PROTECTING YOUR OFFICE

Canon

HOW SECURE IS INFORMATION IN YOUR OFFICE?

Today's businesses greatly rely on information, creating complex networks of connected technology, processes, people and organisations, spanning beyond national boundaries. New agile working practices emerge, reshaping the office and how people create, share, and consume information. Securing data in this intricate environment is more challenging than ever before, and most businesses invest in sophisticated technologies such as robust firewalls, up-to-date anti-virus protection, security software and more. However, they often fail to recognise the need to extend that protection to their office printers, leaving themselves more vulnerable than they realise.

THINK ABOUT YOUR PRINTERS

Modern multifunctional printers (MFPs) have evolved into powerful tools, which just like PCs and servers have operating systems, huge hard disk drives, connect to the network and Internet, and are shared by users to process huge numbers of business-critical documents daily.

WHAT ARE THE RISKS?

- Unauthorised users viewing sensitive information stored on unprotected MFPs
- The availability of your printing infrastructure being compromised due to wrong operation
- Malicious outsiders gaining access to your network via the printer and using it for further attacks
- Exposure of confidential documents forgotten in the output tray after printing
- Mixing up printed matter belonging to different users
- Documents being faxed or e-mailed to the wrong recipients as a result of typing mistakes
- Print or scan data in transit being intercepted by hackers
- Loss of data due to careless disposal of printers at the end of their lease.

"Adopting baseline standards of information security is well worth doing in the office where you're potentially handling huge amounts of data. A printer nowadays is no longer a dumb machine, it's a server that just happens to print paper."

(CISO, Publicis Groupe)

SECURE PRINTING SOLUTIONS FOR YOUR BUSINESS

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. That's why our office multifunctional printers are equipped with a wide variety of security features, both standard and optional, which enable businesses of any size to achieve the desired level of protection for:

DEVICES | NETWORKS | DOCUMENTS | YOUR ENTERPRISE

INTERNATIONALLY RECOGNISED STANDARDS AND CERTIFICATIONS

Our imageRUNNER ADVANCE multifunctional printers are routinely evaluated and certified using the Common Criteria methodology and in accordance with the requirements of the IEEE2600 standards for hardcopy device security.

SECURITY TESTING

Canon employs one of the most rigorous security testing regimes in the office equipment industry. Technologies adopted into our product portfolio undergo the same high standards of testing we expect for our own business.

As an industry leader in the development of innovative printing and information management solutions for the office and business, Canon works together with customers to help them embrace an inclusive approach to information security, one that considers the security implications of our office technology as part of their wider information ecosystem.

PROTECT YOUR DEVICE

Comprehensive protection for your physical assets

USER AUTHENTICATION SOLUTIONS

Protect your device against unauthorised use by implementing user access control through authentication. This also offers the added benefit of providing users with quicker access to their preferred settings and print jobs, while enhancing accountability and control. Our departmental printers are equipped with Universal Login Manager, which is a flexible login solution, enabling user authentication against a user database created on the device, domain authentication through Active Directory or uniFLOW server. This gives businesses the opportunity to control device access, while achieving the right balance between user convenience and security.

DEVICE ADMINISTRATION CONTROL

Device configuration, such as network settings and other control options are available to only those users who have administrator privileges preventing intentional or accidental alterations.

ACCESS MANAGEMENT SYSTEM

This feature provides granular control of access to the device functions. Administrators can use the standard available roles or create tailored ones with a desired level of access privileges. For example, certain users may be restricted from copying documents or using the send function.

SECURITY POLICY SETTING

The latest imageRUNNER ADVANCE devices are also equipped with a security policy function, which enables the administrator to access all security related settings in one menu and edit them before enforcing on the machine.
Once enforced, use of the device and settings changes must comply with the policy. The security policy can be protected with a separate password, so access to this area is restricted to the responsible IT security professional, adding a further level of control and assurance.

PROTECTION OF DATA ON THE HARD DISK DRIVE

At any point in time, the multifunctional printer contains a large amount of data that should be protected – from print jobs waiting to be printed, to received faxes, scanned data, address books, activity logs and job history. Canon devices offer a number of measures to protect your data at each stage of the device lifetime and ensure the confidentiality, integrity and availability of data.

PREVENTATIVE SECURITY

imageRUNNER ADVANCE products offer a number of security settings which allow to safeguard printers from attacks. Secure Boot functionality provides device integrity, while Syslog data provides real time security health of the device (Data can be read by an appropriate third party SIEM system).

