Tekninen asiantuntijaraportti

HP Sure Start

Automaattinen BIOS-tason suojaus ja korjaus

Toukokuu 2018

Sisällysluettelo

Johdanto

HP Sure Start havaitsee ja estää automaattisesti BIOSiin kohdistuvan hyökkäyksen tai korruption ja palautuu niistä ilman IT-osaston väliintuloa pienellä tai olemattomalla keskeytyksellä loppukäyttäjän tuottavuuteen. Joka kerta kun tietokone käynnistetään, HP Sure Start vahvistaa BIOS-koodin eheyden automaattisesti, mikä auttaa varmistamaan, että tietokone on suojattu hyökkäyksiltä. Kun tietokone on käytössä, käytön aikainen tunkeutumisen havaitseminen valvoo muistia jatkuvasti. Hyökkäyksen sattuessa tietokone voi palautua BIOS-varmuuskopion avulla alle minuutissa.

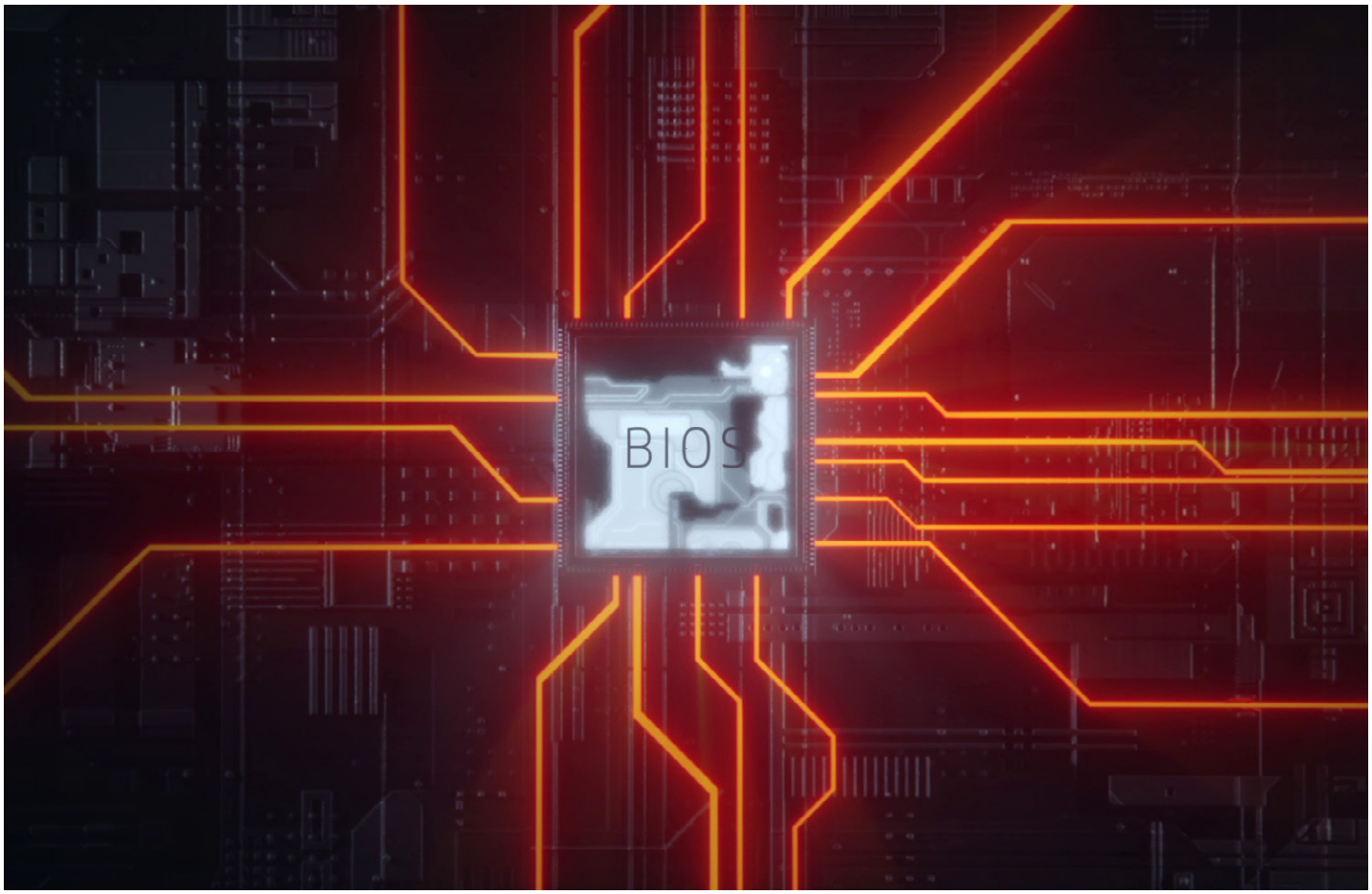
Miksi BIOS-suojaus on tärkeää?

