Teknisk hvitbok

HP Sure Start

Automatisk BIOS-beskyttelse og -reparasjon

Mai 2018

Innhold

Hvorfor er BIOS-beskyttelse viktig? 03

HP Sure Start gir uovertruffen fastvarebeskyttelse 04

Oversikt over arkitektur og ytelse 05

- Verifisering av fastvareintegritet – kjernen i HP Sure Start 05
- Maskinens unike dataintegritet 05
- Beskrivelsesområde 06
- Nettverkskontrollerbeskyttelse 06
- BIOS-innstillingsbeskyttelse 06
- HP Sure Start beskyttet lagring 06
- Sikker beskyttelse av oppstartsnøkler 07
- Runtime Intrusion Detection (RTID) 07

Brukervarsler, hendelseslogging og regelstyring 08

- HP Sure Start sluttbrukervarsler 08
- HP Sure Start hendelseslogging 08
- HP Sure Start regelkontroller 09
- Fjernstyring av HP Sure Start regelkontroller 10

Oppsummering 11

Vedlegg – HP Sure Start, generasjon for generasjon 11

Vedlegg B – Oversikt over System Management Mode (SMM) 12

Innledning

HP Sure Start kan automatisk oppdage, stoppe og gjenopprette fra et BIOS-angrep eller BIOS-korrupsjon uten IT-intervensjon og med små eller ingen avbrudd i brukerproduktivitet. Hver gang PC-en starter, bekrefter HP Sure Start automatisk integriteten til BIOS-koden, for å sikre at PC-en er beskyttet mot ondsinnede angrep. Når PC-en er i bruk, overvåker inntrengingsdeteksjonen minnet kontinuerlig. Ved et angrep kan PC-en helbrede seg selv ved bruk av en isolert "gyllen kopi" av BIOS på mindre enn et minutt.

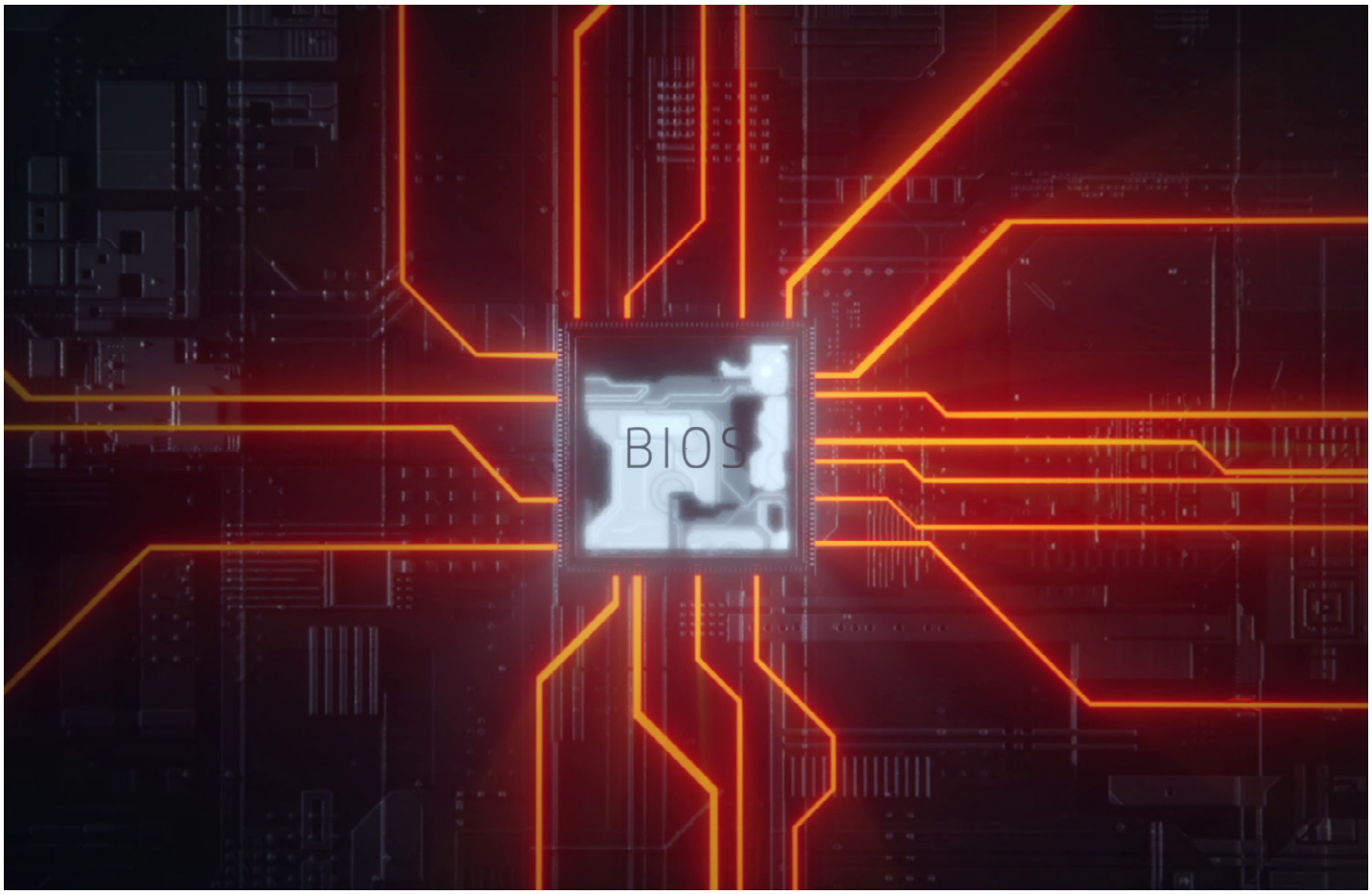
Hvorfor er BIOS-beskyttelse viktig?

Etter hvert som verdenen vår blir enda mer sammenkoblet, blir cyberangrep rettet mot fastvare og maskinvare på klientenheter, stadig hyppigere og mer sofistikerte. Verktøy og teknikker for å angripe fastvare var en gang i tiden kun teoretisk og noe man trodde bare var tilgjengelig for stater. Slike verktøy og teknikker har siden blitt vist ikke bare å eksistere, men også å være lett tilgjengelig for offentligheten.

Enhetens fastvare (eller BIOS) er et attraktivt mål for angripere på grunn av de mulige fordelene et vellykket innbrudd kan gi angriperen:

- Persistens: Fastvare ligger på et ikke-flyktig minne på kretskortet og kan ikke fjernes bare ved å slette harddisken.
- Kontroll: Fastvare kjøres på høyeste privilegienivå – utenfor OS-domenet, som muliggjør OS-uavhengig skadelig programvare.
- Skjult: Fastvare opptar et område av minne som er helt utilgjengelig for operativsystemet og systemprogramvaren; siden det ikke kan skannes av anti-virus, vil det kanskje aldri oppdages.
- Vanskelig gjenoppretting: Alle disse aspektene gjør det ekstremt vanskelig å gjenopprette fra denne typen infeksjon uten å benytte seg av en servicehendelse som inkluderer utskifting av systemkort.

