Securing Multi-Brand Printer Fleets Can Be Easy

Printer fleets can number in the hundreds or thousands, with different makes and models. How can you ensure their firmware is up to date, their device configurations haven't been modified, and their default passwords haven't been changed? Until now, there was no way to cost effectively maintain these security controls across an entire fleet.

DO YOUR PRINTERS HAVE TIME CAPSULE SYNDROME?

Many networked printers haven't been configured for security or had their security settings updated since the day they were installed. This can expose your data on a truly massive scale. The bigger your printer fleet, the bigger your risk.

Printer Fleet Cybersecurity as a Service (PFCaaS)

Have a printer fleet security team work for you. The PFCaaS team assesses all brands in your printer fleet, establishes security controls baseline, and monitors your fleet on an ongoing basis. All this while freeing your staff to focus on your core IT responsibilities.

STEP 1 //

EVERGREEN INVENTORY

All devices in scope are identified, regardless of make, model, or location. After your security requirements are determined, a profile is developed for each device, which includes network protocols, certificates, services, and firmware. These profiles are monitored on an ongoing basis to ensure their integrity.

STEP 2 //

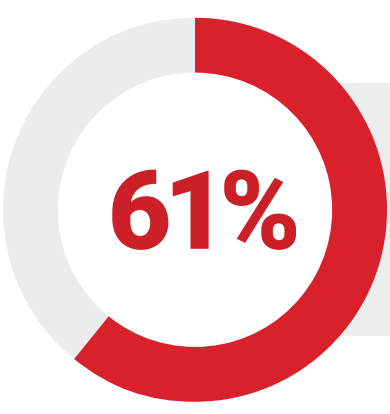
DEVICE BLUEPRINTING

Software then creates a "blueprint" of available and unavailable security settings on each device. It also identifies devices that cannot be updated and should be retired.

STEP 3 //

DEVICE HARDENING

You choose a "Gold Standard" for hardening your security settings, depending on your budget and your level of risk tolerance. This Gold Standard is deployed across your printer fleet.



of organizations have experienced data losses due to unsecure printing practices in the past 12 months.

Quocirca: Executive Summary, Quocirca Print Security Landscape, 2023

What Else Does the Service Provide?

TESTING AND TURN-UP

Each control is tested before deploying it across your fleet. This can help prevent potential disruptions to your business when the controls are fully deployed.

BUILT-IN CONSULTING

Consulting professionals will regularly conference with you and your printer fleet team to help you conduct cyber hygiene and maintain best security practices.

ONGOING REMEDIATION

The alerting and event management system gives you current, historical, and future (trending) visibility into your configurations, inventory, and firmware updates.

PATCH MANAGEMENT

The firmware deployment service helps you update firmware across your fleet. These patches are also included in Testing and Turn-up before deployment.

RECORD MAINTENANCE

The documentation process matches many security mandates for regular assessment and recordkeeping.

CONCIERGE REPORTING

You get comprehensive reporting from hundreds of available reports, ad hoc reporting from available data, and custom reporting that may require coding.

THE 5 PILLARS OF SECURITY

DEVICE SECURITY
DOCUMENT SECURITY
PRINT SECURITY
CYBERSECURITY
INFORMATION SECURITY

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

For more information about cybersecurity and Canon Solutions America's 5 Pillars of Security contact us today or visit our website at USA.CANON.COM/SECURITY.

11/25-0135-9368