HOW SECURE ARE YOUR DEVICES?

1
Are your devices shared and located in public areas?

2
Can users gain unsecured access to devices?

3
Do you have measures in place to protect information on the device hard disk?

4
Can unauthorised users change device settings?

5
Have you considered the lifecycle of your device and its secure disposal?

HARD DISK ENCRYPTION

Our imageRUNNER ADVANCE devices encrypt all data on the hard disk drive, enhancing security. The security chip responsible for data encryption complies with the FIPS 140-2 Level 2 security standard established by the U.S. government and is certified under the Cryptographic Module Validation Program (CMVP) established by the U.S. and Canada, as well as the Japan Cryptographic Module Validation Program (JCMVP).

HARD DISK ERASE

Some data, such as copied or scanned image data, as well as document data that is printed from a computer, is only temporarily stored on the hard disk drive and deleted after the operation is complete. To ensure no residual data is retained, our devices equipped with a hard disk drive offer the possibility to routinely erase residual data as part of job processing.

INITIALISE ALL DATA AND SETTINGS

To prevent data loss when replacing or disposing of the hard disk, you can overwrite all documents and data on the hard disk, and restore machine settings to defaults.

HARD DISK MIRRORING*

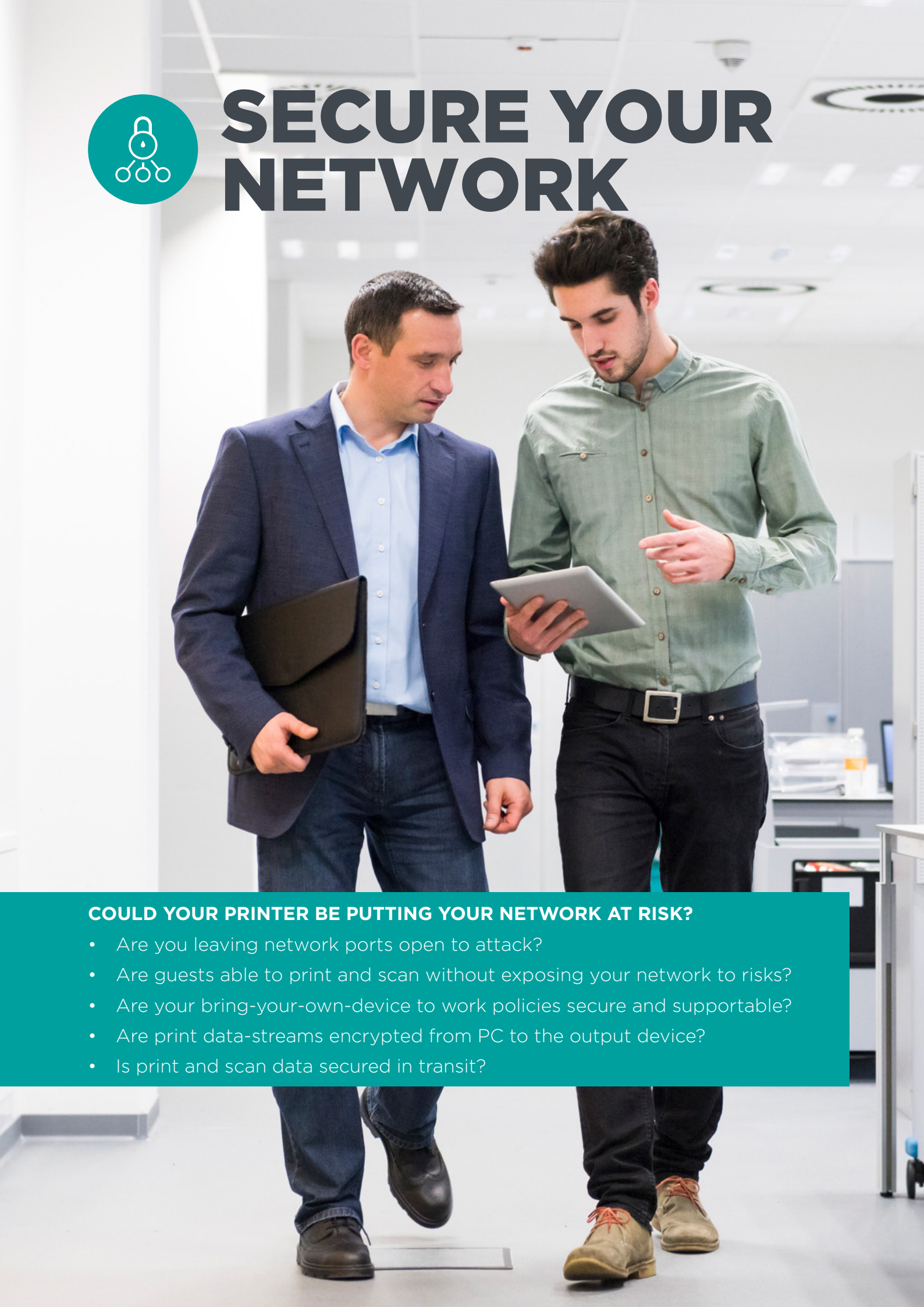
Businesses have the possibility to back up the data on their device hard disk drive using an additional optional hard disk. When mirroring is performed, data on both hard disk drives is fully encrypted.

