Print Security Landscape, 2026

How AI, Identity, and Quantum are reshaping the threat landscape

Print security trends in the US and Europe
Excerpt report: Ricoh
July 2026

QUOCIRCA

Executive summary

Quocirca's Print Security Landscape 2026 study reveals a stark reality: despite heightened awareness of cybersecurity threats, print infrastructure remains a significant vulnerability for many organisations. Two-thirds (67%) of organisations in the UK, France, Germany, and the US have experienced print-related data losses in the past year, and given that 80% remain heavily reliant on printing to support their business operations, this is a risk vector that is not going away. Print infrastructure continues to present an 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 only sustainable response is to increase resilience through a layered, continuously managed print security strategy that protects devices, users, documents, and workflows as part of the wider enterprise security environment.

The research uncovers a widening 'security divide' between organisations that have prioritised print security modernisation and those that lag behind. Organisations classified as security leaders in our Print Security Maturity Index, having implemented at least six areas from a list of security solutions, experience significantly fewer data losses than laggards (56%, compared with 73%), validating the business case for print security investment. Print security leaders are also more likely to report that they are very satisfied with print security capabilities from their supplier (48%) than laggards (23%). This means organisations with more mature print security strategies are not only reducing risk more effectively but also deriving greater value and confidence from their supplier relationships.

Print remains a growing security vulnerability

The proportion experiencing at least one data loss due to a print-related security breach has increased from 56% in 2025 to 67% today. More concerningly, 43% report multiple data losses (compared to 34% a year ago), with 6% suffering 'many' data losses, indicating systemic rather than isolated failures. Given the wide-reaching impacts of data loss – financial costs (on average, each breach costs £1 million), disruption leading to operational delays, reputational and brand damage, and loss of sensitive details including intellectual property – it is essential that organisations address the reality of an evolving threat for which there is no easy 'silver bullet' solution.

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. The role for providers to support and enable this process is clear, and the lack of confidence many customers profess, especially with regard to hybrid and home printing, suggests a strong appetite for guidance.

Mixed-fleet environments continue to present a risk vector

Mixed fleets are becoming more common. Quocirca's research finds that 64% of respondents are currently operating a multivendor fleet (a rise from 59% in 2025), with 36% operating a standardised, single-vendor fleet (down from 41%). Organisations reliant on mixed fleets and those with older 'legacy' print devices face a range of security risks. 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. Data loss is slightly more common among those with more complex environments (69% compared to 64% among those with standardised fleets), with 45% of those with mixed fleets reporting two or more incidents (compared to 37% of those with single-vendor fleets).

Identity is becoming central to print security

The findings underline the critical role of identity in closing print security gaps. Integration between user identity management platforms, such as Active Directory and Azure AD, and print infrastructure is now seen as a security priority: 41% say this is extremely important, up from 34% in 2024, while a further 43% say it is very important. This rises to 52% among print security leaders, highlighting how more mature organisations recognise identity as foundational to access control. Secure release, mandatory authentication, cloud identity integration, and zero

trust controls help ensure only authorised users can print, scan, or release sensitive documents, connecting users, devices, and documents securely.

Widespread AI integration presents both risk and reassurance

AI creates both concern and opportunity. Organisations are highly alert to AI-driven attacks, with 54% very or extremely concerned, while 47% believe agentic AI represents a threat for which they are not yet prepared. At the same time, the role of AI and machine learning in strengthening print security is strongly recognised, with 85% saying it is very or somewhat important that suppliers develop these capabilities. Integrating AI-driven security and preparing for quantum-safe transitions are therefore becoming strategic imperatives. By helping customers navigate these emerging risks, MPS providers and the wider print supply chain have a clear opportunity to differentiate through proactive guidance, intelligent threat detection, and security-led managed services.

This report highlights key market trends in print security services and solutions and includes a vendor landscape assessing print security offerings from leading print vendors. The vendors included in this report are Brother, Canon, HP, Konica Minolta, Ricoh, Sharp, Toshiba, and Xerox.

