Print Security Landscape, 2024

Mitigating the print infrastructure as a threat vector

Print security trends in the US and Europe
Vendor Excerpt: Xerox
July 2024

QUOCIRCA

Executive summary

The rise of hybrid work has blurred the lines of traditional print infrastructure security. Public networks and less-controlled environments are now commonplace, demanding a more robust approach to print security. Meanwhile, the rise of AI is creating further security challenges, increasing the potential for vulnerable devices to become easier targets and be compromised as a result of weak security protocols. Print manufacturers and channel partners must adapt by offering enhanced security solutions that integrate seamlessly with existing IT infrastructure. This shift presents a significant opportunity. By becoming trusted advisors, the print channel can guide organisations towards comprehensive solutions across device, data, and document security. Prioritising the print infrastructure as a critical element of wider information security strategies will not only safeguard businesses, but also unlock new revenue streams for the print industry.

Quocirca's Print Security Landscape, 2024 study reveals that organisations face ongoing challenges in securing the print infrastructure. Employee-owned printers are viewed as a key security concern by 33% of organisations, which reflects the difficulty in controlling home printing – at both a device and document level – as documents can be exposed to unauthorised users. Despite the growing awareness of printing as a security weakness, organisations are struggling to translate this knowledge into action.

Print-related data breaches remain a significant threat, with 67% of respondents (up from 61% in 2023) reporting at least one data loss incident in the past year. This number jumps to 74% for midmarket organisations. This is leading to a decline in confidence, particularly among small and medium-sized businesses (SMBs), in the overall security of their print infrastructure.

Notably, organisations operating a standardised fleet are less likely to report one or more data losses (59%) than those operating a multivendor fleet (70%). This reflects the challenge of maintaining consistent security across mixed brands compared to proprietary security platforms that are embedded in a standardised fleet. Third-party print management solutions can help with securing printing across a mixed fleet. However, the extra workload for IT in managing a mixed fleet, along with the additional difficulties and hard costs of sourcing multiple print device drivers, integration systems, and monitoring and reporting systems, makes mixed fleets less attractive than standardised ones.

The latest research exposes a concerning gap in print security perception between chief information officers (CIOs) and chief information security officers (CISOs). While both expect increased security spending (77% of CIOs and 78% of CISOs), CISOs are significantly less confident in current print security measures than CIOs. This disconnect is further emphasised by the higher percentage of CISOs (41%, versus 34% of CIOs) who find managing print security challenges difficult. Interestingly, CIOs exhibit greater concern (52%, versus 32% of CISOs) about unsecured home printers, which highlights a potential blind spot.

This fractured view creates a key obstacle. Aligning CIO and CISO perspectives on security is essential for achieving robust information security. Bridging this gap is no longer an option – it is a necessity. Fortunately, Print Security Leaders, as defined by Quocirca's Print Security Maturity Index, are mitigating risks. Leaders are organisations that have implemented a higher number of print security measures than Followers and Laggards. Leaders report lower levels of data loss and have higher confidence in the security of their print infrastructure.

This presents a valuable opportunity for suppliers to position themselves as strategic partners and strengthen their security propositions to help customers mitigate risks associated with unsecured printing in both the home and office environments. By identifying and promoting the best practices employed by these Leaders, suppliers across the print ecosystem can play a crucial role in guiding Followers and Laggards to improve their security posture.

