Print Security Landscape, 2024

Mitigating the print infrastructure as a threat vector

Print security trends in the US and Europe
Vendor Excerpt: HP
July 2024

QUOCIRCA

Executive summary

The rise of hybrid work has blurred the lines of traditional print infrastructure security. Public networks and less-controlled environments are now commonplace, demanding a more robust approach to print security. Meanwhile, the rise of AI is creating further security challenges, increasing the potential for vulnerable devices to become easier targets and be compromised as a result of weak security protocols. Print manufacturers and channel partners must adapt by offering enhanced security solutions that integrate seamlessly with existing IT infrastructure. This shift presents a significant opportunity. By becoming trusted advisors, the print channel can guide organisations towards comprehensive solutions across device, data, and document security. Prioritising the print infrastructure as a critical element of wider information security strategies will not only safeguard businesses, but also unlock new revenue streams for the print industry.

Quocirca's Print Security Landscape, 2024 study reveals that organisations face ongoing challenges in securing the print infrastructure. Employee-owned printers are viewed as a key security concern by 33% of organisations, which reflects the difficulty in controlling home printing – at both a device and document level – as documents can be exposed to unauthorised users. Despite the growing awareness of printing as a security weakness, organisations are struggling to translate this knowledge into action.

Print-related data breaches remain a significant threat, with 67% of respondents (up from 61% in 2023) reporting at least one data loss incident in the past year. This number jumps to 74% for midmarket organisations. This is leading to a decline in confidence, particularly among small and medium-sized businesses (SMBs), in the overall security of their print infrastructure.

Notably, organisations operating a standardised fleet are less likely to report one or more data losses (59%) than those operating a multivendor fleet (70%). This reflects the challenge of maintaining consistent security across mixed brands compared to proprietary security platforms that are embedded in a standardised fleet. Third-party print management solutions can help with securing printing across a mixed fleet. However, the extra workload for IT in managing a mixed fleet, along with the additional difficulties and hard costs of sourcing multiple print device drivers, integration systems, and monitoring and reporting systems, makes mixed fleets less attractive than standardised ones.

The latest research exposes a concerning gap in print security perception between chief information officers (CIOs) and chief information security officers (CISOs). While both expect increased security spending (77% of CIOs and 78% of CISOs), CISOs are significantly less confident in current print security measures than CIOs. This disconnect is further emphasised by the higher percentage of CISOs (41%, versus 34% of CIOs) who find managing print security challenges difficult. Interestingly, CIOs exhibit greater concern (52%, versus 32% of CISOs) about unsecured home printers, which highlights a potential blind spot.

This fractured view creates a key obstacle. Aligning CIO and CISO perspectives on security is essential for achieving robust information security. Bridging this gap is no longer an option – it is a necessity. Fortunately, Print Security Leaders, as defined by Quocirca's Print Security Maturity Index, are mitigating risks. Leaders are organisations that have implemented a higher number of print security measures than Followers and Laggards. Leaders report lower levels of data loss and have higher confidence in the security of their print infrastructure.

This presents a valuable opportunity for suppliers to position themselves as strategic partners and strengthen their security propositions to help customers mitigate risks associated with unsecured printing in both the home and office environments. By identifying and promoting the best practices employed by these Leaders, suppliers across the print ecosystem can play a crucial role in guiding Followers and Laggards to improve their security posture.

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: HP

Quocirca opinion

HP has advanced its leadership position in Quocirca's 2024 vendor assessment of the print security market. In the past year the company has made significant advancements in its security strategy across all segments – consumer, office, large-format, and 3D print. Of particular note are its new zero-trust print architecture (ZTPA) framework, new embedded security features, integration of security as fundamental to print and PC development processes, and improved alignment and refinement of HP Wolf Security across its print and PC offerings.

In December 2023, HP announced renewed focus in several key areas – its approach to threat containment, end-point isolation for zero-trust environments, and stronger alignment across its PC and print security offerings. Additionally, it views AI as a powerful tool for continuing to stay ahead of novel attacks and is focused on enhancing AI-driven fleet management across its printers, PCs, and collaboration equipment.

HP has also made progress integrating its global security programmes, product strategy, product management, global solutions and services, and technical development teams to elevate customer and partner security outcomes. Additionally, HP continues to lead in brand perception in Quocirca's annual Print Security Study, testament to a mature presence in both the personal systems and print markets.