Key findings

- **Print manufacturers continue to advance their security offerings.** Quocirca's vendor assessment reveals strong momentum among the leading OEMs, with security increasingly positioned as an endpoint, identity, and workflow discipline rather than a device feature set. HP stands out for its zero trust print architecture, hardware-enforced protection, and post-quantum readiness. Xerox offers a broad, integrated portfolio spanning device, fleet, user, workflow, and content security, strengthened by its Lexmark acquisition. Canon is investing in layered controls, secure-by-design devices, and machine learning to reduce configuration risk. Konica Minolta is advancing cloud-based governance through Shield Guard, independent assurance, and Microsoft-aligned cloud print. Ricoh emphasises managed services, assessment-led remediation, and device-agnostic fleet visibility, while Sharp combines advanced hardware security with IT-led cybersecurity services, SOC capability, and SME-focused security education.

- **Print security remains under-prioritised despite continued reliance.** While print remains embedded in business operations (80% describe their organisation as reliant on print to support their activities), only 31% of respondents identify office print infrastructure as a top security risk, ranking it seventh behind wider IT security concerns such as cloud, AI, and email. This gap means many organisations may be underestimating the exposure created by print endpoints, print servers, and document workflows, even as they continue to depend on them for regulated and document-heavy processes. For MPS providers, this creates a clear opportunity to raise awareness, quantify risk, and position print security as an integral part of broader cyber resilience, compliance, and data protection strategies.

- **Print driver deployment is an overlooked security exposure.** Almost a third (31%) cite outdated drivers as a risk, while 28% say vendor-provided drivers may introduce vulnerabilities. These risks are compounded by the challenge of integrating print drivers with cloud identity management and zero trust security frameworks, cited by 34% of respondents. Emerging approaches such as Windows Protected Print highlight the direction of travel towards more secure, driverless print architectures, but adoption remains early and will require careful migration support. Without strong controls, print dependence becomes a larger security issue, particularly across mixed fleets and distributed environments. This creates an opportunity for MPS providers to reduce complexity through secure driver management, modern print architecture guidance, and stronger policy-led controls.

- **Multivendor fleets face higher print security pressure.** AI-driven cyber threats are the top print infrastructure security concern, with 31% of respondents commenting on this risk, rising to 40% in the UK. The pressure is greater among multivendor fleet users, who are more likely than those with standardised fleets to identify AI-driven threats (33%, compared with 28%), firmware and hardware vulnerability management (30%, compared with 25%), and insider threats (29%, compared with 21%). This suggests that mixed fleets create more complexity and control gaps than standardised environments, increasing the need for consistent security policies, stronger fleet visibility, and expert support from MPS providers.

- **Print-related data loss remains widespread and costly.** Two-thirds (67%) of organisations report at least one print-related breach in the last year. The average cost of a print-related data breach now exceeds £1 million, underlining the financial exposure created by unsecured print infrastructure and the value of comprehensive print security controls. Print security maturity has a measurable impact: print security leaders report lower data loss rates (56%) than followers (72%) and laggards (73%), demonstrating the value of comprehensive print security controls.

- **A range of measures are in place to secure print infrastructure, but there are significant gaps for most.** Secure pull printing is now used by 51% of organisations and has become the most universal policy, but, as with most measures, this is led by larger firms, and SMBs and midmarket companies are likely to be leaving their systems exposed. Zero trust architecture is slightly less adopted than in 2025 (just 33% report using it, compared to 37% previously, but led, as last year, by large organisations and MPS customers). For providers, the opportunity is to help customers close maturity gaps through assessment-led services, secure architecture guidance, and managed controls that make advanced print security easier to adopt.

- **Identity integration is becoming foundational to print security.** As print environments move further into cloud and hybrid architectures, user identity is becoming the control layer that connects people, devices, and documents securely. Overall, 41% say integrating identity management platforms such as Active Directory and Azure AD with print infrastructure is extremely important, up from 34% in 2024, while a further 43% say it is very important. This rises to 52% among print security leaders, showing that more mature organisations increasingly view identity-led access control, secure release, and cloud identity integration as essential to reducing print-related exposure.
- **AI is reshaping print security as both threat and defence.** Almost half (49%) of organisations are extremely or very concerned that AI will be used to create more sophisticated and evasive print-related threats, up from 40% in 2025. Security leaders show heightened concern, reflecting greater awareness of emerging risks and more frequent scrutiny of the threat landscape. At the same time, expectations for AI-enabled protection are rising quickly: 55% now consider it very important that providers use AI and machine learning to identify potential security threats and cyberattacks, compared with 41% in 2025 and 34% in 2024. As risk awareness increases, suppliers have a clear opportunity to differentiate through intelligent threat detection, automated remediation, and proactive security guidance.
- **Quantum resilience is moving onto the print security agenda.** Over half (57%) of organisations say quantum-resilient security planning is very important, with a further 30% considering it somewhat important. The issue is most pressing among US and UK organisations, large enterprises, finance firms, and print security leaders, indicating that more security-mature buyers are already considering how print infrastructure fits into wider cryptographic modernisation plans. While print-specific quantum threats may not be immediate, suppliers have an opportunity to provide clear post-quantum roadmaps, guidance on device refresh planning, and education for less mature customers.
- **The security divide creates a clear call to action.** Across the findings, the pattern is consistent: organisations with a more mature, proactive approach to print security are more likely to use managed print services, report higher satisfaction with their security posture, and experience fewer print-related data breaches. Those that treat print as part of the wider cybersecurity environment experience stronger outcomes, while those that leave print outside core security, identity, cloud, and compliance programmes remain more exposed. Buyers should move from reactive controls to continuous governance, while print vendors should help close the divide through assessment-led services, identity controls, fleet visibility, AI-enabled protection, and future-ready security roadmaps.

