The Small and Medium-Sized Business Guide to Securing Printers

Considerations for improving printer security across modern business printers and common printing practices

EPSON®
EXCEED YOUR VISION

Contents

Executive Summary

- **Purpose:** This guide is intended to raise awareness of security issues related to modern business printers and common printing practices, as well as considerations for improving printer security in small- and medium-sized businesses (SMBs).
- **Audience:** This guide is intended for SMB professionals responsible for buying, installing, and securing printers in enterprise networks. This guide refrains from highly technical information to remain accessible to readers with limited backgrounds in IT and security.
- **Content Scope:** This guide focuses on high-level security concepts rather than how-to implementation. Use this guide as a starting place for evaluating security issues, but refer to product documentation for detailed instructions. While many recommendations apply to printer settings, some measures must be implemented via other devices (e.g., network routers).

“

Use this guide as a starting place for evaluating security issues, but refer to product documentation for detailed instructions

”

Part I: Managing the Conflict Between Business Productivity and IT Security

Printers have rapidly advanced technologically in recent decades, bringing SMBs the benefits of increased productivity and efficiency, as well as decreased costs.

However, unlike printers of yore, printers today are essentially powerful computers. Consider the following printer features and functionality that are commonly available off the shelf:

> *"However, unlike printers of yore, printers today are essentially powerful computers"*

- **"Smart" capabilities** – Printers now integrate into print management systems, allowing SMBs to centrally administer enterprise printing practices. "Smart" features, such as log in to print and pull printing, help reduce waste, such as print-and-forget copies.
- **Multifunction features** – Printers often provide a range of capabilities in one device, from printing and scanning to faxing. Many newer models integrate with apps for features such as printing or scanning to cloud-based servers, increasing the efficiency and productivity of mobile employees.
- **Native hard disk drive (HDD) and random access memory (RAM)** – Many printers contain local storage that, in years past, was available only on computers.
- **Connectivity within the Internet of Things (IoT)** – Given their powerful features and connectivity to other IT devices, printers are nodes in an ever-expanding IoT.

But the features and functionality that provide benefits also introduce potential security vulnerabilities and business risk, if not secured. The conflict between business productivity and IT security is present in organizations of all sizes, but it can be especially pronounced in SMBs. SMBs must carefully balance this conflict to ensure profitability while not leaving the enterprise exposed to cyber risks.

Some criticize describing threats and vulnerabilities as spreading fear, uncertainty, and doubt (FUD). The purpose here is not to stir FUD but to raise awareness of facts

Part II: A Pragmatic Approach to Securing SMB Printers

The first step in balancing business productivity and IT security is to understand the security threats to and vulnerabilities in printers, as well as the business risks they pose. Some criticize describing threats and vulnerabilities as spreading fear, uncertainty, and doubt (FUD). The purpose here is not to stir FUD but to raise awareness of facts. Whether acknowledged or not, security threats and printer vulnerabilities exist. Ignoring them will not decrease the potential business risks they pose.

Four Categories of Security Threats to Printers

Security threats to printers entail four broad categories. Determining the likelihood that a threat will materialize as an attack can be tricky, given industry statistics on printer attacks are sparse.

However, industry surveys of IT security professionals provide some insight. These surveys report on the types and frequency of attacks encountered by enterprises over a specific timeframe, as well as what professionals view as the most concerning threats based on recent experiences.

> *The easier an attack, the more likely the threat will materialize*

The difficulty of conducting a type of attack must also factor into the threat's likelihood. The easier an attack, the more likely the threat will materialize.

Here, then, are the four categories of threat, ordered from the least to highest likelihood.

> *shared passwords are prevalent throughout businesses; compromising a log in to print password could turn up the password for data-rich user devices or even IT admin credentials*

- **Targeted Printer Attacks** – Industry statistics suggest that hackers rarely target printers specifically. However, it has occurred on occasion. For example, a "white hat" hacker carried out a targeted cyberattack against printers [1] in early 2017 to raise awareness of printer vulnerabilities. This attack was limited to forcing compromised devices to print a security warning for their owners.

