CONTROL

SECURITY FOR MFPs, NETWORK COMMUNICATIONS, AND DOCUMENTS

Your organization relies on complex networks of connected people, processes, and technology to get the job done. And securing data is more important than ever before. Your multifunction printers are an integral part of this connected network helping to safeguard sensitive information, protect employee and customer data, and assist in your regulatory compliance efforts. With built-in and frequently updated security features, the Canon imageRUNNER ADVANCE DX and imagePRESS Lite Series, along with the imageFORCE C7165 model can help you gain high levels of control over your MFPs, your network communications, and your documents.

CONTROL
YOUR MULTIFUNCTION PRINTERS

Advanced security features for your MFPs—many standard and all consistent across the product line for peace of mind.

CONTROL DEVICE ACCESS

Using a host of flexible authentication methods, administrators can control who has access to the MFP and to which features. This can be done using a PIN, username and password, or card log in (with the addition of an optional card reader). Restrictions, such as access to color copying and scanning functions, can be applied by individual, group, or through customized roles. You can also define whether to allow unregistered users, such as visitors, to log in as guests and then specify their level of access.

CONTROL ACCESS TO ADMINISTRATION SETTINGS

Device configurations, such as network settings and other control options, are available only to users with administrator privileges, enhancing security by helping to prevent intentional or accidental changes to device functions and permissions. Administrators can set requirements for passwords, such as expiration period, lockout time, and complexity. They can even access the device remotely with comprehensive control, from changing permissions to monitoring activity—even turning on or off devices, or locking down specific equipment or functions.

Note: Many authentication and restriction features described above require the optional uniFLOW Online solution.

CENTRALIZED SECURITY SETTINGS

Security settings can be configured from a centralized location, password protected, and accessible only to authorized users. This gives organizations the ability to separate security administration and device administration, reserving access to certain controls to security professionals. Security policy settings can be monitored at regular intervals, with notifications set to alert administrators when changes are made. After establishing these settings, an administrator can use device management tools to export across other devices in the fleet, building consistent security settings system-wide with little time and effort.
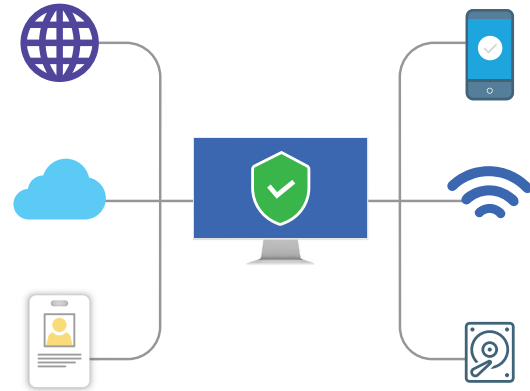
For environments who are unsure which settings to implement, a security settings navigator tool can help recommend printer security settings based on the type of usage environment. These settings can be applied all at once by authorized users within the device settings screen. Upon device setup, the imageFORCE C7165 uses an estimation algorithm developed by Canon and recommends a usage environment type based on the data obtained from the user's environment. If there are changes to the environment, a message will be displayed on the local UI suggesting review of the current security settings to help stay ahead of possible security vulnerabilities.

YOUR VALUABLE DATA

Select Canon MFP models provide standard support for storage device encryption, leveraging a cryptographic module that complies with the FIPS 140-3 security standard. This helps protect sensitive information stored on the storage device. The system also provides protection with robust data erase features that can overwrite previous data on a Solid State Drive; this helps prevent stored data from being read/written on PCs or a different MFP. These models feature the ability to help verify that the device boot process, firmware, and applications initialize at startup, without any alterations or tampering by malicious third parties. Select models support automatic recovery of boot process for self resiliency. During operation, Trellix™ Embedded Control utilizes a whitelist to protect against malware and tampering of firmware and applications.
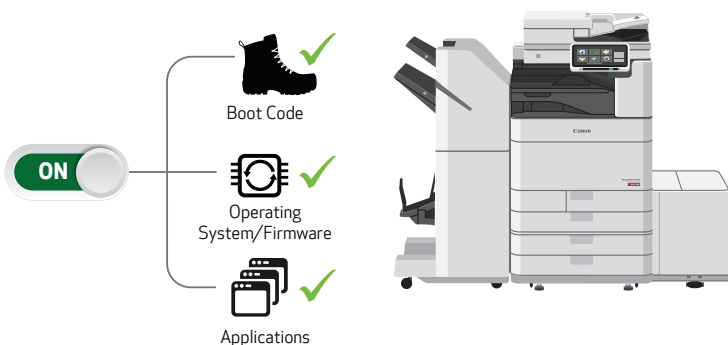
Verify System at Startup with Automatic Recovery[1]

Trellix Embedded Control

CONTROL
YOUR NETWORK COMMUNICATIONS

A range of security solutions to help keep data safe from internal and external attacks as it travels the network.

