KYOCERA
Document Solutions

MFP SECURITY GUIDE

MFP SECURITY GUIDE

INTRODUCTION

Print devices have come a long way from the standalone hardware of old to today's fully-networked multi-function printers (MFP) running sophisticated operating systems. And yet, with IT professionals focused on the challenges of protecting core infrastructure like servers, databases and desktops from the ravages of malware and hacking exploits, MFPs have become a cyber security blindspot within many organisations.

This represents significant risk, particularly in the light of increased cybercriminal activity directly targeting networked devices as a weak link in the defence against corporate data theft and malicious attack. With regulation such as GDPR threatening ruinous financial and legal consequences for non-compliance, organisations must take immediate action to incorporate MFPs into data protection strategy.

This KYOCERA paper offers practical guidance for IT professionals to harness the in-built security features of leading MFPs and adopt further, enhanced data protection capabilities. These basic, medium-level and high-level measures combine to make it as difficult as possible both to gain unauthorised access to corporate networks via the MFP route, and undertake cybercriminal activity should they make it inside.

HOW SECURE IS MY DEVICE?

All KYOCERA MFPs/printers are embedded with an Operating System (OS) as standard. Like a Personal Computer, the device can contain a Hard Disk Drive (HDD) or Solid State Drive (SSD) which can store potentially sensitive information. MFPs can be exposed to advanced and diversified threats, such as unauthorised access to the devices via the network, alteration of information in transit over the network and leakage of data from the device's HDD.

KYOCERA devices provide the customer with a variety of security functions. This document is designed to provide guidance on securing a device in the workplace and is split into three areas:

1) **Basic Configuration:** Deals with securing the device using features and functions available as standard.

2) **Medium-Level Configuration:** Addresses some of the optional features that can enhance data security and further secure the machine.

3) **High-Level Security:** Introduces further ways to secure the device at a network level using extra hardware such as firewalls.

BASIC LEVEL SECURITY CONFIGURATION

The capabilities in this section are the simplest and quickest to initiate, and they address security vulnerabilities at their most fundamental level. KYOCERA recommends all should be engaged or actively considered by every organisation running MFPs. Further security measures should be employed in addition to these, rather than instead.

RECOMMENDATIONS

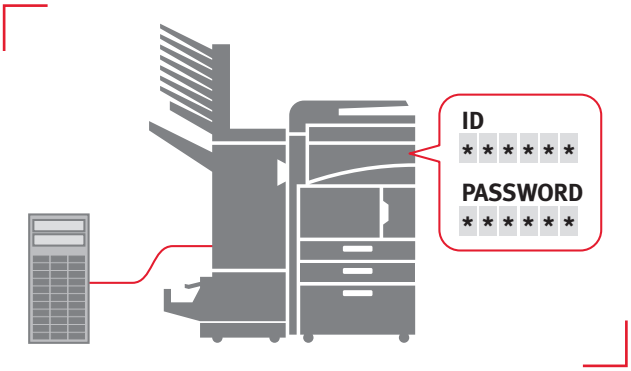
- Change the default Administrator password.
- Use an Authentication method
- Turn off protocols that are not required/lock specific communication ports
- Use secure communication protocols
- Operation panel lock
- Disable USB port functions and optional interfaces
- Email/scan/send restrictions

Change the default Administrator password

Devices are supplied from the factory with a default password. It is highly recommended that this be changed. Pick a suitably strong password that complies with local policy and do not use an existing computer account username/password. Note: If an MFP password is forgotten then the device will require a factory-reset to be performed by a KYOCERA technician.

Use an Authentication method

KYOCERA devices support a number of different ways to enable user logon. Access is in three levels - User, Administrator, and Machine Administrator. The security levels can be modified only by the Machine Administrator. Users that are not able to login to the machine can be allowed to use the functions of the machine on a restricted basis.



Local Authentication: Authenticates users based on the user data registered on the local user list on the MFP/printer. Only registered users can access the device.

Network Authentication: Authentication via a Domain controller. NTLM and Kerberos methods are supported. A password policy can be enabled enforcing password complexity and password age, together with logging of failed attempts.

Guest Function: When User Login Administration is enabled, a guest mode can be set so that only certain functions of the machine can be accessed without requiring authentication. This can also be used to reduce operating costs, for example by prohibiting colour copy in Guest Mode so that only users who login can use colour copying. This level of security can protect the device against information leakage whilst still maintaining user friendliness.

