Symphion

Print Fleet Cyber Security as a Service™

Benefits

- **Visibility to hidden enterprise-wide risk** at the imaging device & fleet levels—an existing gap in cyber security plans.

- **A unique turn-key solution to address cyber security risk in multi-vendor print fleets** (regardless of make, model or location). No employees required.

- **A regular, systematic process** of automated cyber security examination **& remediation** of your print fleet security settings.

- **Historical records automatically generated & maintained** documenting your cyber security efforts.

- **A Print Fleet Cyber Security Maturity Model** and support transitioning to maturity including **Gold Standards** for device settings.

Weaknesses in Your Print Fleet Expose Your Entire Enterprise

Less than 2% of all networked printers are secure. Yet, most cyber security plans don't even mention, let alone address them. To further complicate matters, print fleets often number in the 1000's of printers and are typically multiple makes and models. Until now, there has been no way to establish and maintain cyber security controls in multi-vendor print fleets without costly, inefficient manual effort.

The Answer: Symphion's Print Fleet Cyber Security as a Service™

We specifically designed our **turnkey** Print Fleet Cyber Security as a Service™ solution to economically and systematically address this unaddressed gap.

Where are we at risk?
How do we address it?
How are we doing?

Print Devices— A Hidden Cybersecurity Risk

Print fleets can number in the 1000's of devices with each device representing many potential open, but hidden doorways that can expose not only that device, but also your entire network and company to information theft or sabotage.

Print Devices are Vulnerable Complex Workstations

Just like desktop computers and servers, printers offer advanced capabilities that provide great business benefits such as accessing the internet, storing data on hard drives, emailing in and out of the domain, downloading and uploading software, opening communications ports and enabling storage on USB thumb drives. These very same capabilities expose your entire business to risk of information theft and sabotage.

Complex Security Settings Built in, But Not Used, Not Visible

To address these known risks, all printer manufacturers have built in rich security features in their printers. But, they haven't provided a way to monitor those settings in large **multi-vendor** print fleets. Even if security settings are turned on at commissioning, they often get turned off during routine service and maintenance. Cyber Security teams have no way of knowing—no visibility. Managed Print Service providers are equally without visibility.

What devices make up our fleet?
What security settings to use?
How are we doing?

Our Solution—Print Fleet Cyber Security as a Service™

Identifying enterprise risk requires not just cutting-edge software but also an ever-vigilant effort to address the rapid changes associated with today's IT eco systems. It requires an information driven, regular process and technology to monitor, alert, report, remediate and record.

Our Print Fleet Cyber Security as a Service™ solution does that by combining: our leading-edge technologies, dedicated remote concierge teams and proven delivery process. **(Products, People & Process)** We've also included a best practices model and support transitioning to cyber security maturity, on-going automated remediation of your chosen controls and regular records of it all for compliance and audit response.

It Starts with Essential Evergreen Inventory through Device Lifecycle Management

First, our solution inventories these devices (regardless of make, model or location). We maintain an accurate evergreen inventory with comprehensive device lifecycle management throughout the term of the service—The Foundation of All Effective Risk Management.   We automatically account for changes in device location, IP address, and device configuration and other changes.

Next, Security Settings "Gold Standard" Controls Determined & Established

Next, we inventory the available security settings on each device for you to decide on your "Gold Standard" settings for each device, device type, groupings and enterprise wide. If you don't already have a plan, we provide recommended best practices "Gold Standards" for each device's security settings. You can choose ours, choose your own or can use both. Symphion then sets those security settings (except settings requiring maintenance mode) to establish those Gold Standards.

Ongoing Remediation: Symphion Automation Maintains Settings

Then, for the term of the service, Symphion will automatically maintain your top device security settings (not requiring maintenance mode) across your entire print fleet to your "Gold Standards" — so you don't have to!

