Technische White Paper

HP Sure Start

Automatische bescherming en automatisch herstel op BIOS-niveau

Mei 2018

Inhoudsopgave

Inleiding

HP Sure Start kan automatisch een BIOS-aanval of -beschadiging detecteren, stoppen en ervan herstellen zonder IT-tussenkomst en met weinig tot geen onderbreking van de gebruikersproductiviteit. Elke keer als de pc opstart, valideert HP Sure Start automatisch de integriteit van de BIOS-code om ervoor te zorgen dat de pc beschermd is tegen kwaadaardige aanvallen. Zodra de pc draait, monitort de Run-time intrusion detection doorlopend het geheugen. In het geval van een aanval kan de pc zich zelf in minder dan een minuut herstellen met een geïsoleerde "gouden kopie" van het BIOS.

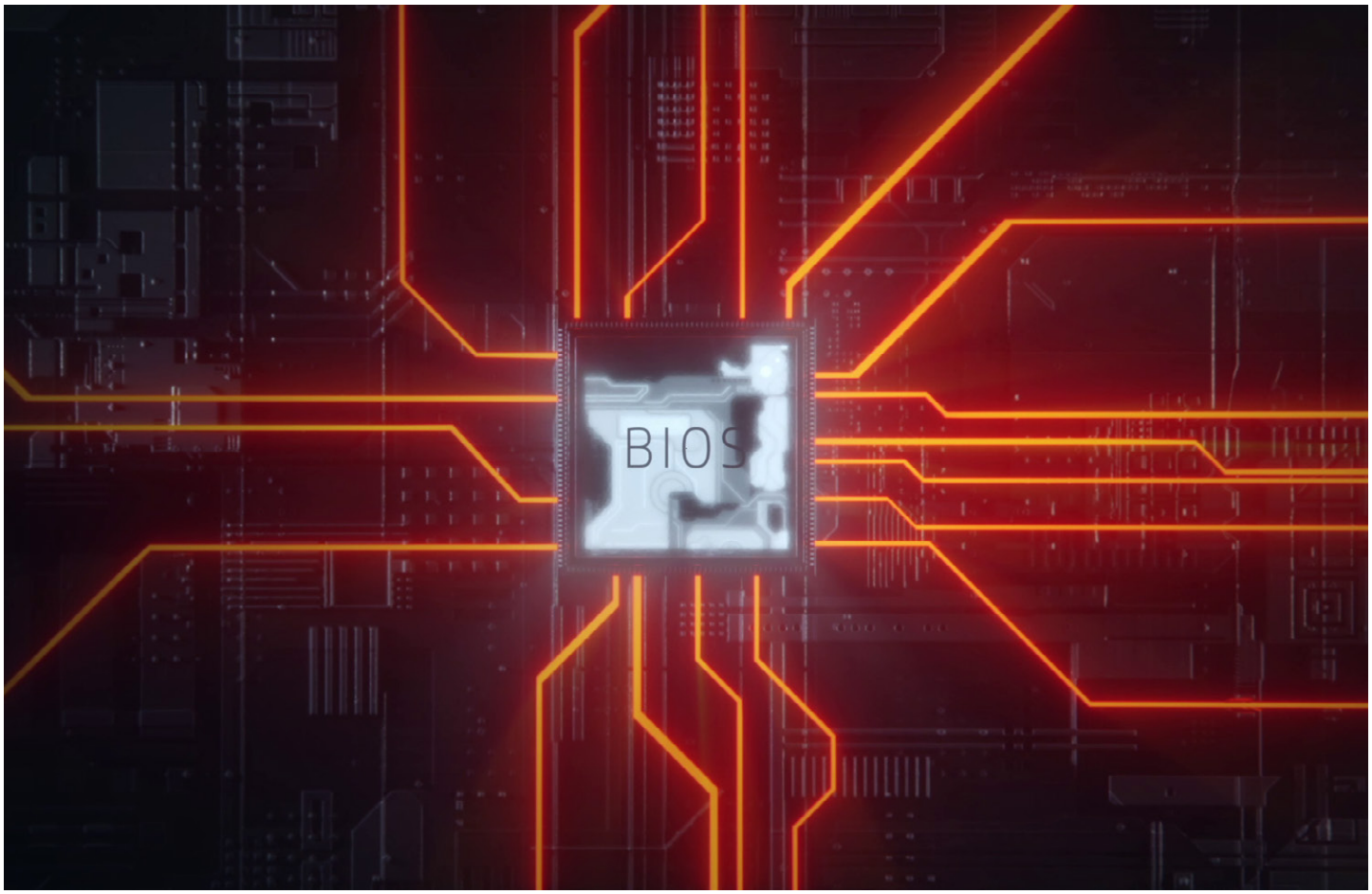
Waarom is BIOS-beveiliging belangrijk?

Omdat onze wereld steeds meer verbonden raakt, richten cyberaanvallen zich met toenemende frequentie en sofisticatie op de firmware en hardware van consumentenapparaten. Van tools en technieken om firmware aan te vallen werd ooit gedacht dat deze alleen door overheden konden worden ingezet. Dergelijke tools en technieken blijken niet alleen te bestaan maar zijn al kant en klaar beschikbaar in het openbare domein.

De firmware (of BIOS) van het apparaat is een aantrekkelijk doelwit voor aanvallers vanwege de mogelijkheden die een succesvolle inbreuk kan bieden aan de aanvaller:

- Persistentie: De firmware bevindt zich in niet-volatiel geheugen op het moederbord en kan niet eenvoudig worden verwijderd door het wissen van de harde schijf.
- Controle: Firmware draait op het hoogste rechtenniveau – buiten het domein van het besturingssysteem, waardoor OS-onafhankelijke malware mogelijk is.
- Verborgenheid: De firmware gebruikt een deel van het geheugen dat compleet ontoegankelijk is voor het besturingssysteem en de systeemsoftware; omdat het niet kan worden gescand door een anti-virus wordt het mogelijk nooit gedetecteerd.
- Moeilijk te herstellen: Al deze aspecten maken het buitengewoon moeilijk om van dit type infectie te herstellen zonder het moederbord te moeten vervangen.

De ideale oplossing om apparaten te beschermen tegen dit soort aanvallen is ontworpen vanaf de hardware volgens de principes van "cyberweerbaarheid". Deze principes erkennen dat het buitengewoon moeilijk, zo niet onmogelijk is om elke mogelijke aanval te voorzien en te voorkomen. De ideale oplossing biedt niet alleen verbeterde bescherming van de firmware, maar omvat ook de hardware-gebaseerde capaciteit om zowel een succesvolle aanval te detecteren als ervan te herstellen.



