Print Security Landscape, 2025

Identity, AI, and Quantum: Navigating the New Threat Landscape

Print security trends in the US and Europe
Excerpt report: Ricoh
July 2025

QUOCIRCA

Executive summary

The print infrastructure continues to present a significant, evolving threat vector within corporate networks. Increasingly sophisticated and connected multifunction printers (MFPs), including those leveraging artificial intelligence (AI) and the future computational power of quantum computing, are vulnerable endpoints susceptible to advanced cyber threats.

The risks of mixed fleet environments

Organisations reliant on mixed fleets and those with older 'legacy' print devices face a range of security risks. Quocirca's research found that 59% of respondents are currently operating a multi-vendor fleet, with 41% operating a standardised, single vendor fleet. Mixed fleets require more robust management to ensure that each device is kept at the latest security patch level and that security across the fleet does not leave gaps that can be easily compromised.

Unlike modern MFPs that are engineered with advanced security features, older legacy devices lack robust embedded security, such as hardware roots of trust, secure boot functionalities, or self-healing firmware, leaving them more susceptible to low-level attacks or firmware manipulation. Legacy devices may not support advanced network security features like granular port control, complicating efforts to segment and isolate them effectively from critical network infrastructure. There are also limitations in terms of patching and updates, older models reaching end-of-life for crucial security fixes are exposed to newly discovered and unmitigable vulnerabilities. In addition, authentication mechanisms are often inadequate, offering only basic or no user verification at the device itself, which contributes to the risk of uncollected sensitive documents and unauthorised access to confidential information.

The integration of older assets into modern, centralised security management platforms is often difficult or impossible, hindering consistent policy enforcement and real-time monitoring. Quocirca's research shows that organisations operating complex, often multi-vendor print environments, face elevated risks and increased costs associated with potential data breaches. While just 19% of organisations managing a standardised print fleet are concerned about sensitive documents being printed, this compares to 34% of those with a multi-vendor fleet.

This disparity extends to the perceived threat from AI; 49% of organisations with multi-vendor fleets deem it very important that vendors employ AI to protect against AI threats, a figure that drops to 28% for those with standardised fleets. Furthermore, authentication methods often vary significantly across differing environments, exacerbating the complexity of maintaining a consistent security posture. Awareness of quantum threats is also high, with 66% of IT decision-makers (ITDMs) acknowledging the importance of printers being protected against such attacks.

Print-related data losses are falling – but are still significant

Overall data losses stemming from insecure printing practices have decreased to 56% from 67% in 2024, indicating progress. However, a significant gap persists; print security leaders, defined by the implementation of more security measures, report substantially fewer data losses (47%) compared to laggards (79%), underscoring the direct efficacy of proactive security investments. Documents on home printers constitute the top factor for data loss at 53%, followed by improper document disposal at 44%. This 'human factor' vulnerability is particularly pronounced in sectors such as retail (73% for home printers) and financial services (63% for home printers), indicating a critical need for both comprehensive user education and technological solutions to mitigate risks associated with decentralised printing. The need for print management systems that fully embrace hybrid working is clear. The average cost of a print-related data loss stands at £820,000, escalating to £937,000 for organisations managing multi-vendor fleets, while those with standardised fleets report a lower average of £630,000.

All this – the increasing sophistication of device-level threats to access the network, the ongoing human element of paper-related data loss, and the amplified risks and costs associated with multi-vendor environments, presents an urgent imperative for organisations and the print market itself. Improving print security posture requires a multi-layered approach - prioritising standardised, secure print infrastructure, implementing robust identity and access management frameworks including mandatory authentication across all devices, and deploying solutions that prevent sensitive document printing in unsecured home environments.

AI security and quantum computing concerns on the rise

Alongside this runs the emerging promise and threat provided by AI and quantum computing. Overall, 40% of respondents are extremely or very concerned about the risks presented by AI, with 86% stating that it is either very or somewhat important that vendors use AI and machine learning (ML) in identifying and managing security risks in the print environment. 66% also state that it is either extremely or very relevant that they look to OEMs to develop quantum-resistant print devices, and that they would then want to adopt these within their print environment.

Integrating AI-driven security capabilities and preparing for quantum-safe transitions are now strategic imperatives. Addressing these areas will not only reduce the incidence and financial impact of data breaches but also strengthen overall corporate cybersecurity resilience. Those in the print supply chain that do not prepare to deal with these issues or attempt to ‘AI-‘ or ‘quantum-wash’ their portfolio will struggle in the market, losing customer confidence and loyalty as the provided systems fail to live up to expectations.

