brother
at your side

BROTHER SECURITY

WHITE PAPER NOVEMBER 2017

SECURING YOUR BUSINESS INFRASTRUCTURE

Today's Security Challenges & What You Can Do About Them

The last decade has seen many exciting advances in connectivity accelerated by the near universal availability of smartphones and tablets – leading to a highly interconnected world.

The security of networks - and the businesses and individuals that rely on them - has become top of mind for the IT Security professionals who are responsible for ensuring the safety of the data and the networks where this information is utilized.

As high-visibility security breaches occur - affecting ecommerce, banking, retail and other industries - the critical importance of the security of the infrastructure these businesses rely on continues to grow.

Security in the workplace is a daily fact of life. From using ID cards to control physical access, to entering passwords to join the network, to using software to monitor and prevent unauthorized access, all are routinely used to protect critical assets and information.

However, there is one key area where many organizations still have potential vulnerabilities. This is where networked devices (including printers or scanners) connect to the network; in this instance, relying on perimeter-based security alone is not enough to protect the network or a company's critical data.

Developing and implementing proactive security policies, while simultaneously being challenged by a variety of threats creates a major dilemma for IT Security professionals. This is further complicated by having to outwit the next threat while managing to comply with many different standards and regulations.

Brother offers IT Security professionals a number of solutions. Whether developing a proactive policy based on the CIS 20 Critical Security Controls, or complying with regulation standards such as PCI DSS, or HIPPA, Brother can help address your security concerns and objectives.

What exactly are the threats?

There are three key areas that networked printers, all-in-ones or scanners can pose a threat to an organization.
These include:

1. **Device Security – Individual Access**
2. **Securing Documents and Data**
3. **Securing Devices on the Network**

To help eliminate these common security threats, this paper outlines the specific risks administrators should be aware of, the types of technology included with Brother devices, and how these devices can be integrated with existing security measures to help improve the security of your organizations most critical information.

DEVICE SECURITY INDIVIDUAL ACCESS

What are the dangers?

It doesn't matter how effective your organization's security policy is - if an individual can simply walk up to a printer, pick up uncollected pages and then walk away with them, then your confidential data is at risk.

In mid to large size organizations, there's always a risk that uncollected print jobs – some with highly sensitive documents or data - can be left exposed to anyone walking past them.

What can organizations do about it?

The best means to effectively address this issue is to delay printing until the authorized user is at the machine using a PIN or secure card reader. Depending on the size of the organization, we recommend several different solutions.

The first is to use Brother's **Secure Print** feature, designed primarily for people who only occasionally print confidential documents. Secure Print allows users to delay the actual printing process until they are physically at the printer.

When printing a sensitive document, a worker just needs to assign a PIN number to the print job as its being sent to the device. If printing confidential documents is done more frequently, using **Active Directory Secure Print** can be more effective.

Where organizations share printers between multiple users or need to put them in public places, controlling abuse without obstructing normal use can be difficult. By using Active Directory or LDAP authentication, any user with login credentials can easily use their existing network login credentials to gain access to printers on the go.

This feature completely restricts physical access to any function on the printer by locking out any unauthorized user. It uses an existing Windows Active Directory username and password to unlock the printer and enables the user to collect their document. If desired, the job may be stored in the printer's internal memory until it is collected.

To use this capability, an organization must already be using Microsoft Active Directory. For organizations that do not use Active Directory, Brother also supports secure printing via LDAP supported database servers. This works the same way as the Active Directory Secure Print method, but communicates with an LDAP enabled server instead.

For an extra layer of security (using Active Directory or LDAP secure print functions), administrators can specify a time limit for how long print jobs can remain in device memory, ensuring that confidential documents do not remain inside the machine indefinitely.

Even with these measures, there is always the potential for additional issues. For example, using certain software applications can allow data to be intercepted as it travels to the printer itself

To safeguard against this, Brother devices have built-in Transport Layer Security (TLS) encryption for features such as IPPS and HTTPS management, the same technology used in e-commerce to protect bank and credit card information. This ensures that the most confidential files can be transmitted over the network using modern 256 bit AES encryption.

Despite having security rich features, unless printers are physically locked away in secure facilities, unauthorized users can still walk up and attempt to retrieve information from them. For mid-sized businesses with little or no IT infrastructure, some form of physical security is especially important.