Using a network authentication protocol is an effective method of achieving authentication for secure communication. KYOCERA MFPs/printers support IEEE802.1x network authentication, SMTP authentication and POP before SMTP authentication protocol when using 'send to email' functionality **(see Appendix A – Authentication Protocols).**

Turn off protocols that are not required/lock specific communication ports

Network Security Level: KYOCERA MFPs/printers can limit communications on a network to receive/transmit on a set range of IP addresses and port numbers.

IP Address Filter: This restricts network access to the MFPs/printers by setting ranges of IP addresses or types of protocols. **(see Appendix B – Ports and Protocols).**

Use secure communication protocols

Secure communication protocols ensure secure protection of the network communication channel. Depending on purposes or encryption schemes, there are a variety of protocols is available, thereby effectively protecting data against alterations or leakage via the Network. **(See Appendix C – Secure Communication Protocols).**

Operation panel lock

Partial Lock function allows certain functions to be disabled and has three levels: Operation panel use, job management/execution and paper settings. The operation panel lock has the ability to lock out access to the system settings and job cancellation settings.

Disable USB port functions and optional interfaces

If a USB memory device is connected to a MFP through one of the USB hosts on the device, there is a risk of data loss or unauthorised access to data held on the device. The Administrator can disable the USB Storage Class feature which disables storage devices but allows connection of other USB devices such as card readers, keyboards, etc. The administrator can also disable the Optional Interfaces (Slots 1 & 2) to prevent fitting of unauthorised interfaces.

Email/scan/send restrictions

Email send destinations can be restricted using the Email Send Restriction function for permission or rejection. Permitted send destination addresses are registered in advance so emails can only be sent to the permitted registered destination addresses. Rejected send destination addresses can also be registered in advance so that emails to that destination would be rejected.

KYOCERA MFPs/printers have a function to print files attached to emails. Email reception can be restricted through the email sender restriction function based on pre-registration. Permitted sender addresses are registered in advance so that emails can only be received from the permitted sender. Rejected sender addresses are also registered in advance so that incoming emails from the rejected sender addresses would also be rejected.

PDF Password and Encryption: The Encrypted PDF function enables users to choose PDF file or high-compressed PDF for the file format, and securely protects the scanned data by encrypting and setting password. Restriction can be applied when opening, printing, or modifying the received PDF file by entering the correct password.

MEDIUM-LEVEL SECURITY CONFIGURATION

The measures detailed in this section should be used to complement those already executed in the Basic list. These are available as modules for all KYOCERA MFPs.

RECOMMENDATIONS

- Enable HDD/SSD data protection
- Implement ID Card/RFID Access
- Protect Job Storage
- Use Secure Print
- Enable Copy Protection

HDD/SSD Data Protection

Sensitive or confidential information can be stored on the device's HDD or SSD and extra protection can be implemented which conforms to the Common Criteria Certification (ISO 15408). These functions include:

HDD/SSD ENCRYPTION

HDD/SSD encryption function is a security function that encrypts documents, user settings and device information stored on the HDD or SSD. Encryption is applied to the data using the 128-bit and 256-bit AES (Advanced Encryption Standard: FIPS PUB 197) algorithms. If the HDD or SSD is removed from the MFP, the sensitive or confidential information stored in the HDD or SSD would not be accessible.

HDD OVERWRITE-ERASE

HDD Overwrite-Erase is a security function that disables a third party's ability to read a variety of data such as user settings, device information and image data stored on the HDD.

When printing or copying, scanned data is temporarily stored in the HDD and then output. Users also register various settings such as scan destinations and email addresses which are stored on the device. This information remains on the HDD until the data is overwritten with other data, even after the output or deletion of the data by users. There is a possibility that the data remaining on the HDD can be restored using special tools and utilities, leading to leakage of information.

The HDD Overwrite-Erase function is configured to overwrite the actual data area of the output or deleted data with random meaningless data so that the actual data cannot be restored. The overwrite-erase process is performed automatically so no manual operation is required from the user. HDD data is immediately overwritten even when respective jobs are cancelled during operation or directly after an entire job has finished.

Three overwrite-erase methods are available and subject to MFP model.

ONE-TIME OVERWRITE-ERASE

Unnecessary data area is overwritten once with null data, making the data difficult to restore or recover.

THREE-TIME OVERWRITE-ERASE

Unwanted data area is overwritten twice with random data, and then once with null data. The three-time overwrite-erase function removes the ability to restore the data even if using highly skilful restoration techniques. The three-time overwrite-erase method is more rigorous compared to the one-time overwrite erase method. In case of overwrite-erasing bulk data, the three-time overwrite-erase method may take longer.