Key findings

- **Printer and MFP manufacturers continue to enhance and deepen their security focus.** HP has advanced its position because of ongoing innovation across its hardware portfolio and establishing a zero-trust print architecture (ZTPA) framework and stronger alignment of HP Wolf Security across its print and PC offerings. Xerox has a comprehensive security offering across hardware and solutions, particularly with respect to its workflow and content security portfolio. Canon offers a globally consistent security offering, supported by its mature uniFLOW platform. Other vendors in the leadership category include Lexmark with a mature secure-by-design approach across its hardware range, Ricoh which stands out for its cybersecurity services, and Konica Minolta with its bizHUB secure offerings. Sharp has made strong investments in security over the past year, exemplified by a multi-layered security approach and partnership with Bitdefender. Major players include Epson, Brother, Kyocera, and Toshiba.
- **Print security has climbed the security agenda compared to 2023.** While public networks are seen as posing the top IT security risk (35%), this is closely followed by employee-owned home printers (33%), up from 21% in 2023. This potentially reflects the growth in 'shadow printing' caused by increased home working and the use of printers outside corporate controls. Office printing is in third position (29%), up from eighth in 2023 (20%).
- **Organisations are making progress in addressing print security challenges.** Overall, 30% say it is very or somewhat difficult to keep up with print security demands, down from 39% in 2023. The top print security challenge is protecting sensitive and confidential documents from being printed (28%), rising to 34% in the US. Notably, organisations operating a multivendor print environment are more likely to cite this as a challenge (30%), compared to 24% of those using a standardised fleet.
- **In the past 12 months, 67% of organisations have experienced data losses due to unsecure printing practices, up from 61% in 2023.** As in 2023, midmarket organisations are more likely to report one or more data losses (70%) than large organisations (63%), with business and professional services suffering the greatest volume of breaches at 71%, followed by the public sector (70%). On average, the cost of a print-related data breach is over £1m, compared to £743,000 in 2023.
- **Quocirca's Print Security Maturity Index reveals that only 20% of organisations are classed as Leaders.** Leaders are those organisations that have implemented six or more security measures. The number of Leaders rises to 25% in the US and falls to 14% in France, which also has the highest number of Laggards (23%). Leaders are likely to spend more on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment.
- **Artificial intelligence (AI) is creating further concerns around security risks.** Overall, 62% report that they are extremely or moderately concerned about AI creating more IT security risks. Overall, 83% of respondents state that it is very (34%) or somewhat important (49%) that vendors use AI or machine learning (ML) to identify print security threats. These findings suggest a promising opportunity for print vendors to develop and deliver innovative solutions using ML and AI for print security – whether this involves on-device AI security or AI-based remote monitoring solutions.
- **Over a third (36%, up from 32% in 2023) are very satisfied with their print supplier's security capabilities.** This rises to 47% among US organisations and drops to 19% in Germany. Those using an MPS have far higher satisfaction levels (43% are very satisfied) than those not currently using an MPS or with no plans to use one (23%).

Table of Contents

Buyer recommendations

The increased move from simple print devices to intelligent MFPs, which have multiple vectors for attack, presents an increasingly weak link in IT security. This can be mitigated with a range of measures based on an organisation's security posture.

Buyers should consider the following actions:

- **Start by conducting in-depth print security and risk assessments.** With awareness of print security issues growing, organisations still appear to be doing little to plug the gaps. Where in-house skills are lacking, organisations need to look to providers that can offer in-depth assessments of the print environment. Security audits can uncover potential security vulnerabilities across device and document security, and this can help devise means of dealing with them. For organisations operating a mixed fleet, such an audit may also provide the value proposition required for a move to a more standardised fleet, with which a consistent and cohesive approach to security can be taken.
- **Treat print security as a strategic priority – but not in isolation.** Print and IT security must be integrated and considered a higher business priority. The importance of securing the print infrastructure must be elevated to both CIO and CISO stakeholders so they are aligned on understanding the risks to the IT platform and business. Focus must be placed on how measures can be implemented to mitigate the risks of unsecured printing, as well as monitoring and managing the flow of information created by the increasing use of digitised workflows.
- **Evaluate AI security.** Vendors should be looking to embrace and integrate AI in both the device and software to provide advanced security benefits. Real-time analytics of data on the device can help prevent the use of the device as a direct attack vector. However, maintaining the AI capabilities at a hardware level in such a rapidly evolving market may be problematic. Using AI with software provides a good means of enabling a more flexible level. Overall, a multi-level approach of hardware plus software should be used to provide the greatest security capabilities possible.
- **Include remote and home workers in the managed print environment.** Consumer-grade printers may not conform to corporate security standards, but MPS may be able to provide the controls around such printers to ensure content and information security are in place. Security guidelines need to be developed and enforced on whether and how these printers can be used.
- **Build a cohesive print security architecture.** Piecemeal security solutions rarely deliver consistent and robust security, particularly across a hybrid work environment. Consider an integrated security platform that can support capabilities such as pull printing, remote monitoring, and reporting across the full fleet. Extend print security to content and workflow through the use of content security and data loss prevention (DLP) tools at the application level. Carefully evaluate vendor zero-trust claims and ensure integration with multifactor authentication platforms already used in the organisation. Evaluate whether secure print management solutions can operate in a micro-segmented network.
- **Create, formalise, and continuously review processes to respond to print security incidents.** Organisations must ensure that they are prepared for what are essentially inevitable security incidents and have the right processes in place to deal with the technical, legal, and reputational fallout from such incidents. This requires the organisation to work together to create an embracing set of policies.
- **Continuously monitor, analyse, and report.** A lack of cohesive monitoring and reporting will lead to breaches that are unseen, with longer-term impacts and costs greater than if the incident had been seen and managed earlier. Ensure that print data is integrated with other data from existing security devices, such as security information and event management (SIEM) devices, and analysed to show what has been happening, what is happening now, and what may happen in the future. Ensure that such systems cover as much of the overall platform as possible, and use the insights gained to work on plugging holes in your organisation's security on an ongoing basis.