This report analyses the findings from Quocirca’s Industry Survey conducted among 400 IT decision-makers involved in the print infrastructure in their organisations in May/June 2025.

Key findings

- **Print manufacturers continue to advance their security offerings.** Over the past year, most vendors have enhanced both hardware and software security. HP has advanced its leadership position, evidenced by the introduction of quantum-resistant printers which sets a new benchmark for the industry along with ongoing development of its zero trust print architecture (ZTPA), and its new Workforce Experience (WXP) platform. Xerox has a broad security offering across hardware and solutions and particularly excels in content security and advanced authentication. Additionally, its acquisition of ITsavvy boosts its IT-led security services capabilities. Canon continues to invest in an information security approach across its devices, notably, its new imageFORCE platform uses machine learning and AI-trained algorithms to recommend optimal device security settings. Lexmark stands out for its mature secure-by-design approach. Ricoh's secure-by-design approach delivers protection from endpoint to cloud, enabling secured workflows and data protection. Konica Minolta uses machine learning and automation across its bizhub i-Series MFPs, along with its Shield Guard cloud platform, and its bizhub SECURE offering. Sharp continues to deepen its IT-led cybersecurity services for SME clients, supported by a range of industry partnerships. A key differentiator for Epson is its multi-core printer/scanner system on a chip (SoC) which presents fewer potential vulnerabilities for attackers to exploit and provides robust hardware security across its MFP product portfolio.

- **Organisations expect to increase print security spend.** Overall, organisations expect to increase their print security spend by 13% in the coming year, rising to 16% amongst organisations operating a mixed fleet. Top concerns are securing home printing (28%), protecting confidential or sensitive documents from being printed (28%) and understanding the type of threats and vulnerabilities of the print infrastructure (25%). Organisations operating a mixed fleet tend to be the most concerned, because managing security across multiple vendors introduces inherent complexities and inconsistencies that can amplify risk.

- **Broader implementation of print security measures.** Top measures include secure cloud print submission (45%), reporting and analytics (43%) and operating a formal process to respond to security incidents including remediation (43%). 37% have adopted a zero trust approach for their print environment and 37% have implemented user authenticated printing (for instance using smart cards). The majority (85%), use and manage device certificate management but of these, just 19% say they actively deploy and manage these across their complete print infrastructure on an ongoing basis. This rises to 33% amongst print security leaders and drops to 10% amongst laggards. The high adoption of certificate management, contrasted with its limited comprehensive deployment, suggests that many organisations are not yet achieving the full benefits of such an approach and therefore may still have vulnerabilities.

- **User authentication methods are varied.** The most common authentication methods are Windows authentication (47%) and passwords or PINs entered directly at the print device (47%). 38% use biometric authentication and 37% use mobile authentication. The diverse range of authentication methods indicates a varied and somewhat fragmented approach to print device security. The lower adoption rates for more advanced authentication methods points to a potential security gap for many organisations and a clear opportunity for print solution providers to educate clients and offer more sophisticated, integrated authentication solutions that align with modern cybersecurity best practices.

- **Print security leaders less likely to report a data loss.** Organisations classified as print security leaders, are less likely to report a data loss – 47% compared to 79% of laggards. This highlights the effectiveness of proactive print security strategies and for vendors, reinforces the opportunity to educate clients on the benefits of comprehensive print security and to provide scalable solutions that elevate security maturity across all organisational sizes. Overall, 56% of organisations report a print-related data breach, down from 69% in 2024. This reduction is mainly due to a fewer number of UK organisations reporting a data breach – just 24% in 2025, compared to 70% in France. Notably, more small and medium-sized businesses (SMBs) (60%), report a print-related data loss compared to 53% of large enterprises.

- **Lost IT time is the top impact of a data loss.** Of those that reported a print-related data breach, 24% report that the top impact was lost IT time responding/managing the breach, rising to 27% amongst larger enterprises, and 30% for those operating a mixed fleet environment. The top impact for SMBs was negative impact on business continuity (28%). This reflects that the true cost of a print-related data breach extends far beyond direct financial penalties. For larger enterprises and those with complex mixed print fleets, the substantial diversion of IT resources towards breach management underscores the hidden burden of inadequate print security. Meanwhile, for SMBs, the direct threat to business continuity highlights their heightened vulnerability and the critical need for solutions that minimise downtime and simplify incident response.