ENCRYPT NETWORK TRAFFIC

imageRUNNER ADVANCE DX, imageFORCE, and imagePRESS Lite models include several security features to help protect data they send across the network. IPsec (Internet Protocol Security) safeguards the exchange of data at the communications level by encrypting inbound and outbound network traffic, confirming sender identity, and helping ensure unaltered transmission receipt. TLS 1.3 (Transport Layer Security) encryption further prevents access to, and tampering of, data being exchanged, helping keep information safe in transit.

NETWORK CONNECTIONS

Canon imageRUNNER ADVANCE DX, imageFORCE, and imagePRESS Lite systems support the IEEE 802.1x protocol, providing authentication to network devices and establishing a closed connection. The protocol is designed to help keep unwanted users from connecting to the network, whether they use a wired connection or mobile device.

INTEGRATES WITH SIEM SYSTEMS

Security Information and Event Management (SIEM) systems can be valuable tools, providing network administrators with real-time, comprehensive insights into their network activity. The imageRUNNER ADVANCE DX, imageFORCE, and imagePRESS Lite platforms are built to integrate with your existing SIEM infrastructure, communicating directly with these third-party tools to help deliver insights into your print environment. Administrators can set up alerts to be notified of potential issues such as failed authentication attempts, changes in settings, new applications, and more. This communication between the MFPs and SIEM systems can provide visibility into potential threats to your network and printers.
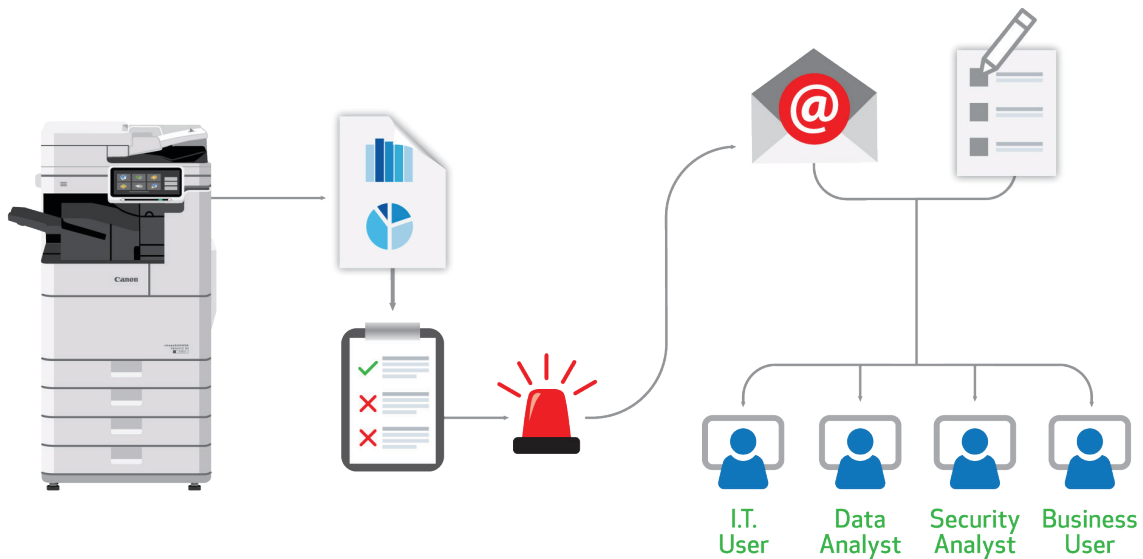
CONTROL
YOUR DOCUMENTS

Various security solutions to help protect sensitive documents throughout their life cycle.

KEEPING DOCUMENTS IN THE RIGHT HANDS

All organizations deal with sensitive documents. Should documents get into the wrong hands, consequences can range from damaged reputation to heavy fines or even legal action. Sensitive and confidential information—including employee records, customer information, and proprietary intellectual property—is vulnerable when left unattended in output trays. To avoid having such documents left at the printer, users can leverage features that require them to be at the device to release the job. Or administrators can require that users log in before printing their jobs using one of the various authentication methods.