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 vendor positioning in the global print security market (Figure 11). 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 and services 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.

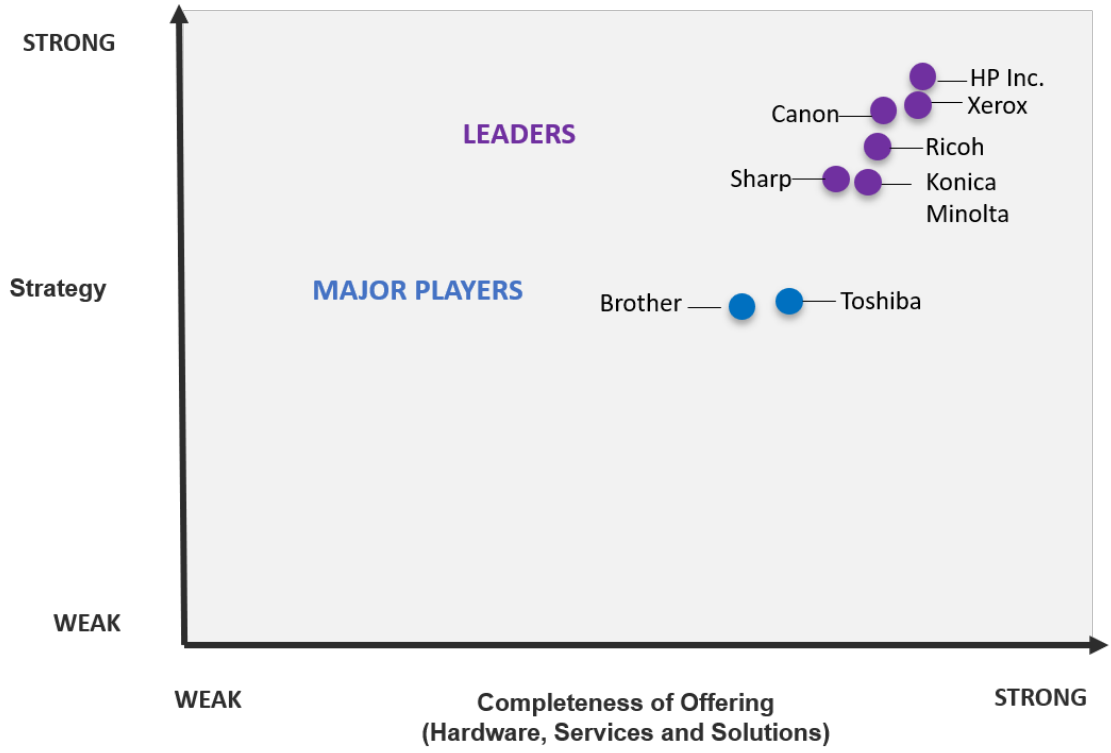

Figure 1. Quocirca Print Security Vendor Landscape, 2026

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.

Recommendations

Supplier recommendations

Suppliers across the print ecosystem should treat security as the defining basis of market differentiation. The findings show that customers face rising levels of print-related data loss, growing pressure from AI-enabled threats, uneven maturity across identity and zero trust adoption, and increasing complexity in mixed and distributed fleets. The supplier opportunity is therefore to help organisations move decisively from fragmented controls to measurable, continuously governed print security outcomes.

