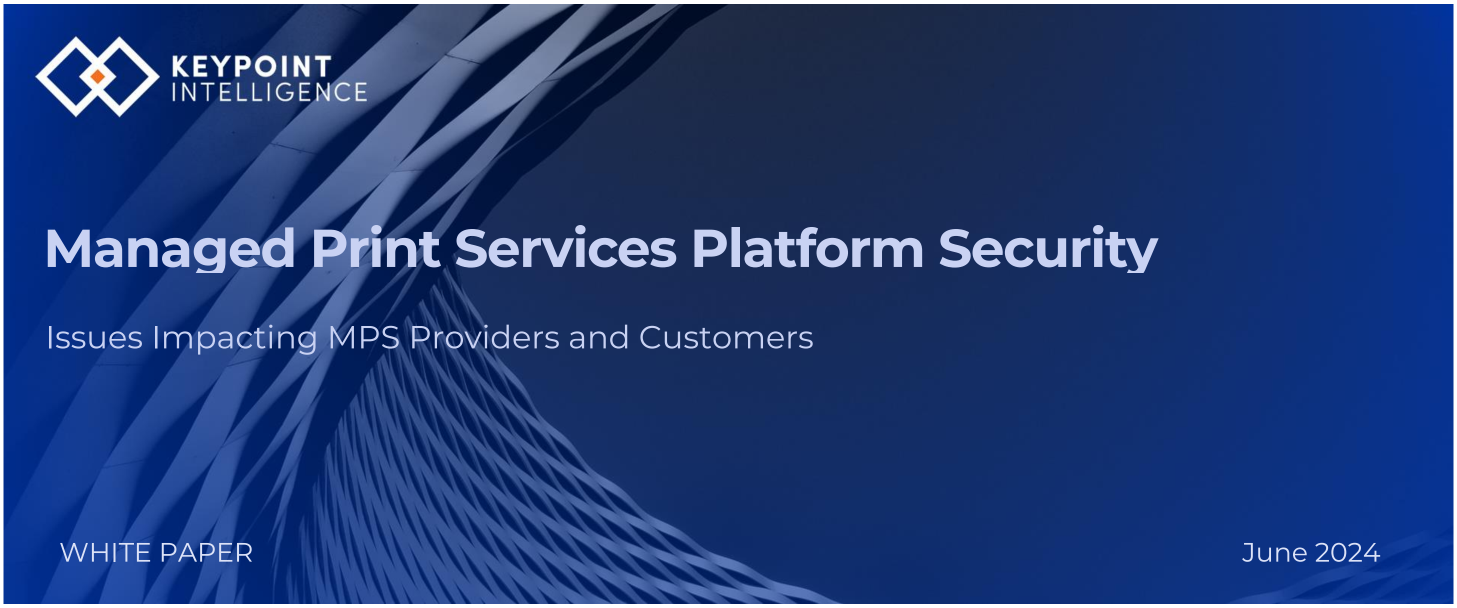


Managed Print Services Platform Security

Issues Impacting MPS Providers and Customers

WHITE PAPER

June 2024

TABLE OF CONTENTS

FIGURES

TABLES

INTRODUCTION

Managed Print Services (MPS) providers face a long list of pressures in an ever-evolving market landscape, from maintaining profitability while keeping costs low for clients to protecting and (ideally) growing market share in the face of competition on many fronts. There are also the challenges brought on by remotely monitoring and managing devices efficiently while consistently delivering high-quality service that meets or exceeds customer expectations.

But arguably the most complex issues revolve around cybersecurity challenges. Not only do MPS providers need to worry about the cyber-readiness of their own businesses, but they also have the additional responsibility of keeping customer environments and information secure. As they handle sensitive customer data and integrate their services into broader IT environments, cybersecurity issues become particularly critical.

According to a Keypoint Intelligence research study, nearly 60% of IT-purchase decision-makers in the US reported that that they outsource management of their organizations' print infrastructure to an MPS provider. Not surprisingly, Keypoint Intelligence studies consistently have shown that cybersecurity is viewed as the top priority for IT managers. But the cybersecurity focus of IT departments tends to be on thwarting phishing attacks and securing traditional targets such as network infrastructure, PCs, and servers; relatively little attention is paid to printers and MFPs that are every bit as vulnerable. With their robust operating systems and key placement at the intersection of the Internet and the corporate network, printers and MFPs are an ideal target for bad actors looking to gain access to the network or enlist "bots" to serve in a denial of service (DNS) attack.

