Technical whitepaper

HP Sure Start for AMD

July 2019
L75214-001

Table of contents

List of figures

List of tables

1 Introduction

HP Sure Start for AMD®[1] can automatically detect, stop, and recover from a BIOS attack or corruption without IT intervention and with little or no interruption to user productivity. Every time the PC powers on, HP Sure Start for AMD automatically validates the integrity of the BIOS code to help ensure that the PC is safeguarded from malicious attacks. In the case of an attack, the PC can self-heal using an isolated "golden copy" of the BIOS in less than a minute.

1.1 Why is BIOS protection important?

As our world becomes more connected, cyber-attacks are targeting client device firmware and hardware with increasing frequency and sophistication. Tools and techniques to attack firmware were once theoretical and thought only to be available to nation-states. Such tools and techniques have since been shown to not only exist, but to be readily available in the public domain.

The device firmware (or BIOS) is an attractive target for attackers because of the potential advantages a successful breach could provide:

- Persistence: Firmware resides in a nonvolatile memory on the circuit board and can't be removed simply by erasing the hard drive.
- Control: Firmware executes at the highest privilege level—outside of the OS domain—which enables the possibility of OS-independent malware.
- Stealth: Firmware occupies a region of memory that is completely inaccessible to the operating system and system software; since it can't be scanned by antivirus it may never be detected.
- Difficulty of recovery: All these aspects make it extremely difficult to recover from this type of infection without resulting down time and a potential system board replacement.

The ideal solution to protect devices against this type of attack is designed from the hardware up using "cyber resiliency" principles. These principles acknowledge that it is extremely difficult, if not impossible, to foresee and prevent every possible attack. The ideal solution not only provides enhanced protection of the firmware, but also includes a hardware rooted ability to both detect a successful attack and recover from it.

1.2 HP Sure Start for AMD provides superb firmware protection

HP Sure Start for AMD is HP's unique and groundbreaking approach to provide advanced firmware protection and resiliency to HP PCs. It uses hardware enforcement via the HP Endpoint Security Controller (HP ESC) to provide protection of the BIOS that reaches well beyond the industry standard and ensures that the system will only boot Genuine HP BIOS.

Summary of HP Sure Start for AMD features:

- HP core platform firmware authenticity enforcement and tamper protection—HP Endpoint Security Controller hardware enforcement of the system boot, so only authentic and unmodified HP firmware and HP BIOS are loaded
- Firmware health monitoring and compliance—Logging of firmware health-related events via isolated HP Endpoint
- Security Controller; presents the platform firmware state along with any anomalies that could indicate thwarted attacks
- Self-healing—Automatic repair of HP BIOS and HP firmware corruption, using the HP Endpoint Security Controller isolated backup copy of HP BIOS and HP firmware
- BIOS setting protection—Extension of the HP Endpoint Security Controller protection of the BIOS code to include HP ESC backup and integrity-checking of all user or admin-configured BIOS settings
- Secure boot keys protection—Significantly enhanced protection of databases and keys stored by the BIOS that are critical to the integrity of the OS secure boot feature versus standard UEFI BIOS implementation

[1] HP Sure Start for AMD is available on select HP PCs with AMD processors. See product specifications for availability.

- Protected storage—Strong cryptographic methods to store BIOS settings, user credentials, and other settings in the HP Endpoint Security Controller hardware to provide integrity protection, tamper detection, and confidentially protection for that data
- Manageability—Administrator management of HP Sure Start for AMD capabilities with the Manageability Integration Kit (MIK) plug-in for Microsoft® System Center Configuration Manager (SCCM)

1.3 Third-party security certification

The HP Endpoint Security Controller hardware used in HP Sure Start for AMD has undergone third-party security assessment and has been certified to provide hardware enforcement so that only authorized firmware can start on the target PC.[2]

Assurance that a security solution works as stated is a critical piece of any purchase decision related to security products. And because a reputation for quality can only go so far, HP has exposed the HP Endpoint Security Controller inner workings for review and testing by an independent and accredited laboratory to validate that it works as claimed per publicly available criteria, methodology, and processes.

1.4 Cyber-resilient design

Not only does HP Sure Start for AMD provide enhanced BIOS protection beyond the industry standard approach, but it is designed from the hardware up to provide unmatched platform cyber-resilience to ensure BIOS recovery even in the event of a breach or destructive attack. HP business PCs with HP Sure Start for AMD exceed the National Institute of Standards and Technology (NIST) Platform Firmware Resiliency guidelines (Special Publication 800-193) for host processor boot firmware and other critical platform device firmware, as discussed in Appendix A. NIST SP 800-193 is one of the leading public sector efforts to formalize requirements for cyber-resilient platforms. For more details about HP Sure Start for AMD and NIST 800-193, see Appendix A.