- **Lead with security outcomes, not feature checklists.** Suppliers should position print security around measurable risk reduction, resilience, and compliance outcomes. Certifications, zero trust alignment, firmware integrity, secure release, identity integration, and automated remediation must be translated into clear business value: fewer breaches, lower operational disruption, stronger audit readiness, and greater confidence in print as a managed endpoint category.
- **Address fleet complexity as a strategic security problem.** Mixed and legacy fleets remain a persistent source of risk through inconsistent configuration, uneven patching, and fragmented management. Suppliers should offer clearer paths to fleet-wide visibility, policy enforcement, and remediation across heterogeneous environments while also articulating the security benefits of standardisation where this is operationally and commercially realistic.
- **Make AI and quantum readiness credible and actionable.** Customer concern about AI-enabled attacks is rising quickly, while quantum resilience is moving onto the planning agenda for more mature buyers. Suppliers should publish practical roadmaps that explain how AI will be used for anomaly detection, automated remediation, and content protection and how post-quantum cryptography will be introduced across devices, firmware, certificates, and secure communications.
- **Elevate education into a core security service.** Many organisations still underestimate print as a security exposure, particularly in hybrid, home, and midmarket environments. Suppliers should provide structured education, assessment tools, maturity benchmarking, and executive-level guidance that helps customers understand their exposure, prioritise investment, and embed print security within broader cyber resilience programmes.
- **Reframe managed print around continuous security governance.** MPS and managed service propositions should move beyond device availability and cost control to encompass assessment, configuration management, patching, compliance reporting, incident response, and policy lifecycle management. Security-led managed print creates a stronger value proposition and supports longer-term, higher-trust customer relationships.
- **Prioritise segments with the greatest exposure and weakest maturity.** Midmarket organisations, business and professional services firms, retail organisations, and customers operating complex multivendor fleets show elevated risk indicators. Suppliers should tailor propositions for these segments with packaged assessments, rapid remediation programmes, identity-led secure print controls, and pragmatic migration plans that reduce implementation friction.
- **Integrate print security into enterprise security operations.** Suppliers should strengthen SIEM, SOC, identity, DLP, and vulnerability management integration so print events are visible, actionable, and governed alongside other endpoint and cloud risks. The market will increasingly reward providers that can deliver event taxonomies, response playbooks, compliance dashboards, and evidence of reduced time to detect and remediate print-related exposures.

Buyer recommendations

Buyers should treat print infrastructure as key element of the enterprise attack surface. Print-related data loss is widespread, costly, and increasingly linked to maturity gaps in identity, fleet governance, incident response and continuous monitoring. Organisations that act now to bring print into mainstream cybersecurity, cloud, and compliance programmes will be better positioned to reduce exposure, improve resilience and extract greater value from supplier relationships.

- **Elevate print security to the enterprise risk agenda.** Printers and MFPs should be managed as networked endpoints that process sensitive data, connect to identity systems, and interact with cloud workflows. Buyers should ensure print security is represented in cybersecurity governance, risk registers, compliance reviews, and endpoint security planning rather than being treated as an operational print management issue.
- **Build a layered control model based on maturity, not minimum compliance.** The lower breach rates among print security leaders demonstrate the value of implementing multiple reinforcing controls. Buyers should prioritise formal risk assessments, secure release, mandatory authentication, incident response processes, DLP, SIEM integration, firmware governance, zero trust alignment, and reporting. The objective should be continuous resilience, not isolated technology deployment.
- **Establish continuous assessment and remediation.** Print security audits should not be occasional exercises. Buyers should maintain an up-to-date view of device configurations, firmware status, driver exposure, authentication coverage, print server dependencies, cloud print controls, and home or hybrid worker risks. Findings should feed directly into documented remediation plans, ownership models, and incident response procedures.
- **Quantify the cost of inaction.** With the average print-related breach now exceeding £1 million, poor print security should be evaluated as a business risk rather than a discretionary IT cost. Buyers should assess the financial, operational, regulatory, and reputational impact of data loss and use this analysis to justify investment in proactive controls, managed services, and fleet modernisation.
- **Prepare for AI-driven threats and post-quantum transition.** Buyers should challenge suppliers on how AI is being used to detect anomalies, protect content, automate remediation, and strengthen security operations. They should also assess cryptographic exposure across print devices, firmware, certificates, secure communications, and document workflows, aligning future device refresh plans with wider post-quantum security roadmaps. The priority is structured preparation rather than wholesale replacement, so print infrastructure is not left behind as enterprise cryptographic modernisation accelerates.

