Teknisk hvidbog

HP Sure Start

Automatisk BIOS-beskyttelse og -genopretning

Maj 2018

Indholdsfortegnelse

Introduktion

HP Sure Start kan automatisk registrere, stoppe og gendanne efter et BIOS-angreb eller beskadigelse uden indgriben fra IT-afdelingen og med lille eller ingen forstyrrelse af brugerproduktiviteten. Hver gang pc'en tændes, validerer HP Sure Start automatisk integriteten af BIOS-koden for at hjælpe med at sikre, at pc'en beskyttes mod ondsindede angreb. Når pc'en er i gang, overvåger Run-time Intrusion Detection konstant hukommelsen. I tilfælde af et angreb kan pc'en reparere sig selv med en isoleret "gylden kopi" af BIOS på under et minut.

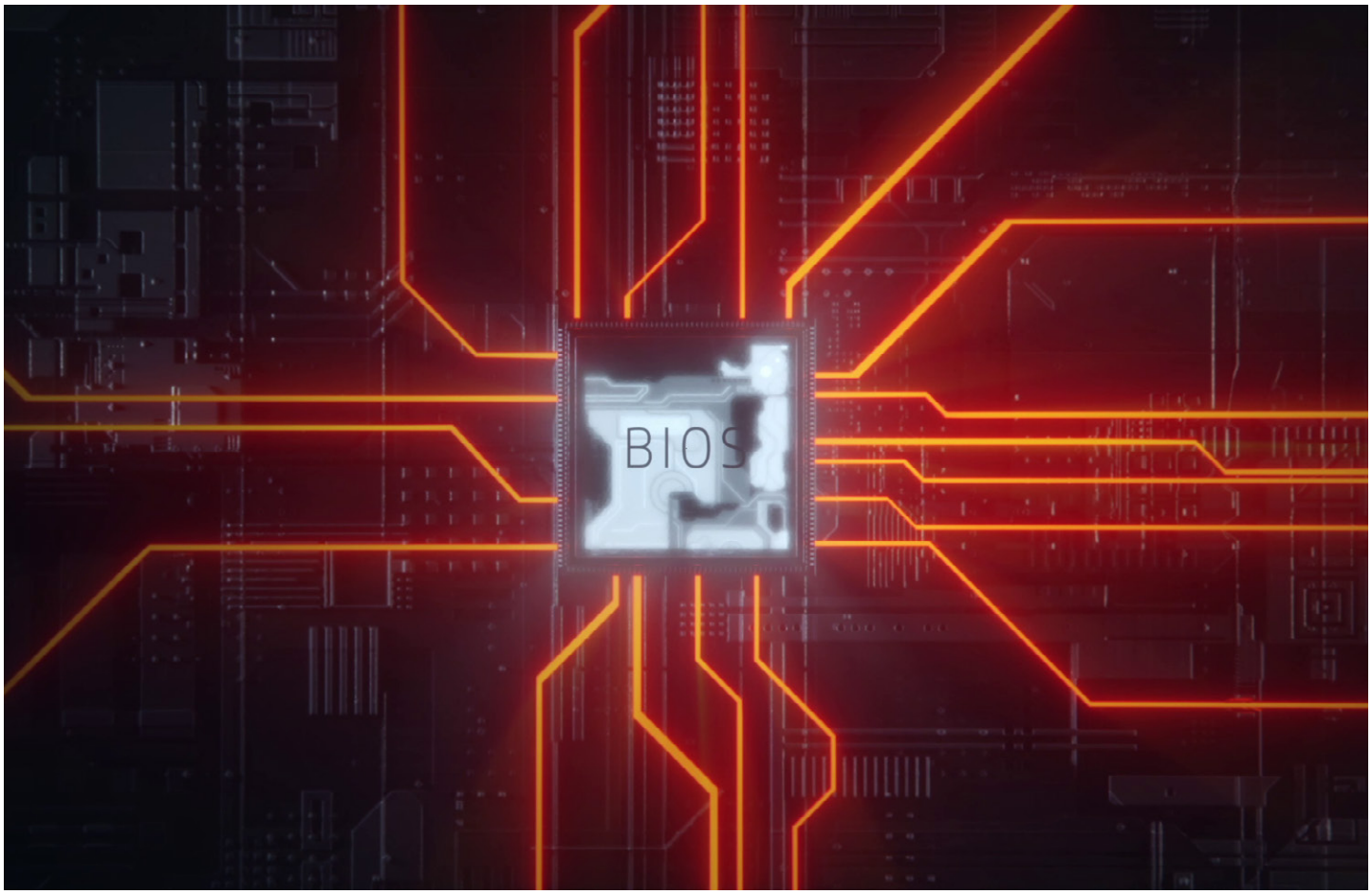
Hvorfor er BIOS-beskyttelse vigtig?

Efterhånden som vores verden bliver endnu mere forbundet, er der stadigt oftere mere og mere sofistikerede cyberangreb rettet mod klientenhedsfirmware og -hardware. Værktøjer og teknikker til angreb på firmware var engang teoretiske, og man troede, at de kun var tilgængelige for nationalstater. Sådanne værktøjer og teknikker har siden vist sig ikke bare at eksistere, men også være let tilgængelige i det offentlige domæne.

Enhedsfirmwaren (eller BIOS) er et attraktivt mål for hackere grundet de potentielle attributter, en succesfuld indtrængen kunne give angriberen:

- Ihærdighed: Firmware ligger i en non-volatile hukommelse på printkortet og kan ikke fjernes blot ved at slette harddisken.
- Kontrol: Firmware arbejder på højeste privilegieniveau – uden for OS-domænet, hvilket giver muligheden for OS-uafhængig malware.
- Hemmeligt: Firmware optager et område i hukommelsen, som er helt utilgængelig for operativsystemet og systemsoftwaren; idet den ikke kan scannes af antivirus, bliver den muligvis aldrig opdaget.
- Vanskelig gendannelse: Alle disse aspekter gør det ekstremt vanskeligt at gendanne fra denne type infektion uden at bruge en servicehændelse, der inkluderer en systemkortudskiftning.

Den ideelle løsning til beskyttelse af enheder mod denne type angreb er designet helt fra hardwaren ved brug af principperne om "cyberfleksibilitet". Disse principper anerkender, at det er ekstremt vanskeligt, hvis ikke umuligt, at forudse og forhindre ethvert muligt angreb. Den ideelle løsning giver ikke kun forbedret beskyttelse af firmwaren, men inkluderer også en hardwarebaseret mulighed for både at opdage et succesfuldt angreb og komme videre efter det.