[2] The HP Sure Start for AMD controller hardware has been certified per the CSPN certification framework.

2 Architectural overview and capabilities

HP Sure Start for AMD consists of two major architectural components:

- HP Endpoint Security Controller running HP Sure Start for AMD firmware
- HP Sure Start for AMD BIOS working in conjunction with the HP Endpoint Security Controller hardware and firmware

2.1 Firmware integrity verification—the core of HP Sure Start for AMD

The HP Endpoint Security Controller (HP ESC) is the first device in the system to execute firmware when the system powers up, active well before the system boots. The HP ESC activities include, but are not limited to, monitoring the system power button and power sequencing the start of the host CPU execution when the user presses the power button.

When power is first applied to the platform (before the system is turned on), the HP ESC validates that its own firmware is authentic HP code before loading and executing the code. The HP ESC hardware uses industry-standard, strong cryptographic methods to perform the integrity verification. The method employs a 2048-bit HP RSA public key contained within internal permanent read-only memory. Therefore, the HP ESC is the built-in hardware-based Root of Trust (RoT) for the platform, used to validate its firmware and the HP BIOS before they are executed. This hardware Root of Trust protects against firmware replacement attacks regardless of their deployment method and serves as the foundation upon which HP platform security is built.

Figure 1 illustrates the firmware integrity verification process. Once the HP ESC authenticates and starts executing the HP Sure Start for AMD firmware, that firmware uses the same strong cryptographic operations to verify the integrity of the system flash BIOS boot block. If a single bit is invalid, the HP ESC replaces the system flash contents with its own copy of the HP BIOS boot block that is stored within an isolated nonvolatile memory (NVM) dedicated to the HP ESC.

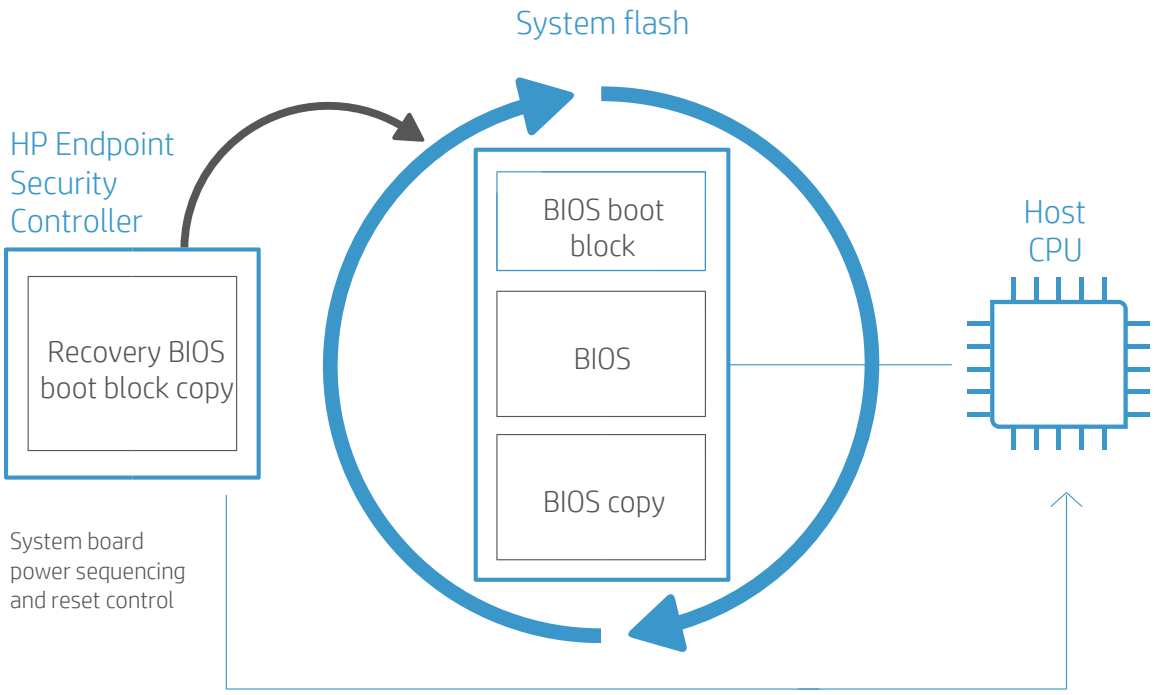

Figure 1 Firmware integrity verification process

The HP Sure Start for AMD design ensures all the firmware and BIOS code running on both the HP ESC and the host CPU is the code HP intended to be on the device.

NOTE: The system flash boot block integrity checking, and any needed recovery performed by the HP ESC, take place while the host CPU is off. Therefore, from a user point of view, the entire operation takes place when the system is still off, in sleep mode, or hibernate mode.