  Historically, targeted printer attacks have been limited for a few reasons. First, while attractive for sabotage (e.g., forcing a printer to produce thousands of junk printouts), older printers offered hackers limited financial or intelligence value as a target. However, now that devices possess local HDD/RAM (e.g., files sent to print) and often integrate with identity and access management (IAM) systems (e.g., user passwords), printers are viewed as more valuable targets than in the past. For instance, shared passwords are prevalent throughout businesses; compromising a log in to print password could turn up the password for data-rich user devices or even IT admin credentials.

  Printer firmware (a native operating system, of sorts), historically, has been proprietary, which provided a degree of obscurity and a learning curve for hackers. But more information is available online today, decreasing the time and effort for hackers to learn underlying printer software and hardware systems for carrying out attacks.

- **Remote Hacks** – Perhaps slightly more common than targeted printer attacks are incidents that compromise printers as part of a broader-scale hack. In this scenario, unsecured printers can serve as a hacker beachhead into an otherwise secure network environment. Printers can be mapped as part of the enterprise network and, potentially, enable hackers to move laterally

In remote-hack scenarios, the SMB may not be the end goal

across the SMB network in search of more valuable targets, such as domain controllers that store passwords for many users and accounts. Such attacks require advanced skill, such as that exhibited by professional cybercriminals or nation-state hackers.

In remote-hack scenarios, the SMB may not be the end goal. It's not uncommon for sophisticated hackers to exploit an SMB as an avenue to another victim, such as a government agency or larger business. An example of this occurred in the 2013 hack of Target Corp. Hackers first compromised one of the retailer's HVAC contractors, an SMB that had remote access to a Target intranet, which allowed hackers entry into Target's enterprise network.

Finally, printers can be affected by attacks such as ransomware, in which hackers encrypt the victim SMB's data and require a ransom payment to decrypt it. Ransomware requires considerably less skill than sophisticated multi-step hacks while also promising a more immediate financial reward for cybercriminals. SMBs are often compelled to pay because of the attack's paralyzing effects on the business.

Devices under the remote control of hackers are called bots, and many bots form a botnet

- **Remote Harvesting** – Hackers sometimes compromise large numbers of computers or IoT devices (e.g., printers, webcams, smart TVs, etc.), which can then be controlled remotely as part of a distributed network. Devices under the remote control of hackers are called bots, and many bots form a botnet. Botnets range in size from tens of thousands to tens of millions. Recent examples include Mirai, Hajime, and Reaper, a new botnet discovered by security researchers [2] in October 2017.

  Botnets are useful to hackers in conducting certain types of attacks, such as using the distributed computing power to mine for cryptocurrencies. Botnets are also commonly used for distributed denial of service (DDoS) attacks, which overwhelm victim systems (e.g., web server) with network traffic that makes the hosted resource unavailable to users (e.g., websites). DDoS attacks can target printers.

To build a botnet, hackers often use automated tools to scan the internet for IoT devices with known security vulnerabilities

To build a botnet, hackers often use automated tools to scan the internet for IoT devices with known security vulnerabilities. Once discovered, a hacker's remote server initiates an automated script that exploits the vulnerability. The hacker then controls the compromised device as part of the botnet. Machines co-opted in a botnet often give no apparent warning to owners, which means there are thousands of compromised gadgets in botnets without the owners' knowledge.

Building a botnet doesn't require the skill of other attacks, such as remote hacks, and the tools (e.g., scanners, scripts, etc.) to build and control a botnet are readily available online. For these reasons, this attack is slightly more likely than a targeted printer attack or remote hack.

Perhaps most likely of all, unsecured printers lend themselves to insider threats, whether malicious or unintentional. Insiders may obtain and/or disclose confidential, sensitive, or proprietary data from printers

- **Insider Threat** – Perhaps most likely of all, unsecured printers lend themselves to insider threats, whether malicious or unintentional. Insiders may obtain and/or disclose confidential, sensitive, or proprietary data from printers. For insiders, obtaining the data can require little to no technical expertise or skill.

  Insiders are trusted users on SMB networks and premises. The insider threat, therefore, underscores the importance of physical security for printers.