HP Sure Start leverer fremragende firmwarebeskyttelse

HP Sure Start er HP's unikke og banebrydende tilgang til at levere avanceret firmwarebeskyttelse og fleksibilitet til HP-pc'er. Den bruger hardwarehåndhævelse via HP Endpoint Security Controller (HP ESC) for at sørge for beskyttelse af BIOS, som går langt ud over branchestandarden og sikrer, at systemet kun starter ægte HP BIOS. Hvis HP Sure Start derudover registrerer manipulation med BIOS, firmware eller run-time System Management Mode (SMM) BIOS-kode, kan det gendannes ved hjælp af en beskyttet sikkerhedskopi.

Resumé af HP Sure Start-funktioner

- Håndhævelse af autenticitet for HP-kerneplatformsfirmware og beskyttelse mod manipulation – HP Endpoint Security Controller-hardwarehåndhævelse af systemopstart, så kun autentisk og ikke-modificeret HP-firmware og HP BIOS indlæses
- Overvågning og overholdelse af firmwaresundhed – registrering af firmwaresundhedsrelaterede hændelser via isoleret HP Endpoint Security Controller; præsenterer platformsfirmwaretilstanden sammen med eventuelle uregelmæssigheder, der kunne indikere forhindrede angreb
- Selvreparerende – automatisk reparation af HP BIOS og HP-firmwarebeskadigelse ved hjælp af isoleret HP Endpoint Security Controller-sikkerhedskopi af HP BIOS og HP firmware
- BIOS-indstillingsbeskyttelse – udvider HP Endpoint Security Controller-beskyttelsen af BIOS-koden til at inkludere HP ESC-sikkerhedskopi og integritetskontrol af alle bruger- eller administratorkonfigurerede BIOS-indstillinger
- Run-time Intrusion Detection – løbende overvågning af kritisk BIOS-kode i run-time hukommelse (SMM), mens OS kører
- Sikker beskyttelse af startnøgler – væsentligt forbedret beskyttelse af databaser og nøgler opbevaret af BIOS, som er kritiske for integriteten af sikker OS-opstartsfunktion i forhold til UEFI BIOS-standardimplementering
- Beskyttet lagring – HP Sure Start bruger stærke kryptografiske metoder til lagring af BIOS-indstillinger, brugeroplysninger og andre indstillinger i HP Endpoint Security Controller-hardware for at levere integritetsbeskyttelse, manipulationsregistrering og fortrolig beskyttelse af de pågældende data
- Intel® Management Engine-firmwarebeskyttelse – forbedret beskyttelse og gendannelse af Intel Management Engine-firmware
- Administrerbarhed – administratorer kan administrere HP Sure Start-funktioner med Manageability Integration Kit-plugin'en (MIK) til Microsoft® System Center Configuration Manager (SCCM)

Et resumé over funktioner tilføjet i hver generation af HP Sure Start kan findes i bilag A på side 11.

Tredjepartssikkerhedscertificering

HP Endpoint Security Controller-hardwaren, der bruges i HP Sure Start, har gennemgået en tredjepartssikkerheds-vurdering og er blevet certificeret til at levere hardware håndhævelse, som kun autoriseret firmware kan starte på pc'en.[1]

Forsikring om, at en sikkerhedsløsning fungerer som angivet, er et kritisk element i enhver købsbeslutning relateret til sikkerhedsprodukter. Og fordi der er grænser for, hvor langt et ry for kvalitet kan gå, har HP udsat HP Endpoint Security Controllers indre virkemåde for en bedømmelse og test af et uafhængigt og akkrediteret laboratorium for at validere, at den fungerer som angivet i offentligt tilgængelige kriterier, metodologi og processer.

Cybersikkert design

HP Sure Start leverer ikke kun forbedret BIOS-beskyttelse, der overgår branchens standardtilgang, men er designet helt fra hardwaren til at levere uovertruffen platformscybersikkerhed for at sikre BIOS-gendannelse selv i tilfælde af et brud eller destruktivt angreb. HP erhvervs-pc'er med HP Sure Start overgår Draft National Institute of Standards

Technology (NIST) Platform Firmware Resiliency-retningslinjerne (Special Publication 800-193), som er en af de førende indsatser i den offentlige sektor for at formalisere kravene til cybersikre platforme.

HP Sure Start-understøttede modeller

HP introducerede Sure Start i 2014. Siden det tidspunkt har HP forbedret Sure Start og udvidet antallet af produkter, der inkluderer Sure Start. HP Sure Start leveres med hele Elite-produktserien fra 2018, herunder tabletter, notebooks, stationære computere og All-in-One-enheder (AIO'er). HP Sure Start Gen4 er tilgængelig på HP Elite- og HP Pro 600-produkter udstyret med 8. generation af Intel- eller AMD®-processorer.

Arkitekturoversigt og muligheder

HP Sure Start består af to større arkitekturmæssige komponenter:

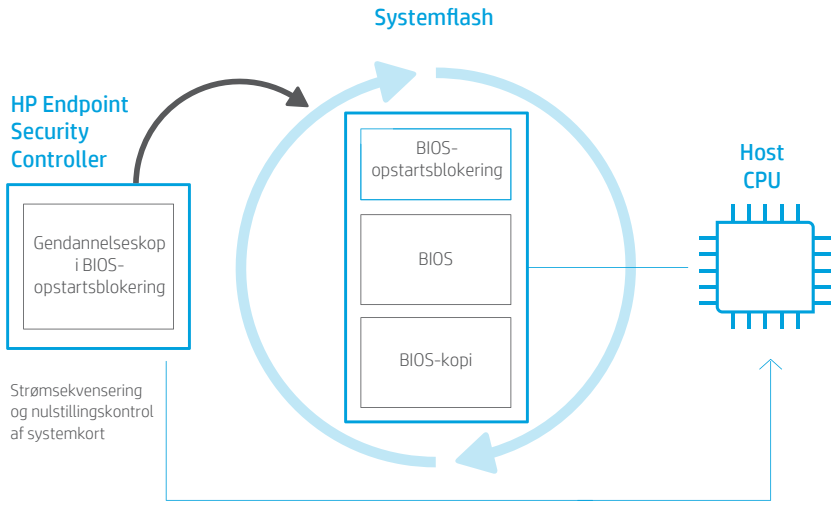
- **HP Endpoint Security Controller,** der kører HP Sure Start-firmware
- **HP Sure Start BIOS**, der arbejder sammen med HP Endpoint Security Controller-hardware og -firmware

Verifikation af firmwareintegritet – kernen i HP Sure Start

HP Endpoint Security Controller (HP ESC) er den første enhed i systemet til at udføre firmware, når systemet starter, aktiv i god tid, inden systemet starter. HP ESC-aktiviteter inkluderer, men er ikke begrænset til, overvågning af systemstartknappen og strømsekvensering af starten af værts-CPU-udførelse, når brugeren trykker på strømknappen.

