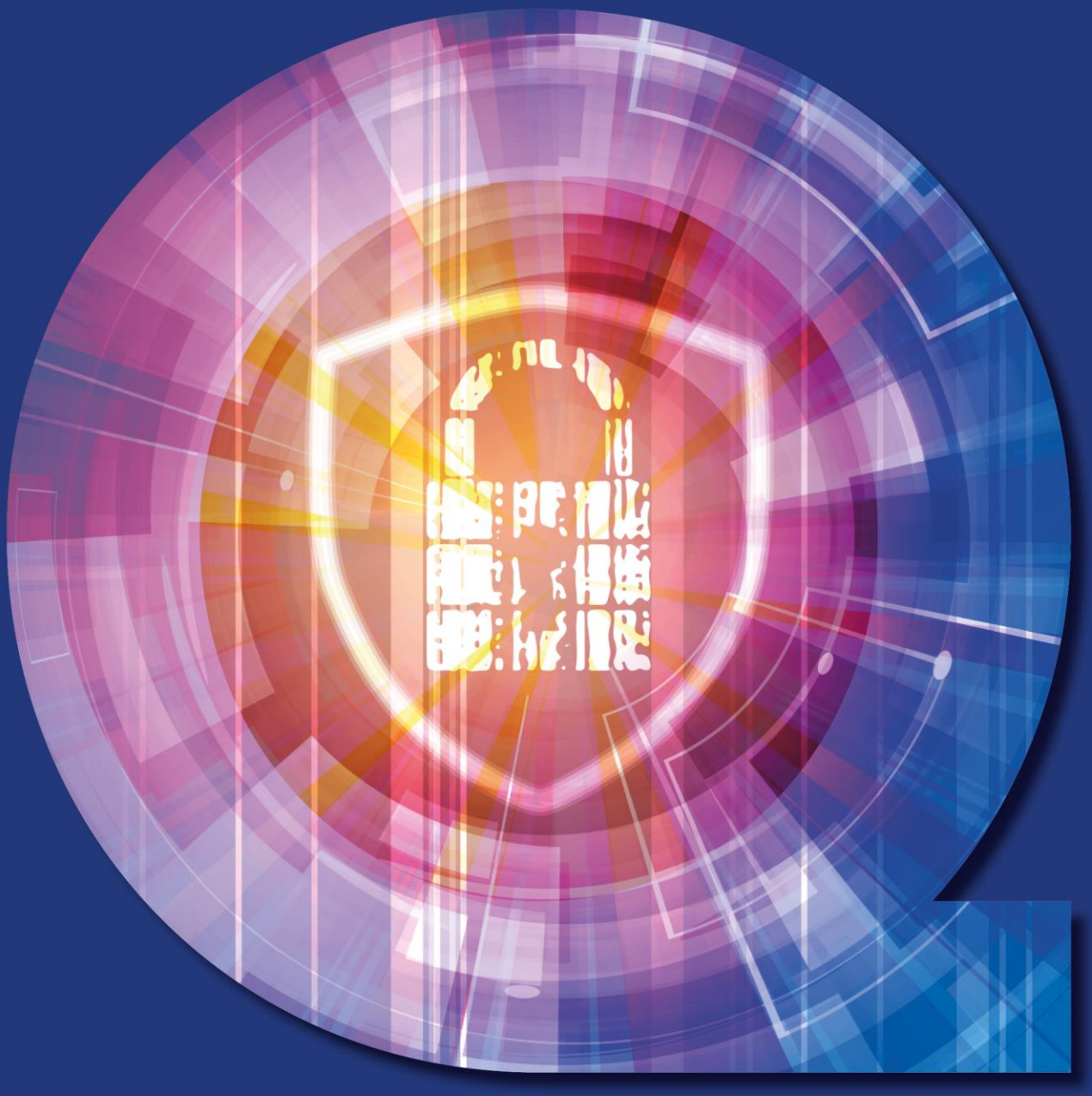
Panorama de seguridad en impresión, 2023

Asegurar la infraestructura de impresión dentro de un panorama con amenazas crecientes



Tendencias de seguridad en impresión en Estados Unidos y Europa
Extracto del informe: Xerox
Mayo de 2023

QUOCIRCA

Resumen ejecutivo

El informe del panorama global de seguridad en impresión de Quocirca 2023 revela que las organizaciones enfrentan continuos desafíos para asegurar la infraestructura de impresión. La impresión en casa sigue generando inquietud sobre la seguridad, y las compras particulares de los empleados dificultan el control de la seguridad de los documentos. Las fugas de datos relacionadas con la impresión siguen presentes. El 61 % de los encuestados reportaron por lo menos un evento de pérdida de datos en los últimos 12 meses, llegando a 67 % en las organizaciones de mercado intermedio. Esto está disminuyendo la confianza en la seguridad de la infraestructura de impresión, en particular entre las pymes.

