KYOCERA
Document Solutions

PRINT SECURITY GUIDE

PRINT SECURITY

HIGH-LEVEL SECURITY CONFIGURATION

This final group provides guidance on the kinds of advanced MFD-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 MFD 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 MFD, 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.

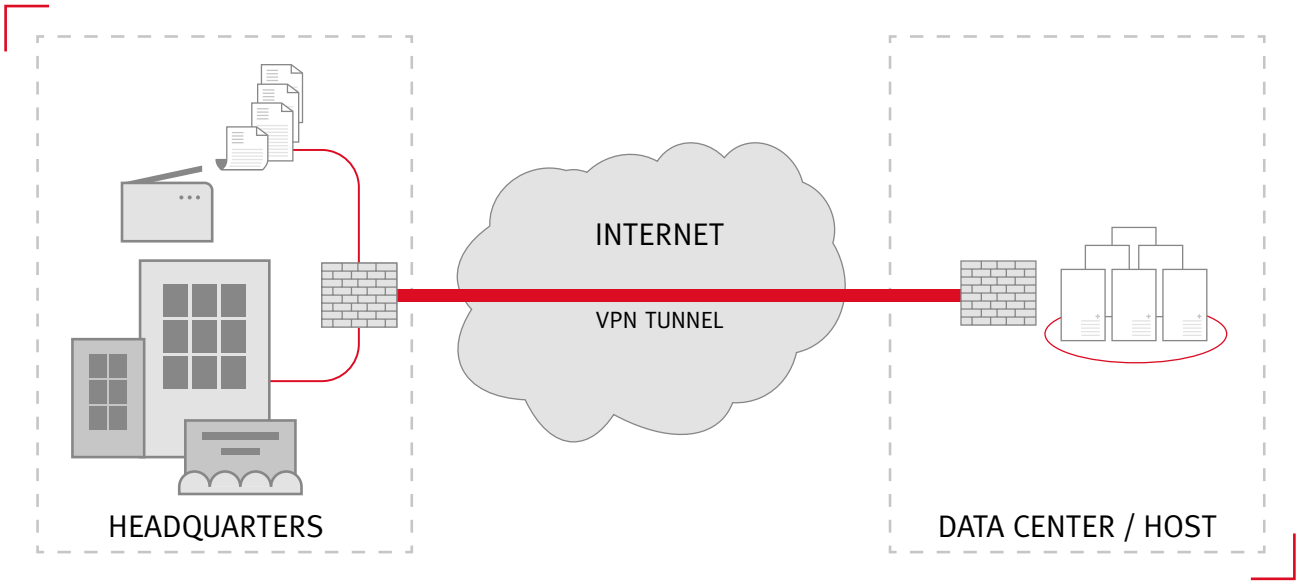
The latest applications can also control access to scanning, limit destinations and control settings with access permissions based on global, group or individuals.

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.



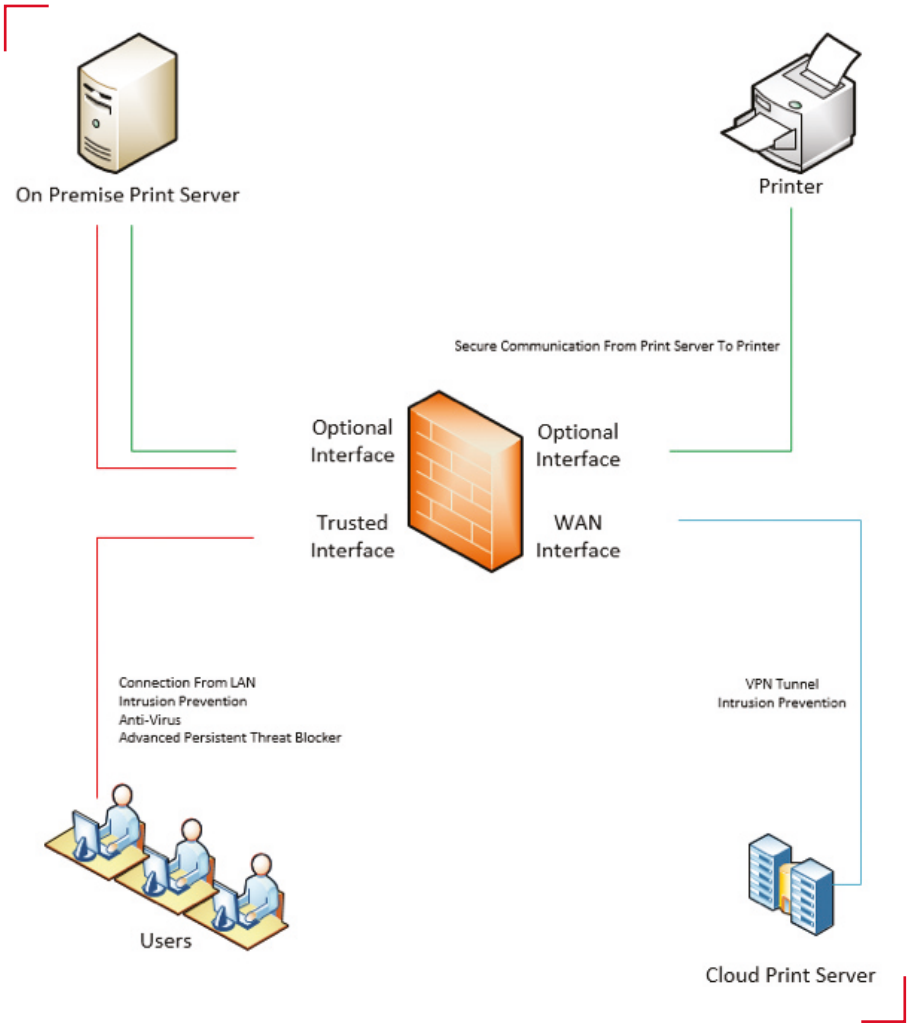
NETWORK DATA MONITORING

A perceived or potential threat to MFDs 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 MFD 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.