Når platformen tilsluttes strøm første gang (inden systemet tændes), validerer HP ESC, at dens egen firmware er autentisk HP-kode inden indlæsning og udførelse af koden. HP ESC-hardwaren bruger stærke kryptografiske metoder, der overholder branchestandarden, til at udføre integritetsverificeringen. Metoden anvender en offentlig 2048-bit HP RSA-nøgle indeholdt i intern, permanent, skrivebeskyttet hukommelse. Derfor er HP ESC den indbyggede hardwarebaserede Root of Trust (RoT) for platformen, som anvendes til at validere firmwaren og HP BIOS, inden de udføres. Denne Root of Trust-hardware beskytter mod firmwareudskiftningsangreb uanset implementeringsmetode og fungerer som det fundament, hvorpå HP-platformssikkerhed er bygget.

Figur 1. Proces for verificering af firmwareintegritet.



Figur 1 illustrerer processen for verificering af firmwareintegriteten. Når HP ESC autentificerer og begynder udførsel af HP Sure Start-firmwaren, bruger den pågældende firmware samme stærke kryptografiske handlinger til at verificere integriteten af systemflash-BIOS-startblokken. Hvis en enkelt bit er ugyldig, erstatter HP ESC systemflash-indholdet med dens egen kopi af HP BIOS-startblokken, som er lagret i en isoleret, non-volatile hukommelse (NVM) dedikeret til HP ESC.

HP Sure Start-designet sikrer, at al firmware og BIOS-kode, der kører på både HP ESC og værts-CPU er den kode, som skulle være på enheden ifølge HP.

Bemærk: Systemflash-startblokkens integritetskontrol, og eventuel gendannelse udført af HP ESC, finder sted, mens værts-CPU'en er slået fra. Set fra brugerens side foregår hele handlingen derfor, mens systemet stadig er slukket, i slumretilstand eller i dvaletilstand.

Systemflash-BIOS-startblokken er fundamentet for HP BIOS. HP ESC-hardwaren sikrer, at BIOS-startblokken er den første kode, som CPU'en udfører efter en nulstilling. Når HP ESC afgør, at BIOS-startblokken indeholder autentisk HP-kode, tillader den systemet at starte som normalt.

HP ESC kontrollerer også integriteten af systemflash-startblokkoden, hver gang systemet slukkes eller sættes i dvale- eller slumretilstand. Idet CPU'en er slukket i alle disse tilstande, og CPU'en derfor skal genudføre BIOS-startblokkoden for at starte igen, er det af afgørende betydning hver gang at kontrollere integriteten af BIOS-startblokken for manipulation.

For HP/Intel modeller kontrollerer HP Sure Start derudover med jævne mellemrum (hvert 15. minut) integriteten af systemflash-BIOS-startblokken, mens systemet kører.[2]

Unik dataintegritet for maskinen

HP ESC og BIOS arbejder sammen om at levere avanceret beskyttelse af fabrikskonfigurerede kritiske variabler, der er unikke for hver enkelt maskine, som skal være konstante gennem levetiden for en hvilken som helst specifik platform.
I fabrikken gemmes en sikkerhedskopi af disse variable data i HP ESC non-volatile hukommelseslager. Sikkerhedskopien stilles til rådighed for HP Sure Start BIOS-komponenten (i skrivebeskyttet tilstand), som så kan udføre integritetskontrol af dataene ved hver opstart. Hvis en indstilling i den delte flash er ændret sammenlignet med fabriksindstillingerne, vil HP Sure Start BIOS-komponenterne automatisk gendanne dataene i systemflash fra den sikkerhedskopi, der stilles til rådighed af HP ESC.

Deskriptorområde

For HP/Intel modeller beskytter HP Sure Start deskriptorområdet for systemflashen. Unikt for Intel-arkitektur indeholder deskriptorområdet kritiske konfigurationsparametre, som Intel Core™-logik foretager stikprøvekontroller af ved nulstilling, og som derefter bruges til konfiguration Core-logikken. Deskriptorområdet indeholder også partitioneringsinformation for den systemflash, der bruges af Intel Core-logikken til at fastslå, hvor BIOS-området befinder sig i flashen, og derfor hvor deres CPU henter kode til udførelse fra nulstilling. HP Sure Start overvåger integriteten af dette område og gendanner det til den påtænkte konfiguration i tilfælde af manipulation eller beskadigelse.

Netværkscontrollerbeskyttelse

Desuden beskytter HP Sure Start for HP/Intel modeller indstillingerne for netværkscontrolleren (NIC) indeholdt med systemflashen. Visse HP-kunder har use cases, der kræver berettigede ændringer af fabrikskonfigurerede NIC-indstillinger. Derfor forhindrer HP Sure Start ikke som standard ændringer af NIC-indstillinger. I stedet har HP Sure Start en funktion, der, når den er aktiveret, advarer brugeren om, at NIC-indstillingerne blev ændret. Desuden tilbyder HP Sure Start en metode til gendannelse af NIC-indstillingerne til fabriksværdierne. Beskyttede indstillinger inkluderer MAC-adressen, Pre-boot Execution Environment-indstillingerne (PXE) og Remote Initial Program Load (RPL). Denne gendannelse er mulig via en skrivebeskyttet sikkerhedskopi beskyttet af HP ESC.

BIOS-indstillingsbeskyttelse

Som tidligere beskrevet verificerer HP Sure Start integriteten og autenticiteten af HP BIOS-koden. Idet denne kode er statisk, når den er blevet oprettet af HP, kan digitale signaturer bruges til at bekræfte begge kodens attributter. BIOS-indstillingernes dynamiske og brugerkonfigurerbare natur giver imidlertid yderligere udfordringer i forhold til at beskytte disse indstillinger. Digitale signaturer kan ikke genereres af HP og bruges af HP Sure Start ESC-hardwaren til at verificere disse indstillinger.

HP Sure Start BIOS-indstillingsbeskyttelse giver mulighed for at konfigurere systemet, så HP ESC-hardwaren bruges til at sikkerhedskopiere og kontrollere integriteten for alle de BIOS-indstillinger, som brugeren foretrækker.

Når denne funktion er aktiveret på platformen, sikkerhedskopieres alle politikindstillinger anvendt af BIOS efterfølgende, og der udføres en integritetskontrol af hver opstart for at sikre, at ingen af BIOS-politikindstillingerne er blevet ændret. Hvis der registreres en ændring, bruger systemet sikkerhedskopien fra HP Sure Starts beskyttede lager for automatisk at vende tilbage til den brugerdefinerede indstilling.

