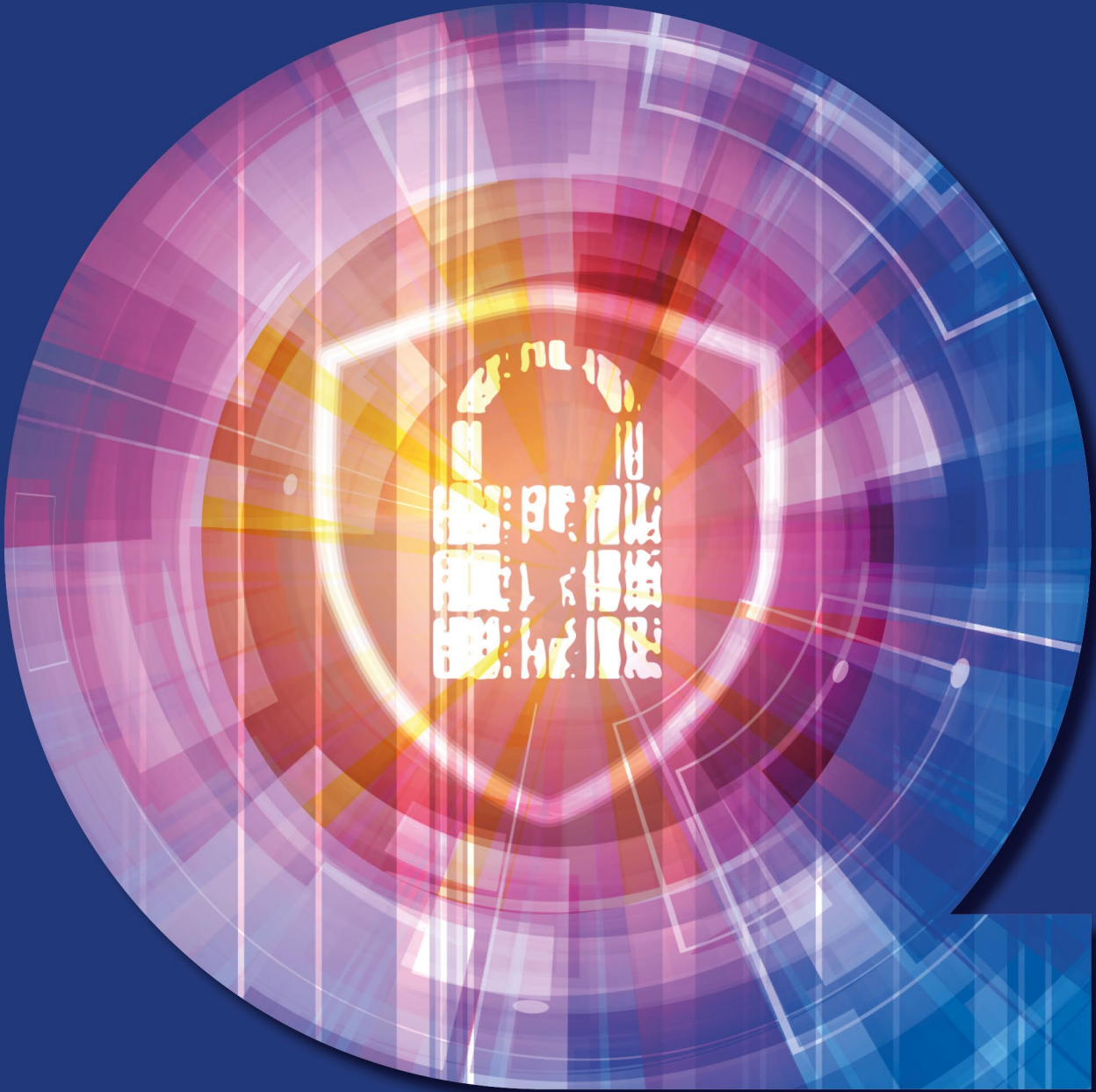


The Print Security Landscape, 2023

Securing the print infrastructure amidst a growing threat landscape



Executive summary

Quocirca's Global Print Security Landscape 2023 report reveals that organisations face ongoing challenges in securing print infrastructure. Home printing continues to cause security concerns, with employee shadow purchasing making it harder to control document security. Print-related data breaches remain prevalent, with 61% of respondents reporting at least one data loss in the last 12 months, rising to 67% amongst midmarket organisations. This is leading to lower confidence, particularly among SMBs, in the security of print infrastructure.