  Along with ransomware, respondents identified insider threats as most concerning in the 2017 SANS Data Security Survey [3]. The insider threat is notoriously difficult to detect and prevent. Further, the chances of an insider succeeding are high, even at organizations with world-class security, as illustrated by repeatedly successful insider attacks at the U.S. National Security Agency and Central Intelligence Agency.

Because of their prevalence and integral role in business, printers have recently attracted the attention of security researchers to raise awareness of vulnerabilities.

Printer Security Vulnerabilities

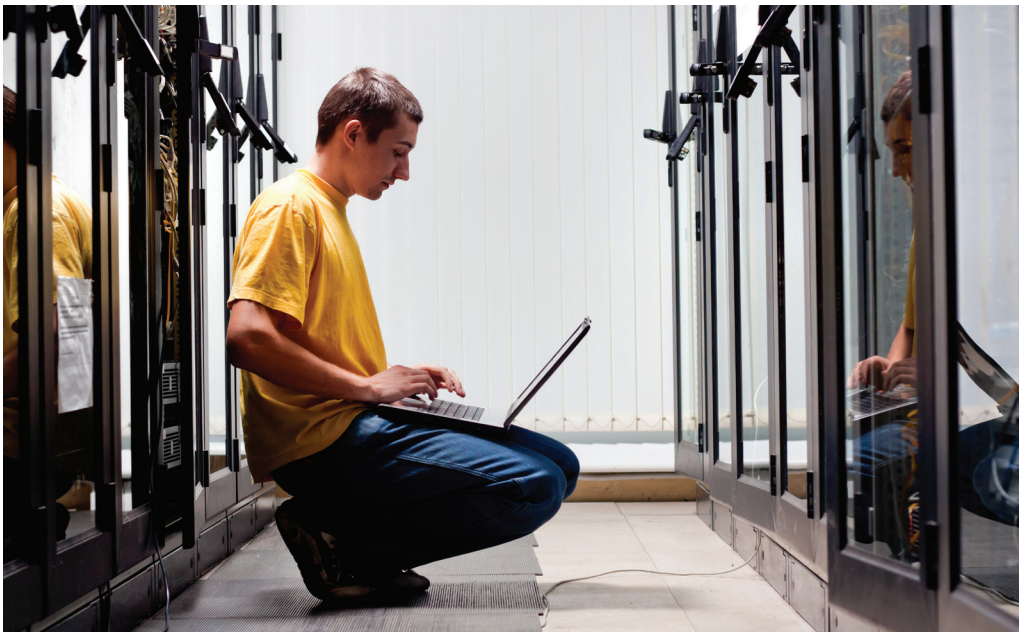
Threats comprise one side of the risk equation. Vulnerabilities comprise the other. For threats to succeed as exploits, vulnerabilities must exist.

Given printers' rich features and robust functionalities, as well as networking capabilities, they present hackers with a large "attack surface." In security, the attack surface is analogous to a target: The bigger the target, the greater the chance someone will hit it, eventually. In a security context, the more code and the more network connectivity, the higher the probability a determined hacker can find and exploit some underlying vulnerability therein.

Because of their prevalence and integral role in business, printers have recently attracted the attention of security researchers to raise awareness of vulnerabilities. For instance, Jens Müller, Juraj Somorovsky, and Vladislav Mladenov have published academic papers [4] and a blog [5] describing common printer security vulnerabilities.

These researchers also built a tool called the PRinter Exploitation Kit (PRET) [6] for penetration testing, which is the practice of allowing hired hackers to attack systems and networks to test security. The rationale is that it's better for so-called

Thanks to emerging research and tools, white hats are discovering vulnerabilities in printers and alerting vendors, who then develop security patches to fix the vulnerabilities



white hats – hackers employed by legitimate businesses – to discover security vulnerabilities and alert organizations to them before so-called black hats discover them.

Thanks to emerging research and tools, white hats are discovering vulnerabilities in printers and alerting vendors, who then develop security patches to fix the vulnerabilities. Explaining every printer vulnerability is beyond the scope of this guide, but the Hacking Printers Wiki [7] provides an overview.