HP Sure Start BIOS-indstillingsbeskyttelsesfunktionen genererer hændelser til HP Sure Start ESC-hardwaren, når der registreres et forsøg på at modificere BIOS-indstillingerne. Hændelsen registreres i HP Sure Start-revisionsloggen, og den lokale bruger vil modtage en notifikation fra BIOS under opstart.

Beskyttet HP Sure Start-lager

Beskyttet lager rodfæstet i HP Endpoint Security Controller-hardwaren leverer den højeste grad af beskyttelse for BIOS/firmwaredata og indstillinger beskyttet af HP Sure Start. HP Sure Starts beskyttede lager er designet til at sikre fortrolighed, integritet og registrering af manipulation selv i tilfælde af fysiske angreb, hvor en angriber demonterer systemet og opretter en direkte forbindelse til den non-volatile lagerenhed på printkortet.

Dataintegritet

Integriteten af de dynamiske data gemt i den non-volatile hukommelse af firmware og brugt til at kontrollere tilstanden for forskellige funktioner har afgørende betydning for sikkerhedsholdningen for den samlede platform. Dynamiske data inkluderer alle BIOS-indstillinger, som kan modificeres af slutbrugeren eller administratoren af enheden. Eksempler inkluderer (men er ikke begrænset til) opstartsmuligheder som f.eks. den sikre opstartsfunktion, BIOS-administratoradgangskode og relaterede politikker, Trusted Platform Module-tilstandskontrol og HP Sure Start-politikindstillinger.

Eventuelle succesfulde angreb, der slipper forbi de eksisterende adgangsbegrænsninger til forebyggelse af uautoriserede ændringer af disse indstillinger, kunne overvinde platformssikkerheden. Overvej f.eks. en situation, hvor en angriber foretager en uautoriseret ændring af den sikre opstartstilstand for at deaktivere den uden at blive opdaget. I denne situation ville platformen starte angriberens rootkit, inden OS starter, uden at brugeren ved det.

Branchestandarden Unified Extensible Firmware Interface (UEFI) BIOS implementerer adgangsbegrænsninger, der skal forhindre uautoriserede ændringer af disse variabler, og HP implementerer dem ligesom resten af computerbranchen.

Grundet den risiko et brud på disse mekanismer udgør for platformen, tilbyder HP Sure Start sekundære forsvarsværker, som er stærkere end branchens basis standard.

BIOS-indstillinger og andre dynamiske data, der bruges af firmware til at kontrollere den tilstand, der er beskyttet af HP Sure Start, er gemt i den isolerede, non-volatile hukommelse i HP Endpoint Security Controller, som ikke er direkte tilgængelig for software, der kører på værts-CPU'en.

Derudover opretter og tilføjer HP ESC unikke integritetsmålinger, hver gang et dataelement gemmes i dette non-volatile hukommelseslager. Integritetsmålinger er baseret på en stærk kryptografisk algoritme (hashing-baseret meddelelses godkendelseskode, der bruger SHA-256-hashing), som er rodfæstet til en hemmelighed indeholdt i HP ESC. Hemmeligheden er unik for hver HP ESC, så hver controller genererer en unik integritetsmåling givet et identisk element.

Når dataelementet læses fra den non-volatile hukommelse, genberegner HP ESC integritetsmålingen for det pågældende dataelement og sammenligner den med den integritetsmåling, der er tilføjet til dataene. Alle uautoriserede ændringer af dataene i det non-volatile hukommelseslager medfører en manglende overensstemmelse. Ved hjælp af denne tilgang kan HP ESC opdage manipulation med dataelementer, der er gemt i det non-volatile hukommelseslager.

Datafortrolighed

For mange af de dataelementer, der er gemt af platformen, er det af afgørende betydning at bevare fortroligheden. Eksempler er BIOS-administratoradgangskodehashes, brugeroplysninger og hemmeligheder, der gemmes af firmware på vegne af brugeren til firmwarebaserede funktioner som f.eks. HP Sure Run og HP Sure Recovery.

Beskyttelse af disse hemmeligheder er udfordrende ved hjælp af UEFI BIOS-branchestandardtilgange, idet det non-volatile lager typisk kan læses af software, der kører på værtsprocessoren. Hensigten med HP Sure Starts beskyttede lager er at tilbyde meget større beskyttelse af disse fortrolige data end en UEFI BIOS-standardimplementering.

Ud over et separat, isoleret lager er HP Sure Start-tilgangen at udnytte den AES-hardwareblokering (Advanced Encryption Standard), der er indeholdt i HP ESC for at udføre AES-256-kryptering på alle fortrolige dataelementer gemt i HP Sure Starts non-volatile hukommelse, ud over dataintegritetsmålingerne for disse elementer. Den anvendte krypteringsnøgle er unik for hver enkelt HP ESC og forlader aldrig den pågældende controller, så data krypteret af en individuel HP ESC-komponent kan kun dekrypteres af den samme HP ESC.

Sikker beskyttelse af startnøgler

HP Sure Start tilbyder forbedret beskyttelse af de sikre UEFI-startnøgledatabaser, som gemmes af firmwaren, i forhold til den sikre UEFI-opstartsimplementering, der er branchestandard. Disse variabler er afgørende for korrekt drift af den sikre UEFI-opstartsfunktion, der kontrollerer integritet og autenticitet for OS-bootloaderen, inden den får lov til at gå i gang med opstarten.

HP Sure Start beskytter de sikre UEFI-startnøgledatabaser ved at bevare en masterkopi i det beskyttede HP Sure Start-lager. Alle autoriserede ændringer af sikre UEFI-standardstartnøgledatabaser af OS under run-time spores af HP Sure Start og anvendes på masterkopien af HP ESC. HP Sure Start bruger derefter masterkopien i HP Sure Starts beskyttede lager til at identificere og afvise eventuelle uautoriserede ændringer af de sikre UEFI standard startnøgæe databaser.

