Canon

THE 5 PILLARS OF SECURITY

SECURITY SOLUTIONS AND SERVICES

A multi-layered approach to help protect your organization

OUR MISSION

Securing your workplace has never been more important than it is today. Establishing and maintaining a security posture that adequately balances risk and business productivity is top of mind for many business leaders.

Our mission is to offer our customers solutions and services that can help enable business growth, provide improvements in productivity and efficiency, and protect information as it flows both inside and outside of an organization.

FIVE PILLARS OF SECURITY

Security is not a destination, it is a journey—through a multi-dimensional threat environment that can compromise your information from many different sources. On any given day, information flows throughout your organization through the hands of employees who have varying degrees of risk awareness, while threats from the outside remain pervasive. Consequently, Canon U.S.A. approaches security through a holistic, multi-layered approach, comprising five key pillars.

DEVICE SECURITY

- Authentication
- Role-based Access
- HD Overwrite
- HD Encryption
- Network & Protocol

DOCUMENT SECURITY

- Secure storage
- Encryption
- Role-based access
- Copy-lock

CYBERSECURITY

- Consultation
- Assessments
- Penetration testing
- MDRaaS
- PFCaaS
- Virtual CISO
- Training & awareness

PRINT SECURITY

- Authentication
- Pull printing
- Encryption *(in transit and at rest)*
- Auditing

INFORMATION SECURITY

- File encryption
- Access control
- Tracking & auditing
- Data loss prevention

DEVICE SECURITY

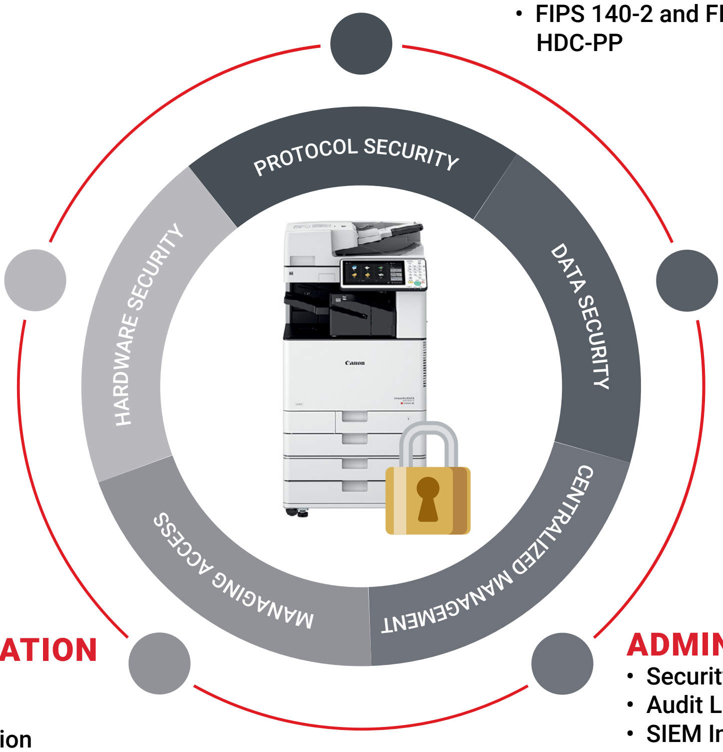
WHAT ABOUT PRINTERS AND MFDS? PRINTERS AND MULTIFUNCTIONAL DEVICES ARE OFTEN OVERLOOKED.

Canon’s imageRUNNER ADVANCE third generation devices all come equipped with the ability to “harden” the configuration to help lessen the chances of being an attack surface for malicious actors. Our National Consulting Services (NCS) organization is prepared to assist our customers’ IT personnel and administrators to harden their endpoint devices.

For more information about device hardening, please visit Canon U.S.A.’s Security Solutions and Services website at *usa.canon.com/security* and view the Canon imageRUNNER ADVANCE white paper and hardening guides.

