Print Security Landscape, 2025

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

Print security trends in the US and Europe
Excerpt report: MPS Monitor
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

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.

Vendor profile: MPS Monitor

Quocirca opinion

MPS Monitor is a well-established provider of vendor-agnostic print fleet management solutions, with a core differentiation built around its robust technology, comprehensive feature-set, and strong emphasis on security and data integrity. MPS Monitor has adopted a proactive and comprehensive approach to security and data protection. The company is continuously assessed and certified by independent third-party organisations and continues to strengthen its security framework through regular audits, ensuring ongoing reliability and protection against evolving cyber threats.

MPS Monitor technology enables office equipment dealers, MPS providers and aftermarket supplies resellers, to remotely monitor and manage diverse print fleets for their end customers. This is achieved through highly reliable data collection agents (DCAs), including multi-platform support (Windows, Mac, XOA, HyPAS, FutureSmart, Raspberry), and innovative technologies like DCA clustering for redundancy, ensuring continuous and accurate data flow from devices.

MPS Monitor has a strong commitment to security and compliance, underscored by certifications like SOC 2 Type 2, CSA Star Level 2, and ISO/IEC 27001. It emphasises a security-by-default and by-design approach throughout its platform, protecting sensitive customer data and mitigating the risk of print devices and DCAs being used as attack vectors. Furthermore, its deep integration with key industry platforms like HP Smart Device Services (SDS) provides seamless functionality, user management, job tracking, and reporting, all from a single cloud portal. Integration with Microsoft Power BI, provides users with granular insights into print costs, usage patterns, and predictive analytics without requiring extensive technical knowledge.

Security strategy

Comprehensive approach to security

MPS Monitor continues to proactively invest in cybersecurity. In 2024, it significantly increased security testing and monitoring activities, utilising both internal resources and specialised external security firms. Key initiatives undertaken include penetration tests, code reviews, incident response exercises, vulnerability assessments, disaster recovery testing, and log analytics monitoring.

The company reports that during the last penetration tests performed by DOT Security's red team, MPS Monitor's portal applications, distributed architecture, and surrounding infrastructure demonstrated exceptional resilience, withstanding some of the most common and sophisticated attacks targeting modern web platforms and the organisations that develop them. In addition, a review of the data collection agent's latest code was performed, and the auditor determined that the source code was 'skilfully crafted, well-documented and securely built'.

Code reviews

Before every DCA code release, an external security firm conducts a code review. The code review activity also includes testing both the source code and the compiled components against a pre-defined security checklist which ensures that the package being released complies with the stringent security requirements set for the DCA component. The code testing activities are performed by adopting a hybrid approach that combines a static code analysis phase with a dynamic application analysis. This approach allows to deliver a high coverage over the attack surface and to discover both superficial vulnerabilities as well as problems that reside deeper in the application logic and therefore not immediately identifiable.

Security standards

The company has achieved globally recognised security standards including ISO 27001, SOC 2 Type 2 and CSA STAR Level 2, and reaffirmed its commitment to security in 2024 by successfully completing compliance audits for these security standards.

Security features

MPS Monitor provides a cloud-native SaaS solution for remote monitoring and management of printers, multifunctional devices, Zebra label printers and HP large-format printers. Currently, the MPS Monitor platform connects over 2.5 million devices across 75 countries, with more than 450,000 DCAs actively operating in customers' networks, managing over 350,000 end customers.

Robust security controls

MPS Monitor has adopted a security-by-design and by default development model and applies robust security controls throughout the software development and deployment process. These include version control, file integrity monitoring to permit only authorised changes, separate testing environments for quality assurance and user acceptance, and digital signatures for all components within a release package. In addition, enhanced user authentication security is achieved through features like single sign-on integration and multi-factor authentication.

AI-powered chatbot

In 2024, MPS Monitor introduced an AI-powered chatbot which supports dealers by providing instant assistance and guidance on specific features, troubleshooting tips, as well as addressing security concerns and assisting in the completion of security questionnaires.