Den ideelle løsningen for å beskytte enheter mot denne type angrep, er designet fra maskinvaren og opp ved bruk av prinsipper for "cyber-motstandsdyktighet". Disse prinsippene erkjenner at det er ekstremt vanskelig, om ikke umulig, å forutse og forhindre ethvert mulig angrep. Den ideelle løsningen gir ikke bare forbedret beskyttelse av fastvaren, men inkluderer også en maskinvarebasert evne til både å oppdage et vellykket angrep og gjenopprette fra det.



HP Sure Start gir uovertruffen fastvarebeskyttelse

HP Sure Start er HPs unike og banebrytende tilnærming til avansert fastvarebeskyttelse og motstandsdyktighet for HP-PC-er. Det bruker maskinvarehåndhevelse via HP Endpoint Security Controller (HP ESC) til å gi beskyttelse av BIOS som går langt ut over bransjestandarden, og sikrer at systemet bare starter opp original HP BIOS. Hvis HP Sure Start oppdager manipulering med BIOS, fastvare eller System Management Mode (SMM) BIOS-kode under kjøring, kan det i tillegg gjenopprette ved hjelp av en beskyttet sikkerhetskopi.

Sammendrag av HP Sure Start-funksjoner

- Autensitetshåndhevelse og innbruddsbeskyttelse for HP-kjerneplattform-fastvare – HP Endpoint Security Controller maskinvarehåndhevelse av systemoppstart, slik at bare autentisk og umodifisert HP-fastvare og HP BIOS lastes
- Overvåking av fastvarehelse og regeletterlevelse – Logging av hendelser relatert til fastvarehelse via isolert HP Endpoint Security Controller; presenterer status for plattformens fastvare sammen med uregelmessigheter som kan indikere forhindrede angrep
- Selvretting – Automatisk reparasjon av HP BIOS og HP fastvarefeil ved bruk av HP Endpoint Security Controller-isolert sikkerhetskopi av HP BIOS og HP-fastvare
- BIOS-innstillingsbeskyttelse – Utvider HP Endpoint Security Controller-beskyttelse av BIOS-koden til å inkludere HP ESC sikkerhetskopi og integritetssjekk av alle bruker- eller administratorkonfigurerte BIOS-innstillinger
- Runtime Intrusion Detection – Løpende overvåking av kritisk BIOS-kode i kjøreminnet (SMM) mens operativsystemet er aktivt
- Sikker beskyttelse av oppstartsnøkler – Betydelig forbedret beskyttelse av databaser og nøkler lagret av BIOS som er kritiske for integriteten for sikker oppstart av operativsystem versus standard UEFI BIOS-implementering
- Beskyttet lagring – HP Sure Start bruker sterke krypteringsmetoder til å lagre BIOS-innstillinger, brukerinnloggingsdetaljer og andre innstillinger i HP Endpoint Security Controller-maskinvaren for å gi integritetsbeskyttelse, inntrengningsdeteksjon og sikring av dataenes fortrolighet
- Intel® Management Engine fastvarebeskyttelse – Utvidet beskyttelse og gjenoppretting av Intel Management Engine-fastvaren
- Styrbarhet – Administratorer kan styre HP Sure Start-ytelse med tillegget Manageability Integration Kit (MIK) for Microsoft® System Center Configuration Manager (SCCM)

En oppsummering av ytelse i hver generasjon av HP Sure Start finnes i Vedlegg A på side 11.

Tredjeparts sikkerhetssertifisering

HP Endpoint Security Controller-maskinvaren som brukes i HP Sure Start, har gjennomgått en sikkerhetsvurdering fra tredjepart og har blitt sertifisert for levering av maskinvarehåndhevelse slik at bare autorisert fastvare kan starte på PC-en[1].

Å vite at en sikkerhetsløsning fungerer som oppgitt, er kritisk for enhver kjøpsavgjørelse knyttet til sikkerhetsprodukter. Og fordi et rykte for å levere kvalitet alene ikke er nok, har HP avslørt HP Endpoint Security Controllers interne funksjon for gjennomgang og testing av et uavhengig og godkjent laboratorium, for å validere at det fungerer slik det hevdes, i henhold til offentlig tilgjengelige kriterier, metodikk og prosesser.

Et cyber-motstandsdyktig design

HP Sure Start gir ikke bare forbedret BIOS-beskyttelse ut over bransjestandard, men er designet fra maskinvaren og opp for en uovertruffen plattform-cyber-robusthet som sikrer BIOS-gjenoppretting selv ved innbrudd eller ødeleggende angrep. HPs bedriftsmaskiner med HP Sure Start overgår NISTs (National Institute of Standards

Technology) utkast til retningslinjer for plattform-fastvare-motstandsdyktighet (spesialutgivelse 800-193), som er et av de ledende offentlige programmene for formalisering av krav til cyber-robuste plattformer.

Modeller med HP Sure Start-støtte

HP introduserte Sure Start i 2014. Siden den tid har HP utvidet Sure Start og utvidet antall produkter som inkluderer det. HP Sure Start leveres for hele 2018 Elite-produktserien, inkludert for nettbrett, notebooks, skrivebordsmaskiner og såkalte AIO-er (All in Ones). HP Sure Start Gen4 er tilgjengelig på HP Elite- og HP Pro 600-produkter som er utstyrt med 8. generasjons Intel- eller AMD®-prosessorer.

Oversikt over arkitektur og ytelse

HP Sure Start består av to store arkitektoniske komponenter:

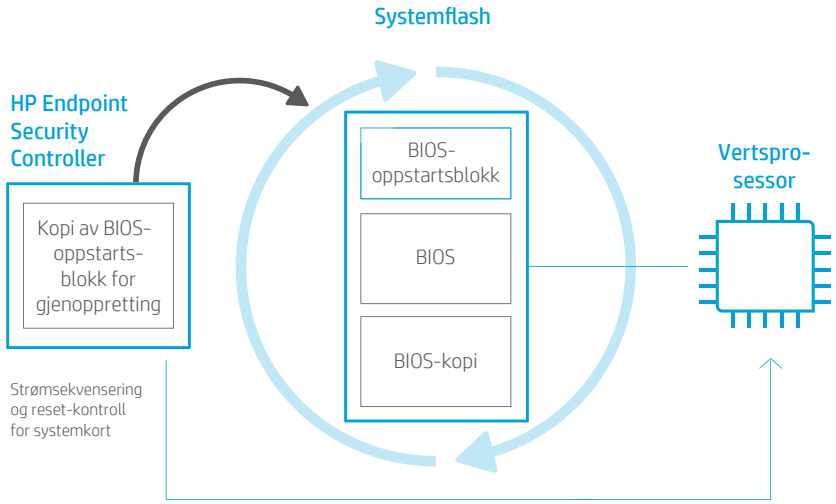
- **HP Endpoint Security Controller** som kjører HP Sure Start fastvare
- **HP Sure Start BIOS** som arbeider sammen med HP Endpoint Security Controller maskinvare og fastvare

Verifisering av fastvareintegritet – kjernen i HP Sure Start

HP Endpoint Security Controller (HP ESC) er den første enheten i systemet som kjører fastvare når systemet slås på, og aktiveres før systemoppstart. HP ESC-aktivitetene inkluderer, men er ikke begrenset til overvåking av systemets på-knapp og strømsekvensering av oppstarten av prosessorkjøringen på verten når brukeren trykker på på-knappen.