The system flash BIOS boot block is the foundation of the HP BIOS. The HP ESC hardware ensures that the BIOS boot block is the first code that the CPU executes after a reset. Once the HP ESC determines that the BIOS boot block contains authentic HP code, it allows the system to boot as it normally would.

The HP ESC also checks the integrity of the system flash boot block code each time the system is turned off or put into a hibernate or sleep mode. Since the CPU is powered off in each of these states and the CPU is therefore required to re-execute BIOS boot block code to resume, it is crucial to re-verify the integrity of the BIOS boot block each time to check for tampering.

2.2 Machine-unique data integrity

The HP ESC and BIOS work together to provide advanced protection of factory-configured critical variables unique to each machine that are intended to be constant over the life of any specific platform. In the factory, a backup copy of this variable data is saved in the HP ESC nonvolatile memory store. The backup is made available to the HP Sure Start for AMD BIOS component on a read-only basis to perform integrity checking of the data on every boot. If any setting in the shared flash is different from the factory settings, the HP Sure Start for AMD BIOS components will automatically restore the data in the System Flash from the backup copy provided by the HP ESC.

2.3 BIOS setting protection

As previously described, HP Sure Start for AMD verifies the integrity and authenticity of the HP BIOS code. Since this code is static after it is created by HP, digital signatures can be used to confirm both attributes of the code. The dynamic and user-configurable nature of BIOS settings, however, create additional challenges to protecting those settings. Digital signatures cannot be generated by HP and used by the HP Sure Start for AMD ESC hardware to verify those settings.

HP Sure Start for AMD BIOS setting protection provides the capability to configure the system so the HP ESC hardware is used to back up and check the integrity of all the BIOS settings preferred by the user.

When this feature is enabled on the platform, all policy settings used by BIOS are subsequently backed up and an integrity check is performed on each boot to ensure that none of the BIOS policy settings have been modified. If a change is detected, the system uses the backup from the HP Sure Start for AMD–protected storage to automatically revert to the user-defined setting.

The HP Sure Start for AMD BIOS setting protection feature generates events to the HP Sure Start for AMD ESC hardware when an attempt to modify the BIOS settings is detected. The event is logged in the HP Sure Start for AMD audit log, and the local user will receive a notification from BIOS during boot.

2.4 HP Sure Start for AMD-protected storage

Protected storage rooted in the HP Endpoint Security Controller hardware provides the highest level of protection for BIOS/firmware data and settings protected by HP Sure Start for AMD. HP Sure Start for AMD–protected storage is designed to provide confidentiality, integrity, and tamper detection even if an attacker disassembles the system and establishes a direct connection to the nonvolatile storage device on the circuit board.

2.4.1 Data integrity

The integrity of the dynamic data stored in nonvolatile memory by firmware and used to control the state of various capabilities is critical to the security posture of the overall platform. Dynamic data includes all BIOS settings that can be modified by the end user or administrator of the device. Examples include (but are not limited to) boot options such as the secure boot feature, BIOS administrator password and related policies, Trusted Platform Module–state control, and HP Sure Start for AMD policy settings.

Any successful attack that bypasses the existing access restrictions designed to prevent unauthorized modifications to these settings could defeat the platform security. As an example, consider a scenario where an attacker makes an unauthorized

modification to the secure boot state to disable it without being detected. In this scenario, the platform would boot the attacker's root kit before the OS starts, without the user's knowledge.

Industry-standard Unified Extensible Firmware Interface (UEFI) BIOS does implement access restrictions that should prevent unauthorized modifications to these variables, and HP implements these just like the rest of the PC industry. However, given the risks a breach of these mechanisms poses to the platform, HP Sure Start for AMD provides secondary defenses that are stronger than the baseline industry standard.

BIOS settings and other dynamic data used by firmware to control the state that is protected by HP Sure Start for AMD are stored in the isolated nonvolatile memory of the HP Endpoint Security Controller that is not directly accessible to software running on the host CPU.

Additionally, the HP ESC creates and appends unique integrity measurements each time a data element is stored in this nonvolatile memory store. The integrity measurements are based on a strong cryptographic algorithm (hashed-based message authentication code utilizing SHA-256 hashing) that is rooted to a secret contained within the HP ESC. The secret is unique to each HP ESC, such that each controller generates a unique integrity measurement given an identical element. When the data element is read back from the nonvolatile memory, the HP ESC recalculates the integrity measurement for that data element and compares it to the integrity measurement that is appended to the data. Any unauthorized changes to the data in the nonvolatile memory store result in a mis-compare. Using this approach, the HP ESC can detect tampering with data elements stored in the nonvolatile memory store.

