The Print Security Landscape, 2022

Securing the remote and hybrid workforce

Report Excerpt: MPS Monitor

January 2022

QUOCIRCA

Executive summary

Quocirca's Global Print Security Landscape 2022 report reveals that many organisations are struggling to keep up with print security demands in today's hybrid work environment. Home printing is creating new security concerns, exacerbated by shadow purchasing of devices. SMBs and mid-size organisations are finding it harder to keep up with print security challenges leading to a higher incidence of print-related data loss. This is leading to a lower confidence, particularly among SMBs, in the security of their print infrastructure. However, in Quocirca's Print Security Maturity Index, those organisations classed as leaders that have implemented a range of technology and policy measures are seeing lower levels of data loss and have higher confidence in the security of their print infrastructure. Print manufacturers and channel partners must strengthen their security propositions for organisations of all sizes to help customers mitigate risk in the new era of hybrid work.

The study is based on the views of 531 IT Decision Makers (ITDMs) in the US and Europe. 23% of the respondents were from SMBs (250 to 499 employees), 29% from mid-size organisations (500 to 999 employees) and 47% from large enterprises (1,000+ employees).

The following vendors participated in this study:

Manufacturers: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, Xerox
ISVs: EveryonePrint, Kofax, MPS Monitor, MyQ, PaperCut, Ringdale

Key findings

- **Remote working is here to stay and is creating an expanded threat landscape.** Pre-pandemic approaches to securing the print environment focused around a primarily static, office-based workforce now need to move to supporting workers who spend some time in the office, and some in the home environment. On average, 44% of employees are expected to work remotely as offices fully reopen. Hybrid work creates significant security challenges for IT teams to manage as the exploitable attack surface increases. The proliferation of shadow IT and unsecured home networks means that organisations need to rethink their security posture around the print environment.
- **IT security remains the top investment priority over the next 12 months.** 53% of respondents say it is one of their highest three priorities. MPS (managed print services) are second in importance (41%) followed by managed IT services (38%) and cloud services (35%). 70% of organisations expect to increase their print security spend over the next 12 months, with only 11% expecting a decrease.
- **A reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, many organisations remain reliant on printing. Printing will remain critical or very important for 64% of organisations in the next 12 months. 44% anticipate that office print volumes will increase, and 41% that home print volumes will do likewise. Printers and networked MFPs pose a security risk not only in terms of printed documents being accessed by unauthorised users, but also as an ingress point to the network if left unprotected.
- **Just a quarter (26%) feel completely confident that their print infrastructure will be secure when offices fully reopen.** Organisations are struggling to keep up with print security demands: more than half (53%) say it has become considerably or somewhat harder to do so. 67% of respondents are concerned about the security risks of home printing, compared to 57% who are concerned about office print security.
- **Print security is lower on the security agenda than other elements of the IT infrastructure.** Top security risks are considered to be cloud or hybrid application platforms, email, public networks and traditional endpoints. Employee-owned home printers come in as the 5th top security risk (24%) ahead of the office print environment (21%). This suggests both a lack of awareness and complacency in not

fully appreciating the security vulnerabilities around printing, which remains an integral endpoint in the IT environment.

- **There are marked differences between MPS users and non-MPS users.** Organisations that use an MPS provider foresee much greater growth in print volumes and are most confident in the security of their print environment – despite having a higher awareness of the risks. They are also twice as likely to state that keeping up with print security challenges has become somewhat or a lot easier. The visibility and control provided by an MPS appears to ease the security burden for users, increase assurance that they can ramp up print volumes if needed, and reduce complacency, therefore lowering the likelihood of being blindsided by a security incident.

- **In the past 12 months, over two thirds (68%) of organisations have experienced data losses due to unsecure printing practices.** This has led to a mean cost per data breach of £631,915. Such quantified financial losses are bad enough for organisations to manage, but they also state many other negative impacts, such as a loss of business continuity and ongoing business disruption after the breach. Customer loss is reported to be the biggest impact for SMBs. Large organisations are less likely to have suffered a print-related data loss, with 36% reporting no breaches compared to 24% of SMBs. The public sector is the most affected vertical. Vulnerabilities around home printers were cited as the top reasons for data loss – such as home workers not disposing of confidential information securely, and interception of documents stored in the home printer environment.

