Security Guide

Protecting your documents, safeguarding your business

www.sharp.eu

SHARP

Be Original.

Shutting out the cyber criminals

If left unprotected, printers are an open backdoor into your business to steal or compromise your valuable data.

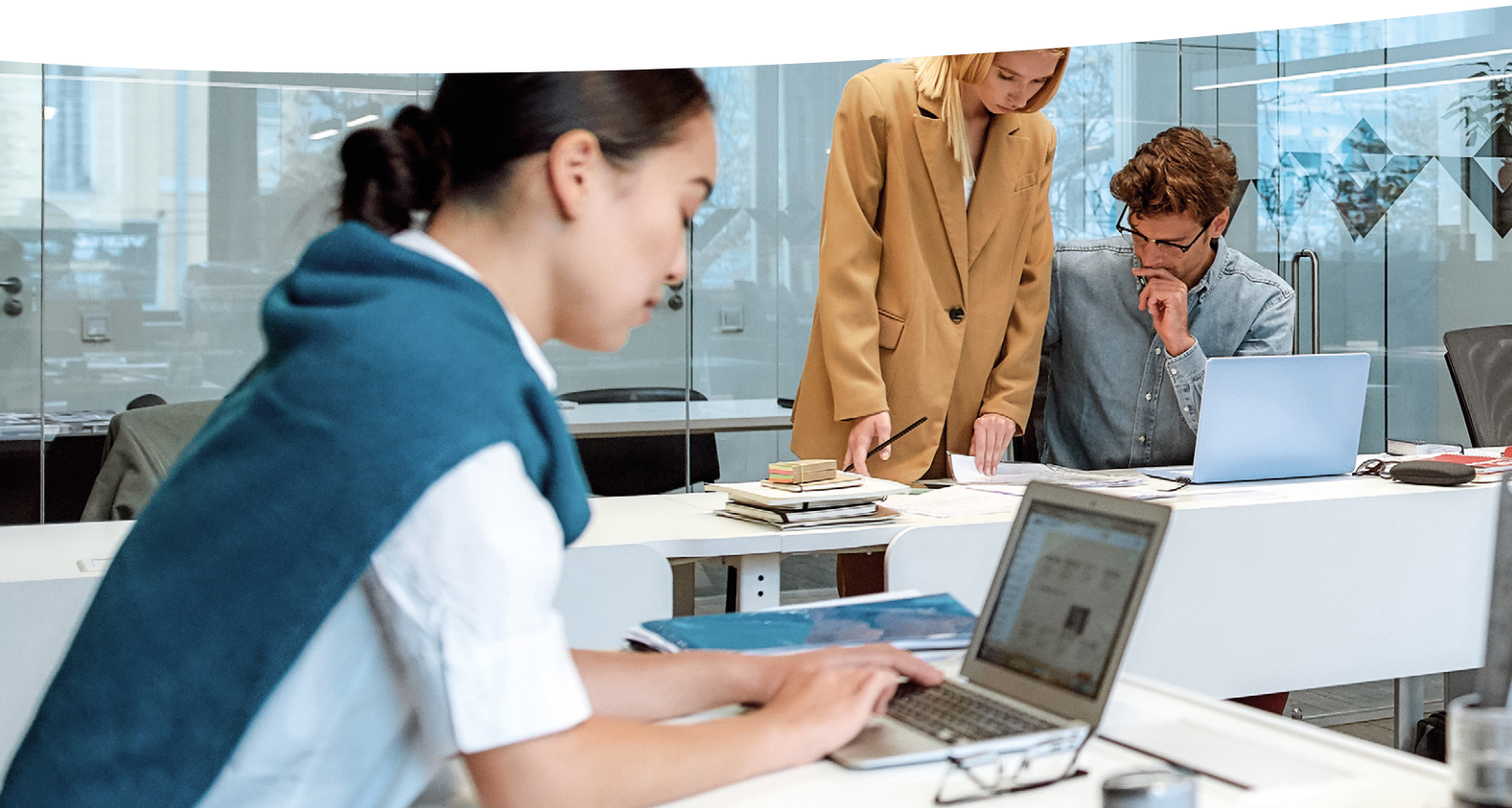
Printers are a familiar fixture in most workplaces. Used routinely every day, on the outside they may not appear to have changed much over the last ten or even twenty years. However, as IT administrators know, multifunctional printers (MFPs) and printers have evolved to become sophisticated computer systems that are connected to your business network and the Internet.

Unfortunately, while the issue of data security is high on the agenda of most organisations, their print devices are often overlooked. In fact, a third of European SMEs have no IT security measures in place that cover printers*. It makes them a key target for hackers and malicious actors, especially as the move towards hybrid workplaces has opened up more vulnerabilities. Unsecured printers often provide an easy gateway into your business and enable access to sensitive information contained in the print and scan jobs and potentially your entire IT network.

The threat is very real – and being exploited. Almost one fifth (19%) of European SMEs have been impacted by a printer security breach*. In addition, when data is compromised, it can cause a huge amount of long-lasting reputational damage.

Every business, no matter how large or small, needs to ensure that their document production environment is protected through technology and safe user behaviour – as much as every business laptop or PC. That is why security is at the heart of all of Sharp's product development. We want to ensure that our products and services make people's working lives easier and more productive, while keeping data safe at the same time.

*Research conducted by Censuswide in February 2023 with 5,770 IT decision makers in SMEs in Austria, Belgium, France, Germany, Italy, Netherlands, Poland, Spain, Sweden, Switzerland and UK.