2.4.2 Data Confidentiality

For many of the data elements stored by the platform, maintaining confidentiality is critical. Examples include BIOS administrator password hashes, user credentials, and secrets optionally stored by firmware on behalf of the user for firmware-based features such as HP Sure Run and HP Sure Recovery.

Protection of these secrets is challenging when industry-standard UEFI BIOS approaches are used, since the nonvolatile storage is typically readable by software running on the host processor. HP Sure Start for AMD–protected storage is intended to provide much greater protection of this confidential data than a standard UEFI BIOS implementation.

In addition to a separate isolated storage, HP Sure Start for AMD leverages the Advanced Encryption Standard (AES) hardware block contained within the HP ESC to perform AES-256 encryption on all confidential data elements stored in the HP Sure Start for AMD nonvolatile memory, in addition to the data integrity measurements for those elements. The encryption key used is unique to each HP ESC and never leaves that controller, so data encrypted by any individual HP ESC component can only be decrypted by that same HP ESC.

2.5 Secure boot keys protection

Compared to the industry-standard UEFI secure boot implementation, HP Sure Start for AMD provides enhanced protection of the UEFI secure boot key databases that are stored by the firmware. These variables are critical to proper operation of the UEFI secure boot feature that verifies integrity and authenticity of the OS bootloader before allowing it to start at boot.

HP Sure Start for AMD protects UEFI secure boot key databases by maintaining a master copy in HP Sure Start for AMD–protected storage.

Any authorized modifications to the UEFI standard secure boot key databases by the OS during runtime are tracked by HP Sure Start for AMD and applied to the master copy by the HP ESC. HP Sure Start for AMD then uses the master copy in HP Sure Start for AMD– protected storage to identify and reject any unauthorized changes to the UEFI standard secure boot keys databases.

This capability, enabled by default, covers the following databases:

- Signature database (db)
- Revoked signatures database (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) updated dynamically at runtime by the OS

3 User notifications, event logging, and policy management

3.1 HP Sure Start for AMD end user notifications

Under normal operating conditions, HP Sure Start for AMD is invisible to the user. When HP Sure Start for AMD identifies a problem, recovery operations are automatic, using the default settings with no end user or IT interaction usually required.

If any significant event is detected or action is taken, HP Sure Start for AMD displays a warning message on the next boot.

3.2 HP Sure Start for AMD event logging

The HP Endpoint Security Controller records critical events related to the firmware/BIOS code and data monitored by HP Sure Start for AMD. These events are stored within the Sure Start nonvolatile memory store. When HP Notifications software is installed, the events are copied from the HP ESC to the Windows Event Viewer to facilitate access to these events by the local user as well as the customer's preferred manageability agent.

The following events trigger the HP Notifications Software to gather all events from the HP Sure Start for AMD subsystem and ensure that the Windows Event Viewer is updated with any events that are not already recorded there:

- Windows Boot
- Windows Resume from Sleep/Hibernate
- Runtime Sure Start for AMD events

HP Notifications Software populates HP Sure Start for AMD events into a unique "HP Sure Start" application event log. Only HP Sure Start for AMD events will be included in this log. The Windows Event Viewer path to the HP Sure Start for AMD events is the following: System Tools/Event Viewer/Applications and Services Logs/HP Sure Start.

The Windows Event Viewer level categories related to HP Sure Start for AMD events are defined in the table on the next page.

The events are populated into Windows Event Viewer in the order that they were generated by HP Sure Start for AMD. The oldest event in the HP Sure Start for AMD subsystem is added to the Windows Event Viewer first and the most recent event is added last.

The timestamp for each Windows Event Viewer entry is the time it was added to that log, NOT the time the event occurred. Each Sure Start Windows Event Viewer entry includes detailed data within the event details, which includes the timestamp of the actual occurrence.

NOTE: Events are persistent in the HP Endpoint Security Controller even after being copied to the Windows Event Viewer. If the Windows Event Viewer is cleared, the HP Notifications Software application will replace all HP Sure Start entries on the next event that triggers it to check for HP Sure Start for AMD event logs.

Table 1 Types of HP Sure Start for AMD Windows Event Viewer events

Event Level	Definition
Info	Events that are expected to occur during the normal course of operation (e.g., updating the BIOS).
Warning	Unexpected events that have occurred but were fully recovered from by HP Sure Start for AMD and no user/admin action is required for the platform to be fully operational. These events are anomalous operations that the user/admin may want to investigate further, especially if there is a trend of these events across multiple machines.
Error	Events that require the admin/HP service to act on the platforms to fully recover.

3.3 HP Sure Start for AMD policy controls

Out of the box, the HP system BIOS enables and optimizes HP Sure Start for AMD policies for the typical user. Since HP Sure Start for AMD is enabled by default, the typical user is protected by HP Sure Start for AMD without having to modify the settings. For advanced users, the system BIOS provides some control of HP Sure Start for AMD behavior, using policy settings in the (F10) BIOS Setup. Unless otherwise noted, these settings and functions are located under Security/BIOS Sure Start.