HP Sure Start biedt superieure firmwarebescherming

HP Sure Start is HP's unieke en baanbrekende aanpak om geavanceerde firmwarebescherming en weerbaarheid te bieden voor pc's van HP. Het gebruikt hardwarematige afdwinging via de HP Endpoint Security Controller (HP ESC) om BIOS-bescherming te bieden die veel verder gaat dan de industrienorm en om te garanderen dat het systeem alleen met een authentieke HP-BIOS zal starten. Bovendien kan het zich herstellen door een beschermde back-up te gebruiken indien HP Sure Start misbruik detecteert in de BIOS-code, de firmware of in de runtime System Management Mode (SMM) BIOS-code.

Samenvatting van HP Sure Start-karakteristieken

- Afdwinging van firmware-authenticiteit en misbruikprotectie voor HP basisplatform – Hardwarematige afdwinging van de systeemstart door HP Endpoint Security Controller, zodat enkel authentieke en ongewijzigde HP-firmware en HP-BIOS geladen wordt
- Firmware-gezondheidsbewaking en -conformiteit – Logging van gezondheidsgerelateerde events van de firmware via geïsoleerde HP Endpoint Security Controller; toont de firmwarestatus van het platform samen met eventuele afwijkingen die kunnen duiden op verijdelde aanvallen
- Zelfherstellend – Automatisch herstel van HP-BIOS en HP-firmwarecorruptie met de geïsoleerde back-up van het HP-BIOS en HP-firmware gemaakt door de HP Endpoint Security Controller
- Bescherming van BIOS-instellingen – Vergroot de bescherming van de BIOS-code door de HP Endpoint Security Controller met HP ESC back-up en integriteitscheck van alle door gebruikers of beheerders ingestelde BIOS-instellingen
- Runtime Intrusion Detection – Doorlopende monitoring van kritische BIOS-code in runtime memory (SMM) terwijl het besturingssysteem actief is
- Beveiligde boot key-bescherming – Verhoogt significant de bescherming van databases en sleutels die zijn opgeslagen in het BIOS en die kritiek zijn voor de integriteit van de secure boot van het besturingssysteem ten opzichte van standaardimplementatie in UEFI BIOS
- Beschermde opslag – HP Sure Start gebruikt sterke encryptiemethoden om BIOS-instellingen, gebruikersgegevens en andere instellingen op te slaan in de hardware van de HP Endpoint Security Controller die instaat voor integriteitsbescherming, misbruikdetectie en vertrouwdheidsbescherming voor die gegevens
- Intel® Management Engine firmware-bescherming – Verbeterde bescherming en herstel van de Intel Management Engine-firmware
- Bestuurbaarheid – Beheerders kunnen HP Sure Start-functies beheren met de Manageability Integration Kit (MIK)-plugin voor Microsoft® System Center Configuration Manager (SCCM)

Voor een overzicht van de capaciteiten in elke versie van HP Sure Start, zie Bijlage A op pagina 11.

Beveiligingscertificering door derden

De hardware van de HP Endpoint Security Controller die in HP Sure Start gebruikt wordt is door derden onderzocht en is gecertificeerd voor het hardwarematige afdwingen van het opstarten van de doel-pc door enkel en alleen geautoriseerde firmware.[1]

Verzekering dat een beveiligingsoplossing werkt zoals aangegeven is een kritiek onderdeel van elk aankoopbesluit aangaande beveiligingsproducten. En omdat een kwaliteitsreputatie maar tot een bepaald punt kan gaan, heeft HP de interne werking van de HP Endpoint Security Controller aangeboden voor beoordeling en tests door een onafhankelijk en geaccrediteerd laboratorium om te valideren dat het werkt zoals geclaimd op basis van openbaar beschikbare criteria, methodieken en processen.

Cyberbestendig ontwerp

Niet alleen biedt HP Sure Start verbeterde BIOS-bescherming die verder gaat dan de industrienorm, maar het is ook ontworpen vanuit de hardware om ongeëvenaarde cyberbestendigheid van het platform te waarborgen en zelfs bij een inbraak of vernietigende aanval een BIOS te kunnen herstellen. Zakelijke pc's van HP met HP Sure Start overtreffen de richtlijnen van de Draft National Institute of Standards

Technology (NIST) Platform Firmware Resiliency (Speciale publicatie 800-193), wat een van de toonaangevende inspanningen van de publieke sector is om vereisten voor cyberbestendige platformen te formaliseren.

Modellen ondersteund met HP Sure Start

HP introduceerde Sure Start in 2014. Sindsdien heeft HP Sure Start verbeterd en het aantal ondersteunde producten uitgebreid. HP Sure Start wordt geleverd over de hele 2018 Elite productlijn, inclusief tablets, notebooks, desktops, en all-in-ones (AIO's). HP Sure Start Gen4 is beschikbaar op HP Elite- en HP Pro 600-producten uitgerust met de 8ste generatie Intel- of AMD-processoren.

Architectuuroverzicht en capaciteiten

HP Sure Start bestaat uit twee grote architectuuronderdelen:

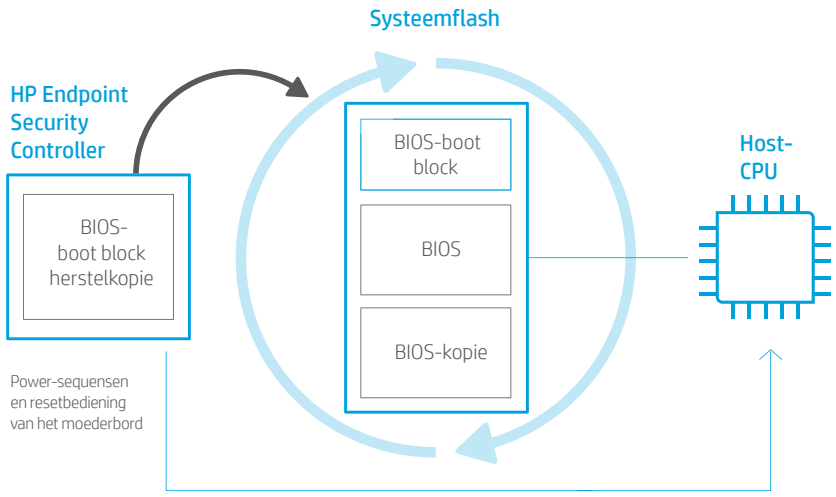
- **HP Endpoint Security Controller** met HP Sure Start-firmware
- **HP Sure Start BIOS** die samenwerkt met de HP Endpoint Security Controller-hardware en firmware

Integriteitsverificatie van firmware – het hart van HP Sure Start

De HP Endpoint Security Controller (HP ESC) is het eerste apparaat in het systeem dat de firmware uitvoert wanneer het systeem wordt opgestart en actief is lang voor de systeemboot. De HP ESC-activiteiten omvatten, maar zijn niet beperkt tot, het monitoren van de aan/uit-knop en het power-sequensen van de start van de uitvoer van de host-CPU wanneer de gebruiker de startknop indrukt.