- **Home printing environment is growing source of data loss.** Overall, 53% report that documents have been accessed by unauthorised people in the home environment, rising from 43% in 2024. This rises to 57% amongst SMBs and drops to 49% among large enterprises. A further 44% state that a breach has occurred due to a document not having been disposed of correctly after use. Notably, larger enterprises are more likely to provide home printers that adhere to company security policies (43%) than SMBs (34%). This indicates that the shift to hybrid and remote work models has made the home printing environment a primary and growing source of data loss, highlighting a significant and persistent human factor vulnerability.

- **The average cost of print-related data breaches has fallen.** Compared to 2024, the average cost of a print-related data breach has fallen from over £1m to around £820k. SMBs report an average data loss of £639k, the mid-market £795k and larger enterprises £937k. For all organisations, these figures show that print-related breaches carry a significant financial penalty, reinforcing the need for security investments that align with an organisation's size and risk profile to mitigate these substantial potential losses.

- **AI security concerns loom large.** Overall, 40% are either extremely or very concerned over the bad impacts AI can have in the wrong hands when it comes to their pint infrastructure. However, 41% believe that it is very important that print vendors use machine learning) and AI to identify potential security threats and cyber-attacks, rising from 34% in 2024. This indicates that customers are increasingly looking to vendors to provide intelligent, proactive defence mechanisms against sophisticated cyber threats. For print vendors, this presents a compelling opportunity to differentiate their offerings by integrating and clearly articulating their AI/ML capabilities, transforming their role from hardware providers to essential partners in an enterprise cybersecurity strategy.

- **Familiarity with quantum computing is relatively high.** 52% of respondents state that they are either expertly or very familiar with the concept of quantum printers, and 66% of organisations say it's important that print vendors develop post-quantum or quantum-resistant print devices, indicating a strong willingness to procure and implement such technologies within their fleets. This high level of awareness and readiness for quantum-resistant print devices, even in the nascent stages of quantum computing, signals a forward-thinking approach among ITDMs. It presents a significant, long-term strategic imperative for print vendors to invest in quantum-safe cryptography research and development. The expressed willingness to procure these devices also suggests that early movers in this space could gain a substantial competitive advantage by positioning themselves as future-proof and security-conscious partners.

- **Satisfaction with print security offerings is on an upward trend.** Overall, 40% indicate they are very satisfied, with a further 54% indicating they are quite satisfied. UK respondents are the most satisfied (54% are very satisfied) compared to France (25%). Those using an MPS are most satisfied (46%), along with print security leaders (55%). There is a distinct CIO-CISO satisfaction gap when it comes to print security offerings. While 53% of CIOs report being satisfied, only 25% of CISOs share this sentiment. This suggests that current vendor offerings might not be fully addressing the granular security requirements or advanced threat concerns that CISOs prioritise. A key finding is the clear demand from organisations for more education and guidance from suppliers, particularly at a consultancy level, regarding print security. While satisfaction with print security offerings is on an upward trend, the persistent request for better education and consultancy reveals a significant opportunity for suppliers. This indicates that customers are not just seeking products, but also expertise and strategic guidance to navigate the complexities of their print environments.

Table of Contents

Vendor Landscape

Quocirca's vendor assessment is based on a range of criteria that determine an overall score for strategy and completeness of offering. Each score is based on a scale of 1 to 5, where 1 is weak and 5 is very strong. This evaluation of the print security market is intended as a starting point only. Please note that Quocirca's scoring is based on an unweighted model, although prospective buyers may wish to weight the scores to meet their own specific needs.

Strategy criteria

- **Strategy and vision.** The comprehensiveness of the vendor's print security strategy, how recently the vision and strategy were updated, the quality of its overall value proposition, and its evolutionary vision for print security.
- **Maturity of offerings.** How long the vendor has been active in the market and how developed its offerings are.
- **Partnerships and alliances.** The strength of the vendor's partner and alliance network, especially relating to specialist security skillsets.
- **Market credibility.** The effectiveness of the vendor's initiatives to promote its brand, increase awareness of its service offering, and influence market development. This also includes the clarity, differentiation, and internal/external consistency of the vendor's marketing messages.
- **Channel enablement.** Channel programmes and tools to support partners in building security propositions.
- **Geographic reach.** A vendor's geographical reach, either via direct engagement or through partners or channels.
- **Investment and dedicated resources.** The vendor's investment in its print security portfolio and resources, as well as innovation that will add improvements in approach, processes, or service offerings.

