KEYPOINT INTELLIGENCE

PREPARED FOR:

MPS Monitor, s.r.l.

WHITEPAPER

MANAGED PRINT SERVICES PLATFORM SECURITY

ISSUES IMPACTING MPS PROVIDERS & CUSTOMERS

SEPTEMBER 2021

contents

Document

Introduction 2
Cloud platforms can become attack vectors 4
Secure MPS is the Answer 5
MPS Monitor 5
Device Configuration Policy Compliance Validation Testing 6
MPS Monitor DCA – Code reviews 6
DCA Code signing 7
DCA Update process 7
Web Penetration Testing 8
Advanced User Authentication 9
GDPR compliance 9
Certifications and Compliance to international security standards 10
Disaster recovery and Incident response 10
Security features and best practices in place in MPS Monitor Platform 11
Opinion 12
Appendix: Reference 13

Figures

Figure 1: Which of the following are business priorities for your organization for the next three years? 3

Introduction

Cybersecurity is the most pressing issue facing corporations and government agencies. Indeed, Keypoint Intelligence studies consistently have shown that cybersecurity is viewed as the top priority for IT managers and decision makers surveyed. This need is being driven by high-profile security breaches that get covered in the media, actual experience with security breaches or attempts, and steep penalties tied to security violations for heavily regulated industries such as healthcare and financial services. The financial and reputational repercussions of one security breach could potentially force a business to close its doors.

Unfortunately, the problem is only growing worse. The 2020 Internet Crime Report from the U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center revealed a 70% increase in cybercrimes from 2019 to 2020, with a continued rise throughout 2021. Interpol and other agencies worldwide are reporting similarly disturbing trend lines. While e-mail phishing scams are by far the most prevalent type of attack and their potential to bring harm to an organization should not be minimized, more severe threats are posed by disruptive malware (ransomware and DDoS attacks) and data-harvesting malware that makes its way into the corporate IT systems.

The cybersecurity focus of IT departments tends to be on thwarting phishing attacks and securing traditional targets such as network infrastructure PCs and servers. But relatively little attention is paid to printers and MFPs that are every bit as vulnerable. Indeed, 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.

Compounding the issue is the fact that most printers and MFPs in mid-size and larger businesses are placed and monitored by Managed Print Services (MPS) providers, who are responsible for ensuring that devices are running properly and that the customer account is properly billed for usage. Accomplishing that requires a data collection agent (DCA) to reside on the customer's network to send device information back to the service provider. This opens several more potential attack vectors associated with the print fleet, including the possible corruption of the DCA code by unwanted malware, "man in the middle" attacks during data transmission and other communications, and (in the case of cloud-based services) infiltration in the supply chain of the management platform by hackers. So, it is incumbent upon providers and purchasers of MPS services to ensure that the solutions they choose are verifiably secure.

Keypoint Intelligence was commissioned by MPS Monitor, s.r.l., to provide an analysis of, and an opinion on, the overall security posture of its platform regarding the provision of Managed Print Services in customers' environments. This whitepaper reports the findings of this analysis.

Print Infrastructure is an Attractive Target

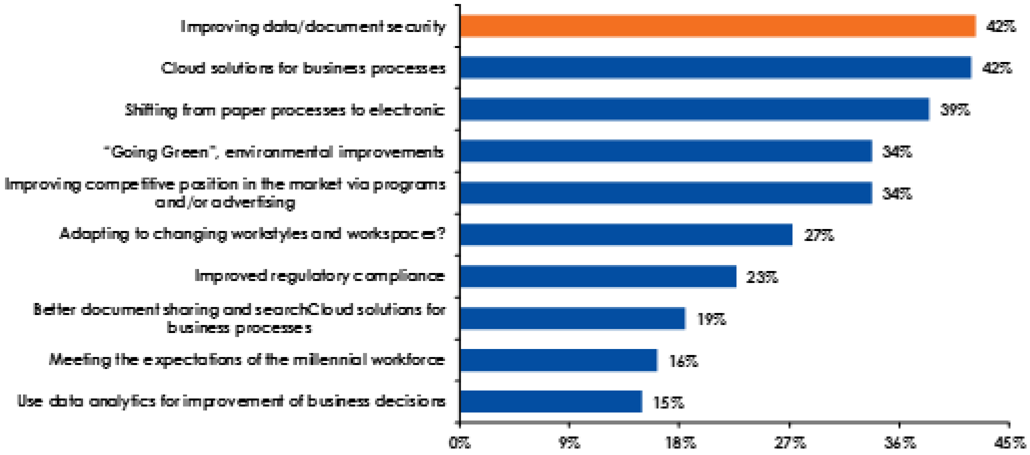
A myth of cybersecurity breaches is that organizations are targeted because they likely hold valuable data (think financial institutions) or have a high public profile (as in the Apple and Sony breaches). But the reality is much simpler: Organizations get hacked because they have exposed vulnerabilities. Attackers look everywhere for weaknesses and use automated tools that run 24/7, probing any IP address for a weakness that can be exploited. Once a "chink in the armor" is identified, the hacker decides if the potential victim is a worthy target.

