

# Five Pillars of Security

A Multilayered Approach to Help Protect Your Organization  
from Cyber Threats



# Worried About Security? You're Not Alone.



**Cybercrime keeps a lot of people awake at night.** While the cost of a data breach keeps rising, cybercriminals keep looking for new places to strike. It could be an unsecured printer, an employee who falls for a phishing scheme, or a sensitive document that was sent halfway around the world as an email attachment.

We developed our Five Pillars of Security model with your most precious asset in mind—information. It flows through the hands of people who have varying degrees of risk awareness. That's why we made this model easy to understand for everyone who is involved in your security effort. Within each pillar, you'll find a wide range of solutions and services available to you as a Canon U.S.A. customer.

As you read this e-book, remember that security is not a destination. It's a journey through a multidimensional environment that's full of hidden threats. But don't worry, we've got your back.

## PILLAR #1

# Device Security



**Printers, multifunction devices, and other networked office equipment can be easy targets for cybercriminals.** In fact, any device that is connected to the internet can be exploited to breach the security perimeter.

As a first line of defense, your IT team should close unused communication ports on these devices, encrypt hard disk drives, and optimize data flow protocols that are designed to help minimize their attack surface. If you're adding or replacing devices in your organization, Canon U.S.A. has some great options.

### Canon imageRUNNER ADVANCE DX Series

These powerful, reliable multifunction devices come equipped with the ability to "harden" the configuration to lessen the chances of being an attack surface for malicious actors.

Canon U.S.A. can also help your IT personnel and administrators harden your existing endpoint devices.



[LEARN MORE](#)

## PILLAR #2

# Print Security



Much of the information in your organization still moves around on paper. Think about how often your employees print files at work. What could happen if someone left a payroll report on the printer tray? Or how about personal health information? Paper-based privacy breaches are common and can be very damaging to your business.

### 3 critical security features for office printers:

**ACCESS CONTROL** Authenticates users at the printer with a PIN code, password, or proximity card. For each user, access can be granted or restricted to specific functions, such as copying, printing, scanning, or faxing.

**PULL PRINTING** When a user launches a print job, they must authenticate at the device before it will print. This can help prevent documents from lying on the output tray, where they may be exposed to unauthorized individuals.

**WATERMARKING** This feature places a watermark across the pages when it is printed or scanned. A document can be watermarked as confidential, as copyright-protected, or as a draft version not for distribution.

[LEARN MORE](#)

## PILLAR #3

# Document Security



Information is one of your most valuable assets. It should be thoroughly protected, meticulously managed, and easily accessible. But as your organization grows, so does the amount of information you have to protect. Before you know it, you've lost track of how many documents you have, where they're stored, and whether they're secure.

### **Enterprise Content Management (ECM)**

It's important to understand that information must be protected both when it is in transit and at rest. That includes limiting access to authorized users, making secure backups, and keeping an accurate audit log. Our ECM solutions provide a full battery of security features to help protect your documents throughout their life cycle:

- // System permissions to control access to document repositories
- // Fully customizable access permissions for specific content and data
- // Anti-tamper measures to help ensure document authenticity
- // Automatic document backup for disaster recovery
- // Audit Trail for tracking user and document activity
- // Automated Retention Policy configuration
- // Governance and classification to help ensure proper access

[LEARN MORE](#)

## PILLAR #4

# Information Security



Most organizations focus on protecting assets within their security perimeter. But what happens to information when it travels outside your firewall in an email or on a thumb drive? Could it be copied and sent to a competitor or simply make its way into the wrong hands?

### **Enterprise Digital Rights Management (EDRM)**

EDRM strips away the limitations of perimeter security. Using a dynamic, cloud-based encryption key, you can grant or revoke access to your files anytime, no matter how far they travel. So you can collaborate and share information while maintaining control over it.

EDRM parameters and controls can include:

- // Access privileges
- // Activity restrictions
- // Editing rights
- // Real-time revocation
- // Non-editable audit trails
- // Availability time frame
- // Global file tracking

[LEARN MORE](#)

## PILLAR #5

# Cybersecurity



**Securing your entire organization can be a complex task.** It takes professional subject matter experts, stakeholders from every line of business, and executive leadership. It's a big task that is never one-and-done.

You can rise to the challenge with help from our cybersecurity service providers. These companies provide human resources with top-level skills who collaborate with your teams at every level.