Vendor profile: Xerox

Quocirca opinion

Xerox has retained a leadership position in Quocirca's assessment of the print security market in 2024. Over the past year, it has further refined its security strategy across both its office and production print product portfolio and enhanced its channel sales enablement. Its depth of capabilities across content security and workflow automation is among the strongest in the industry. It continues to enhance its Workflow Central content security offerings, which include new security apps such as auto-redaction that use AI algorithms to protect and secure documents.

Xerox's comprehensive security offerings are built around its security framework, which encompasses ConnectKey platform security, secure fleet management, secure print management, and secure data and content management. Its security-centric hardware portfolio is complemented by a broad range of flexible and scalable security services and solutions that it delivers to both SMBs and large multiregional and global customers.

Multi-layered security approach

Over the past year, Xerox has amplified its global security messaging and adopted a multi-layered security portfolio that conforms to a set of zero-trust principles. In particular, Xerox has deepened its capabilities across device security, fleet management, and content security. Notable advancements have been made in areas such as certificate management, firmware management, vulnerability management, security monitoring, and automated remediation. Xerox products conform to a broad range of industry certifications, including ISO 27001, ISO 22301, SOC2, SOC3, and FedRAMP. Robust security extends to Xerox cloud services such as Workplace Cloud, which enables secure print management and fleet management. It is also FedRAMP authorised.

Strong MPS and workflow expertise

Xerox particularly stands out for its strong legacy in the managed print services (MPS) sector and expertise in delivering comprehensive security assessments. Recent developments include adding new features to its cloud fleet management solution to better meet the needs of enterprise and SMB clients and a distributed workforce, enhancing its Workplace Cloud and Suite print management solutions to further secure documents and content across a distributed workforce, investment in apps, and its Workflow Central platform.

Notably, Xerox Workflow Central now encompasses document-level protection. Xerox believes it is the first printer vendor to offer document-level protection beyond encryption and password protection. This includes Workflow Central Redact to conceal sensitive data within physical or digital documents, as well as Workflow Central Protect to restrict and control who can view content even when shared with external parties.

In addition, for the production print environment, Xerox Beyond Secure Technology is an advanced set of technologies that embed fraud-proof security into production printing systems, electronic information, and printed documents.

Channel enablement

Xerox continues to invest in its Printer Security Operations Center (PSOC), which will make it easier to sell and administer security services to SMB clients through its XBS and partner channels.

Xerox offers an extensive security portfolio across hardware, software, and services to enhance document protection at both the physical and digital levels. As such, Xerox is a good choice, particularly for businesses looking to enhance security across the document lifecycle. It has particularly strong expertise in supporting large enterprises that are highly dependent on paper-based processes and need to securely digitise their workflows.

Security offerings

Xerox's products and services portfolio includes a range of solutions and services that encompass Managed Print Services (MPS), Capture & Content Services (CCS), Customer Engagement Services (CES), and IT Services. As a result of continued R&D investment, Xerox has filed more than 600 security-related patents. All Xerox-developed products comply with the Xerox Product Security Standard (XPSS) modelled on NIST SP 900-53. Vulnerability

scans, penetration testing, and ethical hacking are performed throughout the product lifecycle to uncover, fix, and validate vulnerabilities.

Security-centric hardware portfolio

Xerox's comprehensive security architecture is built into its full portfolio of products, from small desktop printers through to large production presses. Xerox ConnectKey technology-enabled devices are purpose-built to be trusted end points, and MFPs leverage innovative technologies to safeguard devices, documents, and data. In 2023, the company introduced the AltaLink devices' robust security features, including Trusted Boot, Security Dashboard, Configuration Watchdog, and Fleet Orchestrator, to its A4 VersaLink portfolio.

Xerox ConnectKey Technology-enabled devices are certified to Common Criteria (ISO/ IEC 15408) and FIPS 140-2/140-3 and include a range of capabilities to prevent malicious attacks, malware, and unauthorised access. This includes intrusion prevention, digital signed system software, user authentication, firmware verification (either at start-up on selected devices or upon user activation), Trellix whitelisting technology, and integration with Cisco's Identity Services Engine, which can be used for security policy and compliance. Xerox also offers cloud Identity Provider (IdP) integration with Okta, Ping Identity, and Microsoft Azure as standard and provides multifactor authentication. In addition, further device and document security functionality, such as encrypted PDF, hardware disk and memory overwrite, and audit logs, are supported.