Kun maailma muuttuu entistä yhdistyneemmäksi, kyberhyökkäykset kohdistuvat yhä useammin ja yhä edistyneemmin asiakaslaitteiden laiteohjelmistoihin ja laitteisiin. Laiteohjelmistoihin kohdistuvat hyökkäykset ovat olleet aiemmin teoreettinen konsepti, ja niiden on katsottu olevan vain kansallisvaltioiden käytettävissä. On kuitenkin käynyt ilmi, että tällaisia työkaluja ja tekniikoita käytetään ja niitä on saatavilla yleisesti.

Laiteohjelmisto (tai BIOS) on hyökkääjille houkutteleva kohde, koska onnistunut hyökkäys voi palkita hyökkääjän seuraavasti:

- Pysyvyys: Laiteohjelmisto sijaitsee piirilevyn säilyvässä muistissa, ja sitä ei voida poistaa yksinkertaisella kiintolevyn tyhjennyksellä.
- Kontrolli: Laiteohjelmiston suoritus tapahtuu korkeimmalla käyttöoikeustasolla käyttöjärjestelmän toimialueen ulkopuolella, mikä mahdollistaa käyttöjärjestelmästä riippumattoman haittaohjelman.
- Piilottaminen: Laiteohjelma sijaitsee muistialueella, jota käyttöjärjestelmä tai järjestelmäohjelmisto ei voi käsitellä, ja koska virustorjuntaohjelmisto ei voi skannata sitä, siinä sijaitsevaa haittaohjelmaa ei voida ehkä koskaan havaita.
- Palautumisen vaikeus: Kaikkien näiden tekijöiden vuoksi tämän tyypin tartunnasta palautuminen on vaikeaa ilman palvelua, joka sisältää emolevyn vaihtamisen.

Ihanteellinen ratkaisu laitteiden suojaamiseksi tällaista hyökkäystä vastaan on rakentaa laitteisto alusta asti käyttäen kyberkestävyyden periaatteita. Näiden periaatteiden avulla otetaan huomioon, että kaikkien mahdollisten hyökkäysten ennakointi on äärimmäisen vaikeaa, ellei mahdotonta. Ihanteellinen ratkaisu tarjoaa parannetun laiteohjelmiston suojan sekä laitteistopohjaisen tavan onnistuneen hyökkäyksen havainnointiin ja siitä palautumiseen.



HP Sure Start mahdollistaa loistavan laiteohjelmistosuojauksen

HP Sure Start on HP:n erityinen, mullistava lähestymistapa, joka mahdollistaa HP-tietokoneille edistyneen laiteohjelmiston suojan ja vastustuskyvyn. Siinä käytetään laitteistopohjaista tietoturvaa HP Endpoint Security Controller -ohjaimen (HP ESC) avulla, mikä suojaa BIOSin huomattavasti tehokkaammin kuin toimialan standardiratkaisut ja varmistaa, että järjestelmä käynnistää vain aidon HP:n BIOSin. Lisäksi, jos HP Sure Start havaitsee, että BIOSia, laiteohjelmistoa tai BIOSin järjestelmän hallintatilan (System Management Mode, SMM) koodia on peukaloitu, se voi palauttaa suojatun varmuuskopion.

