CANON SOLUTIONS AMERICA

CANON SEE IMPOSSIBLE

ADVANCED SECURITY SOLUTIONS FOR LEGAL PROFESSIONALS

Solutions that address the security challenges facing today's law firms.

Law practices are facing a technology crossroads when it comes to information governance, compliance, and security. Is your firm ready to turn challenges into competitive advantages? Canon Solutions America can help your firm navigate the evolving regulatory landscape while safeguarding sensitive client information.

ENSURING SECURITY AND CONFIDENTIALITY OF CLIENT INFORMATION

Trust is implicit in attorney-client privilege. Sensitive content moves in many directions as it passes through legal workflows. What would the real cost be to your firm if there were a security breach? Ensuring that each link is secured can be daunting unless you collaborate with an organization like Canon Solutions America that understands that security needs to be a multi-layered approach.

Device Security

CONTROLLER SECURITY

Security starts with hardware. The Canon imageRUNNER ADVANCE series operating system is powered by an embedded version of Linux that has been hardened to remove all unnecessary drivers and services that are not essential to the operation of the device. The configuration of this system, coupled with rigorous vulnerability testing, helps our devices meet or exceed your law firm's security requirements.

AUTHORIZED ACCESS

Unrestricted access to functions like copy, scan, and print can be a risk to sensitive client information. With Canon's standard Access Management System, only authorized users have access to these functions. Law firms can configure user roles based on predetermined user rights—for example, an attorney may have access to specific device functions such as copy or fax, while paralegals can only access stored forms on the device. The imageRUNNER ADVANCE series offers multiple ways to authenticate users at the device.

TAMPER DETECTION FEATURES

The imageRUNNER ADVANCE series features the Verify System at Startup function, which runs a process during startup to verify that no tampering of the system BIOS, firmware, or MEAP applications has occurred. If a suspicious program is detected, the system will not start.

McAfee PROTECTED

McAFEE EMBEDDED CONTROL

Canon has included McAfee Embedded Control as an additional standard security feature on all Third Generation imageRUNNER ADVANCE Third Edition multifunction printers. McAfee Embedded Control helps protect against zero-day and advanced persistent threat (APT) attacks by blocking the execution of unauthorized applications through intelligent whitelisting. This helps reduce your firm's risk of exposure to sophisticated malware such as worms, viruses, and Trojans. It also helps ensure that only Canon-approved, authorized updates can be implemented within the supported imageRUNNER ADVANCE system.

Print Security

Sensitive client documents are often sent and received via copy, print, scan, and fax. Law practices have a responsibility to their clients to ensure that confidentiality, integrity, and availability are maintained at each point.

CHALLENGES	ADVANCED SOLUTIONS
Print	
• Sensitive materials left on output tray • No record of who printed the document. • Sensitive materials leaving the firm.	• Secure print allows print jobs to be held at the device until authorized personnel release the print materials with a password or access card. • Forced hold printing allows IT administrators to enforce secure print for all or select users.
Copy	
• Unrestricted copying can allow sensitive content to leave without a trace.	• Discourage unauthorized copying by embedding secure watermark on unauthorized copy jobs.
Scan	
• Users scanning documents to email. • Diverse scan destinations result in information management chaos. • Lack of controls limits accountability.	• Optional Document Scan Lock & Tracking feature embeds a hidden tracking code on documents restricting ability to copy, scan, send, or fax jobs.

Document Security

When client documents are copied, scanned, printed, or faxed, image data lives on the hard drive of the device. Canon Solutions America offers a variety of solutions to help ensure that the security of copy, print, scan, and fax data on your hard disk drive (HDD) is protected daily and at end-of-life.

The **standard HDD** format provides up to **9x** overwrite. All case files that were stored on the device are erased at end-of-life.

The **standard HDD Data Erase Kit** helps ensure that sensitive data is deleted daily and properly erased with standard format overwriting **(up to 3x)** as part of routine job processing.

The optional **HDD Data Encryption Kit** uses AES 256-bit encryption to help protect all case files stored on the internal hard drive.