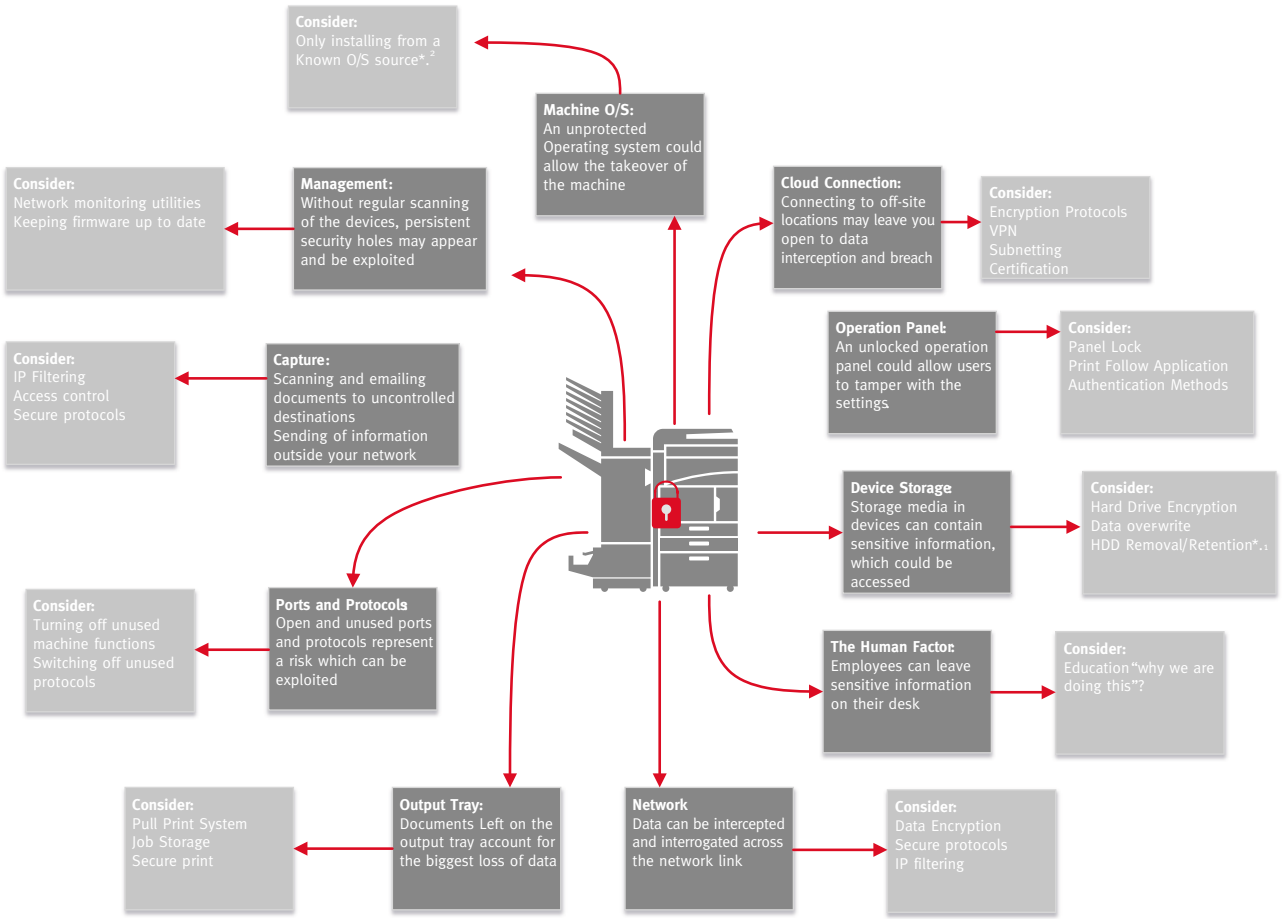


CONCLUSION

IT professionals must consider MFDs 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 MFDs 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/MFDs/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/MFDs/Printers for a network connection. This also enables users to detect (install) MFPs/MFDs/Printers device or send/receive data easier. Original documentation image scanned through MFP/MFDs/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/MFDs/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/MFD/ 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/MFD/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/MFDs/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/MFD/printer, and scanned data to be sent from a MFD 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/MFDs/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/MFDs/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/MFD/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/MFD/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/MFD/printer. This prevents masquerading, tapping or modifying data in transmit.

KYOCERA Document Solutions

KYOCERA Document Solutions Australia
Ph: 13 59 62
www.kyoceradocumentsolutions.com.au

KYOCERA Document Solutions New Zealand*
Ph: 0800 459 623
www.kyoceradocumentsolutions.co.nz

* KYOCERA Document Solutions New Zealand is the trading name of the New Zealand branch of KYOCERA Document Solutions Australia Pty Ltd a corporation incorporated in Australia.

KYOCERA Document Solutions Australia Pty. Ltd ABN 77 003 852 444