DEVICE HARDENING

- SNMP
- SSL/TLS
- Certificates
- Network & Web
- FIPS 140-2 and FIPS 140-3 HDC-PP



DATA AT REST

- Trusted Platform Module (TPM)
- SSD Drives
- SSD Encryption
- SSD Erase
- Startup Verification
- Runtime Intrusion Detection

DATA IN TRANSIT

- Encrypted PDF
- SSL/TLS Encryption
- IPSec Support
- Wireless LAN/IEEE 802.1

AUTHENTICATION

- Device Based
- Card Based
- User Authorization
- AD/LDAP

ADMINISTRATOR CONTROL

- Security Policy Management
- Audit Logging
- SIEM Integration with Syslog Protocols RFC5424 & RFC5426
- Auto Certificate Update

YOU CANNOT MANAGE WHAT YOU CANNOT SEE

CYBERCRIMINALS INVEST THEMSELVES IN PERSISTENT EXPLOITS IN SEARCH OF CONFIDENTIAL DATA AND INTELLECTUAL PROPERTY.

Your security and IT teams need to have visibility into the infrastructure to stay aware of any perimeter and endpoint security failures or anomalies that may indicate malicious activity. Deploying a security information event management (SIEM) system can help to aggregate security data from across your organization, assist security teams with detecting and responding to security incidents, and create compliance and regulatory reports about security-related events.

DOCUMENTS LEFT ON PRINTER

UNAUTHORIZED REPRODUCTION

PRINTED DOCUMENTS LEAVE A TRAIL

AGILE STAFF DESKING

DOCUMENTS IN THE RECYCLE BIN

UNSECURED PERSONAL PRINTERS

PRINT SECURITY

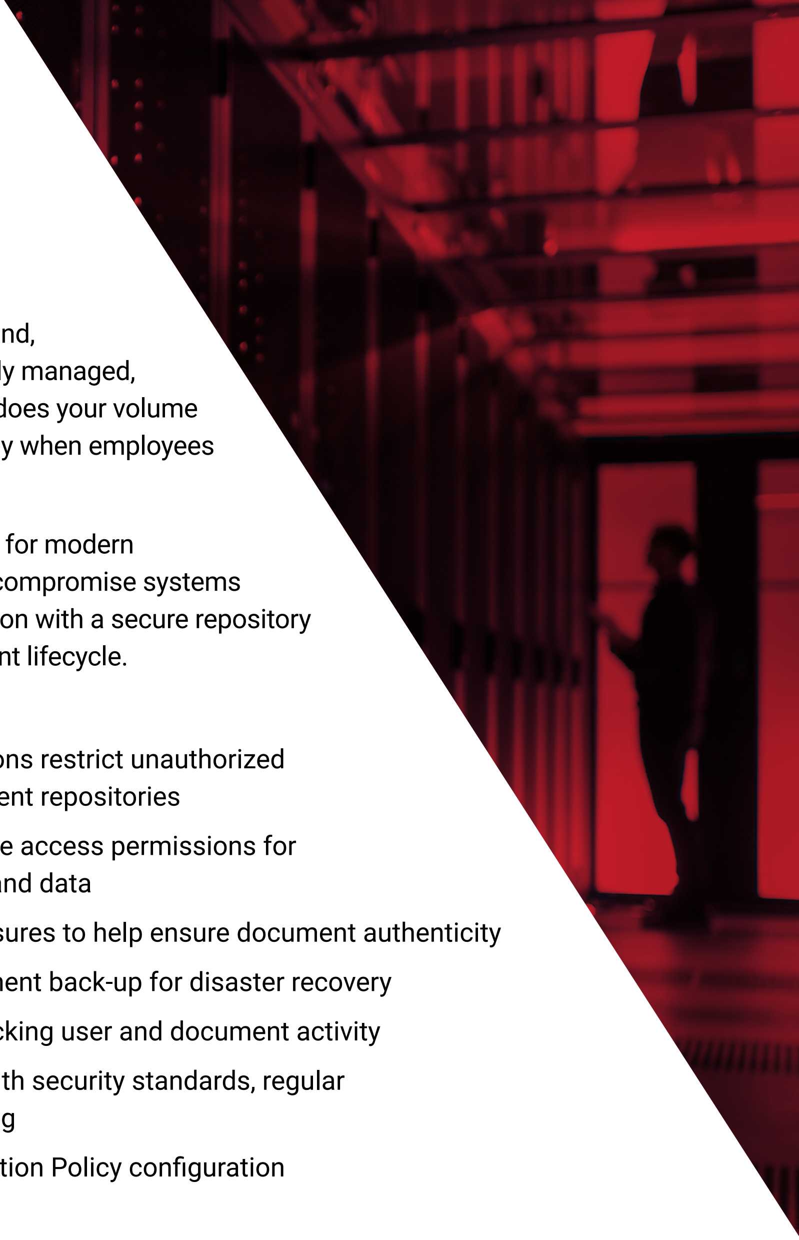
Much of the data that moves throughout organizations is still paper-based. The next logical progression after securing printers and a multifunctional device fleet is to secure the output of those devices. Closing security gaps in your printing and imaging environment is an important piece of your overall security strategy. There are key features and functionality embedded in many print management solutions that can aid you in your security journey.