Når strømmen først tilføres plattformen (før systemet slås på), bekrefter HP ESC at dens egen fastvare er autentisk HP-kode før koden lastes og kjøres. HP ESC-maskinvaren bruker sterke kryptografiske metoder av industristandard til å utføre integritetsbekreftelsen. Metoden anvender en 2048-biters HP RSA offentlig nøkkel som ligger i det interne permanente skrivebeskyttede minnet. HP ESC er derfor den innebygde maskinvarebaserte RoT (Root of Trust) for plattformen, som brukes til å validere plattformens fastvare og HP BIOS før de kjøres. Denne ROT-en beskytter mot fastvareutskiftningsangrep, uavhengig av distribusjonsmetoden, og fungerer som grunnlaget som HP-plattformsikkerheten bygges på.

Figur 1. Verifiseringsprosess for fastvareintegritet.



Figur 1 illustrerer verifiseringsprosessen for fastvareintegritet. Når HP ESC autentiserer og begynner å kjøre HP Sure Start-fastvaren, bruker fastvaren den samme sterke kryptografiske operasjonen til å verifisere integriteten til systemflashens BIOS-oppstartsblokk. Hvis en enkelt bit er ugyldig, erstatter HP ESC systemflashens innhold med sin egen kopi av HP BIOS-oppstartsblokken som er lagret i et isolert, ikke-flyktig minne (NVM) dedikert til HP ESC.

HP Sure Start-designet sikrer at all fastvare og BIOS-kode som kjører på både HP ESC og vertsprosessoren, er koden HP har ment skal være på enheten.

Merk: Kontrollen av integriteten for systemflashens oppstartsblokk og eventuell nødvendig gjenoppretting utført av HP ESC, finner sted mens vertsprosessoren er slått av. Fra brukerens synspunkt skjer hele operasjonen derfor når systemet fortsatt er av, i hvilemodus eller dvalemodus.

Systemflashens BIOS-oppstartsblokk er grunnlaget for HP BIOS. HP ESC-maskinvaren sikrer at BIOS-oppstartsblokken er den første koden som prosessoren utfører etter en reset. Når HP ESC har bestemt at BIOS-oppstartsblokken inneholder autentisk HP-kode, kan systemet starte opp som det normalt ville gjort.

HP ESC kontrollerer også integriteten til systemflashens oppstartsblokkkode hver gang systemet slås av eller settes i hvile- eller dvalemodus. Siden prosessoren er slått av i hver av disse tilstandene, og prosessoren derfor er pålagt å utføre BIOS-oppstartsblokkkoden for å gjenoppta driften, er det avgjørende å kontrollere BIOS-oppstartsblokkenes integritet på nytt hver gang for tegn på angrep/endring.

For HP Intel-modeller kontrollerer HP Sure Start i tillegg integriteten til systemflashens BIOS-oppstartsblokk regelmessig (hvert 15. minutt) mens systemet kjører.[2]

Maskinens unike dataintegritet

HP ESC og BIOS jobber sammen for å gi avansert beskyttelse av fabrikk-konfigurerte kritiske variabler som er unike for hver maskin, og som skal være konstante gjennom en bestemt plattforms levetid. I fabrikken lagres en sikkerhetskopi av disse variabeldataene i det ikke-flyktige HP ESC-minnet. Sikkerhetskopien gjøres tilgjengelig for HP Sure Start BIOS-komponenten på skrivebeskyttet basis for utførelse av integritetssjekk av dataene ved hver oppstart. Hvis en innstilling i det delte flashminnet har endret seg i forhold til fabrikkinnstillingene, gjenoppretter HP Sure Start BIOS-komponentene automatisk dataene i systemflashen fra sikkerhetskopien fra HP ESC.

Beskrivelsesområde

For HP Intel-modeller beskytter HP Sure Start systemflashens beskrivelsesområde. Unikt for Intel-arkitekturen inneholder beskrivelsesområdet kritiske konfigurasjonsparametere som samples av Intel Core™-logikken ved reset, og som deretter brukes til å konfigurere Core-logikken. Beskrivelsesområdet inneholder også partisjoneringsinformasjon for systemflashen som brukes av Intel Core™-logikken til å bestemme hvor på flashen BIOS-området ligger, og derfor hvor prosessoren henter kode for kjøring fra reset. HP Sure Start overvåker integriteten til dette området og gjenoppretter det til den tiltenkte konfigurasjonen i tilfelle manipulering eller feil.

Nettverkskontrollerbeskyttelse

For HP Intel-modeller beskytter HP Sure Start i tillegg nettverkskontroller-innstillingene (NIC) som ligger på systemflashen. Noen HP-kunder har brukssituasjoner som krever legitime endringer i fabrikkonfigurerte NIC-innstillinger. HP Sure Start forhindrer derfor som standard ikke endringer i NIC-innstillinger. I stedet har HP Sure Start en funksjon som, når den er aktivert, varsler brukeren om at NIC-innstillingene er endret. I tillegg har HP Sure Start en metode for å tilbakestille NIC-innstillingene til fabrikkverdiene. Beskyttede innstillinger inkluderer MAC-adresse, PXE-innstillinger (Pre-boot Execution Environment) og RPL (Remote Initial Program Load). Denne gjenopprettingen er mulig via en skrivebeskyttet sikkerhetskopi beskyttet av HP ESC.

BIOS-innstillingsbeskyttelse

Som tidligere beskrevet verifiserer HP Sure Start integriteten og autentisiteten til HP BIOS-koden. Siden denne koden er statisk etter at den er opprettet av HP, kan digitale signaturer brukes til å bekrefte begge kodens attributter. BIOS-innstillingenes dynamiske og brukerkonfigurerbare karakter skaper imidlertid flere utfordringer for beskyttelse av disse innstillingene. Digitale signaturer kan ikke genereres av HP og brukes av HP Sure Start ESC-maskinvaren til å verifisere disse innstillingene.

Beskyttelsen av BIOS-innstillinger i HP Sure Start gir mulighet til å konfigurere systemet slik at HP ESC-maskinvaren brukes til å sikkerhetskopiere og kontrollere integriteten til alle BIOS-innstillingene foretrukket av brukeren.