Denne funktion, der er aktiveret som standard, omfatter følgende databaser:

- Signaturdatabase (db)
- Tilbagekaldte signaturer-database (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) opdateret dynamisk ved run-time af OS

Runtime Intrusion Detection (RTID)

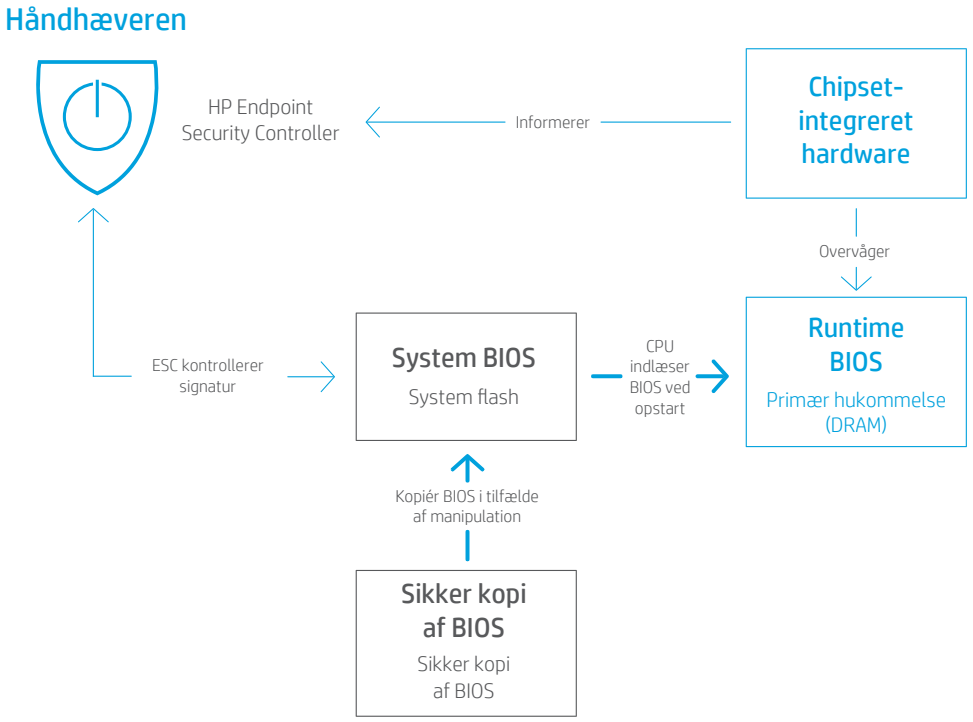
Ved hver opstart starter BIOS-koden udførelse fra flashhukommelse på en fast adresse. Dette kaldes BIOS-opstartskode og leverer præ OS opstarts-funktioner, som skal bruges, inden OS starter. Der er imidlertid en del af BIOS, som forbliver i DRAM, der skal bruges til at levere avancerede strømstyringsfunktioner, OS-tjenester og andre OS-uafhængige funktioner, mens OS kører. Denne BIOS-kode, der omtales som System Management Mode-kode (SMM), forbliver i et specielt område i DRAM, som er skjult fra OS. Vi henviser også til denne kode som "Run-time" BIOS-kode i forbindelse med HP Sure Starts Runtime Intrusion Detection-funktion. (Yderligere oplysninger om SMM, og hvordan det fungerer, kan findes i bilag B på side 12).

Integriteten af SMM-kode er kritisk for klientsikkerheds holdningen. HP Sure Start kontrollerer for at sikre, at HP SMM BIOS-kode er intakt ved OS-start. Runtime Intrusion Detection leverer mekanismer til at sikre, at SMM BIOS-koden forbliver intakt, mens OS kører, ved at tilføje nye beskyttelsesfunktioner og/eller levere en metode til registrering af et angreb på den pågældende kode.

Runtime Intrusion Detection-arkitektur

RTID-funktionen anvender specialiseret hardware i platform-schipsættet til at opdage uregelmæssigheder i Runtime HP SMM BIOS. Opdagelse af eventuelle uregelmæssigheder medfører en notifikation til HP Endpoint Security Controller, som kan udføre den konfigurerede politikhandling uafhængigt af CPU'en.

Figur 2. Runtime Intrusion Detection bruger specialhardware integreret i platformschipsættet til at overvåge SMM-kode for eventuelle ændringer.



Brugernotifikationer, hændelsesregistrering og administration af politikker

HP Sure Start-slutbrugernotifikationer

Under normale driftsforhold er HP Sure Start usynlig for brugeren. Gendannelseshandlinger anvender automatisk standardindstillingerne, og der er normalt ikke behov for slutbruger- eller it-interaktion ved gendannelsen, når HP Sure Start identificerer et problem. Brugere kan muligvis se runtime-notifikationer i tilfælde af et BIOS-integritetsproblem, der blev opdaget via funktionerne HP Sure Start Dynamic

Protection eller Runtime Intrusion Detection, mens OS kører. Hvis der registreres en væsentlig hændelse, eller der træffes foranstaltninger, viser HP Sure Start en advarselsmeddelelse via Windows®-notifikationer ved næste opstart. HP Notifications Software skal muliggøre visningen af disse Windows-notifikationer.

HP Sure Start-hændelsesregistrering

HP Endpoint Security Controller registrerer kritiske hændelser relateret til firmwaren/BIOS-koden og data overvåget af HP Sure Start. Disse hændelser gemmes i Sure Starts non-volatile hukommelseslager. Disse hændelser kopieres fra HP ESC til Windows Logbog, når HP Notifications Software er installeret, for at gøre adgangen til disse hændelser nemmere for den lokale bruger samt kundens foretrukne manageability agent.

Følgende hændelser vil få HP Notifications Software til at indsamle alle hændelser fra HP Sure Start-undersystemet og sikre, at Windows Logbog er opdateret med eventuelle hændelser, der ikke allerede er registreret her:

- Start af Windows
- Windows Resume fra slumre/dvale
- HP Sure Start med dynamiske beskyttelsesnotifikationer om runtime-hændelser
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Notifications Software udfylder HP Sure Start-hændelser i en unik "HP Sure Start"-programhændelseslog. Kun HP Sure Start-hændelser bliver inkluderet i denne log. Windows Logbog-stien til HP Sure Start-hændelser er følgende: Systemværktøjer/Logbog/Logfiler for programmer og tjenester/HP Sure Start.

Windows Logbog-niveaukategorierne relateret til HP Sure Start-hændelser er defineret i tabellen herunder.

Hændelserne udfyldes i Windows Logbog i den rækkefølge, de blev genereret af HP Sure Start. Den ældste hændelse i HP Sure Start-undersystemet tilføjes til Windows Logbog først, og den nyere hændelse tilføjes til sidst.

Tidsstemplet for hver registrering i Windows Logbog er det tidspunkt, den blev tilføjet til den pågældende log, IKKE det tidspunkt, hvor hændelsen opstod. Hver Sure Start Windows Logbog-registrering indeholder detaljerede data i hændelsesoplysningerne, hvilket inkluderer tidsstemplet for den faktiske forekomst.

Bemærk: Hændelser er permanente i HP Endpoint Security Controller selv efter kopiering til Windows Logbog. Hvis Windows Logbog ryddes, vil HP Notifications Software-programmet erstatte alle HP Sure Start-registreringer ved næste hændelse, der får det til at søge efter HP Sure Start- hændelsesregistreringer.