Completeness of offering criteria

- **Breadth and depth of service offering.** The range of services available and consistency across devices, including complementary ones such as business process services and IT services.
- **Hardware security.** How extensive the security designed into the hardware is. What embedded security features are included and how are these are updated.
- **Document security.** How documents are protected at device, user, and application level. What type of user authentication is supported and how digital documents are protected (e.g., encrypted PDF, digital signature, and watermarks).
- **Network security.** Features to ensure the device remains secure on the network it is attached to, including, but not limited to, IP address filtering, MAC filtering, IPv6, and IPSec support.
- **Certification.** Whether the devices have successfully undergone independent security testing and certification, including ISO certification.
- **Security services.** Whether the company offers a portfolio of security services, including security assessment services, proactive monitoring, MPS/secure MPS, and monitoring of home printing.
- **Software integration.** Whether SIEM, content security/DLP, and print management security tools are offered.
- **Vulnerability and remediation.** Vulnerability management and device remediation, firmware updates/installation, configuration setting changes, and remote management.
- **Threat intelligence.** Anomaly detection, alert generation and data collection, and vulnerability management.
- **Application of AI.** How AI and machine learning are used to help with anomaly detection in real-time and the automation of patches and updates. Whether AI is used to ensure data security compliance (e.g., GDPR) when secure and sensitive documents are printed.
- **Analytics and reporting.** User analytics, security analytics, dashboards, and reporting.

The Quocirca Print Security Vendor Landscape graphic represents Quocirca's view of the positioning of vendors in the global print security market (Figure 13). Vendors are categorised as:

- **Leaders.** Vendors with a strong strategic vision and a comprehensive print security product and service offering. Leaders have made significant investments in their hardware, solutions, and services portfolio and demonstrate a strong vision for future strategy.
- **Major players.** Vendors that have established, proven offerings and are continuing to develop their solutions service portfolio. These vendors are most likely to focus on the SMB market with a hardware-centric approach.

Please note that this is intended for guidance only because of varying service offerings for each vendor and regional differences.

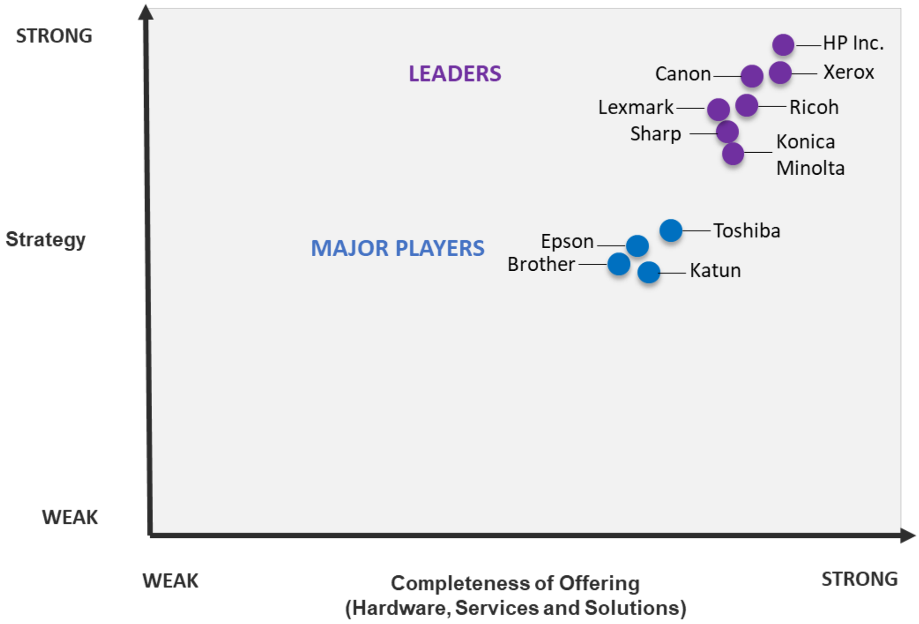

Figure 1. Quocirca Print Security Vendor Landscape, 2025

The Quocirca Vendor Landscape is a graphical representation of Quocirca's opinion of the market and is based on Quocirca's scorecard methodology. This information is provided as a visual representation only and should be combined with other sources to determine the suitability of any vendor. Quocirca does not endorse any vendor, product, or service. Information is based on best available resources and opinions reflect judgment at the time. All opinions are subject to change.

Vendor profile: Ricoh

Quocirca opinion

Ricoh retains its position as a Leader in Quocirca's assessment of the Print Security Landscape in 2025. Ricoh has built on its strong print heritage and expanded its offering to include IT and cloud services, digital workflows, AV technologies, and managed services – all designed with security at the core. Ricoh's secure-by-design approach delivers protection from endpoint to cloud, enabling secured workflows, protected data, and trusted operations across the digital workplace. The company continues to drive innovation through its growing network of Centres of Excellence, which incubate emerging technologies such as IoT, cybersecurity, blockchain, and AI (for example, with the recent acquisition of Natif.ai).

