Technical whitepaper

HP Sure Start Gen3

Available on HP Elite products equipped with
7th generation Intel® Core™ processors
January 2017

Table of contents

1 HP Sure Start Gen3

1.1 Background

HP has a holistic view of client security that aims to address security at every layer of the client device computing stack. Our focus is not just within the OS or on cloud-based security solutions—we believe that "Below the OS" device firmware and hardware security are also crucial.

As our world becomes even more connected, cyber-attacks are targeting client device firmware and hardware with increasing frequency and sophistication. Since the device firmware executes on the hardware first and is responsible for securely booting the OS, you cannot trust the client device OS if you cannot trust the firmware.

It is extremely difficult, if not impossible, to foresee and therefore prevent every possible attack, which is why HP also designs our client devices with "cyber-resiliency," the ability to both detect a successful attack and recover from it.

HP Sure Start is HP's unique and groundbreaking approach to provide advanced "Below the OS" protection to the client device that uses hardware enforcement to ensure the system will only boot Genuine HP BIOS. Additionally, if HP Sure Start detects tampering with HP BIOS, it has the ability to recover Genuine HP BIOS using a protected backup copy.

1.2 HP Sure Start Gen3 overview

HP Sure Start Gen3 includes the same baseline capabilities as previous generations of HP Sure Start, plus new capabilities that significantly raise the bar for HP Sure Start advanced protection, detection of attack, and recovery of HP system firmware.[1] There are two primary features that are added to the client device:

- Runtime Intrusion Detection
- BIOS Setting Protection

Additionally, HP will begin to offer a Manageability Integration Kit (MIK) including a Microsoft System Center Configuration Manager (SCCM) plugin that will provide IT administrators with a straightforward mechanism to manage existing and new HP Sure Start Gen3 capabilities using their existing SCCM infrastructure. The focus of this whitepaper will be on the two new client device capabilities rather than the turnkey remote management capabilities enabled by the MIK.

1.3 Runtime Intrusion Detection (RTID)

1.3.1 Context

To provide context for how the HP Sure Start Gen3 Runtime Intrusion Detection feature differs from the baseline capabilities provided by HP Sure Start prior to Gen3, it is helpful to review that baseline illustrated in **Figure 1**. This figure provides a high-level view of what is provided by baseline HP Sure Start. Note that the focus of this baseline capability is to ensure that (at boot) the host CPU will never start executing firmware code that has been replaced or modified. Thus, HP Sure Start provides assurances that the system will only boot Genuine HP firmware that will securely configure the client device hardware as required to securely boot the OS.

Note that even in the case of HP Sure Start with Dynamic Protection, the focus is on monitoring the BIOS code in the system flash that is executed by the host CPU at boot.[2] This is an important distinction from BIOS code that remains resident in the main (DRAM) memory to provide power management and other critical services after the system has booted to OS. Next, we explore that distinction in greater detail.

