Technical brief

Defend your network with our most secured printers[1]

HP print security features

Protect, detect, and recover

The latest generation of HP Enterprise printing devices are unique in the marketplace, because they offer three key technologies together designed to thwart attackers' efforts and self-heal. These features automatically trigger a reboot in the event of an attack or anomaly.

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] There's no need for IT to intervene. Administrators can be notified via HP management applications such as JetAdvantage Security Manager and ArcSight.

HP Sure Start

The BIOS is a set of boot instructions used to load fundamental hardware components and initiate the HP FutureSmart firmware of an enterprise-class HP device. HP Sure Start technology works behind the scenes when devices power on—helping to safeguard your printing and imaging device from attack. HP Sure Start validates the integrity of the BIOS at every boot cycle. If a compromised version is discovered, the device restarts using a safe, "golden copy" of the BIOS.

Whitelisting

Enterprise-class HP devices feature FutureSmart firmware. Like a PC's operating system, firmware coordinates hardware functions, runs the control panel, determines what features are available when printing, scanning, or emailing, and provides network security. Compromised firmware could open your device and network to attack. Whitelisting helps ensure only authentic, known-good HP code that has not been tampered with is loaded into memory. If an anomaly is detected, the device reboots to a secure, offline state. It then sends a notice to IT to reload the firmware.

Run-time intrusion detection

Most of us wouldn't leave our computers running unguarded. Yet few vendors offer this basic level of protection for their imaging and printing devices.[1] HP's run-time intrusion detection helps protect devices while they are operational and connected to the network—right when most attacks occur. This feature checks for anomalies during complex firmware and memory operations. In the event of an intrusion, the device automatically reboots.

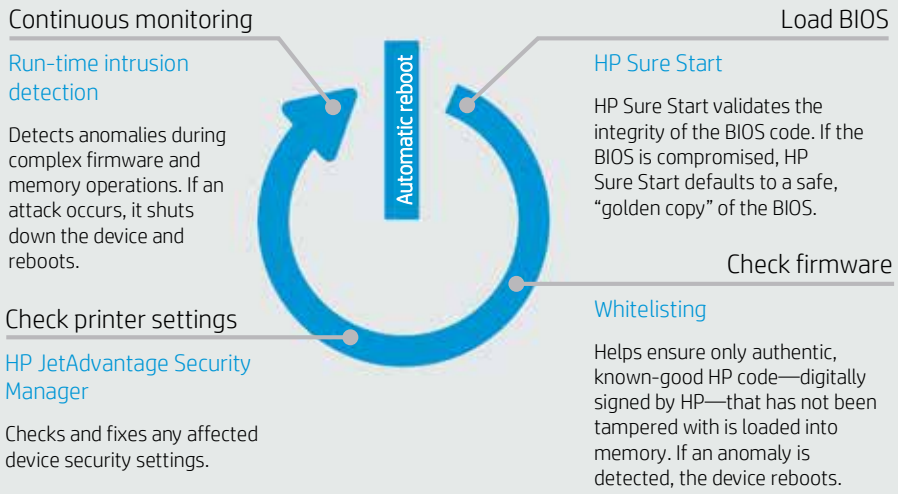
Learn more: hp.com/go/PrintersThatProtect

[1] A FutureSmart service pack update may be required to activate security features. Some features will be made available as a HP FutureSmart service pack update on selected existing Enterprise printer models. For list of compatible products, see hp.com/go/LJCompatibility.
[2] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

How does it work?

The embedded security features address three primary steps in the cycle of an HP device.

HP JetAdvantage Security Manager completes the check cycle.



Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA6-1167EECI, February 2016