Technical brief

The world's most secure printers[1]

HP Wolf Enterprise Security embedded print security features

Only HP Enterprise devices have these self- healing embedded security features. With the investment protection that HP FutureSmart[4] firmware provides, you can add new features to many existing HP Enterprise printer models.[1]

Protect, detect, and recover

HP printers have the industry's strongest security[1], with five 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 the BIOS

The first step of the startup lifecycle is to load the BIOS, which performs hardware initialization during the boot process. It is essential that this code is protected since it is the "Root of Trust." All other device-hardening measures depend on a safe and secure BIOS. Any malware in this layer would not be detectable by other layers. HP's innovative Sure Start technology validates the integrity of the BIOS code and provides a self-healing capability if the BIOS becomes compromised. HP uses hardware to isolate and protect the "Golden Copy" of the BIOS which prevents access during normal run-time execution on the device. The BIOS is hashed and signed with a cryptographic signature, which is verified during boot. The device can revert to the "BIOS Golden Copy" in the event that the BIOS becomes compromised. Boot time is an opportunity for attackers to load a rootkit, enabling cybercriminals to control and infect anything that loads after the BIOS. Sure Start protects against BIOS rootkits like LoJax.

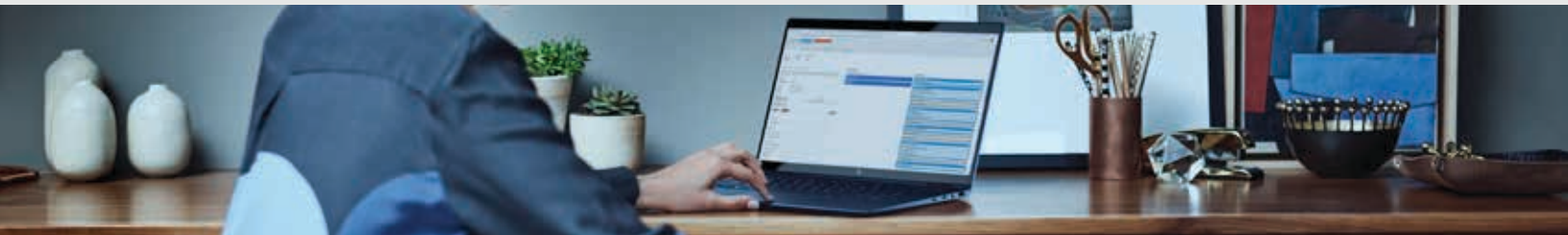
Whitelisting—checks for authentic firmware, digitally signed by HP

The second step in the startup lifecycle is to ensure that the device only loads HP-authentic code. HP provides a dynamic Whitelisting technology that ensures only authentic, untampered, executable code can run on HP printers. To clarify the terminology, a blacklist is used by antivirus scanners today, which rely on identifying fingerprints of known malware. However, the problem with a blacklist is that it typically takes about four days or more to isolate a new virus after a zero-day attack and publish an anti-virus update that needs to be downloaded by the system.

Embedded devices, such as printers, being a closed system, have the luxury of knowing the code that should be loaded and can restrict execution to only "known good files' on a system. HP supports this whitelist feature by loading only known software into memory and calculating the hash of this code that is compared against the known "good" signed hash value to verify its integrity.

HP Security Manager[2]

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



HP Memory Shield™ 3 Runtime Intrusion Detection—monitors the memory of the Kernel OS

The fourth step provides a series of functions. HP Memory Shield's™ Runtime Intrusion Detection is one of the most effective ways to protect against unknown or new attacks (zero-day attacks) since it looks for behavioral anomalies in memory. Runtime Intrusion Detection is built into the hardware which has the benefit of making it more difficult to circumvent the detection capability than firmware-based solutions.

HP Memory Shield™ Control Flow Integrity—monitors the execution flow of the firmware

HP Memory Shield™ Control Flow Integrity (CFI) provides a deterministic way to identify when potential malware is being injected into a vulnerable interface. HP's Memory Shield™ CFI locks down each device according to its factory image, preventing the execution of any calls or operations that are not manufacturer-defined. It does not need to rely on malware signatures to block both current and future malware.

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

How does it work?

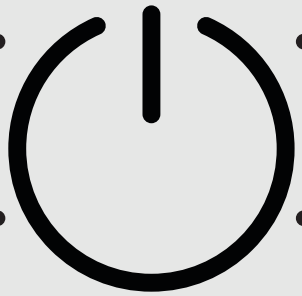
The embedded security features address three primary steps in the cycle of an HP Enterprise device. HP Security Manager completes the check cycle.

1. Check BIOS code

HP Sure Start
Checks BIOS code and, if compromised, restarts with a Golden copy of the BIOS

2. Check firmware

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



3. Check printer settings

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

4. Continuous monitoring

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

Control Flow Integrity
Monitors the execution flow of firmware

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 Managed and Enterprise devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of published features as of February 2023 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. HP Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager
3. HP Memory Shield™ is available on the HP Color/Mono LaserJet Enterprise M400 series, the HP Mono/Color LaserJet E40000 series and any future HP Enterprise LaserJet devices running FS 5.4 or later.
4. Some features enabled by future HP FutureSmart firmware upgrades may not be available on older devices, if for example, physical product characteristics limit the functionality of the new feature.

Sign up for updates hp.com/go/getupdated

4AA6-1168ENW, July 2023, Rev. 8