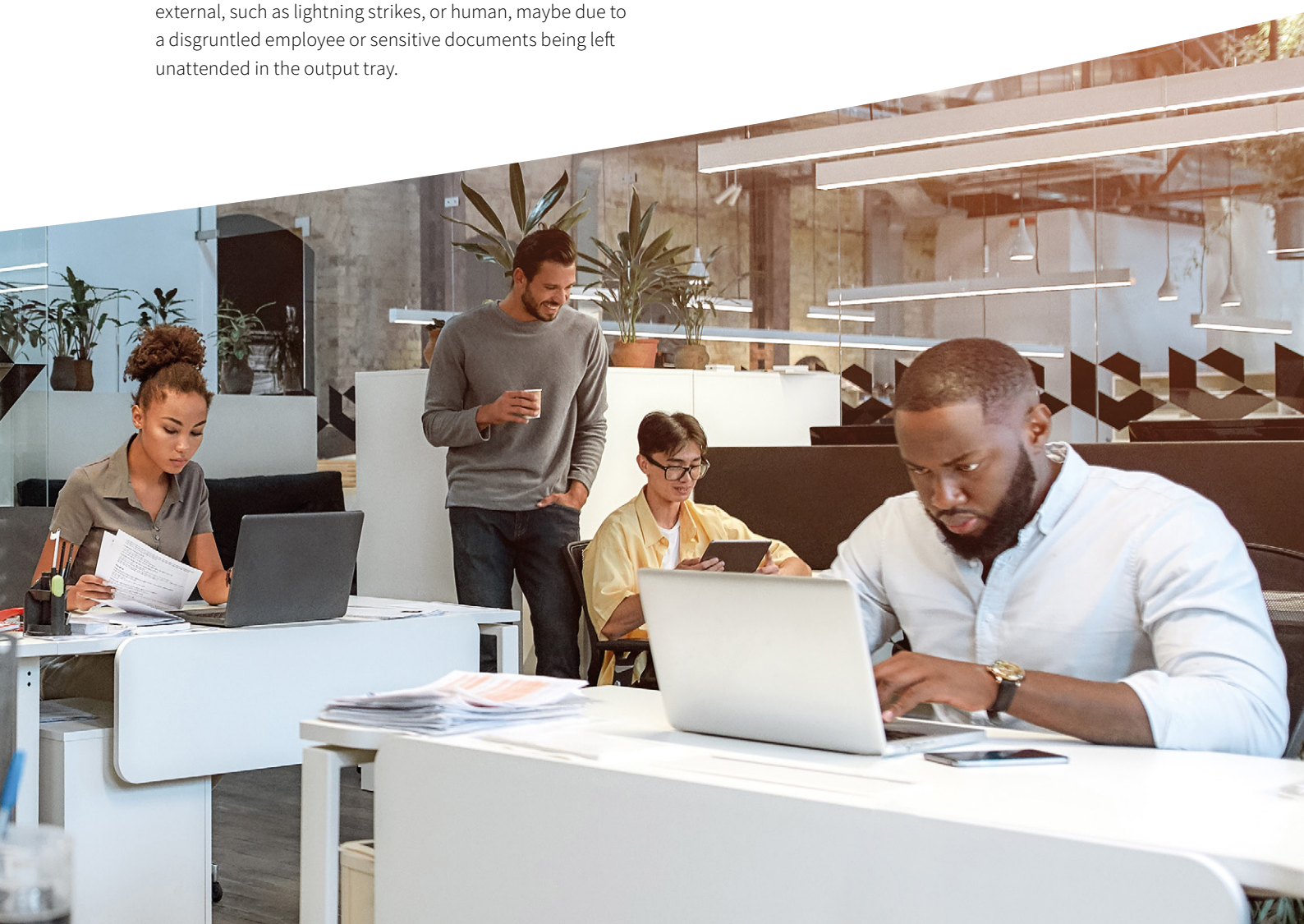


Understanding the risks

Modern businesses process a lot of information, but often don't have true visibility of how it is all produced, stored, shared and accessed. This inevitably leads to potential security and compliance risks, including data breaches, unsecured files, human errors and unauthorised access to information.

To be fully effective, your information security needs to protect your printers and business information from all forms of unauthorised access, use, disclosure, modification or destruction.

- **Physical threats** – any physical actions and events that could cause serious loss or damage of information or systems, whether internal, like an unstable power supply, external, such as lightning strikes, or human, maybe due to a disgruntled employee or sensitive documents being left unattended in the output tray.
- **Network threats** – any activity that enables unauthorised access to your network, usually to access or compromise data, such as viruses and malware, steal confidential information, like phishing campaigns, or prevent access to your systems through Denial-of-Service (DoS) attacks or ransomware.
- **Legal responsibilities** – the protection of any sensitive data that a business holds, wherever it is held, such as employee records, customer information and account data, as required by prevailing government or industry regulations, such as GDPR.



Keep safe and stay productive

In today's always-on, connected world, threats are becoming increasingly sophisticated. Print security should be too – without impacting productivity.

