IDC Spotlight sponsored by MPS Monitor
July 2024

Driving Higher Standards in SaaS Security for Managed Print Services

Tim Greene
Research Director
Hardcopy Solutions, IDC

Geoffrey Wilbur
Research Manager
Imaging, Printing, and Document Solutions, IDC

Robert Palmer
Vice President
Imaging, Printing, and Document Solutions, IDC

IDC

SPOTLIGHT

Sponsored by: MPS Monitor

The growing adoption of SaaS solutions as a core element of managed print services necessitates a more sophisticated look at SaaS security.

Driving Higher Standards in SaaS Security for Managed Print Services

July 2024

Written by: Tim Greene, Geoff Wilbur, Robert Palmer

I. Introduction

As of 2024, 53% of organizations worldwide are using software-as-a-service (SaaS) solutions, and a reported 80% of organizations plan to convert all their systems to SaaS by 2025. This rapid adoption is being spurred by the key benefits SaaS delivers, such as fast adoption of solutions, a reduced burden on in-house development teams, and less operational complexity for IT teams. However, IDC believes there is a need to focus on security with SaaS applications, which has been somewhat of an afterthought compared to the focus that adopters have on achieving these benefits.

AT A GLANCE

WHAT'S IMPORTANT

The adoption of SaaS solutions is growing rapidly across markets, including in the print and device management space.

KEY TAKEAWAYS

Many of the leading print and device management SaaS solutions have insufficient security certifications. It is critically important to select SaaS solution partners that prioritize security.

The move to SaaS solutions is accelerating across an array of applications, including those that are core to managed print services (MPS). Print and device management software is a critical piece of the MPS domain, and the move to a SaaS model is well underway in this category. IDC recognizes almost half (49%) of organizations globally with more than 100 employees have already adopted a cloud-based print solution. Some print and device management software suppliers have reported up to 50% year-on-year growth for their cloud-based offerings. However, the fact is that many of the leading print and device management software vendors have not invested in or developed strong enough security capabilities. Most software vendors in the MPS space describe their approach to security in terms of how their solutions can increase document and/or device security in customer environments; however, this platform-focused approach is not enough to ensure holistic security, as on-premises agents are quite often the main targets for malicious intent. It is also the responsibility of SaaS providers to ensure they store and process customer data in compliance with established security and privacy standards and regulations.

Figure 1 – The Four-Step Process for Adopting SaaS

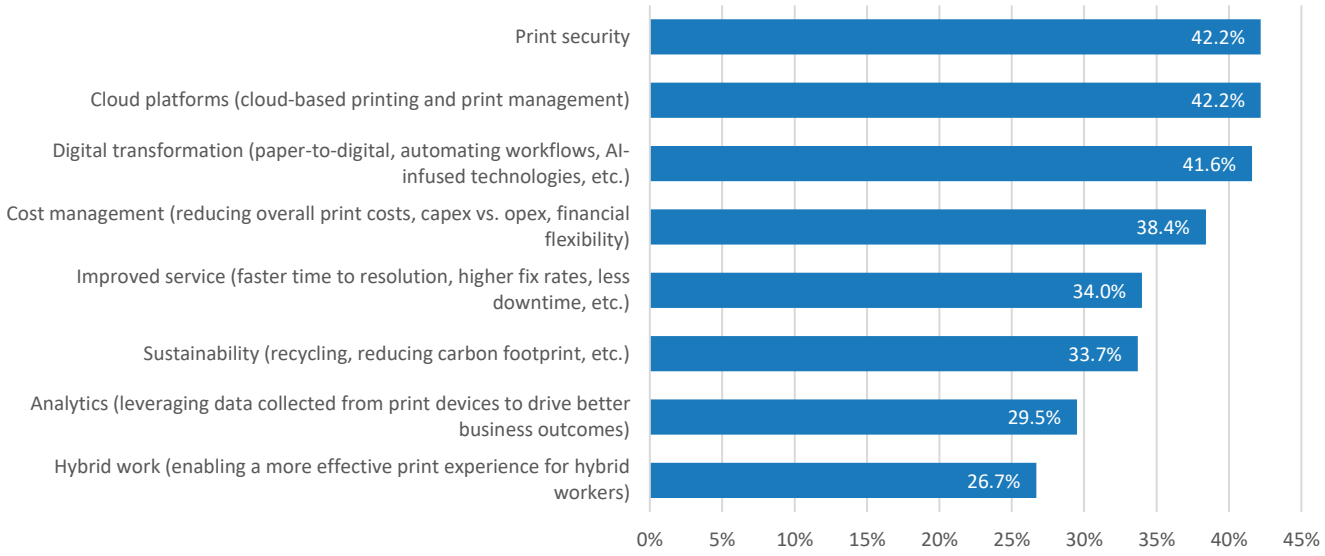
Source: IDC, 2024

While some form of security in managed print environments can be provided by the print and device management software vendor, real security comes from also adopting a software solution that is continuously and independently tested, and that complies with international standards. It is this vital fourth step in the SaaS adoption process that needs to be addressed.