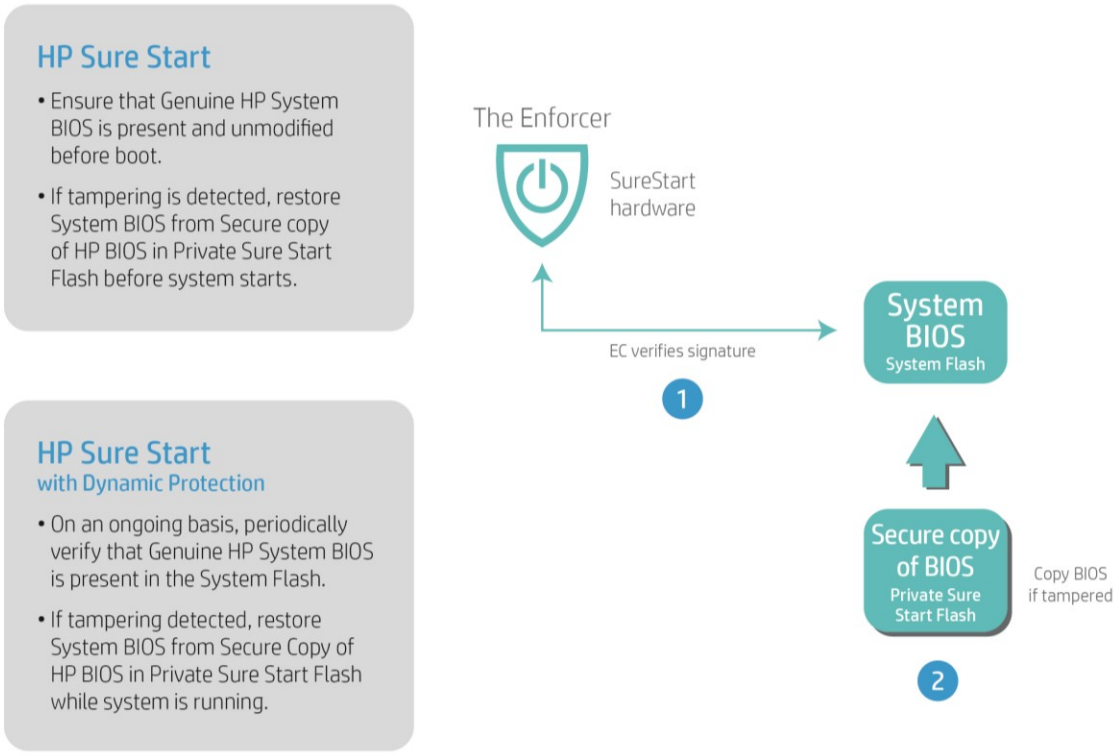

Figure 1 Baseline HP Sure Start overview (applies to HP Elite products equipped with 6th generation Intel® Core™ processors and higher)

1.3.2 Runtime BIOS code versus startup BIOS code

On each boot, the CPU starts execution of BIOS code from the flash memory at a fixed address. This BIOS code then initializes the hardware including the DRAM memory and copies all routines from flash into volatile (DRAM) memory. A large portion of that BIOS code is used to provide "Pre-OS" capabilities that are needed before the OS is started. Examples of "Pre-OS" BIOS support include video drivers, PXE boot support, keyboard and mouse drivers, pre-boot authentication, and unlocking of mass storage encryption, to name a few. Most of these routines are no longer needed once the OS is running, since the capabilities are either only relevant before handoff to the OS, or the OS has its own drivers.

However, there is a portion of BIOS that remains in DRAM that is needed to provide advanced power-management features, OS services, and other OS-independent functions while the OS is running. This BIOS code, referred to as System Management Mode (SMM) code, resides in a special area within the DRAM that is hidden from the OS.[3] We also refer to this code as "Runtime" BIOS code in the context of HP Sure Start Runtime Intrusion Detection.

The integrity of SMM code is critical to the client device security posture. The baseline HP Sure Start implementation provides assurance that ***all*** code is Genuine HP BIOS each time the system starts, including the SMM code that is present in DRAM when the OS starts.

The opportunity that remains is to move beyond not only ensuring that that starting place for HP SMM BIOS code is good at OS start, but to provide mechanisms to ensure that it ***remains*** good while the OS is running either by adding new protection capabilities and/or providing a means to detect any attack that manages to bypass the existing mechanisms providing protection for the HP SMM BIOS code.

1.3.3 Runtime Intrusion Detection architecture

Figure 2 provides details on the Runtime Intrusion Detection (RTID) capability implementation. The RTID feature utilizes specialized hardware in the platform chipset to detect attempts to modify the Runtime HP SMM BIOS. Additionally, the chipset hardware is used to enforce behavioral restrictions on the code running in an SMM context to provide the ability to detect and report any behaviors that are indicative of compromised SMM code. Detection of any of these conditions results in a notification to the HP Sure Start hardware, which can take the configured policy action independent of the CPU.

