Canon

THE 5 PILLARS OF SECURITY

Securing Printer Fleets, Regardless of Manufacturer

The evolving cybersecurity landscape requires organizations to be increasingly aware of the threats infiltrating their network environments. While servers and traditional computer endpoints often receive the lion's share of attention, a significant security gap remains largely unaddressed—securing the printer and Internet of Things (IoT) endpoints. These devices, often overlooked, are becoming critical vectors for cyber attacks.

This e-book explores the challenges associated with securing printer and IoT endpoints, contrasts in-house management with third-party service solutions like Printer Fleet Cybersecurity as a Service (PFCaaS), and makes a compelling case for why IT managers and IT Security (ITSEC) managers should seriously consider adopting PFCaaS as a key component of their cybersecurity strategy.

Why Printers and IoT Devices Are Vulnerable

Unlike servers and computers, which are typically secured through comprehensive cybersecurity protocols, printers and IoT devices often exist on the periphery of the cybersecurity strategy. This oversight can have severe consequences.

Vulnerability and Exposure

- **Printers as Data Repositories:** Modern printers are not just output devices; they store and process sensitive data, often retaining copies of scanned, printed, or faxed documents. Even if this data is only stored for a short time, unauthorized access could lead to significant breaches.
- **Outdated Firmware and Software:** Many printers and IoT devices run on outdated firmware, leaving them exposed to known vulnerabilities that hackers can exploit. Regular updates are often neglected, further exacerbating the risk.
- **Weak Authentication Mechanisms:** Default or weak passwords on printers and IoT devices can easily be exploited by attackers. Without robust authentication mechanisms, these endpoints serve as low-hanging fruit for cybercriminals.

Why Traditional Security Approaches Fall Short

Traditional cybersecurity measures focus heavily on securing servers and computers, but the same rigorous protocols are not always applied to printers and IoT devices. This gap in security leaves organizations vulnerable to:

- **Data Breaches:** Unsecured printers and IoT devices can be entry points for attackers, leading to data theft and breaches.
- **Network Compromise:** Once inside, attackers can move laterally across the network, compromising other critical systems.
- **Operational Disruptions:** Cyber attacks on printers can disrupt business operations, leading to downtime and loss of productivity.

Challenges in Securing Multi-Manufacturer Printer Fleets

Managing and securing a fleet of printers from multiple manufacturers presents unique challenges. These challenges can often overwhelm in-house IT teams, leading to inconsistent security practices and increased risk exposure.

- **Inconsistent Security Features and Standards**
  Different manufacturers offer varying levels of security features. For instance, while one brand may provide robust encryption and frequent firmware updates, another might lag in these areas. This inconsistency makes it difficult to apply uniform security policies across all devices.
- **Complex Firmware and Software Management**
  Updating firmware across a multi-manufacturer fleet is a complex task. Each brand may require different tools, processes, and schedules for updates. This complexity can often result in delays or errors in applying critical security patches, leaving devices exposed to known vulnerabilities.
- **Diverse Monitoring and Logging Capabilities**
  Printers from different manufacturers may have varying capabilities as it relates to monitoring and logging. Some devices might not integrate well with the organization's existing Security Information and Event Management (SIEM) systems, making it challenging to detect and respond to security incidents in a timely manner.

Leveraging Third-Party Expertise: PFCaaS

PFCaaS can help organizations ensure consistent and robust security across all endpoints, regardless of manufacturer.

- **Expertise and Specialization**
  With dedicated teams focused solely on printer and IoT device security, PFCaaS helps to ensure that all devices are secured using the latest threat intelligence and best practices. This level of specialization is difficult to achieve internally, where IT staff are often spread thin across multiple responsibilities.
- **Scalability and Efficiency**
  As the number of devices in an organization grows, PFCaaS can scale its operations without compromising security. This is particularly valuable for large organizations with thousands of printers and IoT devices, where managing security in-house would be resource-intensive and challenging.
- **Standardization and Consistency**
  PFCaaS helps to ensure that all devices, regardless of manufacturer, adhere to standardized security policies. By using advanced automation tools, PFCaaS maintains consistent security configurations across the entire fleet, helping to reduce the likelihood of configuration errors and ensuring that all endpoints are equally protected.

PFCaaS vs. In-House Security Management

Managing and securing a fleet of printers from multiple manufacturers presents unique challenges. These challenges can often overwhelm in-house IT teams, leading to inconsistent security practices and increased risk exposure.