Når denne funksjonen er aktivert på plattformen, sikkerhetskopieres alle regelinnstillinger som brukes av BIOS, og en integritetskontroll utføres ved hver oppstart for å sikre at ingen av BIOS-regelinnstillingene er endret. I tilfelle en endring oppdages, bruker systemet sikkerhetskopien fra HP Sure Start beskyttet lagring til å gå tilbake til den brukerdefinerte innstillingen automatisk.

Funksjonen for beskyttelse av BIOS-innstillingene i HP Sure Start genererer hendelser til HP Sure Start ESC-maskinvaren når et forsøk på å endre BIOS-innstillingene oppdages. Hendelsen logges inn i HP Sure Start-revisjonsloggen, og den lokale brukeren vil motta et varsel fra BIOS under oppstart.

HP Sure Start beskyttet lagring

Beskyttet lagring med rot i HP Endpoint Security Controller-maskinvaren gir det høyeste beskyttelsesnivået for BIOS-/fastvaredata og innstillinger beskyttet av HP Sure Start. HP Sure Start beskyttet lagring er utformet for å gi konfidensialitet, integritet og manipuleringsdeteksjon selv ved fysiske angrepsscenarioer der en angriper demonterer systemet og etablerer en direkte forbindelse til den ikke-flyktige lagringsenheten på kretskortet.

Dataintegritet

Integriteten til dynamiske data som er lagret i ikke-flyktig minne av fastvare, og som brukes til å kontrollere tilstanden til ulike funksjoner, er kritisk for plattformens overordnede sikkerhetsstilling. Dynamiske data inkluderer alle BIOS-innstillinger som kan endres av sluttbrukeren eller administratoren av enheten. Eksempler er (men ikke begrenset til) oppstartsalternativer som sikker-oppstart-funksjon, BIOS-administratorpassord og tilhørende regler, Trusted Platform Module tilstandskontroll og HP Sure Start-regelinnstillinger.

Ethvert vellykket angrep som omgår de eksisterende tilgangsbegrensningene for å forhindre uautoriserte endringer i disse innstillingene, vil kunne lure plattformsikkerheten. Tenk for eksempel et scenario der en angriper gjør en uautorisert endring av den sikre oppstartstilstanden og deaktiverer den uten å bli oppdaget. I dette scenarioet ville plattformen startet opp angripers rotsett før operativsystemet starter, uten brukerens kunnskap.

UEFI-BIOS (Unified Extensible Firmware Interface) etter bransjestandard implementerer tilgangsbegrensninger som skal forhindre uautoriserte modifikasjoner av disse variablene, og HP implementerer disse akkurat som resten av PC-bransjen.

Men med tanke på risikoen som et brudd på disse mekanismene utgjør for plattformen, gir HP Sure Start sekundære forsvar som er sterkere enn vanlig bransjestandard.

BIOS-innstillinger og andre dynamisk data som brukes av fastvaren til å kontrollere tilstanden som er beskyttet av HP Sure Start, lagres i det isolerte, ikke-flyktige minnet for HP Endpoint Security Controller som ikke er direkte tilgjengelig for programvare som kjører på vertsprosessoren.

I tillegg vil HP ESC opprette og tilføye unike integritetsmålinger hver gang et dataelement lagres i dette ikke-flyktige minnet. Integritetsmålingene er basert på en sterk kryptografisk algoritme (hashed-basert meldingsautentiseringskode som benytter SHA-256-hashing) med rot i en hemmelighet i HP ESC. Hemmeligheten er unik for hver HP ESC, slik at hver kontroller genererer en unik integritetsmåling gitt et identisk element.

Når dataelementet leses tilbake fra det ikke-flyktige minnet, beregner HP ESC integritetsmålingen på nytt for dette datalementet og sammenligner det med integritetsmålingen som legges til dataene. Eventuelle uautoriserte endringer i dataene i det ikke-flyktige minnet resulterer i en feil-sammenligning. Ved hjelp av denne tilnærmingen kan HP ESC oppdage manipulering av dataelementer lagret i det ikke-flyktige minnet.

Datafortrolighet

For mange av dataelementene som lagres av plattformen, er det viktig å opprettholde konfidensialitet. Eksempler inkluderer hash-koder for BIOS-administratorpassord, brukerlegitimasjon og hemmeligheter som lagres valgfritt av fastvare på vegne av brukeren for fastvarebaserte funksjoner som HP Sure Run og HP Sure Recovery.

Beskyttelse av disse hemmelighetene er utfordrende ved bruk av UEFI BIOS-tilnærminger etter bransjestandard, siden det ikke-flyktige minnet typisk er lesbart av programvare som kjører på vertsprosessoren. HP Sure Start beskyttet lagring er ment å gi mye bedre beskyttelse av disse konfidensielle dataene enn en vanlig UEFI BIOS-implementering.

I tillegg til en separat, isolert lagring er HP Sure Start-tilnærmingen å utnytte AES-maskinvareblokken (Advanced Encryption Standard) som finnes i HP ESC, for å utføre AES-256-kryptering på alle konfidensielle dataelementer som er lagret i det ikke-flyktige HP Sure Start-minnet, i tillegg til dataintegritetsmålingene for disse elementene. Krypteringsnøkkelen som brukes, er unik for hver HP ESC og forlater aldri kontrolleren, slik at data som er kryptert av en enkelt HP ESC-komponent, kun kan dekrypteres av samme HP ESC.

Sikker beskyttelse av oppstartsnøkler

HP Sure Start gir forbedret beskyttelse av de sikre UEFI-databasene med oppstartsnøkler som er lagret av fastvaren, i forhold til implementeringen av sikker UEFI-oppstart. Disse variablene er avgjørende for riktig drift av funksjonen for sikker UEFI-oppstart som verifiserer integriteten og autentisiteten til OS-oppstartslasteren før den tillates det å starte ved oppstart.

HP Sure Start beskytter databaser med sikre UEFI-oppstartsnøkler ved å holde en hovedkopi i HP Sure Start beskyttet lagring. Alle autoriserte modifikasjoner av databasene med sikre UEFI-oppstartsnøkler av operativsystemet under kjøretid spores av HP Sure Start og legges til hovedkopien av HP ESC. HP Sure Start bruker deretter hovedkopien i HP Sure Start beskyttet lagring til å identifisere og avvise eventuelle uautoriserte endringer i databasene med sikre UEFI-oppstartsnøkler.