HP Sure Startin ominaisuuksien yhteenveto

- HP:n ydinalustan laiteohjelmiston aitouden varmistaminen ja suojaaminen peukaloinnilta – HP Endpoint Security Controller -ohjainlaite varmistaa turvallisen käynnistyksen niin, että vain aito ja muokkaamaton HP-laiteohjelmisto ja HP:n BIOS voidaan ladata
- Laiteohjelmiston tilan seuranta ja vaatimustenmukaisuus – Laiteohjelmiston kuntoon liittyvien tapahtumien kirjaaminen lokiin eristetyllä HP Endpoint Security Controller -ohjaimella mahdollistaa laiteohjelmiston tilan ja estettyihin hyökkäyksiin viittaavien häiriöiden tarkastelun
- Itsepalautuva – HP:n BIOSin ja HP-laiteohjelmiston korruption automaattinen korjaus HP Endpoint Security Controller -ohjaimen eristetyillä HP-BIOSin ja HP-laiteohjelmiston varmuuskopioilla
- BIOS-asetusten suojaus – Tämä laajentaa HP Endpoint Security Controller -ohjaimen BIOS-koodin suojauksen koskemaan kaikkia käyttäjän tai järjestelmänvalvojan tekemiä BIOS-asetuksia HP ESC:in varmuuskopioiden ja eheystarkistusten avulla
- Käytön aikainen Runtime Intrusion Detection -havainnointi – Kriittisen BIOS-koodin suojaus käyttöjärjestelmän ollessa päällä (SMM)
- Käynnistysavainten suojaus – BIOSin käyttöjärjestelmän turvallista käynnistämistä varten tallentamien tietokantojen ja avainten huomattavasti parempi suojaus verrattuna toimialan standardimallisiin UEFI-tyyppisen BIOSin toimintoihin
- Suojattu tallennus – HP Sure Start käyttää vahvoja kryptografisia menetelmiä BIOS-asetusten, käyttäjätunnistetietojen ja muiden asetusten tallentamiseen HP Endpoint Security Controller -ohjaimessa, jotta varmistetaan eheyden suojaus, peukaloinnin havainnointi ja tietojen luottamuksellinen suojaus
- Intel® Management Engine -laiteohjelmiston suojaus – Parannettu Intel Management Engine -laiteohjelmiston suojaus ja palautus
- Hallittavuus – Järjestelmänvalvojat voivat hallita HP Sure Startin ominaisuuksia Microsoft® System Center Configuration Managerin (SCCM) Manageability Integration Kit (MIK) -laajennuksella

Katso sivulla 11 olevasta liitteestä A HP Sure Startin eri sukupolvien sisältämät ominaisuudet.

Kolmannen osapuolen tietoturvasertifikaatti

HP Sure Startin käyttämälle HP Endpoint Security Controller -laitteen tietoturva on kolmannen arvioima, ja se on saanut sertifikaatin, jonka mukaan laitteisto varmistaa kohdetietokoneella valtuutetun laiteohjelmiston käynnistyksen.[1]

Tietoturvaratkaisun oikean toiminnan varmistava sertifikaatti on kriittinen tietoturvatuotteen ostoratkaisua varten. Koska pelkkä hyvä maine ei riitä, HP on antanut itsenäisen ja valtuutetun laboratorion arvioitavaksi ja testattavaksi HP Endpoint Security Controller -ohjaimen sisäiset rakenteet, jotta sen kuvauksen mukainen toimivuus voitiin varmistaa julkisesti saatavilla olevilla kriteereillä, menetelmillä ja prosesseilla.