That means that any potential MPS engagement needs to start with a conversation about the security of the platform housing the customer's data, as well as steps taken to harden the data collection agent (DCA) employed to communicate between the customer's site and the remote platform. It is incumbent upon providers and purchasers of MPS services to ensure that the solutions they choose are verifiably secure. Dealers must carefully select and manage third-party vendors to ensure they meet the security standards their customers expect. This includes assessing the security practices of any cloud services or software solutions integrated into the MPS offering.

ANALYSIS

MPS Providers Are in the Middle...and on the Hook

Office equipment dealers and other resellers who provide MPS to their clients are in a difficult position. On the one hand, their customers hold them responsible for the protection of their data and network integrity as it relates to the print infrastructure under management. But on the other hand, the dealer is not the developer of the monitoring and management tools employed, and hence must put their faith in the suppliers of those tools that vulnerabilities have been tested for and remediated.

Indeed, the past few years have seen the emergence of a dangerous type of threat, now widely known as supply-chain attacks. In the software and cloud-services realm, the malicious actor targets the weakest point in the software supply chain of the on-premises or cloud platforms used by providers and exploits that to plant malware. This gives the attacker access to many thousands of endpoints and customer networks through a single successful hack. MPS providers need to be aware of such risks—and select partner suppliers accordingly.

The solution: Secure MPS. MPS providers need to seek out software platforms ensuring proven end-to-end security for the entire print infrastructure. SaaS vendors that develop and provide MPS software platforms are required to demonstrate their security posture by providing proof of their security features, audit and testing activities, and certified compliance to recognized security standards and regulations. To alleviate customer concerns about the security of MPS systems and their data, MPS dealers can implement and communicate a comprehensive approach to cybersecurity. This builds trust and reassures customers that their sensitive information is handled responsibly and securely.

Here are key requirements that MPS dealers should insist upon from these providers to ensure robust security and service quality:

- **Security Standards and Compliance:** The upstream provider must adhere to recognized cybersecurity standards (such as ISO/IEC 27001, SOC2, CSA Star) and industry-specific regulations (like GDPR, HIPAA, or PCI DSS if applicable). This adherence should be verifiable through regular audits and compliance certifications.

- **Transparent Security Practices:** Providers should clearly document and communicate their security practices, including data encryption, access controls, and their policies for handling security breaches. This transparency helps dealers assess the security measures in place and communicate these effectively to their customers.
- **Regular Security Updates and Patch Management:** The provider should have a robust system for regularly updating and patching their software to protect against known vulnerabilities. This includes providing timely security patches, firmware updates, and informing the dealers of any required actions on their part.
- **Advanced Data Protection Features:** Ensure the provider offers advanced data protection features such as end-to-end encryption for data at rest and in transit, secure authentication methods, and comprehensive logging and monitoring capabilities.
- **Incident Response and Support:** The provider should have a well-defined incident response plan and be capable of providing immediate support in the event of a security breach or technical issue. This includes providing resources for forensic analysis and helping contain and mitigate the incident.
- **Vendor Security Assessment:** Regular security assessments and evaluations of any third-party vendors used by the provider are crucial. This helps ensure that all components of the MPS ecosystem maintain high security standards.

Secure MPS: What to Look For

A Secure MPS infrastructure will take into account potential cybersecurity exposures at every stage, from the print devices themselves to the DCA that monitors them, and to the back-end platform that enables remote management and houses the data. Here are attributes to insist upon in a comprehensive, holistic approach to security in an MPS engagement:

- **Device Security:** Printers and other office devices are potential entry points for cyber attacks. MPS providers need to maintain the security posture of these devices to prevent unauthorized access, data theft, or access to the wider network via the device’s Internet and network connections. This involves regular updates to firmware, ensuring that device I/O and security settings remain in compliance with an organization’s desired policies, and disabling of protocols with known security vulnerabilities (such as SNMP v1) that could be exploited.