THE U.S. DEPARTMENT OF DEFENCE DOD 5220.22-M (THREE PASSES)

The DoD 5220.22-M three-pass is the highest level security mode, compared to "One-time Overwrite-Erase" and "Three-time Overwrite-Erase". It significantly reduces the risk of information leakage.

ID Card / RFID Access

If proximity ID media is used as access control to the building or for time management, the same ID media can be used to give controlled access to output devices like printers and MFPs. This is both convenient and offers improved efficiency.

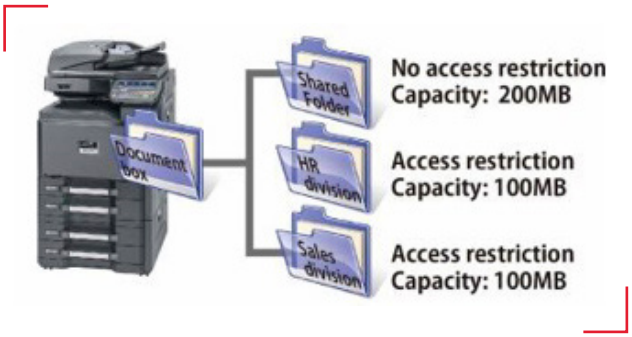
Combining this with the Job Storage function available on the MFP allows jobs to be retrieved from the device with access restrictions in place.

Job Storage

User Boxes, Job Boxes and Fax Boxes that store received and printed data can be created on the MFPs. Access to the data saved in these boxes can be restricted.

USER BOX

Users can create User Boxes to store data on the MFPs. Box usage restrictions, data retention periods and passwords can be set for the respective boxes.



A User Box can only be accessed by a user who has been registered as an owner for their User Box, and cannot be accessed by an unauthorised user. A Shared Box can be created allowing users who are not registered as owners can access to the box.

After a period of time set by the administrator, the stored document data can be automatically erased enabling effective HDD self-management and data security.

JOB BOX

Data for Private Print, Quick Copy, Proof and Hold and Stored Job can be stored in a Job Box, which cannot be created or deleted by users. The box can be PIN code-protected controlling access to the data. The stored document data can be automatically erased after a set period of time enabling effective HDD self-management and data security.

FAX BOX

This box receives Fax data. The fax data can be stored in the Fax Box using a memory forward function and data will be assigned to the respective boxes based on sender sub-addresses or fax numbers. The fax-received data can be previewed on the panel of the MFP so wanted faxes can be printed right away, whereas unwanted faxes can be deleted.

Secure Print

Secure Print is a print function for MFPs/printers and can be used for printing company confidential or personal documents without the risk of leaving unattended printed documents at the device.

PRIVATE PRINT

Private print is a function that holds a print job sent from a user workstation on the MFP/printer until the appropriate password is entered through the operation panel of the device. This feature requires the user to set an access code in the printer driver when sending a print job from the workstation and entering it again at the device of when printing a document. After printing is finished the data is erased. If the main power switch is turned off before retrieving/printing the document, the data will still be erased.

Copy Protection

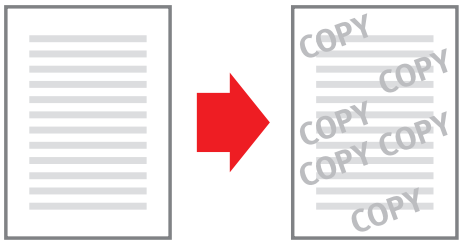
When copying, the following functions can prevent unauthorised copies by enhancing document security capabilities.

TEXT STAMP/BATES STAMP

Users can choose document stamps such as “Confidential”, “Do Not Duplicate” and “Privacy”, depending on the type of document they are printing. These are overlaid on the printed document and users can edit the text stamp if required. The Bates Stamp function “Serial Number” will print the serial number of the machine used for the print-out and a numbering function which will print page numbers in sequence onto the printed documents. In addition, the function “Date” and “User Name” are also available.

SECURITY WATERMARK

The printed document can be embedded with a security watermark pattern or text. When printed material embedded with the pattern is copied, the security watermark pattern will become visible. This clearly indicates that an unauthorised copy was made.



DOCUMENT GUARD KIT

The Document Guard Kit offers an optional function that embeds a security pattern in a document material. When users try to copy, scan or fax the document embedded with the special guard pattern, the device ceases operation and prohibits unauthorised copying. This prevents the leakage of valuable information. If the Document Guard Kit is not installed on the device, the security watermark pattern will appear, warning users that it is an unauthorised copy.