Kyberkestävä suunnittelu

HP Sure Start tarjoaa toimialan standardit ylittävän BIOS-suojauksen, ja se on suunniteltu aina laitteistosta alkaen tarjoamaan alustalle verraton kyberkestävyys, jolla varmistetaan BIOSin palautuminen myös tietomurron tai vahingollisen hyökkäyksen tapauksessa. HP Sure Startilla varustetut HP-yritystietokoneet ylittävät alustan laiteohjelmiston kestävyyden Draft National Institute of Standards

Technology (NIST) -ohjeet (Special Publication -julkaisu 800-193). Tämä on yksi johtavista julkisen sektorin menetelmistä kyberkestävyysalustojen vaatimusten muodollistamisessa.

HP Sure Startin tukemat mallit

HP lanseerasi Sure Startin vuonna 2014. Siitä lähtien HP on parantanut Sure Startia ja laajentanut sen tukemaa tuotevalikoimaa. HP Sure Start on tarjolla koko vuoden 2018 Elite-tuotevalikoimalle, johon kuuluu tabletteja, kannettavia, pöytäkoneita ja All-in-One-tuotteita (AIO). 4. sukupolven HP Sure Start on saatavilla HP Elite- ja HP Pro 600 -tuotteille, joissa on 8. sukupolven Intel- tai AMD®-suoritin.

Arkkitehtuurin yleiskatsaus ja ominaisuudet

HP Sure Startin arkkitehtuuri koostuu kahdesta pääosasta:

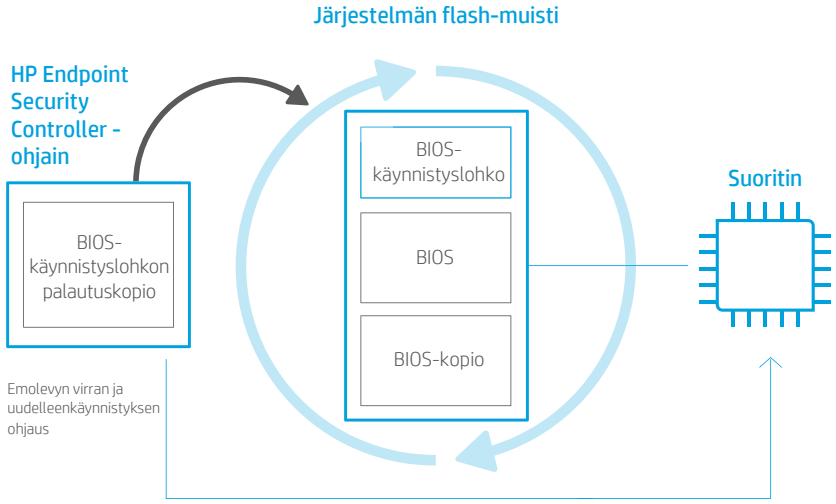
- **HP Endpoint Security Controller -ohjain** ja sen HP Sure Start -laiteohjelmisto
- **HP Sure Start BIOS**, joka toimii yhdessä HP Endpoint Security Controller -laitteen ja -laiteohjelmiston kanssa

Laiteohjelmiston eheyden varmistus – HP Sure Startin ydin

HP Endpoint Security Controller -ohjain (HP ESC) on ensimmäinen laite, joka suorittaa laiteohjelmiston tietokoneen käynnistymisen yhteydessä. Se on aktiivisena ennen kuin käyttöjärjestelmä käynnistetään. HP ESC:in toimintoihin kuuluvat muun muassa järjestelmän virtapainikkeen valvonta ja suorittimen virran kytkeminen, kun käyttäjä painaa virtapainiketta.

Kun alustalle annetaan virtaa (ennen järjestelmän käynnistämistä), HP ESC vahvistaa oman laiteohjelmistonsa HP-koodin aitouden ennen sen lataamista ja suorittamista. HP ESC käyttää toimialan standardien mukaisia vahvoja kryptografisia menetelmiä eheyden varmistamiseksi. Menetelmässä on käytössä 2 048 bitin julkinen HP RSA -avain, joka sijaitsee sisäisessä, pysyvässä vain luettavassa muistissa. HP ESC on siis rakennettu alustan laitteistopohjaiseksi luotettavuuden varmistavaksi järjestelmäksi (Root of Trust, RoT), jolla varmennetaan laiteohjelmisto ja HP:n BIOS ennen niiden suorittamista. Tämä laitteistopohjainen luotettavuuden varmistus suojaa alustaa laiteohjelmiston korvaavilta hyökkäyksiltä riippumatta niiden hyökkäysmenetelmästä, ja se toimii HP-alustan tietoturvan perustana.

