Five Considerations for MFP Security

Security is one of the top three considerations when procuring printers and Multifunction Printer ("MFP") devices according to Infotrends in their December 2016 "Office Document Technology Security Study & Industry Security Score Card". Your company's information security needs, corporate policies, and IT infrastructure are key considerations when choosing the right MFP.

In today's interconnected world, there is a vital need to help limit data loss, protect against unwanted device use, and mitigate the risk of information networks being compromised. Canon has prepared this document to help in the selection of the right MFP device for your organization's print security requirements by considering the following five information security areas:

1. Managing and Monitoring Access
2. Document and Data Protection
3. Security Policies and Management
4. Network Protection
5. Compliance

Ultimately, it is the responsibility of each organization to select the methods most appropriate for implementing controls to secure its information and network. Canon does not warrant that use of the information contained within this document will prevent malicious attacks, or prevent misuse of your MFP systems. We hope you find the information helpful when thinking about the features an MFP device should have in order to meet your information security needs.

Note:
The security features discussed in this document pertain to third generation imageRUNNER ADVANCE models. Capabilities may vary for previous generations of the imageRUNNER ADVANCE product line.

Managing and Monitoring Access

For many organizations, the foundation for printer and MFP security is implementing a method for controlling device access to only authorized users. Having the capability to restrict user access to specific devices, or only specific functions on network devices, provides flexibility that could also help improve your company's ability to meet its information security needs. Questions to ask when evaluating MFP device security include the following:

- **Does the device have, as a standard feature, an authentication and log-in solution ranging from PIN, picture and PIN, network user name/password or proximity card?** Canon imageRUNNER ADVANCE systems come standard with three server-less authentication features, including Universal Log-in Manager, which can be selected to provide various log-in methods.

- **Can the authentication and log-in solution be easily integrated with Active Directory (AD) and quickly create user and usage reports for audit purposes?** The standard Universal Log-in Manager can be seamlessly integrated with AD and can create reports for audit purposes.

- **Is there the ability to limit user privileges to specific features and functions of the MFP device?** Canon imageRUNNER ADVANCE systems provide an Access Management System (AMS) to provide this level of access control and flexibility.

Document and Data Protection

Having controls in place to protect confidential information could be crucial to help satisfy your contractual and regulatory obligations. A variety of controls should be available to help prevent unclaimed printed documents from sitting openly in the exit tray of the device, to encrypt data in transit to the MFP device, to encrypt data that is stored on the device's internal hard disk drive (HDD) and/or memory, to help protect information on documents scanned and sent from an MFP, and to help protect all passwords, address books, encryption keys and certificates that may be stored on the device. Consider the following questions during your device selection process:

- **Does the device have an embedded serverless Secure Print function that can be centrally implemented and managed by an administrator?** Canon imageRUNNER ADVANCE systems have a standard "Forced Hold" secure print feature. This allows an administrator to centrally enforce and manage secure print policies so users can see and print only their print jobs.

- **When using Secure Print can users be restricted to access and preview only their print jobs, and if needed, change print settings at the MFP user interface?** This can be achieved using the standard "Forced Hold" and one of the standard authentication methods of Canon imageRUNNER ADVANCE systems. Canon's exclusive uniFLOW software option provides additional Secure Print and access options for use across a fleet, with detailed usage reporting for management and audit needs.

- **Does the device support strong encryption for data in transit?** As a standard feature, Canon imageRUNNER ADVANCE systems include IPsec, which encrypts all communication to and from the device when needed. The Encrypted Secure Print option uses AES 256-bit encryption to provide secure transfer of print data to the device.

- **Does the HDD of the MFP device provide standard encryption that is FIPS 140-2 validated and erase capabilities that support DoD standards?** The Canon imageRUNNER ADVANCE systems HDD provides standard encryption capability that is FIPS 140-2 validated and has data erase capabilities that are in compliance with Department of Defense standards. The optional HDD Erase Scheduler can be added to erase data at specific times and can provide a printed confirmation of the data erasure.

- **When sending a PDF does the device allow integration with Adobe® Rights Management to help protect the integrity of the PDF and data, and provide a way to use Digital Signatures that help verify the source and authenticity of the document?** Canon imageRUNNER ADVANCE systems have standard support for Adobe Digital Rights Management. Digital Signature capabilities are optional features of Canon imageRUNNER ADVANCE systems.

- **Is there a way to help prevent printed documents being recopied or scanned and sent to unauthorized persons?** Canon's Document Scan Lock option embeds an encrypted code into hard-copy documents. If a user later tries to copy, scan, or fax one of those hard copies from any networked, compatible imageRUNNER ADVANCE system, the device can respond in a number of ways: asking the user for authentication; locking down the device; and even notifying an administrator about the activity and the identity of the user.

- **Does the MFP device contain a tamper resistant system that helps protect highly sensitive information resident on the device, such as passwords, encryption keys, and certificates?** A standard feature of Canon imageRUNNER ADVANCE systems is the Trusted Platform Module that, when enabled, provides this type of security.

Security Policies and Management

Establishing print security policies could help your company limit access to documents, personal data or confidential information, keeping them from falling into the wrong hands. Print security policies should be easy to implement, centrally managed, exported to print devices across the network, and be monitored with a way to reset settings if security policy changes on a device are observed. Consider the following questions:

- **Does the device have the ability to establish a password protected security administrator area separate from the device administrator?** As a standard feature of the imageRUNNER ADVANCE systems, a dedicated password can be created (separate from the device administrator password) so that only the information security manager has access to modify security settings.

- **Can print security policies be exported and monitored across a fleet and are they able to be reset if a change occurs?** Using Canon's imageWARE Enterprise Management Console (a free downloadable network management utility from Canon) and the Device Configuration Management plug-in, imageRUNNER ADVANCE security settings can be exported across a compatible device fleet, monitored and be set to reapply the policy settings if a change occurs on a device.