Notably, the research reveals a strong disconnect between the perceptions and attitudes to print security amongst chief information officers (CIOs) and chief information security officers (CISOs). Expectations for security spend growth in the coming 12 months are similar, with 84% of CIOs and 81% of CISOs expecting their print security spend to increase. Only 28% of CISOs believe it has become harder to keep up with print security challenges, compared to 50% of CIOs. Similarly, only 45% of CISOs are very or somewhat concerned about the risks of unsecured printers, compared to 72% of CIOs. This chasm between CIOs and CISOs means the two individuals responsible for the overall technical security of the print environment when serving the business are not seeing things in the same light – and this has ramifications for the business itself.

Fortunately, print security leaders are mitigating risks. As shown by Quocirca's Print Security Maturity Index, organisations classed as leaders, which 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. For print manufacturers, MPS providers, and the rest of the print channel, bridging this gap between the two security camps is a must. However, this cannot be done simply – it will require a two-pronged approach to bring the two parties closer together, as well as ensuring the business itself is more aware of the security issues around print.

Therefore, 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. Becoming a trusted advisor and provider of print security solutions that fit with an organisation's existing security environment is key. Ensuring data and information flow, along with device and output security, will create new revenue capabilities for the print channel.

The Global Print Security Landscape 2023 study is based on the views of 507 IT decision-makers (ITDMs) in the US and Europe. Respondents include 20% from the UK, 20% from France, 20% from Germany, and 40% from the US. In terms of organisation size, 24% represent small and medium-sized businesses (SMBs) (250 to 499 employees), 26% are from mid-size organisations (500 to 999 employees), and 50% are from large enterprises (1,000+ employees). Respondents are drawn from a range of verticals, including business and professional services, finance, industrials, public sector, and retail.

The study also includes the print security vendor landscape, which features Quocirca's assessment of service offerings from major print manufacturers.

The following vendors participated in this study: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, and Xerox.

Key findings

- **Cybersecurity incidents continue to rise.** Overall, 42% of organisations report an IT security breach in the past year, rising to 55% among mid-market organisations and dropping to 36% amongst large enterprises, along with 51% in the finance sector, dropping to 32% in the public sector. The highest incidence across all organisations is malware, with phishing highest in the mid-market. Security breaches increased for 61% of organisations in the past year, rising to 70% in the US and 66% in business and professional services. On average, 27% of IT security incidents were related to paper documents.
- **Reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, 70% remain dependent on print today, rising to 72% in large organisations. A majority (80%) have changed the composition of their printer fleet over the last two years, rising to 88% in the mid-market. Overall, 79% expect to increase their print security spend in the next year, rising to 86% in the US and 85% in business and professional services and retail.
- **Print security is lower on the security agenda than other elements of IT infrastructure.** Cloud or hybrid application platforms, email, public networks, and traditional end points are seen as top security risks. Employer-owned home printers come in as the seventh top security risk (21%), ahead of the office print environment (20%). Notably, there is a disparity between CIOs and CISOs. Just 18% of CIOs consider office printing a key security risk compared to 30% of CISOs.
- **Organisations are taking different approaches to managing the security of their print infrastructure.** While 31% indicate they use an MPS provider, over half (54%) indicate that they use a managed security services provider (MSSP) to manage both print and IT security. This rises to 58% amongst smaller organisations (249–499 employees).
- **Organisations are finding it harder to keep up with print security demands.** Overall, 39% say it is becoming harder, rising to 50% in the midmarket (500–999 employees). The top challenge is keeping print management software up to date (35%), protecting sensitive and confidential documents from being printed (34%), and securing printing in the remote/home environment (31%). Hardware security is a key concern for SMBs (29%), and highest in the finance and industrial sectors (31%) and for CISO respondents (38%).
- **Organisations using MPS or that are classified as print security leaders are more confident in the security of their print infrastructure.** The visibility and control provided by an MPS appears to ease the security burden for users. While overall, only 19% of respondents are completely confident in the security of their print infrastructure, this rises to 26% amongst organisations using MPS. Overall, a further 50% say they are mostly confident. This reflects the growing complexity and challenges associated with securing both devices and documents across a hybrid workplace.
- **In the past 12 months, 61% of organisations have experienced data losses due to unsecure printing practices.** This is a fall from 68% in our 2022 study. Mid-market organisations are more likely to report one or more data losses (67%) than large organisations (57%) and the public sector (49%). On average, the cost of a print-related data breach is £743K. Beyond the financial loss, the top impact of a data breach is the lost time in addressing the breach and the impact on business continuity (30%). Vulnerabilities around home printing, such as home workers not disposing of confidential information securely, was cited as a top factor contributing to data losses.
- **Quocirca's Print Security Maturity Index reveals that only 27% of the organisations studied can be classed as Print Security Leaders,** meaning they have implemented six or more security measures. The number of leaders rises to 31% in the US and falls to 18% in Germany, which also has the highest number of laggards (29%). Print Security 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. When compared by vertical, business and professional services have the largest percentage of leaders (37%), with the public sector having the least (18%).
- **Less than one-third (32%) are very satisfied with their print supplier's security capabilities.** This rises to 50% amongst US organisations and drops to 17% in Germany. Those using an MPS have far higher satisfaction levels (39% are very satisfied) than those not currently using an MPS or with no plans to use one (23%). Print security leaders – those that have adopted a range of measures, including security assessments, pull printing, and formal print security policies, are most likely to report higher satisfaction levels – 53% of leaders are very satisfied, compared to 27% of followers and only 15% of laggards.