Kuva 1. Laiteohjelmiston eheyden varmistusprosessi.



Kuvassa 1 on esitetty laiteohjelmiston eheyden varmistusprosessi. Kun HP ESC on vahvistanut HP Sure Start -laiteohjelmiston ja alkaa suorittamaan sitä, laiteohjelmisto käyttää vahvoja kryptografisia toimintoja järjestelmän flash-muistin BIOS-käynnistyslohkon eheyden varmistamiseksi. Jos yksikin bitti on virheellinen, HP ESC korvaa järjestelmän flash-muistin sisällön omalla HP:n BIOS-käynnistyslohkon kopiolla, joka sijaitsee HP ESC:ille tarkoitetussa säilyvässä muistissa (non-volatile memory, NVM).

HP Sure Startin suunnittelulla varmistetaan, että kaikki laiteohjelmisto- ja BIOS-koodi, jota suoritetaan HP ESC:illä ja suorittimella, on HP:n laitteelle suunnittelemaa koodia.

Huomautus: Järjestelmän käynnistyslohkon eheyden tarkistus, ja tarvittaessa HP ESC:in suorittama palauttaminen, tapahtuvat suorittimen ollessa pois päältä. Näin ollen käyttäjän näkökulmasta koko toiminto suoritetaan, kun järjestelmä on pois päältä tai valmius- tai lepotilassa.

Järjestelmän flash-muistin BIOS-käynnistyslohko on HP:n BIOSin perusta. HP ESC -laitteistolla varmistetaan, että BIOS-käynnistyslohko on ensimmäinen suorittimen ajama koodi uudelleenkäynnistyksen jälkeen. Kun HP ESC on määrittänyt, että BIOS-käynnistyslohko koostuu aidosta HP-koodista, se sallii tietokoneen normaalin käynnistyksen.

HP ESC tarkistaa järjestelmän flash-muistin käynnistyslohkon koodin myös joka kerta, kun järjestelmä sammutetaan tai kytketään valmius- tai lepotilaan. Koska suoritin näissä tiloissa on pois päältä ja sen täytyy suorittaa BIOS-käynnistyslohko uudelleen toiminnan jatkamiseksi, BIOS-käynnistyslohkon tarkistaminen joka kerta on erittäin tärkeää peukaloinnin havaitsemiseksi.

Lisäksi HP Intel -malleissa HP Sure Start tarkistaa säännöllisesti (15 minuutin välein) järjestelmän flash-muistin BIOS-käynnistyslohkon eheyden järjestelmän ollessa käytössä.[2]

Laitekohtaisten tietojen eheys

HP ESC ja BIOS toimivat yhdessä ja mahdollistavat jokaiselle koneelle tehtaalla määritettyjen, alustan käyttöiän ajaksi muuttumattomiksi suunniteltujen kriittisten muuttujien kehittyneen suojauksen. Tehtaalla HP ESC:in säilyvään muistiin tallennetaan varmuuskopio näistä muuttujatiedoista. Varmuuskopio on HP Sure Startin BIOS-komponentin käytettävissä vain luku -tilassa tietojen eheyden tarkistamista varten jokaisen käynnistyksen yhteydessä. Jos mikä tahansa jaettuun flash-muistiin tallennettu asetus on muuttunut tehdasasetuksista, HP Sure Startin BIOS-komponentit palauttavat järjestelmän flash-muistin tiedot HP ESC:in antaman varmuuskopion mukaisesti.