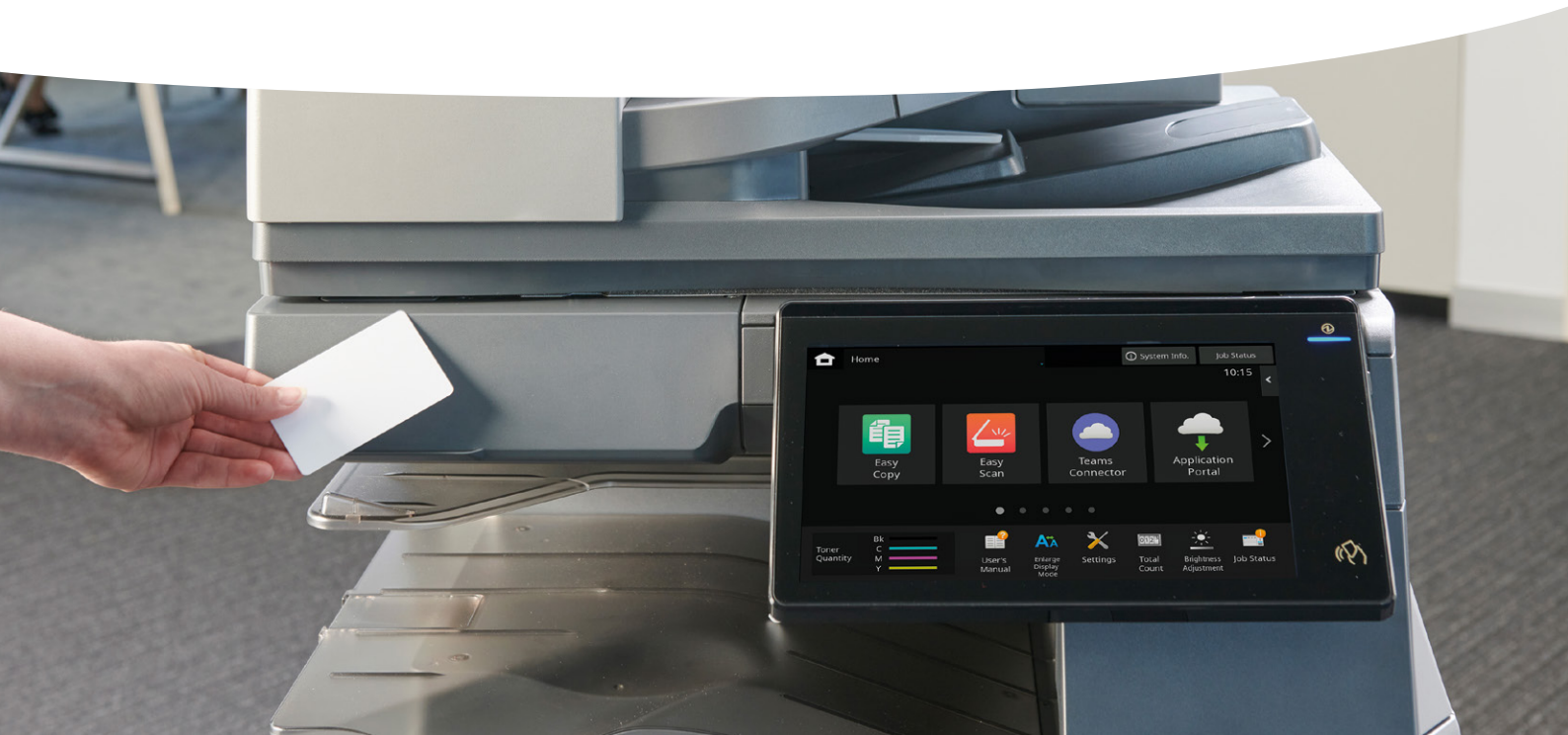
All the protection you need

Sharp recognises that protecting your business and user data is critical to your success – and survival. However, we also understand that if security measures are too stringent or implemented ineffectively, they can have a serious impact on productivity.

Our printers and MFPs include a suite of advanced Security Information and Event Management (SIEM) features designed to protect your information and document assets from a multitude of physical and cyber security threats, including the most sustained and determined attacks. They also help you comply with increasingly stringent legal and regulatory requirements, such as the General Data Protection Regulation (GDPR).

We will give you the tools to control and manage your print security policies and securely access your confidential information however it is being captured, stored, printed or shared over your network.

- **User Authentication** before you can use a device
- **Serverless Print Release** so users can securely print and release jobs from up to 5 other devices on the same network
- **Automatic Encryption** of any documents stored on or emailed from the device
- **Self-Healing Technology** to safely recover a device in the event of an attack
- **Flashing LED** to remind you to retrieve your documents after scanning
- **Whitelisting** of applications and firmware that can communicate with the device
- **SSL/TLS Certificate Validation** to check that third party servers communicating with your device are safe
- **Audit Trail** and job log features to provide comprehensive review of all user activity
- **Anti-malware monitoring**, using Bitdefender, to keep your data, device and network secure (optional).



Print security made simple

If you lack technical resources or simply want to focus on managing your business, Sharp can provide the security expertise you need to protect your business and unsuspecting staff from sophisticated cyber criminals.

Our Complete Print Security service is a fully managed service that provides the kind of proactive security monitoring that is normally only available in large corporates. However, it is delivered using an 'as a service' model for a simple monthly fee with no upfront costs.

We will monitor your Sharp MFP fleet 24/7 using an industry-leading SIEM system, so we can immediately identify any attempts at unauthorised access, system changes or other security events – and mitigate them.

- **Simple, centralised control**
  We will install and configure a security device that connects to cloud security service. It includes everything that is needed to manage the security and control the printing on your fleet of MFPs.

- **Active threat detection**
  We continually monitor your MFPs to ensure that they are running safely. Any deviations will prompt an automatic reset or a security alert that can be investigated by our security experts. We also deliver around-the-clock monitoring and threat analysis of the MFPs. It can rapidly identify suspicious activity or potential threats, so that they can be quickly addressed and mitigated.

- **Support where you need it**
  If any severe threats are identified, we can take the appropriate action to prohibit an attack or resolve the issue. For low-level security alerts, we will provide the remedy and any support you need, such as configuration amendments. You will also receive regular reports on the security alerts and remedial action taken.