Vendor profile: Ricoh

Quocirca opinion

Ricoh is positioned as a leader in Quocirca's Print Security 2026 Vendor Assessment, reflecting the breadth of its device security controls, its continued shift toward platform-based management, and its emphasis on operationalising security through assessment and managed services.

Ricoh continues to develop its print security proposition in line with enterprise priorities for hybrid work, cloud adoption, and stronger cyber resilience across a growing mix of endpoints. For many organisations, printers and MFPs remain a persistent blind spot, often managed outside the core security stack while still holding credentials, processing sensitive documents, and connecting into segmented networks. Ricoh's positioning reflects an understanding of this challenge, combining baseline device controls with governance, assessment, and ongoing service delivery to support customers that want print security to be treated as an operational discipline rather than a one-time configuration exercise.

A key feature of Ricoh's approach is its focus on operationalisation through managed services, built around a six-phase lifecycle that covers discovery, assessment, planning, remediation, metrics and reporting, and maintenance. This structured methodology aligns with how larger organisations typically manage other security domains, such as endpoint posture or vulnerability management, and can provide a clearer governance framework for distributed fleets and multivendor environments. Ricoh's emphasis on metrics and reporting also supports internal accountability, particularly in sectors where auditability and evidence of control implementation are required. The challenge for customers is often less about enabling controls and more about maintaining them through organisational change, firmware evolution, and ongoing shifts in user behaviour. Ricoh's lifecycle framing is well suited to these realities.

Ricoh has strengthened its capability base through acquisitions and partnerships that extend beyond traditional print. The acquisition of MTI Technology in Europe enhances its cyber and data security services footprint, while natif.ai supports intelligent document processing capabilities that can be embedded into workflow solutions such as DocuWare and RICOH Streamline NX. Ricoh also maintains a broad partner ecosystem across identity, networking, endpoint security, and IT service management platforms. In Quocirca's view, this breadth can add value where integration is delivered consistently and repeatably, rather than relying on bespoke projects. As security teams increasingly expect print infrastructure to integrate with established processes for identity, monitoring, and incident handling, Ricoh's ability to provide pre-built integrations and clear operating models will be a key determinant of differentiation.

Ricoh's strengths sit primarily in the breadth of its managed services-led approach and in the development of platform capabilities that help customers maintain policy and visibility across distributed fleets. The market is increasingly split between buyers that seek deep, embedded threat detection on the device and those that prioritise governance, compliance, and operational control across a heterogeneous estate. Ricoh is well aligned with the latter, with a clear emphasis on lifecycle services, policy enforcement, and integration with existing IT management processes.

Ricoh's portfolio and messaging suggest it is targeting organisations that want to consolidate supplier relationships and reduce the fragmentation between print operations and broader IT and security management. Its device-agnostic monitoring capabilities and security services model support this ambition, particularly for enterprises with diverse fleets and limited internal resources to manage configuration drift and patch hygiene at scale. Buyers that prioritise deep, device-resident threat detection will need to assess the balance between preventative controls, telemetry export, and services-driven response. Ricoh's roadmap, including planned AI-enabled DLP in Streamline NX, indicates a shift toward more proactive policy enforcement and content-led security, but the maturity of these capabilities will be an important factor in near-term evaluations.

Security strategy

Overview and pillars

Ricoh positions print security within a wider digital workplace and information security strategy, with emphasis on security by design across devices, software, and services. Its strategy is framed around three pillars, product

and application security, infrastructure security, and organisational governance and management. This is a practical structure, as it maps well to the way many enterprises organise responsibilities across IT operations, information security, and compliance. In particular, Ricoh's focus on governance helps elevate print security from a set of technical features to a managed capability that can be aligned with internal policy, risk appetite, and audit requirements.

Device security controls

At the device layer, Ricoh highlights controls that are increasingly expected for enterprise endpoints, including role-based access control, support for multi-factor authentication, encryption for data in transit, and firmware and application signing. Support for TLS 1.3 and TPM 2.0 contributes to a stronger hardware-rooted security posture, supporting trusted boot and improved key protection. Ricoh also emphasises secure lifecycle measures such as HDD overwrite and certified end-of-life data cleansing services, which remain important where devices are leased, redeployed, or decommissioned under strict data handling rules. The presence of these capabilities is important, but Quocirca notes that customer outcomes depend on the ease of enforcing consistent policy across fleets, including legacy models and devices outside the primary vendor environment.