- User Authentication
- Pull Printing
- Watermarking
- Auditing
- Device Personalization

UNAUTHORIZED REPRODUCTION SECURITY

As production printing migrates more and more from traditional analog offset print processes into the world of digital high speed variable print processes, so must the security features used to secure crucial hard copy documents and documents with intrinsic value. Whether you need to prevent altering or copying and pasting from a digital document, or photocopying a hardcopy original, the need for protection is paramount.

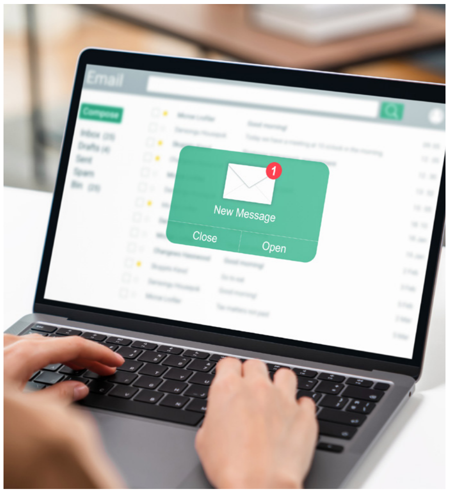
If you are a service provider, you can help address your clients' concerns by demonstrating your ability to offer a variety of solutions to help protect their intellectual property and sensitive data.



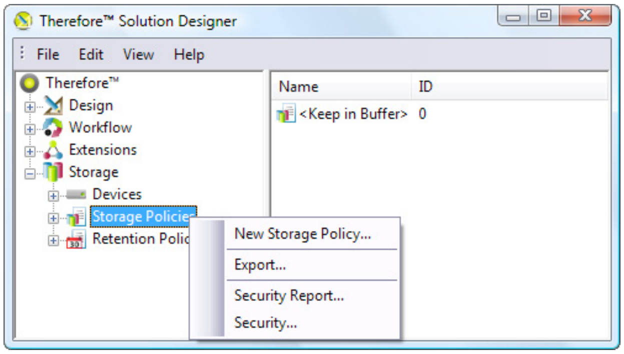
DOCUMENT SECURITY

Information is one of your organization's most valuable assets and, as with any asset, it should be thoroughly protected, meticulously managed, and easily accessible. However, as your organization grows, so does your volume of information. This can quickly become cumbersome, especially when employees apply their own disparate filing methods.

Protecting sensitive data both in transit and at rest is imperative for modern organizations as attackers find increasingly innovative ways to compromise systems and steal data. An enterprise content management (ECM) solution with a secure repository can help protect your information throughout the entire document lifecycle.



