

THE WEAKEST LINK

Are Your Printers Part of Your
Endpoint Security Plan?



ALLIED
BUSINESS SOLUTIONS

Putting Print Security on the C-Level Agenda

Regardless of size, security is a major concern for every business. Did you know that a common area of exploit for hackers is networked printers? Today's printers are much like any computer on your network. They have built-in hard drives, internet connectivity, and wireless access and as a result, need to be kept as secure as every other device on your network or your data is at risk.

Older print devices in particular can pose an increased security risk, especially if you haven't kept up with firmware and security updates.

In this eBook, we'll look at the nature of, and how to identify, security risks, best practices you can use to secure your printers, and how upgrading to the latest multifunction technology can not only lower your risks but can improve productivity and work flows through automation.



43% of businesses ignore printers in endpoint security plan

ALLIED.*tech*

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

Identifying Security Risks

Security threats are not just limited to PCs, servers or networks. As print devices have become more sophisticated, even basic printers offer wireless network capabilities, hard drive storage, and internet accessibility. As a result, your print environment needs to be protected against a diverse range of threats.

Multifunction printers have evolved into information terminals and core IT assets. The computing power of what were traditionally printers or copiers has grown and with it, and so have the potential threats to your business. Identifying threats, deploying superior technology, commitment, and threat awareness are essential for keeping your network safe. Here are some threats to be aware of.

60%
of enterprises
suffer data loss
due to printer
security breaches

Data High-jacking and Alteration

MFPs exchange data with computers and servers over your network. If left unprotected, this data can be intercepted while in transit to or from the printer. It can be taken or altered with malicious intent. Encrypting data at the source can eliminate this risk.

Unauthorized Access at the Device

MFPs in an open office environment can be exploited from within your organization via the operations panel at the device. Reduce risks by installing authorization protocols – whether it's a key card, password or PIN.

Unsecured Firmware or Malware

If your printer or MFP's firmware is compromised, then that device can be used as an open door to the rest of your network.

Malicious Access via Your Network

In a connected world, the number of entry points has increased, and MFPs can be discovered over your network. Using features like user authentication and filtering can help prevent an intruder from accessing internal features.

ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCATELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

Printer Hard Drive Breach

MFPs have a hard drive used to store address books and documents. The drive may also contain temporary copies of data scheduled for transmission or printing. This data can be accessed and stolen if safeguards are not put into place. Data encryption and overwrite software can help prevent information from leaking.

Hard Copy Leaks

A document left on the printer tray can be a major risk. Whether taken deliberately or accidentally, paper documents are often overlooked and can leave you vulnerable. Protect your information by using authentication measures at the device (pull-printing) or consider a digital approach.

Breaches Due to Carelessness

Information can be accidentally leaked. For example, sending a confidential fax to the wrong number, or making extra copies and leaving them at the printer. There have been major breaches due to carelessness, like the 2017 breach that cost Aetna \$17.2 million in fines. Confidential drug information was visible through the envelope windows of thousands of letters sent out.



ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

Best Practices to Secure Your Printers

Print security needs to address three areas – securely designed and deployed hardware, software, and networking. Here are some best practices to consider when designing your print environment security protocols.

Manage Accessibility

It's important to secure the device from external threat, but many data breaches happen from inside, so controlling internal access is critical. "Pull-printing" can eliminate documents left at the device by requiring authentication measures like a PIN, key card or unique password. Today's printers can easily log access so if a breach does occur, you have a record of who used the device.

Change the Default Password to the Administration Control Panel Web page

If your printer's administration panel is left unsecured (or set to default) attackers can change the printer's network address to reroute jobs,

implement a denial of service (DOS) attack and shut down the device, or use the printer as an open doorway to another system on your network.

Check for Unnecessary Services

Many printers default to unsecured and unnecessary protocols like Telnet, FTP or HTTP. Leaving them enabled, or not being aware they're open puts your entire network at risk.

ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

Keep Your Firmware and Security Updates Current

Just like computers, your printers and MFPs need firmware updates and security patches. Check for updates for printers and network devices regularly. Updates often add enhanced security features and fix other issues that can put you at risk.

Choose the Right Printer

Many offices provide small office printers to employees to use as a personal device. Whenever possible, keep these printers off of your network. If they are networked, treat them like any other device in terms of security. The fact is, a networked small business printer is less likely to have the necessary security features built in and can be a big risk to your business.



These best practices can help you keep your print environment secure. You'll also want to include encryption for any data traveling on your network transit, secure the document (pull-printing can keep paper documents from prying eyes) and secure the device, both to and from the printer. To keep your data protected you must secure it.



ALLIED.*tech*

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY

Upgrading Your Technology

If your current fleet of printers or MFPs is three to five years old your security is probably outdated. One of the best ways to improve security as well as lower cost-per-page and improve productivity is to invest in the latest multifunction printer technology.

Upgrading to new MFP technology can not only make your business more secure, it can improve productivity. Using the scan function with built-in software allows you to digitize hard copy documents for storage in the cloud.

Digital documents are more secure, collaboration is easier, and final documents can be delivered via email directly into the recipient's inbox. Automating workflows can save you time and money, while improving your print security.

The easier an attack, the more likely the threat will materialize.

New MFPs have advanced security features built in that take security to the next level.

- Deepest security to detect, stop, and self-heal from attacks automatically
- Embedded features that protect the device from boot-up to shutdown
- Digitally signed firmware updates
- Encrypted communications
- Encrypted hard drives
- Image overwriting
- Password protection



ALLIED.tech

BOISE · ONTARIO · IDAHO FALLS · POCA TELLO · SALT LAKE CITY

Managing
IT

Managing
PRINT

Managing
DOCUMENTS

Managing
SECURITY



Are you ready to review your print security strategy?

Contact us to get started with a print assessment for your organization.

Contact Us!



Let's talk about your document workflows and our quick assessment services to help you understand where the biggest opportunities exist.

Allied Business Solutions, we're ready when you are!

www.allied.tech | 208-344-3833