HIGH-LEVEL SECURITY CONFIGURATION

This final group provides guidance on the kinds of advanced MFP-related security capabilities that are possible when using complementary solutions. This should be considered as supplementary to the foundation measures detailed at Basic and Medium Level.

Print Control solutions

There are many different types of print control systems available, offering cost savings and control. However they also share the ability to provide security for information in transit across the network.

The basic premise of print control solutions is that the user prints a job to a shared 'virtual' queue hosted on a central print server. The job is held on that server until the user authenticates with a device and selects the job(s) to be printed. The print job is then sent to the device and output. Audit information is then recorded at the server for reporting purposes.

This method offers a number of advantages:

- Jobs are delivered while the user is present at the device
- No information is held on the device
- Restrictions on user rights can be made
- Print costs are reduced
- It delivers enhanced device security

RECOMMENDATIONS

- Enforce Print Control solutions
- Implement VPN connections
- Enable network data monitoring

CENTRALISED PRINT SERVERS/PRIVATE CLOUD PRINTING

In recent times, some print control systems have evolved further to address issues of bandwidth utilisation and document security when printing to offsite or cloud-based servers.

A process of 'Local Print Spooling' can be employed using either the user's PC or a designated MFP on the local network to hold the print job, with only audit and print policy information being sent to the server. When a user authenticates on a MFP, the held print job is then sent, printing on the selected device. This method dramatically reduces bandwidth utilisation, and keeps documents within the local network boundary. The addition of an onsite secondary server can also be utilised which manages devices, users and audit information which can be synchronised with a central master server.

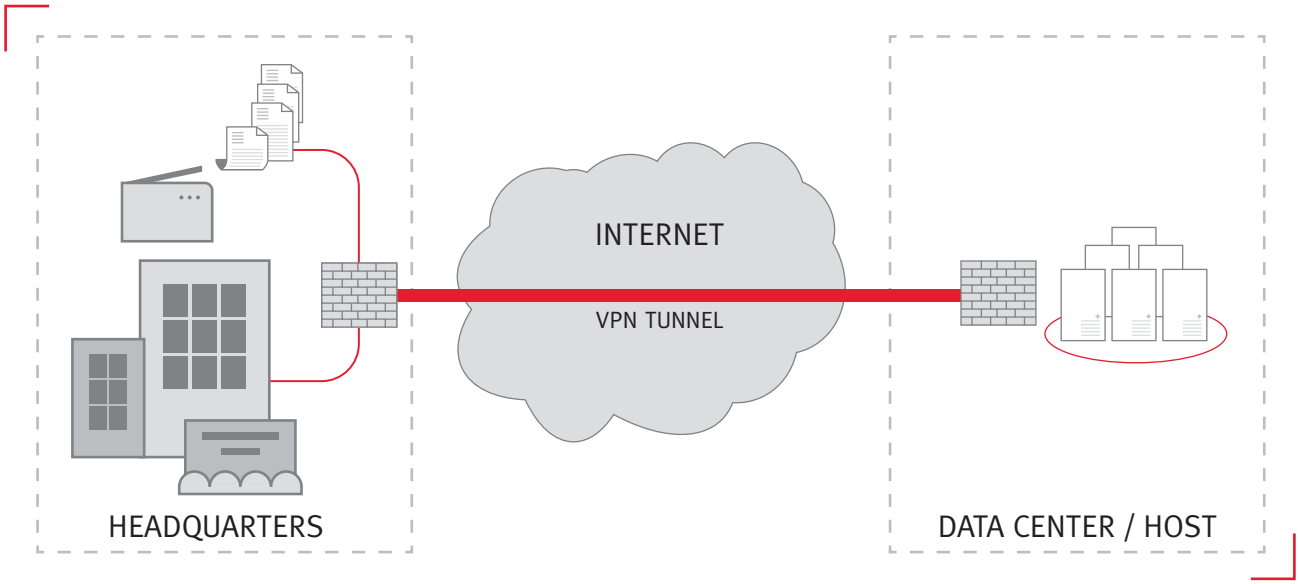
The latest applications can also control access to scanning, limit destinations and control settings with access permissions based on global, group or individuals.

KYOCERA can assist in the selection of the best solutions for an organisation's requirement. Please contact your local office for more information.