- **Quocirca's Print Security Maturity Index reveals that only 18% of the organisations can be classed as Print Security Leaders**, meaning they have implemented six or more security measures. The number of leaders rises to 22% in the US and falls to 12% in France, which also has the highest number of laggards (37%). Print Security Leaders are likely to spend a higher amount on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment. When compared by vertical, finance has the largest percentage of leaders (23%).

- **Less than a third (28%) of ITDMs are very satisfied with their print supplier's security capabilities.** This drops to 20% in the public sector. US organisations are most satisfied, with those in Germany least happy. ITDMs who use an MPS have far higher satisfaction levels (42% are very satisfied) than those who don't (20%).

- **Most ITDMs turn to managed security service providers (MSSPs) for print security advice.** MSSPs are the primary source of security guidance for 35% of organisations overall, rising to 40% in the US. Just 18% of ITDMs overall would turn to an MPS provider for print security guidance, while 21% would consult a print manufacturer. This points to an opportunity for MPS providers and channel partners to collaborate more closely with MSSPs.

- **CIOs and CISOs differ in their views on the future of print, and their handling of security challenges relating to the hybrid print environment.** CISOs are more bullish, with 53% and 58% respectively expecting a rise in office and home print volumes, compared to 42% and 40% of CIOs. Notably, CIOs (32%) and CISOs (33%) show the most concern around home printing compared to other IT respondents, ranking it as their second top security risk. CIOs also seem to be finding it harder than CISOs to keep up with print security challenges – 61% stated that they were finding it considerably or somewhat harder, compared to only 44% of CISOs, where 29% also stated that they were finding it somewhat or a lot easier.

Buyer recommendations

Print devices continue to become more sophisticated, with greater intelligence being built into even low-end consumer printers. Such intelligence can be used by those with malicious intent to access a print environment, and if that then provides direct access back into the corporate environment, chaos could ensue. Organisations must therefore pay far closer attention to protecting the print environment, particularly when looking to the continuation of hybrid working.

Organisations need to look at investing in the following areas to ensure that the print environment is secured to the same levels expected across any other area of the IT platform.

- **Conduct in-depth print security and risk assessments.** Most organisations have these in place for the overall IT environment, but the print platform often seems to be left out. Given the increasing threat landscape associated with hybrid work, organisations must ensure that the print infrastructure is fit for purpose across device, document and network security. This can be carried out internally, or by third parties such as managed security service providers (MSSPs) or managed print service (MPS) providers. New assessments must fit in with the broader IT security and risk assessments.
- **Implement a zero trust architecture.** Zero trust operates on the basis of 'never trust, always verify', assuming that an environment will be compromised and no device should ever be fully trusted. Organisations have started to implement zero trust environments, but mainly within the constraints of their owned and managed IT environment. This now needs to be extended to the wider hybrid environment, embracing home workers and all the devices that are being used for work purposes across that environment – including print devices.
- **Provide defined and authorised printers for home workers.** Individuals still require access to printed output when working from home. However, basic consumer printers do not come with the capabilities they may require, such as print speed and quality, and will not generally adhere to the needs of the organisation – such as security and manageability. Organisations should move to defining classes of printer that individuals can use, depending on need. These should then be supplied and provisioned by the organisation, along with the means of managing and controlling what business content the individual prints on the device.
- **Revise BYOD policies to include employee printers.** For many organisations, supplying and provisioning printers to all employees working from home may not be practical. Existing bring-your-own-device (BYOD) policies must now be updated to cover the home environment – moving to a BYOO (bring your own office) approach, with policies covering desktop/laptop PCs, tablets, mobile devices, desk phones and print devices. An effective BYOD/BYOO policy will help ensure that each individual's environment adheres to an organisation's basic security needs.
- **Evaluate content security solutions.** Content management systems based around document metadata, where documents are classified based on their sensitivity – along the lines of 'Public', 'Commercially sensitive', and 'Internal use only' for example – allow specific policies to be set, such as '*this document cannot be printed*' or *'this document can only be printed on an approved printer*'. This enables home-based employees to use their own printers for routine jobs without the risk of restricted documents ending up in their wastebins.
- **Implement pull printing.** Requiring a PIN or a Bluetooth or NFC token to release a job at a printer means that the print job owner has to be present before the job is printed out. Pull printing is most useful in shared access environments, as is the case for many office printers. However, it could also be applied to allow home users to submit print jobs securely via the cloud to office printers, or even their own printer – enabling them to be tracked at a central level. Jobs that the owner forgets about are held, and can be securely deleted if not printed out after a defined period of time.
- **Continuously monitor through reporting and analytics.** Risk assessments, tuning content security and configuring SIEM (security information and event management) systems all require insight provided by gathering reports from across an organisation's network, including its extension into employees'

homes. SIEM systems themselves can often provide this information, as can other log management tools.