If an organization is seeking to improve document security without the need for additional or expensive middleware, servers or IT infrastructure, Brother offers an alternative cost-effective solution.

What can organizations do about it?

Brother devices have a range of security functions that will prevent unauthorized people from tampering with them.

Setting Lock restricts access to the device's settings through the control panel. This is ideal for organizations that do not want to limit the devices functionality, but want to ensure unauthorized users are not able to change any settings.

Secure Function Lock takes that device security further by preventing access to both the device's settings and select device functions, allowing administrators to decide who can do what with each machine, for each machine function.

This can include allowing access to machine functions and page limits through unique PIN numbers or NFC access cards.

Adding Brother's optional Storage Print capability to SFL enables a low-cost method for releasing print jobs only when a user logs into a device - securely protecting confidential information that should not be inadvertently seen or shared.

In the following example, the Director is able to print, scan, copy and FAX anything they want, however, the Manager is unable to print or scan. In the case of the assistant manager, they are only able to receive faxes.

In addition to blocking a function, it is also possible to restrict how much a function is used.

For example, instead of blocking the print function completely to the Manager, it would be possible to restrict the number of pages the Manager could print every month This would be one means of limiting the amount of color printing they can perform, helping to control costs.

DIRECTOR	MANAGER	ASSISTANT MANAGER
PRINT	PRINT ⊗	PRINT ⊗
SCAN	SCAN ⊗	SCAN ⊗
COPY	COPY	COPY ⊗
FAX SENDING	FAX SENDING	FAX SENDING ⊗
FAX RECEIVING	FAX RECEIVING	FAX RECEIVING

SECURING DOCUMENTS & DATA

What are the dangers?

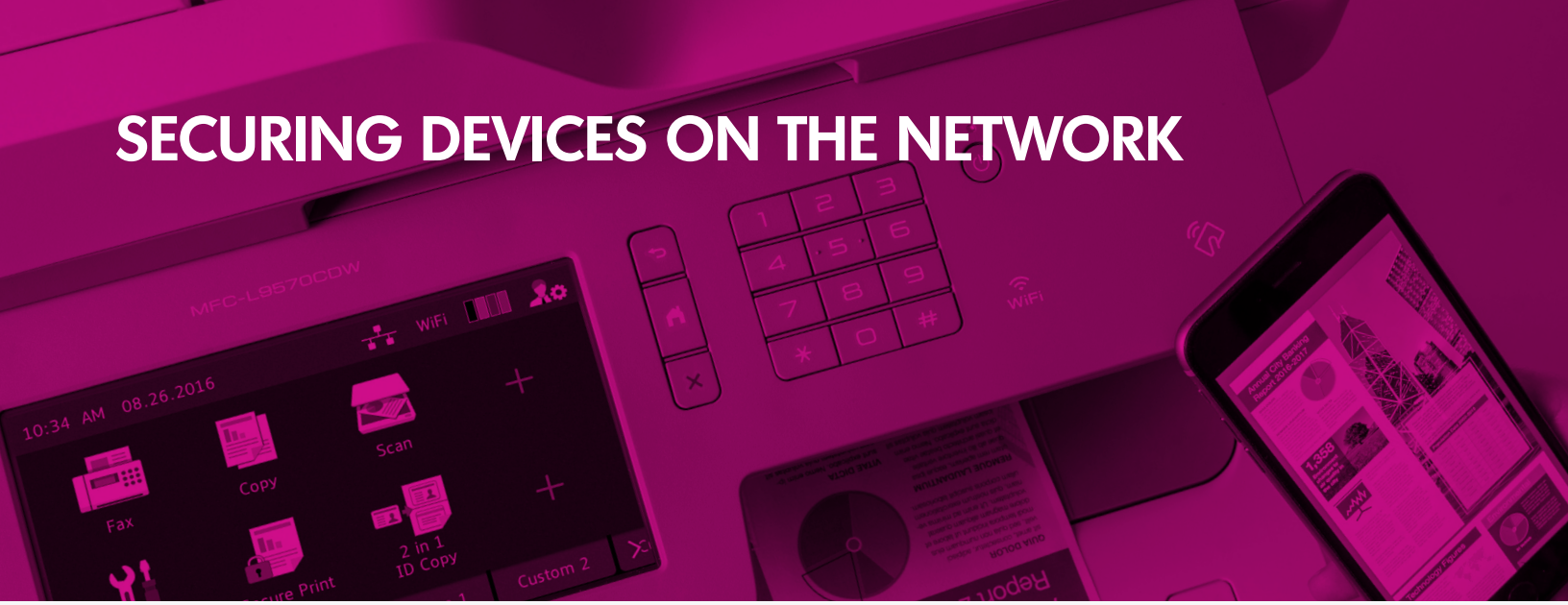
Even if your printer is secure, another potential threat can arise from documents that have been scanned. Once captured, there are many ways to store or share these documents. Sending scanned documents by email, or uploading them to a shared folder can be highly risky, especially if they contain sensitive data. In addition, since these can easily get sent to the wrong individual, there is no limit as to the number of copies that could be made or individuals it can be shared with.

