Canon

ARE YOU CONFIDENT YOUR OFFICE PRINTER HAS SECURITY FEATURES THAT CAN **PROTECT YOUR SENSITIVE DATA?**

AVERAGE HEALTHCARE DATA BREACH COST ACROSS 17 COUNTRIES = **OVER $10 MILLION**[1]

HEALTHCARE INFORMATION PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) FINE = **$100 TO $50,000 PER VIOLATION (OR RECORD)**[2]

Healthcare providers of all sizes can't afford the financial and reputational costs related to compromised data. While larger hospitals and health systems may have greater access to cybersecurity professionals, non-acute or independent facilities may be challenged to keep on top of monitoring, detecting, and mitigating risk. This is further exacerbated if practice managers and clinical staff are dealing with legacy systems.

While endpoints such as laptops, tablets, desktop computers, and even mobile phones are generally updated with patches and security enhancements designed to help limit risk and protect valuable data in healthcare settings, networked office multifunction printers (MFPs) may be overlooked and not necessarily integrated into regular cybersecurity monitoring.

MFPS CAN BE USED TO ACCESS VALUABLE CREDENTIALS, SENSITIVE DATA, AND PROPRIETARY INFORMATION IN SEVERAL WAYS

Configuration Changes: MFPs digitize and route data to multiple destinations; these can be manipulated to send information to unauthorized recipients.

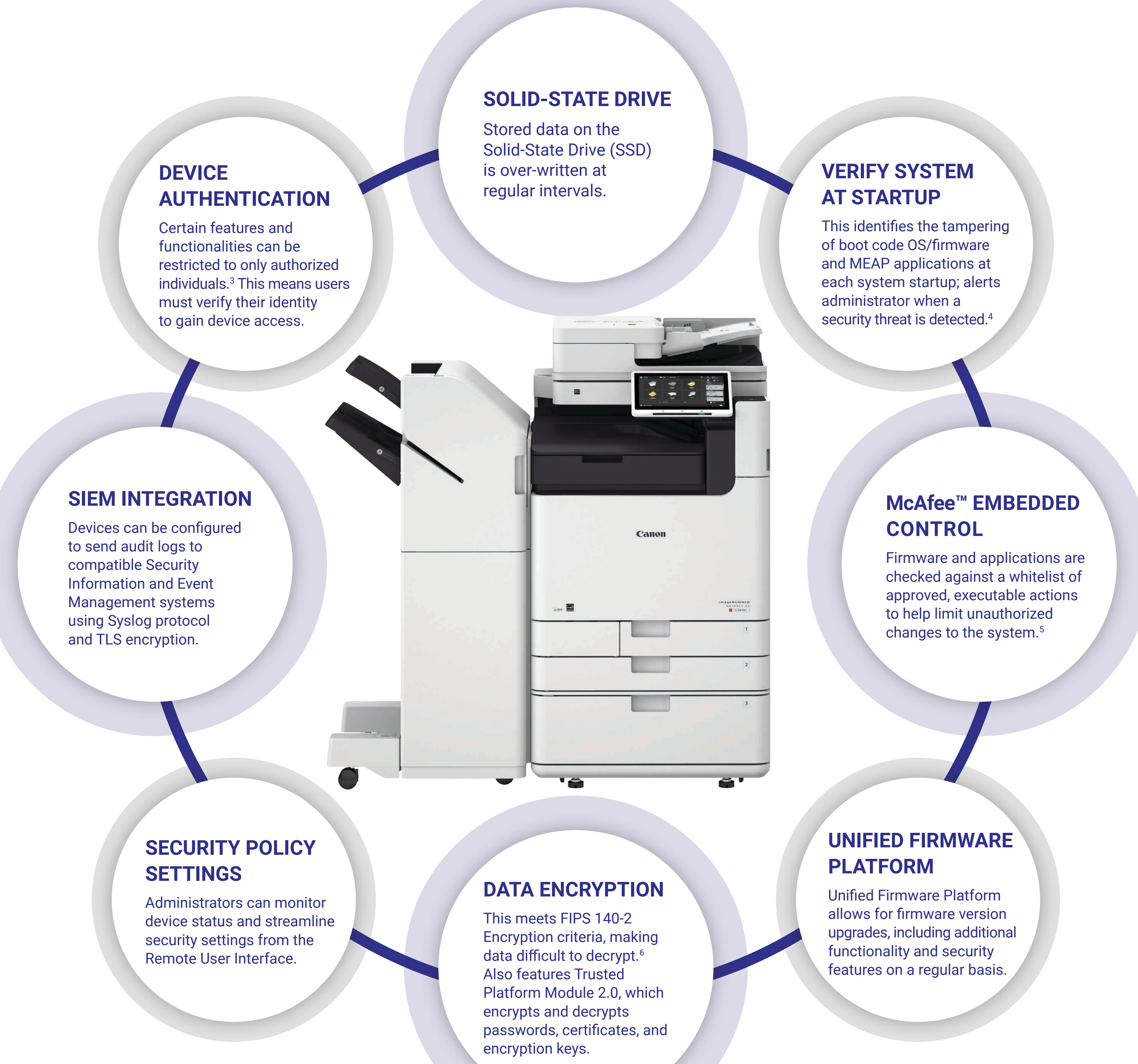
Disk and Media Storage: Scanned images stored on MFP hard disks can potentially be accessed if not adequately protected and regularly erased.