Ricoh implements a comprehensive, multi-layered approach to MFP security deeply integrated within its secure-by-design philosophy, ensuring protection across the entire information lifecycle from the device itself to data in transit and at rest. This foundational security begins with hardened hardware, operating systems, and customised kernels designed to minimise vulnerabilities. Key device-level safeguards include digitally signed firmware updates, the use of Trusted Platform Module (TPM) 2.0 for secure boot and key storage, and machine data encryption.

Logical access is controlled through robust user authentication methods and role-based access controls, ensuring only authorised individuals can operate specific functions. Beyond the physical device, Ricoh's strategy extends to robust network and document security. All data transmitted to and from the MFP is protected using industry-standard encryption protocols such as TLS 1.2/1.3, HTTPS, and IPsec, preventing unauthorised interception. Document confidentiality is maintained through features such as Locked Print (pull-printing), password-protected PDFs, and digital signatures for scanned documents, alongside Unauthorised Copy Control to deter physical duplication. Furthermore, all embedded applications undergo stringent testing and digital signing by Ricoh, preventing the installation of malicious software and ensuring platform integrity.

Ricoh's security commitment is reinforced by its adherence to stringent international standards such as ISO/IEC15408 (Common Criteria) for printing devices and a suite of supporting services. Its cloud-based solutions leverage secure platforms with strong encryption, facilitating secure digital workflows. The effectiveness of this multi-layered approach is independently validated through certifications such as ISO/IEC27017, confirming its adherence to rigorous IT security benchmarks.

Ricoh has opportunities to further enhance its position in the market. Integrating advanced AI into its solutions, as seen with the acquisition of natif.ai, will bolster its document processing and automation capabilities. Additionally, articulating a cohesive security service offering and developing a stronger channel-led security programme will enable Ricoh to provide more consistent and robust security solutions across different regions.

Security strategy

Globally scalable platform
Ricoh's expertise spans process acceleration, IoT resource orchestration, automation, and actionable insights. The company's vision is to unify these elements into a comprehensive Ricoh-developed platform that connects devices, managing digital capture, device management, configuration, and security across offices, co-working spaces, and homes.

By consolidating all capabilities into a single platform, both customers and Ricoh service delivery teams can visualise the entire IT landscape, including print and MPS, from a single dashboard. By creating a unified platform that can manage physical spaces, digital collaboration tools, security, and ESG requirements across multiple locations and different regions, Ricoh will ensure a consistent, high quality experience for global clients.

Cybersecurity expertise
Ricoh has strategically acquired IT services and cybersecurity companies to enhance its portfolio. In 2024, it acquired natif.ai, an AI company specialising in intelligent document processing (IDP). By integrating natif.ai's advanced AI technology, Ricoh is well-positioned to offer more robust and secured document management solutions, helping secure sensitive information throughout its lifecycle.

A key differentiator is Ricoh's CDP (Customer Data Platform) cyber AIOps capability, which facilitates detection of and response to cyber threats, whether they affect a single device or an entire network. CDP's extended security capabilities, such as digital device fingerprinting and threat hunting, enable Ricoh to intercept nefarious activities before they impact device and business performance.

Zero trust
Ricoh's zero trust approach across devices, solutions, and cloud services, ensures robust security across all aspects of the print and document environment and helps organisations build a resilient security posture that can adapt to evolving threats and maintain the integrity of their operations.

Security policy enforcement, micro-segmentation, automation, data classification and protection, end-to-end encryption, user authentication, auditing functionality, and integration with cloud-based identity providers offer comprehensive protection.

Security offerings

Hardware security
New and circular remanufactured Ricoh print devices feature end-to-end security protection and the latest security features, including improved privileged account control, Transport Layer Security (TLS1.3), TPM 2.0, multi-factor authentication, and integration with multiple identity providers. Role-based access controls and end-to-end data encryption safeguard critical information. Features such as authentication secure print release, disabling of device settings, a built-in firewall to limit access to the device, and its Data Overwrite Security System to protect latent data, support typical DLP strategies.

Ricoh MFPs and printers use a digital signature to judge firmware validity. The public key associated with the digital signature is stored in a write-protected, non-volatile memory location. This storage is secured using an encryption key derived from the TPM, ensuring both integrity and confidentiality. Ricoh uses a Trusted Boot procedure that employs two methods to verify the validity of programs/firmware - detection of alterations and validation of digital signatures.

