[1] ePO proporciona funciones completas de generación de informes para ejecutar consultas preconfiguradas y consultas personalizadas sobre información de productos gestionados en la red o sobre acciones de los usuarios en su servidor ePO.

Los resultados del informe se pueden mostrar en distintos formatos, como tablas o gráficos circulares, y exportarse para crear informes PDF.

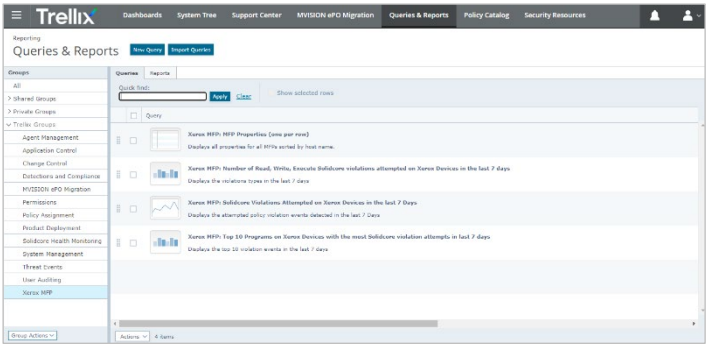


TRELLIX[1] EPOLICY ORCHESTRATOR® Y EXTENSIÓN EPO PARA MFP XEROX®[2]

Trellix[1] ePO se vende directamente a través de Trellix[1] y no forma parte de la instalación de los controles internos. Sin embargo, si actualmente es cliente de Trellix[1], es posible que ya esté utilizando Trellix[1] ePO. En ese caso, puede aprovechar la extensión ePO para equipos multifunción Xerox®, que permite ver los dispositivos de Xerox® elegibles y las provisiones para recibir eventos de seguridad. Vea hasta 60 atributos para una mejor gestión e información más detallada sobre las configuraciones de seguridad.

Además, la extensión ePO para MFP Xerox® proporciona:

- Una respuesta automatizada para que los administradores puedan recibir notificaciones automáticas por correo electrónico
- Una vista de aproximadamente 60 atributos de configuración de seguridad y sus opciones actuales
- Posibilidad de ver si el firmware del dispositivo está actualizado
- Capacidad de cargar firmware de dispositivos en ePO y, a continuación, actualizar uno o más dispositivos Xerox®
- Ver en tiempo real qué puertos de escucha están activos en el dispositivo Xerox®
- Ver puertos de escucha no permitidos
- Ver un evento de seguridad de dispositivos Xerox® en el panel de control proporcionado
- Utilizar las consultas e informes proporcionados por Xerox
- Personalizar consultas o informes para realizar rápidamente comprobaciones de cumplimiento de la seguridad en toda su flota de servicios



[1]Trellix, conocido anteriormente como McAfee Enterprise business
[2]Dispositivos Xerox® AltaLink®, Xerox® WorkCentre® iSeries y Xerox® Serie EC7800/8000

EQUIPOS COMPATIBLES

El Control integrado Trellix[1] está disponible para los dispositivos Xerox® AltaLink®, Xerox® VersaLink® Serie 7100, WorkCentre® iSeries y Serie EC7800 y 8000. En el futuro se añadirán más productos.

RECURSOS ADICIONALES

- Seguridad de datos de Xerox y Trellix[1]
  https://www.xerox.es/es-es/connectkey/mas-informacion/seguridad-trellix
- Preguntas frecuentes sobre Xerox y Trellix[1]
  https://www.xerox.es/oficina/latest/SECFS-14S.pdf
- Xerox, Trellix[1] y Cisco®: Uniendo fuerzas para una respuesta ante amenazas cibernéticas en tiempo real
  https://www.xerox.es/es-es/connectkey/mas-informacion/seguridad-para-impresoras-de-red
- Ficha técnica del Control integrado de Trellix[1]
  https://www.trellix.com/en-us/assets/data-sheets/trellix-embedded-control-datasheet.pdf
- Seguridad para una confianza total
  https://www.xerox.es/es-es/quienes-somos/soluciones-de-seguridad/seguridad-confianza-cero
- Soluciones de seguridad de Xerox
  https://www.xerox.es/es-es/quienes-somos/soluciones-de-seguridad

[1]Trellix, conocido anteriormente como McAfee Enterprise business

AUTORES

- Zia Masoom, Manager de marketing de productos mundial, Xerox
- Doug Tallinger, Manager de planificación de plataformas mundial, Xerox

Para obtener más información sobre los productos Xerox® con el Control integrado de Trellix[1], póngase en contacto con un representante de Xerox o vaya a **www.xerox.es/es-es/connectkey/mas-informacion/seguridad-trellix**.

TSK-3919 03/23 BR38619 SECWP-03SB