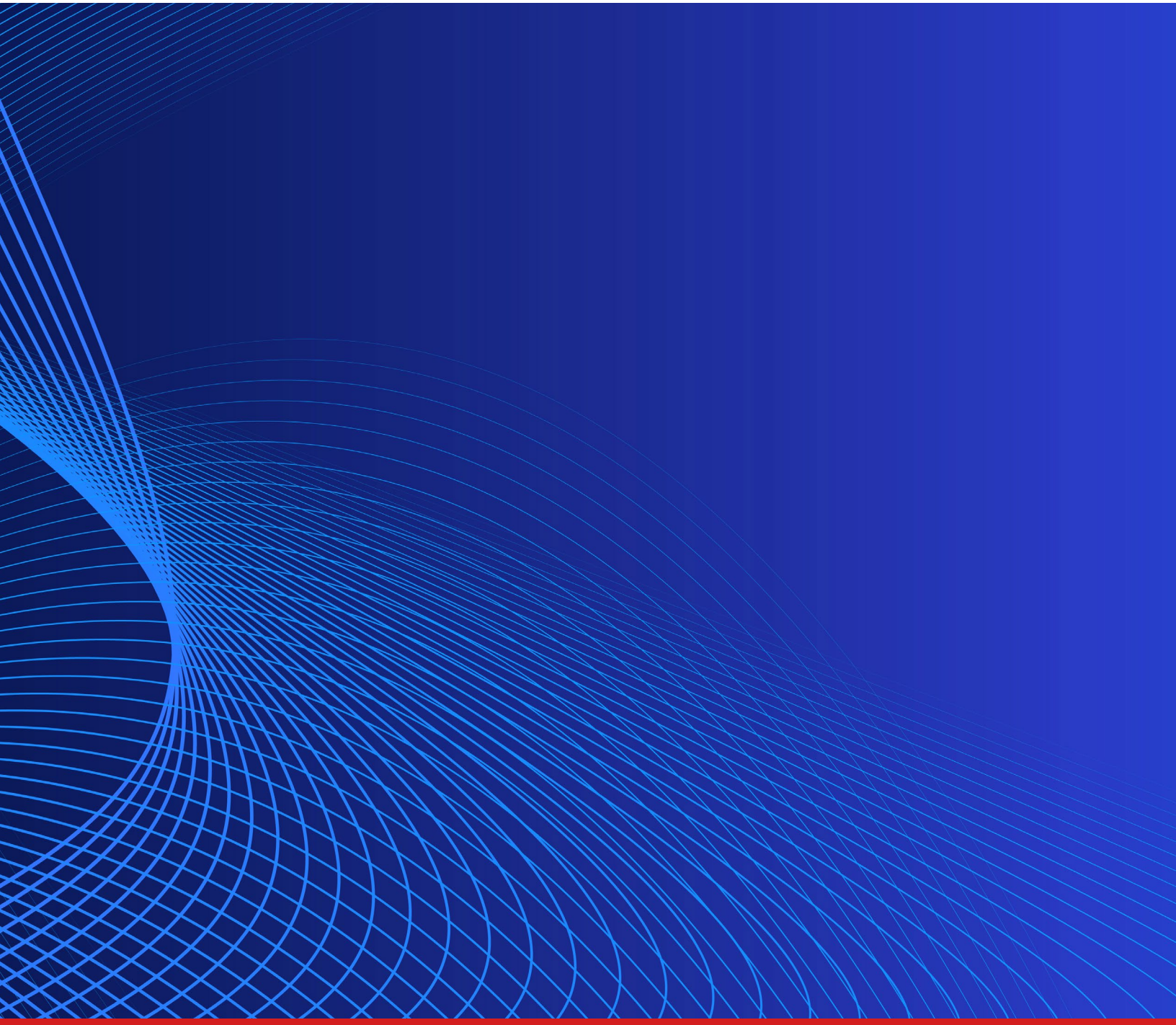
Canon

SYMPHION

THE 5 PILLARS OF SECURITY



WHITE PAPER

SECURING YOUR PRINT FLEET: WHAT TO DO?

