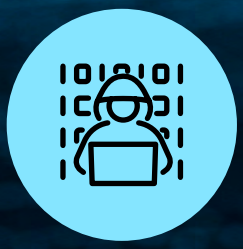
Print Security Threat Landscape



WHY MFPs MATTER AND WHAT'S AT RISK

- Networked endpoints that process and store sensitive business data, with potential exposure through device memory, unattended documents, and insecure end-of-life disposal.



RISING CYBER THREATS

- Attackers increasingly target firmware, BIOS, and embedded systems.
- Zero-day exploits and large-scale attacks abuse unpatched devices.



WEAK DEFAULT CONFIGURATIONS

- Permissive factory settings expose services, ports, and protocols.
- Default credentials and delayed updates remain common entry points.

Source: Keypoint Intelligence Research

To address these concerns, click HERE to read the Canon Zero Trust Model white paper.

Canon 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. Neither Canon U.S.A., Inc. nor its agents are responsible for typographical errors or omissions. Specifications and availability subject to change without notice.

©2026 Canon U.S.A., Inc. All rights reserved.

10.12.26/26-1590-16249