Typer af HP Sure Start Windows Logbog-hændelser

Hændelsesniveau	Definition
Information	Hændelser, der forventes at opstå under normal drift (f.eks. opdatering af BIOS).
Advarsel	Uventede hændelser, der er opstået, men blev gendannet helt af HP Sure Start, og der kræves ingen bruger-/administratorhandling, før platformen er fuldt funktionsdygtig. Disse hændelser er unormale handlinger, som brugeren/administratoren muligvis ønsker at undersøge yderligere, især hvis der er en tendens til disse hændelser på tværs af mange forskellige maskiner.
Fejl	Hændelser, der kræver, at administratoren/HP-service udfører handlinger på platformene for at komme videre.

HP Sure Start-politikkontroller

HP-systemets BIOS aktiverer og optimerer automatisk HP Sure Start-politikker for den typiske bruger. Eftersom HP Sure Start aktiveres som standard, er der ikke behov for, at den typiske bruger ændrer indstillingerne for at være beskyttet af HP Sure Start. For avancerede brugere tilbyder systemets BIOS en vis kontrol over HP Sure Starts adfærd ved hjælp af politikindstillingerne i (F10) BIOS-konfigurationen. Medmindre andet er angivet, findes disse indstillinger og funktioner under Sikkerhed/BIOS Sure Start.

Bemærk: Politikker gemmes i HP ESC non-volatile hukommelsen, som ikke er direkte tilgængelig for værts-CPU'en; derfor kræves en genstart, inden Sure Start-indstillingerne træder i kraft.

Følgende HP Sure Start-indstillinger og -funktioner er tilgængelige:

- Kontrollér startblok ved hver opstart
- Gendannelsespolitik for BIOS-data
- Gendannelse for netværkscontrollerkonfiguration (kun Intel)
- Giv besked ved ændring af netværkscontrollerkonfiguration (kun Intel)
- Dynamisk runtime-scanning af startblok (kun Intel)
- HP Sure Start BIOS-indstillingsbeskyttelse
- Sikker beskyttelse af HP Sure Start-startnøgler
- Forbedret HP-firmware Runtime Intrusion Prevention and Detection (kun Intel)
- HP-firmware Runtime Intrusion Detection (kun AMD)
- HP Sure Start-sikkerhedshændelsespolitik
- HP Sure Start-sikkerhedshændelsesstartnotifikation
- Lås BIOS-version
- Gem/gendan MBR for systemharddisk
- Gem/gendan GPT for systemharddisk
- Gendannelsespolitik for startsektor (MBR/GPT)

Kontrollér startblok ved hver opstart

HP Sure Start kontrollerer altid integriteten for systemflash-BIOS-startblokken, inden der fortsættes efter slumretilstand, dvaletilstand eller slukning. Når HP Sure Start er **aktiveret**, kontrolleres også integriteten af startblokken ved hver varm start (Windows-genstart). Det er et spørgsmål om hurtigere genstart i forhold til større sikkerhed. Indstillingen for denne funktion er som standard **deaktiveret**.

Gendannelsespolitik for BIOS-data

Ved indstilling til **Automatisk** reparerer HP Sure Start automatisk BIOS eller de unikke data for maskinen, hvis det er nødvendigt. Ved indstilling til **Manuel** kræver HP Sure Start en særlig nøglesekvens for at fortsætte med reparationen. I tilfælde af et problem med startblokkoden vil systemet afvise at starte, og en unik blinkesekvens blinker på systemets LED. I tilfælde af et problem med de unikke data for maskinen viser systemet en meddelelse på skærmen. Den krævede nøglesekvens og den viste blinkesekvens varierer, afhængigt af, om systemet er en notebook, en stationær computer eller en tablet. Manuel tilstand er praktisk for brugere, der kan undersøge systemflash-indholdet inden reparation. Typiske brugere opfordres ikke til at bruge den manuelle tilstand. Indstillingen for denne funktion er som standard **Automatisk**.

Gendannelse for netværkscontrollerkonfiguration (kun Intel)

Denne kontrol er kun tilgængelig på Intel-systemer. Når dette er valgt, gendanner HP Sure Start omgående netværkscontrollerkonfigurationen til fabriksstandarderne.

Giv besked ved ændring af netværkscontrollerkonfiguration (kun Intel)

Denne indstilling er kun tilgængelig på Intel-systemer. HP tilbyder en fabriksdefineret netværkscontrollerkonfiguration, som inkluderer MAC-adressen. Når denne indstilling er **aktiveret**, overvåger systemet tilstanden for netværkscontrollerkonfigurationen og giver brugeren besked i tilfælde af en ændring fra den fabrikskonfigurerede tilstand. Indstillingen for denne funktion er som standard **deaktiveret**.

Dynamisk runtime-scanning af startblok (kun Intel)

Denne indstilling er kun tilgængelig på Intel-systemer. I standardindstillingen som **aktiveret** kontrollerer HP Sure Start med jævne mellemrum integriteten for BIOS-startblokken, mens OS kører. Når indstillingen er **deaktiveret**, kontrollerer HP Sure Start kun integriteten inden en opstart eller genstart efter slumre- eller dvaletilstand.

HP Sure Start BIOS-indstillingsbeskyttelse

Politikken for BIOS-indstillingsbeskyttelse er som standard **deaktiveret**. For at aktivere funktionen skal ejeren/administratoren af klientenheden først konfigurere alle BIOS-politikker til den foretrukne indstilling. Ejeren/administratoren skal også konfigurere en BIOS-konfigurationsadministratoradgangskode for at bruge HP Sure Start BIOS-indstillingsbeskyttelse.

Når dette er udført, skal politikken for BIOS-indstillingsbeskyttelse ændres til "aktiveret". På dette tidspunkt oprettes en sikkerhedskopi af alle BIOS-indstillinger i det beskyttede HP Sure Start-lager. Fremover kan ingen af BIOS-indstillingerne ændres lokalt eller via fjernadgang. Ved hver opstart kontrolleres det, at BIOS-politikindstillingerne er i den ønskede tilstand, og hvis der er en uoverensstemmelse, gendannes BIOS-indstillingerne fra det beskyttede HP Sure Start-lager.

For at ændre en BIOS-indstilling skal BIOS-administratoradgangskoden angives, og BIOS-indstillingsbeskyttelsen skal efterfølgende deaktiveres, og på det tidspunkt kan der foretages ændringer af BIOS-indstillingerne.