A Strategic Approach

Despite an ongoing transition to digital information, print remains an integral and critical business function and a vital form of communication across all environments (home/personal, education, and office). Companies are seeking ways to modernize IT, and print is part of that discussion, leading to the increasing adoption of SaaS as part of managed print agreements. However, there is a disconnect between what companies report as their top priorities and what current managed print solutions can actually provide. While security is one of the top priorities for companies when it comes to their print and document environments, few MPS solutions offer the highest levels of security that modern print architectures demand.

Figure 2 – Top 3 Business Priorities for Print and Document Environments



Source: IDC, 2024

To meet the needs of modern print architecture, solutions need to be impactful, cloud native, and secure. There are critical risks associated with incomplete security.

- A 2023 study from the Clark School at the University of Maryland indicates that there are over 2,200 cyberattacks every day — that equates to one every 39 seconds. Internet of Things (IoT) cyberattacks alone are expected to double by 2025.
- According to Accenture's *Cost of Cybercrime Study 2023*, 43% of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves.
- According to IBM's *Cost of a Data Breach 2023* report, it takes a company 197 days on average to detect a breach and up to 69 days to contain it.

The consequences of cyberattacks are severe as well. They include:

- Financial losses
- Loss of productivity
- Reputational damage
- Legal liabilities
- Business continuity problems

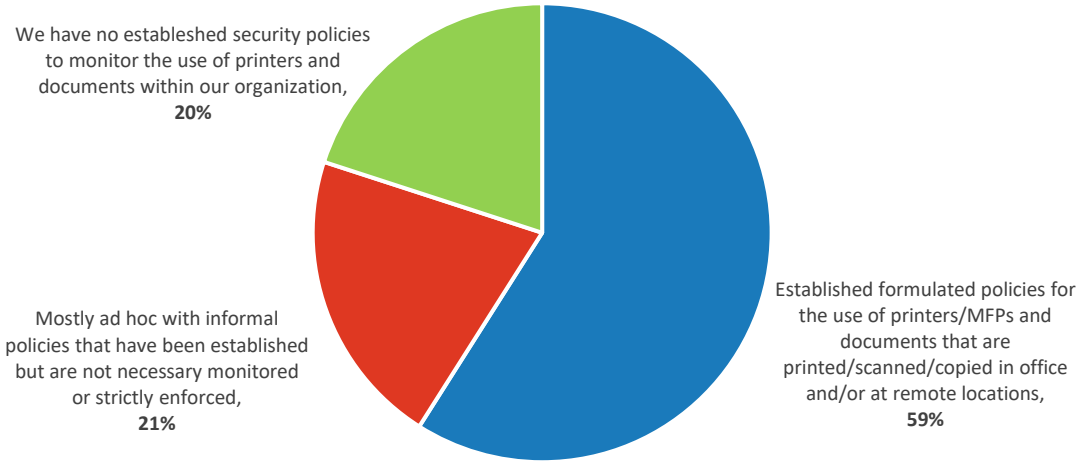
IDC sees more companies adopting managed print services in an effort to modernize systems and gain all the benefits of print and device management, but the majority of organizations (72%) say the impact of the pandemic and subsequent transition to hybrid working has made it harder to keep pace with security challenges. Zero trust architecture is a security model that assumes that every network device and connection is a threat. Globally, 64% of enterprise organizations have already implemented "zero trust" security initiatives and another 34% have plans to do so, but just 34% of businesses are "very confident" in their organization's overall print security program. Identity is the new perimeter; it is no longer safe or

even feasible to assume that everything that sits behind the corporate firewall is protected. This paradigm needs to be applied to SaaS platforms as well: on-premises agents, SaaS platforms, and their user accounts should all be treated with the same zero trust approach that is used for everything else in a company's network environment.

Just as many of the leading print and device management ISVs have not developed robust security capabilities, many customers have underdeveloped security policies. Over 40% of respondents to an IDC survey reported that their approach to print/document security has been mostly ad hoc with informal policies that have been established but are not necessarily monitored or strictly enforced, or that there are no established security policies (formal or informal) to monitor the use of printers and documents within the organization.

