Canon

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 Series 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.

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.
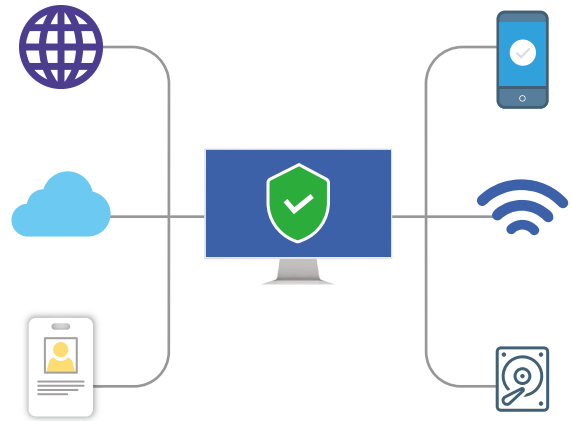
YOUR VALUABLE DATA

imageRUNNER ADVANCE models provide standard support for HDD Encryption, leveraging a cryptographic module that complies with the FIPS 140-2 security standard. This helps protect sensitive information stored on the hard drive. The system also includes robust data erase features that can overwrite previous data as a part of routine job processing as well as initialize and permanently erase all data at the end of equipment life. Hard Disk overwriting can be performed on demand or scheduled, and a confirmation report can be provided.*

imageRUNNER ADVANCE 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. During operation, McAfee Embedded Control utilizes a whitelist to protect against malware and tampering of firmware and applications.**

Boot Code

Operating System/Firmware

Applications

ON

Verify System At Startup

McAfee Embedded Control

McAfee™ PROTECTED

* HDD Erase Scheduler with confirmation report is optional.

** Supported on third generation imageRUNNER ADVANCE (1st, 2nd, and 3rd edition) and imageRUNNER ADVANCE DX models only. McAfee Embedded Control requires Unified Firmware Platform v3.9 or greater.

3

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 models include several security features to help protect data it sends 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 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 platform is 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 imageRUNNER ADVANCE MFPs and SIEM systems can provide visibility into potential threats to your network and printers.

I.T. User   Data Analyst   Security Analyst   Business User
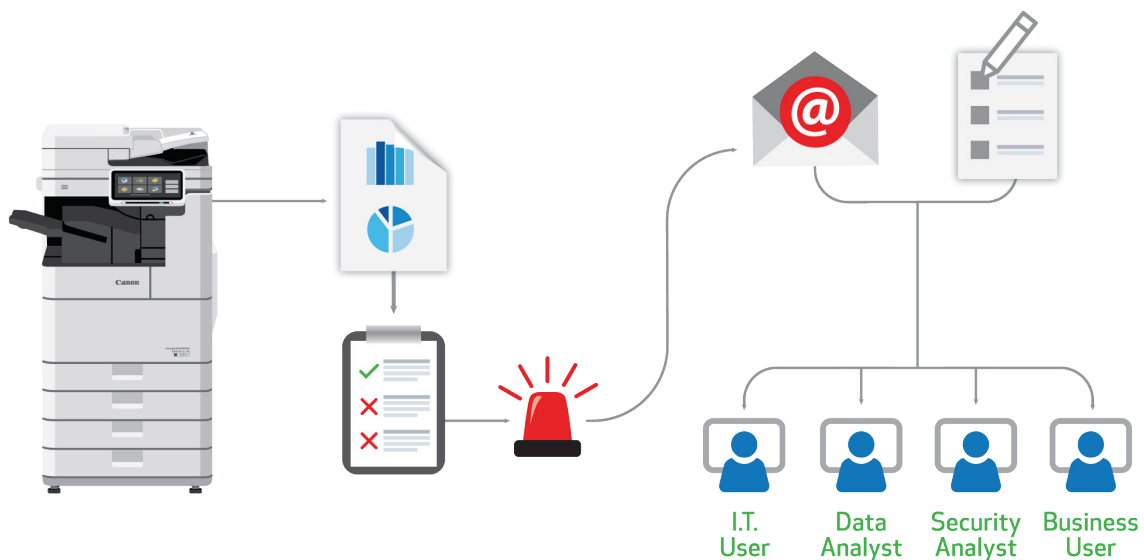
CONTROL
YOUR DOCUMENTS

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 create a PIN that must be entered 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.