- **Formalise processes to respond to print security incidents.** Accept that leaks are likely to happen – and plan how to deal with the repercussions. Most of the respondents to Quocirca's research had at least some security measures in place, and a reasonable belief that their print environment was secure, but 68% still experienced at least one print-related data loss in the past 18 months. Organisations must put appropriate processes in place to respond to data breaches by dealing with the possible legal and reputational damage caused, while building back business capabilities in the shortest possible time.
- **Use cloud routing for certain print jobs.** While a lot of printing is informal and needs to be near to the user to be effective – for example, printing a report in order to review it – other print jobs are part of larger business processes, and the user who submits the job may never see the output. For example, letters to be mailed to customers, marketing output, and forms that make up part of a broader process may be better printed at a more suitable printer. Employees can securely submit such jobs from home to a cloud print service, which can check the veracity of the submission, and seek secondary authorisation before allocating the job to the most suitable print resources available. Even within the office environment, such routing can help in minimising print wastage by making sure that certain print jobs go to the most suitable printer.

Please note that this is a report excerpt. The full report is available at https://quocirca.com/print-security-2022/

Vendor Profile: MPS Monitor

Quocirca opinion

MPS Monitor 2.0 is a cloud-based SaaS device management platform that enables MPS providers and partners to monitor customers' print fleets, proactively manage supplies replenishment and analyse data. Designed to help dealers optimise their operations and improve service margins, the solution is available in a number of OEM-branded versions, and provides direct integration with Microsoft Universal Print and HP Inc.'s Smart Device Services (SDS).

With many organisations operating multi-vendor print and MFP fleets across a remote and office environment, the ability to remotely track and manage devices involves additional layers of risks that need to be adequately mitigated. MPS Monitor adopts a holistic approach to the security of the entire print environment. The platform offers a robust set of security features and capabilities to protect data, user accounts and infrastructure; provide device security services to end customers, enable cloud print services through a secure cloud like Microsoft Azure, as well as remote monitoring without a DCA.

Key security highlights

Security certifications
MPS Monitor achieved ISO/IEC 27001 certification in 2017. 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 Information Security Management System (ISMS).

In April 2021, the company successfully completed its System and Organization Controls 2 Type 1 (SOC 2 Type 1) examination, an accreditation that confirms its security practices and controls meet the AICPA Trust Services Criteria for security, availability and confidentiality.

Advanced DCA technology
While the SaaS platform is entirely cloud-based, data collection relies on an infrastructure of about 230,000 DCAs installed at approximately 160,000 end customers. The cybersecurity risks associated with having a connection between the customer's network and the cloud management platform, through the presence of an active DCA in every customer, are mitigated by ensuring full compliance to broadly recognised security standards such as ISO/IEC 27001 and SOC 2. This requires continuous monitoring and improvement of enforced security policies and best practices. MPS Monitor's security policies include routine penetration tests, code reviews, vulnerability assessments and incident response services, provided by multiple external security firms that continuously assess and verify the DCA's security profile.

MPS Monitor's multi-platform DCA and unique DCA clustering technology ensures continuity of data collection on all customers. For selected brands, the DCA can be installed directly on devices before shipment, or via the cloud.

This year MPS Monitor announced the full integration of HP SDS Cloud DCA into its device management platform. This feature allows HP devices running FutureSmart firmware (version 4.9.0.1 or later) to connect and interact with the cloud without the need for an on-premise connector or other local component. HP devices with supported FutureSmart firmware are permanently connected to the cloud, regardless of the presence of a DCA on the customer's network. By activating the HP SDS Cloud DCA, MPS providers can monitor and manage customers' supported devices remotely and comprehensively.