Whether you need a fresh security approach for your growing organization, training for your employees, or help qualifying for cybersecurity insurance, we can connect you with expert advice and solutions.

- // Vulnerability Assessments
- // Penetration Testing
- // Incident Response
- // Digital Forensics
- // Consulting Services
- // Professional Services
- // Security Awareness Training
- // Security Information and Event Management
- // Threat Intelligence and Vulnerability Management
- // Printer Fleet Cybersecurity as a Service

[LEARN MORE](#)

## SECURITY CHALLENGE

# Identifying Risks

### **Solution 1: Vulnerability Assessment**

You can't protect what you can't see. A vulnerability assessment can help reveal the areas in your technology infrastructure that could be a threat to your business. Armed with these insights, your IT and security teams can develop a comprehensive mitigation strategy.

### **Solution 2: Penetration Testing**

Similar to a vulnerability assessment, the objective here is to validate host and network configurations and produce a list of known vulnerabilities existing on in-scope systems.

A penetration test takes the additional step of exploiting those vulnerabilities to gain access to your email systems, firewalls, routers, VPN tunnels, web servers, and other devices. The testing and exploitation of vulnerabilities helps to reduce false positives and mimics real-world attacks.

**REQUEST AN AUDIT**



## SECURITY CHALLENGE

# Managing Complexity

Your IT team can't be everywhere at once. We offer two cost-effective services to help simplify their work and allow them to focus on supporting your core business.

### **Solution: Comprehensive Managed Cybersecurity Services**

An expert team combines continuous monitoring of your digital assets with an "always-on" threat intelligence and incident response team. It's a smart option to help strengthen your security posture without overtaxing your human and financial resources.

[LEARN MORE](#)

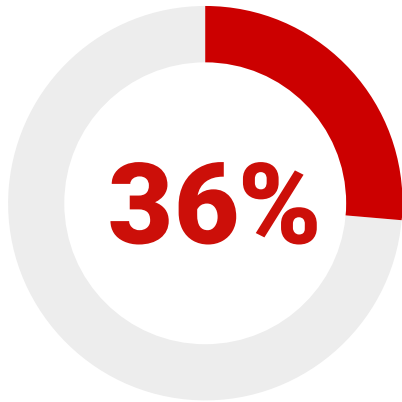
### **Solution: Printer Fleet Cybersecurity as a Service (PFCaaS)**

Many networked printers have not been configured or updated for security since the day they were installed. PFCaaS can help you tackle this problem economically and systematically. Once a "Gold Standard" security configuration is set, it is monitored and maintained automatically across your fleet.

[LEARN MORE](#)

## SECURITY CHALLENGE

# Preventing Human Error



### **Solution: Cybersecurity Education and Training**

According to a survey conducted by Tessian and Stanford University, 36 percent of employees said they are very or pretty certain they have made a mistake at work that has compromised security in the last 12 months.<sup>1</sup>

Two common errors involve phishing and pretexting, where an employee is tricked into answering a fake email or social media page. For this type of threat, your people can be your weakest link—or your best defense. You need to help them spot and report every phishing attempt and run simulated attacks to make sure they're prepared.

We can set you up with a security awareness program that makes learning enjoyable while giving your employees confidence and advanced skills. You can train them no matter where they work, evaluate their progress in real time, and keep them up to date on the latest threats.

**SEE HOW IT WORKS**

1. The Psychology of Human Error, Tessian Research, 2022.


<https://www.tessian.com/resources/psychology-of-human-error-2022/>

# You Need Big Security. But Where Do You Begin?



**You don't have to go it alone.** Canon U.S.A. is here for every business, no matter how big or small. We offer comprehensive cybersecurity and risk-mitigation solutions, as well as some of the brightest minds in the industry. And with our Five Pillars of Security model, we can help you find the security gaps you may have overlooked, assist you in choosing the right technology, and guide you in training your employees.

[CONTACT US](#)



**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. Cybersecurity is a key component of our Five Pillar approach.**



1-844-50-CANON | [usa.canon.com/security](https://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.

Canon and imageRUNNER are registered trademarks of Canon Inc. in the United States and elsewhere. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. Neither Canon Inc. nor Canon U.S.A., Inc. represents or warrants any third-party product or feature referenced hereunder.  
©2025 Canon U.S.A., Inc. All rights reserved.

11/25-0133-9364