Denne funksjonen, som er aktivert som standard, dekker følgende databaser:

- Signaturdatabase (db)
- Tilbakekalt signaturdatabase (dbx)
- Key Enrollment Key (KEK)
- Plattformnøkkel (PEK) oppdatert dynamisk under kjøring av OS

Runtime Intrusion Detection (RTID)

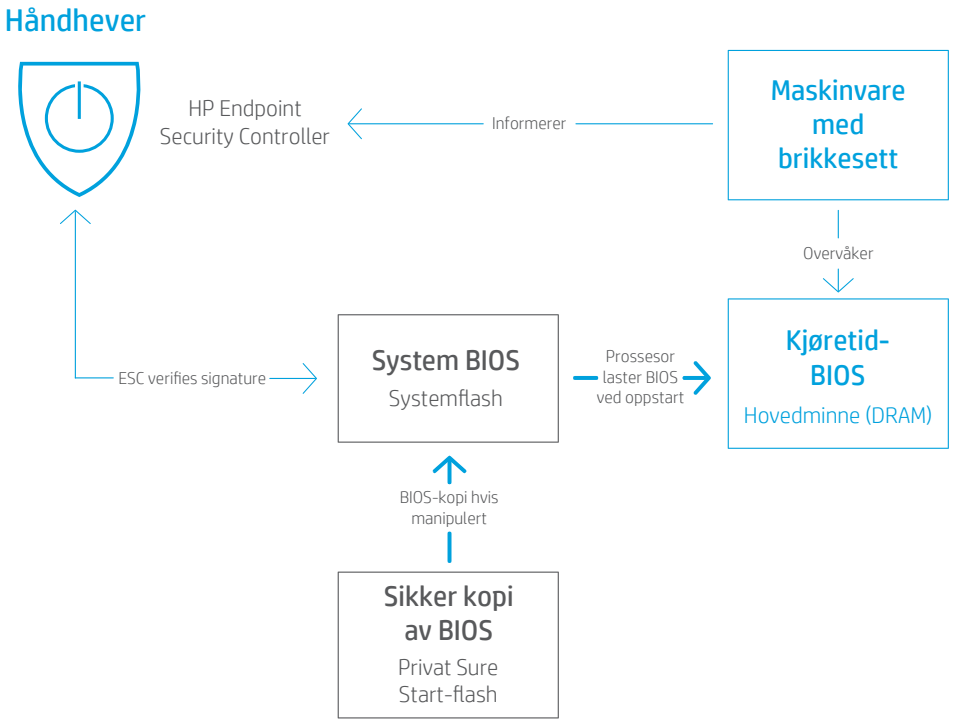
Ved hver oppstart startes BIOS-koden fra flash-minnet på en fast adresse. Dette kalles BIOS-oppstartskoden og har "pre-OS"-funksjoner som trengs før operativsystemet starter. Det er imidlertid en del av BIOS som forblir i DRAM som trengs for avanserte strømstyringsfunksjoner, OS-tjenester og andre OS-uavhengige funksjoner mens operativsystemet kjører. Denne BIOS-koden, referert til som SMM-koden (System Management Mode), ligger på et spesielt område innenfor DRAM som er skjult fra operativsystemet. Vi refererer også til denne koden som "Runtime" BIOS-kode i sammenheng med HP Sure Starts RID-funksjon (Runtime Intrusion Detection). (Mer informasjon om SMM og hvordan det virker, finnes i Vedlegg B på side 12).

SMM-kodens integritet er kritisk for klientens sikkerhetsstilling. HP Sure Start kontrollerer at HP SMM BIOS-koden er intakt ved OS-start. Runtime Intrusion Detection har mekanismer som sikrer at SMM BIOS-koden forblir intakt mens operativsystemet kjører ved å legge til nye beskyttelsesfunksjoner og/eller gi en måte å oppdage eventuelle angrep på koden på.

Runtime Intrusion Detection-arkitektur

RTID-funksjonen benytter spesialisert maskinvare i plattformbrikkesettet til å oppdage uregelmessigheter i Runtime HP SMM BIOS. Deteksjon av eventuelle uregelmessigheter resulterer i et varsel til HP Endpoint Security Controller, som kan utføre den konfigurerte regelhandlingen uavhengig av prosessoren.

Figur 2. Runtime Intrusion Detection bruker spesialisert maskinvare innebygd i plattformbrikkesettet til å overvåke SMM-kode for eventuelle endringer.



Brukervarsler, hendelseslogging og regelstyring

HP Sure Start sluttbrukervarsler

Under normale driftsforhold er HP Sure Start usynlig for brukeren. Gjenopprettingsoperasjoner utføres automatisk ved hjelp av standardinnstillingene, uten at noen sluttbruker eller IT-interaksjon normalt kreves for gjenoppretting når HP Sure Start identifiserer et problem.

Brukere kan se kjøretidsvarsler dersom et BIOS-integritetproblem oppdages via HP Sure Start Dynamic Protection- eller Runtime Intrusion Detection-funksjonene mens operativsystemet kjører. Hvis det oppdages en signifikant hendelse eller en handling utføres, viser HP Sure Start en varselsmelding via Windows®-varslinger ved neste oppstart. HP Notifications Software kreves for å aktivere visning av disse Windows-varslene.

HP Sure Start hendelseslogging

HP Endpoint Security Controller registrerer kritiske hendelser relatert til fastvare/BIOS-kode og data overvåket av HP Sure Start. Disse hendelsene lagres i det ikke-flyktige Sure Start-minnet. Hendelsene kopieres fra HP ESC til Windows Hendelsesliste når HP Notifications Software er installert, for å lette tilgangen til disse hendelsene for den lokale brukeren, samt for kundens foretrukne styringsagent.

Følgende hendelser vil få HP Notifications Software til å samle alle hendelser fra HP Sure Start-undersystemet og sikre at Windows Hendelsesliste oppdateres med hendelser som ikke allerede er registrert der:

- Windows-oppstart
- Windows-gjenopptaking fra hvilemodus/dvalemodus
- HP Sure Start med dynamiske beskyttelsesvarsler i kjøretiden
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Notifications Software fyller ut HP Sure Start-hendelser i en unik "HP Sure Start"-programhendelseslogg. Bare HP Sure Start-hendelser vil være inkludert i denne loggen. Windows Hendelsesliste-banen til HP Sure Start-hendelsene er følgende: Systemverktøy/Hendelsesliste/Program- og tjenestelogger/HP Sure Start.

Nivåkategoriene for Windows Hendelsesliste relatert til HP Sure Start-hendelser er definert i tabellen nedenfor.

Hendelsene fylles ut i Windows Hendelsesliste i den rekkefølgen de ble generert av HP Sure Start. Den eldste hendelsen i HP Sure Start-undersystemet legges først til Windows Hendelsesliste, og den siste hendelsen legges til sist.

Tidsstempelet for hver Windows Hendelsesliste-oppføring er tidspunktet den ble lagt til loggen, IKKE tidspunktet for hendelsen. Hver Sure Start Windows Hendelsesliste-oppføring inneholder detaljerte data i hendelsesdetaljene, som inkluderer tidsstempel for den aktuelle forekomsten.