All-round protection

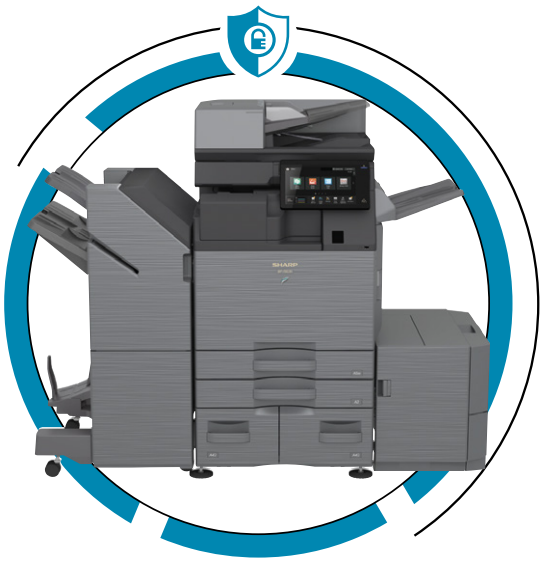
Your on-device security should provide a comprehensive defence against all key vulnerabilities and points of attack.

As PCs, laptops and servers are becoming increasing hardened against attack, other networked devices such as printers are being targeted by malicious actors in an increasingly diverse number of ways. Understanding this rapidly evolving threat landscape is essential to building effective defences.

Real-time Intrusion Detection
detects abnormal connection requests and denies access

BIOS Integrity Check at Startup
helps protect system files from malware attacks

Trusted Platform Module
provides an added layer of protection to safeguard data



Application Whitelisting
prevents unauthorised applications and firmware from being loaded

Active Directory Integration
can join network domain as a trusted device

Bitdefender Antivirus
provides comprehensive protection from malware attacks

Firmware Attack Prevention
checks for abnormal firmware and can restore original from backup

End-of-Lease Data Erase
can protect privacy by deleting all data and personal information at device end of life

	MX-M1xx6 MX-xx81/71S/61S/51 MX-Mxx71S/51 MX-C30xWH MX-Bx56W		BP-30Cxx BP-30Mxx		BP-90/70/60/50/55Cxx BP-70/50Mxx BP-B5xxWD/WR		MX-CxxxF/P MX-BxxxF/W/P/PW
	Standard Security Features	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**
Data Security							
Trusted Platform Module (TPM)	⊗	✓	⊗	✓	✓	✓	⊕
Data overwrite method (HDD)	✓ 0-FF Random Number DoD 5220.22-M	✓ 0-FF Random Number DoD 5220.22-M	⊗	⊗	⊗	⊗	✓ NIST DoD 5220.22-M
Data overwrite method (Flash, SSD)	⊗	⊗	✓ Trim command	✓ Trim command	✓ Trim command	✓ Trim command	✓ eMMC
Data overwrite after job completion	✓ Up to 10 times	✓ Up to 10 times	✓ Trim command	✓ Trim command	✓ Trim command	✓ Trim command	✓ Single or miltipass as defined by NIST
Data overwrite on demand	⊗	✓	⊗	✓ Trim command	⊗	✓ Trim command	✓
Clear all memory	⊗	✓	⊗	✓ Trim command	⊗	✓ Trim command	✓
Clear all data in job status jobs completed list	⊗	✓	⊗	✓ Trim command	⊗	✓ Trim command	✓
Clear document filing data	⊗	✓	⊗	✓ Trim command	⊗	✓ Trim command	✓
Clear address book/registered data	⊗	✓	⊗	✓ Trim command	⊗	✓ Trim command	✓
Auto data deletion after job	⊗	✓	✓	✓ Trim command	✓	✓ Trim command	✓
Auto clear at power on	⊗	✓	⊗	✓ Trim command	⊗	✓ Trim command	⊗
End-of-Lease (Clear all memory and a confirmation report)	✓ "0" value overwrite	✓ Random # overwrite	✓ Secure erase	✓ Secure erase	✓ Secure erase	✓ Secure erase	✓
Data encryption (AES 256 bit)	✓ ECB Mode	✓ CBC Mode	✓ ECB Mode	✓ CBC Mode	✓ CBC Mode	✓ CBC Mode	✓ ECB Mode
Encrypted PDF	✓	✓	✓	✓	✓	✓	✓
Clear document filing: (quick folder, batch print, store/backup document filing data)	✓	✓	✓	✓	✓	✓	✓
Timed deletion of document filing data	✓	✓	✓	✓	✓	✓	⊗
Operational lock for mis-entry of document filing password	⊗	✓	⊗	✓	⊗	✓	✓ User lockout
Application whitelisting	✓	✓	✓	✓	✓	✓	⊗
Firmware Attack Prevention & Self Recovery	✓	✓	✓	✓	✓	✓	⊗

✓ Standard ⊕ Optional ⊗ Not available

NOTE: Not all features and functions are available as standard on all products and may require optional upgrades. MX-C428P, MX-B468P, MX-C607P, MX-B557P and MX-B707P do not support MFP related security features for scan and fax. Please contact your local Sharp representative for details.