WORKFLOW SECURITY

Whether by human error or with harmful intent, everyday office workflows can lead to misdirected information, potentially causing serious security issues. imageRUNNER ADVANCE DX, imageFORCE, and imagePRESS Lite devices have several features that can help—all easy to use and under the administrator's control. Scan destinations can be restricted for all users or certain groups, such as guests, limiting the ability to send documents to those recipients in a specific address book or domain. For even higher levels of control, users can be allowed to send documents only to themselves. Address books can be kept confidential to help protect private details and password protected so that information can be added, edited, or deleted only by authorized users.

For fax transmissions, incoming documents are stored in a proprietary format that helps protect them from malicious activity. Legitimate incoming faxes can be directed to specific mailboxes—or protected by PIN—under the administrator's control. The destination of outgoing faxes can be limited and controlled as well.

PROTECT YOUR PDFS

PDFs often represent some of the most confidential documents in an organization, with the format often used for contracts, reports, proposals, financial statements, and similarly sensitive information. The built-in Encrypted PDF feature supports various levels of encryption for enhanced security when sending these documents. Permissions and passwords can be included to control who can open, read, or print the file. To help ensure the legitimacy of highly sensitive documents, users can add digital signatures to verify document source and authenticity. This signature can be viewed through the document properties or displayed prominently on the PDF's pages.

CLOUD INFORMATION MANAGEMENT

Important business information can be stored in various locations within an organization. Workflow technology that can simplify communication and provide security features is top priority. Canon offers customers powerful capabilities that leverage their existing cloud storage infrastructure. These help address many issues that often come with sending and receiving large files, including the need for security features and the high costs related to email storage. As emails pass through mxHERO, the body and attachments can be automatically routed to an access-restricted and indexed cloud storage account, such as Google Drive, OneDrive, Evernote, and Box. These are then replaced with a cloud storage link—thereby transforming in-boxes from bulky and potentially vulnerable to lightweight and controlled. mxHERO solutions provide users with an array of security features, including the ability to enable automatic expiration of link access, prevention of file downloads, and password protection for supported cloud storage systems.

SECURITY FEATURES	imageRUNNER ADVANCE DX, imagePRESS LITE, and imageFORCE C7165 Models
	imageRUNNER ADVANCE DX C5800 Series / C3900 Series / C359iF Series / C568iF Series / 8900 Series / 6800 Series / 6980i Model / 4900 Series / 719iF Series / imagePRESS Lite C270 Series / imageFORCE C7165
Device Management	
Verify System at Startup	Standard
Verify System at Startup with Automatic Recovery	Select Models[1]
Trellix Embedded Control	Standard
Security Management	
Recommended Security Settings by Environment One-Button Configuration	Standard
Security Policy Settings	Standard
SIEM Integration	Standard
Security Environment Estimation	Standard[2]
Authentication	
Active Directory/SSO/OAuth 2.0	Standard
Universal Login Manager	Standard
uniFLOW Online[3]	Optional
uniFLOW[4]	Optional
Proximity Card or CAC/PIV	Optional
Access Control	
Password-Protected System Setting	Standard
Access Management System	Standard
USB Block	Standard
Data Security	
TPM (Trusted Platform Module)	Standard
Solid State Drive	Standard
Purge Level SSD Erase:	Standard
SSD Password Lock	Standard
SSD Initialize	Standard
Solid State Data Encryption	FIPS 140-2 / FIPS 140-3[5]
Hard Copy and System Security	Standard (HCD-PP)
Document Security	
Secure Print (Driver-Based)	Standard
Encrypted Secure Print (Driver-Based)	Standard
Secure Print (Server/Cloud)	Optional
Secure Watermark	Standard
Mail Box Security	Standard
Encrypted PDF (AES 256 Support)	Standard
Device Digital Signature PDF	Standard
Network Security	
Port Management, IP Address, MAC Filtering	Standard
IPsec	Standard
Cipher Algorithm Selection	Standard
TLS 1.3 Support and SSL3.0 Disabled	Standard
Certifications	
HCD-PP	Standard
FIPS 140-2	IPSEC/CAC/PIV/TLS
FIPS 140-3[4]	SSD Encryption

[1] Automatic Recovery is supported on imageRUNNER ADVANCE DX C3900/C359iF/8900/6980/4900/719iF series models.

[2] Security Environment Estimation is available on the imageFORCE C7165 model only.

[3] uniFLOW Online is an optional cloud based solution. Subscription to a third-party service may be required. Subject to third-party provider terms and conditions.

[4] Available to education and government customers with prior approval.

[5] FIPS 140-3 is not supported on the C568iF Series.

Note: Some features require an update to the latest version of the Unified Firmware Platform.

usa.canon.com/simplyadvanced

To learn about Canon's many awards, visit **usa.canon.com/awards**.