Ensure your printer—and network—are secure

Comparing Ricoh and HP

Today's printers and multifunction devices have the same vulnerabilities as other endpoints on the network. They contain potentially sensitive information and data, making them prime targets for a security breach.

That's why it's critical to consider how your printing technology addresses security to reduce risk and protect your devices, documents, data, and business.

Ricoh claims they provide a range of security features to minimize risk. Given the importance security in the workplace, it's worth comparing how Ricoh's security measures compare with HP.

Ricoh security claims

Ricoh highlights three claims for the security of their devices:

- **Intrusion detection**—For Ricoh, individual users can be identified by the multifunction copier. Ricoh's user authentication functions are based either on user codes of up to eight digits or on combinations of login user names and passwords. Ricoh multifunction copiers allow user authentication via an existing authentication system.[1]
- **Device detection**—To prevent the genuine firmware from being overridden by the unauthorized firmware, Ricoh uses electronic signatures to validate the firmware. Moreover, a Trusted Platform Module (TPM)—a tamper-proof hardware security module—validates the authenticity for MFP firmware and installed applications before permitting the MFP to operate. These technologies ensure device security.
- **Document and data protection**—To increase security against unauthorized use, PDF files can be protected by encryption and password. Using the locked print function, a password is specified when sending the document, and that password must be entered on the multifunction copier before it can be printed. The copy guard function prints/copies documents with special invisible patterns embedded across the background. Address books, authentication information, and documents are encrypted as they are stored in the multifunction copier.

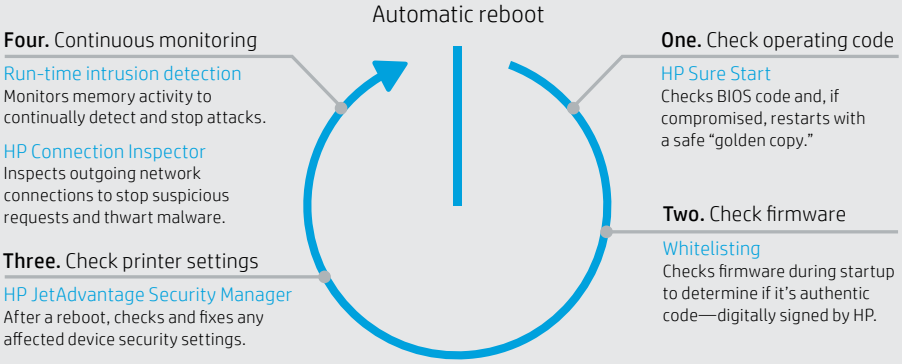
Despite these claims, Ricoh still falls short when compared to HP's end-to-end security offering with HP Security Manager and the embedded, out-of-the box security features.

Self-healing HP Print Security

How does it work?
The embedded security features address three primary steps in the cycle of an HP device.

If attacked, enterprise devices can reboot and self-heal.

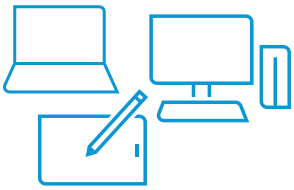
HP JetAdvantage Security Managers completes the check cycle.



New embedded security: HP Connection Inspector

The latest HP security differentiator stops malware from calling home.

- Monitors outbound network connections (packets)
- Learns what's normal, then inspects and stops suspicious packets
- Triggers a reboot to initiate self-healing procedures without IT intervention
- Creates security events that can be integrated with a SIEM tool like Splunk
- No competitor offers these features