Document security
Software solutions enable customers to create automated rules based on document content or attributes to offer more control over the security of documents and sensitive data. Ricoh devices also support copy protection, and specific items (e.g., money) cannot be scanned/copied. RICOH CloudStream and Streamline NX offer additional security features, such as vulnerability audit services, remote management, and automatic updates for device certificates, settings, and firmware, as well as options for data masking in reports.

Specifically, RICOH CloudStream addresses concerns around document security in the cloud in a number of ways:

- **Regional datacentre storage dependent on customer location.** RICOH CloudStream stores data in regional datacentres according to the customer's location. This improves the responsiveness of data access and enables the customer to comply with legal requirements such as the GDPR.
- **Stored data type.** Application metadata, configuration, job metadata, reporting, and generic user information are stored in a cloud provider's managed SQL database.
- **Data encryption.** Platform data is stored using AES 256 encryption, a robust and widely accepted standard for data security. To further safeguard data, Ricoh leverages multiple technologies to ensure that stored data is encrypted at rest. User passwords are hashed according to industry best practices and encrypted at rest, providing an additional layer of security.

End-of-life device security
To mitigate the risk of data leakage during device disposal, Ricoh devices incorporate storage-level data encryption and a bulk overwrite deletion capability.

For comprehensive data sanitisation, users can choose from multiple secure deletion methods – including the NAS overwrite, US Department of Defense (DoD) 5220.22-M standard, and random pattern overwrite – ensuring data is irrecoverable even after the device is decommissioned.

Ricoh offers a data cleansing service, which provides a proven, complete, certified, and documented process for removing data from end-of-contract printers and MFPs. Its secure disposal service covers all potential sources of information from devices.

Secure predictive maintenance and support

@Remote enables a secure connection for devices to provide full status and service alerts, which is used as part of Ricoh managed services to monitor devices. Ricoh also uses comprehensive fleet management tools – Streamline NX and CloudStream – to monitor and report on devices, which includes services such as automatic updates, advanced monitoring and reporting, policy enforcement, and remediation.

IoT Command Center

Ricoh's IoT Command Center (CC) is an all-in-one, device-agnostic platform designed to provide real-time problem detection, resolution, and actionable insights from connected devices. This enterprise-class, global-capable solution can be deployed as a single- or multi-tenant cloud, hybrid, or on-premise platform and provides a centralised view of a fleet of devices from a single dashboard. AI/machine learning analytics for predictive and anomaly detection enable proactive management and auto-remediation of issues, while traffic data analysis helps identify potential security threats and optimise network performance. The IoT CC also integrates with ServiceNow for ticket generation and recall, streamlining the incident management process, and StreamlineNX, which enhances MFP management and monitoring.

Security assessments

Ricoh print security services provide comprehensive protection for printing and overall platform/information security and are tailored to meet specific customer needs, including regulatory compliance. The company employs advanced techniques such as encryption of network communications and print streams, network user authentication, and a range of administrative counter measures such as closing network ports and proactive device management. Ricoh's Vulnerability Service can be employed to specifically scan Ricoh's print devices and its solutions installed on servers to provide detailed reports on vulnerabilities.

Cloud print security

Solutions that Ricoh deploys as a cloud service for global customers are managed by its ISO 27001-certified Digital Operations Centre (DOC) and Global Security Operations Centre (GSOC). Ricoh cloud print services incorporate zero trust security principles, multi-factor authentication, anti-malware measures, patching, encryption, firewall, and monitoring. The company also offers end-to-end encrypted web service communications (HTTPS), AES encryption for data at rest, data segregation in datacentres, and optional local document storage. Authentication options, including FIDO2, provide end-to-end encryption and robust authentication mechanisms to safeguard sensitive documents. Security is further enhanced with industry-leading remote monitoring and management of device security policies, settings, and certificates and compliance with industry standards such as the GDPR, ISO 27001, SOC 2, WCAG, and ISO/IEC27017.

Access and identity management

Ricoh offers a range of identity management, security, and authentication solutions for businesses, ensuring secure access to Ricoh devices and resources. These solutions include centralised management of device access protocols, multi-factor authentication, single sign-on, and user authentication/access restriction, including options for FIDO2 and password-less authentication. Ricoh also emphasises device security through hardened operating systems, secure printing, remediation services, and data cleansing services.

A wide range of authentication methods are supported:

- **Basic authentication.** Users enter a username and password, which are registered locally in the multifunction printer's address book.