Merk: Hendelser er vedvarende i HP Endpoint Security Controller selv etter at de er kopiert til Windows Hendelsesvisning. Hvis Windows Hendelsesvisning tømmes, erstatter HP Notifications Software alle HP Sure Start-oppføringene på den neste hendelsen som utløser den, for å sjekke HP Sure Start-hendelslogger.

Hendelsestyper i HP Sure Start Windows Hendelsesvisning

Hendelsesnivå	Definisjon
Info	Hendelser som forventes å inntreffe under normal drift (for eksempel oppdatering av BIOS).
Advarsel	Uventede hendelser som har inntruffet, men som ble fullstendig gjenopprettet fra HP Sure Start, og ingen bruker-/admin-handling kreves for at plattformen skal være fullt operativ. Disse hendelsene er uregelmessige operasjoner som brukeren/admin kanskje vil ønske å undersøke nærmere, spesielt hvis man ser slike hendelser på flere maskiner.
Feil	Hendelser som krever handling fra admin/HP for at plattformene skal kunne gjenopprettes fullstendig.

HP Sure Start regelkontroller

HP-systemets BIOS aktiverer og optimaliserer HP Sure Start-regler for den typiske brukeren ut av esken. Siden HP Sure Start er aktivert som standard, trenger ikke den typiske brukeren å endre innstillingene for å være beskyttet av HP Sure Start. For avanserte brukere gir systemets BIOS noe kontroll over HP Sure Start-atferden ved bruk av regelinnstillinger i (F10) BIOS Setup. Med mindre annet er oppgitt, finnes disse innstillingene og funksjonene under Sikkerhet/BIOS Sure Start.

Merk: Regler lagres i det ikke-flyktige HP ESC-minnet som ikke er direkte tilgjengelig for vertsprosessoren. Derfor kreves en omstart før noen Sure Start-innstillinger trer i kraft.

Følgende HP Sure Start-innstillinger og -funksjoner er tilgjengelige:

- Verifisering av oppstartsblokk ved hver oppstart
- Regler for BIOS-datagjenoppretting
- Gjenoppretting av nettverkskontroller-konfigurasjon (kun Intel)
- Informasjon om endring av nettverkskontroller-konfigurasjon (kun Intel)
- Dynamisk kjøretidsskanning av oppstartsblokk (kun Intel)
- HP Sure Start beskyttelse av BIOS-innstilling
- HP Sure Start beskyttelse av sikre oppstartsnøkler
- Utvidet HP-forebygging og -deteksjon av fastvareinntrengning under kjøring (kun Intel)
- HP-deteksjon av fastvareinntrengning under kjøring (kun AMD)
- HP Sure Start regler for sikkerhetshendelser
- HP Sure Start varsel om sikkerhetshendelse ved oppstart
- Låsing av BIOS-versjon
- Lagre/gjenopprette systemharddiskens MBR
- Lagre/gjenopprette systemharddiskens GPT
- Gjenopprettingsregel for oppstartssektor (MBR/GPT)

Verifisering av oppstartsblokk ved hver oppstart

HP Sure Start kontrollerer alltid integriteten til systemflashens BIOS-oppstartsblokk før den gjenoppretter fra hvilemodus, dvalemodus eller avslått modus. Når innstillingen er **aktivert**, vil HP Sure Start også verifisere integriteten til oppstartsblokken ved hver varme oppstart (Windows-omstart). Avveiningen man må gjøre, er mellom kortere omstartstid versus mer sikkerhet. Standardinnstillingen for denne funksjonen er at den er **deaktivert**.

Regler for BIOS-datagjenoppretting

Når den er satt til **Automatisk**, reparerer HP Sure Start automatisk BIOS eller maskinens unike data når det er nødvendig. Når den er satt til **Manuell**, krever HP Sure Start en spesiell nøkkelsekvens for å fortsette med reparasjonen. Ved et problem med oppstartsblokk-koden vil systemet nekte å starte opp, og en unik sekvens vil blinke på systemlampen. Ved et problem med maskinens unike data vil systemet vise en melding på skjermen. Nøkkelsekvensen som kreves, og blinkesekvensen som vises, varierer avhengig av om systemet er en notebook, en skrivebordsmaskin eller en nettbrett. Manuell modus er nyttig for brukere som kan utføre undersøkelser på systemets flashinnhold før reparasjon. Typiske brukere oppfordres ikke til å bruke manuell modus. Standardinnstillingen for denne funksjonen er **Automatisk**.

Gjenoppretting av nettverkskontroller-konfigurasjon (kun Intel)

Denne kontrollen er bare tilgjengelig på Intel-systemer. Når den er valgt, gjenoppretter HP Sure Start standard fabrikkinnstillinger for nettverkskontroller-konfigurasjonen.

Informasjon om endring av nettverkskontroller-konfigurasjon (kun Intel)

Denne innstillingen er bare tilgjengelig på Intel-systemer. HP har en fabrikkdefinert nettverkskontroller-konfigurasjon som inneholder MAC-adressen. Når denne innstillingen er **aktivert**, overvåker systemet tilstanden til nettverkskontroller-konfigurasjonen og informerer brukeren ved en endring fra den fabrikkkonfigurerte tilstanden. Standardinnstillingen for denne funksjonen er at den er **deaktivert**.

Dynamisk kjøretidsskanning av oppstartsblokk (kun Intel)

Denne innstillingen er bare tilgjengelig på Intel-systemer. I standardinnstillingen **"aktivert"** kontrollerer HP Sure Start regelmessig integriteten til BIOS-oppstartsblokken mens operativsystemet kjører. Når den er **deaktivert**, kontrollerer HP Sure Start bare integriteten før en oppstart eller gjenopptaking fra hvilemodus eller dvalemodus.

Beskyttelse av HP Sure Start BIOS-innstillinger

Beskyttelsesreglene for BIOS-innstillingene er **deaktivert** som standard. For å aktivere funksjonen må eieren/administratoren av klientenheten først konfigurere alle BIOS-reglene til foretrukket innstilling. Eieren/administratoren må også konfigurere et administratorpassord for BIOS-oppsett for å bruke HP Sure Start BIOS-innstillingsbeskyttelsen.

Når dette er gjort, skal beskyttelsesregelen for BIOS-innstillinger endres til "aktivert". På dette tidspunktet opprettes en sikkerhetskopi av alle BIOS-innstillinger i HP Sure Start beskyttet lagring. I fortsettelsen kan ingen av BIOS-innstillingene endres lokalt eller eksternt. Ved hver oppstart verifiseres det at BIOS-policyinnstillingene er i ønsket tilstand, og hvis det er uoverensstemmelse, gjenopprettes BIOS-innstillingene fra HP Sure Start beskyttet lagring.

For å endre en BIOS-innstilling må BIOS-administratorpassordet oppgis og BIOS-innstillingsbeskyttelsen deretter deaktiveres, hvoretter endringer i BIOS-innstillingene kan gjøres.