Table of Contents

Executive summary	2
Key findings	3
Introduction	5
Vendor landscape	6
Vendor profile: Konica Minolta	7
Recommendations	10
Supplier recommendations	10
Buyer recommendations	10
About Quocirca	12

Introduction

As organisations adjust to managing remote and hybrid teams, supporting digital transformation, and navigating an uncertain and volatile global economy, they face an ever-expanding landscape of vulnerabilities and increasing risk. Quocirca's research reveals that 42% of organisations have experienced a cybersecurity incident in the past year, rising to 51% in the finance sector and 55% amongst midmarket organisations. The volume of security incidents has increased in the past year for 61% of organisations.

Supply chain disruption and geopolitical situations such as the Russia-Ukraine war have further intensified the threat landscape. The increased prevalence of ransomware, ransomware denial of service (RDoS), distributed denial of service (DDoS), social engineering, and supply chain attacks is driving increased concerns around cybersecurity and the resilience of business-critical functions.

This is further compounded by a raft of technological challenges. As organisations migrate more applications and services to the cloud to support digital transformation initiatives, new security challenges emerge. The growing amount of business-critical data hosted in the cloud becomes vulnerable to attack and compromise.

This risk is heightened due to remote workers accessing data from potentially unsecure home networks. Security threats include misconfigured access points, weak passwords, lack of identity and access management (IAM), and failure to use multifactor authentication. A fragmented approach to threat detection and monitoring means security teams are struggling to keep up.

The print infrastructure is not immune to security risks – on average, paper documents represent 27% of IT security incidents. Today's intelligent multi-function printers (MFPs) not only pose a risk of paper output falling into the wrong hands – whether accidentally or maliciously – but also can be exposed as gateways into the rest of an organisation's environment. Home printers pose an additional risk, particularly those that were purchased by employees. This shadow purchasing means home printers may not meet corporate security standards or be monitored through centralised security tools.

Although print remains low on the IT security agenda, organisations continue to report print-related data losses. In our 2023 study, 61% of respondents report a print-related data breach, with an estimated average cost of £743K for one data breach. With both the reputational and financial impact of any security incident far reaching and substantial, organisations cannot afford to be complacent.

These risks can be mitigated through adopting a never trust, always verify zero-trust security approach. Implementing data and network encryption, security monitoring, and remediation, along with micro-segmentation, can help reduce the attack surface, improve threat containment, and strengthen regulatory compliance.

This report highlights the risks and challenges associated with securing the print infrastructure for the hybrid workplace. It discusses security confidence levels, print security measures adoption, and the disconnect between CIOs and CISOs that must be overcome. The report also includes an analysis of the security products, services, and solutions from the major print manufacturers in the market.

Vendor landscape

Quocirca has created a snapshot of the positioning of vendors in the Global Print Security market (Figure 14). Please note, because of varying service offerings for each vendor and regional differences, this is intended for guidance only.

The graphic represents Quocirca's view of the competitive landscape for vendors based on the following categories:

1. **Leaders:** Vendors with a strong strategic vision and a comprehensive print security product and service offering. Leaders have made significant investments in their hardware, solutions and services portfolio, and infrastructure, and also demonstrate a strong vision for future strategy.
2. **Major players:** Vendors that have established and proven offerings and are continuing to develop their solutions service portfolio. These vendors are most likely to be strongly focused on the SMB market with a hardware-centric approach.