Als de stroom voor het eerst het platform bereikt (nog voordat het systeem ingeschakeld wordt), valideert de HP ESC dat zijn eigen firmware authentieke HP-code is voordat de code wordt geladen en uitgevoerd. De HP ESC-hardware gebruikt sterke encryptiemethoden die voldoen aan industrienormen om de integriteitsverificatie uit te voeren. De methode gebruikt een 2048-bit HP RSA public key die is opgeslagen in het permanente, interne read-only memory. Daarom is de HP ESC de ingebouwde hardwaregebaseerde Root of Trust (RoT) voor het platform, waarmee de firmware en het HP-BIOS gevalideerd worden voordat ze worden uitgevoerd. Deze hardwarematige Root of Trust beschermt tegen aanvallen met firmwarevervanging ongeacht hun implementatiemethode en dient als basis waarop de HP-platformbeveiliging is gebouwd.

Afbeelding 1. Integriteitsverificatieproces van firmware.



Afbeelding 1 toont het integriteitsverificatieproces van de firmware. Zodra de HP ESC de HP Sure Start-firmware authenticeert en begint met de uitvoering, gebruikt die firmware dezelfde sterke encryptie om de integriteit van het boot block van de BIOS-systeemflash. Als er ook maar één bit ongeldig is, vervangt de HP ESC de inhoud van de systeemflash door een eigen kopie van de HP BIOS-bootsector die is opgeslagen in geïsoleerd, niet-volatiel geheugen (NVM) speciaal bedoeld voor de HP ESC.

Het ontwerp van HP Sure Start zorgt ervoor dat alle firmware- en BIOS-code op zowel de HP ESC als de host-CPU de HP-code is die bedoeld is voor het apparaat.

Opmerking: De integriteitscheck van de bootsector van de systeemflash en elke benodigde hersteloperatie door de HP ESC, vinden plaats als de host-CPU uitgeschakeld is. Daarom wordt de gehele operatie vanuit het oogpunt van de gebruiker gedaan als het systeem nog uit is of in slaap- of sluimerstand staat.

Het boot block van de BIOS-systeemflash is het hart van het HP-BIOS. De HP ESC-hardware zorgt ervoor dat de BIOS-bootsector de eerste code is die de CPU uitvoert na een reset. Zodra de HP ESC bepaalt dat de BIOS-bootsector authentieke HP-code bevat, laat het het systeem starten zoals normaal.

De HP ESC controleert ook de integriteit van de bootsector van de systeemflash op elk moment dat het systeem wordt uitgeschakeld of in sluimer- of slaapstand wordt gebracht. Omdat de CPU wordt uitgeschakeld in elk van deze omstandigheden en de CPU daarom de BIOS-boot block weer moet uitvoeren om verder te gaan, is het cruciaal om de integriteit van de BIOS-boot block elke keer te controleren om misbruik te detecteren.

Voor HP Intel-modellen controleert HP Sure Start ook periodiek (elke 15 minuten) de integriteit van het boot block van de BIOS-systeemflash terwijl het systeem draait.[2]

Gegevensintegriteit uniek aan apparaat

De HP ESC en BIOS werken samen om geavanceerde bescherming te bieden voor de fabrieksinstellingen van kritieke variabelen die uniek zijn voor elke machine en bedoeld zijn om constant te blijven gedurende de levensduur van elk specifiek platform. In de fabriek wordt een back-up van deze variabele gegevens opgeslagen in het niet-volatiele geheugen van de HP ESC. De back-up is beschikbaar voor de HP Sure Start BIOS-component op een read-only basis om integriteitscontrole te doen van de gegevens tijdens elke boot. Als er een instelling in het gedeelde flashgeheugen gewijzigd is ten opzichte van de fabrieksinstellingen zullen de HP Sure Start BIOS-onderdelen automatisch de gegevens in de systeemflash herstellen op basis van de back-up die door HP ESC geleverd wordt.

Descriptorgedeelte

Voor HP Intel-modellen beschermt HP Sure Start het descriptorgedeelte van de systeemflash. Het descriptorgedeelte, dat uniek is voor Intel-architectuur, bevat kritieke configuratieparameters die door de Intel Core™-logica bij een reset worden ingelezen en daarna gebruikt worden om de Core-logica te configureren. Het descriptorgedeelte omvat ook partitie-informatie voor de systeemflash die gebruikt wordt door de Intel Core-logica om te bepalen waar het BIOS-gedeelte in de flash is opgeslagen en dus waar de CPU de code ophaalt voor een reset. HP Sure Start monitort de integriteit van dit gedeelte en herstelt het naar de gewenste configuratie als er zich misbruik of beschadiging voordoet.

Bescherming van de netwerkcontroller

Voor HP Intel-modellen beschermt HP Sure Start ook de instellingen van de netwerkcontroller (NIC) die op de systeemflash staan. Sommige HP-klanten hebben gebruiksscenario's waarbij er legitieme veranderingen mogelijk moeten zijn aan de fabrieksinstellingen van de NIC. Daarom beschermt HP Sure Start niet standaard tegen wijzigingen aan NIC-instellingen. In plaats daarvan biedt HP Sure Start een functie die, indien ingeschakeld, de gebruiker waarschuwt dat NIC-instellingen gewijzigd zijn. Daarnaast biedt HP Sure Start een methode om de NIC-instellingen naar de fabriekswaarden terug te zetten. Beschermde instellingen omvatten het MAC-adres, de Pre-boot Execution Environment (PXE)-instellingen en de remote initial program load (RPL). Dit herstel is mogelijk via een read-only back-up die beschermd wordt door HP ESC

Bescherming van BIOS-instellingen

Zoals eerder beschreven verifieert HP Sure Start de integriteit en authenticiteit van de HP BIOS-code. Omdat de code statisch is nadat deze is aangemaakt door HP kunnen digitale handtekeningen worden gebruikt om beide attributen van de code te bevestigen. De dynamische en gebruikersconfigureerbare eigenschappen van de BIOS-instellingen creëren echter extra uitdagingen voor het beschermen van deze instellingen. Digitale handtekeningen kunnen niet worden gegenereerd door HP en worden gebruikt door de HP Sure Start ESC-hardware om die instellingen te controleren.

HP Sure Start BIOS-instellingsbeveiliging biedt de mogelijkheid om het systeem te configureren zodat de HP ESC-hardware gebruikt wordt voor back-up en controle van de integriteit van alle BIOS-instellingen die door de gebruiker gewenst zijn.

Als deze functie op het platform is ingeschakeld worden alle beleidsinstellingen die worden gebruikt door de BIOS opgeslagen en wordt er bij elke boot een integriteitscontrole uitgevoerd om er zeker van te zijn dat geen van de BIOS-beleidsinstellingen gewijzigd zijn. Als er een wijziging wordt gedetecteerd, gebruikt het systeem de back-up van de HP Sure Start beschermde opslag om automatisch terug te keren naar de gebruikersinstelling.