User authentication
As with all SaaS cloud solutions, MPS Monitor requires users to manage credentials to access an external cloud service over the internet. The platform has a comprehensive set of features to reduce risk including password complexity, two-factor authentication, and integration with single sign-on for customers using Active Directory for example.

In the first quarter of 2021, MPS Monitor announced a partnership with leading independent identity provider Okta. Okta Identity integration enables users to sign on across domains with a single online identity, increasing the platform's security profile by preventing the use of insecure or weak credentials. It works seamlessly in the background, securely passing authentication details from the user's organisational credentials to the MPS Monitor SaaS service. Customers using Active Directory (or Azure AD) for their identity infrastructure, can connect MPS Monitor to their Active Directory domain using the Okta integration, to achieve a complete single sign-on experience.

Universal Print integration
The integration of MPS Monitor and Universal Print enables MPS providers to deliver remote monitoring and management, user management, job tracking, and pull-printing functionalities to Microsoft 365 customers in a single, integrated and fully secure SaaS service.

MPS Monitor automatically syncs with Azure AD to activate the Universal Print service for each customer. Once the service is active, the MPS Monitor DCA is automatically enabled to work as a Universal Print Connector, removing the requirement to install additional software or hardware components on the customer's network.

The integration also enables printing from zero trust networks via single sign-on. Universal Print stores all print queues in Office data storage, where customers' Microsoft 365 mailboxes and OneDrive files are also stored.

Print security management
Print management is one part of a multi-layered print security model that includes hardware, software and services. A tool like MPS Monitor can detect potential risks through the continual monitoring of devices and support a wider print security strategy that includes assessment, device deployment and remediation from print security incidents.

MPS Monitor offers some notable features which enable channel partners to proactively deliver print security management. The platform allows partners to detect for outdated firmware and apply firmware updates where needed. On HP devices specifically, thanks to the 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.

Security features overview

Key features include:

- **Data security.** MPS Monitor 2.0 systems are operated inside the MPS Monitor ISO/IEC 27001-certified ISMS perimeter.
- **GDPR compliance.** Processing of personal data within the system is performed in full compliance with the GDPR, for all customers and dealers where this regulation is applicable. Confidential information masking can be applied at the user level, and a highly granular user profiles structure is available.
- **User account security.** Two-factor authentication can be activated on all user accounts. Integration with Okta provides single sign-on to Active Directory users. System admins' passwords have to meet specific complexity requirements and are required to be changed every six months or earlier. A sophisticated and highly granular user profiles and capabilities function provides the utmost level of control on features and capabilities enabled or disabled at the user level.
- **Cloud infrastructure and customers' IT security**. MPS Monitor's cloud infrastructure, code and the network is subject to continuous security monitoring, testing and audits.
- **Security certifications and compliance.** MPS Monitor has achieved compliance with broadly recognised security standards including ISO/IEC 27001 and AICPA SOC 2.
- **High security data centre.** The physical infrastructure that hosts the MPS Monitor cloud services is located in a top level, high security data centre.
- **DCA.** 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.

- **Remote monitoring without a DCA.** 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.
- **Security Analytics with Power BI Embedded.** MPS Monitor Analytics, a complete business intelligence platform that includes security performance, based on Microsoft PowerBI Embedded technology provides granular and aggregate visibility to virtually all the data and events related to customers' print environments.
- **Built-in security with HP Smart Device Services.** The SDS integration includes features that allows 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.
- **Microsoft 365 Universal Print integration.** MPS Monitor users can access Universal Print features seamlessly from within their printer management application. Microsoft Power BI Embedded Analytics tools integrate all print job information coming from Universal Print into MPS Monitor to provide a full and comprehensive view of print costs, usage and predictive analytics.

About Quocirca

Quocirca is a global market insight and research firm specialising in analysing 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 is at the forefront of the rapidly evolving print services and solutions market, trusted by clients who are 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.

Disclaimer:
This report has been written independently by Quocirca. During the preparation of this report, Quocirca has spoken to a number of suppliers involved in the areas covered. We are grateful for their time and insights.

Quocirca has obtained information from multiple sources in putting together this analysis. These sources include, but are not limited to, the vendors themselves. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in any information supplied.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data.

All brand and product names are trademarks or service marks of their respective holders.