# 5 CONSIDERATIONS FOR MFP SECURITY

IT managers across various businesses and industries share a common task of putting measures in place to help secure sensitive business information, customer data, and employee information. These efforts are complicated by the increased threat of cyberattacks that target this information and the requirement to understand and adhere to evolving security regulations that fall across all industries or apply to specific verticals. Add to that the challenges associated with a sharp increase in the number of employees working from home.

While an obvious focus is on securing individual computing devices, cloud services, and corporate networks, there's an often overlooked endpoint to be considered – multifunction printers (MFPs).

Traditional MFPs have progressed to now offer scan-and-send capabilities, network integration, and cloud-based functions. And while these features can contribute toward more efficient workflows, they also have characteristics that may introduce additional security risks.

Canon has identified 5 Considerations for MFP Security to be assessed when making a decision on purchasing and deploying printers:

1. Controlling Access
2. Protecting Information Being Transmitted or Stored
3. Protecting Against Cyber Threats
4. Managing and Monitoring Security Settings and Activity
5. Addressing Regulations and Compliance Efforts

## 1. CONTROLLING ACCESS

MFPs are typically shared by employees within a given department and even across departments. They may also be subject to use by authorized guests and are often located in areas of the workplace where they may be accessed by unwanted users. This makes it important to put measures in place to control access and usage of the device itself, restrict specific functions of the device, and limit the destinations to which information can be transmitted.

When assessing Controlling Access, consider if the MFP provides the ability to do the following:

- Implement authentication/log-in to control device access.
- Set specific access rights for individuals, departments, and guests that meet the needs of each role.
- Set access rights at device level or by individual function (copy, send, etc.).
- Restrict send destinations to help prevent information from being sent to unauthorized recipients.

*Key Canon Features*

- uniFLOW Authentication
- Access Management System (AMS)
- Scan and Send Restrictions (Send to Myself/Limit New Destinations/Domain Specification)

## 2. PROTECTING INFORMATION BEING TRANSMITTED OR STORED

MFPs have evolved to become sophisticated, connected devices that can transmit and receive information over a network, store information, and connect to cloud services. This may include sensitive business information, important client data, or confidential employee details that should be protected from being intercepted by unauthorized parties.

When assessing Protecting Information Being Transmitted or Stored, consider if the MFP has the ability to do the following:

- Encrypt image data before storing to the HDD/SSD, overwrite temporary data after each job, and erase all user data/settings at end of life to help protect confidential information stored on the HDD/SSD.
- Disable unused functions and communication ports to limit vulnerability points.
- Configure communication settings with the latest available protocols to help protect data transmission.
- Encrypt the print data in transit from the user's workstation to the MFP.
- Utilize settings to help limit unattended printed output sitting on the tray.
- Integrate directly with an email security solution to automatically save attachments to cloud storage locations for increased security, access control, and tracking capabilities.

*Key Canon Features*

- HDD/SSD Security Features (Encryption, Erase, Initialize at end of life)
- Port Control
- Protocol Version Selection
- Encrypted Secure Print
- Secure Print (Device-native Forced Hold/uniFLOW Secure Print)

## 3. PROTECTING AGAINST CYBER THREATS

With MFPs being connected to a corporate network, they can become a potential target for hackers attempting to gain access to the device or to use the MFP to gain access to the network and corporate data. It's important to put measures in place that are designed to allow only known, approved firmware and applications to run on the device and to protect against the tampering of firmware and applications. IT management should also have the ability to monitor activity so that they can quickly identify and recover from potential threats.

When assessing Protecting Against Cyber Threats, consider if the MFP has the ability to do the following:

- Verify integrity of boot code, OS, and applications during start-up.
- Utilize whitelisting to help prevent malware execution and protect against tampering of firmware and applications.
- Update firmware on a regular basis across the product line to ensure the latest fixes are implemented and to access updated security enhancements and functions.

*Key Canon Features*

- Verify System at Start-up with Auto Recovery
- Trellix™ Embedded Control
- Unified Firmware Platform

## 4. MANAGING AND MONITORING SECURITY SETTINGS AND ACTIVITY

IT teams are typically managing a fleet of MFP devices. This can be a burden if there aren't proper tools in place to help ensure that security settings can be established with ease, made consistent across devices, and deployed across the fleet. Additionally, it's important to put measures in place to help ensure that these security settings remain configured and notification is provided for attempted changes.