While cybersecurity in general is reported as a top priority for IT managers (see Figure 1), there is a relative lack of alarm surrounding the vulnerabilities posed by MFPs and printers connected to a wired or Wi-Fi network. But there should be some urgency: A study commissioned by HP Inc. revealed that 45% of IT decision makers say they have seen evidence of compromised printers being used as an attack point in the past year.

42%

of respondents who indicated that "Improving data/document security" is a top priority for their organizations in the coming years.

Figure 1: Which of the following are business priorities for your organization for the next three years?



Source: Keypoint Intelligence IT Decision-maker Survey 2019

The security integrity of MFP hardware is crucial to protect the information that may reside on the device (such as the e-mail address book and documents stored in a user box on the machine's hard drive). But in the scheme of things that is a secondary threat; such information is likely of little value to an outside hacker. The real prize for an unscrupulous actor is using the device as a "bot" in a planned DNS attack, or as a conduit to the wider corporate network.

How did we reach the point where output devices are now a target? Blame the fact that they sit at the intersection of the network and the Internet, a nexus desired by bad actors. Also to blame is their increasing complexity. Most business-class MFPs have a full operating system embedded in firmware to allow sophisticated processes to run natively on the device—which means they have the power needed to run both simple and sophisticated malware. Some of those operating systems (OS) are proprietary, which offers a measure of security, since the pool of coders who can develop malware for the OS is small. Others, however, are based on common languages such as Linux, Java, and Windows CE. And the latest trend is to have a version of Google's Android OS (popular with device makers and hackers alike) underpinning the MFP control panel's functions. Yes, original equipment manufacturers (OEMs) go to great lengths to secure that OS, but hackers the world over are constantly probing Android for vulnerabilities and posting their findings online.

Unfortunately, these attack vectors are not just theoretical. There is a growing list of real-world incidents that were made possible by flaws in MFP security. For example, in April 2019, security researchers in the Microsoft Threat Intelligence Center discovered infrastructure of known Russian hackers communicating to several external devices and attempts by the hackers to compromise popular Internet of Things (IoT) devices, including an office printer. After gaining access to the devices, the hacker ran a simple tcpdump command-line program to sniff network traffic on local subnets. In another breach, a network-connected MFP was left installed with default settings, which allowed an attacker to copy and execute a rootkit on the hard drive off the MFP. The rootkit allowed the attacker to enumerate all corporate IT networks and gain access to any network segment—even though VLAN security and firewalls were implemented on the network.

Cloud Platforms can Become Attack Vectors

In addition to the devices themselves presenting an avenue for attack, the systems used to monitor and manage them remotely also offer an attractive target for hackers. The majority of mid-size and larger businesses have committed to an MPS model for their print fleets, where an outside provider takes over the day-to-day responsibility for the devices in exchange for a set fee. This frees up IT personnel to focus on areas other than print, while also typically saving money in the long run. Many small businesses also rely on MPS-like lease services for their print devices. In most engagements for businesses large and small, the MPS provider will employ a cloud-based SaaS platform to perform management tasks, monitor page volumes, fulfill consumables needs, and perform routine maintenance activities.

Of course, such remote monitoring and management relies on an entire ecosystem of on-site agents and cloud back-end platforms to gather, house, and analyze the information required by the MPS provider—any of which can serve as an entry point for hackers.

A relatively new and extremely dangerous type of threat has emerged in the last year, 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 hacker. The most recent examples of these types of attacks are the Solarwinds incident in December 2020, and the Kaseya incident in July 2021. In both cases, hackers exploited vulnerabilities in the supply chain of software platforms used by Managed Service Providers to monitor and manage the IT assets and networks of their contracted customers. Using provider's platforms as vectors, attackers were able to gain access, plant malware, steal data, and (in the Kaseya incident) even perform a widescale ransomware campaign on many thousands of managed customers' networks.

Secure MPS is the Answer

MPS providers and dealers need to be aware of the above risks, and they need to build their service offerings and operational infrastructures around a clear vision and a strong focus on mitigating those risks. On the other side, customers need to keep a very hard line on security requirements on all applications that providers suggest and use within their MPS engagements.

Secure MPS need to seek out software platforms ensuring proven end-to-end security for the entire print infrastructure. Independent software vendors (ISVs) that develop and provide the 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.

MPS Monitor

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 is 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 on each risk area.

Device Configuration Policy Compliance Validation Testing

Keypoint Intelligence-Buyers Lab 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 administer 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. (Details of the validation testing process is available at this link.)

MPS Monitor 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 two independent application security testing (AST) and cybersecurity consulting firms. Two different teams of security specialists are alternatively set out 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. 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 very 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, but 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 was subject to an extensive security review and penetration test, performed by an independent AST and cybersecurity consulting firm. The purpose of the testing activity was 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 were reviewed by Keypoint Intelligence.

The test ascertained 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 6 months, to ensure that no vulnerability is introduced in the supply chain by future implementations.