	MX-M1xx6 MX-xx81/71S/61S/51 MX-Mxx71S/51 MX-C30xWH MX-Bx56W		BP-30Cxx BP-30Mxx		BP-90/70/60/50/55Cxx BP-70/50Mxx BP-B5xxWD/WR		MX-CxxxF/P MX-BxxxF/W/P/PW
	Standard Security Features	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**
Network and Communication Security							
Network communication protection: HTTPS, IPsec & TLS	✓	✓	✓	✓	✓	✓	✓
Network communication protection: Wireless LAN	✓	✓	✓	✓	✓	✓	✓
Kerberos	✓	✓	✓	✓	✓	✓	✓
S/MIME encryption	✓	✓	✓	✓ Up to the setting	✓	✓ Up to the setting	⊕
IP address filtering	✓	✓	✓	✓	✓	✓	✓
Mac address filtering	✓	✓	✓	✓	✓	✓	⊗
Port management (enable and disable ports)	✓	✓	✓	✓	✓	✓	✓
SNMPv3 Support – SHA1, AES 128bit	✓	✓	✓	✓	✓	✓	✓
Pre-installed device certificates	✓	✓	✓	✓	✓	✓	✓
Cross-Site Request Forgery (CSRF) protection	✓	✓	✓	✓	✓	✓	⊗
Denial of Service (DoS)	⊗ ✓ MX-xx81 only	⊗ ✓ MX-xx81 only	⊗ ✓ BP-30Cxx only	⊗ ✓ BP-30Cxx only	✓	✓	⊗
IEEE802.1X™ authentication	✓	✓	✓	✓	✓	✓	✓
IPP over SSL	✓	✓	✓	✓	✓	✓	✓
Wireless LAN	✓	✓	✓	✓	✓	✓	✓
E-mail alert/status	✓	✓	✓	✓	✓	✓	✓
FSS	✓	✓	✓	✓	✓	✓	✓
Remote operation	✓	✓	✓	✓	✓	✓	✓
Public folder/NAS, cloud connect, job log/syslog/ audit log export, storage backup, device cloning	✓	✓	✓	✓	✓	✓	✓
Active Directory integration	✓	✓	✓	✓	✓	✓	✓
TLS encryption	✓	✓	✓	✓	✓	✓	✓
Security Policy management	✓	✓	✓	✓	✓	✓	✓

✓ Standard ⊕ Optional ⊗ Not available

NOTE: Not all features and functions are available as standard on all products and may require optional upgrades. MX-C428P, MX-B468P, MX-C607P, MX-B557P and MX-B707P do not support MFP related security features for scan and fax. Please contact your local Sharp representative for details.

	MX-M1xx6 MX-xx81/71S/61S/51 MX-Mxx71S/51 MX-C30xWH MX-Bx56W		BP-30Cxx BP-30Mxx		BP-90/70/60/50/55Cxx BP-70/50Mxx BP-B5xxWD/WR		MX-CxxxF/P MX-BxxxF/W/P/PW
	Standard Security Features	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**
Authentication and Access Control							
User authentication (Local/LDAP/Active Directory/Kerberos)	✓	✓	✓	✓	✓	✓	✓
ID card authentication	✓	✓	✓	✓	✓	✓	✓
NTLMv2 authentication on LDAP	✓	✓	✓	✓	✓	✓	✓
NTLMv2 authentication on SMB	✓	✓	✓	✓	✓	✓	✓
Print policy authentication	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration (MFP to join AD Domain)	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration Single-Sign-On (Folder, E-mail, Home Directory)	✓	✓	✓	✓	✓	✓	✓
Password protected admin access to device home page	✓	✓	✓	✓	✓	✓	✓
Password length and requirements	User 0-255 Admin 5-255	User/Admin N-255 (N: 5 to 32; Admin specifiable) Character: 52 letters, 10 numbers, 10 specified symbols	User 0-255 Admin 5-255	User/Admin N-255 (N: 5 to 32; Admin specifiable) Character: 52 letters, 10 numbers, 10 specified symbols	User 0-255 Admin 5-255	User/Admin N-255 (N: 5 to 32; Admin specifiable) Character: 52 letters, 10 numbers, 10 specified symbols	No specified condition but max length = 128, any special characters are accepted
Admin/user password policy	✗	✗	✗	✗	✓	✓	✓
Protection of admin password (when logged in via FTP)	✓	✓	✓	✓	✓	✓	✓
User lockout	✓	✓	✓	✓	✓	✓	✓
Print Security							
Printer job authentication	✓	✓	✓	✓	✓	✓	✓
PIN/password print release	✓	✓	✓	✓	✓	✓	✓
Server-less print release	✓	✓	✓	✓	✓	✓	✗
USB printing (when it is allowed)	✓	✓	✓	✓	✓	✓	✓
Disabling list print	✗	✓	✗	✓	✗	✓	✓
Disabling document filing	✗	✓	✗	✓	✗	✓	✗
Disabling print jobs other than print hold job	✓	✓	✓	✓	✓	✓	✓
Disabling job status jobs completed list display	✗	✓	✗	✓	✓	✓	✗
Printing of document control pattern	✗	✓	✗	✓	✗	✓	✗
Job stop when document control pattern is detected	✗	✓	✗	✓	✗	✓	✗
Print job force retention	✓	✓	✓	✓	✓	✓	✓

✓ Standard ⊕ Optional ✗ Not available

NOTE: Not all features and functions are available as standard on all products and may require optional upgrades. MX-C428P, MX-B468P, MX-C607P, MX-B557P and MX-B707P do not support MFP related security features for scan and fax. Please contact your local Sharp representative for details.