Es notable que la investigación revela una fuerte desconexión entre las percepciones y actitudes hacia la seguridad en impresión entre los directores de tecnologías de la información (CIO) y los directores de seguridad de la información (CISO). Las expectativas de crecimiento en el gasto por seguridad en los próximos 12 meses es similar, pues el 84 % de los CIO y 81 % de los CISO esperan que sus gastos por seguridad en impresión aumenten. Solo el 28 % de los CISO cree que se ha vuelto más difícil seguir el ritmo de los retos de seguridad en impresión, en comparación con el 50 % de los CIO. De manera similar, solo el 45 % de los CISO están algo o muy preocupados sobre los riesgos de las impresoras sin seguridad, en comparación con el 72 % de los CIO. Este abismo entre los CIO y CISO significa que los dos perfiles responsables de la seguridad técnica en general del ambiente de impresión, al servir a la empresa, no están viendo el problema desde el mismo ángulo y esto tiene un efecto en cadena para la compañía.

Por fortuna, los líderes de seguridad en impresión están mitigando los riesgos. Como muestra el Índice de Madurez sobre Seguridad en Impresión de Quocirca, las organizaciones clasificadas como líderes, que han implementado diversas medidas en políticas y tecnología, enfrentan niveles menores de pérdida de datos y tienen una mayor confianza en la seguridad de su infraestructura de impresión. Para los fabricantes de impresoras, proveedores de servicios gestionados de impresión (MPS) y el resto de los distribuidores de productos de impresión, eliminar esta división entre los dos campos de seguridad es una obligación. Sin embargo, esto no es fácil de lograr. Requerirá de una aproximación desde dos flancos para acercar a ambas partes, además de asegurar que la empresa esté más consciente sobre los problemas de seguridad relativos a la impresión.

Por lo pronto, los fabricantes de impresoras y los distribuidores deben fortalecer sus propuestas sobre seguridad para organizaciones de todos los tamaños y ayudar a los clientes a mitigar el riesgo en esta nueva era de trabajo híbrido. La clave es convertirse en un asesor de confianza y un proveedor de soluciones de seguridad en impresión que se ajusten al ambiente de seguridad existente en una organización. Al asegurar el flujo de información y datos, junto con la seguridad de dispositivos y salidas, se crearán nuevas capacidades de ingresos para los distribuidores.

El estudio del panorama global de seguridad en impresión 2023 se basa en los puntos de vista de 507 responsables de decisiones en TI (ITDM) en los Estados Unidos y Europa. Los porcentajes de encuestados fueron: 20 % del Reino Unido, 20 % de Francia, 20 % de Alemania y 40 % de Estados Unidos. En términos del tamaño de la organización, 24 % fueron pymes (de 250 a 499 empleados), 26 % fueron organizaciones de tamaño intermedio (500 a 999 empleados) y 50 % fueron grandes empresas (más de 1000 empleados). El personal encuestado forma parte de una amplia gama de sectores, incluidos servicios profesionales y de negocios, finanzas, industriales, sector público y ventas al por menor.

El estudio también incluye el panorama del proveedor de seguridad en impresión, donde figura la valoración de Quocirca de las ofertas de servicio de los principales fabricantes de equipo de impresión.

Las siguientes compañías participaron en este estudio: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh y Xerox.

© Quocirca 2023

Hallazgos clave

- **Los incidentes de ciberseguridad continúan al alza.** En general, el 42 % de las organizaciones reportan una brecha en la seguridad de TI en el último año, aumentando a 55 % entre las organizaciones de mercado intermedio y reduciéndose a 36 % entre las empresas grandes, junto con el 51 % del sector financiero, cayendo a 32 % en el sector público. En todas las organizaciones, el mayor problema es el malware, y en las compañías de mercado intermedio, el phishing. Las brechas en la seguridad aumentaron 61 % en las organizaciones el año pasado, elevándose a 70 % en los EE. UU. y 66 % en empresas y servicios profesionales. En promedio, 27 % de los incidentes de seguridad de TI estuvieron relacionados con documentos físicos.
- **La dependencia del material impreso crea la necesidad de una seguridad efectiva en la impresión.** A pesar de la rápida digitalización durante la pandemia, 70 % de las organizaciones dependen de la impresión actualmente, y en grandes organizaciones, esta cifra aumenta a 72 %. La mayoría (80 %) ha cambiado la composición de su equipo de impresión en los últimos dos años, aumentando a 88 % para el mercado intermedio. En general, el 79 % espera aumentar su inversión para seguridad en impresión el próximo año, elevándose a 86 % en los Estados Unidos y a 85 % en servicios profesionales y empresariales y ventas al menudeo.
- **La seguridad en impresión ocupa un lugar más bajo en la lista de preocupaciones en comparación con otros elementos en la infraestructura de TI.** Las plataformas de aplicaciones híbridas o en la nube, correos electrónicos, redes públicas y parámetros tradicionales se perciben como riesgos más importantes para la seguridad. Los empleados con impresoras propias en casa ocupan el séptimo lugar en riesgos para la seguridad (21 %), por arriba del ambiente de impresión de oficina (20 %). Es destacable la disparidad entre los CIO y CISO. Solo el 18 % de los CIO consideran la impresión en oficina como un riesgo clave en comparación con el 30 % de los CISO.
- **Las organizaciones están siguiendo diferentes líneas para gestionar la seguridad de su infraestructura de impresión.** Mientras que el 31 % indican que usan un proveedor de servicios gestionados de impresión (MPS), más de la mitad (54 %) usa un proveedor de servicios gestionados de seguridad (MSSP) para manejar la seguridad tanto de TI como de impresión. Esto se eleva a un 58 % en las organizaciones más pequeñas (de 249 a 499 empleados).
- **Las organizaciones están viendo una dificultad de mantener el ritmo de las demandas de seguridad en impresión.** En general, 39 % comentan que se está volviendo más difícil, elevándose a 50 % en el mercado intermedio (de 500 a 999 empleados). El mayor reto es conservar la gestión de impresión actualizada (35 %), evitar que se impriman documentos confidenciales y privados (34 %) y asegurar la impresión en hogares y ambientes remotos (31 %). La seguridad del hardware es una preocupación vital para las pymes (29 %) y la más alta para los sectores financiero e industrial (31 %) y para los CISO encuestados (38 %).
- **Las organizaciones que usan MPS o que están clasificadas como líderes en seguridad en impresión tienen más confianza en la seguridad de su infraestructura de impresión.** La visibilidad y control que proporcionan los MPS parecen reducir en los usuarios la carga que representa la seguridad. Mientras que, en general, solo 19 % de los encuestados tienen confianza plena en la seguridad de su infraestructura de impresión, esto se eleva a 26 % en las organizaciones que usan MPS. En total, un 50 % adicional menciona que tienen mayor confianza. Esto refleja la creciente complejidad y los retos asociados con el aseguramiento de dispositivos y documentos en un lugar de trabajo híbrido.
- **En los últimos 12 meses, 61 % de las organizaciones han experimentado pérdida de datos debido a prácticas de impresión inseguras.** Esta es una caída a partir del 68 % de nuestro estudio de 2022. Las organizaciones de mercado intermedio son más propensas a reportar una o más pérdida de datos (67 %) que las grandes (57 %) y el sector público (49 %). En promedio, el costo de una fuga de datos relacionada con impresión es de £743,000. Más allá de la pérdida financiera, el mayor impacto de la fuga de datos es la pérdida de tiempo para reparar la brecha y el impacto en la continuidad de la empresa (30 %). Las vulnerabilidades que rodean la impresión en casa, como la no eliminación segura de información confidencial por parte de los empleados, fue citada como uno de los mayores factores que contribuyen a la pérdida de datos.
- **El Índice de Madurez sobre Seguridad en Impresión de Quocirca revela que solo el 27 % de las organizaciones estudiadas se pueden clasificar como líderes de seguridad en impresión,** lo que significa que tienen implementadas seis o más medidas de seguridad. El número de líderes aumenta a

