Un enfoque integral para la seguridad de las impresoras.

Las impresoras y los equipos multifunción cuentan ahora con prestaciones que les permiten situarse en el núcleo de las operaciones de su empresa. Con el crecimiento exponencial de los dispositivos inalámbricos, el software y los servicios alojados en la nube, las impresoras no solo necesitan funcionar con estas nuevas tecnologías, sino que también deben protegerse de ellas.

Prevenir

Detectar

Proteger

Alianzas externas

PROTECCIÓN INTEGRAL PARA SU IMPRESORA

En Xerox, desde hace mucho tiempo reconocimos y adoptamos el cambio tecnológico y las necesidades cambiantes del lugar de trabajo. Ofrecemos una gama completa de funciones de seguridad para proteger las impresoras y los datos. Además, protegemos toda la cadena de datos, incluidos **la impresión, la copia, el escaneado, el fax, la descarga de archivos** y **el software del sistema**. Nuestra estrategia de varios niveles aborda cuatro aspectos clave.

PREVENIR

La primera y más evidente vulnerabilidad es la interfaz de usuario, así como mantener el control de quién dispone de acceso físico a su impresora y sus funciones. Las medidas de seguridad de Xerox comienzan por la prevención de intrusiones mediante la **Autenticación de usuarios** para garantizar que solo puedan acceder los empleados autorizados. Una vez dentro, el **Control de acceso basado en roles** garantiza que cada miembro del equipo vea únicamente las funciones para las que tenga autorización. La activación de **Contraseñas fuertes y complejas** protege contra los piratas informáticos y el software malintencionado, mientras que la compatibilidad con la **autenticación multifactor**[1] proporciona una capa de seguridad adicional. Además, todas las acciones que realizan los usuarios quedan registradas, lo que ofrece un registro completo de **Auditoría**.

Después, abordamos los puntos de intrusión menos evidentes: qué se envía a la impresora y cómo se envía. Nuestro software del sistema está **firmado digitalmente**: cualquier intento de instalación de versiones infectadas y sin firmar dará lugar a que el archivo se rechace automáticamente. Las claves cifradas se almacenan en los chips del TPM, lo que protege a las impresoras de los ciberataques.

xerox™

DETECTAR

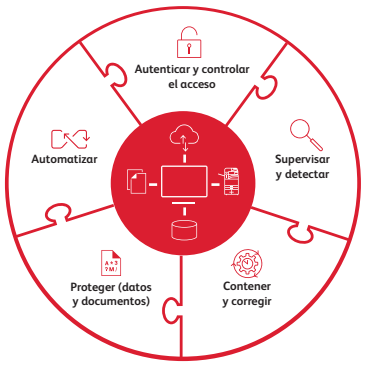
En el caso improbable de que se superen las defensas de la red y los datos, la tecnología Xerox® ConnectKey® ejecuta un **análisis de verificación de firmware** completo, bien al inicio o cuando lo activa un usuario autorizado. Recibirá una alerta si se detectan cambios dañinos en la impresora. Nuestras soluciones integradas más avanzadas utilizan la tecnología de **listas de permitidos de Trellix**[2] que supervisa constantemente el sistema e impide automáticamente la ejecución de software malicioso. La integración con el **Motor de servicios de identidad (ISE) de Cisco®** detecta automáticamente los dispositivos Xerox® en la red y los clasifica como impresoras para la implementación y el cumplimiento de las políticas de seguridad. Los dispositivos Xerox® se integran con las herramientas de software SIEM[3] líderes del mercado para comunicar los datos de eventos de seguridad en tiempo real. Esto facilita la detección temprana de infracciones y elimina o mitiga el daño potencial de amenazas de seguridad a la organización.

PROTEGER

Nuestras soluciones de seguridad integral protegen los documentos impresos y escaneados de su divulgación o modificación no autorizada. La tecnología Xerox® ConnectKey® ayuda a impedir la transferencia deliberada o accidental de datos clave a personas no autorizadas.

Protegemos los documentos impresos utilizando un **código PIN** o un sistema de **liberación mediante tarjetas**. Impedimos que la información escaneada caiga en manos de personas no autorizadas utilizando **formatos de archivos protegidos con contraseña, cifrados y firmados digitalmente**. Las impresoras con tecnología ConnectKey también le permiten **bloquear los campos de correo electrónico "para/cc/cco"** limitando los destinos de escaneado a las **direcciones internas**.

También protegemos toda la información guardada con los niveles más altos de **cifrado**. Eliminamos los datos procesados o almacenados que ya no sean necesarios mediante **algoritmos de limpieza** y **borrado de datos**[4] aprobados por el Instituto Nacional de Normas y Tecnología (NIST) y el Departamento de Defensa de los EE. UU.



XEROX RESPALDA LA CONFIANZA CERO

Con una combinación de hardware, software y procesos, apoyamos el modelo de seguridad de Confianza cero (Zero Trust) para que la implementación sea más sencilla y exhaustiva.

Más información: www.xerox.es/es-es/quienes-somos/soluciones-de-seguridad/seguridad-confianza-cero

ALIANZAS EXTERNAS

Trabajamos con organizaciones que realizan pruebas de conformidad y con líderes del sector de seguridad como **Trellix y Cisco** para adaptar sus estándares y conocimientos a los productos de Xerox.

Para obtener una validación independiente de terceros de nuestros elevados niveles de fiabilidad, los organismos de certificación como **Criterios Comunes (ISO/IEC 15408)** y **FIPS 140-2/140-3** miden nuestro rendimiento en relación con los estándares internacionales. Estos reconocen nuestra estrategia integral para la seguridad de las impresoras.

Nuestro programa de corrección de errores (Bug Bounty)[5] con HackerOne es otra marca de confianza en nuestras medidas de seguridad, además de ser un recurso independiente de validación de la tecnología.

Trellix · cisco · splunk> · LogRhythm · hackerone

SEGURIDAD FÁCIL DE IMPLEMENTAR Y GESTIONAR

Elija entre las plantillas de seguridad predefinidas (Predeterminada, Elevada o Alta) y la impresora configurará automáticamente las opciones de seguridad correspondientes. Supervise hasta 75 opciones de seguridad con el Control de configuración y podrá restablecerlas automáticamente si se detectan cambios no autorizados. Esto ayuda al personal de TI a ahorrar tiempo y elimina las conjeturas a la hora de implementar y cumplir con las políticas de seguridad.

[1] La autenticación multifactor se habilita a través de Xerox® Workplace Solutions y los IdP en la nube

[2] Los dispositivos Xerox® AltaLink®, los equipos multifunción Xerox® VersaLink® C415 color/B415 y C625 color/B625, la impresora Xerox® VersaLink® C620 color/B620, el equipo multifunción Xerox® VersaLink® de la serie 7100 y el equipo multifunción Xerox® de la serie EC7800/8000

[3] Trellix Enterprise Security Manager, LogRhythm y herramientas SIEM Splunk

[4] Solo aplicable a dispositivos con disco duro

[5] La corrección de errores (Bug Bounty) se ofrece a través de HackerOne en los equipos multifunción Xerox® AltaLink®, con la adición de más productos, soluciones y servicios en el futuro

Más información: **www.xerox.es/es-es/quienes-somos/soluciones-de-seguridad**