De HP Sure Start bescherming van BIOS-instellingen genereert events voor de HP Sure Start ESC-hardware als een poging tot wijziging van de BIOS-instellingen wordt gedetecteerd. Het event wordt opgeslagen in de HP Sure Start auditlog en de lokale gebruiker ontvangt een melding van het BIOS tijdens de boot.

HP Sure Start beschermde opslag

Beschermde opslag in de HP Endpoint Security Controller-hardware biedt het hoogste niveau van bescherming voor BIOS/firmwaregegevens en instellingen die beschermd worden door HP Sure Start. De beschermde opslag van HP Sure Start is ontworpen om vertrouwelijkheid, integriteit en inbreukdetectie te bieden, zelfs in het geval van fysieke aanvallen waarbij een aanvaller het systeem ontmantelt en een directe verbinding maakt met het niet-volatiele opslagapparaat op het moederbord.

Gegevensintegriteit

De integriteit van de dynamische gegevens die door de firmware zijn opgeslagen in het niet-volatiele geheugen en gebruikt worden om de status van diverse functies te controleren, is cruciaal voor de veilige status van het hele platform. Dynamische gegevens omvatten alle BIOS-instellingen die kunnen worden aangepast door de eindgebruiker of beheerder van het apparaat. Voorbeelden hiervan zijn (maar zijn niet beperkt tot) bootopties zoals de secure boot-functie, BIOS-beheerderwachtwoorden en gerelateerd beleid, statuscontrole van de Trusted Platform Module en HP Sure Start-beleidsinstellingen.

Elke succesvolle aanval die de bestaande toegangsrestricties weet te omzeilen voor het doen van ongeautoriseerde aanpassingen aan deze instellingen zou de platformbeveiliging kunnen schaden. Neem als voorbeeld een scenario waar een aanvaller een ongeautoriseerde aanpassing doet aan de veilige boot-status om deze uit te schakelen zonder te worden gedetecteerd. In dit scenario zou het platform de rootkit van de aanvaller opstarten voordat het besturingssysteem start, zonder dat de gebruiker het merkt.

De Unified Extensible Firmware Interface (UEFI) BIOS-industrienorm implementeert toegangsbeperkingen die ongeautoriseerde wijzigingen moeten voorkomen aan deze variabelen, en HP implementeert deze net als de rest van de pc-industrie.

Gezien de risico's die een inbreuk op deze mechanismen vormen voor het platform, biedt HP Sure Start echter secundaire beveiligingsmaatregelen die strenger zijn dan de gangbare industrienorm.

BIOS-instellingen en andere dynamische gegevens die door de firmware worden gebruikt om de status te regelen die beschermd is door HP Sure Start, worden opgeslagen in het geïsoleerde niet-volatiele geheugen van de HP Endpoint Security Controller die niet direct toegankelijk is voor de software die draait op de host-CPU.

Daarnaast maakt HP ESC unieke integriteitsmaatregelen aan en past die telkens toe als een data-element wordt opgeslagen in dit niet-volatiele geheugen. De integriteitsmaatregelen zijn gebaseerd op een sterk encryptie-algoritme (hashed-gebaseerde bericht-authenticatiecode op basis van SHA-256-hashing) dat is gekoppeld aan een geheime code binnen de HP ESC. Het geheim is uniek voor elke HP ESC, zodat elke controller een unieke integriteitsmaatregel bij een gelijksoortig element maakt.

Als het data-element wordt teruggelezen uit het niet-volatiele geheugen, herberekent de HP ESC de integriteitsmaatregelen voor dat data-element en vergelijkt het met de integriteitsmaatregel die is toegepast op de data. Alle ongeautoriseerde veranderingen aan de data in het niet-volatiele geheugen resulteren in een niet-geslaagde vergelijking. Met deze benadering kan de HP ESC misbruik detecteren van data-elementen in het niet-volatiele geheugen.

Gegevensvertrouwelijkheid

Voor veel van de data-elementen op het platform is het behoud van vertrouwelijkheid cruciaal. Voorbeelden zijn beheerderwachtwoord-hashes voor het BIOS, gebruikersgegevens en optionele geheimen die voor de firmware namens de gebruiker worden opgeslagen voor firmware-gebaseerde functies zoals HP Sure Run en HP Sure Recovery.

Bescherming van deze geheimen is een uitdaging in het geval van de UEFI BIOS-industrienorm omdat het niet-volatiele geheugen gelezen kan worden door software die op de host-CPU draait. Door HP Sure Start beveiligde opslag is bedoeld om meer bescherming te bieden voor deze vertrouwelijke gegevens dan een standaard UEFI BIOS-implementatie.

Naast een afzonderlijke geïsoleerde opslag is de HP Sure Start-benadering bedoeld om het Advanced Encryption Standard (AES) hardwareblok binnen de HP ESC te houden voor AES-256-encryptie op alle vertrouwelijke gegevenselementen die zijn opgeslagen in het HP Sure Start niet-volatiele geheugen, naast data-integriteitsmaatregelen voor deze elementen. De gebruikte encryptiesleutel is uniek voor elke HP ESC en verlaat die controller nooit, dus gegevens die versleuteld zijn door een afzonderlijke HP ESC-component kunnen alleen ontcijferd worden door diezelfde HP ESC.

Beveiligde boot key-bescherming

HP Sure Start biedt verbeterde beveiliging van de UEFI secure boot key-databases, die zijn opgeslagen door de firmware vergeleken met de industrie-standaard UEFI secure boot-implementatie. Deze variabelen zijn cruciaal voor een juiste werking van de UEFI secure boot-functie die de integriteit en authenticiteit van de OS-bootloader verifieert voordat deze mag starten.

HP Sure Start beschermt de UEFI secure boot key-databases door een moederkopie te beheren in de HP Sure Start beschermde opslag. Alle geautoriseerde wijzigingen aan de UEFI standard secure boot key-databases door het besturingssysteem tijdens de werking worden bijgehouden door HP Sure Start en toegepast op de moederkopie door HP ESC. HP Sure Start gebruikt dan de moederkopie in de HP Sure Start beveiligde opslag om ongeautoriseerde wijzigingen aan de UEFI standard secure boot keys-databases te identificeren en te verwerpen.