Implementing a Security Strategy

Given the threats and vulnerabilities, SMBs should develop and implement a strategy for securing printers (and other IT assets).

A pragmatic approach to retaining the business benefits of printers, while also securing them, is to reduce the attack surface. Using a two-step evaluation process, SMBs can determine which features and functionality are needed or are not needed, and then:

1. Disable unneeded features and functionality.
2. Properly configure and secure the required features and functionality.

With this approach in mind, the next section presents a checklist to use for evaluating printer security.

Part III: A Checklist for Securing Printers

This checklist introduces common security concepts, issues, and safeguards relevant to printers. Refer to the printer's technical documentation for specific, how-to instructions. Some safeguards may need to be implemented via network/security appliances, such as routers and firewalls.

The checklist contains the following subsections:

- **Device** – Recommends safeguards to physical printers, including native software and hardware.
- **Network** – Recommends ways to safeguard printers within the SMB network environment.
- **Data** – Recommends safeguards to content and passwords.
- **User identity and access management (IAM)** – Recommends ways to ensure only authorized individuals can access and use printers.
- **User monitoring** – Recommends ways to create an audit trail of printing activities, which can be useful for business administration and security purposes

Let's explore each of these areas on the next page.

“

This checklist introduces common security concepts, issues, and safeguards relevant to printers

”

Device

"It doesn't matter how big your company is or what industry you're in. From the biggest blue chips to the smallest boutique firms, security is critical, especially when you consider how many ways sensitive data can become exposed, leaked, or stolen. By more tightly controlling the physical end of the network – printers and the print queue – you can now close one of those big open doors that worry security pros to such a great extent."

- Jeff Segarra,
Senior Director at Nuance
Document Imaging Division

- **Physically secure printers**

Given the likelihood of and printer vulnerability to insider threats, prioritize physical security.

- **Situate printers in secure areas** – Space can be tight in any office, especially SMBs, but try to physically isolate printers used for sensitive data, such as financial and HR. A locked closet works, as will situating the printer close to an employee, such as an executive assistant or IT administrator, who can monitor printing activities.
- **Don't leave printouts unattended** – Some information should be limited to as few people as possible, such as payroll data and sensitive HR issues. (The government maxim for determining access to classified information is "Need to Know.") Configuring printers for log in to print or for pull printing, which require the user to authenticate at the device before producing copies, will add a measure of security as well as cost control (e.g., against accidental printing).
- **Enable group security policies** – Many large enterprises devote significant resources to segmenting sprawling networks and administering group policies to limit access to and use of resources by type of employee, department, etc. But what about SMBs? Complicated security policies aren't feasible. Check with the printer vendor because some offer affordable solutions that are easy to set up and simple to use, with enterprise-like features (e.g., Epson Print Admin).

- **Apply security patches regularly**

When researchers discover a security vulnerability, vendors will sometimes issue a security patch, which is an update to the code that fixes the vulnerability. Most standard updates bundle patches, but if the vulnerability is particularly severe and widespread, a vendor may issue a standalone patch. (Such vulnerabilities usually make the news.) Apply patches promptly to prevent hackers from exploiting known vulnerabilities. There are two types of patches to track for printers:

"Apply patches promptly to prevent hackers from exploiting known vulnerabilities"

- **Firmware** – Most printers run a sort of operating system called firmware. Firmware determines how native printer hardware, as well as native and non-native software (e.g., apps), function. Check the printer vendor's website twice yearly to see if any firmware updates and/or security patches have been issued and then to apply available firmware updates/patches promptly.
- **Non-native software** – Some vendors and third parties create software to enhance printers' standard features and functionality. Researchers occasionally discover vulnerabilities in the code for non-native software, such as apps. Firmware patches may not remedy vulnerabilities in non-native software code. Ensuring SMB users are running the most updated version of the software will usually provide adequate security against known vulnerabilities.