- System permissions restrict unauthorized access to document repositories
- Fully customizable access permissions for specific content and data
- Anti-tamper measures to help ensure document authenticity
- Automatic document back-up for disaster recovery
- Audit Trail for tracking user and document activity
- Helps conform with security standards, regular penetration testing
- Automated Retention Policy configuration



SAFEGUARDING THE SECURITY OF YOUR INFORMATION

Canon U.S.A. understands that managing information securely is a fundamental aspect of any content management and collaboration solution. You need to ensure that sensitive information is only available to authorized users, is backed up securely, and can fully and actively be traced via an audit log.

INFORMATION SECURITY

DO YOU EVER WONDER WHAT HAPPENS TO YOUR INFORMATION ONCE IT TRAVELS BEYOND YOUR WALLS?

How do you ensure that only the intended recipient accesses the file?

Do you know if only the intended recipients can access files you send? We offer organizations a flexible enterprise digital rights management (EDRM) solution that helps users protect their data and PII (personally identifiable information) at the file level, as it travels.

Most organizations focus on protecting the perimeter of the IT network through firewalls and protecting the inside with malware and virus protection solutions, but few make the leap to protect their files when they travel outside of the organization.

Now document owners can limit access through cloud-based encryption tools that set parameters around:

- Access privileges
- Real-time revocation
- Editing rights
- Non-editable audit trail
- Availability time frame
- Global file tracking

PREEMPTIVE ACTION CAN HELP PREVENT DISASTER

Today, it's not "if" an organization will experience a data breach, but rather "when."

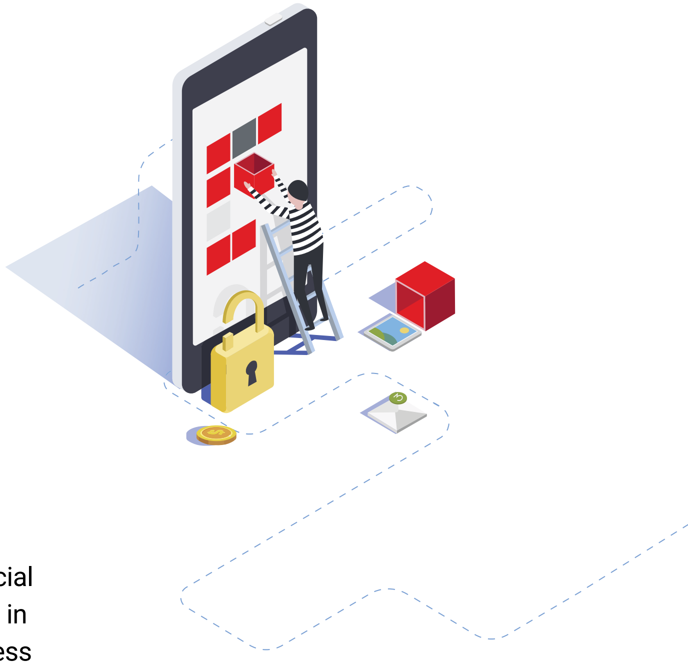
CYBERSECURITY

Have you wondered if your cybersecurity plan is enough to adequately protect your organization? Are your IT and Cybersecurity staffs stretched too thin? You don't have to go it alone. Our cybersecurity services make it easy for you to safeguard your business, connecting you with experts who provide top-notch skills and support to help you build a strong security strategy.

Whether you need training for your employees, a virtual Chief Information Security Officer (CISO), or help with Employee Awareness Training, we've got you covered.

Our services include:

- Managed Vulnerability Service (MVS)
- Penetration Testing
- Consultation
- Security Training & Awareness
- Virtual CISO (vCISO)
- Managed Detection and Response as a Service (MDR)
- Extended Detection and Response (XDR)
- Printer Fleet Cybersecurity (PFCaaS)
- All in One Security Bundle for Medium Sized Enterprises



Ignoring your company's security needs can be costly. It can lead to financial losses, wasted time, a damaged reputation, and lost customers. Investing in cybersecurity awareness and practices is essential to keeping your business healthy and secure.

MANAGED VULNERABILITY SERVICE

MVS continuously identifies vulnerabilities across your on-premises and cloud environments with integrated experts from Supra ITS who act as an extension of your team providing analysis and remediation guidance.