No Longer the Forgotten Endpoints: Symphion's Printer Fleet Cybersecurity as a Service

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Printers aren't going away. Yet, they're the least visible, least controlled, and least secured endpoint on most corporate and government networks. Even one unsecured printer can expose the entire business to risks ranging from denial of service (business interruption), theft of information, and breach of confidentiality to complete shutdown of the business from ransomware. There are hundreds of millions on networks, but they're not inventoried or lifecycle managed, not configured for security, and not patched—all of which is basic cybersecurity hygiene for any other workstation, endpoint, or server. Printers are a known cybersecurity gap, globally.

With cyber crime exploding, all that is changing.

Businesses are reacting by using their vulnerability scanning software for penetration testing on their printer fleets. They're discovering and documenting some of the extreme risk posed and are requiring action.

To truly understand the challenges and develop an effective solution, decision makers need a view from inside the print industry and evaluation criteria to filter through the confusion about what to do. They need a solution that works.

In this white paper, we answer the queston: "What to do?"

CYBER CRIME REALITY MEETS LEGACY OF PRINT INDUSTRY'S FACTORY DEFAULT

It's important to first understand that the underlying factor causing this global issue is based on the human behavior involved. For decades, it has been standard print protocol behavior to install printers on networks set to "factory defaults" (open unconfigured) for ease of management and to reset to "factory defaults" after every maintenance or service, even if configured for security. Despite advanced, built-in security features to protect the data and businesses, the industry ships, installs, and manages them with extreme vulnerabilities—such as published factory default administrator passwords that anyone can look up on the Internet—and all ports open. The industry has not patched printers, and printer OEMs recommend against patching because of risk to the printers.

Also, there has been no technology or automation available to configure printers for security across all of the many makes, models, and ages of printers that comprise even the smallest printer fleets. Unlike their desktop, laptop, and server cousins, each printer OEM has its own device management software, but it's limited to their own brand and latest models and must be operated by customers.

This industry human behavior and lack of automation combine to make printers truly the weakest links for always opportunistic criminals. Even one printer, with its trusted internal network access and lack of controls, can provide the jackpot of a stockpile of valuable data to steal or a direct on-ramp into a business' network for ransomware injection.

Printers are now being "discovered" as the weakest link endpoints in cybersecurity.
The question is "What to do?"

BUSINESSES HAVE AWAKENED: PEN TESTING PRINTERS

Information security departments have awakened to this extreme risk and are using their vulnerability scanning software products with their external only (they can't log into printers like desktops or servers) penetration scanning on printers. They're getting proof of the extreme exposures presented and are demanding that printer endpoint owners immediately address the risk by establishing the basics of cyber hygiene. And, they're continually scanning them in a governance effort.

Provide Open Doorways to Entire Business

The "pass back" exploit occurs when a threat actor using a **published OEM default administrator** password that has not been reset (a print industry standard practice) to use an unsecured printer to gain access to credentials servers and other devices on the network.

SORTING THROUGH THE CONFUSION: WHAT TO DO?

Printer endpoint owners don't know what to do and we're seeing many false starts resulting in unnecessary cost and business disruptions. They're looking for options that actually work, but sometimes falsely believe that the option they've chosen offers the technology, labor force, and expertise to address it.

To evaluate options, the following criteria should be weighed:

- Does it fill the gap? (Is it comprehensive of all the devices in the fleet?)
- Does it keep the gap filled? (E.g., does it address the human behavior of "factory default" reset?)
- Are all the direct costs apparent or are there hidden costs?
- What is its potential to disrupt business?
- Is it designed not to disrupt our business?
- What is the ability to execute?
- Is it adaptable to change within our fleet, network, business, and security controls without cost?