Deze functie, standaard ingeschakeld, omvat de volgende databases:

- Handtekeningdatabase (db)
- Afgewezen handtekeningen database (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) dynamisch bijgewerkt tijdens werking door het besturingssysteem

Runtime Intrusion Detection (RTID)

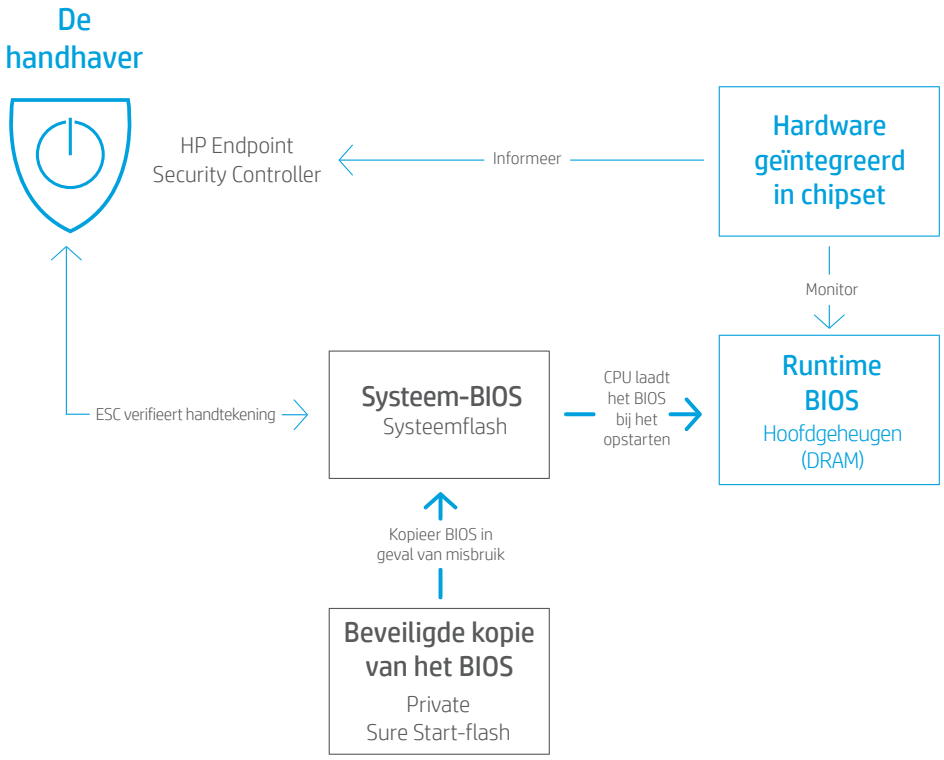
Bij elke boot begint de BIOS-code met de uitvoering vanuit het flashgeheugen op een vast adres. Dit wordt ook wel de BIOS-bootcode genoemd en biedt "Pre-OS"-mogelijkheden die nodig zijn voorafgaand aan het starten van het besturingssysteem. Er is echter een deel van het BIOS dat in het DRAM geladen blijft en nodig is voor geavanceerde stroombeheerfuncties, besturingssysteemdiensten en andere besturingssysteem-afhankelijke functies terwijl het besturingssysteem draait. Deze BIOS-code, ook wel System Management Mode (SMM)-code genoemd, staat op een speciale plaats in het DRAM die verborgen is voor het besturingssysteem. Wij verwijzen ook naar deze code als "Runtime" BIOS-code in het kader van de HP Sure Start Runtime Intrusion Detection-functie. (Voor meer informatie over SMM en hoe het werkt, zie B op pagina 12).

De integriteit van de SMM-code is cruciaal voor de beveiligingsstaat van het cliëntapparaat. HP Sure Start controleert of de HP SMM BIOS-code bij het starten van het besturingssysteem intact is. Runtime Intrusion Detection biedt mechanismen om te verzekeren dat de SMM BIOS-code intact blijft terwijl het besturingssysteem draait door het toevoegen van nieuwe beveiligingsmogelijkheden en/of het bieden van een manier om een aanval op die code te detecteren.

Runtime Intrusion Detection-architectuur

De RTID-functie gebruikt gespecialiseerde hardware op de platform-chipset om afwijkingen te detecteren in de HP SMM BIOS. Detectie van iedere afwijking resulteert in een melding aan de HP Endpoint Security Controller, die de ingestelde maatregel kan nemen onafhankelijk van de CPU.

Afbeelding 2. Runtime Intrusion Detection gebruikt gespecialiseerde hardware die in de platform-chipset zit om SMM-code te controleren op eventuele wijzigingen.



Gebruikersnotificaties, event-log en beleidsbeheer

HP Sure Start eindgebruikersnotificatie

Onder normale omstandigheden is HP Sure Start onzichtbaar voor de gebruiker. Herstelhandelingen gebruiken automatisch de standaardinstellingen, waarbij doorgaans geen interactie van eindgebruikers of IT nodig is voor het herstel indien HP Sure Start een probleem identificeert.

Gebruikers kunnen runtime-meldingen zien als er een BIOS-integriteitsprobleem is gedetecteerd via de HP Sure Start Dynamic Protection of de Runtime Intrusion Detection-functies terwijl het besturingssysteem actief is. Als er een significant event wordt gedetecteerd of actie wordt ondernomen, toont HP Sure Start een waarschuwing via Windows® notificaties bij de volgende boot. HP Notifications Software is vereist om deze Windows-meldingen te bekijken.

HP Sure Start event-log

De HP Endpoint Security Controller registreert kritieke events aangaande de firmware/BIOS-code en gegevens die worden gemonitord door HP Sure Start. Deze events worden opgeslagen in het niet-volatiele geheugen van Sure Start. Deze events worden gekopieerd van de HP ESC naar de Windows Event Viewer als HP Notifications Software geïnstalleerd is om toegang tot deze events te verlenen aan een lokale gebruiker en de geprefereerde beheeragent van de klant.

De volgende events activeren de HP Notifications Software tot het verzamelen van alle events uit het HP Sure Start subsysteem en om te verzekeren dat de Windows Event Viewer wordt bijgewerkt met alle events die daar nog niet zijn geregistreerd:

- Windows opstarten
- Windows herstel uit slaapstand/sluimerstand
- HP Sure Start met dynamic protection runtime eventnotificaties
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Notifications Software zet HP Sure Start-events in een unieke "HP Sure Start" applicatie eventlog. Alleen HP Sure Start-events worden opgenomen in deze log. Het Windows Event Viewer-pad naar de HP Sure Start-events is het volgende: System Tools/Event Viewer/Applications and Services Logs/HP Sure Start.

De Windows Event Viewer niveaucategorieën gerelateerd aan HP Sure Start-events zijn gedefinieerd in onderstaande tabel.

De events worden verzameld in de Windows Event Viewer in de volgorde waarin ze zijn aangemaakt door HP Sure Start. Het oudste event in het HP Sure Start-subsysteem wordt eerst toegevoegd aan de Windows Event Viewer en het meer recente event wordt als laatste toegevoegd.

De tijdstempel voor elke vermelding in de Windows Event Viewer verwijst naar de tijd dat het werd toegevoegd aan die log, NIET de tijd waarop het event plaatsvond. Elk Sure Start Windows Event Viewer record bevat gedetailleerde gegevens in de eventdetails, waaronder de tijdstempel van de daadwerkelijke gebeurtenis.

Opmerking: Events blijven staan in de HP Endpoint Security Controller, zelfs nadat ze zijn gekopieerd naar de Windows Event Viewer. Als de Windows Event Viewer wordt leeggemaakt, zal de HP Notifications Software-applicatie alle HP Sure Start-vermeldingen vervangen bij het volgende event dat plaatsvindt om te controleren op HP Sure Start eventlogs.