31 % en los Estados Unidos y cae a 18 % en Alemania, que tiene también el mayor número de rezagados (29 %). Los líderes de seguridad en impresión son más propensos a gastar más en seguridad en impresión, experimentan menos pérdida de datos y reportan niveles de confianza más altos en la seguridad de su ambiente de impresión. Cuando se compara por sector, los servicios profesionales y empresariales tienen el mayor porcentaje de líderes (37 %), mientras que el sector público tiene el menor (18 %).

- **Menos de un tercio (32 %) están muy satisfechos con las capacidades de seguridad de su proveedor de impresión.** Esto se eleva a 50 % entre las organizaciones de Estados Unidos y cae a 17 % en Alemania. Las que usan MPS tienen, por mucho, niveles de satisfacción más altos (39 % están muy satisfechas) que las que no están usando MPS o no tienen planes de usar uno (23 %). Líderes de seguridad en impresión: aquellos que han adoptado diversas medidas, incluyendo valoraciones de seguridad, *pull printing* y políticas formales de seguridad en impresión, tienen más probabilidades de reportar niveles altos de satisfacción (53 % de los líderes están muy satisfechos, en comparación con 27 % de Seguidores y solo 15 % de Rezagados).

© Quocirca 2023

Cuadro de contenido

Resumen ejecutivo **2**
Hallazgos clave 3
Introducción **6**
Panorama del proveedor **7**
Perfil del proveedor: Xerox **9**
Recomendaciones **12**
Recomendaciones al proveedor 12
Recomendaciones al comprador 12
Sobre Quocirca **14**

Introducción

Mientras que las organizaciones se ajustan para gestionar equipos de trabajo híbridos y remotos, apoyar la transformación digital y navegar en una incierta y volátil economía global, enfrentan al mismo tiempo un panorama de riesgos y vulnerabilidades siempre creciente. La investigación de Quocirca revela que el 42 % de las organizaciones han experimentado un incidente de ciberseguridad durante el último año, elevándose a 51 % en el sector de finanzas y 55 % entre las organizaciones de mercado intermedio. El volumen de los incidentes de seguridad ha aumentado durante el último año para el 61 % de las organizaciones.

La alteración en la cadena de suministros y situaciones geopolíticas como la guerra entre Rusia y Ucrania han intensificado aún más el panorama de riesgos. El aumento de prevalencia de ransomware, la denegación de servicio por ransomware (RDoS), denegación de servicio distribuido (DDoS), la ingeniería social y los ataques a la cadena de suministros están provocando un aumento de preocupación sobre ciberseguridad y la resiliencia de funciones vitales para las empresas.

Esto además está compuesto por una gran cantidad de retos tecnológicos. Al tiempo que las organizaciones migran más aplicaciones y servicios a la nube para apoyar sus iniciativas de transformación digital, surgen nuevos desafíos contra la seguridad. La creciente cantidad de datos vitales para las empresas alojados en la nube las vuelve vulnerables contra ataques y las pone en peligro.