NOTE: Policies are stored within the HP ESC nonvolatile memory that is not directly accessible by the host CPU; therefore, a reboot is required before any Sure Start settings take effect.

The following HP Sure Start for AMD settings and functions are available:

- Verify Boot Block on Every Boot
- BIOS Data Recovery Policy
- HP Sure Start BIOS Setting Protection
- HP Sure Start Secure Boot Keys Protection
- HP Sure Start Security Event Policy
- HP Sure Start Security Event Boot Notification
- Lock BIOS Version
- Save/Restore MBR of System Hard Drive
- Save/Restore GPT of System Hard Drive
- Boot Sector (MBR/GPT) Recovery Policy

3.3.1 Verify Boot Block on Every Boot

HP Sure Start for AMD always verifies the integrity of the system flash BIOS boot block before resuming from sleep, hibernate, or power-off. When set to enable, HP Sure Start for AMD will also verify the integrity of the boot block on each warm boot (Windows restart). The trade-off to consider is faster restart time versus more security. The default setting of this feature is disable.

3.3.2 BIOS Data Recovery Policy

When set to Automatic, HP Sure Start for AMD automatically repairs the BIOS or the Machine Unique Data when necessary. When set to Manual, HP Sure Start for AMD requires a special key sequence to proceed with the repair. In the case of an issue with the boot block code, the system will refuse to boot, and a unique blink sequence will flash on the system LED. The system LED that lights may vary by platform and by instance. In the case of an issue with the Machine Unique Data, the system will display a message on the screen. The key sequence required, and the blink sequence displayed, vary depending whether the system is a

notebook, a desktop, or a tablet. Manual mode is useful to users who can perform forensics on the system flash contents before repair. Typical users are not encouraged to use manual mode. The default setting of this feature is Automatic.

3.3.3 HP Sure Start BIOS Setting Protection

The BIOS setting protection policy is disabled by default. To enable the feature, the owner/administrator of the client device should first configure all BIOS policies to the preferred setting. The owner/administrator also must configure a BIOS setup administrator password.

Once that is completed, the BIOS setting protection policy should be changed to "Enable." At this point, a backup copy of all BIOS settings is created in the HP Sure Start for AMD–protected storage. Going forward, none of the BIOS settings can be modified locally or remotely. On each boot, the BIOS policy settings are verified to be in the desired state, and if there is any discrepancy, the BIOS settings are restored from the HP Sure Start for AMD–protected storage.

To modify a BIOS setting, the BIOS administrator password must be provided and BIOS setting protection subsequently disabled, at which point changes can be made to the BIOS settings.

3.3.4 HP Sure Start Secure Boot Keys Protection

With this setting at the factory default of enable, HP Sure Start for AMD provides enhanced protection of the secure boot databases and keys used by BIOS to verify the integrity and authenticity of the OS bootloader before launching it at boot. When set to disable, only standard UEFI secure boot variable protection is used and no backup copy is kept by the HP Sure Start for AMD subsystem.

3.3.5 HP Sure Start Security Event Policy

This BIOS policy setting controls what action is taken when HP Sure Start for AMD detects an attack or attempted attack while the OS is running. There are three possible configurations for this policy:

- Log event only: When this setting is selected, the HP ESC logs detection events, which can be viewed in the Applications and Services Logs/HP Sure Start for AMD path of the Microsoft Windows Event Viewer.[3]
- Log event and notify user: This is the default setting. When this setting is selected, the HP ESC logs detection events, which can be viewed in the Applications and Services Logs/HP Sure Start for AMD path of the Microsoft Windows Event Viewer.
- Additionally, the user is notified within Windows that the event occurred.[4]
- Log event and power off system: When this setting is selected, the HP ESC logs detection events, which can be viewed in the Applications and Services Logs/HP Sure Start for AMD path of the Microsoft Windows Event Viewer. Additionally, the user is notified within Windows that the event occurred, and that system shutdown is imminent.

3.3.6 HP Sure Start Security Event Boot Notification

This BIOS policy setting controls whether HP Sure Start for AMD warnings and error messages that are displayed when the system is booted require the local user to acknowledge the error before the boot continues. With the default Require Acknowledgement setting, the system halts with the error message displayed. The local user must press a key to continue the boot. If changed to Time out after 15 seconds, the message is displayed, but the boot process continues automatically after the message is displayed for 15 seconds.

3.3.7 Lock BIOS Version

In the (F10) BIOS setup, this feature is located in Main/Update System BIOS.

[3] HP Notification Software must be installed to view HP Sure Start for AMD events in the Windows Event Viewer.
[4] HP Notification Software must be installed to receive notifications.