Xerox security framework across hardware, solutions, and services

The Xerox security framework is based on four key elements: secure device management, fleet management, print management, and secure data and content management. At a device level, this includes a range of capabilities to prevent malicious attacks, malware, and unauthorised access. This includes intrusion prevention, digital signed system software, user authentication, firmware verification (either at start-up on selected devices or upon user activation), Trellix whitelisting technology, and integration with Cisco's Identity Services Engine.

Secure fleet management provides fleet-wide policy enforcement and automated remediation for compliance with security policies aligned to device firmware, passwords, security settings, and device certificates. Xerox also provides proactive security event monitoring. Xerox Printer Security Audit Service uses a centralised policy mechanism and device grouping to streamline fleet management.

Secure data and content management are enabled through the content security feature of Xerox Workplace Cloud and Workplace Suite solution. This provides a capability to detect predefined sensitive content and generate alerts and reports based on how that data is used. In addition, the Xerox Workplace Cloud solution encrypts content in transit and at rest. Content stored in the cloud at Xerox can be encrypted using a client's own encryption key.

Xerox Workplace Cloud

This is a complete platform for security, mobility, and cost control, delivering comprehensive secure fleet management and print management with less IT infrastructure and IT task automation, saving IT teams time. Queue Conductor, an automated print driver deployment feature ensuring all users get the right print driver, for the right printer, for the right location, is a new feature introduced this year. It supports any brand of printer for both direct print and pull print for secure release. Xerox has also introduced additional data centre pairs, covering North America, the EU, and the UK, to address the needs of data-sensitive clients that require data to be hosted within their region.

- **Xerox Workplace Cloud and Suite.** This provides consistent security through print, scan, and copy, regardless of where a user accesses the network. Authentication and access control measures support a variety of authentication methods to access print services or release print jobs easily and securely. The solutions also provide content security to track and manage documents by content. Unapproved activity triggers an immediate alert. Data is also encrypted using a symmetric key cryptography algorithm for enhanced security. Document protection is available through Workplace Protect and Workplace Redact.
- **Workplace Cloud Print Tracker.** This counts print usage and provides content security for jobs submitted from a corporate laptop to any brand of printer in a home office, allowing for enhanced management when devices are not on a corporate network.

- **Xerox Workplace Cloud Direct.** Introduced in 2023, Workplace Cloud Direct enables seamless communication between Versalink and Altalink 8100 and newer models directly with Xerox's cloud-based MPS software. This removes the requirement for on-site middleware infrastructure, which means there are less end points to worry about. This is a good choice for customers that require minimal maintenance and/or have a distributed workforce.
- **Xerox Workplace Cloud Fleet Management.** Recent developments include enhanced monitoring capabilities encompassing proactive/reactive supplies, proactive/reactive break-fix, and automated meter reads. Additionally, Workplace Cloud Fleet Management is now available to Xerox direct clients in addition to its direct sales organisations. Xerox also plans to build Device Certificate Management into its cloud solution, bringing security and automation related to managing device certificates to its SMB/channel partners and clients.

Xerox Printer Security Audit Service

Xerox has enhanced the Xerox Printer Security Audit Service's monitoring functionality, which simplifies delivering device management and security services together for channel partners and their clients. This service is delivered to channel partners via Workplace Cloud Fleet Management.

Xerox Device Manager

Clients using Xerox Device Manager (either on-premise or in a private cloud) benefit from the Security Event Monitoring Service, which enables information about device activity to be collected from printers and MFPs within the fleet. Data is analysed and categorised by severity, enabling proactive measures to address potential risks before they escalate into breaches. Additionally, devices running Trellix whitelisting/allowlisting provide extra layers of information. All data is presented in a Security Event Monitoring Dashboard, a centralised platform to update actions and close open security events to ensure proper management and follow-up. It also integrates with SIEM solutions including Trellix, Splunk, and LogRhythm.

Compliance programme

Xerox's compliance programme provides independent assurance over its security policies and controls and has achieved certifications including ISO 27001, SOC2, and PCI DSS. Additionally, its systems, policies, and practices ensure compliance with the PSTI bill, specifically barring non-unique passwords and enabling the use of strong passwords. It provides firmware updates, including auto-updates and communicating potential vulnerabilities through bulletins and subscription feeds.

