

Un enfoque integral para la seguridad de las impresoras

Las impresoras y los equipos multifunción tienen ahora la capacidad de trabajar en el centro de sus operaciones comerciales. Con el crecimiento exponencial de los dispositivos inalámbricos, el software y los servicios alojados en la nube, sus impresoras no solo necesitan trabajar con estas nuevas tecnologías, sino que también deben protegerse de ellas.



Prevenir



Detectar



Proteger



Asociaciones externas

PREVENIR

La primera y más obvia vulnerabilidad es la interfaz de usuario, así como mantener el control sobre quiénes tienen acceso físico a su impresora y sus funciones. Las medidas de seguridad de Xerox empiezan con la prevención de intrusiones mediante la **Autenticación de usuarios** para asegurar que solo personal autorizado tenga acceso. Una vez ahí, el **Control de acceso basado en roles** asegura que cada miembro del equipo solo vea las funciones que usted quiera que vea. La habilitación de **Contraseñas fuertes y complejas** protege contra los piratas informáticos y el software malicioso, y la compatibilidad con la **Autenticación de múltiples factores**¹ proporciona un nivel adicional de seguridad. También se registran todas las acciones relacionadas con cada usuario, lo que proporciona un registro completo de **Auditoría**.

Luego, abordamos puntos de intrusión menos obvios: qué se envía a la impresora y la forma en que se envía. Nuestro software del sistema está **Firmado digitalmente**: cualquier intento de instalación de versiones infectadas y sin firmar hará que el archivo se rechace automáticamente. Las claves cifradas se almacenan en los chips del TPM, lo que mantiene a las impresoras protegidas contra ataques cibernéticos.

PROTECCIÓN INTEGRAL PARA SU IMPRESORA

En Xerox, desde hace mucho tiempo reconocimos y aceptamos el cambio en la tecnología y las necesidades cambiantes del lugar de trabajo. Ofrecemos un conjunto integral de funciones de seguridad que mantienen a sus impresoras y datos a salvo. Además, protegemos cada parte de la cadena de datos, incluidos **la impresión, la copia, el escaneado, el fax, la descarga de archivos y el software del sistema**. Son cuatro los aspectos más importantes de nuestro abordaje de varios niveles.



DETECTAR

En el improbable caso de que las defensas de sus datos y su red se vean superadas, la tecnología Xerox® ConnectKey® ejecutará una prueba completa de **Verificación de firmware**, ya sea en el arranque² o cuando la activen los usuarios autorizados. Si se detectan cambios dañinos a la impresora, se dará una alerta. Nuestras soluciones integradas más avanzadas usan la tecnología de **Listas blancas/listas de permisos de Trellix**³, que realiza una supervisión constante y previene automáticamente la ejecución de cualquier software malintencionado. La integración con el **Motor de Servicios de Identidad (ISE) de Cisco**⁴ detecta automáticamente los dispositivos Xerox® en la red y los clasifica como impresoras a fin de lograr la implementación y el cumplimiento de las políticas de seguridad. Los dispositivos Xerox® se integran con las herramientas de software SIEM⁴ líderes del mercado para comunicar los datos de eventos de seguridad en tiempo real. Esto ayuda en la detección anticipada de violaciones y elimina o mitiga el daño potencial de las amenazas de seguridad a la organización.



PROTEGER

Nuestras soluciones de seguridad integral también protegen sus documentos impresos y escaneados contra la divulgación o modificación no autorizada. La tecnología Xerox® ConnectKey® le ayuda a prevenir la transferencia deliberada o accidental de datos importantes a personas sin autorización para verlos.

Podemos proteger la salida de impresión usando un **Código PIN** o un sistema de **Liberación de tarjeta**. Gracias a **formatos de archivos protegidos con clave, cifrados y firmados digitalmente**, podemos evitar que la información escaneada llegue a personas que no deberían recibirla. Las impresoras con tecnología ConnectKey también le permiten **bloquear los campos de correo electrónico "para/cc/cco"**, lo que limita los destinos de escaneado a las **direcciones internas**.

Además, mediante los niveles más altos de **cifrado**, Xerox protege toda la información almacenada. Borrarnos cualquier dato procesado o almacenado que no se necesite mediante el uso de **algoritmos de limpieza de datos** y **sanitización** aprobados por el Instituto Nacional de Estándares y Tecnología (NIST) y el Departamento de Defensa de EE. UU.⁵

ASOCIACIONES EXTERNAS

Trabajamos con organizaciones que realizan pruebas de conformidad y con líderes del sector de seguridad, como **Trellix*** y **Cisco** para adecuarnos a sus estándares globales y conocimientos aplicados a Xerox.

Al compararnos con estándares internacionales, organismos de certificación como **Criterios comunes (ISO/ IEC 15408)** y **FIPS 140-2/140-3** brindan pruebas independientes de que cumplimos con los niveles más altos de rendimiento. Estos organismos reconocen nuestro abordaje integral a la seguridad de las impresoras.

Nuestro programa de corrección de errores (Bug Bounty⁶) con HackerOne es otra marca de confianza en nuestras medidas de seguridad, así como un recurso independiente de validación tecnológica.



¹ MFA se habilita a través de Xerox® Workplace Solutions e IdP en la nube

² Impresoras Xerox® VersaLink®

³ Equipos multifunción Xerox® AltaLink®, Xerox® VersaLink® 7100, Xerox® WorkCentre® i-Series, Xerox® EC7800/8000 y Xerox® WorkCentre® EC7836/EC7856

⁴ Trellix Enterprise Security Manager, LogRhythm y herramientas SIEM Splunk

⁵ Aplica solo a dispositivos con unidad de disco duro

⁶ La corrección de errores (Bug Bounty) se ofrece a través de HackerOne en los equipos multifunción Xerox® AltaLink® Serie 8100, con más productos, soluciones y servicios que se añadirán en el futuro

* Trellix antes conocida como McAfee Enterprise Business

Más información en: www.xerox.com/es-ar/quienes-somos/soluciones-de-seguridad