	MX-M1xx6 MX-xx81/71S/61S/51 MX-Mxx71S/51 MX-C30xWH MX-Bx56W		BP-30Cxx BP-30Mxx		BP-90/70/60/50/55Cxx BP-70/50Mxx BP-B5xxWD/WR		MX-CxxxF/P MX-BxxxF/W/P/PW
	Standard Security Features	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**
Scan Features and Sharp OSA® Applications							
Direct domain entry	✓	✓	✓	✓	✓	✓	✓
Sharp OSA: ACM & EAM External Application	✓	✓	✓	✓	✓	✓	✓ via eSF
Scan to shared folders	✓	✓	✓	✓	✓	✓	✓
Scan to USB	✓	✓	✓	✓	✓	✓	✓
Scan to email	✓	✓	✓	✓	✓	✓	✓
Scan to FTP	✓	✓	✓	✓	✓	✓	✓
Scan to email for destinations where S/MIME encryption is not available	✓	✓	✓	✓	✓	✓	✓
Scan to SMB	✓	✓	✓	✓	✓	✓	✓
Scan to USB storage	✓	✓	✓	✓	✓	✓	✓
Remote PC scan	✓	✓	✓	✓	✓	✓	✓
Sharpdesk Mobile	✓	✓	✓	✓	✓	✓	✓
Document Filing - Access to Quick Folder	✓	✓	✓	✓	✓	✓	✓
Document Filing - Data backup/export	✓	✓	✓	✓	✓	✓	✓
Mobile and Cloud Features							
Cloud Connect (Microsoft Teams, OneDrive, SharePoint Online, Google Drive™)	✓	✓	✓	✓	✓	✓	✓
Email Connect (Exchange Server, Gmail™)	✓	✓	✓	✓	✓	✓	✗
Mobile Printing (AirPrint, Android™)	✓	✓	✓	✓	✓	✓	✓ AirPrint only
Mobile Printing (Sharpdesk® Mobile, Sharp Print Service Plugin)	✓	✓	✓	✓	✓	✓	✗
Audit Trail and Other Security							
Job Log and Usage Tracking	✓	✓	✓	✓	✓	✓	✓
Admin Audit Tracking (SIEM and Syslog Integration)	✓	✓	✓	✓	✓	✓	✓
Digitally Signed Firmware	✓	✓	✓	✓	✓	✓	✓

✓ Standard ⊕ Optional ✗ Not available

NOTE: Not all features and functions are available as standard on all products and may require optional upgrades. MX-C428P, MX-B468P, MX-C607P, MX-B557P and MX-B707P do not support MFP related security features for scan and fax. Please contact your local Sharp representative for details.

	MX-M1xx6 MX-xx81/71S/61S/51 MX-Mxx71S/51 MX-C30xWH MX-Bx56W		BP-30Cxx BP-30Mxx		BP-90/70/60/50/55Cxx BP-70/50Mxx BP-B5xxWD/WR		MX-CxxxF/P MX-BxxxF/W/P/PW
	Standard Security Features	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**	**With Data Security Kit Installed**	**Standard Security Features**
Fax Security (Fax option may be required)							
Separation between fax and network	✓	✓	✓	✓	✓	✓	✓
Confidential fax	✓	✓	✓	✓	✓	✓	✗
Filter junk	✓	✓	✓	✓	✓	✓	✓
Data Security Kit (DSK) & Common Criteria Certification							
Common Criteria Certification	✗	✓	✗	✓	✗	✓	✗
Security Management							
Sharp Smart Security	✓	✓	✓	✓	✓	✓	✓
Device security monitoring via SRDM	✓	✓	✓	✓	✓	✓	✗
Complete Print Security Service	✓	✓	✓	✓	✓	✓	✓
Virus Detection powered by Bitdefender	✗	✗	✗	✗	⊕	⊕	✗

MFPs and Printers

MX-M1xx6 MX-xx81/71S/61S/51 MX-Mxx71S/51 MX-C30xWH MX-Bx56W	BP-30Cxx BP-30Mxx	BP-90/70/60/50/55Cxx BP-70/50Mxx BP-B5xxWD/WR	MX-CxxxF/P MX-BxxxF/W/P/PW
A3 MFPs MX-M1206, MX-M1056 MX-8081, MX-7081 MX-6071S, MX-5071S MX-4071S, MX-3571S, MX-3071S MX-4061S, MX-3561S, MX-3061S MX-6051, MX-5051 MX-4051, MX-3551, MX-3051, MX-2651 MX-M6071S, MX-M5071S MX-M4071S, MX-M3571S, MX-M3071S MX-M6051, MX-M5051 MX-M4051, MX-M3551, MX-M3051, MX-M2651 **A4 MFPs** MX-C304WH, MX-C303WH MX-B456W, MX-B356W	**A3 MFPs** BP-30C25 BP-30M35, BP-30M31, BP-30M28	**A3 MFPs** BP-90C80, BP-90C70 BP-70M90, BP-70M75 BP-70C65, BP-70C55 BP-70C45, BP-70C36, BP-70C31 BP-60C45, BP-60C36, BP-60C31 BP-50C65, BP-50C55 BP-50C45, BP-50C36, BP-50C31, BP-50C26 BP-55C26 BP-70M65, BP-70M55 BP-70M45, BP-70M36, BP-70M31 BP-50M65, BP-50M55 BP-50M45, BP-50M36, BP-50M31, BP-50M26 **A4 MFPs** BP-B547WD, BP-B537WR	**A4 MFPs** MX-C607F, MX-C557F MX-C528F, MX-C428F, MX-C507F, MX-C407F MX-C358F, MX-C357F MX-B707F, MX-B557F MX-B468F, MX-B467F, MX-B427W **A4 Printers** MX-C607P, MX-C507P, MX-C407P, MX-C428P MX-B707P, MX-B557P MX-B468P, MX-B467P, MX-B427PW

✓ Standard ⊕ Optional ✗ Not available

NOTE: Not all features and functions are available as standard on all products and may require optional upgrades. MX-C428P, MX-B468P, MX-C607P, MX-B557P and MX-B707P do not support MFP related security features for scan and fax. Please contact your local Sharp representative for details.