Figure 3 – Current Approach to Print Security Rules and Policies

Q. What best describes your organization's approach to establishing formalized print security rules or policies?



Source: IDC, 2024

Best Practices to Ensure Platforms Do Not Induce Additional Security Risks

The potential for significant losses combined with frequent and growing threats make security a vital element of modern network infrastructure. Companies recognize this, with 71% of those surveyed by IDC globally expecting their cybersecurity budgets to increase over the next three years.

While all of the leading print and device management software solutions address security, their focus on security is often limited to the security of documents and devices. Device management tools represent a particularly risky part of a company's network environment because they essentially work through an on-premises data collection agent (DCA) that, if arbitrarily manipulated or corrupted, can be used by bad actors as an attack vector to gain unauthorized and permanent access to the customer's networks.

Most print and device management solutions focus on print cost reduction and effective device management, but vendors have failed to develop robust security features that meet the needs of modern SaaS environments. Ironically, some of the top priorities for managed print agreements are related to security, yet the measurements provided by most print and device management software make comparisons against unmanaged and non-controlled environments. As such, they are insufficient.

Best practices:

- Find or develop your own corporate security policies and integrate security at the outset of a project.
- Carefully evaluate the security posture of your SaaS providers by requesting proof of compliance with internationally recognized standards.
- Find vendors that use software that leverages modern and secure coding techniques.
- Develop a process for regular security audits and stay current with updates and patches.
- Be vigilant; keep your IT team updated and empowered with regular training sessions.
- Build on trusted security frameworks and libraries.
- Limit access, streamline roles, restrict unnecessary permissions, and guard against misuse.

It is imperative that managed print solutions providers select only SaaS vendors that follow these best practices. Software vendors should be expected to have at least the following certifications:

- ISO/IEC 27001
- AICPA SOC2 Type 2
- CSA Star Level 2

In addition, certifications should be recent and renewed/retested regularly. SaaS vendors should also commit to perform recurring sessions of penetration testing, vulnerability assessments, and code reviews, and should be ready to provide customers with proof of their testing results under the terms of a non-disclosure agreement (NDA).

II. Benefits

Printer monitoring and print fleet management software with full device security helps companies meet rigorous compliance objectives and, more importantly, avoid costly data breaches. Furthermore, a strong device management solution also proactively reduces print job tickets, which makes an organization's IT operations more efficient.

An example of a device management platform meeting and exceeding the above requirements is MPS Monitor. This SaaS solution facilitates remote monitoring and management of printers, multifunction devices, and label printers with unparalleled efficiency, while offering an extraordinary commitment to security:

- **Compliance with company and industry security policies and standards:** MPS Monitor invests significant resources in testing and development in print security. These initiatives have seen it secure multiple third-party certifications (ISO/IEC27001 – certified since 2016; AICPA SOC2 Type 2 – audited yearly since 2021; CSA Star Level 2 – renewed yearly) that the rest of the market is only now starting to catch up on.
- **Modern programming language:** While most print and device management software is based on original coding that may be 20 years old, MPS Monitor completely rewrote its code to make it compliant with the latest development standards (like OWASP Top 10 and SANS), meaning its code is very new and up to date, not just an extension of old programming.
- **Continuous testing:** The most critical component of the platform, the MPS Monitor DCA, is code reviewed and security checked by external security firms before every code release, while the associated cloud systems are penetration tested at least every six months.

- **Secure authentication:** While many SaaS providers still just rely on weak authentication techniques like simple logins and passwords, MPS Monitor supports both single sign-on (SSO) using Active Directory or Azure AD, and multifactor authentication (MFA) via mobile app or email.

III. Trends

Software solutions in the print and device management segment are aggressively moving to the cloud, but enabling an older software solution to work in the cloud is not nearly as secure as developing solutions for the cloud from the ground up: a cloud-native design approach involves adopting a security-first mindset throughout the entirety of the solution design and implementation process.

Often, legacy applications are adapted to be executed as cloud services from Microsoft Azure or AWS without any redesigning/rewriting of the old code, without implementing true multitenancy and data separation, and with little or no API security or strong authentication. Software platforms that were designed to run safely and privately inside the inner perimeter of a corporate network are now suddenly exposed to all the risks coming from the public internet, without having been designed, implemented, or tested to ensure protection against these new threats.

Reducing customers' IT and operational costs by moving applications to the cloud cannot be the only goal to reach, particularly if it comes at the expense of decreased security for applications and data. A viable and effective cloud strategy needs to balance budget and cost-saving requirements with a new and much more stringent approach to security and data protection.

The move to a more modern print architecture is not a "one-time" project. Instead, it is a continuous process that seeks to maximize employee productivity through secure anytime, anywhere access to information and resources that meet the needs of a modern workforce. Tools and technologies in the print and device management segment must be adaptable to provide the best possible user experience, while making zero sacrifices in terms of security and rules-based printing.

