5 WAYS TO PROTECT THE DATA IN YOUR OFFICE

#3 MAKE INFORMATION SECURITY WORK FOR YOU

Canon

#3 MAKE INFORMATION SECURITY WORK FOR YOU

Intrusive security tooling can be considered draconian or just plain irritating by users who find their work activities interfered with.

Getting the balance right requires an understanding of the level of risk your business is prepared to accept when it comes to protecting sensitive information.

To achieve the best-fit solution, you will need a range of document services and authentication solutions to choose from. Canon offers your business a broad range of security and user authentication options to make information security work for you blending risk mitigation with optimal user experience.

The Risks

The traditional photo copier has come a long way. Now, known as a multi-functional device, it has the power of a PC server – it's a communications hub between people and systems sitting on your network.

Think about the sort of documents that get printed and distributed on office equipment – contracts, passports, curriculum vitae's, customer letters and agreements, strategy documents, offers of employment...

Your office equipment may hold temporary or stored data originating from print, copy, fax and scan activities. How do you know? And how can you avoid this data from falling into the wrong hands?

CANON SOLUTIONS

YOUR OPTIONS

READY TO PLAY DEVICE SECURITY

Define security policies and enforce them on one or more devices to control settings

UNIVERSAL LOGIN MANAGER (ULM)

Protect your devices against unauthorised use by implementing user controls through authentication

SECURE NETWORK PRINT AND SCAN MANAGEMENT

Install granular control of access to device functions

SECURE GUEST PRINTING AND MOBILE SOLUTIONS

Protect data on device hard disk drives through to final erase

READY TO PLAY DEVICE SECURITY

Could your MFPs, printers and network IoT devices be putting your network at risk?

- Are you leaving network ports open to attack?
- Are guests able to print and scan without exposing your network to risks?
- Are your bring-your-own-device to work policies secure and supportable?
- Are print data-streams encrypted from PC to the output device?
- Is print and scan data secured in transit?

ENCRYPTION OF DATA

Encrypt print jobs in transit from the user PC to the multifunctional printer. By enabling the universal security feature set, scanned data in PDF format may also be encrypted.

IP AND MAC ADDRESS FILTERING

Protect your network against unauthorised access by third parties by only allowing communication with devices having a specific IP or MAC address for both outbound and inbound communication.

PROXY SERVER CONFIGURATION

Set a proxy to handle communication instead of your machine, and use when connecting to devices outside of the network.

IEEE 802.1X AUTHENTICATION

Unauthorised network access is blocked by a LAN switch that only grants access privileges to client devices that are authorised by the authentication server.

LOG MONITORING

Various logs allow you to monitor activity around your device, including blocked communication requests.

PORT CONTROL

Configure ports as part of your security policy setting.

IPSEC COMMS

IPSec communication prevents third parties from intercepting or tampering with IP packets transported over the IP network. Use TLS encrypted communication to prevent sniffing, spoofing, and tampering of data that is exchanged between the machine and other devices such as computers.

WI-FI DIRECT

Enable peer-to-peer connection for mobile printing without the mobile device needing access to your network.

UNIVERSAL LOGIN MANAGER

Universal Login Manager is a free-to-use feature that provides the means for Network Administrators to install fine-grained user access control over Canon print devices. Simple setup and operation minimises IT network admin overheads for maximum value with minimum effort.

1 MULTIPLE AUTHENTICATION MODES

Local device authentication – User accounts and permissions are set directly on devices via a web browser user interface. Active Directory integration – Use network login credentials to login to devices by integrating with an existing company directory service such as Active Directory on Windows Server.

2 DEVICE OR FUNCTION LEVEL ACCESS CONTROL

Login can be implemented at device level or at function level, and access to device functionalities such as scanning, sending or copying/printing in colour can be restricted to enhance security or control output costs.

3 ACT

Identify which Users are accessing which devices and/or functions. Administrators can collect basic usage statistics (print/copy/scan activity) from one or more devices. Data can be consolidated and visualised in a number of standard reports.

SECURE NETWORK PRINT AND SCAN MANAGEMENT

Award-winning Canon network print/scan management software ensures that documents are released only to designated employees, protecting content throughout the print process and beyond.

OUTPUT MANAGEMENT

With our modular output management software, businesses enjoy secure sharing of network devices, enabling them to print jobs securely on any printer connected to the output management server. Mobile users are supported by a centrally controlled service, where both internal, as well as guest users have secure access to printing from mobile devices.

PRINT AND COMMUNICATE WITH CONFIDENCE

Out of the box, Canon network print/scan management software ensures information is securely communicated between its various components (i.e. PC, Server and MFD). It provides additional layers of security when transmitting print jobs across a network by encrypting the data. While jobs are in transit through a network and susceptible to interception, they remain encrypted until they reach the device from where they can be securely released.

SECURE GUEST PRINTING AND MOBILE PRINTING

Protect documents and data when printed, scanned and shared using mobile devices

MOBILE GUEST PRINTING

Our secure network print and scan management software addresses common security risks for mobile and guest printing by providing external job submission pathways via email, web and Mobile App. This minimises attack vectors by locking the MFD to a secure source.

DIRECT WI-FI ON IMAGERUNNER ADVANCE

Did you know that with the latest generation of Canon's MFPs, your users can connect directly to Wi-Fi without requiring administrators to provide access to their secure office networks? Easy for guests, easy for IT!

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.

Our is 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 Inc.
Canon.com

Canon Europe
canon-europe.com

English Edition

Canon Europe Ltd
3 The Square,
Stockley Park,
Uxbridge,
Middlesex
UB11 1ET
UK

Canon U.K. Ltd
Woodhatch
Reigate
Surrey
RH2 8BF
UK

Canon