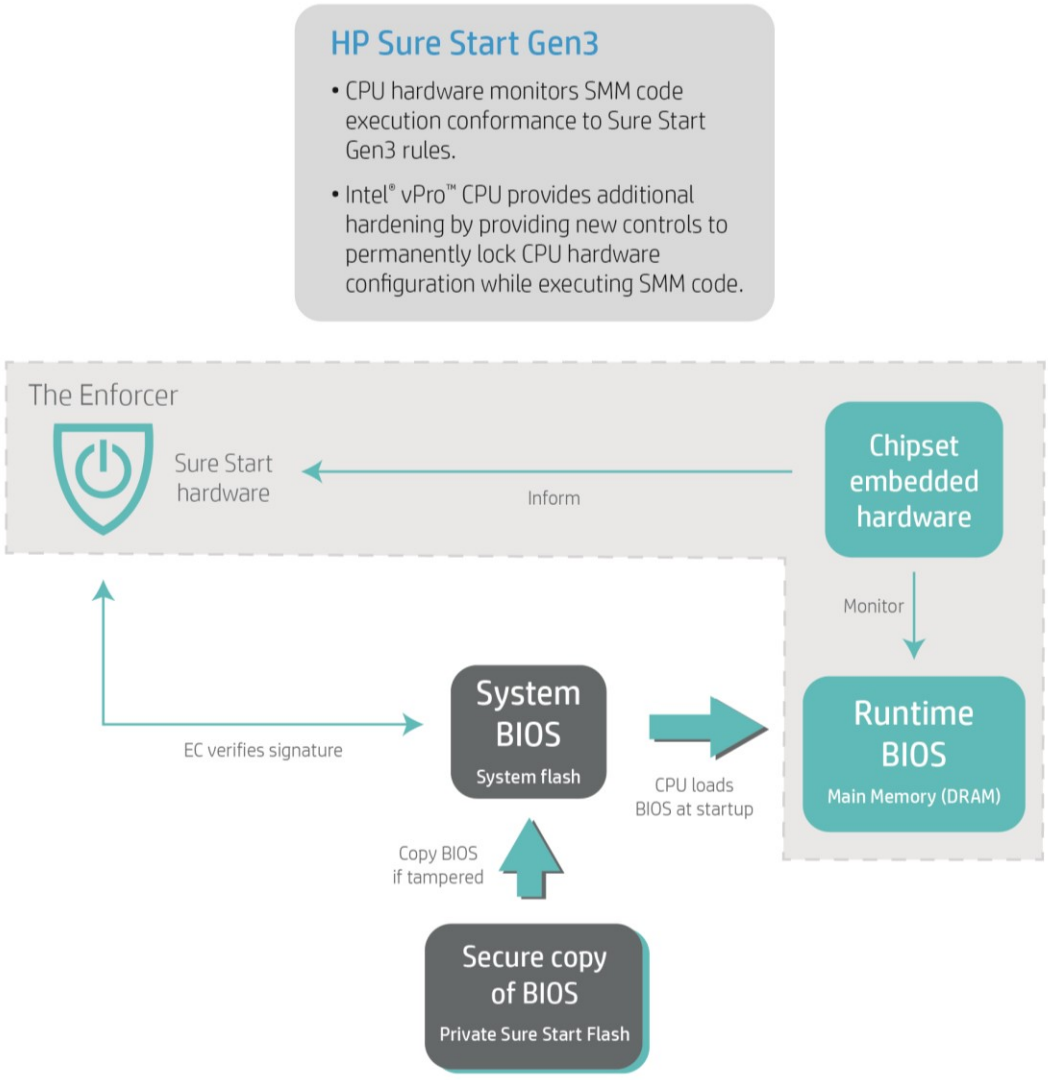

Figure 2 Runtime Intrusion Detection architecture (applies to HP Elite products equipped with 7th generation Intel® Core™ processors and higher)

1.3.4 Events

The HP Sure Start RTID feature will generate events to the HP Sure Start hardware when an attempt to modify the HP SMM BIOS code or any SMM code behavioral anomaly is detected. The HP Sure Start hardware will take the action associated with the event policy configured in BIOS setup.

Regardless of the event policy setting, the event will always be logged in to the HP Sure Start audit log, and the local user will receive a notification from BIOS on the next boot subsequent to an RTID event.

1.3.5 Policy controls

The RTID feature is enabled by default for all platforms shipped from the HP factory. There is no need for the end customer/administrator to enable or otherwise "deploy" the feature to take advantage of HP Sure Start RTID!

There are two BIOS policies related to the RTID feature that can optionally be configured by the platform owner/administrator:

- Enhanced HP Firmware Runtime Intrusion Prevention and Detection (enable/disable)
- Sure Start Security Event Policy

1.3.5.1. Enhanced HP firmware Runtime Intrusion Prevention and Detection

This BIOS policy setting will enable or disable the RTID capability. The default setting for this policy is **enabled**.

