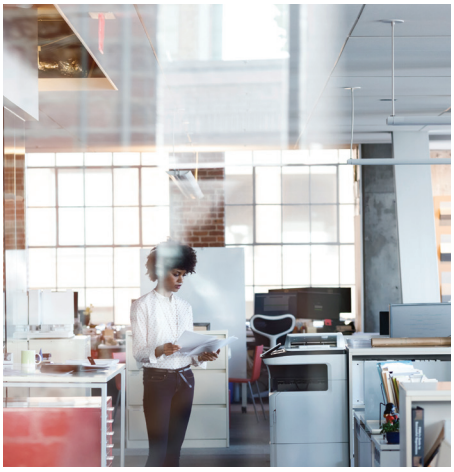
Protect your printer. Protect your business.

Comparing Lexmark and HP

The increasing influx of devices on enterprise networks continues to make security a growing challenge and concern—including printers and multifunction devices, which can have the same vulnerabilities as any other endpoint on the network.



Printer manufacturers are addressing these security issues with a variety of features, technologies, and solutions to help minimize the risks.

However, when it comes to security, not all printers are created equal. When connecting a new printer or MFP to your network, it's vital that you be aware of the security features it includes. And while both HP and Lexmark contend their printers and MFPs provide adequate security measures, a closer look reveals a few discrepancies.

Lexmark security claims

"Full-Spectrum Security" is the term that Lexmark uses when describing their comprehensive approach to securing an enterprise environment. It breaks down into seven keys to product security:

- Secure access
- Network
- Document security
- Secure remote management
- Security solutions
- Hard disk security
- Standards & certifications

Because Lexmark says they understand the multifaceted reality of security threats, they respond with a "holistic, systematic approach that encompasses the device, the fleet, and the whole network infrastructure." When comparing the Lexmark security features, this is a standard approach to security with a newly marketed Lexmark packaged offer.

While Lexmark also claims that security "is built into every Lexmark product, with standard security features appropriate to each product's intended use and available options to fulfill special requirements," compared to other printing solutions, there is no game-changing innovation or true differentiation from industry standards.

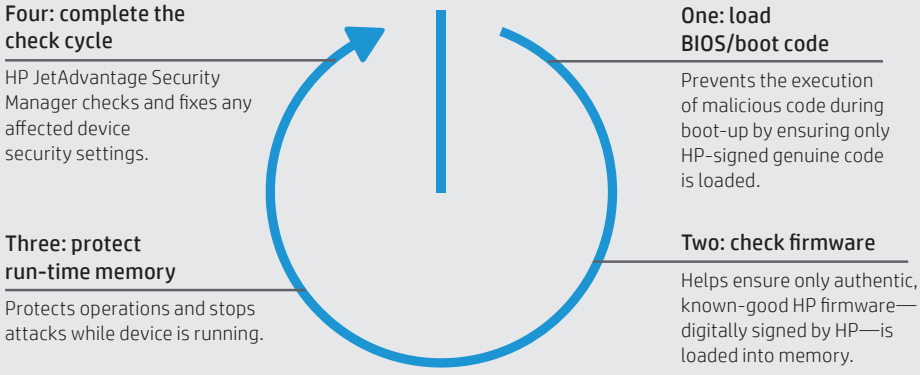
Self-healing HP Print Security—HP vs. Lexmark

Finding the HP advantages when comparing Lexmark against the three primary steps embedded in the HP MFP operating cycle.

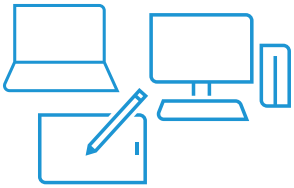
How does it work?
The embedded security features address three primary steps in the cycle of an HP device.

If attacked, only HP Enterprise devices can reboot and self-heal.

HP JetAdvantage Security Manager completes the check cycle.