What can organizations do about it?

The simplest solution is to turn these scanned documents into a Secure PDF. Brother's stand-alone and multifunction-based scanners can instantly secure any new PDF file with a four-digit PIN, so it cannot be opened without permission.

Alternatively, many Brother dedicated and multifunction-based scanners are also able to Scan to SFTP / SSH Server. Using the Secure Shell Protocol establishes a private and safe data stream; by controlling access to SFTP servers more closely, organizations keep their entire network more secure by closing a gateway into and out of their system.

SECURING DEVICES ON THE NETWORK



What are the dangers?

Tablets, laptops, and smartphones are subject to providing proper credentials and using secure authentication when joining a secure network. At the same time, these networks generally do not require new printers to do the same, even though their connectivity can present as much of a threat as these other devices.

What can organizations do about it?

Best Practices: When placing any device on a network, it is imperative that the device's embedded web server is password protected. This ensures that access to the devices' settings are restricted from unauthorized users.

Industry Standards: Because devices have various types of built-in encryption and authentication clients and servers, Brother can offer several means to improve security and help close any gaps.

802.1x: Brother devices all conform to the security standards supported under 802.1x, whether connected to the network via cable or as part of an organization's wireless infrastructure.

HTTP over TLS (HTTPs): In client mode, this is used to connect to Secure SMTP servers such as Office 365, Gmail and others. It is also used to provide secure scan to cloud functionality using Brother Web Connect or to integrate with third-party applications. In server mode, it allows secure remote administration via the internal web server.

IPP over TLS (IPPs): As data moves across the network, this capability provides encryption of print data streams, ensuring that it cannot be accessed by others that should not see it.

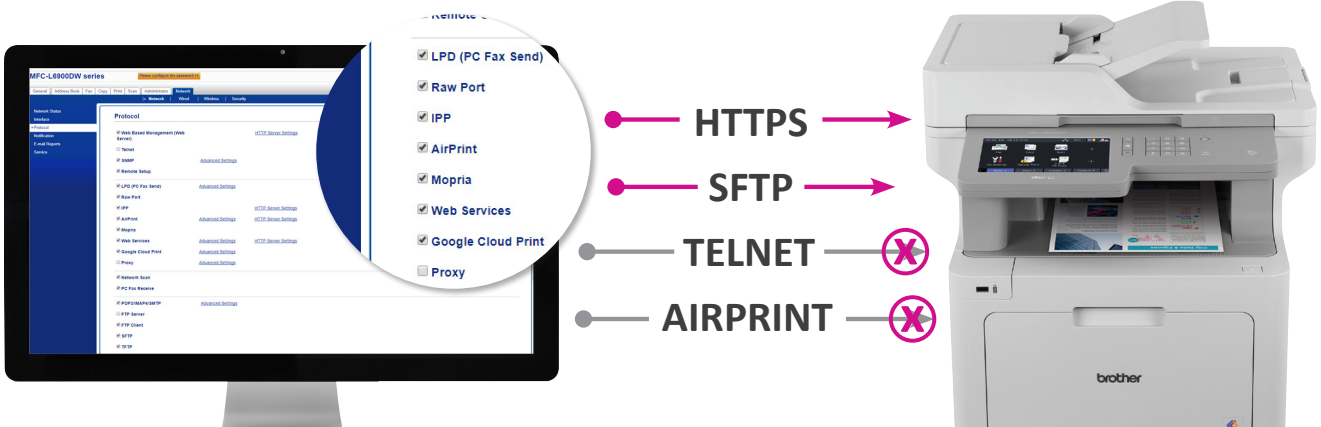
Secure Shell Client (SFTP/SSH Server): Used to provide robust end to end security using RSA encryption and Public Key Authentication for highly secure scan to cloud applications. This capability is available standalone or can be incorporated into BSI (Brother Solutions Interface) workflows.

