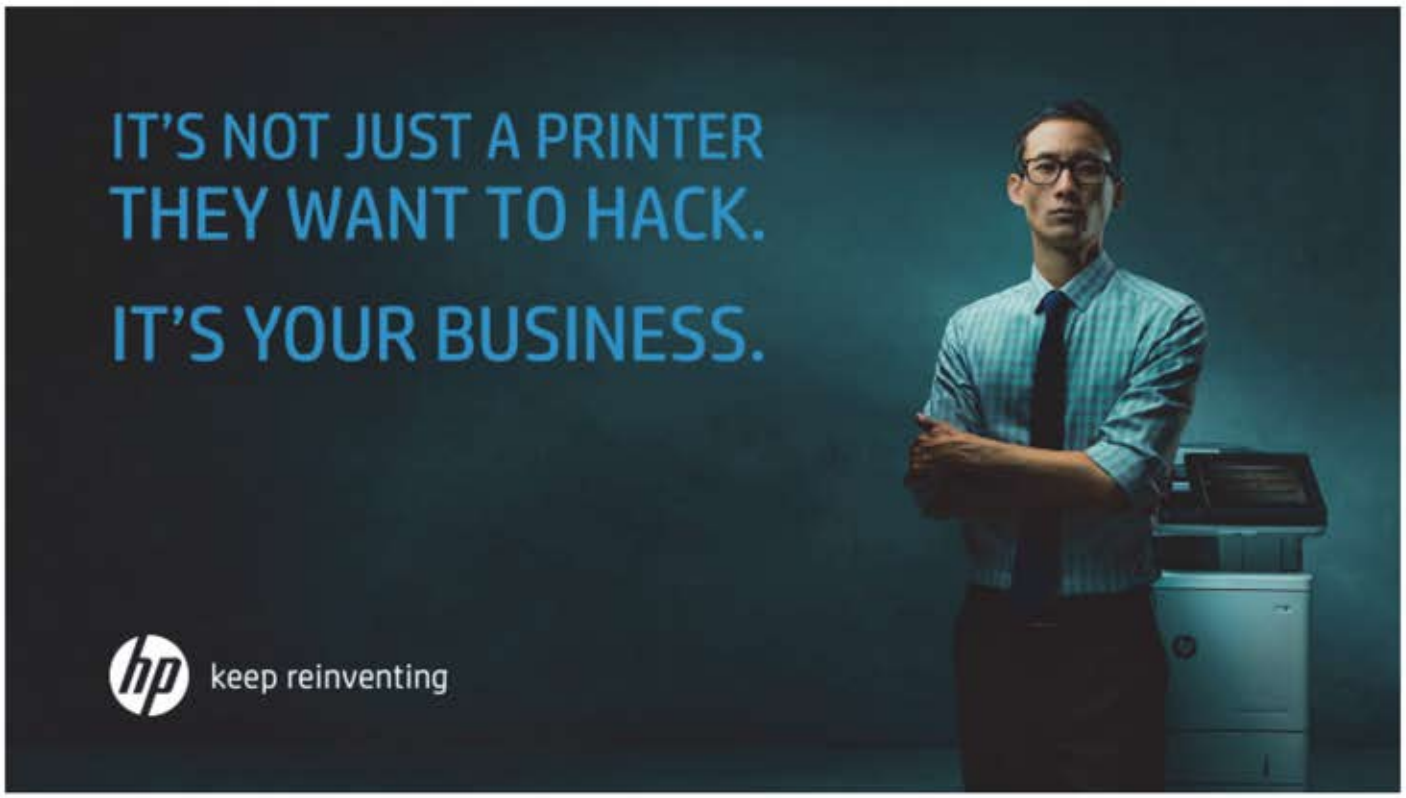
HP's Printer Security – 5 Key Areas & Robust Features To Protect Your Business

HP says that in a survey of 2,000 IT pros, 56% didn't see printers as a risk and 46% said that they need additional training for it.

The truth is that printers are a part of the network that needs to be secured, and they can be easily overlooked, making them a target. Vulnerabilities can range from leaving documents in the printer tray, to exposed network ports, to data being compromised in transit.



Your printer has a CPU, an operating system that probably doesn't receive security patches much, if at all, and truth be told, it's probably the least secure node on your network. It's not all that different from a PC. HP says there are five key areas of printer security (which many of their fleet have this technology):

1. **Sure Start:** a secure boot process. this includes validating the BIOS when the device is booted, and if it's corrupted, replace it with a hardware-protected copy of it. The term "self-heal" is used a lot here, as the best security measures are ones that can be automated. As anyone with knowledge of IT security knows, the weakest point is always the people.

2. **Whitelisting:** the printer also validates firmware integrity upon booting. As with secure boot, an administrator will be notified of any issues.

3. **Run-time intrusion detection:** is "continuous monitoring for in-memory malware injection attacks", the printer will automatically halt all operations and reboot if any malware is detected, bringing us right back to Sure Start and Whitelisting. The algorithm to detect this is inserted into different places in the code, and HP says that those places are random, which would make it harder to corrupt.

4. **Continuous assurance of security policy settings:** the idea behind this is bringing devices that aren't compliant into compliance. The tool has an 'Intuitive Security Policy editor', which will help the admin to make the appropriate settings.

5. **Real-time threat detection and analysis**: this is done with a SIEM, or Security Information Event Management system. This will integrate with other nodes on the network, focusing on one of the top security concerns, which is the exposure of data while it's in transit between nodes.

One of the solutions that HP provides is called JetAdvantage Secure Print. This makes sure that printed documents can only be sent to authorized devices. This takes a number of risk factors out of the equation, such as an employee that's working from home and using their own personal printer. It can also minimize other human-based risks, such as sensitive documents that are left out in the open.

These aren't the old days anymore, when printers weren't attached to a network. Now, your printer is probably attached to a network cable - if not Wi-Fi - and through that, it's just waiting for a command.

Part of the problem is that many IT pros don't take it seriously enough, and if HP knows it, you can bet that hackers know it as well. On top of general negligence, most printers simply aren't made to be secure, and unlike a modern PC, they receive very few security patches, and this leaves the job up to you.

Luckily, HP is one of the companies that's doing a lot of work in this area. Being able to check for a corrupt BIOS or firmware is a major step, as is the ability to automatically reboot the device when malware is detected. This is what's meant by self-healing, as the printer is actually fixing itself. After all, many PCs have antivirus software, so if your printer is even less secure, why wouldn't that have software to fix itself as well?

Your printer is probably already behind a firewall, so if it gets infected, there's nothing stopping the attack from spreading across the entire network. As HP points out, your printer is an endpoint, so if you're an IT pro, it's certainly something that you should be aware of.

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, 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

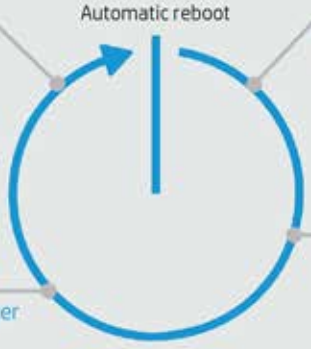
[1] HP's most advanced embedded security features are available on HP Enterprise-class devices with FutureSmart firmware 4.5 or above and is based on HP review of 2016-2017 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: www.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.

Three. Check printer settings

HP JetAdvantage Security Manager
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.

Sign up for updates

Share with colleagues

4AA6-1168ENW, September 2017, Rev. 4