Este riesgo se incrementa debido a los trabajadores remotos que tienen acceso a los datos mediante redes en el hogar potencialmente inseguras. Las amenazas contra la seguridad incluyen puntos de acceso mal configurados, contraseñas débiles, falta de gestión de identidades y accesos (IAM) y no usar una autenticación multifactor. Un enfoque fragmentado para el monitoreo y detección de amenazas significa que los equipos de seguridad están batallando para no quedarse atrás.

La infraestructura de impresión no es inmune a los riesgos contra la seguridad. En promedio, los documentos impresos representan el 27 % de los incidentes de seguridad de TI. Las impresoras multifunción (MFP) inteligentes de la actualidad no solo representan un riesgo porque sus productos pueden caer en las manos equivocadas, ya sea accidental o intencionalmente, sino que pueden estar expuestas como acceso al resto del ambiente de la organización. Las impresoras en el hogar representan un riesgo adicional, en particular las compradas por los empleados. Estas compras particulares significan que las impresoras en el hogar podrían no cumplir los estándares de seguridad corporativa ni ser monitoreadas por medio de herramientas de seguridad centralizadas.

Aunque la impresión sigue siendo una prioridad baja en la agenda de seguridad de TI, las organizaciones continúan reportando pérdidas de datos relacionadas con esta actividad. En nuestro estudio de 2023, 61 % de los encuestados reportaron una fuga de datos relacionada con la impresión, con un costo promedio estimado de £743,000 por una fuga de datos. Las organizaciones no pueden ser complacientes, porque cualquier incidente de seguridad tiene una gran repercusión sustancial en su reputación y sus finanzas.

Estos riesgos se pueden mitigar mediante la adopción de un enfoque de seguridad de confianza cero (zero trust) y verificación permanente. La implementación de encriptado de redes y datos, monitoreo y reparación de seguridad, junto con la microsegmentación, pueden ayudar a reducir las áreas vulnerables, mejorar la contención de amenazas y fortalecer el cumplimiento de las reglas.

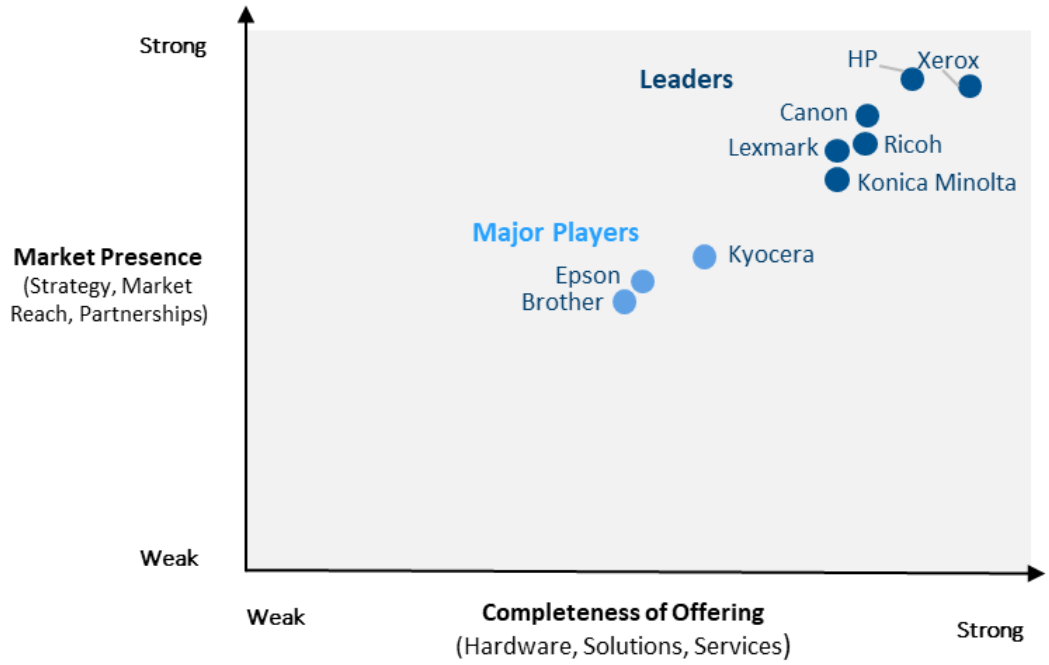
Este informe enfatiza los riesgos y retos asociados con el aseguramiento de la infraestructura de impresión para el lugar de trabajo híbrido. Habla sobre los niveles de confianza en seguridad, la adopción de medidas de seguridad en la impresión, y la desconexión entre los CIO y los CISO que debe solventarse. Este informe también incluye un análisis de los productos, servicios y soluciones de seguridad de los mayores fabricantes de impresoras del mercado.

Panorama del proveedor

Quocirca ha creado una imagen del posicionamiento de los proveedores en el mercado global de seguridad en impresión (Figura 14). Tenga en cuenta que, debido a la variedad de ofertas de servicio de cada proveedor y a diferencias regionales, esto es solo con fines de orientación.

La gráfica representa la visión de Quocirca del panorama competitivo para los proveedores según las siguientes categorías:

1. **Líderes:** Proveedores con una visión estratégica fuerte y una oferta variada de servicios y productos de seguridad en impresión. Los líderes han hecho inversiones significativas en su infraestructura y catálogo de servicios, soluciones y hardware, y también demuestran una visión sólida para estrategias futuras.
2. **Participantes importantes:** Proveedores que han establecido y comprobado propuestas y continúan desarrollando su catálogo de servicio de soluciones. Estos proveedores tienen más probabilidad de estar fuertemente centrados en el mercado de pymes enfocándose en el hardware.