	Ricoh	HP
 **Device detection/ whitelisting**	• Ricoh Security Solutions are described as a multi-layered approach that helps close the door on those who wish to exploit vulnerabilities. • Focuses on standard, legacy device security such as securing ports, user authentication, network protocols, data overwrite, and encryptions. • Makes no claim of memory scanning for injection attacks. • Does not provide Secure Boot to protect the BIOS code on their devices.	• Exceeds the Ricoh Security offer with comprehensive, industry-leading capabilities and protections including self-healing BIOS, firmware code integrity, and intrusion detection. • Leads the industry with device Intrusion Detection which continuously monitors memory for malicious malware. • HP's FutureSmart Value Proposition provides device investment protection and has provided Intrusion Detection and whitelisting as a firmware upgrade on 3.7 FutureSmart Devices since 2012
 **Document and data protection**	• Considers end-user education to be important in reducing the risk of data breach; however, does not provide the level of technology to safeguard once this type of threat is inside a firewall and taking root in devices. • Focuses on standard data document security requirements that are on par with the industry but falls short of HP print security. • Acknowledges their full set of security features do not provide the necessary protections to fully eliminate human-error caused risks.	• Offers superior security monitoring and management solutions to help identify vulnerabilities and establish a unified, policy-based approach to protecting data, strengthening compliance, and reducing risk—all while saving significant time and resources. • Exceeds Ricoh's security requirements in end-to-end security including policy-based security monitoring and assessment, "Instant On" security, device-level SIEM integration, U.S. NIST checklist inclusion and DLP keyword searching.
 **Security software**	• Does not possess a Secure Boot process that protects the BIOS. • Provides firmware validation only for devices with a TPM chip. • Does not provide protection against memory injection or monitor for anomalous behavior run-time code execution. • Lacks robust, security-focused solutions that ensure device security compliance with defined policies. • Does not provide real-time threat detection and analytics, or integration with SIEM tools like ArcSight or Splunk to provide insight into possible attacks. • Fleet Management tool offer lacks: 1. A base security policy that aligns with NIST standards to apply to all devices. 2. A robust policy creation process to fine-tune security policies to the customer's specific needs. 3. Instant-On Technology that ensures policies are assigned as devices come online. 4. Auto remediation of up to 250 security settings that do not comply with the defined policies.	• Offers HP Jet Advantage Security Manager—an industry-first, policy-driven, BLI award-winning compliance manager that's sold by HP, and developed and maintained by HP staff. • Solution can assess, report, and remediate up to 250 settings, and is designed to work with 115 HP device models. • Features "Instant On" technology which automatically assess compliance of compatible HP devices.

Print security Frequently Asked Questions

Q1: My company leverages firewalls to protect my network; why do we need security on our printers?

A: Do you use malware/virus protection on your PCs and laptops? Also, you have to protect devices from other devices on your network. If a PC gets infected with malware through email phishing, there is little a firewall can do to protect the systems within against that.

Q2: Given the complexity of our network and the data available on our servers and other endpoints, why would hackers target printers?

A1: Hackers do not necessarily attack systems directly, they look for the weakest point like a lioness goes after the lame gazelle in the herd. Printers are often ignored in security policies therefore they can be the lame gazelle. Once they are on your network they can access other resources, which is why having embedded print device security out of the box is so important.

A2: Printers often process, even store highly sensitive data - they could be serious targets for a data breach.

Q3: What happens if a hacker tries to install malware onto my printer?

A: HP printers provide protection against the installation of malicious programs—including malware. Our whitelisting technology ensures that only authentic HP code gets installed on the system, including the firmware (the operating system of a print device) and any solutions.

Q4: Do we really need all of this security for our printers?

A1: Printers really should be treated as equal citizens on your network. They are as likely a target as any other endpoint and handle highly sensitive information regularly.

A2: Security requires constant diligence—it only takes one chink in your armor to perpetrate a data breach that could cost a company millions of dollars to recover from.

Q5: What is HP's key security differentiator against Ricoh?

A: Our ability to auto-recover from potential security risks—either at the individual device level with self-healing or at the fleet level via HP Jet Advantage Security Manager.

Assessment tools

How secure are your printers? Assess the security of your print environment with these helpful HP online tools:

- **HP Secure Print Analysis survey**—online self-assessment to determine if you are following best practices in print security: hp.com/go/SPA
- **HP Quick Assess**—free technical evaluation of top 13 settings on up to 20 HP printers (phone consultation is available in the U.S.): hp.com/go/quickassess

1 Source: https://www.ricoh.com/security/products/mfp/function/

4AA7-1567ENUS, Rev. 2, February 2018