In today's time-sensitive, "on-demand" world, users increasingly rely on knowledgeable channel partners to help identify processes and products that contribute to the effective running of modern IT architectures.

IV. Vendor Profile

Established in 2010, MPS Monitor has emerged as a pioneering force in the global MPS industry. Since its inception, MPS Monitor has drawn a path of success across all continents, with headquarters in Europe and direct operations in North America and Asia. At the heart of its mission lies a commitment to establishing itself as the market leader in remote monitoring and management (RMM) of printers and multifunction devices of all brands.

MPS Monitor's mission is to help office equipment dealers, MPS providers, and aftermarket supplies resellers to proactively and effectively manage their fleets remotely using a modern and secure SaaS solution. Presently, MPS Monitor boasts a global presence, with over 3,500 active dealers spanning across 75+ countries worldwide overseeing the monitoring of over 2 million print devices generating 50 billion pages annually. Supporting this vast network are support teams strategically positioned across Europe, the Middle East, and Africa (EMEA), North and South America, and Asia/Pacific.

At the forefront of MPS Monitor's offering stands MPS Monitor 2.0, the latest iteration of its flagship product. Purpose built as a cloud-native SaaS solution, MPS Monitor 2.0 represents a paradigm shift in device management, facilitating the delivery of managed print services with unparalleled efficiency. Designed to empower dealers with streamlined processes for billing, meter reading, and automated supplies fulfillment, MPS Monitor 2.0 represents the pinnacle of fleet management technology.

In today's evolving MPS landscape, cloud print and remote management technologies are powerful tools that help MPS providers deliver top-notch service at lower prices. However, they also introduce new challenges to the MPS model, including heightened security risks, due to a much larger attack surface, and regulatory compliance obligations. The adoption of MPS software is no longer solely based on expected ROI but also on its ability to ensure holistic security. The complexity of MPS SaaS security demands a comprehensive approach — one that involves routine penetration testing, vulnerability assessments, continuous monitoring, mitigation and disaster recovery plans, and adherence to recognized security standards.

Dealers and MPS providers must treat these as essential prerequisites for the SaaS platforms integrated into their services. Data collection agents are no exception, residing within the network infrastructure while maintaining continuous connectivity to the SaaS cloud service. This connectivity involves data exchange, command reception, software updates, and, in some instances, external user access, amplifying the potential for security vulnerabilities.

MPS Monitor stands out as a leader in this arena, offering an unparalleled commitment to security. With full compliance to stringent security standards and certifications, including ISO/IEC 27001, SOC 2 Type 2, and CSA Star Level 2, MPS Monitor ensures maximum confidentiality, integrity, and availability of data. The platform's information security management system (ISMS) extends its security features to benefit dealers and clients, facilitating GDPR compliance and addressing the rigorous requirements for handling personally identifiable information (PII).

Moreover, MPS Monitor's back-end cloud infrastructure, hosted within secure datacenters, undergoes continuous monitoring, extensive logging, and bi-annual penetration testing by external cybersecurity firms. The platform follows the principles of "security and data protection by default and by design," implementing robust security controls throughout the development and release process. Features such as single sign-on (SSO) integration and multifactor authentication (MFA) enhance user authentication security, while stringent physical security measures safeguard the datacenter against unauthorized access.

With a comprehensive business continuity and disaster recovery plan in place, MPS Monitor ensures the continuity of its cloud services, even in the face of unforeseen events.

The platform helps dealers and MPS providers to improve operational efficiency and reduce their service and support costs by means of unique features like device web access (DWA), which allows a user to connect to the printer's embedded web server remotely and seamlessly. By means of this access, an MPS provider may remotely reconfigure devices, apply security policies, disable unnecessary protocols and ports, and ultimately make print devices more secure.

The DWA feature is very powerful but also extremely critical because, if misused or accessed by malicious actors, it may grant unauthorized access to the customer's network resources. MPS Monitor has implemented a high number of security measures, procedures, and controls to ensure that the usage of DWA does not introduce additional security risks.

MPS Monitor's global web infrastructure is protected by a third-party web application firewall cloud system that not only blocks malicious web activities and defends the system from distributed denial-of-service attacks (DDoS), but also provides local web endpoints for the various regions (EMEA and Americas currently available). This ensures that customers who have strict policies on IP geo-blocking can still use the service in a secure way, without creating exceptions to their security policies.

