Often Overlooked, Printers Require Protection Strategies

How prevention, authentication and modernization expand endpoint security

We rely on printing and document sharing so often it's easy to overlook the security vulnerabilities inherent to them. However, both pose significant risks.

Printers are usually connected to the organization's network, exposing them to the same vulnerabilities as other network devices. When workers at home or in the field connect remotely to print, scan or copy, the risk of breaches and cyberattacks is even greater.

"Printers and copiers have powerful processors, store information and integrate to line-of-business systems," says John Spiak, senior manager of solutions consulting at Canon. "However, organizations typically don't protect them in the same way they would a laptop or desktop workstation. These devices have become low-hanging fruit for cybercriminals."

Printers are usually connected to the organization's network, exposing them to the same vulnerabilities as other network devices.

Proactively Protect Your Printers

Agencies often find including printers, scanners and copiers in their organization-wide cybersecurity practices is an intuitive way to quickly improve their security posture. They just need to expand what they're already finding successful.

The first step for many organizations is regular training for all staff, which must include training on printer and scanner protection. And it's not enough to have employees take a course once per year.

"The risks and what cybercriminals are doing change daily," says Bill Rials, senior fellow for the Center for Digital Government. "Trainings should be at least monthly and in small chunks."

When it comes to technology, agencies should harden devices by closing unused ports. Changing the default administrator password that comes with each device should be a top priority.

"People don't always pay attention to what ports are open," Spiak says. "That's a huge threat vector when you consider your most critical business information passes through these devices on a daily basis."

IT teams must update printers and other firmware regularly to patch vulnerabilities and address new exploits just as they would other devices. Additionally, printer devices need to be included in security assessments and testing going forward.

The following strategies are also necessary to improve security:

Make integration a priority. Integrate devices with your security information and event management tools to help identify patterns in user and device behavior, detect potential breaches and respond quickly and decisively to alerts.

Establish configuration baselines. Each device may have dozens of controls users can turn off or adjust. Configuration baselines serve two functions. First, a device integrity check is activated when the device starts up. If the check detects malicious behavior or changes, it automatically returns the device to its baseline configuration. The second function standardizes security controls across printer fleets, simplifies management and accelerates recovery if printer configurations are deleted or corrupted.

Encrypt data at rest and in transit. Once an encrypted file reaches a device, the device should encrypt data during processing and purge the data from the device once a print, scan or other job is complete.

> **"The risks and what cybercriminals are doing change daily. Trainings should be at least monthly and in small chunks."**
>
> — Bill Rials, Senior Fellow,
> Center for Digital Government

Deploy Authentication and Access Controls

Authentication protects sensitive information by verifying the identity of users. When used with role-based access control and principles of least privilege, it ensures users can only access documents and print functions they need to do their job. In addition, it enables auditing by attributing activity to a specific user and providing granular reporting on how the device is utilized (e.g., what time a person logged in or released their job or whether they changed device settings).

To prevent unauthorized reproduction, alteration, sharing or viewing of printed and digital documents, agencies should choose solutions that incorporate key components of a Zero Trust security framework. This approach requires that users continuously verify their identity as they access additional documents, apps or programs rather than relying on just one username and password combination to gain complete access.

In poorly secured environments, print jobs may remain in printer trays for hours or days, where anyone can maliciously or inadvertently view or take documents they're not entitled to. Requiring users to authenticate themselves before accessing documents protects this critical information.

Advanced print management solutions offer flexible authentication methods such as username/password, proximity-based cards and USB keys. They also allow users to apply watermarks to sensitive documents and set time limits on the availability of shared documents.

Modernize the Print Infrastructure

The print architecture in many organizations is based on management tools and utilities that have not been updated in years. These systems were not designed for today's security threats and are more prone to vulnerabilities.

Moving to cloud-based systems equips organizations with modern, secure-by-design tools that are regularly patched and updated by the cloud provider.

"The provider handles updates to firmware and certificates without requiring the intervention of the IT or print admin," says Aaron Hale, senior manager of vertical marketing for Canon. "It takes some of the burden off the resident IT team to focus on more critical things."

Another important benefit of leading cloud services is adherence and certification. The Federal Risk and Authorization Management Program (FedRAMP) uses National Institute of Standards and Technology guidelines to provide standardized security requirements for cloud services.

By independently verifying and monitoring monthly that a particular cloud service adheres to the requirements, they help reduce internal security evaluation requirements and provide a level of assurance that allows organizations to adopt cloud services more confidently.

Deploying these strategies as they fit for an organization immediately improves their security posture by protecting more endpoints and securing critical information.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Canon.

Produced by the Center for Digital Government

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

www.centerdigitalgov.com.

Sponsored by Canon USA

Canon is a trademark or registered trademark of Canon Inc. in the United States and elsewhere. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged.

For more information, visit **usa.canon.com/federal-government.**

SHUTTERSTOCK.COM