Glossary

Active Directory (AD)
A database and set of services that connect users with the network resources they need to get their work done. The database (or directory) contains critical information about your environment, including what users and computers there are and who is allowed to do what. In particular, they make sure each person is who they claim to be (authentication), usually by checking the user ID and password they enter, and allow them to access only the data they're allowed to use (authorisation).

BIOS
In computing, BIOS is firmware used to provide runtime services for operating systems and programs and to perform hardware initialisation during the booting process.

Bitdefender Antivirus
Bitdefender is an award-winning anti-malware engine that helps protect users against a full range of cyber threats. It complements native security features of the MFP, protecting it against known and unknown malware threats such as: Viruses, Trojans, Worms, Ransomware, Spyware and Persistent Threats.

Common Criteria
A set of guidelines used to evaluate information technology equipment. It is the technical basis for an international agreement and the specification is tested by independent laboratories. Meeting evolving security standards, such as Common Criteria, is important to ensure organisations confidently handle the most sensitive data on Sharp devices. Recently Sharp achieved the industry's first Common Criteria certification against the latest HCD-PP v1.0.

Data Security Kit (DSK)
The Sharp DSK brings device security to a higher level with features such as manual data overwrite, auto data overwrite at power-up, hidden pattern printing and detection, and more to help meet regulatory requirements or mitigate specific threats. In addition, selected DSK models are equipped with a TPM chip which helps further prevent unwanted access to data storage areas including Hard Disk Drive (HDD) and Solid-State Drive (SSD).

Denial of Service/Distributed Denial of Service (DoS/DDoS)
DoS is a type of disruptive attack where normal operation or service provided by a network or device is blocked or disrupted. DDoS is a type of DoS attack using multiple (numerous) attacking systems to amplify the amount of network traffic, thereby flooding and perhaps swamping the target systems or networks.

End-of-Lease
When a device is retired, it is important that the data retained within the device be removed or rendered in an unreadable format. Sharp devices offer standard End-of-Lease features to ensure that all confidential data is overwritten before the device leaves the facility or customer environment. Once executed the data is overwritten up to 10 times. If a DSK is installed or standard MFP security feature is enabled, the data is overwritten with random numbers.

IEEE802.1x
A network authentication protocol that opens ports for network access when an organisation authenticates a user's identity and authorises them to access the network. The user's identity is determined based on their credentials or certificate.

Internet Printing Protocol (IPP)
A network printing protocol capable of authentication and print job queue management. IPP is supported and enabled by default on most modern printers and MFPs.

Internet Protocol (IP) address
Every device connected to the internet must have a unique number (IP address) to connect with other devices. There are currently two versions of IP addressing: IPv4 and a later upgraded version called IPv6.

IP or MAC address filtering
IP and MAC addresses are unique numbers used to identify devices on the Internet (IP) or on a local network (MAC). Filtering ensures that IP and MAC addresses are checked against a 'whitelist' before devices can connect to your network.

Internet Protocol Security (IPSec)
A suite of protocols for securing IP communications at the network layer. IPsec also includes protocols for cryptographic key establishment.

Media Access Control (MAC) address
A MAC address of a device is a unique identifier assigned to a Network Interface Controller (NIC). This means that a network connected device can be uniquely identified by its MAC address.

Malware attack
Malicious software (malware) can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet.

Man-in-the-Middle (MITM) attack
An MITM attack is where the attacker secretly sits between two parties who believe they are connected directly and privately communicating with each other. The attacker eavesdrops and may also alter the communication between the parties.

Network services
Network services facilitate a network's operation. They are typically provided by a server (which can be running one or more services), based on network protocols. Some examples are Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Voice over Internet Protocol (VoIP).

Phishing attack
Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ports
Ports are used by networked devices (PCs, servers, printers etc.) for communication with each other (e.g. a workstation connecting to a printer). Unguarded open ports and services can be used as an attacker vector, for example, to upload malware.

Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)

HCD-PP v1.0 (dated September 10, 2015) is the latest requirement for MFPs based on the security requirements specified by the U.S. and Japanese governments, providing the most up-to-date security validation for businesses, government and military offices. It aims to protect the information processed by an MFP from security threats and includes specifications for encryption and firewalls.

Protocols

A protocol is defined as a set of rules and formats, permitting information systems to exchange information. In a network context, for example, IP and TLS/SSL are protocols.

Single Sign-On (SSO)

Selected Sharp MFPs offer options for single sign-on to add operational convenience while validating user access to the device and network. When an MFP joins a domain, the MFP establishes trusted relationships with network resources. IT administrators can provide secure Kerberos token-based SSO to network and home folders as well as Microsoft® exchange server. For Google Drive™ online storage service, Gmail™ webmail service and selected cloud services, an OAuth token is used to establish SSO.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

A set of specifications for securing email. S/MIME is based upon the widely used MIME standard and describes a protocol for adding security through digital signatures and encryption.

Spoofing attack

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls.