VPN (Virtual Private Network) connections

A Virtual Private Network (VPN) is a highly secure method of connecting an office network infrastructure across a public network. All data travelling over these connections is encrypted to a high degree allowing the use of the internet to host the connection.

VPNs require specialised equipment and require set-up by a suitably qualified person to create the VPN 'tunnel'. There are two types of VPN in use; Site to Site and Client Based Connection, the latter being used as an 'ad-hoc' connection method by individual clients via a mobile device whereas Site to Site is typically employed to connect office infrastructures.



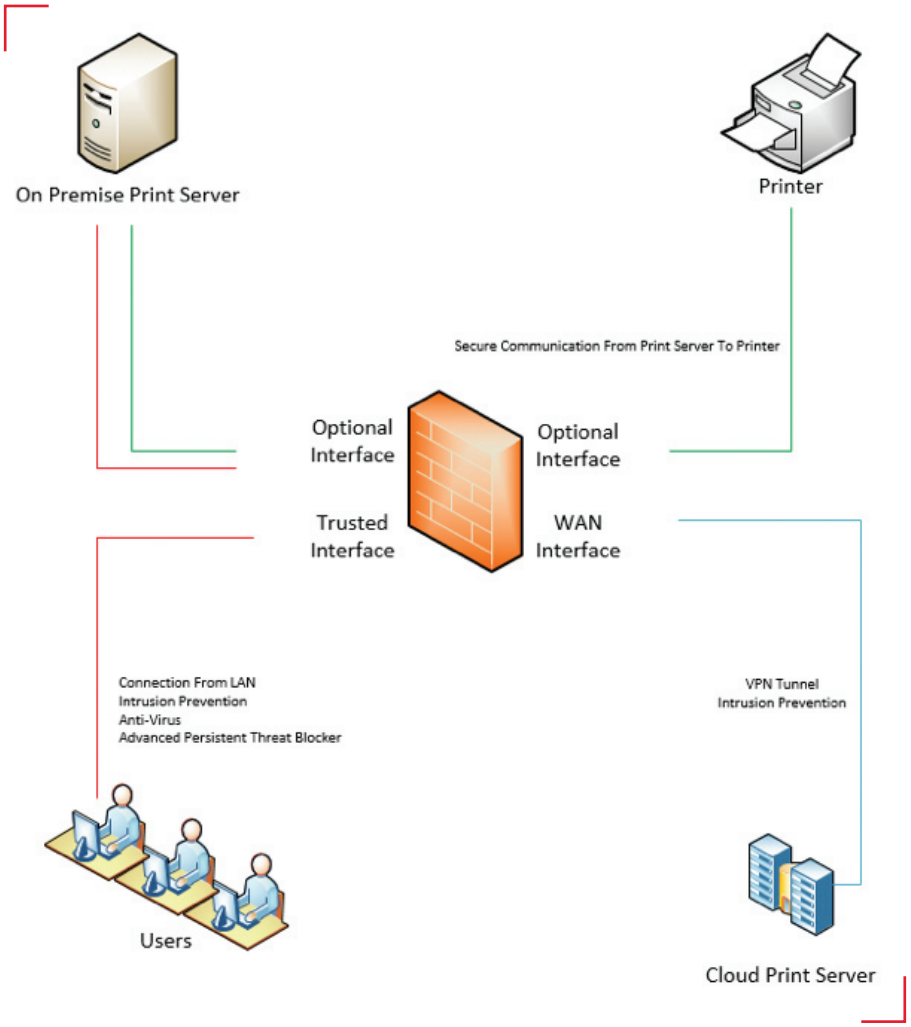
NETWORK DATA MONITORING

A perceived or potential threat to MFPs on the network is inevitable due to the devices running advanced operating systems. These make the devices a potential target for theft of both data and user/network credentials for cybercriminals to gain deep, persistent presence on the network.

Using network monitoring devices like the WatchGuard T10 within the network, and connecting the devices on a separate sub-net, allows the unit to act as a gateway for incoming and outbound traffic to the MFP fleet. This also supports the monitoring of data packets for suspected threats.

Malware is eclipsing traditional viruses as the most prevalent threat on the internet. New strains of advanced malware are often referred to as Advanced Persistent Threats (APTs).

The WatchGuard appliance receives updates and definitions from a cloud-based repository and if it detects malware, these can immediately be blocked at the firewall. In some cases, a true zero-day threat may pass through while analysis takes place in the cloud. In such cases, the WatchGuard system can provide immediate alerts that a suspect piece of code is on the network so that the organisation's IT department can follow it up immediately.