Completeness of Offering (Hardware, Solutions, Services)	Oferta integral (hardware, soluciones, servicios)
Market Presence (Strategy, Market Reach, Partnerships)	Presencia en el mercado (estrategia, alcance, socios)
Weak	Debilidad
Strong	Fortaleza
Major Players	Participantes importantes
Epson	Epson
Brother	Brother
Kyocera	Kyocera
Leaders	Líderes
HP	HP
Xerox	Xerox
Canon	Canon

Ricoh	Ricoh
Lexmark	Lexmark
Konica Minolta	Konica Minolta

Figura 1. Panorama de proveedores de seguridad en impresión Quocirca, 2023

El panorama de proveedores Quocirca es una representación gráfica de la opinión de Quocirca sobre el mercado y se basa en la metodología de puntuación de Quocirca. Esta información se proporciona solo como una representación visual y deberá combinarse con otras fuentes para determinar la conveniencia de un proveedor. Quocirca no apoya a ningún proveedor, producto o servicio. La información se basa en las mejores opiniones y recursos disponibles que reflejan el criterio en el momento. Todas las opiniones están sujetas a cambios.

Perfil del proveedor: Xerox

Opinión de Quocirca

Xerox ha avanzado en su posición de liderazgo en la valoración de Quocirca del mercado de seguridad en impresión de 2023. Xerox ha refinado su estrategia de seguridad, acentuado la inversión en su catálogo de servicios y ha mejorado su ejecución para lanzamiento al mercado. Su catálogo de hardware centrado en la seguridad se complementa mediante una amplia gama de servicios y soluciones de seguridad flexibles y escalables que satisfacen las rigurosas necesidades de seguridad de pymes y clientes grandes globales y multirregionales. Xerox destaca particularmente por su sólido legado en el sector de servicios gestionados de impresión (MPS) y su experiencia para proporcionar valoraciones de seguridad detalladas. Su profunda experiencia y capacidad para asegurar y optimizar los procesos de flujo de trabajo con documentos está entre las más fuertes de la industria.

Desde el último año, ha amplificado su mensaje sobre seguridad global y adoptado un catálogo de seguridad multinivel que conforma una serie de principios de confianza cero (zero trust). En particular, Xerox ha profundizado sus capacidades sobre seguridad de dispositivos, gestión de flota y seguridad de contenido. Se han hecho notables avances en áreas como gestión de certificados, gestión de firmware, gestión de vulnerabilidad, monitoreo de seguridad y reparación automatizada.

Los productos Xerox cuentan con una amplia gama de certificaciones de la industria, que incluyen ISO 27001, ISO 22301, SOC2, SOC3 y FedRAMP. En fechas recientes, introdujo un programa privado de recompensas para cazadores de errores (bug bounty) en asociación con HackerOne para identificar proactivamente y remediar las vulnerabilidades potenciales en las impresoras Xerox de la serie AltaLink 8100. La solidez de la seguridad se extiende a los servicios de Xerox en la nube como Workplace Cloud, que habilita la gestión de impresión segura y la gestión de flota, y también tiene autorización FedRAMP.

Debido a sus sólidas capacidades de impresión, captura y flujo de trabajo, Xerox es una buena elección estratégica para organizaciones que dependen mucho del trabajo impreso y buscan disminuir los riesgos de seguridad en sus procesos con documentos.

Aspectos destacados del proveedor

El catálogo de servicios y productos de Xerox incluye diversas soluciones y servicios, entre los que se encuentran soluciones gestionadas de impresión (MPS), Capture & Content Services (CCS), servicios de participación del cliente (CES) y servicios de TI. Como resultado de una continua inversión en investigación y desarrollo (I+D), Xerox ha presentado más de 600 patentes relacionadas con seguridad. Todos los productos desarrollados por Xerox cumplen con el Estándar de Seguridad de Producto (XPSS) modelado en NIST SP 900-53. Durante todo el ciclo de vida útil del producto se ejecutan escaneos de vulnerabilidad, pruebas de intrusión y hackeo ético con el fin de descubrir, arreglar y validar vulnerabilidades.

Catálogo de hardware centrado en la seguridad

Los dispositivos con Tecnología Xerox ConnectKey tienen certificados Common Criteria (ISO/IEC 15408) y FIPS 140-2/140-3, e incluyen diversas capacidades para evitar ataques maliciosos, malware y ataques no autorizados. Esto incluye prevención de intrusiones, software de sistema de firma digital, autenticación de usuario, verificación de firmware (ya sea al inicio en dispositivos seleccionados o mediante activación del usuario), tecnología de lista blanca e integración con Identity Services Engine de Cisco, que se puede usar para política de seguridad y cumplimiento. Xerox también ofrece integración de proveedor de identidad (IdP) en la nube con Okta, Ping Identity y Microsoft Azure como estándar y proporciona una autenticación multifactor. Además, se ofrece soporte adicional para funciones de seguridad de documentos y dispositivos, como PDF cifrados, discos de hardware y sobreescritura de memoria y registros de auditoría.