Kuvainalue

HP Sure Start suojaa HP Intel -mallien järjestelmän flash-muistin kuvainaluetta. Intel-arkkitehtuurin oma kuvainalue sisältää kriittisiä konfiguraation parametreja, jotka Intel Core™ -logiikka lukee uudelleenkäynnistyksen yhteydessä ja joita käytetään Core-logiikan konfigurointiin. Kuvainalue sisältää myös järjestelmän flash-muistin osiotiedot, joita Intel Core -logiikka käyttää määrittämään, missä flash-muistin kohdassa BIOS-alue on ja mistä suoritin noutaa uudelleenkäynnistyksen jälkeen suoritettavan koodin. HP Sure Start valvoo tämän alueen eheyttä ja palauttaa sen asianmukaisen konfiguraation, jos tapahtuu peukalointia tai korruptiota.

Verkko-ohjaimen suojaus

Lisäksi HP Intel -malleilla HP Sure Start suojaa verkko-ohjaimen (NIC) asetukset, jotka sijaitsevat järjestelmän flash-muistissa. Joidenkin HP-asiakkaiden käyttötapaukset vaativat muutoksia verkko-ohjaimen tehdasasetuksiin. Siksi HP Sure Start ei oletuksena estä verkko-ohjaimen asetusten muutoksia. Sen sijaan HP Sure Start sisältää ominaisuuden, joka käytössä ollessaan varoittaa käyttäjää muuttuneista verkko-ohjaimen asetuksista. Lisäksi HP Sure Start tarjoaa menetelmän verkko-ohjaimen asetusten palauttamiseksi tehdasarvoihin. Suojattuihin asetuksiin kuuluvat MAC-osoite, käyttöjärjestelmän käynnistystä edeltävän suoritusympäristön (PXE) asetukset ja Remote Initial Program Load -toiminto (RPL). Tämä palauttaminen on mahdollista HP ESC:in suojaaman, vain luettavan varmuuskopion ansiosta.

BIOS-asetusten suojaus

Kuten aiemmin kuvailtiin, HP Sure Start varmistaa HP:n BIOS-koodin eheyden ja aitouden. Koska tämä koodi ei muutu sen jälkeen, kun HP on luonut sen, koodin eheyden ja aitouden varmistamiseksi voidaan käyttää digitaalisia allekirjoituksia. BIOS-asetusten dynaaminen ja käyttäjämuokkausten mahdollistava toiminta kuitenkin luo lisähaasteita asetusten suojaukseen. HP ei voi luoda näiden asetusten varmistamista varten digitaalisia allekirjoituksia käytettäväksi HP Sure Start ESC:issä.

HP Sure Startin BIOS-asetusten suojaus mahdollistaa järjestelmän määrittämisen niin, että HP ESC -laitteistoa käytetään kaikkien käyttäjän haluamien BIOS-asetusten varmuuskopiointiin ja eheyden tarkistamiseen.

Kun tämä ominaisuus on käytössä alustalla, kaikki BIOSin käyttämät käytäntöjen asetukset varmuuskopioidaan ja niiden eheys tarkistetaan jokaisen käynnistyksen yhteydessä sen varmistamiseksi, että BIOSin käytäntöjen asetuksia ei ole muutettu. Jos havaitaan muutos, järjestelmä käyttää HP Sure Startin suojatun tallennustilan varmuuskopiota käyttäjän määrittämän asetuksen automaattiseen palautukseen.

HP Sure Startin BIOS-asetusten suojausominaisuus ilmoittaa tapahtumista HP Sure Start ESC -laitteistolle, kun havaitaan yritys muuttaa BIOS-asetuksia. Tapahtuma kirjataan HP Sure Startin auditointilokiin, ja käyttäjä saa BIOSilta ilmoituksen käynnistyksen yhteydessä.

HP Sure Startin suojattu tallennus

HP ESC -ohjainlaitteen suojattu tallennus mahdollistaa HP Sure Startin suojaamien BIOS-/laiteohjelmistotietojen ja -asetusten korkeimman suojaustason. HP Sure Startin suojattu tallennus on suunniteltu mahdollistamaan luottamuksellisuus, eheys ja peukaloinnin havainnointi jopa fyysisen hyökkäyksen tapauksessa, jossa hyökkääjä purkaa järjestelmän ja luo suoran yhteyden laitteen piirilevyn säilyvään muistiin.