BIOS and Firmware: Malicious actors can hack into firmware and access other applications, execute harmful code, or shut down multiple systems to launch a denial-of-service attack that requires ransom payment.

Unattended Output Trays: Leaving documents unattended in MFP output trays can mean that anyone can pick up and view sensitive documents.

Cloud/Wireless Printing: Printing on misconfigured or exposed wireless and cloud infrastructure can leave sensitive information susceptible to middleman attacks or system intrusion attempts.

SECURITY FEATURES ON CANON imageRUNNER ADVANCE DX AND imagePRESS LITE MODELS CAN HELP SUPPORT ESTABLISHED CYBERSECURITY GOALS



SOLID-STATE DRIVE
Stored data on the Solid-State Drive (SSD) is over-written at regular intervals.

DEVICE AUTHENTICATION
Certain features and functionalities can be restricted to only authorized individuals.[3] This means users must verify their identity to gain device access.

VERIFY SYSTEM AT STARTUP
This identifies the tampering of boot code OS/firmware and MEAP applications at each system startup; alerts administrator when a security threat is detected.[4]

SIEM INTEGRATION
Devices can be configured to send audit logs to compatible Security Information and Event Management systems using Syslog protocol and TLS encryption.

McAfee™ EMBEDDED CONTROL
Firmware and applications are checked against a whitelist of approved, executable actions to help limit unauthorized changes to the system.[5]

SECURITY POLICY SETTINGS
Administrators can monitor device status and streamline security settings from the Remote User Interface.

DATA ENCRYPTION
This meets FIPS 140-2 Encryption criteria, making data difficult to decrypt.[6] Also features Trusted Platform Module 2.0, which encrypts and decrypts passwords, certificates, and encryption keys.

UNIFIED FIRMWARE PLATFORM
Unified Firmware Platform allows for firmware version upgrades, including additional functionality and security features on a regular basis.

imageRUNNER ADVANCE DX C5870i shown with optional accessories.

- ✓ Canon imageRUNNER ADVANCE DX devices feature a Security Settings Navigator that prompts users to answer a series of questions to determine device security settings that may be suited to a specific environment.
- ✓ Canon imageRUNNER ADVANCE DX devices have certain functionality and features that can support customers in their efforts to implement the NIST Cybersecurity Framework.
- ✓ Additional fleet management and output management software can be added to Canon imageRUNNER ADVANCE DX devices as part of Canon's FedRAMP-authorized cloud solution, Canon Office Cloud.

Contact your Canon Authorized dealer to learn more about the full range of security options available through the Canon imageRUNNER ADVANCE DX and imagePRESS Lite devices.

[1] Ponemon Institute, "The Cost of a Data Breach Report 2022," IBM Security, 2022. www.ibm.com/downloads/cas/3R8N1DZJ

[2] HIPAA Journal, *"What are the Penalties for HIPAA Violations?"* HIPAA Journal, 2023. www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

[3] Optional uniFLOW software is available for cloud-based authentication, document scanning, tracking, and more.

[4] Verify System at Startup needs to be set to "ON." Automatic recovery available on 2023 models to support organizations in their efforts to meet industry guidelines for system self-resilience; if tampering is detected, the system automatically overwrites and continues booting instead of entering an error mode to prompt a service call.

[5] The McAfee Embedded Control function is 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.

[6] FIPS 140-3 validation is pending.

Canon

PREMIER®
Contracted Supplier

usa.canon.com/healthcare

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. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. 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; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Third-party SIEM system required. Subject to third-party SIEM system's Terms and Conditions. Canon cannot ensure compatibility with all third-party SIEM systems.

As an ENERGY STAR® Partner, Canon U.S.A., Inc. has certified these models as meeting the ENERGY STAR energy efficiency criteria through an EPA recognized certification body. ENERGY STAR and the ENERGY STAR mark are registered U.S. marks. Canon, imageRUNNER, and imagePRESS are registered trademarks or trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. uniFLOW is a registered trademark of NT-ware Systemprogrammierung GmbH. McAfee is a trademark of McAfee LLC in the US and/or other countries. All other referenced product names and marks are trademarks of their respective owners. All screen images may be simulated. All features presented in this brochure may not apply to all Series and/or products and may be optional; please check with your Canon Authorized Dealer for details. Products shown with optional accessories. Specifications and availability subject to change without notice. Not responsible for typographical errors.

09/23-1398