Securing the Print Estate: A Proactive Lifecycle Approach to Cyber Resilience

Print Security: A Procurement Decision with Long-term Implications

Printers are a long-term investment, with refresh cycles spanning years, yet security is often an afterthought. However, by choosing the right print partner, organizations can not only improve cost-efficiency, reliability and performance – they can also enhance their cyber resilience.

Too often printers are seen as a "harmless box", rather than a sophisticated networked device with hard drives, and communication capabilities, just like PCs. But unlike PCs, which commonly have layers of endpoint security to defend against cyber threats, many printers have limited, or lack entirely, endpoint protection, making it harder for enterprises to detect and respond to threats.

Printer platform security—i.e. the security provided by the printer hardware and firmware—is often overlooked in enterprise security strategies.

A lifecycle approach to securing the print estate ensures long-term corporate resilience. By addressing security at every stage, organizations can strengthen their defenses and ensure their print infrastructure remains a trusted part of their IT ecosystem. Read on to explore key challenges and effective strategies for achieving robust platform security.

"When printer platform security is proactively managed and built-in at the foundations, organizations can reduce risks such as data theft, print job interception, ransomware, zero-day, and man-in-the-middle attacks."

- Steve Inch, Global Senior Print Security Strategist & Product Management Lead at HP Inc.

Supplier Selection and Onboarding: Securing the Print Estate from Factory to Fingertips

The print lifecycle begins in the factory, yet the security of the supply chain is often an afterthought in the procurement process. Embedding printer security requirements from the outset helps build resilience against attacks in the future, but only 38% of IT and Security Decision Makers (ITSDMs) say procurement, security and IT teams collectively define security standards when purchasing printers. A further 60% believe this lack of collaboration puts their organization at risk.

38%

Only 38% of IT and Security Decision Makers (ITSDMs) say procurement, security and IT teams collectively define security standards when purchasing printers.

60%

A further 60% believe this lack of collaboration puts their organization at risk.

Despite the critical role of IT and security teams, these stakeholders are frequently excluded from assessing vendor security claims during the procurement process. When evaluating printer RFPs, many organizations fail to:

Once a printer arrives, verifying its integrity is another challenge. More than half (51%) of ITSDMs cannot confirm if printers have been tampered with in the factory or in transit. Since ITSDMs oversee these devices for an average of four years, integrating platform security from day one ensures long-term reliability, efficiency, and resilience.

Recommendations for Supplier Selection and Onboarding:

- Ensure IT, security and procurement teams collaborate effectively to define security and resilience requirements for new printers.
- Request technical briefings and documentation to substantiate vendor claims.
- Require and leverage manufacturer provider security certifications for products and/or supply chain processes.

Ongoing Management: Maintaining Continuous Platform Security Visibility

Once printers are deployed, IT and security teams can strengthen resilience by actively managing their printer security configurations, which is also vital to comply with industry and cybersecurity regulations. With firmware integrity at the core of printer security, continuous monitoring with automatic, self-healing recovery ensures optimal protection and performance throughout the device lifecycle with dramatically reduced impacts on IT and security teams.

One of the biggest print security challenges IT teams face is keeping firmware updated.

36%

Just 36% of ITSDMs apply firmware updates for printers promptly.

Unpatched printers add to an organization's attack surface, exposing them to low-level attacks that bypass software-based security measures. Other challenges include:

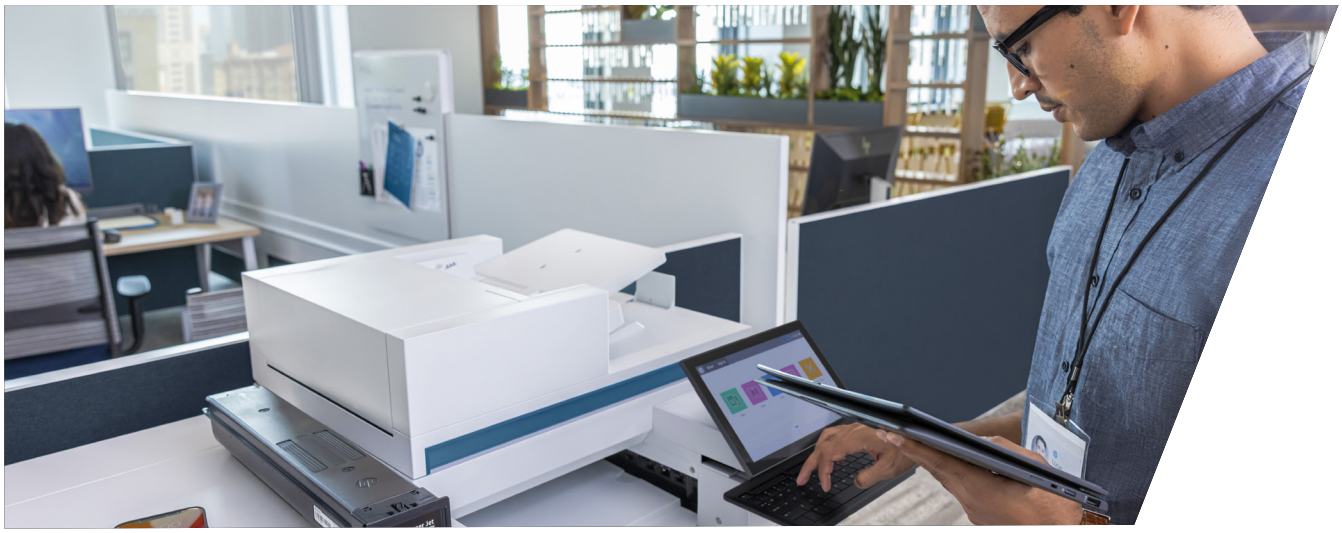
- Managing firmware administration passwords to securely enable configuration changes or technical support.
- Maintaining hardware integrity by controlling changes to physical components.
- Defining the right firmware security configurations and keeping them up to date.

The lack of tools for remote management is also making managing printer security harder and more time-consuming for IT admins, who spend 3.5 hours per printer per month on hardware or firmware security management.

Recommendations for Ongoing Management:

- Apply firmware updates promptly to minimize exposure to security threats.
- Leverage security tools to streamline printer policy-based configuration compliance.
- Monitor event messages generated by your print fleet using security information and event management (SIEM) tools. This helps to comply with industry regulations and standards by continuously monitoring and documenting security events.

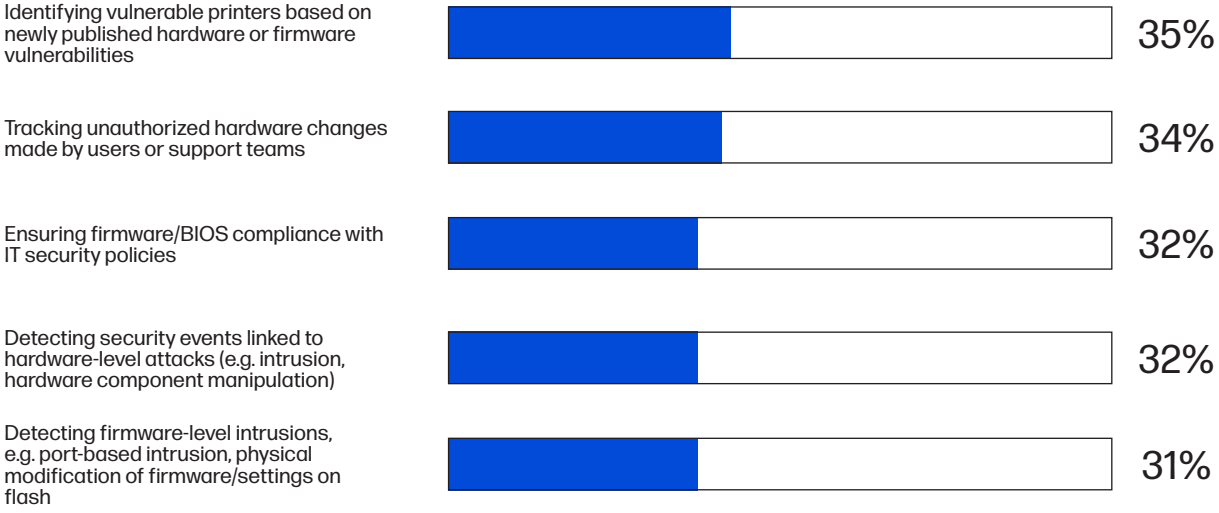
Remediation: Closing Security Gaps Across the Printer Fleet



IT and security teams can further strengthen defenses by monitoring and addressing potential threats to printer hardware and firmware. By proactively securing print devices, organizations can prevent unauthorized access, safeguarding sensitive systems and critical data.

