imageRUNNER
ADVANCE DX

Canon's Award-Winning imageRUNNER ADVANCE DX Devices Can Help Support Your Campus Zero Trust Efforts

Zero Trust security frameworks continue to gain momentum as a best practice in attempting to combat cybersecurity threats. Zero Trust is a strategy that organizations can implement where the permitted access of every user and networked device is continuously verified.

Explore some of the security features offered by Canon's imageRUNNER ADVANCE DX devices and see how they can help support your security efforts. Discover why including your print environment in a Zero Trust strategy can help you to foster trust from the end user to the device as well as the applications and data that reside on it.

Authentication and Access Control

Help Limit User Access

Canon's imageRUNNER ADVANCE DX systems include several authentication options designed to help administrators set up their devices so that only approved users can access the device and its functions, such as the print, copy, scan, and send.

Enabling solutions, such as uniFLOW, can help administrators restrict access to the entire device or just specific functions (e.g., Send-to-Email) while leaving other applications available for general use. Additionally, the standard Access Management System allows administrators to limit device and application features based on the user's role within the organization, supporting context-based access. Roles can be created using a variety of parameters, such as job title, responsibilities, group, or work location, enabling administrators to achieve granular, context-based authentication permissions.

With the uniFLOW software, users of an imageRUNNER ADVANCE DX device are able to authenticate through a variety of methods, including PIN, username/password, contactless cards, chip cards, magnetic cards, or government-issued CAC/PIV or SIPR cards (separate purchase of cards required).

Education institutions interested in adopting a cloud strategy can look to Canon Office Cloud,* a FedRAMP-authorized service. Canon Office Cloud and its uniFLOW Online service also support flexible authentication, including CAC/PIV/SIPR. Canon Office Cloud helps to deliver advanced, cloud-based, print management solutions that adhere to the FedRAMP standards—the federal government's rigorous security compliance framework for cloud-based services and data security.

Device Management and Monitoring

Integrity of Attached Devices

Inherent in imageRUNNER ADVANCE DX models is the ability for administrators to configure a range of security settings to help with an education environment's Zero Trust strategy. Administrators can use Canon's imageWARE Enterprise Management Console (EMC) to centrally manage aspects of their compatible Canon device fleet such as inventory, location, device settings and configuration, alerts, and reporting. Additionally, Canon's FedRAMP-authorized Canon Office Cloud offers Netaphor SiteAudit for a device management solution and service security reporting solution via a cloud-based service.

Security features to help protect against malware/firmware tampering are also available for users to implement in imageRUNNER ADVANCE DX devices. If implemented and turned on, these features protect against installation or execution of programs without a digital signature applied by Canon. These protections apply to updating firmware, executing processes, and activating embedded MEAP applications.

Canon imageRUNNER ADVANCE DX devices Verify System at Startup, a solution that verifies the integrity and validity of the system software at startup once turned on. The platform features also includes a Protect Runtime System function, which monitors software changes at runtime to limit unauthorized alterations, and SIEM (Security Information and Event Management) integration, so organizations can bring print devices into a larger event monitoring structure.

* Canon Office Cloud is available to qualified customers, including federal, state, local, territorial, and tribal government agencies as well as other non-government entities subject to federal data handling regulations.

Administrators can also activate the McAfee Embedded Control technology as a countermeasure for malware. This technology uses an "allow" list (whitelist) to permit only trusted applications to run in the system and help limit unauthorized system changes. To further enhance imageRUNNER ADVANCE DX devices' security, education institutions are given the ability to separate the administration of security features and the device. Using this approach, device functions can be segmented by role, thereby denying administrators automatic access to security settings while helping to support granular, role-based network security.

Network/Environment

Helping to Safeguard Network Communications

To help protect important data and information, Canon's imageRUNNER ADVANCE DX devices provide various measures for helping education institutions with their network security efforts. Network administrators are provided with the ability to configure the specific device protocols and service ports that are accessible.

Administrators can configure the firewall settings of a Canon imageRUNNER ADVANCE DX device to help limit unauthorized access by third parties as well as network attacks and intrusions. This is done by allowing communication only with those devices having a specific IP address. Administrators can also be notified if networking configurations change from the baseline via tools such as Netaphor SiteAudit.

Application Development

Helping to Include Security Features in Custom Applications

End users will often require embedded applications, known as MEAP applications, to provide additional workflow-specific functionality or connections.

Access to the Software Development Kit for MEAP is restricted by Canon and controlled through licensing. Canon's MEAP applications are digitally signed with a special, encrypted signature to help protect the integrity of the application. If the application is modified in any way, the signature code will not match and the application will not be permitted to run on the device.

Canon Office Cloud is Canon's FedRAMP-authorized service platform focused on Managed Print Services. Receiving an Authority to Operate (ATO) means that Canon has met relevant FedRAMP security, process, and monitoring requirements and is authorized to operate this cloud solution with active customers. These requirements include software development best practices, code analysis, security assessments, penetration testing, ongoing system security plans, and regular audits.

Data and Documents

Helping Information Stay Ahead

To help protect your sensitive and confidential information, Canon imageRUNNER ADVANCE DX systems include a standard, solid-state drive (SSD) format utility as well as more advanced features such as SSD Data Encryption (FIPS 140-2, 256 AES). Each device provides a Trusted Platform Module (TPM) and an SSD lock that helps protect the SSD with a password, thus making it difficult to access the data that is on the storage device.

To help limit information from becoming compromised, Canon has built in many controls such as Secure Print, scan destination restrictions, document digital signatures, and PDF encryption, to name a few.

The Canon Office Cloud solution secure print and destination restrictions (Scan to Self, network folder, FedRAMP-authorized version of Box, Google Drive, and Microsoft OneDrive, Exchange, and Teams).

Summary

When planning your Zero Trust strategy, consider print devices, embedded software, and services as you build a comprehensive security approach to data, documents, and networked environments. With a long history of advanced print security solutions, Canon's technologies can help you include print and document management in your Zero Trust strategy.

Learn more about imageRUNNER ADVANCE DX security by visiting usa.canon.com/simplyadvanced.

Learn more about Canon Office Cloud by visiting usa.canon.com/officecloud.

For more information, visit **usa.canon.com**.

The authors of this content are not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the products and suggestions discussed herein. Canon U.S.A., Inc. 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, imageRUNNER, and MEAP are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. All other referenced product names and marks are trademarks of their respective owners. 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. Specifications and availability subject to change without notice.
Not responsible for typographical errors.
©2023 Canon U.S.A., Inc. All rights reserved.

09/23-0997-8481

Canon

usa.canon.com