Soorten van HP Sure Start Windows Event Viewer-events

Eventniveau	Definitie
Informatie	Events die verwacht worden bij een normale werking (zoals een update van het BIOS).
Waarschuwing	Onverwachte events die hebben plaatsgevonden maar volledig hersteld zijn door HP Sure Start en er geen gebruiker/beheerder nodig is om het platform volledig operationeel te maken. Deze events zijn ongebruikelijke activiteiten die de gebruiker/beheerder mogelijk verder wil onderzoeken, vooral als deze events op meerdere machines voorkomen.
Fout	Events die actie van de beheerder/HP-service vereisen om het platform volledig te herstellen.

HP Sure Start beleidscontroles

Standaard activeert en optimaliseert het HP systeem-BIOS HP Sure Start-beleid voor de standaardgebruiker. Omdat HP Sure Start standaard ingeschakeld is, hoeft een gemiddelde gebruiker geen instellingen te wijzigen om beschermd te worden door HP Sure Start. Voor geavanceerde gebruikers geeft het systeem-BIOS enige controle over het gedrag van HP Sure Start, met behulp van beleidsinstellingen in de (F10) BIOS-setup. Tenzij anders aangegeven staan deze instellingen en functies onder Security/ BIOS Sure Start.

Opmerking: Beleid wordt opgeslagen binnen het HP ESC niet-volatiele geheugen dat niet direct toegankelijk is voor de host-CPU; daarom is een herstart nodig voordat instellingen van Sure Start van kracht worden.

De volgende HP Sure Start-instellingen en functies zijn beschikbaar:

- Controle boot block bij elke opstart
- BIOS Data Recovery Policy
- Herstel Netwerkcontroller-configuratie (alleen Intel)
- Melding bij wijziging Netwerkcontroller-configuratie (alleen Intel)
- Dynamic Runtime Scanning van boot block (alleen Intel)
- HP Sure Start BIOS-instellingsbescherming
- HP Sure Start Secure beveiligde boot key-bescherming
- Enhanced HP Firmware Runtime Intrusion Prevention and Detection (alleen Intel)
- HP Firmware Runtime Intrusion Detection (alleen AMD)
- HP Sure Start Security Event Policy
- HP Sure Start Security Event Boot Notification
- Blokkeren van BIOS-versie
- Opslaan/herstellen MBR van systeemschijf
- Opslaan/herstellen GPT van systeemschijf
- Boot Sector (MBR/GPT) Recovery Policy

Verifieer Boot Block bij elke boot

HP Sure Start controleert altijd de integriteit van het boot block van de BIOS-systeemflash voordat herstel uit slaap- of sluimerstand of uitschakelen wordt hervat. Indien ingesteld op **enable (ingeschakeld)** zal HP Sure Start ook de integriteit van het boot block bij elke warme herstart (Windows-herstart) verifiëren. De afweging is sneller herstarten ten opzichte van meer beveiliging. De standaardinstelling van deze functie is **disable (uitgeschakeld)**.

BIOS Data Recovery Policy

Indien ingesteld op **Automatic (Automatisch)** zal HP Sure Start automatisch het BIOS of de unieke machinegegevens repareren indien nodig. Indien ingesteld op **Manual (Handmatig)**, heeft HP Sure Start een speciale toetsencombinatie nodig om verder te gaan met herstel. In het geval van een probleem met de code van de bootsector, zal het systeem weigeren op te starten en een unieke knippervolgorde zal te zien zijn op de systeem-LED's. In het geval van een probleem met de unieke machinegegevens, zal het systeem een melding tonen op het scherm. De vereiste toetsencombinatie en de knippervolgorde variëren afhankelijk of het systeem een notebook, desktop of tablet is. Handmatige modus is handig voor gebruikers die forensisch onderzoek kunnen doen op de systeemflash voorafgaand aan reparatie. Standaardgebruikers worden niet aangemoedigd om de handmatige modus te gebruiken. De standaardinstelling van deze functie is **Automatic (Automatisch)**.

Netwerkcontroller Configuratieherstel (alleen Intel)

Deze instelling is alleen beschikbaar op Intel-systemen. Indien geselecteerd, herstelt HP Sure Start onmiddellijk de fabrieksinstellingen van de netwerkcontroller-configuratie.

Melding bij configuratiewijziging netwerkcontroller (alleen Intel)

Deze instelling is alleen beschikbaar op Intel-systemen. HP biedt een in de fabriek ingestelde netwerkcontroller-configuratie die een MAC-adres omvat. Als deze instelling ingesteld is op **enable (ingeschakeld)**, monitort het systeem de status van de netwerkcontroller-configuratie en waarschuwt de gebruiker indien er een wijziging is van de fabrieksinstellingen. De standaardinstelling van deze functie is **disable (uitgeschakeld)**.

Dynamic Runtime scannen van boot-block (alleen Intel)

Deze instelling is alleen beschikbaar op Intel-systemen. Indien in de standaardinstelling van **enable (ingeschakeld)**, controleert HP Sure Start periodiek de integriteit van het BIOS-boot block terwijl het besturingssysteem actief is. Indien ingesteld op **disable (uitgeschakeld)**, zal HP Sure Start alleen de integriteit controleren vóór een boot of herstel uit slaap- of sluimerstand.

HP Sure Start bescherming van BIOS-instellingen

Het beleid voor bescherming van BIOS-instellingen is standaard **disabled (uitgeschakeld)**. Om de functie in te schakelen moet de eigenaar/beheerder van het cliëntapparaat eerst alle BIOS-beleid naar de gewenste instelling zetten. De eigenaar/beheerder moet ook een BIOS-beheerderwachtwoord instellen om de bescherming van BIOS-instellingen via HP Sure Start te gebruiken.

Zodra dat is voltooid, zou het beschermingsbeleid voor de BIOS-instellingen gewijzigd moeten zijn naar "enabled (ingeschakeld)". Op dat moment wordt een back-up gemaakt van alle BIOS-instellingen in de beveiligde opslag van HP Sure Start. Vanaf nu kan geen van de instellingen van het BIOS lokaal of op afstand worden gewijzigd. Bij elke boot worden de BIOS-beleidsinstellingen geverifieerd en vergeleken met de gewenste status, en als er afwijkingen zijn, worden de BIOS-instellingen hersteld vanuit de HP Sure Start-beschermde opslag.

Om een BIOS-instelling te wijzigen, moet het BIOS-beheerderwachtwoord ingevoerd worden en moet de bescherming van BIOS-instellingen worden uitgeschakeld, waarna er wijzigingen in de BIOS-instellingen kunnen worden aangebracht.

