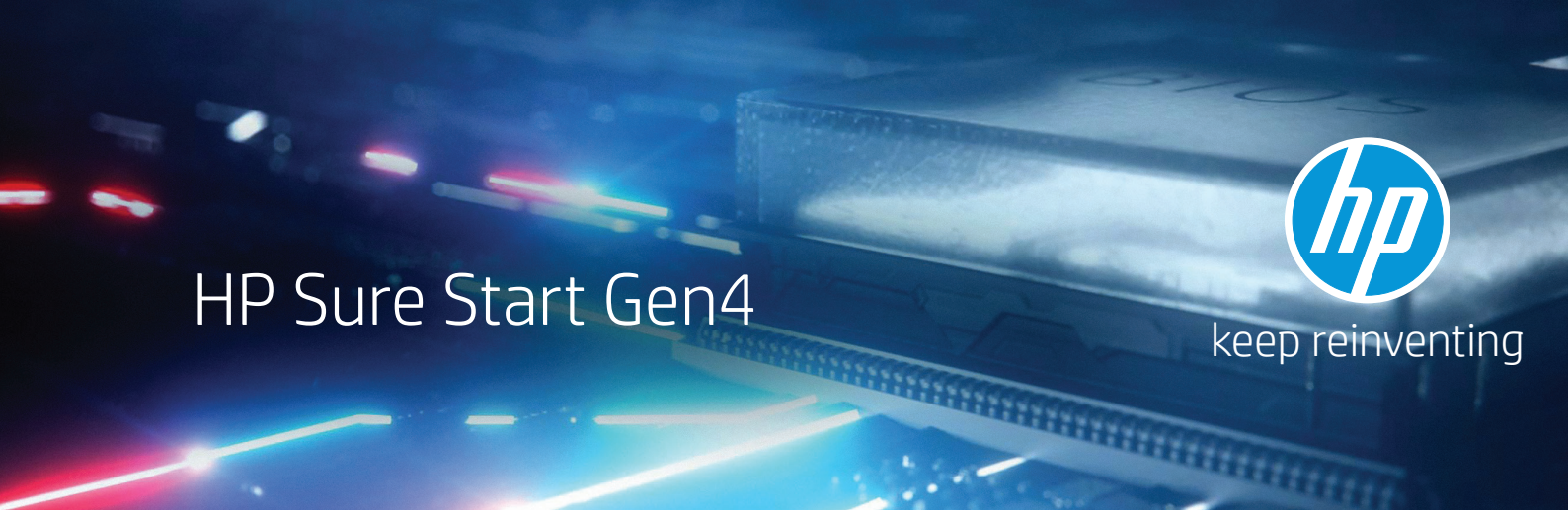

HP Sure Start Gen4

keep reinventing

Protect firmware that antivirus solutions can't with the first and only self-healing PC BIOS. HP Sure Start Gen4[1] automatically self-heals the BIOS from malware, rootkits, or corruption. With Runtime Intrusion Detection and easy manageability, HP Sure Start Gen4 can help you increase security, minimize downtime, and prevent costly security breaches.

BIOS attacks are a growing threat

As our world becomes even more connected, cyber-attacks are targeting endpoint firmware and hardware with increasing frequency and sophistication.

BIOS protection is more important than ever. The BIOS is the first million lines of firmware code run by your PC when you turn it on, and it is responsible for securely booting the operating system (OS).

If malware affects the BIOS, an attacker can get unlimited control of your PC to steal valuable data, insert ransomware, or render your PC inoperable.

Because antivirus software is unable to monitor for attacks in the firmware, malware hiding in the BIOS can be virtually impossible to detect. It can also be incredibly difficult to remove, requiring the replacement of the whole motherboard, or even the entire PC.

Industry's first self-healing BIOS

HP Sure Start is unique, hardware-enforced BIOS protection. In the event of a malware attack on the BIOS, HP Sure Start Gen4 automatically detects the change, notifies the user and IT, and restores the most recent good version of the BIOS.

HP Sure Start works by identifying any unauthorized changes to the BIOS, rather than trying to find known malware—which means that HP Sure Start can protect you against attacks the world has never seen before.

Runtime Intrusion Detection

Your BIOS doesn't just work when you start your PC. Some critical BIOS code continues running in your system RAM while you work.

HP Sure Start Gen4 includes a specialized runtime intrusion capability, which can detect and report changes to this critical BIOS code in runtime memory (SMM) while the OS is running. This offers enhanced protection to critical processes like virtualization that depend on the SMM.

HP provides this type of capability for runtime SMM BIOS.

A legacy of protection

Since 2014, HP Sure Start has been enabled by a unique hardware element—the HP Endpoint Security Controller.

HP Sure Start Gen4 now leverages the HP Endpoint Security Controller for strong, hardware-based protection of the secrets stored by the BIOS, providing best-in-class confidentiality protection of settings and user credentials. HP Sure Start Gen4 also provides expanded protection for additional firmware components.

Manageability

HP Sure Start Gen4 gives you automated protection that can be managed centrally by your IT team. You can set HP Sure Start Gen4 settings remotely and monitor tamper alerts from Microsoft® System Center Configuration Manager through the HP Manageability Integration Kit G2[2] (HP MIK) plug-in.

Frequently asked questions:

Q: What do I need to do to start benefitting from HP Sure Start Gen4?

A: HP Sure Start Gen4, including the Runtime Intrusion Detection feature, is enabled by default for all applicable platforms shipped from the HP factory. There is no need to enable or otherwise "deploy" the feature. If your device ships with HP Sure Start Gen4, you are protected from the very first time you start it.

Q: My company uses a custom software image: does reimaging the machine delete HP Sure Start?

A: HP Sure Start Gen4 is hardware enforced and exists in the BIOS. Reimaging a machine does not delete it or disable its monitoring and self-healing protection of your BIOS.

Certain OS-dependent features of HP Sure Start Gen4 (such as remote runtime monitoring or in-OS notifications in Windows® Event Viewer) can be changed or disabled depending on the OS used.

Q: I have a growing business but no IT department. Can I still use HP Sure Start?

A: Yes. Because HP Sure Start Gen4 is enabled by default, you are automatically protected. No IT action is required.

Q: What kind of attacks does HP Sure Start Gen4 protect against?

A: HP Sure Start protects against any unauthorized changes to the BIOS code or BIOS settings, both for the boot time code and the runtime code. These capabilities protect you from a variety of different attacks, including new BIOS attacks that may arise in the future.

Q: If malware can attack the BIOS, why can't it corrupt HP Sure Start Gen4's copy of the BIOS?

A: HP uses unique technology, backed by the HP Endpoint Security Controller, to isolate the HP Sure Start Gen4 clean copy of the BIOS from the copy of the BIOS that's in use by the machine. It is hardware protected and inaccessible to hackers.

Certifications and Standards:

Certified Hardware:

The HP Endpoint Security Controller used in HP Sure Start Gen4 platforms has been **verified by an accredited independent test lab** to operate as claimed by HP per publicly available criteria, methodology, and processes.

NIST Guidelines:

HP Sure Start Gen4 platforms meet and exceed the Draft NIST Platform Firmware Resiliency Guidelines **for host processor boot firmware** (Special Publication 800-193).

Learn more at www.hp.com/go/computersecurity

1. HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® or AMD processors.
2. HP Manageability Integration Kit can be downloaded from http://www.hp.com/go/clientmanagement.

4AA7-2562ENW