Sikker beskyttelse af HP Sure Start-startnøgler

Når denne indstilling er i fabriksindstillingen **aktiveret**, leverer HP Sure Start forbedret beskyttelse af de sikre opstartsdatabaser og nøgler, der anvendes af BIOS til at kontrollere integriteten og autenticiteten for OS-bootloaderen, inden den starter ved opstart. Ved indstilling til **deaktiveret** bruges kun sikker UEFI-standardopstartsvariabelbeskyttelse, og der opbevares ingen sikkerhedskopi af HP Sure Start-undersystemet.

Forbedret HP-firmware Runtime Intrusion Prevention and Detection (kun Intel) og HP-firmware Runtime Intrusion Detection (kun AMD)

RTID-funktionen er **aktiveret** som standard for alle platforme fra HP-fabrikken. Der er ikke behov for, at slutkunden/administratoren aktiverer eller på anden måde "implementerer" funktionen for at benytte sig af HP Sure Start RTID.

RTID-funktionen kan eventuelt indstilles til **deaktiveret** af platformsejeren/-administratoren.

HP Sure Start-sikkerhedshændelsespolitik

Denne BIOS-politikindstilling kontrollerer, hvilke handlinger der udføres, når HP Sure Start opdager et angreb eller et forsøg på angreb, mens OS kører. Der er tre mulige konfigurationer for denne politik:

- **Registrer kun hændelse**: Når denne indstilling er valgt, registrerer HP ESC opdagelseshændelser, som kan ses i Logfiler for programmer og tjenester/HP Sure Start-stien i Microsoft Windows Logbog.[3]
- **Registrer hændelse, og giv besked til bruger**: Dette er standardindstillingen. Når denne indstilling er valgt, registrerer HP ESC opdagelseshændelser, som kan ses i Logfiler for programmer og tjenester/HP Sure Start-stien i Microsoft Windows Logbog. Derudover får brugeren besked i Windows om, at hændelsen opstod.[4]
- **Registrer hændelse, og sluk systemet**: Når denne indstilling er valgt, registrerer HP ESC opdagelseshændelser, som kan ses i Logfiler for programmer og tjenester/HP Sure Start-stien i Microsoft Windows Logbog. Derudover får brugeren besked i Windows om, at hændelsen opstod, og at systemet snart lukker ned.

HP Sure Start-sikkerhedshændelsesstartnotifikation

Denne BIOS-politikindstilling kontrollerer, om HP Sure Start-advarsler og -fejlmeddelelser, som vises, når systemet starter, kræver, at den lokale bruger anerkender fejlen, inden opstarten fortsætter. Med standardindstillingen **Kræver anerkendelse** stopper systemet, og fejlmeddelelsen vises. Den lokale bruger skal trykke på en tast for at fortsætte opstarten. Hvis den ændres til **Timeout efter 15 sekunder**, vises meddelelsen, men opstartsprocessen fortsætter automatisk, når meddelelsen har været vist i 15 sekunder.

Lås BIOS-version

I (F10) BIOS-konfigurationen findes denne funktion i Hoved/Opdater system-BIOS.

Ved indstilling til **deaktiveret** kan du opdatere BIOS ved hjælp af en hvilken som helst understøttet proces. Når HP ESC registrerer en gyldig startblokopdatering i systemflashen, opdateres sikkerhedskopien af startblokken.

Ved indstilling til **aktiveret** afviser alle HP BIOS-opdateringsværktøjer at opdatere BIOS. Derudover beskytter HP Sure Start BIOS mod forsøg på at ændre BIOS-versionen ved at fjerne systemflashen ved hjælp af en uautoriseret metode. HP ESC registrerer den låste version af BIOS. Når HP ESC registrerer, at BIOS i systemflashen blev ændret, overskriver HP ESC BIOS-startblokken med HP ESC-kopien af startblokken. HP ESC-kopien af startblokken udfører og gendanner resten af den korrekte version af BIOS. Indstillingen for denne funktion er som standard **deaktiveret**.

Gem/gendan MBR for systemharddisk og Gem/gendan GPT for systemharddisk

I (F10) BIOS-konfigurationen findes denne funktion i Sikkerhed/Harddiskhjælpeprogrammer. Kun én af disse funktioner er tilgængelig, afhængigt af partitionstypen for det primære drev (GPT eller MBR), som registreret af HP Sure Start.

Ved indstilling til **aktiveret** beholder HP Sure Start en beskyttet sikkerhedskopi af MBR-/GPT-partitionstabellen fra det primære drev og sammenligner sikkerhedskopien med den primære ved hver opstart. Hvis der registreres en forskel, bliver brugeren spurgt og kan vælge at gendanne fra sikkerhedskopien til den oprindelige tilstand eller at opdatere den beskyttede sikkerhedskopi med ændringerne. **Gendannelsespolitik for startsektor (MBR/GPT)** kan eventuelt bruges til at fjerne brugerbeslutningen for den handling, der foretages i tilfælde af en uregelmæssighed fundet af HP Sure Start.

Ved indstilling til **deaktiveret** (standard) leveres ingen MBR/GPT-beskyttelse af HP Sure Start.

Gendannelsespolitik for startsektor (MBR/GPT)

Ved indstilling til **Lokal brugerkontrol** (standard) bliver brugeren bedt om at foretage en bestemt handling, når HP Sure Start registrerer en ændring i MBR/GPT-partitionstabellen. Ved indstilling til **Gendan i tilfælde af beskadigelse** gendanner HP Sure Start automatisk MBR/GPT til den gemte tilstand, hver gang der registreres forskelle.

Fjernadministration af HP Sure Start-politikkontroller

Helt fra start er HP Sure Start-politikker optimeret til den typiske bruger. Idet HP Sure Start er aktiveret som standard, er der ikke behov for, at fjernadministratoren foretager en handling for at aktivere (eller "implementere") HP Sure Start. Hvis en fjernadministrator har et ønske om at ændre HP Sure Start-politikindstillingerne, kan de samme Windows Management Instrumentation (WMI) API'er eller HP BIOS Configuration Utility-scripts, som bruges til administration af BIOS-politikker på andre platforme, bruges til administration af HP Sure Start-politikker. Derudover kan administratorer fjernadministrere HP Sure Start-funktioner med Manageability Integration Kit-plugin'en (MIK) for Microsoft System Center Configuration Manager (SCCM).

Derudover kan administratorer fjernadministrere HP Sure Start-funktioner og se HP Sure Start-hændelser med Manageability Integration Kit-plugin'en (MIK) for Microsoft System Center Configuration Manager (SCCM).

