Technical brief

The world's most secure printers[1]

HP Enterprise embedded print security features

Only HP Enterprise devices 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.[1]

Protect, detect, and recover

HP printers have the industry's strongest security, 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.[1]

After a reboot occurs, HP JetAdvantage Security Manager automatically assesses and, if necessary, remediates device security settings to comply with pre-established company policies.[2] Administrators can be notified of security events via Security Information and Event Management (SIEM) tools such as ArcSight, McAfee, Splunk, and SIEMonster.

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.

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.

Run-time intrusion detection—monitors memory activity

HP's run-time intrusion detection helps protect printers while they are powered on and connected to the network—right when most attacks occur. This technology checks for anomalies during complex firmware and memory operations, automatically stops the intrusion, and reboots.

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.

Learn more: hp.com/go/PrintersThatProtect

[1] HP's most advanced embedded security features are available on HP Enterprise-class devices with FutureSmart firmware 4.5 or above and is based on HP review of 2018 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/printersecurityclaims.

[2] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

How does it work?

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

HP JetAdvantage Security Manager completes the check cycle.

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 startup to determine if it's authentic code—digitally signed by HP.

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.

Three. Check printer settings

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

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA6-1168ENW, September 2019, Rev. 5