IPsec: Multiple Brother devices can be connected to internal or external secure environments using IPsec, helping save time, money and effort. Because IPsec is built-in, there is no need to install middleware or use third party hardware to connect both end-points together.

SNMPv3: Fleet management tools (including Brother BRAdmin) use SNMP to communicate with devices. Brother devices support SNMP V3 that enables these communications to be protected using industry standard encryption.

Even if an organization is using an alternative print fleet management utility to manage their devices, Brother printers will still integrate seamlessly into their secure networks quickly and easily.

The example below shows how an IT administrator has disabled the following functions: Telnet and AirPrint® while still allowing HTTPS and SFTP protocols.



While encryption protects against external threats, if internal staff can access network-connected printers, there could be a vulnerability. To prevent issues, Brother printers provide Encrypted Communications with Password Protected access to Embedded Web Servers. This prevents unauthorized users from viewing sensitive data stored on the device or making changes to a device's settings.

They also support IP Filtering, which limits access to the device by white listing IP addresses belonging to machines authorized to connect or, conversely, black listing the IP addresses of unauthorized machines. In the following example, the printer will only accept connections from users with the following IP Addresses: 10.45.12.45 and 10.45.12.47.

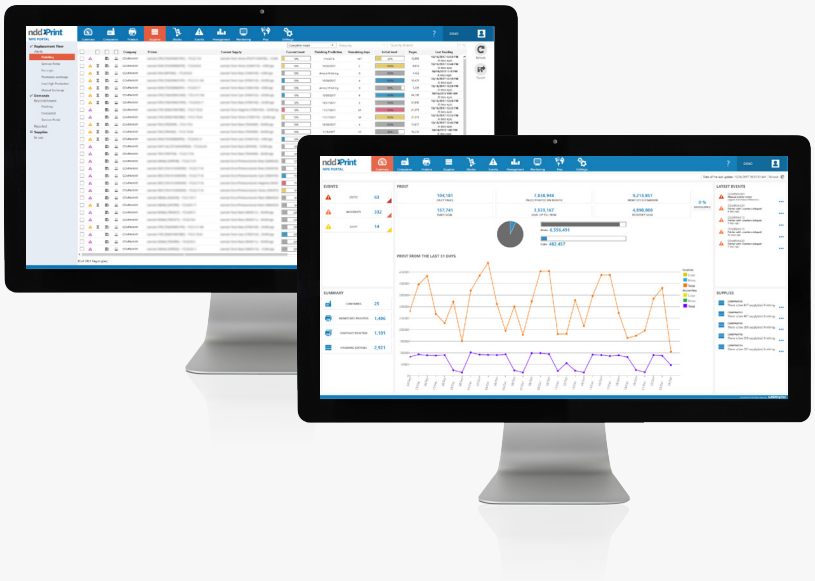
For a less restrictive solution, Protocol Control allows administrators to disable protocols not required without completely blocking access to everything.

THE WHOLE PACKAGE

For organizations that know they want to control their security and see in more detail how their devices are being used.

Using Other Print Solutions

Other print management solutions including PaperCut and nddPrint360 have used the Brother Solutions Interface (BSI) to integrate with Brother devices to support authentication. This can be done using a pin, integrated NFC, or a variety of optional external third party USB HID readers which allow using existing building access cards or other security devices to authenticate to Brother products.



BSI allows developers to integrate their own security, workflow or management solutions with Brother devices quickly and easily, with control over UI, device functions, security and management all possible.

For more information on BSI please visit:
http://www.brother-usa.com/lp/civ/BSI.aspx

Moving Forward

It is imperative that organizations take the security threats to their data and network seriously. Since there is no “one-size fits all” solution available. IT Administrators need to identify and select the appropriate security solutions for their infrastructure, budget, and within the framework of their existing network.

At a minimum, an organization must ensure that it has:

1. **Made its devices secure**
2. **Protected its data en route and after printing**
3. **Protected its network from intrusion**

Once these items are addressed, IT Administrators can be confident that they have taken the necessary precautions to ensure that their print and capture infrastructure is protected against the many security threats that will challenge them in the future.

Brother offers several intelligent and effective security solutions that can help IT Administrators meet these challenges. For more information, please visit www.brother.com.