Establishes a Regular Systematic Process with Records Maintained

In addition to monitoring & remediation, our monthly disciplined process automatically establishes a regular risk assessment, a regular security evaluation of chosen controls and historical records of your chosen controls and measures taken to secure your enterprise. These records are readily available for auditors without requiring a project or dedicating your employees' time. Our process and records match most security mandates for regular assessment and record keeping including NIST RMF, HIPAA Security Rule and others.

Where to Start?

Includes a Cutting-Edge Print Fleet Cyber Security Maturity Model and Support Transitioning

Don't know where to start? We have that covered, too. As part of our Print Fleet Cyber Security as a Service™, we include a cutting-edge Print Fleet Cyber Security Maturity Model. Symphion's dedicated concierge team will work with you to transition to Symphion's Print Fleet Cyber Security Maturity Model, your chosen model or a blend.
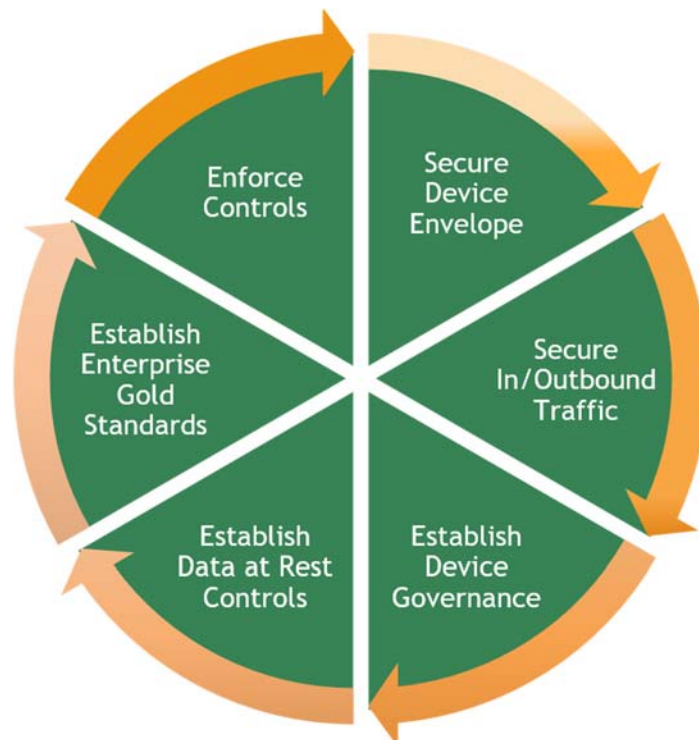
Symphion "as a Service™" Solutions Generally

No FTEs or Projects required

Just as with electrical service being provided to your business or home, your employees are not required to be involved in delivering this valuable service. There are no projects required to implement, upgrade or administer the solution. Your Symphion concierge team will take care of it all.

No Agents to Install

All Symphion solutions are agentless. There is no software to install on target devices to enable scanning. No software to interrupt the operations of your other systems.

No Hidden Costs--Fixed Fee Pricing-- Adjusted (Right-Sized), Predictable

At Symphion, we're focused on returning the highest value to customers and providing predictably in pricing. To do this, our implementation fees and ongoing service fees, unlike the unknowns associated with traditional enterprise software deployments, are both fixed and right-sized (with minimums) based on each customer's number of assets to be scanned and specific needs.

Solutions are Totally Deployed on Customer's Infrastructure inside Customer's Firewall

Our "as a Service™ solutions are all deployed on Customers' virtual servers and hosted in Customers' datacenters. No data leaves Customers' premises; thereby providing the most secure deployment.

About Symphion

Symphion, Inc. is a Dallas, Texas based software and services company focused on continual innovation, seamless delivery and dedication to excellence in customer service since 1999. Our unique "as a Service™" solutions are designed to provide effortless delivery of actionable information and results to eliminate cost and risk and to increase operational efficiency.

Legal Disclaimer
The information contained herein is not a legal analysis, advice or opinion regarding compliance or any other matter. Please consult an attorney.