When set to disable, you can update the BIOS using any supported process. When the HP ESC detects a valid boot block update in the system flash, it updates the backup copy of the boot block.

When set to enable, all HP BIOS update tools refuse to update the BIOS. In addition, HP Sure Start for AMD protects the BIOS from attempts to change the BIOS version by removing the system flash via an unauthorized method. The HP ESC records the locked-down version of BIOS. When the HP ESC detects that the BIOS in the system flash changed, the HP ESC overwrites the BIOS boot block with the HP ESC copy of the boot block. The HP ESC copy of the boot block executes and recovers the remainder of the correct version of the BIOS. The default setting of this feature is disable.

Save/Restore MBR of System Hard Drive and Save/Restore GPT of System Hard Drive

In the (F10) BIOS setup, this feature is located in Security/Hard Drive Utilities. Only one of these capabilities is available, depending on the partition type of the primary drive (GPT or MBR), as detected by HP Sure Start for AMD.

When set to enable, HP Sure Start for AMD maintains a protected backup copy of the MBR/GPT partition table from the primary drive and compares the backup copy to the primary on each boot. If a difference is detected, the user is prompted and can choose to recover from the backup to the original state, or to update the protected backup copy with the changes. The Boot Sector (MBR/GPT) Recovery Policy can optionally be used to remove the user decision for the action taken in the event of a discrepancy found by HP Sure Start for AMD.

When set to disable (default), no MBR/GPT protection is provided by HP Sure Start for AMD.

3.3.8 Boot Sector (MBR/GPT) Recovery Policy

When set to Local User Control (default) the user is prompted for the action to take when HP Sure Start for AMD detects a change in the MBR/GPT partition table. When set to Recover in the event of corruption, HP Sure Start for AMD automatically restores the MBR/GPT to the saved state any time differences are encountered.

3.4 Remote management of HP Sure Start for AMD policy controls

Out of the box, HP Sure Start for AMD policies are optimized for the typical user. Since HP Sure Start for AMD is enabled by default, there is no need for the remote administrator to take any action to enable (“deploy”) HP Sure Start for AMD. If a remote administrator wants to modify HP Sure Start for AMD policy settings, the same Windows Management Instrumentation (WMI) APIs or HP BIOS Configuration Utility scripts that are used to manage other platform BIOS policies can be used to manage HP Sure Start for AMD policies. In addition, administrators can remotely manage HP Sure Start for AMD capabilities with the Manageability Integration Kit (MIK) plug-in for Microsoft System Center Configuration Manager (SCCM).

Also, administrators can remotely manage HP Sure Start for AMD capabilities and view HP Sure Start for AMD events with the Manageability Integration Kit (MIK) plug-in for Microsoft System Center Configuration Manager (SCCM).

4 Conclusion

HP Sure Start for AMD delivers these key benefits:

- Uninterrupted productivity—HP Sure Start for AMD maintains business continuity in the event of an attack or accidental corruption by eliminating downtime waiting for an IT/Service event.
- Lower cost—HP Sure Start for AMD's ability to recover automatically reduces calls to the IT Help Desk and enhances productivity, which ultimately helps lower the maintenance cost for the platform.
- Peace of mind—HP Sure Start for AMD has multiple security features that run across a wide variety of software and hardware platforms.

Protect critical BIOS firmware from malware with the industry-leading firmware intrusion detection and automatic repair offered by HP Sure Start for AMD, exclusively available on select HP Elite PCs.

Learn more: hp.com/go/computersecurity

Links to technical content: support.hp.com/us-en/topic/goIT

5 Appendix A–NIST SP 800-193: Platform Firmware Resiliency Guidelines

Released in May 2018, the NIST SP 800-193: Platform Firmware Resiliency Guidelines describe guidelines for security mechanisms to protect platform firmware against unauthorized changes, detect unauthorized changes that occur, and recover from these unauthorized changes.

These guidelines outline three different resiliency properties:

1. Protected: meets all protection and secure update requirements
2. Recoverable: meets all detection and recovery requirements
3. Resilient: meets all protection, detection, and recovery requirements

Of these three properties, Resilient is the strongest, providing the most benefit to HP customers. HP Sure Start for AMD meets or exceeds all Resilient guidelines in NIST SP 800-193 for host processor boot firmware, also known as the UEFI BIOS. Further, HP Sure Start for AMD also meets requirements for other Critical Platform Device Firmware, as shown in Table 2 below.

5.1 Prior NIST guidelines for BIOS security

NIST SP 800-193 goes beyond NIST SP 800-147, which only addressed protection and the secure update of the platform's UEFI BIOS. HP Sure Start for AMD prior generations of HP Sure Start, along with HP all support NIST SP 800-147.

