#2 SECURE YOUR OFFICE IOT

Canon

#2 SECURE YOUR OFFICE DEVICES

IOT devices – MFDs, printers, scanners – don't always arrive 'data safe' out of the box. Canon offers device hardening profiles and services, configuring devices to precisely align settings with incumbent security policies. Our approach is predicated on a pre-assessment of a customers perceived risk appetite.

The Risks

Modern Multifunction Devices (MFDs) provide print, copy, scan, send and fax functionality. MFDs are computer servers in their own right, providing a number of networked services along with significant hard drive storage.

When an organisation introduces these devices into their infrastructure, there are a number of areas that should be addressed as part of the wider security strategy, which should look to protect the confidentiality, integrity and availability of your networked systems.

Deployments differ and organisations will have their own specific security requirements. While we work together to ensure that Canon devices are shipped with appropriate initial security settings, we aim to further support this by providing a number of configuration settings to enable you to more closely align the device to the requirements of your specific situation.

SMALL OFFICE NETWORK

Designed to satisfy a base level of device hardening expectations for businesses with fewer than five devices.

MID-SIZED BUSINESS OFFICE

Designed to achieve an above average level of device hardening with 5 to 50 devices.

ENTERPRISE OFFICE

Designed to achieve optimal device hardening for more demanding security needs in excess of 50 devices.

CUSTOM SERVICE

Tailored to your discerning device hardening needs. (to-order option)

SMALL OFFICE NETWORK

Small Businesses rarely have in-house technical experts to install devices and offer advice on matters of device, document and office network security. For this reason, out-of-the-box cloud and appliance solutions are generally preferred.

Typically, this will be a small business environment with an un-segmented network topology. It uses one or two MFDs for its internal use and these devices are not accessible on the Internet.

Mobile applications are extremely popular in small businesses that lack infrastructure and these are available, however additional solution components will be required. For those users operating printer services outside of a LAN environment, a secure connection is needed.

Canon's small office network device hardening focuses on basic intrinsic device security, although attention is paid to the security of the data in transit between the device and print infrastructure.

MEDIUM-SIZED BUSINESS OFFICE

Organisations operating more than five multi-functional devices inherit a broader range of information security challenges. As businesses migrate from dedicated stand-alone devices to more feature-rich and capable networked devices, demands for secure User and Guest authentication increase. Document release at point of use means that sensitive content can continue to be printed safely, even on networked devices.

Canon's device hardening specifications for medium-sized businesses take into account the more common of these added security concerns.

LARGE ENTERPRISE OFFICE

Canon encourages organisations with a multi-site, multi-office environment, and adopting a segmented architecture, to operate network print/scan activities on a separate VLAN accessible for internal use via print server(s). In deployments of this nature, it is uncommon for devices to be made accessible from the Internet.

This environment will usually have a permanent expert team to support its networking and back-office requirements along with general computer issues although it may be the case that technicians lack specific knowledge of computer printing and Office IoT device technologies.

Canon's device hardening specifications for large enterprise provide a comprehensive answer for businesses operating complex network topologies and technology infrastructures seeking to minimise office security vulnerabilities.

CUSTOM CONFIGURATION SERVICES

Modern office devices are feature rich - the range of device settings is broad and normally requires expert knowledge to fully appreciate the configuration possibilities and associated risks.

For network administrators seeking to create a custom device hardening profile, what are the most important steps to consider? Here are a few top tips from our information security team:

1

Disable all functionality - Start with a zero-feature capability (i.e. turn everything off) and to then start applying features, appreciating with each added feature the likely consequential vulnerabilities.

2

Determine the functionality, network services/protocols needed to support the solution.

3

Determine device extrinsic controls that are needed to additional protect the network.

4

Enable what is needed to support the solution.

5

Test to identify any risks.

Please refer to Canon's device hardening guides for detailed information on device configuration possibilities.

Canon offers a Pre-Delivery Inspection (PDI) and Installation service that can be tailored to satisfy customer requests as a to-order option. **Please ask for more details.**

INTERESTED?

There is no fool-proof plug and play office security solution.

Every business has to determine what represents an acceptable level of risk.

Canon is a pro-active partner to businesses seeking to keep data safe as part of a resilient enterprise information security policy.

One voice

Our information security team is responsible for both Canon's internal information security, and the advice and solutions we offer to our customer.

An ethos of security and privacy by design

When we design or select technologies, products and services for our customers, we consider their likely information security impact on our customers' environment, and incorporate security and measures to enable protection to the desired level.

An inclusive approach

All organisations are different. There is no one-size-fits-all solution when it comes to formulating a appropriate information security approach for your business. At Canon, our approach is to work closely with our customers to build better information security together.

Satisfy the information security expectations of:

- Shareholders
- Staff
- Customers
- Suppliers

- Partners
- Guests
- Channel Partners
- Contractors

Canon