Discover: Executive summaries for non-technical audiences, and detailed summaries for technical audiences.

Report: Monthly scans of internal assets, and weekly scans of external assets.

Verify: MVS team monitors scans for errors and accuracy.

An MVS team provides guidance and recommendations during remediation process, and ad-hoc scanning to verify vulnerabilities have been remediated effectively. Includes all licensing for vulnerability scanning platform.

PENETRATION TESTING

Simulates the actions of both an external attacker and an internal attacker. Using the latest tactics, techniques, and procedures, the penetration tester attempts to exploit systems and gain access to data. This exercise results in identification of systemic weaknesses with areas of remediation ranked by criticality. Technical and executive level reporting provided.

EXTERNAL AND INTERNAL PENETRATION TESTING FEATURES

Both applications include the following features:

- Tests prevention and detection capabilities
- Utilizes OWASP and OSSTMM methodologies
- Validates external security controls
- Identifies areas of greatest risk and remediation
- Satisfies compliance needs, including HIPAA, PCI 3.x, Cyber Insurance, ISO27001
- Credentials include CISSP, CEH, CTPRP, ITILv5

MANAGED DETECTION AND RESPONSE

Managed Detection and Response is a service that combines continuous monitoring of a business's digital assets with an "always-on" certified incident response team to defend your network to first prevent, and ultimately to respond to, a cyber-attack.

MDR as a Service is a perfect choice for proactive companies who want to strengthen their security postures and remain a step ahead of the cybercriminals.

World's best cybersecurity experts as part of your team

Automated Incident Response

24/7/365 Protection

Advanced Forensics

Customized approach to cybersecurity

VIRTUAL CHIEF INFORMATION SECURITY OFFICER (VCISO)

Not all organizations can afford a fully staffed security operations center that responds to threats all day, every day. However, in today's high-risk business environment, neglecting essential security measures can lead to disastrous outcomes.

There are multiple functions available for vCISO services:

- Audit Backup Process and Retention, and Backup/Restore Testing
- Incident Response Plan Review
- IT Security Policy Review
- Disaster Recover Planning
- Monthly Rate: Ongoing vCISO services available, up to 10 hours per month
- Hourly Rate: Minimum 10 Hours if selling standalone
- Baseline Security Assessment (evaluates organization's security posture through external vulnerability scan, risk questionnaire, and consultation).

MANAGE
ASSESSMENT
CONSULT
vCISO

PRINTER FLEET CYBERSECURITY AS A SERVICE (PFCaaS)

Printers on corporate networks are often overlooked in cybersecurity plans. They are rarely configured or updated for security, leaving a significant risk. Large companies can have hundreds or even thousands of printers of various makes, models, and ages.

Our Printer Fleet Cybersecurity as a Service addresses this gap effectively and affordably. Once we establish a "Gold Standard" for security settings that meets your organization's security objectives, automated services check that these standards are maintained. Our alert and event management system provides real-time and historical insights into security configurations, inventory, asset management, and firmware security events, helping keep your printer fleet secure.

EMAIL AND INBOX PROTECTION

At one time, secure email gateways were considered enough to protect against email attacks. Today's advanced social-engineering attacks demand more advanced protection. These sophisticated threats can bypass traditional security measures, leading to significant losses in time, money, and brand reputation for organizations.

COMPREHENSIVE SECURITY AND DATA PROTECTION FOR MICROSOFT© 365

We offer a solution to help your organization protect email inboxes and back up crucial data in Microsoft 365 safely, efficiently, and affordably. Our service helps protect your users and organization from ransomware and phishing attacks. It also minimizes downtime, helps ensure compliance with retention requirements, and provides fast, reliable recovery of Exchange Online, OneDrive, and SharePoint Online data in case of accidental or malicious deletion.