NIST SP 800-193 also goes beyond NIST SP 800-155, which outlined security components and guidelines to establish a secure BIOS integrity measurement and reporting chain. Likewise, HP Sure Start for AMD and prior generations of HP Sure Start, along all support NIST SP 800-155.

5.2 NIST SP 800-193 Critical Platform Devices in HP Commercial PCs

NIST SP 800-193 acknowledges that the definition of Critical Platform Devices can vary. Critical Platform Devices are defined in section 3.2 (Resiliency Properties):

> *"For a platform as a whole to claim resiliency to destructive attacks, the set of platform devices necessary to minimally restore operation of the system, and sufficient to restore reasonable functionality, should themselves be resilient. We call this set of devices critical platform devices. The particular resiliency properties may vary from platform-to-platform."*

For that reason, it is important to define this set of devices and applicable firmware for HP Sure Start for AMD Commercial PCs. NIST SP 800-193 provides a reference platform architecture in Section 2 along with a list of devices which are "often critical to the normal and secure operation of a platform." The table below provides a mapping to each of those devices/subsystems to the applicable firmware components in HP Sure Start for AMD Commercial PCs.

Note that each customer environment should be evaluated to determine whether there are additional peripheral devices that are critical to restore reasonable functionality specific to the customer's deployment.

Table 2 Critical Platform Device Firmware protected by HP Sure Start for AMD or other technology

NIST SP 800-193 Platform Architecture Reference	HP Commercial PC critical platform device firmware	Protected by:
1. Embedded Controller (EC)/Super I/O (SIO) 4. Host Processor 6. Graphics Processing Unit (GPU) when implemented as Unified Memory Architecture (UMA) 8. Host Controller (HC) for mass storage device 9. Host Processor Boot Firmware 10. Platform Runtime Firmware 11. Power Supply 15. Fans	HP ESC firmware HP UEFI BIOS firmware	HP Sure Start for AMD
2. Trusted Platform Module (TPM)	Discrete TPM component firmware[1]	TPM
3. Baseboard Management Controller (BMC)/Management Engine (ME)	AMD Secure Processor firmware	Not protected
5. Network Interface Controller (NIC)	Network Controller firmware[2]	Not protected[2]
7. Serial Peripheral Interface (SPI) Flash	N/A[4]	N/A[4]
9. Hard Disk Drive (HDD)/Solid State Drive (SSD)	HDD/SSD firmware	N/A[3]
10. Embedded MultiMediaCard (eMMC)/ Universal Flash Storage (UFS)	N/A[4]	N/A[4]
14. Glue Logic (CPLD's, FPGA's)	N/A[4]	N/A[4]

[1] This component is not critical to boot of the platform.
[2] This component is not critical to minimally restore operation of the system but is required to establish Ethernet connectivity in environments where that connectivity is deemed critical to platform resiliency.
[3] Mass storage devices are outside the scope of this document. Resiliency capabilities vary by storage supplier and by storage device. Not all suppliers or devices currently meet all Resiliency requirements in 800-193.
[4] No devices of this type are included.

5.3 Acronyms

- **BIOS** – Basic Input/Output System (aka host processor boot firmware)
- **CPU** – Central processing unit
- **ESC** – HP Endpoint Security Controller
- **HMAC** – Hash-based message authentication code
- **HW** – Hardware
- **OS** – Operating system

- **POST** – Power-On Self-Test
- **RoT** – Root of Trust (defined in NIST SP 800-193)
- **RTD** – Root of Trust for Detection (defined in NIST SP 800-193)
- **RTRec** – Root of Trust for Recovery (defined in NIST SP 800-193)
- **SMM** – System Management Mode
- **UEFI** – Unified Extensible Firmware Interface

Table 3 Required functions for Host Processor Boot Firmware

The table below provides a summary of each function described by NIST SP 800-193.

NIST SP 800-193	HP Sure Start	
Roots of Trust *(Section 4.1)*	**Meets** all Resiliency Requirements	HP Sure Start for AMD uses a hardware-based RoT (the HP ESC) with immutable boot firmware, which cryptographically verifies subsequent firmware before launching it, creating a Chain of Trust. HP Sure Start for AMD includes a key store and approved digital signing algorithms based on FIPS 186-4 to verify the digital signature of firmware update images. HP Sure Start for AMD uses authenticated update, detection, and recovery mechanisms, which are anchored in 's HW-based RoT.
Protection and Update of Mutable Code *(Section 4.2.1)*	**Meets** all Resiliency Requirements	HP Sure Start for AMD uses an authenticated update mechanism anchored in HP Sure Start for AMD 's HW-based RoT. Firmware update images are digitally signed by HP's code signing service (HP Secure Sign) and verified prior to updating. HP Sure Start for AMD integrity protects the HP ESC and UEFI flash regions, so that only its authenticated update mechanism or a secure local update through physical presence can modify those flash regions. HP Sure Start for AMD has no known authenticated update bypass mechanisms and contains the ability to prevent rollback to earlier authentic firmware images with known security vulnerabilities.
Protection of Immutable Code *(Section 4.2.2)*	**Meets** all Resiliency Requirements	HP Sure Start for AMD uses a hardware-based RoT (the HP ESC) with immutable boot firmware.
Runtime Protection of Critical Platform FW *(Section 4.2.3)*	**Meets** all Resiliency Requirements	Critical Platform Firmware executing in volatile storage (RAM) runs and: • ceases its operation prior to the loading of system software. That is, it runs during POST and stops before the OS is loaded. • is protected from system software using SMM protections enforced by the CPU