Assessment and managed services

Ricoh's services-led approach centres on vulnerability assessment, device hardening, and ongoing posture management. The assessment process focuses on identifying missing patches, outdated software versions, open ports, exposed services, and non-compliant configuration settings, with findings translated into remediation actions. This aligns with the direction of travel in the print security market, as organisations increasingly expect printers to be governed like other managed endpoints. Ricoh's inclusion of planning, metrics, and maintenance phases supports repeatable governance and continuous improvement. It also reflects the reality that print environments are subject to frequent change, including firmware updates, new workflow applications, and evolving identity policies. A key consideration for buyers is the clarity of responsibility boundaries between Ricoh, internal IT, and any third-party managed service provider, particularly where security controls span network segmentation, identity, and cloud print.

Zero trust alignment and deployment models

Ricoh's adoption of zero trust principles focuses on strong authentication, policy enforcement, segmentation, and auditing across print and capture workflows. It supports multiple deployment models for secure print, including offline direct print, client-based secure print, and cloud-based secure print, which is relevant for hybrid work patterns and more decentralised office footprints. Quocirca sees particular value in the ability to apply consistent controls across these modes, as hybrid environments can otherwise introduce uneven policy coverage and logging gaps. Ricoh also references micro-segmentation and modern authentication approaches, including integration with multiple identity providers and standards such as OpenID Connect. While these are positive signals, enterprises will typically require clear guidance on reference architectures, recommended segmentation patterns, and log mapping into security operations processes to minimise operational overhead.

Secure engineering and DevSecOps

Ricoh's investment in DevSecOps and secure engineering practices is also relevant as print security increasingly depends on the cadence and quality of software delivery. The shift towards cloud print services and workflow platforms increases the importance of secure development, vulnerability handling, and patch deployment processes across both device firmware and associated applications. Ricoh cites ongoing training and reorganisation around DevSecOps practices, which, if executed consistently, should support faster remediation cycles and a more standardised approach to secure coding and release governance.

Operational oversight and SOC/ITSM integration

From an operational perspective, the market is moving towards clearer expectations for how print infrastructure integrates into enterprise security oversight, including vulnerability management, change control, and incident response. Ricoh's alignment with IT service management platforms and its focus on monitoring and reporting provide a foundation for this, particularly where print is managed as part of wider workplace services. Quocirca expects buyers to probe how Ricoh defines and prioritises security events, how remediation actions are executed and verified, and how responsibilities are governed across customer and supplier teams.

Product and software security

Fleet visibility and policy automation

Ricoh's product and software security direction is increasingly centred on fleet visibility, policy enforcement, and operational automation. Workplace Intelligence and the IoT Command Center provide device- and vendor-agnostic monitoring and analytics across distributed fleets, with capabilities that include configuration drift management, batch policy updates, and firmware orchestration. This is relevant as customers look to reduce the cost of maintaining secure configurations over time, particularly across mixed fleets and geographically dispersed estates. The ability to standardise baseline configurations and track compliance against policy templates is an important enabler of security governance, although customers should evaluate how granular the policy controls are across different device types and how exceptions are handled.

Monitoring, logging, and SIEM considerations

For monitoring and reporting, Ricoh supports device and user activity logging and can transfer operational and audit log information. Ricoh's @Remote capability underpins managed services monitoring through a secure connection for device status and service alerts. From an analyst perspective, the strategic question is the extent to which print security telemetry can be normalised into SOC workflows, enabling meaningful correlation with identity events, endpoint alerts, and network signals. Syslog export is often a necessary baseline, but SOC teams typically seek higher-fidelity, security-relevant event models alongside clear guidance on what constitutes actionable incidents versus operational noise. Ricoh's direction towards broader platform analytics strengthens this foundation, particularly where monitoring can support continuous compliance reporting and faster detection of configuration drift.

Authentication and identity integration

Ricoh offers a broad set of authentication options, including PIN, smartphone-based authentication, biometric methods, FIDO2, and PKI smart cards. Delivery is supported through a combination of device capabilities, print management solutions, and badge reader partnerships. Ricoh also references support for modern identity approaches such as OpenID Connect and integration with multiple identity providers. This breadth is important as enterprises standardise on modern identity, passwordless initiatives, and multi-factor enforcement across endpoints. In Quocirca's view, Ricoh's challenge is to make this breadth easier to adopt in practice, with clear guidance on which authentication approaches are most appropriate for different risk profiles, user journeys, and deployment models, including remote worker scenarios and shared spaces.