- **Network Security:** Managed print devices are connected to the client's network and thus pose a risk if they are not properly secured. MPS providers must ensure that these devices are appropriately segmented within networks, using firewalls and network monitoring tools to detect and mitigate potential intrusions.
- **DCA Security:** A code review by an accredited third party of the DCA's source code will reveal any overlooked risks, such as the use of open-source libraries with known vulnerabilities. Such a review should be conducted with every major release of the DCA before it is deployed at customer sites. The DCA should also be digitally signed, to ensure that it has not been compromised after the fact.
- **Data & Communications Security:** There's a risk of this data being intercepted or modified during transmission. Ensuring that data is encrypted during transit can mitigate this risk.
- **Incident Response and Management:** Having a robust incident response plan is critical. MPS providers should be prepared to respond quickly to security breaches, including notifying affected parties, isolating affected systems, and restoring services securely.

Risks Associated with SaaS Platforms

If your MPS platform provider uses cloud-based management systems, several specific cybersecurity issues arise. These systems provide benefits like remote monitoring and management of print devices, but they also introduce potential vulnerabilities. Here are some key security concerns:

- **Data Transmission Security:** Data transmitted between MPS devices and the cloud platform must be secured to prevent interception or tampering. Using strong encryption protocols, such as Transport Layer Security (TLS), for all data in transit is essential.
- **Cloud Database Security:** Data stored in the cloud must be protected against unauthorized access and breaches. This involves not only using encryption to secure the data at rest but also ensuring that cloud storage configurations are correctly set to prevent data leaks. Additionally, providers must select cloud services that comply with the highest security standards and certifications relevant to their industry.

- **Access Control:** Proper access control mechanisms need to be in place to ensure that only authorized personnel can access sensitive data and management interfaces. This includes using Multi-Factor Authentication (MFA) and Single Sign-On (SSO), managing permissions tightly (principle of least privilege), and regularly reviewing access rights.
- **Service Continuity and Reliability:** Relying on cloud services introduces concerns about service availability. MPS providers must have contingency plans in case of cloud service outages, ensuring minimal disruption to their services. This might involve backup services or redundant systems.
- **Vendor Security Practices:** The security of the cloud-based fleet management system depends heavily on the security practices of the service provider. MPS providers must evaluate the security measures implemented by SaaS vendors, including their compliance with Security regulations and international standards, their incident response capabilities, and their track record of handling security breaches.

The Importance of Testing and Follow-Up Rechecking

In most security incidents involving web and SaaS platforms, the root cause lies in simple yet dangerous flaws in application and infrastructure security, which can be easily discovered by threat actors using automated bots and web scanners. These common issues, when found by hackers, are very often kept silently aside for long time, and then exploited when appropriate by the cyber criminals to reach their malicious goals.

Legacy applications, old and outdated software stacks and libraries, and poorly configured web and server infrastructures are a very rich playground where to find many of these flaws and issues. There is only one effective defense against the risk of exposing a potentially vulnerable system: to run frequent and recurring rounds of penetrations tests and code reviews.

Typical vulnerabilities that can be found during the testing sessions may include:

- Instances of stored cross-site scripting (XSS), which could allow an authenticated user to unknowingly store a malware payload within the server.
- Authentication tokens stored in the browser’s local storage, which is a less secure option for storing data in comparison to cookies. With the existence of XSS, a user’s session token could be exfiltrated from the local storage, ultimately resulting in a session-takeover attack.

- Arbitrary file upload due to unprotected or unsanitized upload functions.
- Arbitrary file read (a vulnerability that allows unauthorized access to a program's ability to read files) and path traversal (a specific type of file read vulnerability that exploits weaknesses in how a program handles file paths), which can lead to unauthorized file downloads from the server.
- User credential exfiltration.
- User enumeration for Login and Reset Password functions.
- Single-sign-on (SSO) Domain enumeration.
- Authentication bypass and infoleak problems.
- Tampering with log messages, where a specific HTTP header can be added to the request, resulting in the spoof of the logged source IP address.

These kinds of problems are very common in most web applications and infrastructures that are not routinely subject to penetration testing activities and, when these are present, they generally remain exposed and vulnerable for long time, as they are extremely difficult to discover by anyone other than an attacker. Once discovered, these problems need to be fixed as soon as possible. Moreover, the effectiveness of the remediation steps taken needs to be tested again. Industry best practices dictate that, after each penetration testing activity, a full recheck needs to be performed not later than 30 days from the testing session, to verify and ensure that issues originally deemed Critical or High-risk have been solved.