Su programa de cumplimiento proporciona aseguramiento independiente sobre sus controles y políticas de seguridad, y ha logrado certificaciones como ISO 27001, SOC2, FedRAMP, PCI DSS y más. Xerox también fue la

primera empresa en recibir autorización de FedRAMP para servicios de impresión gestionados con base en la nube.

Estructura de seguridad robusta mediante hardware, soluciones y servicios.
La estructura de seguridad Xerox se basa en cuatro elementos clave: gestión de seguridad de dispositivos, gestión de flota, gestión de impresión y gestión de contenido seguro. A nivel de dispositivo, esto incluye una serie de capacidades para prevenir ataques maliciosos, malware y ataques no autorizados. Esto incluye prevención de intrusiones, software de sistema de firma digital, autenticación de usuario, verificación de firmware (ya sea al inicio en dispositivos seleccionados o mediante activación del usuario), tecnología de lista blanca Trellix e integración con Identity Services Engine de Cisco.

La gestión de seguridad de flotas proporciona una aplicación de políticas en toda la flota y una solución automatizada para cumplir con las normas de seguridad en línea con el firmware del dispositivo, las contraseñas, las configuraciones de seguridad y los certificados de dispositivos. Xerox también proporciona monitoreo proactivo de seguridad. El Servicio de Auditoría de Seguridad de las Impresoras Xerox usa un mecanismo de política centralizada y agrupamiento de dispositivos para racionalizar la gestión de la flota.

La gestión de seguridad de contenido y datos se habilita mediante la función de seguridad de contenido de Xerox Workplace Cloud y la solución Workplace Suite. Esto proporciona una capacidad para detectar contenido confidencial predefinido y generar alertas e informes a partir de la forma en que se usan los datos. Además, la solución Xerox Workplace Cloud cifra el contenido en tránsito y el almacenado. El contenido almacenado en la nube en Xerox se puede cifrar usando una clave de cifrado propia del cliente.

Integración de software expandido y gestión de vulnerabilidad
La integración con soluciones de seguridad, incluyendo las soluciones para información sobre seguridad y gestión de eventos (SIEM) de Trellix (anteriormente McAfee Enterprise), LogRhythm y Splunk simplifican la gestión e informe de eventos de seguridad. Sobresale el Servicio Printer Security Audit de Xerox (en la oficina o por medio de alojamiento en nube privada) un monitoreo de flota avanzado que incluye monitoreo de seguridad e integración de gestión de eventos e información de seguridad (SIEM).

Los desarrollos recientes incluyen la gestión de certificados de dispositivos, que proporciona configuración remota, monitoreo y resolución automatizada para las políticas de certificados digitales y el lanzamiento de su programa Bug Bounty en asociación con HackerOne en diciembre de 2022.

Extensa capacidad en seguridad de captura y contenidos
Además de su catálogo de hardware ConnectKey con gran número de funciones de seguridad, Xerox destaca particularmente por su gran variedad de soluciones para captura y contenido, que incluye funcionalidad avanzada para prevención de pérdida de datos y contenido. Xerox sobresale en el área de análisis y presentación de informes, al proporcionar estudios a fondo y monitorear continuamente el perfil de riesgo de los ambientes de impresión de sus clientes.

Fortalezas y áreas de oportunidad del proveedor

Fortalezas

- **Fuerte compromiso con la mejora del catálogo de productos mediante estrictas certificaciones de seguridad.** Amplio espectro de certificaciones, como ISO 27001, SOC2, FedRAMP y PCI DSS. Fuerte inversión en I+D, presentación de más de 600 patentes relacionadas con la seguridad.
- **Un claro enfoque en confianza cero.** Xerox ha desarrollado una propuesta clara alrededor del enfoque de confianza cero que incluye autenticación, monitoreo, reparación y automatización. Ahora ofrece funciones de seguridad avanzadas para hardware como Trusted Boot en productos seleccionados, con planes de expandirlo a más equipo del catálogo, así como protección de BIOS y firmware, todos productos de AltaLink y VersaLink. Esto pone a Xerox en una posición fuerte del mercado.
- **Valoración detallada y capacidades analíticas.** Xerox ha probado su experiencia en el mercado de MPS y una profunda capacidad al hacer valoraciones de seguridad. Esto le permite ofrecer una valiosa opinión sobre las vulnerabilidades de seguridad en los ambientes con múltiples proveedores actuales

y demostrar, de la misma manera, cómo la flota estandarizada de Xerox puede reducir el riesgo, apoyada por sus servicios y soluciones de seguridad.

- **Plataforma para habilitar ventas globalmente coherente.** Durante el último año, Xerox ha invertido en capacitación y recursos para apoyar sus canales directos e indirectos. Ha ejecutado una campaña de mercadotecnia efectiva que ayuda a desmitificar la complejidad de la seguridad. Esto fortalece su posición no solo entre los usuarios finales, sino también entre los distribuidores que necesitan construir o mejorar su oferta de servicios de seguridad.

Oportunidades

- **Expandir la oferta de servicios de TI adicionales para el mercado de pymes.** Xerox ha hecho fuertes incursiones en el espacio de servicios de TI y puede favorecerse del apalancamiento con socios con el fin de construir ofertas de servicios de seguridad en paquete para distribuidores tanto en el sector de impresión tradicional como de TI.
- **Mejorar el uso de inteligencia artificial y aprendizaje automático para apoyar la detección de anomalías.** Este avance podría extender las capacidades de Xerox más allá de la protección contra fugas para favorecer la detección y reparación contra nuevas y avanzadas amenazas.
- **Construir relaciones con proveedores de servicios gestionados de seguridad (MSSP).** Si bien, Xerox es más que capaz de proveer seguridad en impresión gestionada por su cuenta, muchos clientes buscan trabajar con un MSSP en todos los aspectos de su seguridad, incluyendo la impresión. Xerox necesita asegurar que tiene las relaciones correctas con los proveedores líderes de esta área.