Vendor highlights

Security-led innovation

HP tightly integrates security and builds resiliency in every aspect of its product development, supply chain, and manufacturing processes. It operates a joined-up approach to security innovation across HP Labs, Print, Personal Systems, Poly/Collaboration, and HP Ventures – a strategy that enables it to view the cybersecurity threat landscape holistically across multiple vectors, including end-point and edge technology devices and infrastructure. These and other vectors provide input and insights that inform its products, solutions and services security features, roadmap, and vision. In addition, the company has an established its Print Security Centre of Excellence, which is staffed with dedicated R&D talent.

Comprehensive and scalable security

HP offers a comprehensive and scalable security portfolio for businesses of all sizes – from small and medium-sized businesses (SMBs) to large enterprises. HP Wolf Security unifies all HP's end-point security capabilities using hardware-based Root of Trust, which protects against firmware replacement attacks regardless of their deployment method and serves as the foundation upon which HP platform security is built. Quocirca believes this is a strong step in ensuring that the security of the hardware is maintained throughout its life.

HP's printer portfolio delivers enhanced security features, including enriched secure boot BIOS protection, hardware-based runtime intrusion detection, control flow integrity, and network behaviour anomaly detection, all with continuous monitoring and self-healing capabilities across HP's print and MFP enterprise portfolio. These are key differentiators in the market. HP also offers several options for multifactor authentication, job accounting, pull-printing, and data loss prevention solutions. Other key investments in 2023 included new operational infrastructure, with device technology advancements in cryptography, embedded device detection, protection, and recovery features. Examples include HP Memory Shield's hardware-based Runtime Intrusion Detection and Control Flow Integrity, HP Security Manager solution enhancements, and the development and launch of HP Authentication Suite and HP Authentication Manager.

Zero-trust print architecture (ZTPA)

In Autumn 2023, HP established an industry-first actionable zero-trust framework principle of 'zero-trust print architecture' (ZTPA) to help clarify requirements needed to streamline and optimise zero-trust implementation at the end point and reduce customer pain points associated with embarking upon and sustaining a zero-trust journey that includes end-point security postures and optimised compliance. The company is also developing a zero-trust end-point playbook for channel and direct customers to speed the planning and implementation of a zero-trust print architecture.

Security offerings

HP's printer portfolio delivers enhanced industry-standard security features, including secure defaults, secure boot, allowlisting (formerly whitelisting), code validation, and write-protected memory. HP enterprise devices enrich the standard secure boot with HP Sure Start start-up protection with self-healing. In addition, HP enterprise printers can continuously monitor themselves for malware, ransomware, and anomalous network communications from the printer and uniquely self-heal from an attack at all levels of the device runtime experience. Rather than setting off an alert and depending on an IT team to come to the rescue, HP's embedded enterprise security automatically reboots and self-heals the device while also providing security operations with integrated SIEM tool system event logs for threat analytics. Another unique feature is the admin-enabled HP Secure Encrypted Print technology, which encrypts and protects customer data and sensitive information from potential man-in-the-middle attacks.

HP Authentication Suite

The new HP Authentication Suite and HP Authentication Manager mobile application comprise an enterprise authentication solution and companion mobile app providing access control and a consistent zero-trust optimised authentication experience across devices.

Zero Trust Print Architecture

Built upon HP's proprietary Sure Start with self-healing technology, ZTPA delivers adaptive detection, protection, and automatic recovery at every level of the BIOS boot-up sequence. HP's core ZTPA functionality includes isolation at the ASIC chip and Trusted Platform Module formatter level, internal continuous monitoring and resiliency of device memory, two-way device communications, HP's Enterprise FutureSmart firmware (that meets and exceeds the NIST SP 800-193 Platform Firmware Resiliency Guidelines), modern end-user authentication, embedded data and document protections, software application security, fleet security management and serviceability tools, external-to-device security compliance and management, and a suite of professional security advisory services.

Advanced hardware security

Key features include:

- **HP Memory Shield.** This includes both hardware-embedded Runtime Intrusion Detection and Control Flow Integrity. These monitor the memory and code execution flow of the printer for unusual activity, detecting alterations such as those associated with zero-day attacks – and initiate automatic recovery without the need for human intervention.
- **HP Sure Start BIOS Integrity.** HP Sure Start validates the integrity of the BIOS code to safeguard the device from malicious attacks. If a compromised version of the BIOS is detected, HP Sure Start restarts the printer from a safe 'golden copy' of the BIOS.
- **Allowlisting (formerly whitelisting)/firmware code integrity.** This checks for authentic firmware digitally signed by HP. Firmware is automatically checked during start-up and throughout the usage of the device. Code is dynamically loaded with integrity checks performed at initial load time and time of use to ensure there has been no tampering with code. If an anomaly is detected, the device reboots to a secure offline state and notifies IT.
- **HP Memory Shield's Hardware-based runtime intrusion detection.** This offers continuous monitoring for in-memory malware injection attacks. It prevents any code alteration in memory when the firmware code is running on the printer. Any anomalous behaviour will cause the device to self-heal back to a safe state prior to the malware injection attack.
- **HP Memory Shield's Control Flow Integrity.** This monitors the execution flow of the device code to detect any anomalies in execution flow. If any anomalous behaviour is detected in execution flow, the device self-heals to a safe state prior to the potential malware attack.
- **HP Connection Inspector.** This provides network behaviour anomaly detection by continuously monitoring and evaluating outgoing network connections to determine what is normal and stop suspicious requests, and automatically triggers a self-healing reboot.

- **HP Security Manager.** This automates continuous assurance and device compliance of security policy settings with its Security compliance tool, which brings printers/MFPs that are out of compliance into compliance based on the customers' global security policies. Security Manager also streamlines device certificate deployment and management and security status visibility of fleet firmware using Security Manager's Firmware Vulnerability Assessment feature.
- **Data protection.** Data protection features include encrypted communications, Trusted Platform Module (TPM), and hard drive encryption with secure storage erase for both Hard-Disk Drive overwrite and Solid-State Drive cryptographic erase. Document security features include pull-print solutions, document and data inspection governance auditing, and counterfeit secure print solutions.

HP Security Manager

HP Security Manager is server-based software that enables customers, partners, and service providers to gain control and management of printer fleet security compliance through the creation, customisation, deployment, management, and reporting of printer security policies with Instant On device compliance automation. In addition, HP has built best security practices into the software for streamlined policy creation, deployment, and remediation. HP Security Manager also provides streamlined device certificate deployment to prevent man-in-the-middle attacks when printing. The tool also provides powerful, real-time visibility of firmware vulnerabilities in minutes.

HP Smart Security

HP's Smart Security for HP+ printers provides essential, robust security by default for security-unfamiliar consumers. HP Smart Security and its cloud-based security monitoring functions are integrated into the mobile and desktop versions of the HP Smart Print App and core to telemetry of the printer, like supplies levels.

Strengths and opportunities

Strengths

- **Strong heritage in security innovation across PC and print technology.** The breadth and scale of the HP Wolf Security programme for hardware, services, and solutions across PCs and print are currently unmatched in the industry.
- **Commitment to innovation.** HP is committed to continued innovation across embedded document security and data protection technologies, expanding partnerships with cybersecurity ecosystem tools focused on end-point security and enhancing scan and capture resiliency across its MFP and Scanjet product lines.
- **Cartridge Security.** HP engages third parties to perform penetration testing to harden not only the printer but the supplies that the company provides. In addition, HP takes steps to make sure that its supplies are not tampered with across the supply chain, including construction, shipment, and operation.
- **Broadest range of print security-focused direct and channel programmes in the market.** This enables HP and channel partners to build security practices and deliver secure print environments for their customers.
- **Deep expertise in security assessments.** HP particularly excels in its rigorous approach to security assessments, which are delivered both directly and through its channel. Services including HP Security Advisory Service (expanded in 2023 from print-only to include personal systems), HP Security Manager, Security Event Management and Analytics Service, channel partner Security Assessment Tools, Firmware Vulnerability Assessment Tool & Print Security Assessment Guide are key differentiators for the brand.
- **Extensive channel ecosystem.** HP's leading market position is bolstered by having the most extensive channel network in the sector, supported by a broad range of channel tools and services to help channel partners build and enhance their security-led services.
- **Focus on hybrid workplace security.** HP has expanded its Security Advisory Services to include recommended security settings for remote and home workers, as well as security training and guides.

Opportunities

- **Deepen IT-centric services.** HP Wolf Security is an ideal foundational platform for IT services providers that would like to enhance offerings with MPS or MPS providers looking to support IT environments. HP should expand partnerships in this space.
- **Provide clarity around AI/ML integration into Wolf Security.** HP is well positioned to educate the market around how AI is applied to security at a detection, monitoring, and remediation level. This is an area where HP can build significant competitive advantage because of the technology innovation it has built through the Wolf Security platform.
- **Expand content and workflow security offerings.** HP's strongest focus is on its leading hardware-security features. However, the market is catching up, and differentiation should also be around content security at an application level.

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.