Konklusion

HP Sure Start giver disse væsentlige fordele:

- **Uforstyrret produktivitet** – HP Sure Start bevarer forretningskontinuitet i tilfælde af et angreb eller en hændelig beskadigelse ved at eliminere nedetid, der bruges på at vente på it/service.
- **Lavere udgifter** – HP Sure Starts evne til at gendanne automatisk reducerer opkald til it-afdelingen og forbedrer produktiviteten, hvilket i sidste ende er med til at reducere vedligeholdelsesudgifterne til platformen.
- **Ro i sindet** – HP Sure Start har mange forskellige sikkerheds-funktioner, der kører på en lang række software- og hardwareplatforme.

Beskyt kritisk BIOS-firmware mod malware med brancheførende registrering af firmwareindtrængen og automatisk reparation tilbudt af HP Sure Start, udelukkende tilgængelig på udvalgte HP Elite-pc'er.

Bilag A – HP Sure Start, generation for generation

HP introducerede Sure Start i 2014. Siden det tidspunkt har HP forbedret Sure Start og udvidet antallet af produkter, der bruger det. Tabellen nedenfor indeholder et resumé over funktioner, som blev tilføjet i hver generation.

Generation	Udgivelsesdato	Funktioner tilføjet
HP Sure Start	2014	• Håndhævelse af firmware- og BIOS-autenticitet, med muligheden for selvreparation • Firmwareovervågning og -overholdelse
HP Sure Start med dynamisk beskyttelse	2015	• Understøttelse af Windows Logbog • Dynamisk beskyttelse (for udvalgte Intel-produkter)
HP Sure Start Gen3 (udvalgte Intel-produkter)[5] HP Sure Start med Runtime Intrusion Detection (udvalgte AMD-produkter)[6]	2017	• Runtime Intrusion Detection • BIOS-indstillingsbeskyttelse • Manageability Integration Kit-plugin (MIK) for Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Beskyttet lager – stærke kryptografiske metoder til opbevaring af BIOS-indstillinger, brugeroplysninger og andre indstillinger i HP Endpoint Security Controller-hardwaren for at levere integritetsbeskyttelse, registrering af manipulation og fortrolig beskyttelse af de pågældende data • Sikker opstartsdatabasebeskyttelse – forbedret beskyttelse af databaser og nøgler gemt af BIOS, som er kritiske for integriteten af den sikre OS-opstartsfunktion vs. UEFI BIOS-standardimplementering • På Intel-platforme: forbedret beskyttelse og gendannelse af Intel Management Engine-firmware • Tredjepartssikkerhedscertificering af HP Endpoint Security Controller – test af et uafhængigt og akkrediteret laboratorium for at validere, at HP ESC-hardwarekernefunktionaliteten fungerer som angivet i offentligt tilgængelige kriterier, metodologi og processer[1] • HP-virksomheds-pc'er med HP Sure Start overgår Draft NIST Platform Firmware Resiliency-retningslinjerne (Special Publication 800-193)

Bilag B – oversigt over System Management Mode (SMM)

System Management Mode (SMM) er branchens standardtilgang, der anvendes til avancerede pc-strømstyringsfunktioner og andre OS-uafhængige funktioner, mens OS kører. Mens SMM-termen og -implementeringen er specifik for x86-arkitekturer, bruger mange moderne it-arkitekturer et lignende arkitektonisk koncept.

SMM konfigureres af BIOS ved opstart. SMM-koden udfyldes i hovedhukommelsen (DRAM), og derefter bruger BIOS særlige (låsbare) konfigurationsregistre i chipsættet for at blokere adgang til dette område, når mikroprocessoren ikke arbejder i en SMM-kontekst. Ved runtime er registrering i SMM-tilstand hændelsesdrevet. Chipsættet er programmeret til at genkende mange typer hændelser og timeouts. Når en sådan hændelse opstår, anfører chipsæthardwaren System Management Interrupt-inputpinkoden (SMI). Ved næste instruktionsgrænse gemmer mikroprocessoren hele dens tilstand og går i SMM.

Når mikroprocessoren går i SMM, anfører den en hardwareoutputpinkode, SMI Active (SMIACT). Denne pinkode sender besked til chipsæthardwaren om, at mikroprocessoren går i SMM. En SMI kan anføres når som helst, under enhver procesdriftstilstand, undtagen fra selve SMM. Chipsæthardwaren genkender SMIACT-signalet og videresender alle efterfølgende hukommelsescyklusser til et beskyttet hukommelsesområde (omtales af og til som SMRAM-område), forbeholdt specifikt til SMM. Umiddelbart efter modtagelse af SMI-input og angivelse af SMIACT-output begynder mikroprocessoren at gemme hele sin interne tilstand på dette beskyttede hukommelsesområde.

Når mikroprocessortilstanden er blevet gemt i SMRAM-hukommelsen, begynder den særlige SMM-håndteringskode, som også findes i SMRAM (anbragt der af system-BIOS på opstartstidspunktet), at arbejde i en særlig SMM-driftstilstand. Under drift i denne tilstand suspenderes de fleste hardware- og hukommelsesisoleringsmekanismer, og mikroprocessorerne kan få adgang til praktisk taget alle ressourcer i platformen for at udføre de krævede opgaver. SMM-koden gennemfører den krævede opgave, og det er derefter tid til at returnere mikroprocessoren til den forrige driftstilstand. På det tidspunkt udfører SMM-koden Return from System Management Mode-instruktionen (RSM) for at afslutte SMM. RSM-instruktionen får mikroprocessoren til at gendanne sin tidligere interne tilstandsdata fra den kopi, der er gemt i SMRAM ved SMM-registrering. Ved gennemførsel af RSM er hele mikroprocessortilstanden blevet gendannet til tilstanden umiddelbart før SMI-hændelsen, og det tidligere program (OS, programmer, hypervisor osv.) genoptager udførelsen dér, hvor det stoppede.

[1] HP Sure Start-controllerhardwaren er blevet certificeret iht. CSPN-certificeringsrammen.

[2] HP Sure Start med dynamisk beskyttelse er tilgængelig på HP Elite-produkter udstyret med 6. generation af Intel Core-processorer og nyere.

[3] HP Notification Software skal installeres for at se HP Sure Start-hændelser i Windows Logbog.

[4] HP Notification Software skal installeres for at modtage notifikationer.

[5] HP Sure Start Gen3 er tilgængelig på HP Elite-produkter udstyret med 7. generation af Intel-processorer.

[6] HP Sure Start med Runtime Intrusion Detection er tilgængelig på HP Elite-produkter udstyret med 7. generation af AMD-processorer.

[7] HP Sure Start Gen4 er tilgængelig på HP Elite- og HP Pro 600-produkter udstyret med 8. generation af Intel- eller AMD-processorer.

Få mere at vide
hp.com/go/computersecurity

4AA7-3172DACI, Maj 2018