Notably, the company was the first MPS provider to achieve FedRAMP authorisation, and in 2023, became the first to receive StateRAMP authorisation (the FedRAMP equivalent for US states). It also expanded its authorisation beyond MPS to include digital services solutions and plans to add Scan to OneDrive and Office 365 Xerox ConnectKey apps in 2024. The company also plans to expand use of its Bug Bounty Programme in 2024.

SIEM integration and vulnerability management

Integration with security solutions, including SIEM solutions from Trellix (formerly McAfee Enterprise), LogRhythm, and Splunk, simplifies reporting and management of security events. Of note are Xerox's Printer Security Audit Service (on-premise or via a private hosted cloud) and advanced fleet monitoring, which includes security monitoring and SIEM integration.

IT services

Xerox provides a comprehensive, customisable suite of end-to-end services and solutions designed to solve the top issues faced by SMBs. Services include risk assessments, compliance assessment, managed security operations, and managed end-point detection and response.

Strengths and opportunities

Strengths

- **Strong commitment to enhancing the product portfolio to meet the most stringent security certifications.** This includes a broad spectrum of certifications, such as ISO 27001, SOC2, FedRAMP, and PCI DSS. The company has invested heavily in R&D, with more than 600 security-related patents filed.

- **Robust security framework and partnerships.** A key differentiator is Xerox's security framework across secure device, fleet, print, and data and content management, combined with strategic partnerships with end-point and cybersecurity technology experts including Aruba, Barracuda, Cisco, and HPE, to design and implement right-sized, secure infrastructures for clients.
- **Deep content and capture security capabilities.** Beyond its security feature-rich ConnectKey hardware portfolio, Xerox particularly stands out for its extensive content and capture solutions, which include advanced content and data loss prevention functionality. This includes Xerox Workplace Central Protect and Redact.
- **A clear approach to zero trust.** Xerox provides best practices and recommendations to help clients implement zero trust in a print environment across hardware, software, processes, content, and services consistently with NIST zero-trust architecture. It offers advanced hardware-security features, such as Trusted Boot, on selected products, with plans to expand it to more of the portfolio, as well as firmware and BIOS protection on all AltaLink and VersaLink products. This positions Xerox devices strongly in the market.
- **Comprehensive assessment and analytics capabilities.** Xerox has proven expertise in the MPS market and deep capabilities with security assessments. It particularly excels in analytics and reporting, providing in-depth assessments and continuously monitoring the risk profile of its customers' print environments.
- **Globally consistent sales enablement platform.** Over the past year, Xerox has invested in training and resources to support its direct and indirect channels. It has executed an effective marketing campaign that helps demystify the complexity of security. This strengthens its position with not only end users, but also channel partners that need to build or enhance their security service offering. In addition, its Printer Security Operation Center (PSOC) enables channel partners to deliver specialist security services without investing in security-trained resources and test systems and implementing all the required operational processes.

Opportunities

- **Further expand IT services offerings to the SMB market.** Xerox has made strong inroads into the IT services space and can further leverage partnerships to build packaged security services offerings for channel partners in both IT and the traditional print sector.
- **Enhance the use of ML/AI to support anomaly detection.** This advancement could extend Xerox's capabilities beyond breach protection to further detect and remediate against new and advanced threats.
- **Build MSSP relationships.** While Xerox is more than capable of delivering managed print security in its own right, many customers will seek to work with a managed security services provider for all aspects of their security, including print. Xerox needs to ensure it has the right relationships with the leading providers in this space.

About Quocirca

Quocirca is a global market insight and research firm specialising in the convergence of print and digital technologies in the future workplace.

Since 2006, Quocirca has played an influential role in advising clients on major shifts in the market. Our consulting and research are at the forefront of the rapidly evolving print services and solutions market, trusted by clients seeking new strategies to address disruptive technologies.

Quocirca has pioneered research in many emerging market areas. More than 10 years ago we were the first to analyse the competitive global market landscape for managed print services (MPS), followed by the first global competitive review of the print security market. More recently Quocirca reinforced its leading and unique approach in the market, publishing the first study looking at the smart, connected future of print in the digital workplace. The Global Print 2025 study provides unparalleled insight into the impact of digital disruption, from both an industry executive and end-user perspective.

For more information, visit www.quocirca.com.

Usage rights

Permission is required for quoting any information in this report. Please see Quocirca's Citation Policy for further details.