Transport Layer Security/Secure Sockets Layer (TLS/SSL)

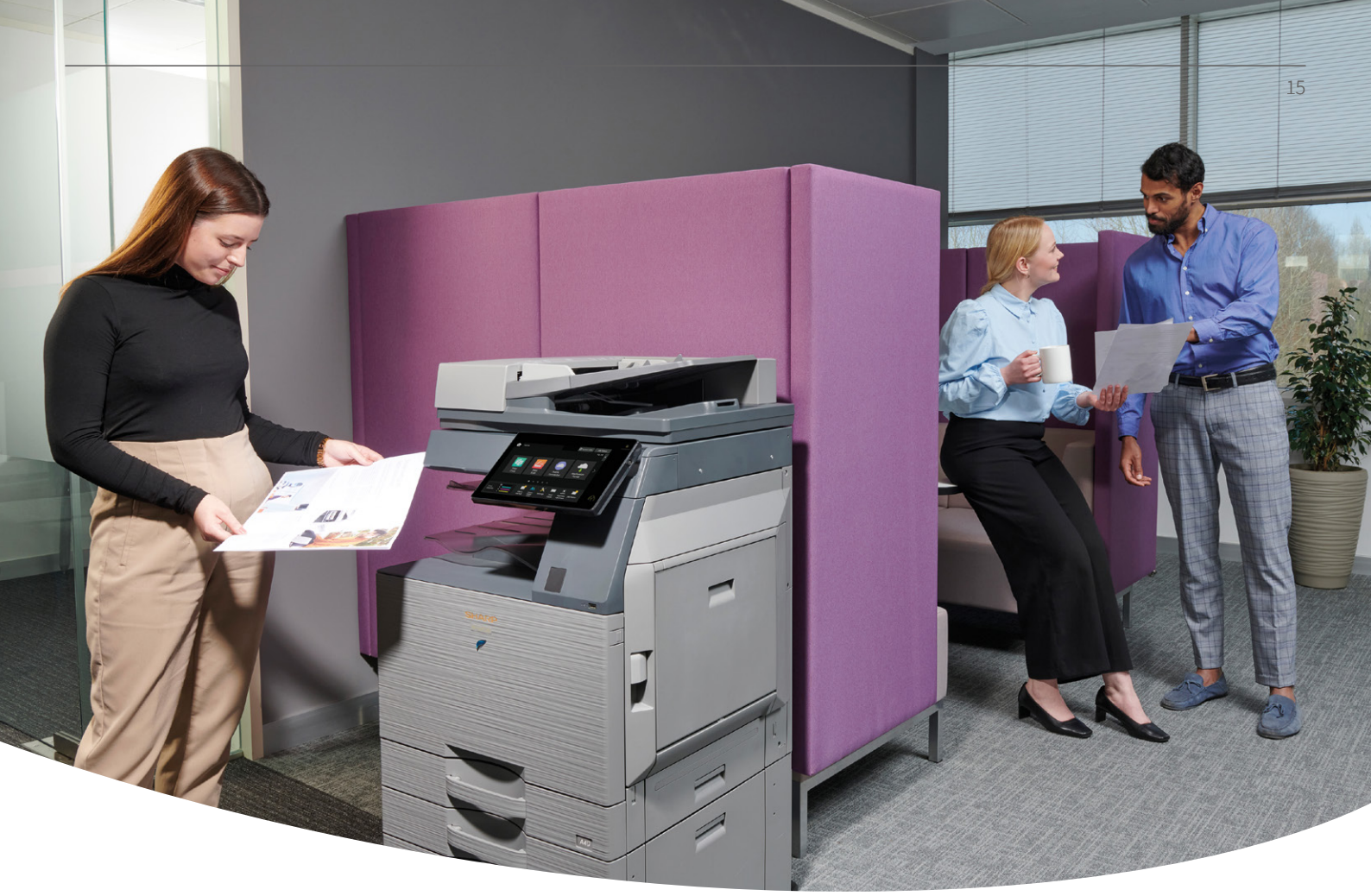
A type of technology that encrypts data when it is being transported or transferred between one device and another to prevent eavesdropping. TLS/SSL is common for websites but can also be used to protect other services.

Trusted Platform Module (TPM)

An industry standard computer chip that uses cryptoprocessor technology to protect hardware such as hard disk drives and solid-state drives inside MFPs and printers. When a Sharp MFP is installed with a data security kit or TPM, the TPM chip initiates a cryptographic key that cannot be accessed by software. A matching cryptographic key is encoded during the boot-up process. If the two keys do not match, access to the device is denied.

Whitelist

A whitelist is an exclusive list of people, entities, applications or processes that are given special permissions or rights of access. In a business sense, this could be for example the staff of an organisation and their rights to access the building, the network and their computers. In a network or computer sense, a whitelist may define applications and processes that have the rights to access data storage in secure areas.



Getting smart about security

Every business is unique and faces unique challenges. So, your security systems should be just as unique.

Instantly effective protection

Securing the print infrastructure – across the office environment – is now a strategic priority, but we also understand that easy access to printing is essential to business productivity.

That is why Sharp has introduced Smart Security Service – an innovative security 'as a service' offering. It is a bespoke profiling service that is designed to ensure that your Sharp MFPs are delivered secure 'out of the box', with advanced security features that are carefully tailored to your needs, so they don't impact your business agility or productivity.

Initially, we will walk you through current and potential data threats to MFPs, so that we can define a suitable print security policy for you. Our security experts can then develop a unique security configuration for your MFPs to match your organisation's exact requirements by activating any number of over 200 security settings.

It ensures that we provide the best possible level of print security without limiting the flexibility you and your employees require. It also means that we can pre-configure, deliver, install and integrate your new MFPs as simply and securely as possible. So, from the very first printed sheet, you can be sure that your devices and information are always as secure as possible.

Welcome to Sharp

Sharp Europe enables small to large enterprises and organisations across Europe to enhance performance and adapt for their workplaces of the future through a range of business technology products and services.

Sharp services and products range from printers and advanced flat screen technologies, collaboration platforms in partnership with other leading brands, through to full IT services for small companies to large enterprises and organisations.

As a manufacturer and a service provider, Sharp is uniquely positioned to provide trusted advice and assurance to customers on how technology can work together seamlessly.