Canon

THE 5 PILLARS OF SECURITY

The Importance of Printer and MFP Security Settings and Features

Introduction

The security of printers and multifunction printers (MFPs) has become as critical as securing computers and other network devices. Printers and MFPs, like the Canon imageFORCE series, are no longer just simple output devices; they are sophisticated endpoints that process, store, and transmit sensitive information. Therefore, robust security settings and features are essential to help protect against data breaches, unauthorized access, and cyber threats.

Security Market Overview

Modern printers and MFPs are designed with components like general-purpose PCs, including memory, CPUs, and hard disks, often running on mainstream operating systems like Windows. This similarity necessitates a comprehensive security strategy that covers all network-connected devices, including printers and MFPs, to help prevent data theft, intellectual property loss, and malware infections.

Device Security

Authentication

Authentication mechanisms are crucial for controlling access to printers and MFPs. Canon's devices offer various authentication methods, including:

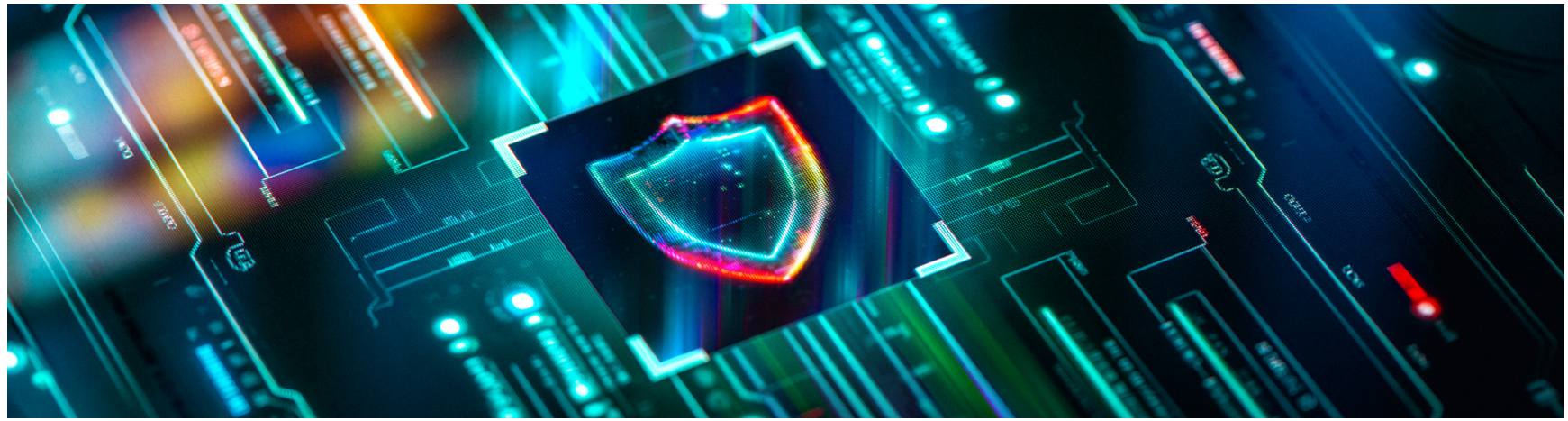
- **Department ID Mode:** Limits device access based on department IDs and passwords, restricting functionality by user role.
- **eULM:** A server-less login application supporting card log-in, PIN codes, and user credentials.
- **uniFLOW:** A print management solution that helps to enhance security by integrating with RFID cards and PIN codes, supporting various authentication technologies.

Password Protection

Password-protected system settings restrict unauthorized changes to device configurations, network settings, and printing protocols. Canon recommends setting an administrator password during installation to help secure critical device settings.

Verify System at Startup

This feature checks the system and applications for tampering during startup, using cryptographic technologies for verification. If tampering is detected, it will restart and replace the firmware with a known good "Gold Master" of the device's system software and continue to restart.



Information Security

Document Storage and Handling

Canon's imageFORCE devices use short-term memory for storing print jobs, automatically deleting data after job completion, power shutdown, or timeout, helping to minimize the risk of data loss.

Encrypted PDFs and Digital Signatures

To secure documents, Canon devices support encrypted PDFs and digital signatures. Encrypted PDFs require a password to access, while digital signatures verify the source and authenticity of the document.

Secure Printing

Secured Print holds print jobs in queue until the user enters a password at the device, ensuring that documents are not left unattended. Canon's uniFLOW software helps to further enhance secure printing by holding jobs at the server until released by the authenticated user at any compatible device.