How MPS Monitor Addresses These Challenges

Clearly, the MPS market is undergoing significant transformation, predominantly influenced by escalating demands for enhanced security measures amidst rising cybersecurity threats. MPS dealers cannot possibly keep abreast of the myriad potential vulnerabilities present at each point in the system. This is where a trusted MPS platform provider is crucial. Such a partner will ensure the robustness of the tools employed by the dealers, so the dealer can focus on their customers and core business activities.

An example of a comprehensive and holistic approach to security in Managed Print Services is provided by MPS Monitor, whose end-to-end security posture is described in this analysis. Its 2.0 platform has passed security-verification testing performed by independent third parties, and it is subject to continuous audits and compliance verifications. Testing and auditing are performed on all the platform's components: the DCA that resides at the customer site, the tool's features for maintaining managed devices in a secure posture, the cloud platform that houses customer data, and the end-to-end software distribution and update process. The company also holds some of the most accredited security certifications available for cloud-services providers. In this analysis we will examine the security approach, methodology, and main procedures that the company applies to maintain its security profile. We will also describe the way the company engages with specialized external partners and consultants that can offer focused and highly skilled support in each risk area.

MPS Monitor Security Features and Best Practices

The table below summarizes the findings of this analysis and can be useful to compare MPS Monitor's security features with platforms from other vendors.

Table 1: MPS Platform Best Practices

Security Feature/Practice	Frequency & Notes
Device configuration policy management	For HP devices through SDS, for other brands through Device Web Access
DCA code review	Before each DCA release
DCA code signing check	Before each DCA release
DCA update process	Every 6 months
Web penetration testing	Every 6 months
Advanced user authentication	Through Okta Identity, or with native SSO to Azure AD and MFA
GDPR compliance	Ongoing
Compliance to standards	ISO/IEC 27001, SOC 2 Type 2, CSA Star Level 2
Disaster recovery	Ongoing
Incident response	Ongoing

MPS Monitor Testing and Certifications

Some of the security measures MPS Monitor has undertaken for its platform components are detailed below.

Web Penetration Testing

MPS Monitor submits its back-end systems, which house data of MPS providers and their customers, to regular rounds of penetration testing conducted by specialized security firms. This kind of testing is performed at least two times a year. The aim of the testing is to verify the overall security resiliency of the company's IT infrastructure via penetration-test activity that mimics what real-world hackers might attempt. In other words, the testing firms' "white-hat" hackers attempt to break into MPS Monitor's IT systems from various entry points and using many different attack techniques.

MPS Monitor has in place a policy that requires the company to perform two rounds of web penetration tests each year and, where possible, to get the testing done by different security firms so that different teams can potentially find and exploit different vulnerabilities. The benefit of frequent testing is that any vulnerabilities inadvertently added during ongoing development of the platform and implementation of new features will be caught. If a critical vulnerability is found during testing, the company commits to fix it and perform a re-test by the same security team, to ensure that the issue has been remediated, within 30 days from initial testing.

Device Configuration Policy Compliance Validation Testing

Keypoint Intelligence was commissioned by MPS Monitor to conduct validation testing to determine if the company's MPS Monitor 2.0 platform—when used in conjunction with compatible devices—satisfied the functional requirements put forward in Keypoint Intelligence's Policy Compliance test methodology. Through hands-on testing, Keypoint's analysts verified the claimed features and effectiveness of the MPS Monitor 2.0 platform in its ability to:

- Discover and highlight at-risk firmware (that is, out-of-date firmware with known and/or likely vulnerabilities) that are still in use on devices.
- Provide fleet-scalable, secure firmware update capability.
- Ensure a customer's devices are secured to a vendor's and/or customer's recommended settings (via templates, policies, or similar mechanism).
- Provide a method to discover out-of-compliance devices.
- Generate a report (or dashboard view) showing at-risk devices.
- Provide a way to automatically apply the desired settings to bring devices back into compliance.
- Provide on-going checks to ensure the devices are still in compliance with the recommended settings.
- Automatically detect newly connected but un-configured device(s) attached to the network and automatically apply the policy designated by the administrator for new devices.

These important fleet-security features were verified to work when used to manage HP Inc. printers and MFPs fully supported by the HP SDS platform.