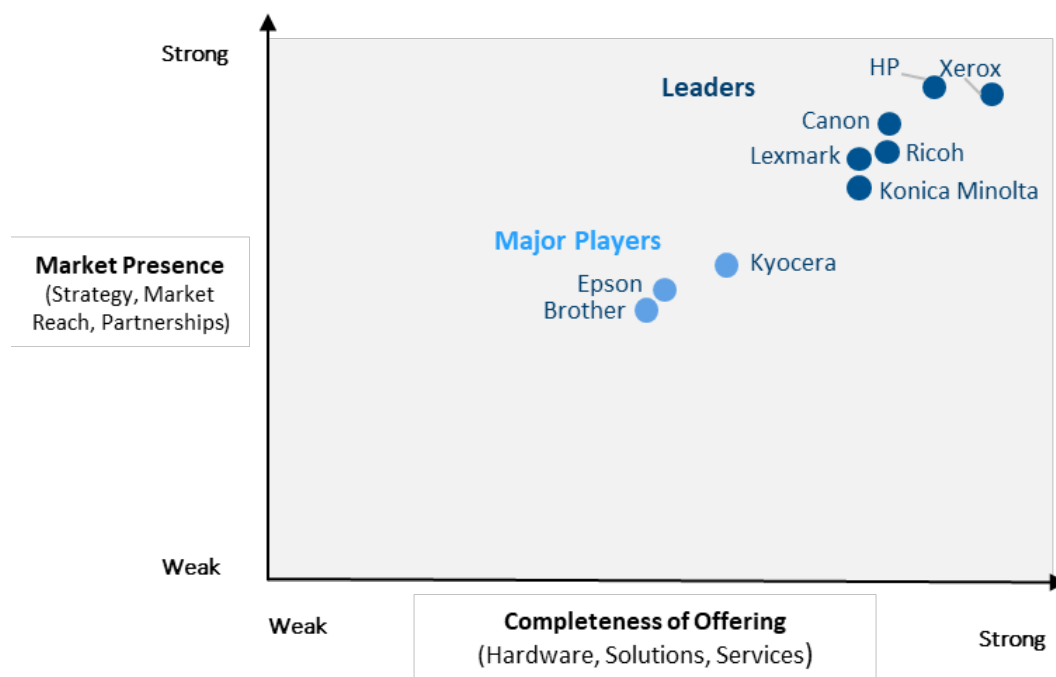


Figure 1. Quocirca Print Security Vendor Landscape, 2023

The Quocirca Vendor Landscape is a graphical representation of Quocirca's opinion of the market and is based on Quocirca's scorecard methodology. This information is provided as a visual representation only and should be combined with other sources to determine the suitability of any vendor. Quocirca does not endorse any vendor, product, or service. Information is based on best available resources and opinions reflect judgment at the time. All opinions are subject to change.

Vendor profile: Konica Minolta

Quocirca opinion

Konica Minolta has retained a leading position in Quocirca's 2023 assessment of the print security market. Konica Minolta's security portfolio spans print and document security across its MFP portfolio, IT security services, video security, and compliance and risk management. Its managed print security services provide monitoring and management of print devices and systems, including device security profile management, vulnerability scanning and intrusion detection, and print policy enforcement.

Security is a core component of its Intelligent Connected Workplace portfolio, which encompasses a range of solutions to address the digital transformation needs of businesses of all sizes. Many of its security offerings, such as Shield Guard, are proprietary, so most suited to a Konica Minolta environment. Most recently Konica Minolta has bolstered device protection for its bizhub i-Series through its partnership with Bitdefender. The Bitdefender antivirus solution is embedded in Konica Minolta's MFP hardware and monitors all scanned files and documents in real time. In addition, Konica Minolta offers Shield Guard, a cloud-based solution offering remote security monitoring and management of printer fleets, and a SIEM service that can include an optional dedicated SOC.

Of note are its custom-tailored security services – bizhub SECURE – which have been available since 2011, and additional security layers offered by its bizhub SECURE Platinum and bizhub SECURE Ultimate options. In addition, over the past year, Konica Minolta has been actively shifting its customers to its cloud-based secure print management platform. This provides flexible options depending on whether a customer is looking for a fully cloud hosted, hybrid cloud, or on-premise infrastructure. The platforms are available both locally and globally.

This is complemented by a range of managed IT services offerings. Depending on the region, Konica Minolta can offer a range of cybersecurity services, which include security assessments. For example, its US cybersecurity practice provides HIPAA assessments to meet healthcare sector privacy requirements, as well as financial assessments for community banks to satisfy PCI compliance requirements.