Cybercriminals are constantly searching for weaknesses in organizations' IT infrastructure. It's therefore essential that organizations are protected across their entire estates, including printers.

This means detecting and remediating low-level threats against printer hardware and firmware, so that they don't become the "weak link" that attackers can exploit. However, IT and security teams report facing several challenges:



70%

Beyond cyber threats, 70% of ITSDMs are also increasingly concerned about offline threats, such as people printing and taking away sensitive company information.

Recommendations for Remediation:

- Deploy printers that can continuously monitor for zero-day threats and malware with the ability to prevent, detect, isolate and recover from low-level attacks.
- Monitor device audit logs using SIEM tools to track firmware changes, detect unauthorized modifications, and identify signs of exploitation.
- Choose devices that support secure encrypted printing and data loss prevention (DLP) to protect sensitive information from threats such as unauthorized access, document interception and data exfiltration.

"Printers and other IoT are powerful computing devices, making them attractive targets for attackers to exploit and use as footholds into enterprise infrastructure. As such, organizations must learn to develop mature security requirements when procuring new devices, and to proactively manage their security configuration over the entire device lifecycle."

- Boris Balacheff, Chief Technologist for Security Research and Innovation at HP Inc.

Decommissioning: Overcoming Data Security Barriers to Printer Second Life

Securely decommissioning printers is a crucial final step in the print lifecycle, whether they are being reused, redeployed, resold or recycled. On average, ITSDMs report that their organization has approximately 80 printers that are redundant or are in the process of being decommissioned, presenting an opportunity to improve security and sustainability.

When printers reach end-of-life, ITSDMs say their organizations:

60%	19%	17%	13%	13%
Recycle them	Wipe and donate them	Wipe and redistribute them internally	Destroy them	Sell them

However, data security concerns are a major roadblock, preventing many organizations from repurposing usable devices. 86% of ITSDMs cite data security as an obstacle to reuse, resale or recycling printers – with 39% calling it a “major” or “severe” concern.

Many ITSDMs lack confidence in current sanitization solutions, with 35% uncertain whether printers can be fully and safely wiped. Meanwhile, 1-in-4 believe it’s necessary to physically destroy printer storage drives, and 1-in-10 insist on destroying both the device and its storage drives to ensure data security.

Recommendations for End of Life and Decommissioning:

- Select printers with built-in secure erasure of hardware and firmware data to enable safe second life and recycling.
- To protect private data and prevent data leaks, choose printers that use encrypted storage and can securely delete data when decommissioning, such as through a multiple pass overwrite of hard disk drives or cryptographic erasure of solid state drives.

Taking Control of Print Security: Resilience Through Lifecycle Management

Securing the print estate can be seamless with the right approach and tools. A lifecycle-driven strategy enables IT and security teams to take control at every stage. This means embedding strong security from the outset, including robust requirements during procurement, maintaining visibility and control during operation, and ensuring safe, secure decommissioning when devices reach end-of-life.

By fostering collaboration between procurement, IT, and security teams, organizations can ensure that every printer deployed is not only cost-effective and efficient, but also resilient against evolving threats. Unified management tools and enhanced factory-level security provisioning streamline administration, while advanced monitoring capabilities provide real-time intelligence to detect and respond to threats before they escalate.

When printers are viewed not as a security challenge, but as an integral and manageable part of the digital estate, organizations can unlock long-term value, efficiency and peace of mind. The future of print security lies in being proactive, collaborative, and lifecycle-focused – and it starts today.

Supplier Selection and Onboarding

Ongoing Management

Remediation

Decommissioning & Second Life

About the data
The findings in this report are from a survey of 803 IT and security decision makers in the US, Canada, UK, Japan, Germany and France in 2024. The survey was carried out online by Censuswide