REMOVABLE HARD DISK KIT*

This option enables you to remove the hard disk drive from the machine for secure storage when the machine is not in use.

*Optional. For detailed information on the availability of the features and options throughout the office printing portfolio, please contact your Canon representative.

SECURE YOUR NETWORK



COULD YOUR PRINTER 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?

Canon offers a range of security solutions to keep your network and data safe from internal and external attacks.

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.

IPSEC COMMUNICATION

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.

PORT CONTROL

Configure ports as part of your security policy setting.

CERTIFICATE AUTO ENROLLMENT

With this feature, the pain of maintaining security certificates is dramatically reduced. Using industry recognized technology, a system administrator can automatically update and release certificates, making sure security policies are met at all times.

LOG MONITORING

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

WI-FI DIRECT

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

ENCRYPTION OF DATA IN TRANSIT TO AND FROM THE DEVICE

This option encrypts 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.

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 minimizes attack vectors by locking the MFD to a secure source.

PROTECT YOUR DOCUMENTS

All businesses deal with sensitive documents such as contractual agreements, staff payroll information, customer data, research and development plans and more. Should documents get into the wrong hands, consequences range from damaged reputation to heavy fines or even legal action.

Canon offers a range of security solutions to protect your sensitive documents throughout their lifecycle.

CONFIDENTIALITY FOR THE PRINTED DOCUMENT

Secured print
The user can set a PIN code for printing, so that only after the correct PIN code has been entered at the machine can the document be printed. This enables individuals to secure those documents they deem confidential.

Hold all print jobs
On imageRUNNER ADVANCE, the administrator can enforce a hold on all submitted print jobs, so that users are required to log-in first before jobs can be printed to protect the confidentiality of all printed matter.

Mailboxes
Print jobs or scanned documents can be stored in a mailbox for access at a later stage. Mailboxes can be protected with a PIN code to ensure only its allocated owner can view the content stored in it. This secure space on the machine is suitable for holding documents which need to be frequently output (such as forms), but require careful handling.

uniFLOW secure printing*
With uniFLOW MyPrintAnywhere secure printing, users submit print jobs via the universal driver and collect them from any printer on the network.

DISCOURAGE OR PREVENT DUPLICATION OF DOCUMENTS

Print with visible watermarks
Drivers have the capability to print out visible marking on the page, overlaid on top or behind the document content. This discourages copying by raising user awareness about the confidentiality of the document.

Print/Copy with invisible watermarks
With this option enabled, documents can be printed or copied with embedded hidden text within the background, so that when duplicated the text appears on the document and acts as a deterrent.

Data loss prevention at corporate level
Upgrade your basic data loss prevention capabilities to iW SAM Express in combination with uniFLOW. This server based solution allows you to capture and archive documents sent to and from the printer, analyse and interpret using text or attributes with the ultimate goal to act to security theats.

Document Scan Lock*
This option embeds hidden code in printed or copied documents, which forcefully prevents further duplication at a machine with the function enabled. The administrator can choose to enforce this for all jobs or at user discretion. TL code or QR code can be embedded.

Tracking of document origin*
Through embedded code, the document can have its origin traced to the source.

HOW SECURE ARE YOUR DOCUMENTS ?

1 Are unauthorised users prevented from accessing sensitive documents at the printer?

2 Can you assure confidentiality of all users' documents passing through the shared device?

3 Can you trace the origins of printed documents?

4 Could someone walk off with sensitive documents from your printer?

5 Can you prevent common mistakes when sending documents from the device?

EXERCISE CONTROL OVER DOCUMENT SENDING AND FAX

Limit destinations for sending
To reduce the risk of information leakage, administrators can restrict the available sending destinations to only those in the address book or LDAP server, the logged in user's address, or certain domains.