Challenges

All SaaS companies face a similar challenge in that, as the number of features, the size of their databases, and the number of subscribers all increase, so does their security exposure and attack surface. The more a SaaS platform evolves from being a local, niche player to becoming a global market leader, the more it becomes an attractive target for hackers and malicious actors.

Similar challenges affect end users where, with the many different print and device management SaaS solutions available, one of their bigger concerns is recognizing solutions that meet certain industry standards for security. At the same time, they do not want a vendor that shows compliance on a "one-time" basis, instead preferring solutions that are continuously tested to provide a truly secure architecture.

For SaaS software, one of the major risks is account hijacking, where hackers take advantage of employees' unsecured personal devices to gain access to business-critical SaaS solutions. Another one, directly related to that, is supply chain compromise, where bad actors infiltrate themselves into the SaaS development pipeline and plant malware into the legitimate code base that the SaaS vendor deploys as part of its solution — often across hundreds of thousands, or even millions, of customer networks.

Data collection agents are a critical element of a SaaS supply chain, as they can easily become a gateway to the customer's networks, making print and device management platforms a very appealing target for bad actors. High-profile historical examples of vulnerable SaaS supply chains being hacked are likely to draw even greater focus to this category of potential weaknesses in network security.

Other issues identified in a recent IDC survey point to budgets as being a major factor. Companies report that they believe "security risks are too small to justify the costs to fix" or that their "IT security budget is not big enough." These objections fail to consider that the average cost of a breach is close to $1 million, while the cost of a SaaS solution for protection against these breaches is a miniscule fraction of that figure. At the same time, SaaS solutions provide additional operating benefits. The same IDC survey points to the fact that many companies either do not have an IT security strategy or their employees do not adhere to print security policies. The fact that many companies report that they "don't see a need for a printer/copier/MFP security policy" or that they believe their devices are safe because they are behind the company's network firewall is only further proof that there is a major awareness problem when it comes to print and device security.

V. Conclusion

IDC believes the office print market is undergoing a period of modernization. In this new era, IDC observes increased adoption of managed print services that limit print costs, reduce the requirements for on-premises print infrastructure, and align print resources with an increasingly mobile workforce. Many MPS solutions include document security as a component of print and device management software, but fall short when it comes to device security and the disciplined, constant, testing required to maximize device security and comply with zero trust architecture. Security in SaaS solutions for device and print management is generally misunderstood, and very few technology suppliers match the level of focus, investment, and achievement that MPS Monitor has shown. Dealers play a vital role in helping the buyers of print solutions identify how to reduce the risks associated with insecure solutions.

"We're in an era of modernization in the office printing market, and device and print management SaaS security is generally misunderstood."

MESSAGE FROM THE SPONSOR

In today's digital landscape, safeguarding information within IT and printing infrastructures is paramount. The aftermath of a security breach extends beyond financial implications, impacting an organization's reputation irreparably. Therefore, businesses, both public and private, are meticulously scrutinizing SaaS platforms and cloud applications for their security credentials, recognizing their critical role in decision-making processes. As customer demand for secure solutions rises, prioritizing secure MPS platforms becomes imperative for instilling confidence and safeguarding network integrity and protecting valuable data assets. In this modern landscape, where SaaS is replacing most old and legacy systems, a holistic security approach is essential, emphasizing routine testing, vulnerability assessments, and adherence to recognized standards such as ISO/IEC 27001, SOC 2 Type 2, and CSA Star Level 2. For further information and a deeper understanding of MPS Monitor's approach to cybersecurity, please read our Technical Whitepaper and visit our website at www.mpsmonitor.com/mps-monitor-security.

About the Analyst

Tim Greene, *Research Director, Hardcopy Solutions*

Tim Greene is a research director within IDC's Hardcopy Solutions group. He is responsible for coverage of the large-format printing, 3D printing, and digital signage markets. Tim's research and insights help companies in these areas understand and take action on digital transformation of their business. Prior to joining IDC, Tim held roles with InfoTrends, BIS Strategic Decision, and GIGA Information Group covering the digital printing market.

Geoffrey Wilbur, *Research Manager, Imaging, Printing, and Document Solutions*

Geoff Wilbur is a research manager within IDC's Imaging, Printing, and Document Solutions group. He produces research, forecasts, and analysis in the printer, multifunction peripheral (MFP), and adjacent markets. Geoffrey has two decades of experience producing market research and analysis within the technology and telecommunications industries.

Robert Palmer, *Vice President, Imaging, Printing, and Document Solutions*

Robert Palmer has more than 25 years of experience in product management, strategic planning, market research and analysis, and forecast development within the document imaging industry. Prior to joining IDC, Robert served as chief analyst for BPO Research, and had previously led the Digital Peripherals Solutions practice for InfoTrends.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com