Secure back-end cloud infrastructure

MPS Monitor’s back-end cloud infrastructure which is securely hosted within datacentres in Italy is owned by the company. This benefits from 24x7 system monitoring, real-time alerting on all main security-related events, extensive log analytics management, continuous vulnerability assessment and monitoring on all assets, and bi-annual penetration tests conducted by external cybersecurity experts. In addition, rigorous physical security measures protect the data centres from unauthorised access.

Secure DCA

MPS Monitor’s multi-platform DCA and unique DCA clustering technology ensures continuity of data collection on all customers. The DCA utilises SNMP to scan for network-connected MFPs and printers and supports SNMP v1, v2c, and the most secure v3. The latest version - DCA 4 - enhances security and traffic optimisation by using HTTPS2/GRPC over port 443 and incorporates MQTT, a lightweight IoT communication protocol, utilising Azure IOT Hub as a message broker. This significantly boosts the speed of communication between the DCA and devices on the local network and the MPS Monitor cloud service.

DCA4 is available for Windows, MacOS, and Linux platforms and includes enhanced functionalities such as expedited and more secure communication and the addition of Device Web Access (DWA) which allows MPS Monitor Console users to browse the embedded web server pages of any customer's printer. Mandatory multi-factor authentication or Active Directory integration ensures that only authorised users can use the DWA feature.

Information Security Management System

Notably, the MPS Monitor Information Security Management System (ISMS) extends advanced security capabilities directly to dealers and their clients, facilitating GDPR compliance and ensuring adherence to stringent data protection requirements.

HP Smart Device Services integration

The integration with HP Smart Device Services offers a seamless and efficient solution for monitoring and managing HP printing devices without installing a DCA or any other piece of software or hardware on the customer’s network. The SDS integration includes features that allow channel partners to access the embedded web server of any HP printer from inside MPS Monitor, to update devices’ firmware remotely, and to create, assess, and remediate fleet-wide security policies. Once policies are created, checks can be run on a daily basis to ensure compliance.

Key differentiators

- **Security certifications.** MPS Monitor has achieved compliance with broadly recognised security standards including ISO 27001, SOC 2 Type 2 and CSA STAR Level 2.,
- **Ongoing Testing.** systems are subject to continuous vulnerability assessment and monitoring, with bi-annual penetration testing performed by at least two different external security firms. Upon each testing session, when critical or high-risk vulnerabilities are discovered, a recheck is performed within 30 days to ensure those vulnerabilities are solved.
- **High security datacentre.** The physical infrastructure that runs the MPS Monitor cloud services is hosted in the British Telecom datacentre located in Milan, Italy, one of the largest and most secure datacentre facilities in Europe, where some of the largest national and European public and private institutions host their Internet and data infrastructures. It is a high security facility, with physical security measures, 24x7 surveillance by armed guards and video monitoring, access control and visitor management, fire suppression and flood protection, power protection and multi-redundant Internet connections.
- **Data protection.** The MPS Monitor system collects and stores only technical data related to the printing activity of devices. It does not collect, process and store any information contained in the printed documents or related to the content and quality of print jobs. The system does not collect PII or PHI from devices, and it does not manage payment data, thus it does not require compliance to standards like HIPAA and PCI-DSS. Users have the option, upon their discretion, to store names and email addresses of customers into the platform's database, with full confidence that those data are processed and stored in full compliance with EU GDPR. All data is stored in servers located in the EU.
- **Secure data collection technology.** A multi-platform DCA and clustered DCA technology provides maximum reliability and security in data collection. From a cybersecurity point of view, the DCA is continuously assessed by a team of security experts, to ensure that its installation within the customer's internal network poses no security risk for the IT environment.
- **User account security.** Multi-factor authentication can be activated on all user accounts. Single sign-on integration, both natively to Azure Active Directory services, and via Okta, Inc.'s identity and access management platform, provides secure access to authenticate users to MPS Monitor portal.
- **Secure Device Web Access.** This allows users to securely browse the embedded web server pages of any customer's printer. It ensures limited and safe printer HTTP access through different measures, such as MFA and other strict access policies.

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:

© Copyright 2025, Quocirca. All rights reserved. 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.