FOUR COMMON APPROACHES THAT FALL SHORT

Here are four common approaches that we see most companies attempt and how they match up:

Attempt to Do it Themselves (DIY).
While DIY may seem attractive at first glance, it's complicated, if not impossible, to execute for this niche of cybersecurity. It's more likely to disrupt business operations than secure the printers in the involved printer fleet and also includes a very high hidden labor cost. Each printer OEM offers device management software to manage its own brand and devices, however, the software only works with the latest models. The tendency has been for businesses to assign employees to obtain, learn, operate, update, and vigilantly ***try to cobble each software product together to operate all the makes, models, and ages of printers that comprise the fleet.*** This approach has always been destined to fail. Even the brightest IT or IS employees are not familiar with the intricacies of printer configuration or patch management—especially across the diversity presented by even a small fleet. This effort is guaranteed to disrupt print service delivery and interrupt business, to not be comprehensive to fill the gap, and to distract otherwise productive employees from important core business efforts. Moreover, DIY includes substantial hidden labor cost, not only from the manual effort involved to operate the software products, but also from the cost of cross-device printer training and managing and cybersecurity expertise and the high cost of guaranteed human error. Additionally, the DIY option does not address the security risk created by the print industry human behavior of managing and resetting to factory default after servicing printers, thereby eliminating even the best-intentioned security configuration.

Buy All New Printers and Standardize on One Brand.
This is the most common recommendation from printer OEMs—as you can imagine. Printer OEMs want customers to buy and standardize on their newest printers. They tout advanced cybersecurity hardware features managed by their own proprietary brand and latest model-limited proprietary device management software and some offer professional services teams to help customers "get started." However, the reality is that budgets are tight and printer fleets are necessarily comprised of many makes, models, and ages of printers. Those printers are already working in that business (legacy) and changing them out, without visibility and control of the whole fleet, is complicated and is guaranteed to have disruptive and costly consequences. While the sales discussion may be in terms of "automatic" configuration or operation, this approach also involves the same DIY risk and labor cost in operation because OEMs do not operate their device management software for customers.

Rely on Managed Print Services (MPS).
The biggest issue with this strategy is that most MPS vendors are not focused on or trained in security. Instead, they're focused on supplying and servicing the printers and supplying the consumables (toner and staples) to maintain the important print service for which they get paid. The common printer fleet management tools that MPS providers use to track image counts (commonly referred to as "clicks") and consumables do not report, monitor, or remediate printer security settings. Security settings are hidden to them. MPS providers offer other software such as pull printing (also referred to as secure release) software to protect printer output (printed sheets or otherwise) from being seen by the wrong eyes and enterprise output management software products to establish administrative rules for printing (like printing on both sides or only in ***black-and-white)*** to eliminate cost. But these products, while delivering an aspect of security, do not address the printers' security configurations or patch management. MPS providers may attempt to cobble together OEM brand-limited software products or attempt to manually address this risk, but they face the same limitations discussed in the first two strategies above.

Rely on Managed Security Services Providers (MSSPs).
Managed security service providers do provide excellent solutions to address most IT security needs; however, if they include printers in the scope of their services, they are similarly limited to reporting externally scanned vulnerabilities and recommending security controls (not delivering controls). Other software products, such as Security Information Event Management (SIEM), simply do not report or manage printer security configurations or patch printers because they cannot access printers. Similarly, there are software products that inventory Internet of Things (IoT) devices on corporate networks by sniffing the network traffic, but these products also do not provide basic printer cyber hygiene of printer security configuration management or patch management.

THE WAY FORWARD

What's the way forward? How do businesses address this urgent, niche need when they don't have the available labor force, skill set, or technology to cyber harden a printer fleet? The last things anybody wants are for their business to be disrupted, or to engage in manual efforts such as trying to regularly log into each printer to check all the printers in the fleet, or to have to check the work of somebody else trying to do it manually or with cobbled together printer OEM software, or trying to install multi-versioned printer firmware that might break the printers. The way forward is also not through any existing security software like vulnerability managed detection and response (VMDR) solutions because they cannot access printers internally to harden them or patch them. Yet, VMDR, security configuration management (SCM), patch management, and IT asset lifecycle management (ITAM) are necessary cyber hygiene for printers and other configurable IoT devices.