- **Secure HDD/RAM**

It's not uncommon for printers to possess native storage. As with PCs, printer storage can be HDD or RAM. Safeguard the printer's native storage by:

- **Securing removable HDDs** – Some models include a removable HDD. The HDD often stores print metadata, as well as files sent to the device. Secure removable HDDs to ensure insiders cannot steal or temporarily remove them to extract data.
- **Enabling secure file erase** – Some printers offer a feature that completely erases files stored in the HDD and/or RAM once the files are deleted. Ensure this feature is enabled, if available.

- **Disable unused physical ports**

Printers possess two types of ports: physical and network. The next section addresses network ports. Physical ports refer to the printer's female connectors (e.g., sockets, jacks, etc.), which work in conjunction with male connectors (e.g., USB drives and cables). Disable all unused physical ports on the printer. Some types of multifactor authentication will require enabling at least one physical port to authenticate users via the second factor (e.g., USB stick).

"Disable all unused physical ports on the printer"

An IT networking expert should consult on implementing these measures because misconfigured network settings can severely impact high volumes of SMB network traffic

Network

The safeguards recommended in this section are among the most important. Unfortunately, some are potentially complicated to implement because they require changing settings on other network appliances, such as routers and firewalls. An IT networking expert should consult on implementing these measures because misconfigured network settings can severely impact high volumes of SMB network traffic. If there is no in-house networking expertise, first check with the vendor to see if it can provide remote or on-site support. If not, hire a trusted IT consultant to assess and configure network settings to minimize disruptions to the business.

- **Do not expose printers to the public internet**

Of all the security measures in this guide, this is perhaps the single, most effective one. This measure alone is not enough, but it makes many attacks – including entire classes of remote hacks – far more difficult, if not impossible, to achieve.

There is no reason to expose printers to the public internet because there is no reason anyone outside of the SMB's network should have access to or be allowed to use the SMB's printers. If guests need to print, then they should first be required to access the secured SMB network via a password provided to them by an authorized employee. Once on the SMB network as authenticated users, guests can print.

> *If the SMB uses hardware firewalls, a networking professional can create a rule that blocks all ingress traffic from and egress traffic to the public internet via the printer's communications ports*

Unfortunately, this measure's implementation can be as complicated as it is important. Consult a networking specialist.

Depending on the SMB network architecture, this step can be implemented in many ways. The most common include:

- Creating a firewall rule – If the SMB uses hardware firewalls, a networking professional can create a rule that blocks all ingress traffic from and egress traffic to the public internet via the printer's communications ports. (Communications ports differ from physical ports. See the next section for more on communications ports.) This setting, appropriately configured, will not affect authenticated employees and guests on the SMB network. There are less secure settings, but creating a rule to block all ingress traffic to the printer from the public internet and all egress traffic from the printer to the public internet will provide maximum security.
- Configuring network traffic at the router – If the SMB does not use a hardware firewall, many routers designed for small businesses include built-in firewall functionality. The router can be configured with a rule to block all ingress and egress traffic to the printer via the firewall or the router's network settings.

- **Disable unused communication ports**

In a communications context, network ports are analogous to ramps on a communications highway: They provide a numbered ramp on and a numbered ramp off for data traveling along communications channels. The source port (e.g., employee computer) and destination port (e.g., printer) are the endpoints for data.

Within the standard Transmission Control Protocol/Internet Protocol (TCP/IP), there are 65,535 available ports. All the printer's unused ports should be disabled.

Depending on the printer model and network architecture, there are two common ways to disable unused ports:

- Printing device – Some printers allow a limited number of network configurations via the device itself.
- Networking appliances – Rules can be created via firewalls or routers.

As with other safeguards in this section, consult the technical documentation and seek out a networking professional to advise on implementation.

- **Secure the SMB Wi-Fi Network**

Wi-Fi safeguards rank equally in importance with not exposing printers to the public internet. They are also easier to implement, as many require selecting from a menu of options in standard router settings.