Disable address auto-completion
Prevent sending documents to wrong destinations by disabling auto completion of e-mail addresses.

Address book protection
Set a PIN code to protect the device address book from unauthorised editing by users.

Fax number confirmation
Prevent documents from being sent to unintended recipients by requiring users to enter the fax number twice for confirmation before sending.

Confidentiality for received fax
Set the machine to store documents in memory without printing. You can also protect the confidentiality of received fax documents by applying conditions to determine the storage location for a confidential inbox, as well as set PIN codes.

VERIFY DOCUMENT ORIGIN AND AUTHENTICITY THROUGH DIGITAL SIGNATURES

Device signature
Device signature can be applied to scanned documents in PDF or XPS format, using a key and certificate mechanism, so that the recipient can verify the origin of the document as well as its authenticity.

User signature*
The option enables users to send a PDF or XPS file with a unique digital user signature obtained from a certificate authority. In this way the recipient is able to verify which user signed it.

APPLY POLICIES WITH ADOBE LIFECYCLE MANAGEMENT ES INTEGRATION

Users can secure PDF files and apply persistent and dynamic policies to control access and usage rights to protect sensitive and high-value information against inadvertent or malicious disclosure. Security policies are maintained at server level, so rights can be changed even after a file is distributed. The imageRUNNER ADVANCE series can be configured for Adobe® ES integration.

*Optional. For detailed information on the availability of the features and options throughout the office printing portfolio, please contact your Canon representative.

ENTERPRISE INFORMATION SECURITY

Canon can make a contribution to the overall protection of information in your organisation.

COMPLETE CONTROL FOR YOUR END-TO-END CAPTURE AND OUTPUT NEEDS

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.
For enterprise capture needs, the scanning module provides capture, compression, conversion and distribution of documents from the multifunctional device to a wide variety of destinations, including cloud-based systems. You can also safely reroute print jobs to the most appropriate printer, optimising the cost of print for each document.
Our solution enhances the security of documents throughout your business, combined with full document accounting providing complete visibility of activity per user, device and department.

CENTRALISED FLEET MANAGEMENT

Our device management software IW MC enables device settings, security policies, passwords and certificates, as well as firmware to be updated and pushed out to your fleet of Canon devices across the network, saving your IT team valuable time and helping to keep the security of your print infrastructure up to date.

COMPREHENSIVE DOCUMENT AUDITS

Our office document services architecture can be enhanced with to-order options to capture a complete record (i.e. scan plus job meta-data) of all documents processed through imageRUNNER ADVANCE devices.

MANAGED PRINT SERVICES

Canon MPS combines innovative technology and software with the right services, to provide you with your desired print and document experience without the associated hassle for your IT teams. Through proactive management and continual optimisation of your print infrastructure and document workflows, we can help you achieve your security objectives while optimising cost and increasing productivity throughout your business.

CUSTOM DEVELOPMENT

We have a team of in-house developers who can propose and develop a custom solution to suit your specific situation or unique requirements.

HOW INCLUSIVE IS YOUR ENTERPRISE SECURITY APPROACH?

- Does your security policy also extend to your fleet of multifunctional devices?
- How do you ensure your printing infrastructure is up to date and enhancements and bug fixes are implemented timely and efficiently?
- Are guests able to print and scan without exposing your network to risk?
- Are bring-your-own-device policies secure and supportable throughout your print fleet?
- Does your IT team have enough time to investigate security concerns?
- Do you have the right balance between security provisioning and user convenience?

WHY CANON?

EXPERTISE

Hardware and software integration reduces the potential for system violations.

PARTNERSHIP

We help customers do better business knowing that we will **proactively address data security threats.**

SERVICE

The **same information security team** for customers manages our own internal IT security.

We consider all potential threats both within and beyond the enterprise firewall.

INNOVATION

Our products and services **incorporate smarter ways** to minimise the likely information security risks.

SC 2017 awards EUROPE

BLI PACESETTER MOBILE Print 2017-2018

COPIER MFP LINE OF THE YEAR 2018 BLI BUYERS LAB LINE OF THE YEAR

'Highly commended' in the best security team category at the **2017 SCA Awards Europe** which recognise cybersecurity expertise.

Canon U.S.A. received two **BLI PaceSetter Awards 2017** (Document Imaging Security and Mobile Print).

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

English Edition

Canon