HP Sure Start beskyttelse av sikre oppstartsnøkler

Med denne innstillingen **aktivert** (som er fabrikkstandard) gir HP Sure Start forbedret beskyttelse av databasene for sikker oppstart og nøkler som brukes av BIOS for å verifisere integriteten og autentisiteten til OS-opplasteren før den startes ved oppstart. Når den er **deaktivert**, brukes bare standard sikker UEFI-oppstartsvariabelbeskyttelse, og ingen sikkerhetskopier holdes av HP Sure Start-undersystemet.

Utvidet HP-forebygging og -deteksjon av fastvareinntrengning under kjøring (kun Intel) og HP-deteksjon av fastvareinntrengning under kjøring (RTID) (kun AMD)

RTID-funksjonen er **aktivert** som standard for alle plattformer som sendes fra HP-fabrikken. Sluttkunden/administratoren trenger ikke å aktivere eller på annen måte "rulle ut" funksjonen for å dra nytte av HP Sure Start RTID.

RTID-funksjonen kan eventuelt **deaktiveres** av plattformens eier/administrator.

HP Sure Start regler for sikkerhetshendelser

Denne BIOS-regelinnstillingen styrer hva som skjer når HP Sure Start oppdager et angrep eller forsøk på angrep mens operativsystemet kjører. Det er tre mulige konfigurasjoner for denne regelen:

- **Bare logg hendelse**: Når denne innstillingen er valgt, logger HP ESC deteksjonshendelser, som kan vises under banen program- og tjenestelogger/HP Sure Start i Microsoft Windows Hendelsesvisning.[3]
- **Logg hendelse og varsle bruker**: Dette er standardinnstillingen. Når denne innstillingen er valgt, logger HP ESC deteksjonshendelser, som kan vises under banen program- og tjenestelogger/HP Sure Start i Microsoft Windows Hendelsesvisning. I tillegg informeres brukeren i Windows om at en hendelse har inntruffet.[4]
- **Logg hendelse og slå av system**: Når denne innstillingen er valgt, logger HP ESC deteksjonshendelser, som kan vises under banen program- og tjenestelogger/HP Sure Start i Microsoft Windows Hendelsesvisning. I tillegg informeres brukeren i Windows om at hendelsen skjedde, og at en systemavstenging er nært forestående.

HP Sure Start varsel om sikkerhetshendelse ved oppstart

Denne BIOS-regelinnstillingen bestemmer om HP Sure Start-advarsler og -feilmeldinger som vises når systemet startes, krever at den lokale brukeren bekrefter feilen før oppstarten kan fortsette. Med standardinnstillingen **"Krev bekreftelse"** stopper systemet når feilmeldingen vises. Den lokale brukeren må trykke på en tast for å fortsette oppstarten. Hvis endret til **"Tidsavbrudd etter 15 sekunder"** vises meldingen, men oppstartsprosessen fortsetter automatisk etter at meldingen har blitt vist i 15 sekunder.

Lås BIOS-versjon

I BIOS-oppsettet (F10) finnes denne funksjonen i hoved-/oppdateringssystem-BIOS.

Når den er **deaktivert**, kan du oppdatere BIOS ved bruk av hvilken som helst støttet prosess. Når HP ESC oppdager en gyldig oppstartsblokkoppdatering i systemflashen, oppdateres oppstartsblokkens sikkerhetskopi.

Når den er **aktivert**, nekter alle HP BIOS-oppdateringsverktøy å oppdatere BIOS. I tillegg beskytter HP Sure Start BIOS-en fra forsøk på å endre BIOS-versjonen ved å fjerne systemflashen via en uautorisert metode. HP ESC registrerer den låste versjonen av BIOS. Når HP ESC oppdager at BIOS i systemflashen er endret, overskriver HP ESC BIOS-oppstartsblokken med HP ESC-kopien av oppstartsblokken. HP ESC-kopien av oppstartsblokken utføres og gjenoppretter resten av den riktige versjonen av BIOS. Standardinnstillingen for denne funksjonen er at den er **deaktivert**.

Lagre/gjenopprette systemharddiskens MBR og lagre/gjenopprette systemharddiskens GPT

I BIOS-oppsettet (F10) finnes denne funksjonen i verktøyene for sikkerhet/harddisk. Bare en av disse funksjonene er tilgjengelige, avhengig av primærdiskens partisjonstype (GPT eller MBR), som detektert av HP Sure Start.

Når den er **aktivert**, holder HP Sure Start en beskyttet sikkerhetskopi av MBR/GPT-partisjonstabellen fra primærdisken, og sammenligner sikkerhetskopien med primærversjonen ved hver oppstart. Hvis en forskjell oppdages, informeres brukeren, som så kan velge å gjenopprette fra sikkerhetskopien til den opprinnelige tilstanden eller å oppdatere den beskyttede sikkerhetskopien med endringene. **Gjenopprettingsregelen for oppstartssektoren (MBR/GPT)** kan eventuelt brukes til å fjerne brukerbeslutningen for handlingen som skal tas i tilfelle en uoverensstemmelse blir detektert av HP Sure Start.

Når den er **deaktivert** (standard), gir HP Sure Start ingen MBR/GPT-beskyttelse.

Gjenopprettingsregel for oppstartssektor (MBR/GPT)

Når den er satt til **Lokal brukerstyring** (standard), blir brukeren bedt om hvilken handling som skal utføres når HP Sure Start oppdager en endring i MBR/GPT-partisjonstabellen. Når den er satt til **Gjenopprett ved feil**, gjenoppretter HP Sure Start automatisk MBR/GPT til lagret tilstand når eventuelle forskjeller oppdages.

Fjernstyring av HP Sure Start regelkontroller

HP Sure Start-reglene er optimalisert for den typiske brukeren ut av esken. Siden HP Sure Start er aktivert som standard, trenger ikke ekstern administrator å gjøre noe for å aktivere (eller "rulle ut") HP Sure Start. Hvis en ekstern administrator ønsker å modifisere HP Sure Start-regelnnstillinger, kan de samme Windows Management Instrumentation (WMI) API-ene eller HP BIOS Configuration Utility-skriptene som brukes til å administrere andre BIOS-plattformer for plattformen, brukes til å administrere HP Sure Start-reglene. I tillegg kan administratorer eksternt administrere HP Sure Start-funksjoner med MIK-tillegget (Manageability Integration Kit) for Microsoft System Center Configuration Manager (SCCM).

I tillegg kan administratorer eksternt administrere HP Sure Start-funksjoner og se HP Sure Start-hendelser med MIK-tillegget (Manageability Integration Kit) for Microsoft System Center Configuration Manager (SCCM).