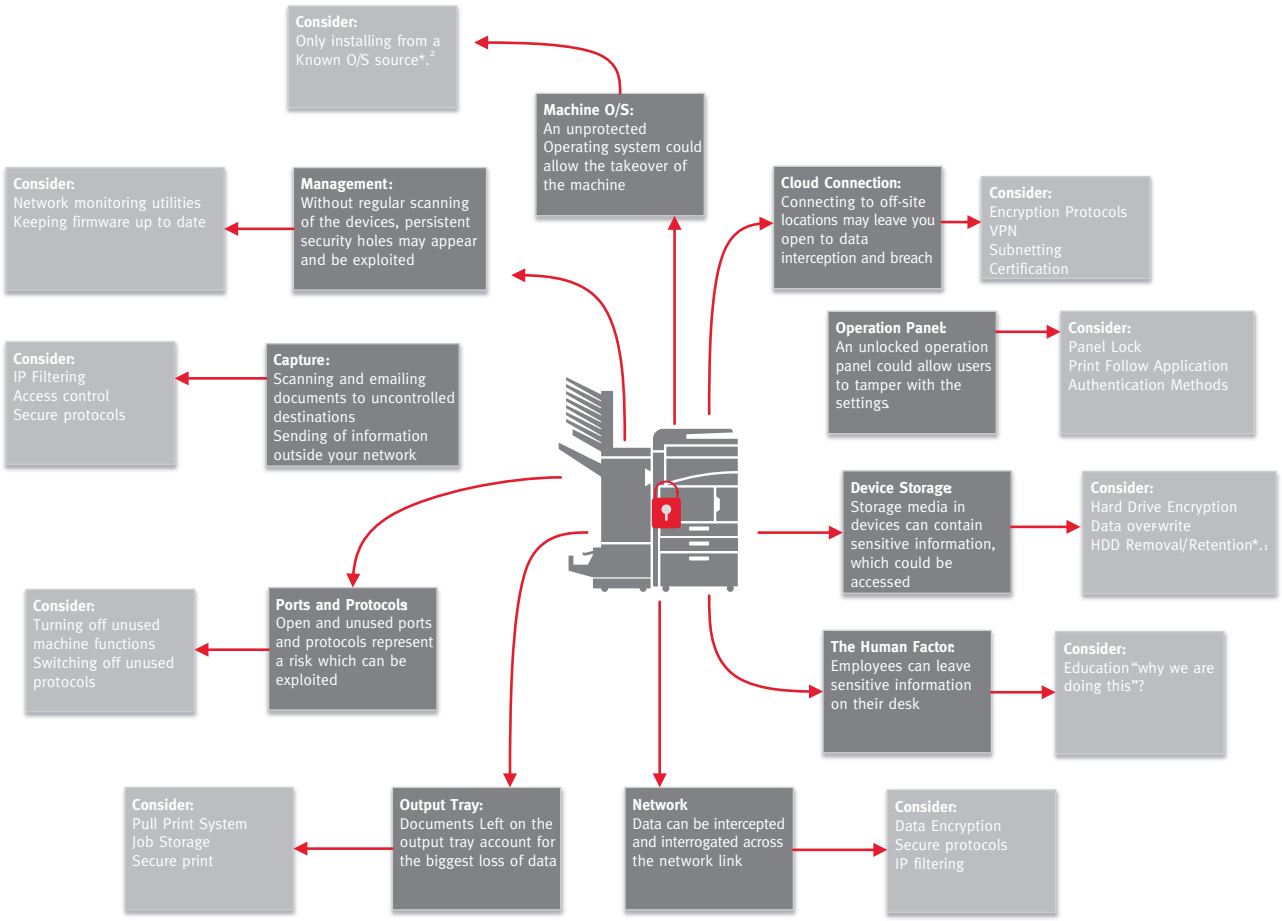


CONCLUSION

IT professionals must consider MFPs as part of a strategic approach to network and data security. Beginning with the simplest steps outlined in this paper, and progressing to more enhanced measures as required, organisations can equip themselves to safeguard sensitive data from cybercriminals and other malicious parties.

Moreover, in the context of increasing industry debate around securing the 'Internet of Things' and addressing emerging data protection compliance such as GDPR, IT professionals must use the first available opportunity to convert MFPs from a security blindspot to a visible component of their networked IT estates.

The measures required are comparatively simple and low-cost, but the consequences of overlooking them could prove dire.