Security features—a side-by-side comparison

	Lexmark	HP
 **Device detection/ whitelisting**	• Makes no claim to memory scanning for injection attacks. • Can only detect the load of malicious firmware on the device (aka, whitelisting). • Secure boot technology validates the integrity of the BIOS at startup. • Encrypted and signed firmware ensures that only firmware created by Lexmark's systems can be installed on the devices (aka, whitelisting). • Should non-genuine firmware be detected, users receive notification. Continuous verification ensures the firmware has not been tampered with during operation. • If firmware is corrupted, devices turn to stop-print state and a physical intervention must occur to correct.	• With HP's SureStart, the BIOS code integrity is validated. If the BIOS is compromised, the HP MFP reboots the device and loads a safe "golden copy" that is digitally signed by HP. Printing is not interrupted. • Supports on-device Intrusion Detection that continuously monitors and scans memory for malicious malware.
 **Document and data protection**	• Protects print data from unauthorized parties using a standardized Secure Pull Print Model. • Indicates that scanned information is protected from unauthorized users—but does not specify how. • Can require customers to use third-party MPS providers to perform many management tasks remotely.	• Conforms to leading, industry standard for stored data, and is encrypted using highest level of encryption (assume AES-256). • Overwrite capability provided is NIST and US DoD compliant. • Offers several pull printing solutions: cloud-based, on premise, and hybrid—to help organizations meet their unique confidential printing needs and reduce print costs. • Helps users protect sensitive documents from packet sniffing with end-to-end encryption that safeguards their company's most valuable information—in transit and at rest. • Provides additional protection with comprehensive security on the device from start-up to shutdown with self-healing to minimize business disruption— backed by solid enterprise solutions.
 **Security software**	• Lexmark's MarkVision Enterprise security policy is both manual and device specific—the initial configuration can be arduous and if the device is changed out and a new device model placed on the network, the manual process may need to be repeated. • Multiple devices and their capabilities dictate the individual security configurations across the enterprise. • MVE lacks Instant-On technology and a built-in policy based on NIST standards.	• Instant-On security protection automatically assesses compliance of compatible HP devices. • Changing devices does not impact the enterprise policy management efforts. • HP Jet Advantage Security Manager—an industry-first, policy-driven, BLI award-winning compliance manager—can configure up to 250 security settings. By comparison, Lexmark MVE only configures 115 settings.

HP's view of BLI analysis

BLI recently conducted an analysis of print security features, software, and service offerings by major printer manufacturers for BLI's PaceSetter awards program. Through the analysis, BLI concluded that a number of manufacturers, including Lexmark and HP, stood out for their security efforts across eight categories. Each of these manufacturers received a BLI Pacesetter Award for print security.

According to Jamie Bsales, Director of Software Analysis at Keypoint Intelligence, "Lexmark's device security is second to none and includes advanced features such as a firmware integrity check at boot-up, BIOS integrity checking, intrusion detection and reporting, and much more. It easily landed in the top tier among the 13 OEMs included in our study."

However, according to HP's research, we feel that a stronger weighting should be applied to the importance of features based on their impact to the level of security, ease of implementation, and maintenance. A closer look at the data reveals significant differences between the level of security and capabilities offered by Lexmark and HP.

	Lexmark	HP
BIOS Integrity Checking	• Device will shut down if a corrupt BIOS is detected	• Device will shut down if a corrupt BIOS is detected • Device will self-heal and restart in a good state with no IT intervention
Intrusion Detection	• Security events can be sent to a remote server (i.e., Intrusion Detection system)	• Security events can be sent to a remote server (i.e., Intrusion Detection system) • Security events are configured to be consumed by a SIEM tool (Splunk, Arcsight, SIEMonster) • Security events are stopped real-time by embedded technology in the device scanning run-time memory. If malware is detected, the device flushes the memory and restarts in a good state.
Policy Compliance	• Security settings can be pushed on a schedule	• Security settings can be pushed on a schedule • Instant-On security ensures that a device automatically receives proper settings when it is added to the network • Baseline policies are easily established using built-in policy based on NIST best practices

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

4AA7-1566ENUS, November 2017, Rev. 1