- **Inconsistent Security Features and Standards**
  Different manufacturers offer varying levels of security features. For instance, while one brand may provide robust encryption and frequent firmware updates, another might lag in these areas. This inconsistency makes it difficult to apply uniform security policies across all devices.
- **Complex Firmware and Software Management**
  Updating firmware across a multi-manufacturer fleet is a complex task. Each brand may require different tools, processes, and schedules for updates. This complexity can often result in delays or errors in applying critical security patches, leaving devices exposed to known vulnerabilities.
- **Diverse Monitoring and Logging Capabilities**
  Printers from different manufacturers may have varying capabilities as it relates to monitoring and logging. Some devices might not integrate well with the organization's existing Security Information and Event Management (SIEM) systems, making it challenging to detect and respond to security incidents in a timely manner.

Discover the Power of PFCaaS

PFCaaS offers robust security for printers and IoT endpoints, helping to ensure sensitive data protection and regulatory compliance.

- **Evergreen Inventory and Lifecycle Management**
  PFCaaS begins by inventorying all in-scope devices, maintaining an accurate and up-to-date record of each device's status. This printer fleet inventory is continuously monitored and updated, helping to ensure that any changes in the fleet are promptly reflected and addressed.

- **Blueprinting and Gold Standard Configuration**
  PFCaaS's blueprinting process identifies the available security settings on each device and establishes a "Gold Standard" configuration tailored to the organization's needs. Whether aligning with NIST or DOD standards, PFCaaS helps to ensure that all devices meet the required security criteria.

- **Automated Patch Management**
  PFCaaS includes a robust Firmware Deployment Service™, which automates the deployment of firmware updates across all devices. This ensures that all printers and IoT devices are running the latest security patches, which helps to significantly reduce the risk of exploitation.

- **Ongoing Monitoring and Remediation**
  PFCaaS continuously monitors all devices, maintaining the established security settings and configurations. Any deviations are promptly addressed through automated remediation processes, helping to ensure that the fleet remains secure at all times.

- **Comprehensive Reporting and Documentation**
  PFCaaS provides extensive reporting capabilities, offering hundreds of stock reports, ad-hoc reporting, and custom reports tailored to the organization's needs. These reports are essential for compliance audits and provide valuable insights into the security posture of the fleet.

Strategic Implications of Adopting PFCaaS

- **Improved Security Posture**
  By ensuring consistent and comprehensive security across all printer and IoT endpoints, PFCaaS helps to significantly improve the organization's overall security posture. This also helps to reduce the risk of breaches, protecting both the organization's data and its reputation.
- **Enhanced Compliance and Risk Management**
  PFCaaS helps organizations meet industry-specific regulatory requirements, reducing the risk of non-compliance and the associated fines. The service's continuous monitoring and reporting capabilities also provide valuable documentation for audits and incident response.
- **Operational Efficiency**
  Outsourcing printer and IoT device security to PFCaaS allows internal IT staff to focus on core business objectives, helping to improve overall operational efficiency. This reallocation of resources can lead to faster innovation and a more agile response to business challenges.
- **Cost Savings and ROI**
  While there is an initial cost associated with adopting PFCaaS, the long-term savings from reduced breach risk, compliance fines, and operational inefficiencies can result in a strong return on investment (ROI). Organizations can also benefit from the predictable pricing models offered by PFCaaS, which helps to simplify budget planning.

The Case for PFCaaS

In a world where cyber threats are constantly evolving, the importance of securing all endpoints—including printers and IoT devices—cannot be overstated. PFCaaS offers a comprehensive alternative to employing in-house resources. Scalable—and cost-effective—PFCaaS is a sound solution to consider for managing the security of these often-overlooked endpoints.

By providing specialized expertise, automation, and consistent security management, PFCaaS helps to ensure that organizations can protect their data, maintain compliance, and improve operational efficiency. For IT managers and ITSEC managers, adopting PFCaaS is a strategic decision that can help enhance the organization's security posture, support business continuity, and ultimately provide a competitive advantage in the digital age.

Whether managing a fleet of 500 or 5,000 devices, PFCaaS offers the tools, expertise, and assurance needed to keep these critical endpoints secure—today and in the future.

For more information about Canon U.S.A.'s Five Pillars of Security, our comprehensive approach to cybersecurity, contact us today.

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. Device Security is a key component of our Five Pillar approach.

Canon

1-844-50-CANON | usa.canon.com/security

09/25-0511-11926