SYMPHION'S PRINTER FLEET CYBERSECURITY AS A SERVICE™ IS A SOLUTION

Symphion provides that much-needed cyber hygiene for all printers in any printer fleet. Symphion's unique vendor-agnostic solutions fill the cybersecurity gap for print fleets by establishing and maintaining cyber hygiene including perpetual ITAM, VMDR, SCM, and patch management for all the printers in ***any printer fleet.***

What Does Printer Fleet Cybersecurity as a Service do?

Everything. Establishes and maintains visibility, control, and foundational cyber hygiene for these forgotten endpoints and delivers it turnkey, without DIY or hidden labor costs.

Symphion's solution, aptly named "Printer Fleet Cybersecurity as a Service™ in concert with Canon U.S.A.", is ***turnkey, perpetual printer security configuration management*** for printer fleets—remotely delivered by Symphion. Symphion's complementary solution Firmware Deployment Service™ addresses the unique complexities presented in patch management with ***turnkey, perpetual printer patch management of printer fleets.***

Implement, Discover, and Establish Baseline Inventory

It all starts with implementation. Symphion remotely implements its unique software products inside customers' data centers and on customers' servers and then remotely accesses those servers to deliver its perpetual service. Symphion is never on site.

Symphion professionals, known as "concierges" (professionals trained in Symphion software, processes, printer cybersecurity and operating in sensitive highly security environments), use Symphion's unique software products to scan and inventory ***the entire diverse printer fleet*** including "blueprinting" each printer's available built-in security settings and the status of each—all without installing any software (agents) on the printers.

Printer Fleet Cybersecurity Program Management Office and Printer Management Consulting

Importantly, Symphion solutions include a Printer Fleet Cybersecurity Program Management Office (PMO) with customers' stakeholders, led by Symphion. Symphion will assist customers in identifying stakeholders including printer endpoint owners, involved application owners, managed print services providers, and IT and information security professions to establish this forum for the introduction of printer fleet cybersecurity and decisioning. The PMO works together for the term of the service as a regular forum for establishing, maintaining, and adapting printer fleet cybersecurity policy for the term of the service. PMO activities include planning, status and execution of testing, and turn up of controls and defining change control.

Turnkey, remotely delivered concierge service

No Employees, Contractors, or Projects required.

Testing and Turn Up of Security in Establishing Controls

After inventorying the fleet, Symphion works with customers to establish their printer fleet cybersecurity controls that Symphion calls "Gold Standards", security settings and policies ***for each printer, type, and work group*** taking into account each printer's available settings, cybersecurity best practices and customers' various business needs.

Symphion's "prime directive" is to not interrupt customers while introducing cyber controls to printer fleets. Testing is essential before turning up security settings where none have existed. Otherwise, introducing change is likely to disrupt business.

Symphion's approach aptly called "Testing and Turn Up" is Symphion's proven process to support a ***phased and prioritization approach*** allowing customers, through Symphion, to establish priorities of controls and to continually refine those controls, without interrupting their business while doing so.

Symphion's ***software products set each printer's security configuration*** to that printer's "Gold Standard", either in the field or with new printers as they are commissioned.

Continuously Monitor for Changes and Remediate

Printer Fleet Cybersecurity as a Service then provides automated and perpetual inventory and controls surveillance and remediation of changes.

Evergreen Inventory. Changes to Printer Fleet Inventory. Printer Fleet Cybersecurity as a Service monitors printer and fleet inventory changes. Accurate printer fleet inventory is essential to effective risk management and is not a one-time effort or a list on some piece of paper. If the inventory is not accurate, security is compromised. Symphion's software has built-in capabilities to address the challenges presented by inventory changes including identifying new printers connected to the network and printers leaving the network and state changes in printers, all with the most advanced IT asset lifecycle management capabilities specifically designed to address the mobility of printers in printer fleets and human behavior of the print industry. Symphion's software identifies printers through the lifecycle of the printer and end-of-life policies and procedures.

Prime Directive

Symphion solutions are designed with prime directive to facilitate and establish and maintain cybersecurity controls for printer fleets but not interrupt customer business while doing that.