Securing the SMB's Wi-Fi network entails a few steps:

> ***Wi-Fi safeguards rank equally in importance with not exposing printers to the public internet.***

- **Enabling Wi-Fi Protected Access (WPA) Security** – Most off-the-shelf wireless routers provide three options for securing the Wi-Fi network: Wired Equivalent Privacy (WEP), WPA, and WPA2. The technical distinctions between these options are beyond the scope of this guide, but the recommended setting is WPA2. WPA2 will password protect the SMB Wi-Fi network and encrypt local network traffic. Note that WPA2 does not encrypt traffic beyond the SMB's edge devices (e.g., routers); Secure HTTP (HTTPS) provides end-to-end encryption of internet traffic. Still, WPA2 adds a layer of protection against local eavesdroppers and for user authentication to the network. WPA2 can usually be enabled via the click of a button in standard wireless router settings. It's uncommon for this option to affect network traffic, but consult a networking professional for recommendations based on the specific SMB network. Check twice yearly for updates to router firmware to protect against newly discovered vulnerabilities, such as KRACK [8].
- **Secure Bluetooth, Near Field Communication (NFC), and Wi-Fi Direct** – Check the printer's technical documentation to see if these features are included. Disable features not needed or refer to the documentation for steps to securely configure them.

- **Deploying IEEE 802.1X Port Security** – This option is recommended only for organizations whose day-to-day business focuses primarily on highly sensitive data, such as companies in defense and financial services. Deploying 802.1X can be complicated, requires special networking appliances, and should be undertaken only by certified network engineers. But 802.1X provides a highly secure wireless networking environment.

- **Follow Microsoft's advice: Disable Server Message Block v 1.0**

> *Disabling SMB1 and using another protocol for resource sharing is good security for printers and organizations more broadly*

Server Message Block v 1.0 (SMB1) is a communications protocol commonly used in Microsoft Windows for sharing network resources, such as files and peripheral devices like printers. SMB1 has long been considered by security professionals to be a fundamentally insecure protocol. Most recently, the prevalent use of SMB1 contributed to 2017 ransomware attacks, dubbed WannaCry and NotPetya, reaching a global scale. SMB1 is also commonly leveraged in smaller-scale ransomware attacks to maximize the spread and damage of this debilitating malware throughout victim organizations. Disabling SMB1 and using another protocol for resource sharing is good security for printers and organizations more broadly. Some legacy multifunctional printers still require SMB1 because their firmware uses a feature called "scan to share." Organizations should upgrade these printers and take other steps to update systems and devices to eliminate the need to use SMB1, as Microsoft has repeatedly warned [9].

Data

"To reduce leakage of confidential or sensitive data, it is important that SMBs consider encrypting print jobs in transit or at rest from the PC to the printer."

- Eric Crump, Director of Strategic Alliances at Ringdale

- **Encrypt data at rest and data in transit**

Every security measure recommended in this guide is ultimately intended to protect data. And the most direct way to secure data is via encryption. Encrypt data in two states.

- **Data at rest** – This refers primarily to data that resides in the printer's native storage, particularly the HDD. Many newer printers offer the functionality to encrypt data stored in the native HDD. Sometimes this functionality is enabled by default, but other times it must be turned on or implemented with non-native software. Check your printer's technical documentation for instructions on encrypting data stored in the HDD.
- **Data in transit** – Most data that must be printed originates on a device other than the printer, which means it must be sent over a network from the source device to the printer. Sensitive data includes not only the printed content but also the passwords used to authenticate devices and users. In part, this requires network-level encryption, such as that provided by WPA2 wireless security, which uses the Advanced Encryption Standard (AES). Another common

safeguard is Internet Printing Protocol (IPP), which encrypts data in transit using HTTPS. IPP also supports other security features, such as access control and user authentication. Enable IPP, if available.

User Identity and Access Management (IAM)

"Securing the print environment is an important part of any company's overall IT security program, yet most organizations simply don't do enough to focus on this area. When you consider that 70% of companies today have experienced a data breach through their printing practices, it's easy to tell how much still needs to be done. Printers and MFPs play a major role in an organization's transfer of information. As such, print security should be considered vital to a comprehensive IT security strategy."

- Jeff Segarra,
Senior Director at Nuance
Document Imaging Division

- **Change default passwords**

Most printers come with default passwords created by vendors. Change default passwords immediately. This guide [10] provides updated best practices for creating strong passwords. In addition to creating strong passwords, SMB employees should not reuse passwords for different accounts (e.g., printer and email). Every account should have a strong password unique to each user and each account.