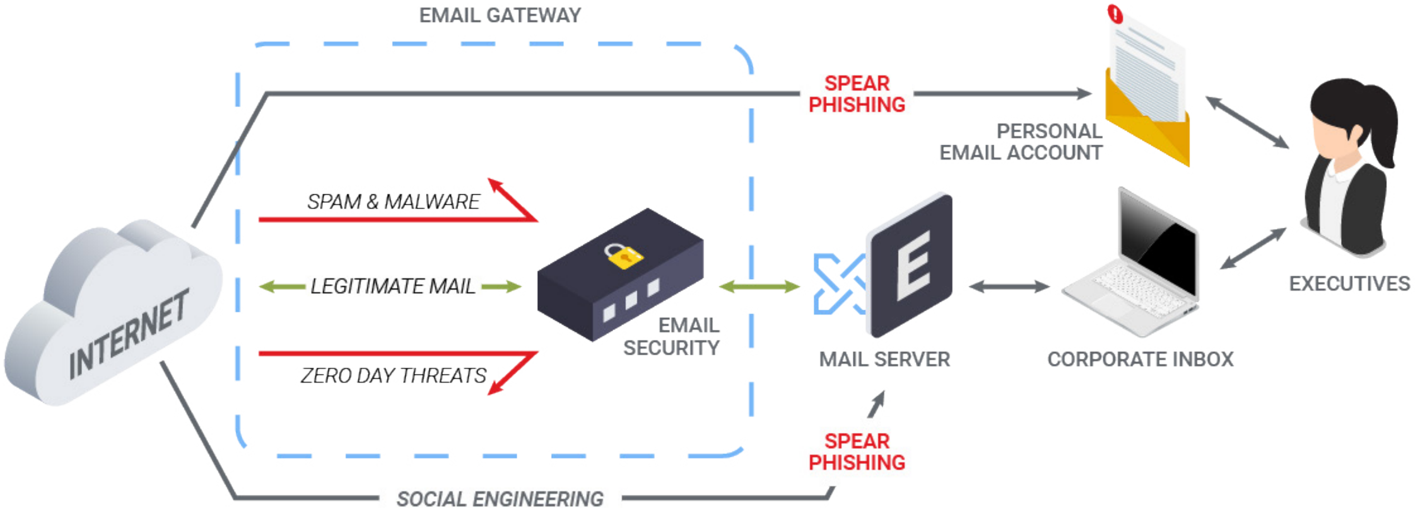
ARTIFICIAL INTELLIGENCE FOR REAL-TIME EMAIL PROTECTION

Business email compromise (BEC), spear phishing, and account takeover are today's top email threats. These hyper-targeted attacks trick employees into making terribly costly mistakes.

We can offer a combination of artificial intelligence, deep integration with Microsoft Office 365, and brand protection into a comprehensive cloud-based solution that helps to guard against these potentially devastating attacks.

FIGHT PHISHING WITH CONTINUOUS SECURITY AWARENESS TRAINING

Social engineering simulation campaigns train users to understand and respond correctly to the latest phishing techniques, recognize subtle phishing clues, and prevent email fraud, data loss, and brand damage. It helps transform employees into a powerful line of defense against damaging phishing attacks.



Deploying a phishing simulation platform in your organization can provide a flexible and consistent way to modify, test, and measure employee behavior with electronic communications. You can convert potential risk takers into front-line defenders.

PEOPLE – YOUR WEAKEST LINK OR YOUR BEST DEFENSE?

LEVERAGE PHISHING SIMULATION TRAINING AS A HUMAN FIREWALL

Social Engineering has been the culprit of some of the most catastrophic data breaches to date. It has never been more critical to create awareness of this threat vector and to educate your personnel to not fall prey to phishing and pre-texting as email has become weaponized and the medium of choice for malicious cybercriminals.

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.

Canon

1-844-50-CANON

usa.canon.com/security

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, 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. Some security features may impact functionality/performance; you may want to test these settings in your environment.Neither Canon Inc., nor Canon U.S.A., Inc., represents or warrants any third-party product or feature referenced hereunder. Canon imageRUNNER is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. All other referenced product names and marks are trademarks of their respective owners. Specifications and availability subject to change without notice. Not responsible for typographical errors.