APPENDIX A

Authentication Protocols

IEEE802.1x
This protocol allows communications only to authorised users (and authenticated devices) when connecting to the network, and prevents unauthorised devices from connecting to the network. KYOCERA devices support the IEEE802.1x which does not allow unauthorised access by unauthenticated clients to the network, preventing unauthorised disclosure of information. The KYOCERA MFPs/printers employ six types of authentication modes as described below.

PEAP-TLS/PEAP (Protected Extensible Authentication Protocol-Transport Layer Security)
The client is authenticated based on the ID and certificate and the certificate of authentication server is checked at the same time.

EAP-PEAP (Extensible Authentication Protocol-Protocol Extensible Authentication Protocol)
The client is authenticated based on the ID/password and only the common name of the authentication server certificate is checked.

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling)
EAP-FAST is an IEEE802.1.x/EAP authentication method developed by Cisco Systems, Inc. Mutual authentication is performed for the client and authentication server based on the user ID and password and PAC (Protected Access Credential) establishes a tunnel for the user based on the unique shared secret key.

EAP-TTLS (Extensible Authentication Protocol-Tunnelled Transport Layer Security)
The client is authenticated based on the user ID and password, and the authentication server is authenticated based on the electronic certificate.

Using EAP-TTLS, client and server electronic certificates are required for authentication, whereas for EAP-TTLS, the user ID and password are used instead of a client certificate. This makes EAP-TTLS easier to introduce compared to EAP-TLS. Electronic certificates are used to prove the validity of authentication server. Therefore, it helps improve more secure and trusted communications.

SMTP Authentication
SMTP authentication is a function that permits to send an email only when the ID and password are successfully authenticated on an SMTP server. The function prevents unauthorised users from sending emails through the SMTP server by limiting access to the SMTP server.

POP before SMTP
POP before SMTP performs POP authentication before sending emails from the SMTP server. The emails can be sent within the specified period after completion of POP authentication. POP authentication before sending an email prevents masquerading.

APPENDIX B

Ports and Protocols

Protocol	Port No.	Setting	Note
FTP Server	TCP 21	Enable/Disable	FTP server is a protocol for receiving a document
HTTP	TCP 80	Enable/Disable	HTTP is a protocol that is used when receiving/sending data from a web page between www server and browser.
NetBEUI	TCP 139	Enable/Disable	NetBEUI is a protocol for a small network that is used for file sharing and print services, as well as for receiving a document.
HTTPS	TCP 443	Enable/Disable	HTTPS is a protocol that performs encryption using SSL/TLS.
IPP over SSL/TLS	TCP 443	Enable/Disable	IPP over SSL/TLS is a protocol that combines SSL/TLS which encrypts a channel, and IPP which is used for internet printing. In addition, the IPP over SSL/TLS can have a valid certificate.
LPD	TCP 515	Enable/Disable	LPD is a printing protocol that is used for printing text files or Postscript.
IPP	TCP 631	Enable/Disable	IPP is a protocol that controls to send/receive print data via TCP/IP including internet, or print devices.
ThinPrint	TCP 4000	Enable/Disable	ThinPrint is a print technology available in Thin client environment, and also supports SSL/TLS.
WSD Scan	TCP 5358	Enable/Disable	Windows Vista WSD is a protocol that enables a MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier. Original documentation image scanned through MFP/Printer can be stored in WSD PC as a file.
WSD Print	TCP 5358	Enable/Disable	Windows Vista WSD is a protocol that enables MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier.
Enhanced WSD	TCP 9090	Enable/Disable	Enhanced WSD takes a procedure for easily connecting the various devices connected to a network, and using. The status of MFP/Printer can be monitored by the status monitor through this port 9090.
Enhanced WSD over SSL/TLS	TCP 9091	Enable/Disable	Enhanced WSD (SSL/TLS) is a security protocol as well as an enhanced WSD with using SSL/TLS. This provides encryption, authentication and safety (Protect against alteration).
RAW	TCP 9100 - 9103	Enable/Disable	RAW protocol takes different steps, compared to LPR for printing. In general, MFP/Printer uses port number 9100, and also uses SNMP or MIB to configure and monitor printer status.
SNMPv1/v2	UDP 161	Enable/Disable	SNMP protocol is used in network management systems. Normal communication will be performed using read and write community names.
SNMPv3	UDP 161	Enable/Disable	SNMP protocol is used in network management systems. Normal communication will be performed using user name and password. Authentication option or encryption option can be used.