- **Actively administer user authentication**

To control who is authorized to access and use printers, SMBs should administer an IAM program. Common components of IAM programs include password management and group policies. The most common tool for administering IAM programs – for SMBs running Microsoft Windows – is called Microsoft Active Directory (AD). If the SMB currently uses passwords for anything IT related, there's a good chance user names and passwords are administered using AD. Printer IAM can also be administered via AD.

There are two common methods of authenticating users.

- **Enable single-factor authentication** – The most common form of single-factor authentication is the password. Microsoft AD allows administrators to set up role-based access control (RBAC). RBAC grants users access to and privileges based on their positions and job duties. So, for instance, project engineers are not granted access to finance department printers, since SMB finances do not pertain directly to project engineering job functions.
- **Consider two-factor authentication (2FA)** – 2FA requires users to provide a password (one factor) plus another factor. This second factor could be a special USB drive inserted into the physical port of a printer, a badge that must be scanned to gain physical access to the printer, or a token that confers a unique code that users must enter in addition to the user password for each new print job. 2FA is commonly used for pull printing, which holds print jobs on the source device (e.g., PC) or a print server until the user authenticates at printer (via password and/or PIN, USB, etc.). Note that the use of some implementations of 2FA will require leaving at least one physical port enabled on the printer.

Consult Microsoft's technical documentation [11] on AD for implementation.

- **Enable Internet Printing Protocol (IPP) printing**

In addition to network-level data encryption, IPP enables IAM program administration via access control and user authentication. Check the printer's technical documentation to see if IPP is available and how to configure it.

"Some awareness of security threats to printers exists, but most SMBs don't realize the extent of vulnerabilities when printing. An important capability – for both security and business management purposes – is auditing and tracking information by user as it's printed, whether from phone, tablet or PC."

- Eric Crump, Director of Strategic Alliances at Ringdale

User monitoring

- **Audit and track printing**

Some newer printers provide native auditing and tracking functionality. Others provide it via non-native software (vendor or third party). Many newer models can also be integrated into an enterprise print management system to provide this capability. Regardless of SMB size, the practice of auditing and tracking print jobs is good for security and business administration, as it allows metrics on usage and, ultimately, costs.

If there is a security incident involving printers, this capability will allow tracking the malicious behavior to its source. The clues provided will be valuable to the investigation. Check the printer's technical documentation to see if auditing and tracking functionality is native or available as an add-on feature.

- **Create and regularly review logs**

A subset of auditing and tracking, logs provide valuable data on IT usage for security and business purposes.

In the event of a security incident, logs will provide valuable clues to security analysts as they piece together what happened. SMBs should create and retain logs on enterprise devices and network activities. These logs often integrate with a security information and event management (SIEM) tool. SIEMs allow data from logs to be collected, stored, and visually displayed on a central dashboard to enable analysis. SIEMs are invaluable in security investigations.

Conclusion

Securing printers in SMB networks requires a delicate balance between business productivity and IT security. By evaluating which features the business needs and then ensuring their proper configuration – as well as disabling unneeded features – SMBs can reduce the attack surface available to hackers seeking to spy on, steal, or destroy business data.

Thank you for spending the time to learn more about printer security at Epson.

For additional resources, product information, or to schedule an on-site meeting with one of our print solution experts, please contact:

Linda Presutti – Business Development Manager, Business Imaging

Linda.Presutti@ea.epson.com

732.672.3924

Jose Espinoza – Sr. Technical Sales Support Representative, Business Imaging

Jose.Espinoza@ea.epson.com

949.667.1902

About Epson WorkForce® Printers for Business

From small offices and departmental workgroups, the full lineup of heavy-duty and reliable business printers from Epson delivers high performance.

Managed Workgroups

Epson printers for business workgroups and teams offer a variety of features, including single and multifunction options, high-yield ink and lower printing costs.†

WorkForce Enterprise

Experience high-volume printing for hard-working groups with fast print speeds in a full-color, A3 department MFP designed to deliver everything that large workgroups need.