1.3.5.2. Sure Start security event policy

This BIOS policy setting controls what action is taken when the RTID feature detects an attack or attempted attack. There are three possible configurations for this policy:

- **Log event only:** When this setting is selected, the HP Sure Start hardware will log detection events, which can be viewed in the "Applications and Services Logs/HP Sure Start" path of the Microsoft Windows Event Viewer.[4]
- **Log event and notify user:** This is the default setting. When this setting is selected, the HP Sure Start hardware will log detection events, which can be viewed in the "Applications and Services Logs/HP Sure Start" path of the Microsoft Windows Event Viewer. Additionally, the user will be prompted within windows that the event occurred.[5]
- **Log event and power off system:** When this setting is selected, the HP Sure Start hardware will log detection events, which can be viewed in the "Applications and Services Logs/HP Sure Start" path of the Microsoft Windows Event Viewer. Additionally, the user will be prompted within windows that the event occurred and the system shutdown is imminent.

1.4 BIOS setting protection

1.4.1 Context

The baseline HP Sure Start verifies the integrity and authenticity of the 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 creates additional challenges to protecting those settings as digital signatures cannot be generated by HP and used by the HP Sure Start hardware to verify those settings.

1.4.2 BIOS setting protection overview

HP Sure Start Gen3 BIOS setting protection provides the capability to configure the system such that the HP Sure Start hardware is used to back up and provide integrity-checking 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. In the event a change is detected, the system uses the backup from the HP Sure Start protected back area to automatically revert back to the user defined setting.

1.4.3 Events

The HP Sure Start BIOS setting protection feature will generate events to the HP Sure Start hardware when an attempt to modify the BIOS Settings is detected. The event will be logged in the HP Sure Start audit log and the local user will receive a notification from BIOS during boot.

1.4.4 Policy controls

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 needs to configure a BIOS setup administrator password to use HP Sure Start BIOS setting protection.

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

2 Appendix A

2.1 System Management Mode (SMM) overview

System Management Mode (SMM) is an industry-standard approach used for PC advanced power-management features and other OS-independent functions while the OS is running. While the SMM term and implementation is specific to x86 architectures, many modern computing architectures use a similar architectural concept.

SMM is configured by the BIOS at boot time. The SMM code is populated into the main (DRAM) memory and then BIOS uses special (lockable) configuration registers within the chipset to block access to this area when the microprocessor is not executing in an SMM context. At runtime, entry into SMM mode is event-driven. The chipset is programmed to recognize many types of events and timeouts. When such an event occurs, the chipset hardware asserts the System Management Interrupt (SMI) input pin. At the next instruction boundary, the microprocessor saves its entire state and enters SMM.

As the microprocessor enters SMM, it asserts a hardware output pin, SMI Active (SMIACT). This pin serves notice to the chipset hardware that the microprocessor is entering SMM. An SMI can be asserted at any time, during any process operating mode, except from within SMM itself. The chipset hardware recognizes the SMIACT signal and redirects all subsequent memory cycles to a protected area of memory (sometimes referred to as the SMRAM area), reserved specifically for SMM. Immediately after receiving the SMI input and asserting the SMIACT output, the microprocessor begins to save its entire internal state to this protected memory area.

After the microprocessor state has been stored to SMRAM memory, the special SMM handler code that also resides in SMRAM (placed there by system BIOS at boot time) begins to execute in a special SMM operation mode. While operating in this mode, most hardware and memory isolation mechanisms are suspended and the microprocessor can access virtually all resources in the platform to enable it to perform required tasks. The SMM code completes the required task, and then it's time to return the microprocessor to the previous operating mode. At that point, the SMM code executes the Return from System Management Mode (RSM) instruction to exit SMM. The RSM instruction causes the microprocessor to restore its previous internal state data from the copy saved in SMRAM upon SMM entry. Upon completion of RSM, the entire microprocessor state has been restored to the state just prior to the SMI event, and the previous program (OS, applications, hypervisor, etc.) resumes execution right where it left off.

1. HP Sure Start Gen3 is available on HP Elite products equipped with 7th generation Intel Core processors and higher.
2. HP Sure Start with Dynamic Protection is available on HP Elite products equipped with 6th generation Intel Core processors and higher.
3. For more details on SMM and how it works, see Appendix A.
4. HP Notification Software is required to be installed to view HP Sure Start events in the Windows Event Viewer.
5. HP Notification Software is required to be installed to receive notifications.

4AA6-9339ENW, February 2017