From a global perspective Konica Minolta has developed a range of standardised packages for customers depending on their security requirements. These range from basic remote monitoring to proactive and predictive monitoring. Konica Minolta particularly excels in an IT-centric approach to security through its Microsoft Managed Global Partner status. Konica Minolta is currently working to achieve Microsoft Cloud Solution Partner for Security Designation in 2023. Konica Minolta is also expanding its cloud print and scan portfolio, which includes secure document services hosted in the cloud.

Beyond its traditional print security offerings, Konica Minolta's deep expertise across IT services strongly sets it apart from some of its key competitors, particularly in the SMB market. An opportunity is for Konica Minolta to build integrated cybersecurity professional services that encompass printing and include in-depth security assessments across a multivendor fleet environment (across home and office devices).

Konica Minolta's security portfolio is most suited to customers operating a standardised Konica Minolta environment that wish to enhance the security across their print environment. Its range of flexible and scalable offerings enables Konica Minolta to address the varying needs of businesses of all sizes.

Vendor highlights

Extensive embedded security

Konica Minolta's print security offerings extend beyond embedded device security to encompass document, data and network security. The company says it has a wider range of Common Criteria/ISO 15408 EAL3 standard certified MFPs than any other OEM, and offers standard document protection measures including data encryption, secure deletion, watermark copy protection, and PDF signatures.

Konica Minolta's devices are subject to rigorous internal cybersecurity tests to protect their systems and ensure they meet PCI, HIPAA, FERPA, and GDPR regulations. The company has also invested in an extra layer of threat protection – penetration tests provided by NTT DATA Security Services, an internationally respected IT services provider, and the security division of NTT Ltd.

Konica Minolta partners with Bitdefender for detecting and preventing malware intrusion on its bizhub i-Series. Bitdefender's antivirus solution has been embedded in the product's firmware and monitors all scanned files and documents transferred to and from it in real time. It also enables automatic virus scanning on hard drives, as well as manual on-demand scans.

Scalable bizhub SECURE managed security service

Konica Minolta offers bizhub SECURE, a managed service offering. This includes three different service levels: bizhub SECURE, bizhub SECURE Platinum, and bizhub SECURE Ultimate. bizhub SECURE protects documents, data and corporate information. bizhub SECURE Platinum adds an extra layer of network security, including access control to activate automatic log-off for accounts to keep devices safe. bizhub SECURE Ultimate includes Bitdefender with real-time scanning and sets up periodic scanning times. It provides security beyond a basic level and notifies the user whenever the bizhub faces a potential risk.

With the additional bizhub SECURE Notifier, customers have an application running on their device, which visualises the status of security settings on the MFP user panel. In addition, the application proactively sends an email to the administrator in case a security-related setting has been changed.

The bizhub SECURE service can be activated on any Konica Minolta bizhub MFP, either on-premises or prior to delivery. Since April 2022, Konica Minolta has offered ShieldGuard, a cloud monitoring platform, which works together with bizhub SECURE. The Starter package offers basic monitoring capabilities, the Business package offers unique password management features, and the Enterprise package provides remediation through Shield Guard to ensure devices security policies are met.

Konica Minolta's SIEM service includes a dedicated SOC that works together to fully protect customers' business 24/7/365. A future bizhub i-Series MFP firmware update will support SIEM systems. Currently the devices support scheduled automated Syslog export to an external system.

Cloud security

Konica Minolta has also been actively shifting its customers to its cloud-based secure print management platform. The Konica Minolta Cloud Print Service Portfolio includes multiple options to support and increase customers' security. Data and document security is assured through encryption and use of certified data centres, follow-me authentication, roles-based access controls, and controlled guest access. ISO 27001 accreditation provides independent assurance that systems are designed and operated with cloud-first security principles, and that robust processes are in place to build resilience and help avoid potential data security issues.

Vendor strengths and opportunities

Strengths

- **Robust hardware and software security.** Common Criteria validation and the bizhub SECURE service, combined, provide additional assurance that Konica Minolta devices are highly secure. Konica Minolta Remote Monitoring and Management Services (RMM) offer centralised monitoring and management of the IT infrastructure.
- **IT-centric expertise through partnerships.** Beyond its traditional print security offerings, Konica Minolta's deep expertise across IT services strongly sets it apart from some of its key competitors, particularly in the SMB market. Its broad approach delivers a complete service across cybersecurity, helping businesses to identify, contain and analyse network penetration, including attacks by malware, ransomware, or hackers.