Web Penetration Testing

MPS Monitor also submitted its back-end systems, which house data of MPS providers and their customers, to penetration testing conducted by the above-mentioned security firms. This kind of testing was performed three times during 2021. The aim of the testing was to verify the overall security resiliency of the company's IT infrastructure via penetration-test activity that mimicked what real-world hackers might attempt. In other words, firm's "white-hat" hackers attempted to break into MPS Monitor's IT systems from various entry points and using many different attack techniques.

This undertaking was not without its risks, as one of the primary obstacles to the adoption of cloud services by some IT purchasers is concerns about the security integrity of the provider. Possible vulnerabilities other MPS cloud services providers may expose customers to include:

- Instances of stored cross-site scripting (XSS), which could allow an authenticated user to unknowingly store a malware payload within the server
- Endpoints utilized by the cloud connector to create and assign connector details to the target customer, where a hacker would be able to intercept the traffic and set up subsequent connections without authenticating to the cloud server
- Authentication tokens stored in the browser's local storage, 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

Technicians from both security firms verified that, in the latest testing rounds, MPS Monitor's platform suffered none of these vulnerabilities, and that the overall risk score of the platform is low.

Moreover, MPS Monitor has in place a policy that requires the company to perform one web penetration test each quarter, and to get the testing done by the two security firms in an alternate way, 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.

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 Single Sign-On (SSO) integration via Okta, Inc.'s identity and access management platform. This integration provides secure access to authenticate users on the MPS Monitor 2.0 portal, ensuring fully secure access to the platform.

Okta 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.

In addition, customers relying on Microsoft Active Directory (or on Azure AD) for their identity infrastructure can simply connect MPS Monitor to their Active Directory domain using the Okta integration 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 at least to use two-factor authentication, which can be enabled to all user profiles using mobile or e-mail One-Time-Password generation.

GDPR Compliance

For businesses located in the EU, GDPR compliance is required by law when they manage and process Personally Identifiable Information (PII). While in other geographies the local regulations on PII management can be different from EU, in general GDPR is known to be one of the most restrictive regulations in the world for data protection. MPS Monitor, being an EU-based company, needs to adhere fully to GDPR requirements in processing EU citizens' PIIs, but the same best practices are in place for foreign customers and providers who manage personal information of any other countries' citizens.

For EU-based dealers and MPS providers, the platform ensures that a proper Data Processing Agreement (DPA) is signed, and this is made via an easy and automated e-signing process. Until the customer does not e-sign the DPA, the platform does not allow to insert personal information, (like person's names, e-mail addresses and, telephone numbers) into the database.

In all cases where an MPS provider wants to delegate external entities to manage some of its processes (like, for example, consumable shipping through an external logistic partner), the platform provides a specific PII masking feature that ensures no one outside the MPs provider can see or access any PII present in the platform, as all PII fields are masked with asterisks (********) in the UI of the external user.

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 two 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 2023 and is subject to annual surveillance audit.

- **System and Organization Controls 2 (SOC2)**, 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 Type 1 examination in April 2021, and has planned a yearly review of SOC 2 Type 2, starting April 2022. The Soc 2 Type 1 Report, a 56-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 portals by customers after e-signing a specific NDA.

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, also:

1. 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.

2. 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.

Security Features and Best Practices in Place in MPS Monitor Platform

The table below summarizes the findings of this analysis, and can be useful to compare MPS Monitor's security features with other similar solutions:

Security feature / practice	MPS Monitor	Frequency / Notes
Device configuration policy management	✓	Only for HP devices through SDS
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 4 months
Advanced user authentication	✓	Through Okta Identity, or with native 2FA
GDPR compliance	✓	Ongoing
Compliance to standards	✓	ISO/IEC 27001 and SOC 2
Disaster recovery	✓	Ongoing
Incident response	✓	Ongoing

opinion

Opinion

MPS providers are an essential partner for many businesses, and they have been entrusted with full access to customers' network infrastructures. As such, it is incumbent upon the provider to place the most secure system possible with their customers. That means selecting a platform that has 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.

appendix

Appendix: Reference

All the facts reported in this analysis are based on evidence. MPS Monitor provided to Keypoint Intelligence all the documents, reports, and certifications that support the statements present in the analysis.

The original sources of the mentioned documents and related information are the following:

- Keypoint Intelligence – for Device Policy Compliance Testing
- ECSC plc (UK) – for Penetration Testing and Code Reviews
- Ethical Security (Italy) - for Penetration Testing and Code Reviews
- TÜV Sud – For ISO/IEC 27001 certification
- A-LIGN (US) for SOC 2 Compliance
- OKTA Inc. (US) for Single Sign-On procedures

authors

Jamie Bsales

Director

+ 1 973.797.2156

✉

Jamie Bsales is an award-winning technology journalist who has been covering the high-tech industry for more than 25 years, 14 of those at Keypoint Intelligence. In his role as Director, Smart Workplace & Security Analysis, Jamie is responsible for KPI's coverage of document imaging software and related services, smart workplace products and initiatives, and MFP security.

Comments or Questions?

This material is prepared specifically for clients of Keypoint Intelligence. The opinions expressed represent our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies. We believe that the sources of information on which our material is based are reliable and we have applied our best professional judgment to the data obtained.