Technical brief

HP Wolf Enterprise Security

Embedded enterprise-level print security features

Featuring the world's most secure printing[1], only HP Enterprise MFPs and printers have these self-healing embedded security features. With the investment protection that HP FutureSmart firmware provides, you can add some features to many existing HP Enterprise printer models.

Detect, protect and recover

HP printers have the industry's strongest security[1], with four key technologies that are always on guard, continually detecting and stopping threats while adapting to new ones. Only HP Enterprise printers automatically self-heal from attacks by triggering a reboot—IT doesn't need to intervene.

HP Sure Start—checks operating code

The BIOS is a set of boot instructions used to load critical hardware components and initiate firmware. HP Sure Start technology works behind the scenes by validating the integrity of the BIOS when powering up. If a compromised version is discovered, the device restarts using a safe "golden copy" of its BIOS.

Run-time intrusion detection—monitors memory activity

Memory activity is monitored in real time, right when most attacks occur, to continually detect and stop attacks. Common Criteria certified[2] to check for anomalies during complex firmware and memory operations, automatically stop intrusions, and reboot to heal itself.

HP Connection Inspector—inspects network connections

Stop malware from "calling home" to malicious servers, stealing data, and compromising your network. HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and automatically trigger a self-healing reboot.

Whitelisting—checks for authentic firmware, digitally signed by HP

Because compromised firmware could expose your whole network to an attack, whitelisting helps ensure the code that coordinates your printer's functions, controls, and security hasn't been tampered with. Firmware is automatically checked during startup, and if an anomaly is detected, the device reboots to a secure, offline state and notifies IT.

Secure cartridges you can trust[3]

At every step of the design, supply chain, and production process for Original HP office cartridges, security is built-in with tamper-resistant chips, firmware and packaging.

Learn more: hp.com/go/PrintersThatProtect

How does it work?

The self-healing embedded security features address four primary steps in the cycle of an HP Enterprise device.

Automatic reboot

One. Check operating code

HP Sure Start
Checks BIOS code and, if compromised, restarts with a safe "golden copy."

Two. Check firmware

Whitelisting
Checks firmware during tartup to determine if it's authentic code—digitally signed by HP.

Three. Check printer settings

HP Security Manager[4]
After a reboot, checks and fixes any affected device security settings.

Four. Continuous monitoring

Run-time intrusion detection
Monitors memory activity to continually detect and stop attacks.

HP Connection Inspector
Inspects outgoing network connections to stop suspicious requests and thwart malware.

[1] HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2021 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit hp.com/go/PrintersThatProtect. For more information, visit hp.com/go/PrinterSecurityClaims.

[2] Third-party certification based on Common Criteria Information Technology Security Evaluation ISO/IEC 15408 Standard requirements as of May 2019-2024. Certification applicable to HP Enterprise and Managed devices running HP FutureSmart Firmware version 4.5.1 and later. For more information: https://www.commoncriteriaportal.org/-files/epfiles/Certification%20Report%20-%20HP%-20Intrusion%20Detection.pdf.

[3] HP office-class printing systems are select Enterprise and Managed devices with FutureSmart firmware 4.5 and up, Pro devices, LaserJet models 200 and up, with respective Original HP Toner, PageWide and Ink Cartridges. Does not include HP integrated printhead cartridges. Digital supply-chain tracking, hardware and packaging security features vary locally by SKU. See hp.com/go/SuppliesThat-Protect and hp.com/go/SuppliesSecurityClaims.

[4] HP Security Manager must be purchased separately. For details, see hp.com/go/securitymanager.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA6-1168ENW, June 2021, Rev. 6