Taking measure of print security measures

Comparing Xerox and HP

Print security isn't just about establishing the security of your printer. It's also about providing the security of your entire network. With that in mind, it's critical to consider how your printing technology addresses security to reduce risk and protect your devices, documents, data, and business.

And while Xerox claims that they provide "benchmark security"—including real-time protection from both internal and external security threats—it's important that you make an informed decision about print security by taking a closer look into Xerox print security claims and how they compare to HP.

Security dimensions

Xerox highlights four dimensions to the security of their devices:

- **Intrusion prevention**[1]—Xerox centers this security dimension on the device access through authentication. Beyond limiting access to only authenticated users, authorization provides the ability to control usage of color output, by user, group, time of day, and application.
- **Device detection**[2]—Xerox partners with McAfee to protect both data and device from malicious intrusions.
- **Document and data protection**—Above network security, Xerox ensures both the protection of data between users and the hard-copy document is only received and viewed by the intended recipients.
- **External security software partners**—Xerox relies on their own malware protection features available on Xerox® ConnectKey® Technology enabled MFPs, while relying on third-party solutions to protect printing assets with security policies centrally at the network level.

When comparing the four security dimensions from Xerox, HP offers a clear difference: HP is able to protect and self-heal within the embedded security features of the HP device's operating cycle.

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.

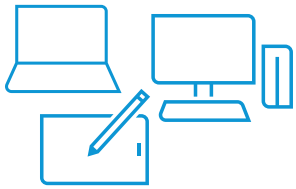
HP JetAdvantage Security Managers completes the check cycle.

1 **One: load BIOS/boot code**
Prevents the execution of malicious code during boot-up by making sure only HP-signed genuine code is loaded.

2 **Two: check firmware**
Helps confirm only authentic, known-good HP firmware—digitally signed by HP—is loaded into memory.

3 **Three: protect run-time memory**
Protects operations and stops attacks while device is running.

4 **Four: complete the check cycle**
HP JetAdvantage Security Manager checks and fixes any affected device security settings.

	Xerox	HP
 **Device detection/ whitelisting**	• Relies purely on whitelisting technology (via partnership with McAfee) that verifies the authenticity of firmware at startup or on-demand—this is not new technology. • Can only detect the load of malicious firmware (aka whitelisting). • Secure boot, run-time intrusion detection, and SIEM integration are not available. • Does not offer a Trusted Platform Module (TPM) for added security. • Provides device-level certificate management through the Embedded Web Server that may take 15 minutes per device.	• HP FutureSmart firmware offers the same basic, industry-standard whitelisting—ensuring only authentic, known-good HP firmware is loaded into memory. • HP SureStart ensures the BIOS code integrity is validated. If the BIOS is compromised, the device reboots and loads a safe "golden copy" that is digitally signed by HP. • Supports on-device Intrusion Detection that continuously monitors memory for malicious malware. • HP JetAdvantage Security Manager streamlines security by establishing a single policy and can save users time and increase productivity.
 **Document and data protection**	• Offers the Xerox Unified Secure Access Unified ID System via third-party Equitrac that integrates Xerox MFPs with existing authentication systems (Badge/PIN/employee ID), basic audit export log and secure release (via Nuance SafeCom pull print document solution). • Provides server-based job accounting functionality as an upsell to the third-party Equitrac Office solution. • Protects print data from unauthorized parties using a standardized Secure Pull Print Model.	• Has comparable technology in the document and data protection space. • Offers several pull printing solutions: cloud-based, on premise, and hybrid—to meet the unique confidential printing and cost efficiency needs of businesses. • Protects sensitive documents from packet sniffing with end-to-end encryption that safeguards a company's most valuable information—in transit and at rest. • Provides additional protection with comprehensive security on the device from startup to shutdown with self-healing to minimize business disruption backed by solid enterprise solutions. • Offers superior security monitoring and management solutions that 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. • Provides full functionality with HP single- and multi-function printers—no need to purchase or upgrade to a third-party vendor for job accounting.
 **Security software**	• Relies on a third-party software solution (McAfee ePolicy Orchestrator or ePO). • Customer must already own McAfee ePO or purchase the license from McAfee. • Integration is enabled via an add-on and requires manual configuration of each device. • Solution can assess and report on 60+ security settings—and is designed to work for about 30 device models. • MFP extension does not work with the latest version of McAfee ePO. • MFP extension requires DNS settings that could make a network vulnerable to man-in-the-middle attacks. • Lab results indicate the client task functionality is mostly absent for MFPs.	• 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?

A1: 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 Xerox?

A1: 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 Intrusion Prevention: a comprehensive set of capabilities prevents malicious attacks, proliferation of malware, and misuse of unauthorized access to the printer. Whether from transmitted data or directly at the MFP, all access points are protected through user authentication and access controls. https://www.xerox.com/en-us/connectkey/printer-security

2 Device detection: a comprehensive Firmware Verification test, either at start-up or when activated by authorized users, provides alerts if any harmful changes to the printer have been detected. McAfee® Whitelisting technology constantly monitors for and automatically prevents any malicious malware from running. https://www.xerox.com/en-us/connectkey/printer-security

All defined security features can be found in "Xerox and Information Security—Your Data, Your Business, Partnering to Protect What's Most Important" ©2016 Xerox Corporation. 04/16 BR18557SECGD-01UD

4AA7-1568ENUS, November 2017, Rev. 1