Cloud print and remote worker security

Across cloud print and remote worker scenarios, Ricoh highlights encryption at the protocol and application layers, including IPPS, TLS 1.2, and TLS 1.3, and stronger encryption within RICOH Streamline NX. RICOH Streamline NX and RICOH CloudStream provide features that support a zero trust architecture. Quocirca notes that as print management moves into cloud architectures, buyers increasingly evaluate security through the lens of shared responsibility, tenant isolation, logging, and integration with identity and conditional access policies. Ricoh's platform approach provides a pathway to meet these expectations, although the maturity of governance controls and the depth of integration into broader cloud security tooling will be key selection criteria.

Lifecycle hardening, patching, and certificates

Ricoh's fleet management and automation capabilities also support security outcomes through ongoing device hardening. Features such as automated firmware updates, remote configuration, and policy compliance checking can reduce reliance on manual intervention, which is often a source of inconsistency in large estates. Ricoh highlights mechanisms such as Automatic Remote Firmware Update and Always Current Technology, alongside platform-based monitoring of firmware versions against reference baselines. Certificate enrolment and management capabilities further support enterprise requirements for encrypted communications and device trust. As regulatory pressure increases around product security and patch hygiene, these lifecycle capabilities are likely to become more visible differentiators in competitive evaluations.

Content security and DLP roadmap

On content security, Ricoh's current capabilities emphasise rules-based controls, device-level safeguards, and workflow governance through its software portfolio. It also references copy protection controls on devices and configurable rules based on document attributes or content signals. A significant stated development is the

planned AI and machine learning enabled DLP service within Streamline NX, intended to automate classification and apply rule-based actions such as allow, deny, review, archive, and notification workflows. If delivered with strong governance controls, including administrative oversight, reporting, and tuning mechanisms, this could address a key market requirement, which is reducing reliance on user behaviour while applying consistent policy at the point of print. Buyers will expect clarity on how classification decisions are made, how false positives are handled, and how the service integrates with existing information protection and DLP tooling.

Partnerships

Ricoh's print security proposition is reinforced by an expanding partner ecosystem that spans identity, networking, endpoint security, and IT service management. This partner-led approach is increasingly important as enterprises look to pull-print infrastructure into established operating models for access control, vulnerability management, monitoring, and incident response, rather than managing print as an isolated domain.

Strengths and opportunities

Strengths

- **Global device-agnostic approach to customer security support**: Through its Technology Centres and Security Services, Ricoh offers support in 200 countries and territories. Ricoh Managed Services are device-agnostic for print security vulnerability analysis and remediation.
- **Expanding platform-based visibility and automation.** Workplace Intelligence and the IoT Command Center extend monitoring and remediation workflows across diverse device estates and provide a basis for drift management and policy enforcement at scale.
- **Security for remanufactured devices.** Ricoh explicitly assures that its circular remanufactured models achieve the same security standards as new products.
- **Investment in workflow and AI.** The natif.ai acquisition and the roadmap for AI-enabled DLP within Streamline NX strengthen Ricoh's positioning around secure workflows and information-centric security beyond the device layer.

Opportunities

- **Continue developing DevSecOps focus.** Ricoh recognises that print infrastructure security is increasingly linked to secure software development and delivery. It is adopting DevSecOps principles to improve collaboration between development, security, and operations teams to ensure code is delivered quickly and securely across its print and workplace platforms.
- **Accelerate productisation of AI-enabled DLP.** The planned Streamline NX DLP service will benefit from strong governance features, including policy design guidance, tuning, explainability, audit reporting, and clear privacy and data handling controls.
- **Sharpen differentiation in cloud print security.** As cloud print adoption increases, Ricoh can further articulate its approach to tenant isolation, shared responsibility, resilience, and cloud governance to support risk and compliance evaluation.

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's analysis spans the technologies and market forces shaping the future workplace, including cloud services, security, artificial intelligence, managed print services (MPS), sustainability, and the future of work. Its research helps technology vendors, channel partners, and enterprise buyers understand market disruption, identify growth opportunities, and develop strategies for digital transformation.

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.