- **Is there automatic tracking and logging of actions undertaken by users, developers, and administrators on the MFP device you select?** Canon imageRUNNER ADVANCE systems come with a standard audit log feature that can export logs for auditing purposes to help facilitate compliance with regulations, security standards and enterprise guidelines. These logs can be imported into a SIEM.

- **Is there a way implement a security policy to make documents traceable or provide an alert if they contain sensitive keywords or phrases?** When using Canon's optional uniFLOW software with imageWARE Secure Audit Manager Express, any document that's printed, scanned, copied, or faxed becomes traceable by your IT department. Once an employee authenticates at a device, their documents become digitized and stored as an image record. If specified keywords and phrases are used and identified within a document, IT can be alerted to begin an investigation with a documented audit trail already in place.

Network Protection

Often, networked printer and MFP devices are 'end points' that could be entry points for malicious activity. In general, printer and MFP devices should not be allowed to have an open connection to the internet, should have a private IP address and should always be placed behind a corporate firewall, among other protections. However there are a number of network security features an MFP device should have to help guard against the consequences of unauthorized network intrusions. Consider the answers to the following questions:

- **Does the device include, in its standard configuration, support for IP/MAC address filtering, protocol version selection and the ability to disable unused network ports?** Canon imageRUNNER ADVANCE systems have standard network security features that, when enabled, permit only authorized users and groups to access and print to the device. They can also limit network communications to the device to designated IP/MAC addresses, provide version selection of network protocols such as TLS versions, and can disable unused ports including USB.

- **How is the device protected when it starts up?** During startup, if the BIOS code of an imageRUNNER ADVANCE system is corrupted or missing, the system will not start.

- **How is firmware of the printer/MFP protected?** imageRUNNER ADVANCE system firmware files and updates are digitally signed by Canon Inc. using SHA-256 hashing algorithm. This helps to assure authenticity and only allow Canon files and updates to be downloaded to the device – no executable files are accepted by, or stored on, the device.

- **Does the manufacturer of the device test for vulnerabilities during product development?** Canon uses security consulting companies to test imageRUNNER ADVANCE devices during various phases of the development process.

- **If a new vulnerability threat appears how does the manufacturer of the printer respond and remediate that new threat?** Canon monitors for vulnerabilities and if a new threat appears, has processes in place to investigate the threat, communicate how these vulnerabilities may affect the Canon imageRUNNER ADVANCE system, and provide information on how to address the issue.

Compliance

A good security practice includes partnering with someone who shares your concerns in meeting security and regulatory requirements. A good partner understands the various security requirements of regulations or legislative acts and how security features and functions can be used to help meet those requirements. Consider the following question:

- **Does the partner you are considering view security as important as you do illustrated by their own security approach within their company?** At Canon we understand the need to comply with industry regulations. In our day to day operations, we utilize many of the security features that have been outlined in this paper to help protect information, privacy and confidentiality. We understand the challenges our customers face every day in meeting regulations such as HIPAA, Gramm-Leach-Bliley and SOX, and work hard to ensure what we deliver has the security needs of our customers in mind.

Five Considerations for MFP Security

The above is a small, but important, group of security questions your MFP device provider should be prepared to answer. Canon knows protecting your device, document, data, network – and reputation – is increasingly more important, and difficult, each day. Be sure your provider doesn't focus on just a small subset of security. Canon can help you choose and implement an MFP security strategy for your enterprise. For a view of all the security features, functions and capabilities, both standard and optional for imageRUNNER ADVANCE systems, contact your local Authorized Canon dealer or visit the security section of *usa.canon.com/advancingbusiness*

Canon recognizes the importance of information security and the challenges that your organization faces. This paper provides some of the information security facts for Canon imageRUNNER ADVANCE systems. It provides some details on imageRUNNER ADVANCE security technology for networked and stand-alone environments, as well as an overview of Canon's device architecture, framework and product technologies as related to document and information security. For more information contact your local Authorized Canon imageRUNNER ADVANCE dealer or go to www.usa.canon.com. This paper is primarily intended for those parties involved in creating or reviewing Request for Proposals (RFP) and may be helpful to the administrative personnel of a customer charged with responsibility for the configuration and maintenance of imageRUNNER ADVANCE systems. The imageRUNNER ADVANCE system offers a number of standard and optional capabilities that, when used by a customer, can help facilitate effective management and security of data processed and stored by the system. Ultimately, it is the customer's responsibility to select the method(s) most appropriate for securing their information. Canon does not warrant that use of the information contained within this document will prevent malicious attacks, or prevent misuse of your imageRUNNER ADVANCE systems.

Five Considerations for MFP Security

The information provided in this document is the most current information available at the time of its creation. Canon hereby expressly disclaims all warranties of any kind, express or implied, statutory or non-statutory, in relation to the information provided in this document.

In no event shall Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers be liable for any direct, special, consequential, incidental or indirect damages of any kind (including without limitation loss of profits or data or personal injury), whether or not Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers have been advised of the possibility of such damages, and Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers shall not be liable for any claim against you by a third party arising out of the use or performance of canon's products or information referenced herein.

Regulatory Disclaimer:
Statements made in this document are the opinions of Canon U.S.A. None of these statements should be construed to customers or Canon USA's dealers as legal advice, as Canon U.S.A. does not provide legal counsel or compliance consultancy, including without limitation, Sarbanes Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

Canon
SEE IMPOSSIBLE

1-800-OK Canon
usa.canon.com/advancingbusiness

Canon U.S.A., Inc.
One Canon Park
Melville, NY 11747