HP Sure Start beveiligde boot key-bescherming

Met deze instelling die standaard op **enable (ingeschakeld)** is ingesteld, biedt HP Sure Start verbeterde bescherming van de veilige boot-databases en sleutels die het BIOS gebruikt om de integriteit en authenticiteit van de OS-bootloader te verifiëren voordat deze bij het opstarten geladen wordt. Indien op **disable (uitgeschakeld)** ingesteld, wordt alleen standaard UEFI secure boot variabele bescherming gebruikt en wordt er geen back-up bewaard door het HP Sure Start-subsysteem.

Uitgebreidere HP Firmware Runtime Indringerspreventie en -detectie (alleen Intel) en HP Firmware Runtime Indringersdetectie (alleen AMD)

De RTID-functie is standaard **enabled (ingeschakeld)** voor alle platformen die worden verzonden vanuit de HP-fabriek. De eindgebruiker/beheerder hoeft deze eigenschap niet in te schakelen of te installeren om te profiteren van HP Sure Start RTID.

De RTID-functie kan optioneel worden ingesteld op **disable (uitschakelen)** door de platformeigenaar/beheerder.

HP Sure Start Security Event Policy

Deze BIOS-beleidsinstelling beheert welke actie er wordt uitgevoerd als HP Sure Start een aanval of poging daartoe detecteert terwijl het besturingssysteem actief is. Er zijn drie mogelijke configuraties voor dit beleid:

- **Alleen registreren van het event**: Als deze instelling is gekozen, registreert de HP ESC detectie-events die kunnen worden bekeken in de Applications and Services Logs/HP Sure Start-pad van de Microsoft Windows Event Viewer.[3]
- **Event registreren en gebruiker op de hoogte brengen**: Dit is de standaardinstelling. Als deze instelling is gekozen, registreert de HP ESC detectie-events die kunnen worden bekeken in de Applications and Services Logs/HP Sure Start-pad van de Microsoft Windows Event Viewer. Daarnaast wordt de gebruiker op de hoogte gebracht in Windows dat het event heeft plaatsgevonden.[4]
- **Event registreren en systeem uitschakelen**: Als deze instelling is gekozen, registreert de HP ESC detectie-events die kunnen worden bekeken in de Applications and Services Logs/HP Sure Start-pad van de Microsoft Windows Event Viewer. Daarnaast krijgt de gebruiker een melding in Windows dat het event heeft plaatsgevonden en dat het systeem zich zal uitschakelen.

HP Sure Start Security Event Boot-notificatie

Deze BIOS-beleidsinstelling bepaalt of HP Sure Start waarschuwingen en foutmeldingen die worden weergegeven wanneer het systeem wordt opgestart, vereisen dat de lokale gebruiker de fout bevestigt voordat het opstarten wordt voortgezet. Met de standaardinstelling **Require Acknowledgement (Bevestiging vereist)**, stopt het systeem als de foutmelding getoond wordt. De lokale gebruiker moet op een toets drukken om door te gaan met het opstarten. Indien gewijzigd naar **Time out after 15 seconds (Time-out na 15 seconden)**, zal de melding worden getoond maar gaat het bootproces automatisch verder nadat de boodschap 15 seconden is weergegeven.

BIOS-versie vergrendelen

In de (F10) BIOS-setup is deze functie te vinden in Algemeen/Bijwerken systeem-BIOS.

Indien **disable (uitgeschakeld)**, kunt u het BIOS bijwerken met alle processen die ondersteund worden. Als de HP ESC een geldige boot block-update detecteert in de systeemflash, wordt de back-up van het boot block bijgewerkt.

Indien **enable (ingeschakeld)** zullen alle HP BIOS updatetools weigeren om het BIOS bij te werken. Daarnaast beschermt HP Sure Start het BIOS tegen pogingen om de BIOS-versie te wijzigen door de systeemflash via een ongeautoriseerde methode te verwijderen. De HP ESC slaat de geblokkeerde versie van het BIOS op. Als de HP ESC detecteert dat het BIOS in de systeemflash is gewijzigd, overschrijft de HP ESC het BIOS-boot block met de HP ESC-kopie van het boot block. De HP ESC-kopie van het boot block wordt uitgevoerd en herstelt de rest van de juiste versie van het BIOS. De standaardinstelling van deze functie is **disable (uitgeschakeld)**.

Opslaan/herstel van systeemschijf en Opslaan/herstel GPT of systeemschijf

In de (F10) BIOS-setup is deze functie te vinden in Hulpprogramma's voor beveiliging/vaste schijf. Slechts een van deze mogelijkheden is beschikbaar, afhankelijk van het partitietype van de primaire drive (GPT of MBR), zoals gedetecteerd door HP Sure Start.

Indien **enable (ingeschakeld)**, maakt HP Sure Start een beschermde back-up van de MBR/GPT partitietabel van de primaire schijf en vergelijkt de back-up met de primaire bij elke boot. Als een verschil wordt gedetecteerd, wordt de gebruiker gevraagd en kan deze kiezen voor herstel uit de back-up naar de originele staat, of om de beschermde back-up bij te werken met de wijzigingen. De **Boot Sector (MBR/GPT) Recovery Policy** kan optioneel worden gebruikt om de gebruikersbeslissing voor de actie te verwijderen als er een verschil wordt gevonden door HP Sure Start.

Indien **disable (uitgeschakeld)** (standaard), wordt geen MBR/GPT-bescherming geboden door HP Sure Start.

Boot Sector (MBR/GPT) Recovery Policy

Indien ingesteld op **Local User Control (Lokaal gebruikersbeheer)** (standaard), wordt de gebruiker om de uit te voeren actie gevraagd als HP Sure Start een wijziging detecteert in de MBR/GPT-partitietabel. Indien ingesteld op **Recover in the event of corruption (Herstel in het geval van beschadiging)**, herstelt HP Sure Start automatisch de MBR/GPT naar de opgeslagen staat op elk moment dat verschillen worden geconstateerd.

Remote beheer van Controlepaneel HP Sure Start-beleid

Standaard is het HP Sure Start-beleid geoptimaliseerd voor de reguliere gebruiker. Omdat HP Sure Start standaard is ingeschakeld, hoeft een beheerder op afstand geen actie te ondernemen om HP Sure Start in te schakelen. Als een beheerder op afstand de beleidsinstellingen van HP Sure Start wil wijzigen, kunnen dezelfde scripts voor Windows Management Instrumentation (WMI) API's of HP BIOS Configuration Utility die gebruikt worden voor het beheer van BIOS-beleid van andere platformen gebruikt worden om HP Sure Start-beleidsregels te beheren. Daarnaast kunnen beheerders op afstand HP Sure Start-functies beheren met de Manageability Integration Kit (MIK)-plugin voor Microsoft System Center Configuration Manager (SCCM).

Daarnaast kunnen beheerders op afstand HP Sure Start-functies beheren en HP Sure Start-events bekijken met de Manageability Integration Kit (MIK)-plugin voor Microsoft System Center Configuration Manager (SCCM).