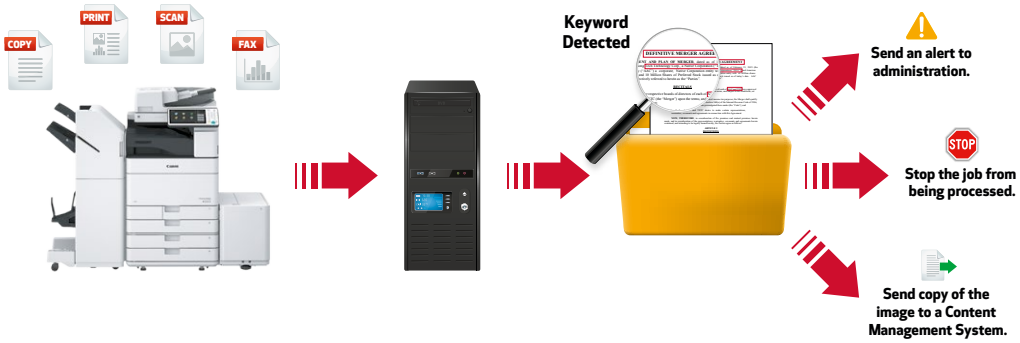
The **HDD Data Erase Scheduler** MEAP application enables you to set devices to automatically erase all copy, scan, print, and other activity data from hard drives on a set schedule.

A tamper-resistant security chip, the **Trusted Platform Module (TPM)** protects information on the internal hard disk drive by encrypting and decrypting information including passwords, certificates, IDs, and cryptographic keys. If the TPM chip is removed, the device will not launch.

HDD Password Lock secures the HDD with a password, making it difficult to access the data even if the HDD is physically removed from the imageRUNNER ADVANCE device.

Network Security

Many law firms require additional security to support the demands of federal regulations such as HIPAA, Sarbanes-Oxley, Patriot Act, Federal Rules of Civil Procedure, GDPR, and other statutes. uniFLOW and imageWARE SAM Express can help. Firms can easily monitor every client document that's scanned, copied, or printed on the imageRUNNER ADVANCE platform. If discrepancies are found, the system automatically logs it and sends it to the appropriate parties.



CERTIFICATE ISSUE REQUEST FUNCTION

The imageRUNNER ADVANCE series saves time and effort by allowing legal technologists to process the certificate issue request function remotely and automatically for many devices. On a regular basis, determined by the IT Administrator, the device sends a certificate issue request to the Simple Certificate Enrollment Protocol (SCEP) server, receives a certificate, and registers it to the device.

IP + PORT FILTERING

With the right configuration, a law firm's firewall should prevent direct external access to multifunction devices and guard against malware and viruses. As an extra precaution, the imageRUNNER ADVANCE series offers IP address and port filtering, which limits network access to specific IP addresses or ranges as part of a holistic protection plan.

VIRUS CONTROL

imageRUNNER ADVANCE systems with Scan and Send capabilities support POP3 and SMTP as email reception protocols. When data is received, the device will always discard any attached viruses in client and other third-party email messages upon receipt.

Cybersecurity

Canon Solutions America provides several tools to help law firms enforce their internal policies and meet regulatory requirements. Whether a single imageRUNNER ADVANCE system is deployed or a fleet of them, these solutions provide the ability to monitor and audit usage and limit access to features and functions at the group and user-level.

Canon myCSA
Secure Account Management

DEVICE MANAGEMENT

Canon Solutions America provides multiple ways to manage fleets more effectively. Through the online self-service portal **myCSA.com**, office administrators can monitor meter reads, order supplies, and handle service issues. Each imageRUNNER ADVANCE device sports imageWARE Remote, an embedded remote diagnostic system that communicates securely only with a Canon server. Law firms can also manage large fleets using the complimentary imageWARE Enterprise Management Console software, which allows administrators to troubleshoot, identify unauthorized access, update user credentials, and perform other tasks to ensure device integrity.

SIEM INTEGRATION

An audit log is a chronological sequence of audit records that automatically tracks every action undertaken by users, developers, and administrators through a SIEM (System Information Event Management) system. All newly released Third Generation imageRUNNER ADVANCE Third Edition devices offer the ability to automatically generate syslogs to your SIEM and log any security incidents involving imageRUNNER ADVANCE devices.

VIRTUAL CISO

There is no fool-proof security solution, but there are best practices that can help law practices establish a stronger security posture. The Agile Cybersecurity Solutions (ACS) Virtual CISO program can offer your firm a full range of services, including training, risk management guidance, general consulting options such as GDPR prep, security policy and procedure development and management, and in the unfortunate event of a breach, just-in-time incident response that can help to minimize the damage.

ACS
agile cybersecurity solutions

CYBERSECURITY INTEGRITY AUDIT

The Cybersecurity Integrity Audit can be an important first step in fully understanding how effective your security posture is in protecting you from outsider threats. With three comprehensive vulnerability assessments and penetration testing options, your law firm will gain insight into any gaps in your security infrastructure that need attention. Performed by ACS, you can rely on these top flight security practitioners to provide a thorough overview of the state of your firm's security.

For more information about Canon Solutions America security offerings or to learn more about the imageRUNNER ADVANCE series for Legal visit csa.canon.com

Canon
CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM

7/19-635-3474