CONFIDENTIAL

PAYROLL
$$$

CONFIDENTIAL

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 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.
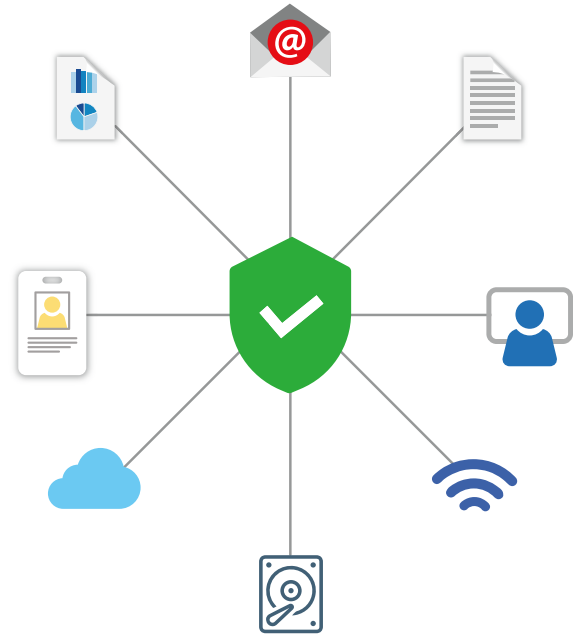
CLOUD CONTENT MANAGEMENT

Important business information can be stored in various locations within an organization. Workflow technology that can simplify communication and provide security features is a top priority. Canon's strong integration with Box and mxHero****** offers customers powerful, cloud-based capabilities to address many issues that often come with sending and receiving large files, including the need for security features and 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 Box—transforming inboxes from bulky and potentially vulnerable to lightweight and controlled. Box solutions provide users with an array of security features, including the ability to restrict when files can be accessed and by whom.

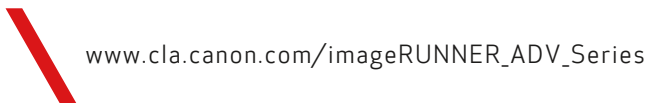| SECURITY FEATURES	Third Generation imageRUNNER ADVANCE (1st, 2nd, and 3rd edition) and imageRUNNER ADVANCE DX models C7500 Series, C5500 Series, C3700 Series, C356iF Series, C475iF Series, 8500 Series, 6500 Series, 4700 Series, 715iF Series
Device Management	
Verify System at Startup	Standard (Third generation imageRUNNER ADVANCE (3rd edition) and imageRUNNER ADVANCE DX models)
McAfee Embedded Control	Standard (Third generation imageRUNNER ADVANCE (3rd edition) and imageRUNNER ADVANCE DX models)
Security Management	
Security Policy Settings	Standard
SIEM Integration	Standard
Authentication	
Active Directory/SSO	Standard
Universal Login Manager	Standard
uniFLOW Online Express	Standard
uniFLOW/uniFLOW Online	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
Hard Drive Password Lock	Standard
Hard Drive Data Format (EOL)	Standard (9x)
Hard Drive Data Erase	Standard
Hard Drive Data Erase Scheduler MEAP	Optional
Hard Drive Data Encryption	Standard (FIPS 140-2 Validated)
Hard Copy and System Security	Optional (IEEE2600 Common Criteria)*
Removable Hard Drive Kit	Optional/NA**
Document Security	
Secure Print (Driver Based)	Standard
Encrypted Secure Print (Driver Based)	Standard: Third Generation imageRUNNER ADVANCE (2nd/3rd edition) and imageRUNNER ADVANCE DX models.***
Secure Print (Server/Cloud)	Optional
Secure Watermark	Standard: Third Generation imageRUNNER ADVANCE (2nd/3rd edition) and imageRUNNER ADVANCE DX models.***
Mail Box Security	Standard
Encrypted PDF (AES 256 support)	Standard: Third Generation imageRUNNER ADVANCE (2nd/3rd edition) and imageRUNNER ADVANCE DX models.***
Device Digital Signature PDF	Standard: Third Generation imageRUNNER ADVANCE (2nd/3rd edition) and imageRUNNER ADVANCE DX models.***
Document Scan Lock	Optional/NA♦
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	
Common Criteria IEEE 2600	Optional*
FIPS 140-2	IPSEC/CAC/PIV/HDD Encryption/TLS

* IEEE 2600 Kits may not be available at the same time of product release; check with your Canon Authorized Dealer for availability.
** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF/C356iF/C475iF Series.
*** Optional on Third Generation imageRUNNER ADVANCE 1st edition models.
♦ Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF/C475iF Series.
  Note: Some features require update to the latest version of the United Firmware Platform.

www.cla.canon.com/imageRUNNER_ADV_Series

Canon

McAfee PROTECTED

CANON GENUINE TONER, CARTRIDGE & PARTS