Conclusie

HP Sure Start biedt deze belangrijke voordelen:

- **Ononderbroken productiviteit** – HP Sure Start handhaaft bedrijfscontinuïteit in het geval van een aanval of accidentele corruptie door het elimineren van de storingsduur bij het wachten op IT/ondersteuning.
- **Lagere kosten** – Het herstelvermogen van HP Sure Start vermindert automatisch het aantal telefoontjes naar de IT-helpdesk en verhoogt de productiviteit, waardoor uiteindelijk de onderhoudskosten van het platform kunnen dalen.
- **Een gerust gevoel** – HP Sure Start heeft meerdere beveiligingsfuncties die verspreid zijn over een breed aanbod aan software- en hardwareplatformen.

Bescherm kritieke BIOS-firmware tegen malware met de toonaangevende firmware indringersdetectie en automatisch herstel door HP Sure Start, exclusief verkrijgbaar op bepaalde HP Elite pc's.

Bijlage A – HP Sure Start, Gen tot Gen

HP introduceerde Sure Start in 2014. Sindsdien heeft HP Sure Start verbeterd en het aantal producten die het gebruikt uitgebreid. De onderstaande tabel geeft een samenvatting van de mogelijkheden die met elke generatie zijn toegevoegd.

Generatie	Releasedatum	Toegevoegde mogelijkheden
HP Sure Start	2014	• Firmware en BIOS authenticiteitshandhaving, met de mogelijkheid voor zelfherstel • Firmware-monitoring en naleving
HP Sure Start met Dynamic Protection	2015	• Windows Event Viewer ondersteuning • Dynamic Protection (voor bepaalde Intel-producten)
HP Sure Start Gen3 (bepaalde Intel-producten)[5] HP Sure Start met Runtime Indringersdetectie (bepaalde AMD-producten)[6]	2017	• Runtime Intrusion Detection • Bescherming van BIOS-instellingen • Manageability Integration Kit (MIK)-plugin voor Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Beschermde opslag – sterke cryptografische methoden om BIOS-instellingen, gebruikersgegevens en andere instellingen in de HP Endpoint Security Controller-hardware op te slaan voor integriteitsbeveiliging, misbruikdetectie en vertrouwensbeveiliging voor die gegevens • Beveiliging van veilige boot-database – verhoogde beveiliging van databases en sleutels opgeslagen door het BIOS die kritiek zijn voor de integriteit van de veilige opstart van het besturingssysteem ten opzichte van de standaard UEFI BIOS-implementatie • Verhoogde beveiliging en herstel van de Intel Management Engine Firmware op Intel-platforms • Beveiligingscertificering van derden van de HP Endpoint Security Controller – testen door een onafhankelijk en geaccrediteerd laboratorium om te valideren dat de HP ESC-kernfunctionaliteit voor hardware volgens de publiek beschikbare criteria, methodologie en processen werkt zoals geclaimd[1] • HP business pc's met HP Sure Start scoren beter dan de Draft NIST Platform Firmware Resiliency-richtlijnen (Speciale Publicatie 800-193)

Bijlage B – Overzicht System Management Mode (SMM)

System Management Mode (SMM) is een industrienorm die gebruikt wordt voor geavanceerde stroombeheerfuncties en andere besturingssysteem-onafhankelijke functies terwijl het besturingssysteem draait. Omdat de SMM-term en implementatie specifiek zijn voor x86-architecturen, gebruiken veel moderne computerarchitecturen een gelijksoortig architectuurconcept.

SMM wordt door het BIOS geconfigureerd tijdens het opstarten. De SMM-code wordt in het hoofdgeheugen (DRAM) geladen en dan gebruikt het BIOS speciale (blokkeerbare) configuratieregisters in de chipset om de toegang tot dit gebied te blokkeren als de microprocessor niet draait in een SMM-context. Tijdens het opstarten is de toegang tot de SMM-modus event-gestuurd. De chipset is geprogrammeerd om veel soorten events en timeouts te herkennen. Wanneer een dergelijke gebeurtenis zich voordoet, forceert de chipset-hardware de System Management Interrupt (SMI) inputpin. Bij de volgende instructieverwerking slaat de microprocessor de gehele status op en start SMM.

Als de microprocessor in SMM komt, forceert die een hardware output pin, SMI Active (SMIACT). Deze pin meldt aan de chipset-hardware dat de microprocessor in SMM gaat. Een SMI kan op elk moment worden geforceerd, tijdens elke procesmodus, behalve vanuit SMM zelf. De chipset-hardware herkent het SMIACT-signaal en leidt alle opvolgende geheugencycli om naar een beschermd deel van het geheugen (soms ook het SMRAM-gebied) genoemd, speciaal gereserveerd voor SMM. Direct na het ontvangen van de SMI-input en het toepassen van de SMIACT-output, begint de microprocessor zijn hele interne status op te slaan in dit beschermde geheugengebied.

Nadat de microprocessor-status is opgeslagen naar het SMRAM-geheugen, begint de speciale SMM handler code die ook in het SMRAM staat (daar geplaatst door het systeem-BIOS tijdens het opstarten), uitvoering in een speciale SMM-werkingsmodus. Tijdens operatie in deze modus, worden de meeste hardware- en geheugenisolatiemechanismes opgeschort en heeft de microprocessor toegang tot vrijwel alle bronnen op het platform om de vereiste taken te kunnen uitvoeren. De SMM-code voltooit de vereiste taak, en dan is het tijd om de microprocessor terug te brengen in de vorige werkingsmodus. Op dat moment voert de SMM-code de Return from System Management Mode (RSM)-instructie uit om SMM af te sluiten. De RSM-instructie zorgt ervoor dat de microprocessor zijn eerdere interne toestandsgegevens herstelt met behulp van de kopie opgeslagen in SMRAM bij de start van SMM. Na voltooiing van RSM is de hele microprocessorstoestand hersteld naar de toestand vlak voor het SMI-event, en het vorige programma (besturingssysteem, applicaties, hypervisor enz.) hervat de uitvoering precies waar het gebleven was.

[1] De HP Sure Start controller-hardware is gecertificeerd volgens het CSPN-certificeringskader.

[2] HP Sure Start met Dynamic Protection is beschikbaar op HP Elite-producten, uitgerust met 6de generatie Intel Core-processoren en hoger.

[3] HP Notification Software moet worden geïnstalleerd om HP Sure Start in de Windows Event Viewer te bekijken.

[4] HP Notification Software moet worden geïnstalleerd om meldingen te ontvangen.

[5] HP Sure Start Gen3 is beschikbaar op HP Elite-producten uitgerust met 7de generatie Intel Core-processoren.

[6] HP Sure Start met Runtime Intrusion Detection is beschikbaar op HP Elite-producten uitgerust met 7de generatie Intel Core-processoren.

[7] HP Sure Start Gen4 is beschikbaar op HP Elite- en HP Pro 600-producten uitgerust met 8ste generatie Intel- of AMD-processoren.

Meer informatie

hp.com/go/computersecurity

4AA7-3172NLNL, Mei 2018