© Quocirca 2023

Recomendaciones

Se espera que el gasto por seguridad en impresión continúe creciendo en los próximos 12 meses, creando constantes oportunidades para los fabricantes de equipo de impresión, proveedores de servicios de impresión gestionada y distribuidores. Está claro que las organizaciones que usan MPS y las que han adoptado diversas medidas de seguridad en impresión están a la vanguardia. Demostrar cómo los MPS pueden mejorar la resiliencia en seguridad de la infraestructura de impresión permitirá que los proveedores moldeen sus propuestas para los ambientes de impresión en casas y oficinas.

Recomendaciones al proveedor

Quocirca recomienda que los proveedores aborden las siguientes áreas:

- **Eliminar la separación entre CIO y CISO.** En las organizaciones más grandes, la responsabilidad de la seguridad en impresión puede estar fragmentada entre los distintos participantes en negocios y TI. Mientras que los CIO tienen un enfoque estratégico de la infraestructura de TI, los CISO están completamente enfocados en la seguridad. Dada la separación entre estos responsables de toma de decisiones, los proveedores deberían cambiar su postura y mensajes sobre la seguridad en impresión a un nivel estratégico más elevado. Esto puede apoyar la alineación de las prioridades de la seguridad en impresión al hacer que los CIO y CISO desarrollen una relación más colaborativa.
- **Proporcionar seguridad consistente a través del ambiente híbrido.** Muchas impresoras en el hogar que fueron compradas por empleados no cumplen con los requisitos de seguridad de la empresa. Asegurar que las ofertas de MPS ideadas para la seguridad ayuden a abordar estas compras particulares por medio de monitoreo remoto centralizado o proporcionando dispositivos autorizados para su uso en casa. Mientras que los ambientes estandarizados por lo general tienen un nivel más alto de seguridad de hardware comparados con un ambiente de flota mixta, muchas organizaciones operan una mezcla de marcas de dispositivos en los ambientes de oficina y hogar. Esto crea la necesidad de plataformas de gestión de impresión integradas por parte de terceros que puedan gestionar consistentemente la seguridad de los documentos a través de una flota heterogénea. Sin embargo, esto presenta una oportunidad para los proveedores de MPS, pues podrán cambiar a los clientes a un ambiente estandarizado para lograr una seguridad más estrecha en toda su infraestructura de impresión.
- **Crear claridad sobre las ofertas que lleven al enfoque de confianza cero.** No hay una solución única para el enfoque de confianza cero. Es importante ser claros sobre la forma en que funciona en los dispositivos con los que ya se contaba y evitar el mal uso del término confianza cero, o «lavarse las manos» porque se usa la política de confianza cero para crear una percepción de sólida seguridad. El enfoque de confianza cero en el panorama de la impresión se puede alcanzar mejor mediante la microsegmentación y la integración con una autenticación multifactor y plataformas de gestión de identidades y acceso (IAM). Hay que mostrar certificaciones y experiencia en esta área al enfocarse en asociaciones y principios estratégicos. Esto también construirá confianza con los clientes que necesitan un cambio seguro hacia una infraestructura de impresión basada en la nube.
- **Hacer uso de MPS como habilitador de una seguridad mejorada.** Las organizaciones que usan MPS y diversas medidas de seguridad (mediante soluciones, auditorías y valoraciones formales de seguridad) están a la vanguardia de la seguridad en impresión en términos de confianza y menor pérdida de datos. Las soluciones y servicios de seguridad flexibles y escalables atraerán a organizaciones pequeñas que no son inmunes a los riesgos de seguridad, pero todavía carecen del presupuesto para implementar medidas avanzadas de seguridad en impresión. Ofrecer revisiones de seguridad regulares mientras cambian las necesidades de negocios también será la clave para mejorar los niveles de satisfacción sobre seguridad en impresión.

Recomendaciones al comprador

El panorama de amenazas a la seguridad en impresión se ha expandido para incluir diversos dispositivos del hogar y la oficina que buscan apoyar nuevas formas de trabajo híbrido. Como dispositivos inteligentes en red,

las impresoras multifunción son un eslabón débil en la seguridad de TI. Esto se puede reducir al tomar diversas medidas basadas en una política de seguridad de la organización.