- **User code authentication.** Users enter a code of up to eight digits, which is compared to the registered data in the address book.
- **Windows/LDAP authentication.** Access to Ricoh multifunction printers can be linked with Windows domain controllers and LDAP servers.
- **Card authentication.** Smartcard authentication using an optional card reader.
- **Common Access Card (CAC) authentication.** The Common Access Card is a US Department of Defense specialised ID card-based authentication system designed for government users that must be compliant with Homeland Security Presidential Directive 12 (HSPD-12).
- **Personal Identity Verification (PIV).** Personal Identity Verification is the civilian version of the CAC card.
- **SIPRNet Token authentication solution.** SIPRNet Token is a variation of the CAC ID designed for controlled networks.

Strengths and opportunities

Strengths

- **Globally consistent security strategy.** Ricoh's secure-by-design philosophy ensures that security is a fundamental aspect of its product and service offerings, providing robust and multi-layered protection.
- **Vendor-agnostic security services.** Ricoh’s print security services programme is not limited to Ricoh devices. The company’s offerings for print security vulnerability analysis and remediation support multi-vendor fleets.
- **IoT Command Center.** The IoT CC can monitor and report on any IP-addressable or IoT-native device. This ensures comprehensive coverage and management of diverse device fleets.
- **IT expertise.** Ricoh has expanded its expertise in IT services and cyber and data security through strategic acquisitions.

Opportunities

- **Expand AI/ML security features.** Integrating advanced AI into its solutions will enhance document processing and automation capabilities, providing a competitive edge in the market.
- **Enhancing channel offerings.** Strengthening its channel-led security programme will ensure that Ricoh's security solutions are consistently and effectively delivered across different regions, addressing the diverse needs of its global client base.

Future outlook and recommendations

Quocirca's Print Security Study 2025 strongly suggests that print security is no longer a niche concern but a critical component of an organisation's overall cybersecurity strategy. Organisations that embrace a proactive, comprehensive approach, often through MPS, are significantly more satisfied with their security posture and better protected against the growing threat of print-related data breaches. Suppliers have a clear mandate to guide and enable all organisations towards a print security leader position, emphasising the tangible benefits of robust print security.

It is also apparent from the research that print laggards in particular, have a much lower visibility of what is happening across their print environment. Although they report lower numbers of data breaches and lower costs for any that do happen, this will be down to a lack of actual capability to monitor, measure and account for what is happening. Laggards are far more likely to fail when a breach happens – through the loss of business capability and customer loyalty, combined with the direct and indirect financial losses involved.

Supplier recommendations

Those in the print market must ensure that they can help in the provision, implementation and maintenance of measures to address customers' security needs. This report has covered a list of measures commonly used by those seen to be leaders in the print security environment. Suppliers must look to ensuring that these are provided in an integrated and easy to use manner. Alongside these measures, suppliers should also look to additional value-add capabilities that can play to a customer's needs.

- **Fully integrated systems.** Print security can no longer be viewed in isolation. It must be integrated into an organisation's wider security systems, including identity management and SIEM systems.
- **Security that covers inputs and outputs.** Modern MFPs are increasingly being seen as digitisation devices, with scan capabilities ramping up in usage. Suppliers must look to how data scanned in and extracted is then secured in the rest of its journey.
- **Data security from digitisation to end-of-life.** The security of information cannot end with what happens at the device – either as information is scanned in or printed out. Data that continues to be held on a device must be secured (for example, via encryption), and must be capable of being securely deleted based on security policies and profiles.
- **Helping customers create suitable security policies and procedures.** This cannot just be carried out based on technical viewpoints, nor just via a focus on print. Suppliers must be able to work across boundaries in the technical and business environments, helping customers to understand their security needs and then creating the right environment that can ensure their needs are met.
- **AI needs to be better managed.** AI is still in its early stages, but it is rapidly morphing and maturing into something that offers both great promise and great threat. Suppliers must now be actively leveraging AI to provide customers with greater business value not only through printing and scanning itself, but also through improved security capabilities, as well as in other areas such as device manageability and sustainability. The capability for the print environment to work in harmony with the wider IT security environment to better identify and deal with malicious AI activity must be better addressed through strategic partnerships with others in adjacent security areas.
- **Plan to deal with future issues now.** For some in the supply chain, AI came and hit them when they were unprepared. This has led to a degree of responsive activity, with AI tools and protections being bolted on to existing devices and software, often with variable results. With quantum computing on the horizon, now is the time for OEMs in particular, but in conjunction with ISVs and MSPs, to ensure that they are fully ready for when quantum computing does become more generally available.
- **Create new revenue streams through helping with end-user education.** Quocirca's research shows that respondents need help in gaining a better understanding of the fast-moving security environment. Doing so should be fairly easy for suppliers and could create strong new revenue streams.