Opportunities

- **Expand IT services-led security services.** By leveraging its mature managed IT services capabilities and IT expertise, Konica Minolta could expand its footprint with its traditional print customer base.
- **Expand services for multi-vendor print environments.** The opportunity to build integrated cybersecurity professional services that encompass printing and include in-depth security assessments across a multi-vendor fleet environment (across home and office devices) is substantial.
- **Use the partner programme to expand the professional services capability.** Many of Konica Minolta's peers have either an in-house professional services capability or strategic partnerships to provide this to customers looking for help in truly embedding print within the heart of their business operations.

Recommendations

Print security spend is expected to continue to grow over the next 12 months, creating ongoing opportunities for print manufacturers, managed print service providers, and channel partners. It is clear that organisations using MPS and those that have adopted a range of print security measures are ahead of the curve. Demonstrating how MPS can improve the security resilience of the print infrastructure will enable suppliers to shape their propositions across both the office and home printing environments.

Supplier recommendations

Quocirca recommends that suppliers address the following areas:

- **Bridge the CIO and CISO divide.** In larger organisations, the responsibility for print security may often be fragmented across different IT and business stakeholders. While CIOs have a strategic focus across the IT infrastructure, CISOs are fully focused on security. Given the awareness gap across these decision-makers, suppliers should elevate positioning and messaging of print security to a strategic level. This can support the alignment of print security priorities as CIOs and CISOs develop a more collaborative relationship.
- **Deliver consistent security across the hybrid environment.** Many home printers that are purchased by employees will not conform to the security requirements of the business. Ensure that security-led MPS offerings help address this shadow purchasing through either centralised remote monitoring or provision of authorised devices for home use. While standardised environments generally have a higher level of hardware security compared to a mixed-fleet environment, many organisations operate a mix of device brands across office and home environments. This creates a need for integrated third-party print management platforms that can manage document security consistently across a heterogeneous fleet. Nevertheless, this presents an opportunity for MPS providers to transition customers to a standardised environment to gain tighter security across their print infrastructure.
- **Create clarity around zero trust-led offerings.** There is no one-size-fits all to zero trust. Be clear on how this works with legacy devices and avoid the misuse of the term zero trust – or ‘zero trust-washing’ – to create the perception of robust security. Zero trust in the print landscape can be best achieved through micro-segmentation and integration with multifactor authentication and identity and access management (IAM) platforms. Demonstrate credentials and expertise in this area through focusing on strategic principles and partnerships. This will also build trust with customers that need a secure move to a cloud-based print infrastructure.
- **Harness MPS as an enabler for enhanced security.** Organisations using MPS and a range of security measures – from formal security assessments, audits, and solutions – are ahead of the print security curve – in terms of both confidence and lower data loss. Scalable and flexible security services and solutions will appeal to smaller organisations that are not immune to security risks yet do not have the budget to implement advanced print security measures. Offering regular security reviews as business needs change will also be key to improving satisfaction levels around print security.

Buyer recommendations

The print security threat landscape has expanded to include a variety of home and office devices to support new hybrid ways of working. As intelligent networked devices, MFPs present a 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:

- **Treat print security as a strategic priority.** Print and IT security must be integrated and considered a higher priority. Elevate the importance of securing the print infrastructure to both CIO and CISO stakeholders so that they are aligned on understanding the risks, and the measures that can be implemented to mitigate risks, of unsecured printing.

- **Conduct in-depth print security and risk assessments.** Organisations should 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. For organisations operating a mixed fleet, this may help in understanding the opportunities for device optimisation using a single fleet with consistent hardware security features.
- **Ensure remote and home workers can print securely.** Ensure printers conform to corporate security standards, and in cases where employees have purchased their own printers, develop security guidelines on whether and how these printers can be used. Evaluate print management platforms for support and security monitoring of home printing.
- **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 multi-factor authentication platforms already used in the organisation. Evaluate whether secure print management solutions can operate in a microsegmented network.
- **Formalise processes to respond to print security incidents.** Organisations must ensure that they are prepared for this and have the right processes in place in order to deal with the technical, legal, and reputational fallout from such a breach. This requires the organisation working together to create an embracing set of policies.

Continuously monitor, analyse, and report. Ensure that data from existing security devices, such as security information and event management (SIEM) devices, is collected 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.

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.

Disclaimer:

© Copyright 2023, 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.