PrecisionCore® Next-generation Print Head Technology

PrecisionCore is a revolutionary step forward in printing technology. Engineered to deliver increased speed and unbeatable image quality, this high-density print chip generates up to 40 million precise dots per second with astonishing ink placement accuracy and fewer distortions and imperfections.

Printing Services & Document Management Solutions

Epson works with the following premier partners to provide array of exceptional business printing software and service solutions:

- *Nuance*
- *FollowMe by Ringdale*
- *Drivve*
- *Gespage*
- *nddPrint*
- *PaperCut*
- *Preo Analytics*

- **To learn more about the full line of Epson WorkForce® Printers, visit: epson.com/business-printing-solutions-services**

† Features and speeds vary by model. See https://epson.com/workforce-office-printers-for-business for more details.

Sources

1. Smith, Ms. "Hacker stackoverflowin pwning printers, forcing rogue botnet warning print jobs." CSO Online. Feb. 5, 2017. <https://www.csoonline.com/article/3165419/security/hacker-stackoverflowin-pwning-printers-forcing-rogue-botnet-warning-print-jobs.html>
2. Check Point Research. "A New IoT Botnet Storm is Coming." Check Point Security Blog. Check Point Security. Oct. 19, 2017. <https://research.checkpoint.com/new-iot-botnet-storm-coming/>
3. Filkens, Barbara. "Sensitive Data at Risk: The SANS 2017 Data Protection Survey." The SANS Institute. September 2017. <https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-sans-2017-data-protection-survey.pdf>
4. Müller, Jens, Juraj Somorovsky, and Vladislav Mladenov. "SoK: Exploiting Network Printers." Horst Görtz Institute for IT-Security, Ruhr University Bochum. <https://www.nds.rub.de/media/ei/veroeffentlichungen/2017/01/30/printer-security.pdf>
5. Ibid. "Printer Security." Horst Görtz Institute for IT-Security, Ruhr-University Bochum. Jan. 30, 2017. <https://web-in-security.blogspot.ro/2017/01/printer-security.html>
6. Ibid. "Printer Exploitation Toolkit - The tool that made dumpster diving obsolete." Github. <https://github.com/RUB-NDS/PRET>
7. Muller, Jens and various authors. "Hacking Printers Wiki." A Project by Jens Muller. <http://hacking-printers.net/wiki/index.php/Main_Page>
8. Bonneau, Joseph. "KRACK Vulnerability: What You Need To Know." Deep Links. Electronic Frontier Foundation. Oct. 19, 2017. <https://www.eff.org/deeplinks/2017/10/krack-vulnerability-what-you-need-know>
9. Mackie, Kurt. "Microsoft Offers More Advice on Disabling Windows SMB 1." Redmond Magazine. May 18, 2017. <https://redmondmag.com/articles/2017/05/18/more-advice-on-disabling-windows-smb-1.aspx>
10. National Institute of Standards and Technology. "NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management." U.S. Department of Commerce. June 2017. <https://pages.nist.gov/800-63-3/sp800-63b.html>
11. Microsoft. "[MS-ADTS]: Active Directory Technical Specification." Microsoft Developer Network. Microsoft Corp. Dec. 1, 2017 [Major Revision]. <https://msdn.microsoft.com/en-us/library/cc223122.aspx>
12. Eric Crump is the Director of Strategic Alliances for Ringdale based outside of Atlanta, Georgia. He leads and develops the strategic alliance activities with global partners and key industry analysts. He has over 22 years' experience in the printing and imaging industry. He has served in this role on the FollowMe Team since June 2014 and is a contributing member of the Standards and Best Practices Committee for the Managed Print Services Association (MPSA).

EPSON®
EXCEED YOUR VISION

EPSON is a registered trademark and EPSON Exceed Your Vision is a registered logomark of Seiko Epson Corporation. All other product and brand names are trademarks and/or registered trademarks of their respective companies. Epson disclaims any and all rights in these marks.
Copyright 2017 Epson America, Inc.

- **Another innovation from Epson Business Solutions.**
- **Find out more at Epson.com/ForBusiness**

Epson America, Inc.
3840 Kilroy Airport Way, Long Beach, CA 90806