Buyer recommendations

For organisations looking to invest in effective print security, navigating the rapidly evolving threat landscape is an increasingly complex and demanding challenge. It is important to build up a better understanding of what the current state of security in the world is, and what is likely to be required in the future. Only from this can a flexible and robust environment be put in place that can help protect against current and future threats. This is highly likely to require bringing in external skills – and these should be found within the leading suppliers in the print environment.

- **Prioritise print security.** Organisations, especially print security followers and laggards, must recognise that printers are network endpoints and potential entry points for cyber-attacks. Print security needs to be elevated on the IT security agenda, moving beyond an afterthought.
- **Invest in comprehensive measures.** Within this report, Quocirca has reported on the measures taken by print security leaders in order to create a stronger security posture. Followers and laggards should aim to implement a wide range of these measures as well as embracing:
  - **Managed print services.** To gain visibility, control and expert management of their print infrastructure, leading to increased confidence and reduced data loss.
  - **Secure print release/pull-printing.** To prevent sensitive documents from sitting unattended and open to unauthorised access.
  - **Strong user authentication.** To ensure only authorised personnel can access specific print functions.
  - **Data encryption.** For data at rest on printer hard drives, and in transit for print and scan job content.
  - **Regular firmware and software updates.** To patch vulnerabilities and gain access to additional functionality and capabilities. Wherever possible, these should be automated to ensure defence against zero-day attacks.
  - **Network segmentation.** To isolate printers from critical network segments, providing an additional layer of security.
  - **Continuous monitoring and auditing.** To detect suspicious activity, with automated actions being taken to remediate or isolate such actions, and notifications being provided to systems and security administrators so that they know what is happening and can take further steps if required.
  - **Employee training.** To foster a security-aware culture around printing. However, user training must be viewed as a minor, first level defence mechanism, users forget things easily, struggle to understand areas where technical descriptions may be required, and it is difficult to maintain levels of education current enough to deal with the changing landscape of the security environment.
- **Proactively assess and address vulnerabilities**. Organisations should conduct regular print security audits to identify weaknesses and then implement solutions to close any gaps. This will require the creation and maintenance of policies and procedures that must be followed to carry out such audits, along with what steps need to be taken to remediate any issues found. These policies and procedures must also cover what needs to happen if a breach occurs.
- **Consider the total cost of poor security.** The cost of a data breach (financial, reputational, operational) far outweighs the investment in proactive print security measures. Organisations need to view print security as a strategic investment, not just an IT expense. However, a full understanding of each individual organisation's security posture needs to be gained.
- **Leverage supplier expertise**. For organisations lacking in-house print and IT security expertise, partnering with suppliers who offer comprehensive security offerings and MPS is essential. This allows them to benefit from specialised knowledge and solutions.
- **AI is already here, and quantum computing is just over the horizon.** Although AI is not the ultimate answer that many thought it would be, it is proving itself to be an effective aid in many areas of business processes. Organisations need to be aware of the darker side of AI, however, particularly when it comes to security, and must question suppliers strongly as to how they are working to counter AI threats. This

must then also be extended to quantum computing - the speed with which AI has moved from advanced rule-based pattern matching through to generative AI systems, points to quantum possibly appearing faster than many think.

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.

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.

Disclaimer:

No part of this document may be reproduced, distributed in any form, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Quocirca. The information contained in this report is for general guidance on matters of interest only. Please note, due to rounding, numbers presented throughout this report may not add up precisely to the totals provided and percentages may not precisely reflect the absolute figures. The information in this report is provided with the understanding that the authors and publishers are not engaged in rendering legal or other professional advice and services. Quocirca is not responsible for any errors, omissions or inaccuracies, or for the results obtained from the use of this report. All information in this report is provided 'as is', with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this report, and without warranty of any kind, express or implied. In no event will Quocirca, its related partnerships or corporations, or its partners, agents or employees be liable to you or anyone else for any decision made or action taken in reliance on this report or for any consequential, special or similar damages, even if advised of the possibility of such damages. Your access and use of this publication are governed by our terms and conditions. Permission is required for quoting any information in this report. Please see our Citation Policy for further details. All product names, logos, brands, trademarks, and registered trademarks mentioned are the property of their respective owners.