DCA Code Reviews

The MPS Monitor DCA for Microsoft Windows, used to collect and transmit device and usage data to the MPS Monitor cloud system, is subject to a rigorous and recurring cycle of Application Security Assessments, carried out by a cybersecurity consulting firm. A team of security specialists is engaged at each code release to verify all the possible vulnerabilities of the MPS Monitor DCA agent. The testers examine the source code as well as any artifacts and events created when the application is running. If critical vulnerabilities are identified and reported, MPS Monitor immediately removes them and submits the code base for a new review.

To complete the review and approve the release of each code base, testers need to perform a detailed and formalized check-list of controls aimed at ensuring that the code being released is fully compliant with the security requirements set out by the company, and it does not contain any unwanted, uncontrolled and potentially dangerous element, that might have been added by mistake by the developers themselves or, worst case, by a malicious actor who compromised the DCA build process by injecting arbitrary code to perform a supply-chain attack.

This routine examination is performed before each new release of the DCA agent, to make sure that the version of DCA installed in customers (even after a self-update) does not introduce new and unexpected vulnerabilities nor additional risks in the target network.

DCA Code Signing

Having a tested code base does not mitigate risks unless the developer ensures that the code hasn’t been altered or tampered with during the software distribution process. A basic yet effective best practice for this is to ensure that all the code that is included in a setup, update, or other kind of distribution package is fully signed with the developer’s code-signing certificate.

Unfortunately, it is very common that developers sign the code only on executables, and sometimes forego signing (or making sure of the existence of a valid signature) all the dynamic-link libraries (DLLs) and other files included in the distribution package. Having unsigned components in a software distribution package opens the door to tampering attempts, because an attacker may find ways to replace the unsigned code with a malicious version of a DLL. With that in place, the main application can be forced to execute arbitrary code on the target machine—even if the executables are all signed and deemed secure.

The MPS Monitor DCA release process includes the crucial step of testing and signature verification, to make sure that all the components included in the distribution package are digitally signed with a valid certificate. This ensures that only those who can access the MPS Monitor digital signature certificates may create and distribute any software component included in the DCA package.

DCA Update Process

The MPS Monitor DCA end-to-end update process is routinely subject to extensive security review and penetration test, performed by an independent cybersecurity consulting firm. The purpose of the testing activity is to ascertain the existence of any vulnerability, flaw, or misconfiguration that might exist in the defined scope, and to ensure that the update process adheres to security best practices. The test methodology and resulting report of previous testing activities were reviewed by Keypoint Intelligence analysts.

The reviewed tests determined that good security practices and measures are in place to ensure that no critical vulnerabilities are present in the DCA update process, and that the overall risk that the process presents to customers' networks is low. The testing of the DCA update process is scheduled to be repeated every year, to ensure that no vulnerability is introduced in the supply chain by future implementations.

Keypoint Intelligence Report on MPS Monitor DCA4

This analysis, conducted by Keypoint Intelligence, highlights DCA4's groundbreaking features, particularly its integration capabilities, enhanced security measures, and overall performance in managing and monitoring printer and MFP environments.

DCA4 represents a significant advancement from its predecessor, designed with a clean-sheet approach to incorporate multi-platform support, which allows operation across various systems including Windows, Linux, and Raspberry Pi platforms. This design supports a wide range of operational environments, enhancing its adaptability and utility in diverse IT infrastructures.

Security was a cornerstone in DCA4's development, with comprehensive testing including code reviews and dynamic penetration tests performed to ascertain its resilience against potential cyber threats. These tests confirmed the robustness of DCA4's security architecture, with no high-risk vulnerabilities found, ensuring reliable protection of sensitive data across networks. Moreover, the introduction of advanced security measures such as MQTT using TLS for encryption and the application of modern authentication methods like OAuth significantly bolster the agent's security framework, addressing modern cybersecurity threats effectively.