Los compradores deberían considerar las siguientes acciones:

- **Tratar la seguridad en impresión como una prioridad estratégica.** La seguridad en impresión y las TI deben estar integradas y ser consideradas como una prioridad alta. Es necesario aumentar la importancia de asegurar la infraestructura de impresión entre los CIO y CISO participantes para que estén orientados hacia la comprensión de los riesgos y las medidas que se pueden implementar para mitigar los riesgos de la impresión no segura.
- **Conducir una profunda valoración de riesgos y seguridad en impresión.** Las organizaciones deberán buscar proveedores que puedan ofrecer valoraciones profundas del ambiente de impresión. Las auditorías pueden descubrir potenciales puntos vulnerables en la seguridad de documentos y dispositivos. Para organizaciones que operen con una flota mixta, esto puede ayudar a comprender las oportunidades para la optimización de dispositivos al usar una flota sencilla con funciones uniformes de seguridad para hardware.
- **Asegurar que los trabajadores remotos y en casa puedan imprimir con seguridad.** Comprobar que las impresoras cumplan con los estándares corporativos de seguridad y, en casos en los que los empleados hayan comprado sus propias impresoras, desarrollar directivas de seguridad que definan si se pueden usar estas impresoras y la forma de hacerlo. Se debe evaluar el soporte y el monitoreo de seguridad de las plataformas de gestión de impresión para la impresión en casa.
- **Construir una arquitectura de seguridad en impresión cohesiva.** Las soluciones de seguridad fragmentadas rara vez logran una seguridad sólida y consistente, en particular en un ambiente de trabajo híbrido. Hay que considerar una plataforma de seguridad integrada que pueda soportar capacidades como *pull printing*, monitoreo remoto e informes a todo lo largo y ancho de la flota. Extender la seguridad en impresión al contenido y el flujo de trabajo por medio del uso de herramientas para seguridad de contenido y de prevención de pérdida de datos (DLP) a nivel de aplicación. Evaluar con cuidado las solicitudes de confianza cero del proveedor y asegurar la integración con plataformas de autenticación multifactor que ya tenga en uso la organización. Evaluar si las soluciones de gestión de impresión segura pueden operar en una red de trabajo microsegmentada.
- **Formalizar procesos que respondan a los incidentes de seguridad en impresión.** Las organizaciones deben estar preparadas para esto y tener los procesos correctos listos para lidiar con las secuelas técnicas, legales y de reputación de una fuga de datos. Esto requiere que la organización trabaje en equipo para crear y adoptar una serie de políticas.
- **Monitorear, analizar e informar continuamente.** Asegurar que los datos de los dispositivos de seguridad existentes, como los dispositivos de gestión de eventos y seguridad de la información (SIEM), estén conectados y analizados para mostrar lo que ha estado sucediendo, lo que sucede y lo que puede suceder. Comprobar que dichos sistemas abarcan lo más posible la plataforma, y que usen los hallazgos obtenidos para cubrir las grietas en la seguridad de su organización.

Sobre Quocirca

Quocirca es una empresa global de investigación e introspección especializada en la convergencia de las tecnologías digital y de impresión en el lugar de trabajo del futuro.

Desde el 2006, Quocirca ha jugado un papel influyente para asesorar a los clientes sobre los principales cambios del mercado. Nuestras consultas e investigaciones están a la vanguardia del mercado en rápida evolución de las soluciones y servicios de impresión y son confiables para clientes que buscan nuevas estrategias para abordar las tecnologías problemáticas.

Quocirca ha sido pionera en la investigación de muchas áreas emergentes en los mercados. Hace más de diez años, fuimos los primeros en analizar el panorama competitivo del mercado global de los servicios gestionados de impresión (MPS), seguido del primer análisis competitivo global del mercado de seguridad en impresión. Más recientemente, Quocirca reforzó su liderazgo y enfoque únicos en el mercado al publicar el primer estudio que examinó el futuro de la conexión y la inteligencia de la impresión en el lugar de trabajo digital. El Global Print 2025 study (estudio global de la impresión 2025) muestra una percepción sin paralelo del impacto de la disrupción digital, desde las perspectivas ejecutiva-industrial y del usuario final.

Si desea más información, visite www.quocirca.com.

Derechos de uso
Es necesario tener permiso para citar cualquier información de este informe. Consulte la Política de citación de Quocirca para más detalles.

Negación de responsabilidad:
© Copyright 2023, Quocirca. Todos los derechos reservados. El presente documento no puede, ni total ni parcialmente, ser reproducido, distribuido, almacenado en un sistema de recuperación, ni transmitido por medio alguno, ya sea electrónico, mecánico, fotocopiado, grabado ni de ninguna otra forma sin autorización expresa por escrito de Quocirca. La información que contiene este informe es con fines de orientación general solo para asuntos de interés. Tenga en cuenta que, debido al redondeo, las cifras presentadas en este informe podrían no cuadrar con precisión con los totales mostrados y los porcentajes podrían no reflejarse de forma absoluta en las figuras. El contenido de este informe se proporciona en el entendimiento de que los autores y editores no tienen el compromiso de brindar servicios o asesoría legal ni profesional de otro tipo. Quocirca no es responsable de ningún error, omisión o imprecisión, ni de los resultados obtenidos por el uso de este informe. Toda la información de este informe se presenta tal cual, sin garantía de ser exhaustiva, precisa u oportuna ni por los resultados obtenidos a partir del uso de este informe, y sin garantía de ningún tipo, expresa o implícita. Bajo ninguna circunstancia, Quocirca, sus colaboradores o empresas asociadas, ni sus socios, agentes o empleados, serán responsables ante usted o cualquier persona por decisiones hechas o acciones tomadas a partir de este informe ni por daños consecuentes, especiales o similares, incluso si se ha advertido de la posibilidad de dichos daños. El acceso y uso de esta publicación están regidos por nuestros términos y condiciones. Es necesario tener permiso para citar cualquier información de este informe. Consulte nuestra Política de citación para más detalles.