Print Security Landscape, 2024

Mitigating the print infrastructure as a threat vector

Print security trends in the US and Europe

July 2024

MPS Monitor Excerpt

QUOCIRCA

Key findings

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

Table of Contents

Buyer recommendations

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

Buyers should consider the following actions:

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

Vendor profile: MPS Monitor

Quocirca opinion

MPS Monitor continues to advance the security features of its device management platform. The company has adopted a security and data protection by default and by design approach, which sees robust security controls implemented throughout the development and release process. MPS Monitor 2.0 is a cloud-native SaaS solution for remote monitoring and management of printers, MFPs, and label printers that enables dealers to streamline billing, meter reading, and automated supplies replenishment. With over 2 million devices connected in 75 countries, MPS Monitor 2.0 has more than 400K DCAs running into customers' networks, monitoring more than 300K end customers.

Its cloud-based SaaS device management platform offers a robust set of security features and capabilities to protect data, user accounts, and infrastructure, such as single sign-on integration and multi-factor authentication, as well as physical security measures to safeguard the data centres against unauthorised access. The platform comes equipped with a full set of APIs for integrating external software solutions. Its highly scalable data collection technology enables managed print providers to streamline tasks associated with fleet management, including recording page volumes and automating toner and consumable replenishment.

In March 2022, MPS Monitor introduced DCA 4, which is built with a strict security-by-design approach, further mitigating the risk that the DCA could be used as an attack vector to the customer's network. It also fully supports SNMP v3 and device authentication to ensure maximum device security. The addition of device web access (DWA), which is hosted on Azure, allows authorised MPS Monitor console users to browse the embedded web server pages of any customer's printer. 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.

Additionally, MPS Monitor Analytics, a complete business intelligence platform that includes security performance based on Microsoft Power BI Embedded technology, provides granular and aggregate visibility to virtually all the data and events related to customers' print environments.

Continual monitoring of devices in the field can help MPS providers mitigate potential risks such as detecting outdated firmware and applying firmware updates where needed, as well as support wider print security strategies. On HP devices specifically, thanks to MPS Monitor's integration with HP SDS technology, security policies can be defined, assessed, and remediated. Device compliance can be continually checked and integrated, and reporting is provided through MS Power BI Embedded analytic dashboards.

Key security features

Information Security Management System

MPS Monitor has continued to focus on ways to improve its Information Security Management System (ISMS) and further strengthen its security posture. It has increased the number of security testing and monitoring activities performed during the year, with both internal resources and external security firms. It is also developing a customised Generative AI system that will allow users to prompt the system for detailed information and documents on the company's security posture and receive timely and accurate answers on how security measures are implemented within the platform.

Secure cloud infrastructure

The platform is compliant with stringent security standards and certifications, including ISO/IEC 27001, SOC 2 Type 2, and CSA Star Level 2. The CSA Star Program is promoted by the Cloud Security Alliance and ensures compliance with Cloud Control Matrix (CCM), a cybersecurity control framework for cloud computing.

MPS Monitor owns the physical infrastructure that hosts its cloud service. The backend cloud infrastructure is located within British Telecom data centres in Milan, Italy. The SaaS printer monitoring platform runs on a secure cloud infrastructure that benefits from 24x7 system monitoring, extensive log analytics management, real-time alerting on all main security-related events, continuous vulnerability assessment and monitoring, biannual penetration testing performed by external cybersecurity companies, and continuous surveillance within annual ISO 27001, SOC 2 Type 2, and CSA STAR Level 2 assessments.

All systems that run the services provided by MPS Monitor to customers and partners worldwide are included in the ISO/IEC 27001 certification perimeter, and all run within a certified ISMS. The ISMS extends its security features to benefit dealers and clients, and personal information is stored in compliance with international security standards including the GDPR.

Multifactor authentication

The platform has a comprehensive set of features to reduce risk, including password complexity, the option to enable multi-factor authentication on any user account, and PII Masking to protect Personally Identifiable Information (PII), alongside a formal documentation e-signing process to ensure that PII management is performed in compliance with the GDPR. Additionally, integration with Okta Identity and Azure AD enables customers to connect MPS Monitor to their Active Directory domain to achieve single sign-on.

Hybrid cloud

The MPS Monitor API is designed for hybrid cloud architectures. In this scenario, confidential customer data such as contracts, volumes, and consumption is stored in a local database inside the subscriber's network, and only data collected from printers is stored in the MPS Monitor cloud database.

HP SDS integration

MPS Monitor's multi-platform DCA and unique DCA clustering technology ensure continuity of data collection on all customers. For selected brands, the DCA can be installed directly on devices before shipment or via the cloud. The integration of HP SDS Cloud DCA into MPS Monitor allows dealers to remotely monitor and manage customers' HP FutureSmart devices without installing a DCA or any other piece of software or hardware on the customer's network.

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.
- **High-security data centre.** The physical infrastructure that hosts the MPS Monitor cloud services is located in a high-security data centre, which benefits from physical security measures, 24x7 system monitoring, real-time alerting, continuous vulnerability assessment and monitoring, Incident Response and Disaster Recovery plan, and biannual penetration testing.
- **Software integrity.** The utmost security measures and controls are use, in both the development and release process, including code review and code signing, checking before every DCA code release, and the process being performed by an external cyber-security firm.
- **Built-in security with HP SDS.** HP 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 create, assess, and remediate fleet-wide security policies.
- **User account security.** Multi-factor authentication can be activated on all user accounts. Single Sign-On (SSO) 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's portal.
- **Secure data collection technology.** A multi-platform DCA and clustered DCA technology provide 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. The DCA uses secure protocols and ports to connect to devices.
- **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.
- **AI-embedded technology.** MPS Monitor is developing a tailored Generative AI system that enables users to request detailed information and documents regarding the company's security posture,

providing timely and accurate insights into the implementation of security measures within the platform.

- **Secure support for label printers**. Thanks to Device Web Access technology, MPS Monitor offers secure monitoring of label printers as well. DWA, integrated into DCA, opens a web page for a printer of any brand or model using built-in unique features and procedures that make it virtually impossible for a threat actor to use this function as an attack vector.

About Quocirca

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

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

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

For more information, visit www.quocirca.com.

Usage rights

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