HP SURE START

INFOSHEET

HP WOLF SECURITY

HP Sure Start[1] is an advanced hardware-enforced solution providing comprehensive firmware and firmware setting security. Starting as the world's first self-healing BIOS, HP Sure Start now extends beyond the BIOS to protect critical firmware that antivirus solutions can't protect. Providing hardware enforced self-healing protection of boot-critical firmware from malware, rootkits, or corruption to help you maintain business continuity in the face of destructive attacks to the firmware.

FIRMWARE ATTACKS ARE A CURRENT THREAT

Mosaic Regressor, like Lojax and other forms of BIOS attacks, have evolved to new categories of threats impacting PCs. These attacks have become difficult to detect, are persistent, and are hard to remove. They are powerful, gaining total control of a PC with the highest level of privilege.

If malware affects the BIOS or critical firmware, the attacker can steal valuable data, insert ransomware, or render your PC inoperable.

Hardware-enforced protection of and resilience for both BIOS and other critical firmware at bootup and during operation is more important than ever.

HARDWARE-ENFORCED PROTECTION

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

HP Sure Start leverages the HP Endpoint Security Controller for strong, hardware-based protection of the code, data, and secrets stored by the BIOS and critical firmware.

INDUSTRY'S FIRST SELF-HEALING BIOS

Starting as the world's first hardware-enforced self-healing BIOS protection, and after generations of enhancements, today's HP Sure Start provides the most comprehensive PC firmware protection and resilience solution available on the market.

In the event of a malware attack on the BIOS or Critical Firmware, HP Sure Start automatically detects the change, notifies the user, securely logs the event for IT and restores the most recent good version of the BIOS or firmware.

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

MANAGEABILITY

HP Sure Start gives you automated protection that can be managed centrally by your IT team. You can set HP Sure Start settings remotely and monitor tamper alerts with the following manageability solutions.

- Microsoft® System Center Configuration Manager through the HP Manageability Integration Kit[2] (HP MIK) plug-in.
- HP Client Management Script Library is a powerful tool that enables straightforward integration with any management console, including modern management consoles.

UNIQUE FIRMWARE PROTECTION

HP Sure Start provides a unique, and robust set of protection capabilities.

- Protection both before firmware is executed and at runtime
- Protects CODE and DATA
- Intel Manageability Engine firmware / AMD Secure Processor / CPU microcode
- Cryptographically protected storage of settings and secrets
- Dedicated/isolated policy and recovery firmware storage
- Active even when PC is off. Operates independently of main CPU
- Closed and Open Chassis Direct Memory Access attack protection

PRODUCT PORTFOLIO SUPPORT

HP Sure Start is included from the factory across a wide range of the HP commercial product portfolio.

- ZBook & Z Workstations
- Pro & Elite Notebooks and Desktops (Intel vPro & non-vPro and AMD processors)
- Select RPOS and Thin Clients

CERTIFICATES & STANDARDS

CERTIFIED HARDWARE

The HP Endpoint Security Controller used in HP Sure Start 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 platforms go significantly beyond the NIST Platform Firm ware Resiliency Guidelines for host processor boot firmware, to protect many other boot critical firmware.

(Special Publication 800-193).

Learn more in the HP Sure Start Whitepaper.

FREQUENTLY ASKED QUESTIONS

Q: What do I need to do to benefit from HP Sure Start?
A: HP Sure Start 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, 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 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 and critical firmware.

Certain OS-dependent features of HP Sure Start (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 is enabled by default, you are automatically protected. No IT action is required.

Q: What is a Direct Memory Access (DMA) attacks?
A: A DMA attack is one where an attacker uses peripheral hardware to bypass all existing OS memory access controls to read or write the OS main memory directly. Systems with HP Sure Start use virtualization hardware to block malicious DMA.

Q: What kind of attacks does HP Sure Start protect against?
A: HP Sure Start protects against any unauthorized changes to the BIOS & critical firmware 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 firmware attacks that may surface in the future.

Q: If malware can attack the BIOS, why can’t it corrupt HP Sure Start ’s copy of the BIOS?
A: HP uses unique technology, backed by the HP Endpoint Security Controller, to isolate the HP Sure Start clean copy of the BIOS & critical firmware from the copy of the BIOS & critical firmware that are in use by the machine. It is hardware protected and inaccessible to hackers.

[1] HP Sure Start Gen6 is available on select HP PCs and requires Windows 10.
[2] HP Manageability Integration Kit can be downloaded from http://www.hp.com/go/clientmanagement.

Learn more at hp.com/go/computer security.

HP WOLF SECURITY