When assessing Managing and Monitoring Security Settings and Activity, consider if the MFP provides the ability to do the following:

- Easily establish print security settings remotely and from a central location.
- Establish a dedicated password to protect these settings. (It should be different from the device administrator's password.)
- Efficiently distribute consistent security settings across multiple devices in the same fleet.
- Monitor print security settings and provide notification of attempted changes.
- Automatically revert back to established security settings if changes are made.
- Integrate with SIEM systems for comprehensive monitoring and notification of suspicious activity.

*Key Canon Features*

- Security Policy Settings (with dedicated password)
- imageWARE Enterprise Management Console (EMC) with DCM Plug-in
- SIEM Integration
- Audit Logs
- Security Settings Navigator

## 5. ADDRESSING REGULATIONS AND COMPLIANCE EFFORTS

In today's digital world, where cyber threats are more prevalent, government regulations compel organizations to meet criteria or risk facing penalties. Responding to regulatory compliance requirements can be complex. And since an organization's sensitive information may be interacting with MFPs, they can become a component of compliance initiatives.

When determining the best office solutions provider for Addressing Regulations and Compliance Efforts, consider the following:

- Align with an office solutions provider with a core interest in, and knowledge of, relevant regulations and standards.
- Consider industry- and government-mandated regulations (such as GDPR, CCPA, HIPAA, Sarbanes-Oxley, PCI, etc.) and their impact on how your organization handles information.
- Leverage a team of dedicated specialists in specific vertical markets and information governance.

In today's connected world, there's no such thing as 100% secure. But a full assessment of these 5 Considerations for MFP Security when selecting and deploying a printer fleet can help to create an environment with protections in place to help limit risk.

When it comes to security, MFPs should be treated just like any endpoint on the network. To achieve that, the MFPs should be equipped with the tools needed to help secure information, protect against threats, comply with organizational security policies, and integrate with network activity monitoring to help users quickly identify and act against potential suspicious activity.

Building a secure system has been a core foundation at the design phase of Canon's imageRUNNER ADVANCE line of MFPs. And, with continuous developments like the incorporation of Trellix Embedded Control and the ability to integrate with an organization's SIEM system, the product line is more protected than ever. Unified Firmware Platform, Canon's common firmware across the third generation imageRUNNER ADVANCE and imageRUNNER ADVANCE DX products, will continue to add value and enhanced security features through updates.

Canon takes the issue of assisting its customers with mitigating their security risks very seriously and is committed to helping organizations create a secure environment for their printers and document workflows. This commitment, when coupled with the strength of its channel partners, can help close the security gaps in today's office environments and equip organizations with the tools and knowledge they need to improve the security of their MFPs.

For more information, visit usa.canon.com/iRADVSecurity, where you'll find tools like the Security Hardening Guide, the Security White Paper, infographics, and brochures.

Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws. Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21, or the USA Patriot Act; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Individuals and organizations should also perform their own research and conduct their own due diligence concerning the products and suggestions discussed in this white paper. Some security features may impact functionality/performance; you may want to test these settings in your environment. Third-party SIEM system required. Subject to third-party SIEM system terms and conditions. Canon cannot ensure compatibility with all third-party SIEM systems. The Verify System at Startup and Trellix Embedded Control functions are set to [Off] by default. It can be turned on by an administrator in Settings/Registration. When this function is set to ON, device startup will increase by 20-40 seconds (depending on the model). Recovery from Sleep Mode is not affected. Canon U.S.A. does not make any warranties concerning the accuracy or completeness of the opinions, data, and other information contained in this content and, as such, assumes no liability for any errors, omissions, or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data, or other information. Canon is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. Trellix and the Trellix logo are trademarks or registered trademarks of Musarubra US LLC or its subsidiaries in the U.S. and other countries. All other referenced product names and marks are trademarks of their respective owners. All features presented in this document may not apply to all Series and/or products and may be optional; please check with your Canon Authorized Dealer for details. Specifications and availability are subject to change without notice. Not responsible for typographical errors.
©2023 Canon U.S.A., Inc. All rights reserved.

12/23-0471-7958

Canon

usa.canon.com

Trellix