Changes to Printer Security Settings. Printer Fleet Cybersecurity as a Service monitors changes to each printer's "Gold Standard" configuration and runs throughout the day, seven days a week, 365 days a year. If a change in configuration is detected, Symphion's software automatically remediates that setting back to that printer's "Gold Standard" in accordance with agreed change control procedures and logs the event. This solution feature combats not only the "factory default" reset human behavior but also addresses undocumented changes introduced by firmware updating that can create vulnerabilities.

Symphion also offers fully automated event management and alerting capabilities.

Adapt to Change That Affects Fleet

Printer fleets are constantly changing including changes in printers, desired security controls, service vendors, in networks and in the business, all of which affect any security solution. Symphion professionals, administering Printer Fleet Cybersecurity as a Service, are experienced in highly secure environments, printer cybersecurity best practices, and customer service and will administer the solution to address those changes, unlike software-only solutions.

Establish Regular Systematic Process and Reporting to Match Cybersecurity Standards and Best Practices

Printer Fleet Cybersecurity as a Service establishes a regular, systematic process that matches the mandates of each organization.

Reporting can include useful security analytics to adapt and refine security, such as remediated security setting statistics, Top 10 lists (models with most and least weaknesses), identified weaknesses (by make or model), and many others.

Integrates with Other Applications

Printer Fleet Cybersecurity as a Service integrates with popular help desk, inventory, configuration management database (CMDB), and change control applications.

Patch Management

In addition to security configuration, Printer Fleet Cybersecurity as a Service offers Firmware Deployment Service™ to deliver patch management for printers. Patch management is a cornerstone of any effective cybersecurity program and is essential cyber hygiene. It's mandated in all security standards but is not being done on printers due to cost of manual effort required (from lack of automation and lack of skill set) and associated risk to printers.

As a part of a wholistic printer fleet cybersecurity platform, Printer Fleet Cybersecurity as a Service offers Firmware Deployment Service™ to fill this need. This turnkey, vendor-agnostic service includes deployment automation for firmware payloads to enable updating and maintaining current firmware on all printers in printer fleets, i.e., cost-effective patch management for printers. It's delivered by Symphion and includes planning and processes to avoid print service and business disruptions.

Platform Extends: Other Configurable IoT

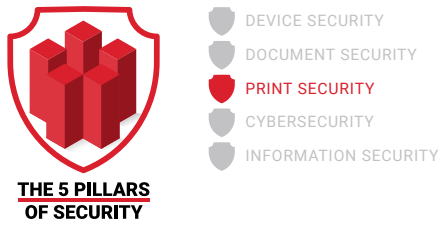
Symphion's IoT Cybersecurity as a Service™ addresses the VMDR, ITAM, SCM, and patch management cyber hygiene needed in the rapidly growing configurable Internet of Things (IoT) market. Regulators are recognizing the increasing exposures from IoT devices on corporate networks, requiring OEMs to add configurability for security. To address the broader IoT market development both as it currently exists and as security configurability increases, Symphion extended its existing platform. Symphion's IoT Cybersecurity as a Service™ is Symphion's turnkey security configuration management service for IoT devices—completely and remotely delivered by Symphion. This affordable service manages the available security setting (regardless of make or model), monitors those settings, and automatically remediates them to their planned, controlled state. Patch management is also available.

ABOUT SYMPHION, INC.

Symphion, Inc., is a Dallas, Texas-based software and services company focused on continual innovation, seamless delivery, and dedication to excellence in customer service. Symphion's leading cybersecurity solutions are designed to provide cybersecurity results to eliminate cost and risk. Symphion is a leader in securing printers and other configurable IoT devices.

ABOUT CANON U.S.A.

Canon U.S.A., Inc. provides industry leading enterprise, production, and large format printing solutions, supported by exceptional professional service offerings. Canon U.S.A. helps companies of all sizes discover ways to improve sustainability, increase efficiency, and control costs in conjunction with high volume, continuous feed, digital and traditional printing, and document management solutions.



Canon U.S.A.'s Five Pillars of Security presents a portfolio of cybersecurity products and services in a comprehensive way that groups solutions in functional areas. Print Security is a key component of our Five Pillar approach.

1-844-50-CANON

usa.canon.com/security

11/25-0142-6983