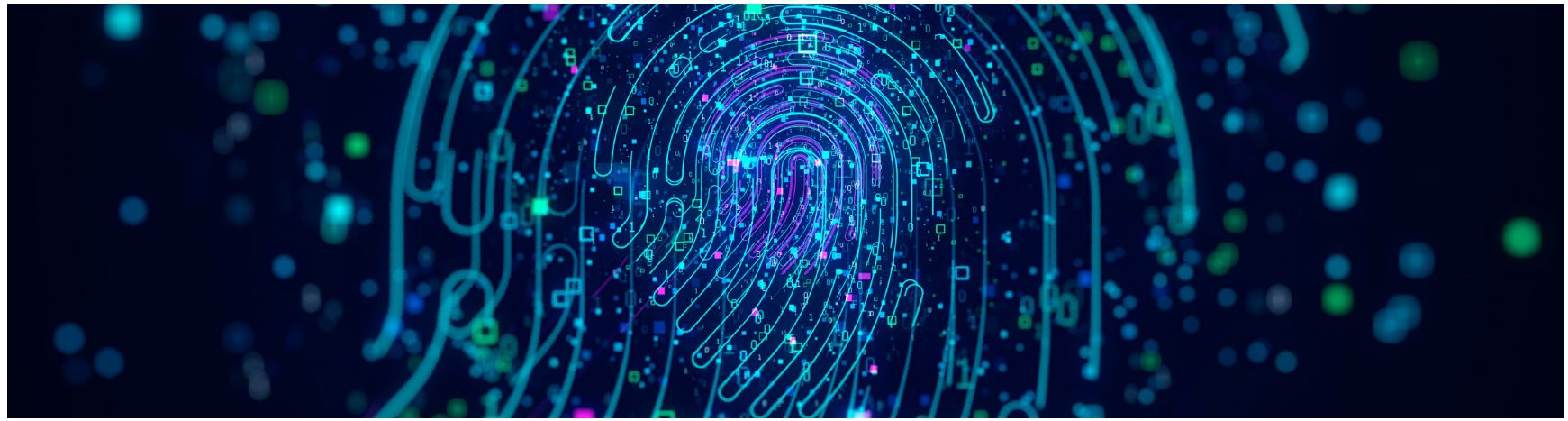
Network Security

Protocol and Port Management

Canon devices allow administrators to enable or disable specific protocols and service ports, blocking unwanted communication and system access. Configurable ports include LPD, RAW, SMB, FTP, HTTP (IPP), and more, with the ability to disable unused TCP/IP ports for added security.

IP and MAC Address Filtering

Administrators can permit or reject access based on IP and MAC addresses. IP filtering allows for the specification of up to 16 individual addresses or ranges, controlling access to various applications like LPD, SMB, and FTP. MAC address filtering is particularly useful in DHCP environments to manage access based on hardware addresses.



Advanced Security Features

Trellix™ Embedded Control

This feature uses whitelisting to help prevent the execution of unrecognized malware and tampering of existing firmware and applications. By ensuring that only verified applications and firmware can run, Trellix Embedded Control helps protect against cyber threats.

Security Information and Event Management (SIEM) Integration

SIEM systems collect and analyze machine data across the IT environment, providing real-time indicators of potential security violations. Canon devices can be configured to send audit logs to SIEM systems using the Syslog protocol, integrating printers into comprehensive security monitoring.

Conclusion

Securing printers and MFPs is a critical aspect of modern IT security strategies. Canon's imageFORCE series offer a comprehensive suite of security features that help protect against unauthorized access, data breaches, and cyber threats. By implementing robust authentication methods, encrypted document handling, secure printing, and integrating with SIEM systems, organizations can support the security and integrity of their information.

Ensuring the security of printers and MFPs not only helps to protect sensitive information but also assists organizations in complying with regulatory requirements and maintaining the trust of their stakeholders. As cyber threats continue to evolve, it is essential to stay vigilant and keep security settings and features up to date to help safeguard against potential risks.

For more information about Canon U.S.A.'s Five Pillars of Security, our comprehensive approach to cybersecurity, contact us today.

THE 5 PILLARS OF SECURITY

- DEVICE SECURITY
- DOCUMENT SECURITY
- PRINT SECURITY
- CYBERSECURITY
- INFORMATION SECURITY

Canon U.S.A.'s Five Pillars of Security presents a portfolio of cybersecurity products and services in a comprehensive way that groups solutions in functional areas. Device Security is a key component of our Five Pillar approach.

Canon

1-844-50-CANON | usa.canon.com/security

05.22.25/25-0207-11810