Print Security Landscape, 2026

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

Print security trends in the US and Europe
Excerpt report: MPS Monitor
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 IT security as both threat and defence.** Almost half (49%) of organisations are extremely or very concerned that AI will create further security risks to IT infrastructure as a whole. More (54%) are concerned that AI may be leveraged to create more sophisticated 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 profile: MPS Monitor

Quocirca opinion

MPS Monitor is strengthening its security credentials by embedding security controls into its cloud platform and the agent layer that connects customer environments to its service. Its approach is aligned with established information security principles, with a strong emphasis on independently validated governance through ISO/IEC 27001 and SOC 2 Type 2, complemented by CSA STAR Level 2 and GDPR alignment. For customers and channel partners looking for a SaaS platform to support managed print services at scale, this focus on assurance, regular testing, and secure software delivery is increasingly important as MPS providers come under greater scrutiny from enterprise security teams.

MPS Monitor's strongest differentiator is the consistency of its security-by-default and by-design posture across governance, monitoring, and remediation. The company highlights cloud-native logging and analytics, continuous vulnerability scanning, and structured incident response. The platform's use of secure identity integration, including SSO, MFA, and role-based access control, supports organisations seeking to extend zero trust principles to operational tooling used by IT and print service providers. However, beyond device posture and access controls, MPS Monitor's security value will depend on how effectively it can translate security telemetry into actionable insights for both dealers and end customers, particularly where fleets are multivendor and operational responsibility is shared.

Security strategy

MPS Monitor positions security as a core design requirement for its SaaS platform and associated Data Collection Agents (DCAs), underpinned by an Information Security Management System aligned with ISO/IEC 27001 and audited against SOC 2 Type 2 and CSA STAR Level 2. This governance model is supported by ongoing improvement processes, with regular external testing and documented incident response procedures for containment, investigation, customer communication, and patch deployment.

For customers, the practical value lies in consistent monitoring across the platform and the distributed DCA footprint. DCAs use secure communications and are designed for resilient telemetry collection, which is important in managed print environments where service providers need reliable visibility across multiple customer sites and networks.

In 2025, MPS Monitor increased its engagement with external specialists for penetration testing, red-team exercises, and secure code reviews, alongside enhancements to vulnerability management, log analytics, and incident response capabilities. This is a pragmatic focus on operational security maturity, particularly as SaaS platforms supporting fleet monitoring and remote access can become attractive targets for attackers.

Product and software security

MPS Monitor's security approach spans platform access controls, secure software development practices, and support for device security posture management on selected print vendors. The platform's emphasis on logging and analytics is designed to provide operational visibility for service providers managing distributed fleets.

- **Compliance and assurance.** Alignment with ISO/IEC 27001, SOC 2 Type 2, CSA STAR Level 2, and GDPR requirements, supported by regular independent assessments.
- **Secure cloud operations.** Centralised logging, real-time event analytics, and continuous vulnerability scanning, supplemented by periodic external penetration testing and red-team exercises.
- **Secure development and supply chain controls.** Security-by-design and security-by-default development practices, with static and dynamic testing, external code reviews for DCA releases, controlled deployment processes, and digital signing of software components.
- **Data Collection Agent security.** Secure communications using HTTPS/TLS 1.3 and support for SNMPv3 encryption. The company also references modern frameworks such as gRPC and MQTT via Azure IoT Hub, with multi-platform support across Windows, macOS, Linux, and embedded platforms.

- **Identity and access management.** SSO integration with enterprise identity providers and MFA support, alongside role-based access control to align permissions with organisational roles.
- **Device posture and compliance management.** Device discovery and inventory, firmware risk identification, policy-based configuration management, and automated remediation and compliance monitoring on selected brands.
- **Controlled remote device access.** Device Web Access capability to interact with device web interfaces using temporary sessions with monitoring and logging, protected by identity integration and MFA.

MPS Monitor works with external cybersecurity specialists for independent validation and integrates with enterprise identity providers such as Microsoft Entra ID and Okta.

Future strategy

MPS Monitor's near-term security roadmap focuses on extending continuous assurance through further independent testing, maintaining alignment with evolving standards such as ISO/IEC 27001 updates, and continued investment in cloud resilience. It also plans to enhance monitoring, analytics, and automation to improve visibility and accelerate response. Quocirca expects increasing customer demand for demonstrable controls around third-party risk and operational resilience, which should keep pressure on MPS Monitor to formalise security metrics and evidence that can be shared with both dealers and end-customer security stakeholders.

Strengths and opportunities

Strengths

- **Security governance with independent validation.** Certification and audit posture provide customers and partners with assurance that controls are measured and maintained over time.
- **Security focus on the agent layer.** Strong attention to DCA security, including secure communications, release validation, and external testing, is relevant given the agent's proximity to customer networks.
- **Identity-centric access controls.** SSO, MFA, and RBAC alignment supports enterprise access governance and helps reduce reliance on local credentials.
- **Operational security maturity.** Regular penetration testing, red-team exercises, and continuous scanning indicate a shift toward continuous assurance rather than point-in-time compliance.

Opportunities

- **Clearer articulation of analytics-driven threat detection.** The company references AI-driven capabilities but would benefit from more explicit detail on use cases, model governance, and measurable outcomes for detection and response in customer environments.
- **Greater integration into enterprise security operations.** With SIEM integration currently indicated as not supported, there is an opportunity to strengthen interoperability with security tooling used by CISOs, particularly for larger, regulated customers.
- **Broader and more consistent device security posture coverage.** Capabilities for policy enforcement and compliance monitoring are positioned for selected vendors. Expanding the breadth and transparency of coverage across multivendor fleets would improve applicability for larger MPS environments.

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.

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.