Konklusjon

HP Sure Start gir følgende hovedfordeler:

- **Uavbrutt produktivitet** – HP Sure Start opprettholder forretningskontinuiteten i tilfelle angrep eller utilsiktet feil ved å eliminere nedetid i påvente av IT/Service-hendelse.
- **Lavere kostnader** – HP Sure Starts evne til å gjenopprette automatisk reduserer antallet telefoner til IT-support og øker produktiviteten, som til syvende og sist bidrar til å redusere vedlikeholdskostnaden for plattformen.
- **Ro i sinnet** – HP Sure Start har flere sikkerhetsfunksjoner som kjører over et bredt spekter av programvare- og maskinvareplattformer.

Beskytt kritisk BIOS-fastvare fra skadelig programvare med HP Sure Starts bransjeledende inntrengningsdeteksjon og automatisk reparasjon, som kun er tilgjengelig på utvalgte HP Elite-PC-er.

Vedlegg A – HP Sure Start, generasjon for generasjon

HP introduserte Sure Start i 2014. Siden den tid har HP utvidet Sure Start og utvidet antall produkter som bruker det. Tabellen nedenfor gir et sammendrag over funksjonene som ble lagt til for hver generasjon.

Generasjon	Utgivelsesdato	Funksjoner lagt til
HP Sure Start	2014	• Fastvare- og BIOS-autentisitetshåndhevelse, med mulighet for selvretting • Fastvareovervåking og -etterlevelse
HP Sure Start med dynamisk beskyttelse	2015	• Støtte for Windows Hendelsesvisning • Dynamisk beskyttelse (for utvalgte Intel-produkter)
HP Sure Start Gen3 (utvalgte Intel-produkter)[5] HP Sure Start med Runtime Intrusion Detection (utvalgte AMD-produkter)[6]	2017	• Runtime Intrusion Detection • BIOS-innstillingsbeskyttelse • MIK-tillegg (Manageability Integration Kit) for Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Beskyttet lagring – sterke kryptografiske metoder for lagring av BIOS-innstillinger, brukerlegitimasjon og andre innstillinger i HP Endpoint Security Controller-maskinvaren for integritetsbeskyttelse, manipuleringsdeteksjon og fortrolighetsbeskyttelse for dataene • Beskyttelse av databaser for sikker oppstart – økt beskyttelse av databaser og nøkler lagret av BIOS som er kritiske for integriteten til funksjonen for sikker OS-oppstart versus standard UEFI BIOS-implementering • Forbedret beskyttelse og gjenoppretting av Intel Management Engine Firmware på Intel-plattformer • Tredjeparts sikkerhetssertifisering av HP Endpoint Security Controller – testing av et uavhengig og godkjent laboratorium for validering av at HP ESC-maskinvarens kjernefunksjonalitet fungerer som angitt i henhold til allment tilgjengelige kriterier, metodikk og prosesser[1] • HP forretningsmaskiner med HP Sure Start overskrider NIST-retningslinjene for motstandsdyktig plattformfastvare (spesialutgivelse 800-193)

Vedlegg B – Oversikt over System Management Mode (SMM)

System Management Mode (SMM) er en tilnærming etter bransjestandard som brukes for avanserte strømstyringsfunksjoner og andre OS-uavhengige funksjoner mens operativsystemet kjører. Selv om SMM-begrepet og -implementeringen er spesifikk for x86-arkitekturer, bruker mange moderne databehandlingarkitekturer et lignende arkitektonisk konsept.

SMM konfigureres av BIOS ved oppstart. SMM-koden fylles ut i hovedminnet (DRAM), hvorpå BIOS bruker spesielle (låsbare) konfigurasjonsregistere i brikkesettet til å blokkere tilgang til dette området når mikroprosessoren ikke kjøres i en SMM-kontekst. Under kjøring er aktivering av SMM-modus hendelsesdrevet. Brikkesettet er programmert til å gjenkjenne mange typer hendelser og tidsavbrudd. Når en slik hendelse inntreffer, kommuniserer brikkesett-maskinvaren en SMI-inngangspin (System Management Interrupt). Ved neste instruksjonsgrense lagrer mikroprosessoren hele sin tilstand og går inn i SMM.

Når mikroprosessoren går inn i SMM, kommuniserer den en maskinvare-utgangspin, SMI Active (SMIACT). Denne pinen varsler brikkesett-maskinvaren om at mikroprosessoren går inn i SMM. En SMI kan kommuniseres når som helst, i hvilken som helst prosessoperasjonsmodus, med unntak av fra SMM selv. Brikkesett-maskinvaren gjenkjenner SMIACT-signalet og omdirigerer alle etterfølgende minnesykluser til et beskyttet område av minnet (noen ganger kalt SMRAM-området), som er reservert spesielt for SMM. Straks etter mottak av SMI-inngangen og kommunikasjon av SMIACT-utgangen, begynner mikroprosessoren å lagre hele sin interne tilstand til dette beskyttede minneområde.

Etter at mikroprosessortilstanden er lagret til SMRAM-minnet, begynner den spesielle SMM-håndteringskoden som også er lokalisert i SMRAM (plassert der av system-BIOS ved oppstart) å kjøre i en spesiell SMM-driftsmodus. Ved drift i denne modusen er de fleste maskinvare- og minneisolasjonsmekanismer suspendert, og mikroprosessoren kan få tilgang til nesten alle ressurser i plattformen slik at den kan utføre nødvendige oppgaver. SMM-koden fullfører den nødvendige oppgaven, hvorpå mikroprosessoren skal returneres til forrige driftsmodus. På dette tidspunktet utfører SMM-koden RSM-instruksjonen (Return from System Management Mode) for å avslutte SMM. RSM-instruksjonen gjør at mikroprosessoren gjenoppretter sine tidligere interne tilstandsdata fra kopien som er lagret i SMRAM ved SMM-inngang. Når RSM er fullført, har hele mikroprosessortilstanden blitt gjenopprettet til tilstanden like før SMI-hendelsen, og det forrige programmet (operativsystem, programmer, hypervisor osv.) gjenoppretter kjøringen akkurat der den ble avsluttet.

[1] HP Sure Start Controller-maskinvaren er sertifisert etter CSPN-sertifiseringsrammeverket.

[2] HP Sure Start med dynamisk beskyttelse er tilgjengelig på HP Elite-produkter utstyrt med 6. generasjons Intel Core-prosessorer og høyere.

[3] HP Notification Software må installeres for visning av HP Sure Start-hendelser i Windows Hendelsesvisning.

[4] HP Notification Software må installeres for mottak av varsler.

[5] HP Sure Start Gen3 er tilgjengelig på HP Elite-produkter som er utstyrt med 7. generasjons Intel-prosessorer.

[6] HP Sure Start med Runtime Intrusion Detection er tilgjengelig på HP Elite-produkter som er utstyrt med 7. generasjons AMD-prosessorer.

[7] HP Sure Start Gen4 er tilgjengelig på HP Elite- og HP Pro 600-produkter som er utstyrt med 8. generasjons Intel- eller AMD-prosessorer.

Finn ut mer
hp.com/go/computersecurity

4AA7-3172NOE, Mai 2018