DSM Scan		Enable/Disable	DSM (Distributed Scan Management) uses Windows Server 2008 R2 which is used for handling a large amounts of user data in a large organisation.
FTP Client		Enable/Disable	FTP client is a communication protocol for forwarding a file via a network.
LDAP		Enable/Disable	Address Book on LDAP server is referred as an external address book. Fax number and mail address can be designated as destination.
POP3		Enable/Disable	POP3 is a standard protocol for receiving emails.
POP3 over SSL/TLS		Enable/Disable	POP3 over SSL/TLS is a protocol that combines POP3 which is used for receiving an email, and SSL/TLS which is used for encrypting a channel.
SMTP		Enable/Disable	SMTP is a protocol for sending emails
SMTP over SSL/TLS		Enable/Disable	SMTP over SSL/TLS is a protocol that combines SMTP which is used for sending an email, and SSL/TLS which is used for encrypting a channel.
SMB Client		Enable/Disable	SMB is a protocol that performs file or printer sharing through a network.
eSCL		Enable/Disable	eSCL is a protocol that is used for remote scan from Mac OS X.
eSCL over SSL/TLS		Enable/Disable	eSCL over SSL is eSCL communication protocol using SSL certificate. All eSCL over SSL communications are encrypted.
LLTD		Enable/Disable	LLTD is a protocol for network topology discovery and quality of service diagnostics.
REST		Enable/Disable	REST is the software architecture of the web application that supports multiple software in a distributed hypermedia system.
REST over SSL/TLS		Enable/Disable	REST over SSL is a REST communication protocol using SSL certificates. All REST over SSL communications are encrypted.

APPENDIX C

Secure Communication Protocols

SNMP v3
SNMP is a standard protocol that monitors and controls devices connecting to the network. Moreover, SNMPv3 provides the ability to protect data confidentiality through authentication and encryption.

IPv6
KYOCERA has obtained the IPv6 Ready Logo up to Phase2. IPv6 support, which is available in the KYOCERA MFPs/printers, can connect to the router, and use basic control protocol like ping. In addition to the above-mentioned basic connections, a more secure connection is ensured by implementing rigorous security measures.

IPSec
A protocol with a functionality that protects data in transit from tapping or alteration by encrypting respective IP packets. Encryption using IPSec is applied to print data sent from a PC to a MFP/printer, and scanned data to be sent from a MFP to a PC. Therefore, IPSec supports a more secure exchange of data.

SSL/TLS
A system to encrypt data for transmissions such as web access or others, and also has a function to mutually check if communication destination parties are reliable for mutual communications. KYOCERA MFPs/printers support SSL/TLS encryption protocols including SSL3.0, TLS1.0, TLS1.1, TLS1.2, and thereby prevent alteration of data or tapping data on the network.

IPP over SSL/TLS
An internet printing protocol that acts as a combination of IPP, which is for exchanging print data on the internet or TCP/IP network, and SSL/TLS, which is for encryption of a communication channel. This allows users to safely send printed documents to the MFPs/printers through the network.

HTTP over SSL/TLS
A protocol that acts as a combination of HTTP, which is for sending/receiving data to and from web browsers or others on the TCP/IP network, and SSL/TLS, which is for encryption of a communication channel. In transmitting data between a PC and a MFP/printer, this mitigates risks of alteration and leakage of data by unauthorised users.

FTP over SSL/TLS
A protocol that acts as a combination of FTP, which is used for forwarding a file on the TCP/IP network, and SSL/TLS, which is for encryption of a communication channel. When sending scanned data from a MFP/printer using the FTP protocol, SSL/TLS encryption is applied to the channel. FTP over SSL/TLS enables more secure transmissions.

SMTP over SSL/TLS
A protocol that acts as a combination of email transmission, and SSL/TLS, which is for encryption of a communication channel between a server and a MFP/printer. This prevents masquerading, tapping or modifying data in transit.

POP3 over SSL/TLS
A protocol that acts as a combination of POP3, which is an email reception protocol, and SSL/TLS, which is for encryption of a communication channel between a server and a MFP/printer. This prevents masquerading, tapping or modifying data in transmit.

KYOCERA
Document Solutions

KYOCERA Document Solutions (U.K.) Limited,
Eldon Court, 75-77 London Road, Reading, RG1 5BS

Tel: 0118 931 1500
Fax: 0118 931 1108
Web: www.kyoceradocumentsolutions.co.uk
Email: info@duk.kyocera.com