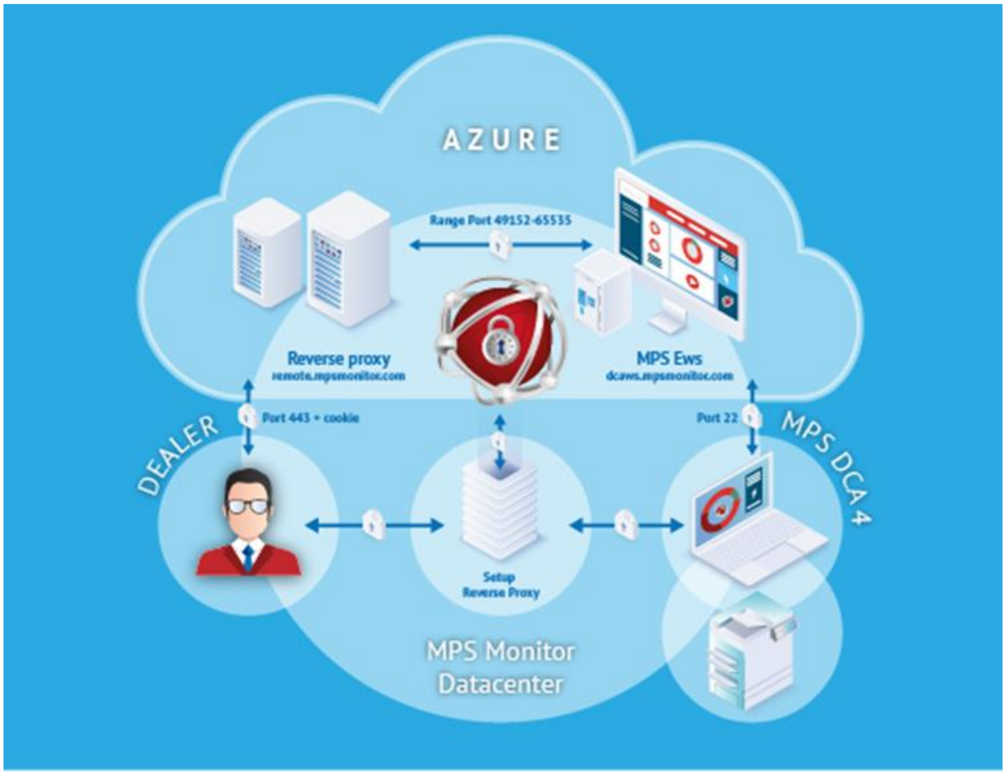
A Critical Feature of DCA 4: Device Web Access

In its latest version of DCA4, MPS Monitor introduced a groundbreaking feature called Device Web Access. It allows users of the MPS Monitor Web Portal to remotely access the printer's Embedded Web Server (EWS), and to be able to remotely configure and troubleshoot the printer sitting inside the customer's network, without having any direct connection with that network nor asking any remote access to the customer. This innovative feature gives MPS dealers a major advantage by being able to perform remote support on devices without any customer interaction, thus increasing the effectiveness of support activity and reducing greatly their costs.

While this brings huge advantages to support operations, it could potentially add a significant layer of cyber risk. This approach means allowing a SaaS / Cloud system being able to access an internal network node from the Internet using an external web browser—and granting to this browser potentially unlimited navigation and interaction capabilities towards web servers which are located inside the customer's security perimeter.

To ensure that the Device Web Access cannot be used to perform any unwanted or malicious activity, MPS Monitor has built-in a number of unique features and procedures that make virtually impossible for a hacker to use this function as an attack vector. Plus, the feature has been subject to many rounds of specific penetration tests centered on trying to exploit any possible weakness and vulnerability in its connection chain.

Figure 1: Device Web Access Ecosystem



The security features of Device Web Access include many elements and procedures:

- A complex cross-check mechanism is in place between the DCA, the services hosted on Azure, and the MPS Monitor datacenter to ensure that every party is legit when a connection is open, so that no man-in-the-middle attack is possible.
- MFA or SSO are required to activate the function, to ensure that stolen credentials can't be used for remote access.
- The tunnel is open only after verifying that device's IP, SN, MAC, Brand and Model match exactly with those in the Portal, so the feature cannot be used to access other devices than the target printer.
- Firewall rules that allow the connection are created and canceled at every session, to avoid reuse of a session's data.
- Sessions have a limit of 10 minutes, after which they are canceled automatically.
- Every session is logged for audit, and customers can see all access logs.
- File upload is disabled, so that remote firmware upload to the printer is not possible.

Advanced User Authentication

The biggest threat to IT systems is access by an individual that has illicitly come into possession of valid login credentials. This is why strong passwords are a must. However, a strong password can itself be the source of a breach, since a hard-to-remember password is more likely to be written down by the user and found by an unscrupulous actor. To help thwart this, MPS Monitor has implemented SSO integration, both natively to Azure Active Directory services, and via Okta, Inc.'s identity and access management platform. These integrations provide secure access to authenticate users on the MPS Monitor 2.0 portal, ensuring fully secure access to the platform.