Protection of Critical Data *(Section 4.2.4)*	**Meets** all Resiliency Requirements	HP Sure Start for AMD Critical Data, such as Secure Boot authenticated variables, are only modifiable through defined APIs provided by device firmware. These APIs employ a mechanism to authenticate that the data is originating from an authorized source before applying the change. HP Sure Start for AMD Critical Data, such as per-platform unique factory configuration settings, are only modifiable through defined APIs provided by device firmware. These APIs employ a mechanism to authenticate that the request is originating from an authorized HP service provider before they allow the change. HP Sure Start for AMD Critical Data, such as BIOS settings that can be configured in the field, are only modifiable through defined APIs. These APIs are accessed only via a system administrator who has configured the BIOS administrator password. HP Sure Start for AMD factory default settings, which are not per-platform-specific, employ the same protection as the code. This includes integrity and authenticity verification via digital signature. These setting updates are controlled and protected in the same manner as the firmware.
Detection of Corrupted Code *(Section 4.3.1)*	**Meets** all Resiliency Requirements	A successful attack on the platform firmware will not impact HP Sure Start for AMD's RTD. The RTD is maintained in a private flash area inaccessible to the system software that might compromise the platform firmware. Firmware code is validated by HP Sure Start for AMD's RTD using approved digital signature algorithms and cryptographic hashes.
Detection of Corrupted Critical Data *(Section 4.3.2)*	**Meets** all Resiliency Requirements	A successful attack on the Active Critical Data will not impact HP Sure Start for AMD's RTD. The RTD is maintained in a private flash area inaccessible to the system software that might compromise Active Critical Data. HP Sure Start for AMD can save and validate critical data through use of digest hashes prior to using that critical data, and can initiate a recovery of the critical data if corruption is detected.
Recovery of Mutable Code *(Section 4.4.1)*	**Meets** all Resiliency Requirements	HP Sure Start for AMD's ESC implements the recovery capability. A successful attack on the platform firmware will not impact HP Sure Start for AMD's RTRec. The RTRec is maintained in a private flash area inaccessible to the system software that might compromise the platform firmware. HP Sure Start for AMD's RTRec has access to a locally stored copy of the platform's UEFI image in its private flash area, which is inaccessible to (protected from) system software. HP Sure Start for AMD can update the locally stored authentic UEFI image in its private flash area through an Authenticated Update mechanism.
Recovery of Critical Data *(Section 4.4.2)*	**Meets** all Resiliency Requirements	HP Sure Start for AMD's ESC implements the recovery capability. A successful attack on Active Critical Data will not impact HP Sure Start for AMD's RTRec. The RTRec is maintained in a private flash area inaccessible to the system software that might compromise Active Critical Data. HP Sure Start for AMD can recover critical data back to factory defaults including per-platform-specific data that is backed up in isolated & protected storage. HP Sure Start for AMD can recover non-per-platform-specific defaults from the backup BIOS image stored in isolated and protected storage. HP Sure Start for AMD does not use policies included as part of Critical Data to restore critical data.

Logging and notification	**Exceeds** all Resiliency Requirements	HP Sure Start for AMD will notify user of corruption and log the event. HP Sure Start for AMD's detection mechanism is capable of logging events when corruption is detected. HP Sure Start for AMD will notify user of a recovery event and log the event. HP Sure Start for AMD's detection mechanism is capable of logging events when a recovery action has taken place.
Rollback prevention	**Exceeds** all Resiliency Requirements	HP Sure Start for AMD's and the UEFI boot block both have controls in place to protect against recovery to an earlier firmware version with security weaknesses.
Physical attack detection	Additional Functionality not required in NISTSP800-193	HP Sure Start for AMD's provides protection against physical attacks to the protected backup copy of dynamic critical data. AES encryption is used on a per-component unique key to provide confidentiality of private data. In addition, HMAC integrity measurements provide tamper prevention/detection of those keys.

Sign up for updates: hp.com/go/getupdated