SSO allows the users to access the platform entering their company account credentials, guarantying the following benefits:

- Avoids the burden of creating and maintaining dedicated logins and passwords for each web application.
- Increases the security profile of the platform by preventing the use of insecure or weak credentials.
- Ensures full and comprehensive compliance with the most stringent security standards and requirements.

Customers relying on Microsoft Active Directory (or on Azure AD) for their identity infrastructure can simply connect MPS Monitor to their Active Directory domain to easily implement SSO across the organization.

For customers who do not use Active Directory, or do not want to implement SSO, MPS Monitor suggests using at least two-factor authentication, which can be enabled to all user profiles using mobile or e-mail One-Time-Password generation.

Certifications and Compliance to International Security Standards

In addition to the security validation of its platform and associated software, MPS Monitor has gone the extra step of earning three key industry certifications, including:

ISO/IEC 27001: Information Security Management System certification, which ensures that MPS Monitor treats data according to three basic principles: confidentiality, data integrity, and system availability--the certification is valid until January 2026 and is subject to annual surveillance audit.

System and Organization Controls 2 (SOC2) Type 2: which is an evaluation of a service organization's controls relevant to security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports are intended to inform users of detailed information and assurance about the controls at the service organization. Earning SOC 2 is a way for a service organization to show its customers how they meet certain criteria prescribed from the American Institute of Certified Public Accountants (AICPA). MPS Monitor passed its first SOC 2 examination in April 2021, and undergoes a yearly review of SOC 2 Type 2 compliance, the last of which was performed in November 2023 (The SOC 2 Type 2 Report, a 300-page document, which details the security controls that the company has in place to ensure compliance to AICPA's TSC, can be downloaded from the MPS Monitor Portal after e-signing a specific NDA).

CSA STAR Level 2: The CSA Star Program is promoted by the Cloud Security Alliance and ensures compliance with Cloud Control Matrix (CCM), a cybersecurity control framework for cloud computing. CCM is composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology. It can be used as a tool for the systematic assessment of a cloud implementation and provides guidance on which security controls should be implemented by which actor within the cloud supply chain. The controls framework is aligned with the CSA Security Guidance for Cloud Computing and is considered a de facto standard for cloud security assurance and compliance. MPS Monitor's CSA Star Level 2 listing and attestation is publicly available on the CSA STAR Registry website.

Disaster Recovery and Incident Response

Regardless of how many security measures are taken to prevent incidents, it is always good practice to "plan for the worst" and to have a clear path to follow should the unexpected happen.

Based on Keypoint Intelligence's evaluation of systems the company has in place, MPS Monitor is well equipped in this regard.

- A Disaster Recovery plan is in place that allows the company to restore its service in a matter of hours, even in the extreme case of a total loss of its main cloud infrastructure. An external consultancy company is contracted to perform continuous testing of the Disaster Recovery remote system, to make sure that it is fully operational in case of need.
- An Incident Response service is in place with one cybersecurity consulting firm. In case of an attack, or any other kind of security breach, a rapid response team is ready to address the situation and apply mitigations, having a continuously updated shared repository of all the needed information on the target environment.

CONCLUSION

MPS providers are now an essential partner for modern businesses of any size and market and, to provide their services effectively, providers' resources and tools need to be entrusted with full access to customers' network infrastructures. As such, it is incumbent upon the provider to enable its services by placing the most secure systems with their customers. That means critically selecting SaaS platforms that have proven security integrity on all fronts:

- The ability to maintain customer devices in a stringent security posture through proactive and automated management of key device settings.
- A proven-secure DCA for their customers' networks.
- A proven-secure back-end system that protects customer data.
- A proven-secure cloud infrastructure that undergoes continuous security testing and auditing from specialized security teams.
- A full and comprehensive set of policies and procedures that meets the requirements for industry-standard security certifications.

In Keypoint Intelligence's analysis, MPS Monitor 2.0 has met these criteria, and the company itself has gone the extra mile to ensure it adheres to stringent security standards. The platform's overall security posture can be taken as an industry benchmark for the definition of a standard set of security requirements to select SaaS platforms for the Managed Print Services environment.