Tietojen eheys

Laiteohjelmiston säilyvässä muistissa säilyttämien ja erinäisten ominaisuuksien tilojen ohjaukseen käytettävien tietojen eheys on kriittistä alustan tietoturvalle. Dynaamisiin tietoihin kuuluvat BIOS-asetukset, joita laitteen loppukäyttäjä tai järjestelmänvalvoja voivat muokata. Esimerkkejä ovat muun muassa käynnistysasetukset, kuten Secure Boot -ominaisuus, BIOSin järjestelmänvalvojan salasana ja siihen liittyvät käytännöt, Trusted Platform -moduulin tilan ohjaus sekä HP Sure Startin käytäntöasetukset.

Näiden asetusten valtuuttamattomien muutosten estävät olemassa olevat käyttörajoitukset ohittava hyökkäys voisi päihittää alustan tietoturvan. Ajatellaan esimerkkinä tilannetta, jossa hyökkääjä tekee valtuuttamattoman muutoksen Secure Boot -ominaisuuteen ilman, että tätä havaitaan. Tässä tilanteessa alusta käynnistäisi ennen käyttöjärjestelmää hyökkääjän root kit -haittaohjelman ilman, että käyttäjä huomaisi sitä.

Toimialan standardina toimivaan UEFI-tyyppiseen BIOSiin kuuluu käyttörajoituksia, joiden tarkoituksena on estää näiden muuttujien valtuuttamaton muuttaminen. HP on ottanut ne käyttöön PC-alan muiden toimijoiden tavoin.

Mutta koska hyökkäykset näitä mekanismeja kohtaan muodostavat alustalle merkittävän riskin, HP Sure Start sisältää lisäsuojauksia, jotka ylittävät toimialan standarditason.

BIOS-asetukset ja muut dynaamiset tiedot, joita laiteohjelmisto käyttää HP Sure Startin suojaaman tilan ohjaukseen, on tallennettu HP ESC -ohjainlaitteen eristettyyn säilyvään muistiin, jota suorittimella toimivat ohjelmat eivät voi suoraan käyttää.

Lisäksi HP ESC luo ja päivittää yksilöllisiä eheysmittauksia joka kerta, kun tähän säilyvään muistiin tallennetaan tietoelementti. Eheysmittaukset perustuvat vahvaan kryptografiseen algoritmiin (SHA-256-hajautukseen pohjautuva viestin todennuskoodi), joka perustuu HP ESC:issä sijaitsevaan salaiseen tietoon. Salainen tieto on yksilöllinen jokaiselle HP ESC:ille, eli jokainen ohjain luo identtisessä ympäristössä yksilöllisen eheysmittauksen.

Kun tietoelementti luetaan takaisin säilyvästä muistista, HP ESC laskee tietoelementin eheysmittauksen uudelleen ja vertaa sitä tietoon liitettyyn eheysmittaukseen. Säilyvän muistin tietojen valtuuttamattomien muutosten seurauksena vertailu havaitsee eroavuuden. Tällä menetelmällä HP ESC voi havaita säilyvään muistiin tallennettujen tietoelementtien peukaloinnin.

Tietojen luottamuksellisuus

Luottamuksellisuuden säilyttäminen on kriittistä useille alustan tallentamille tietoelementeille. Esimerkkejä ovat BIOSin järjestelmänvalvojan salasanan hajautukset, käyttäjien tunnistetiedot ja salaiset tiedot, joita laiteohjelmisto valinnaisesti tallentaa käyttäjän puolesta laiteohjelmapohjaisia toimintoja, kuten HP Sure Runia ja HP Sure Recoveryä, varten.

Näiden salaisten tietojen suojaus on haastavaa toimialan standardimallisella UEFI-tyyppisellä BIOSilla, sillä säilyvä muisti on tyypillisesti suorittimella ajettavien ohjelmien luettavissa. HP Sure Startin suojattu tallennus on suunniteltu suojaamaan näitä luottamuksellisia tietoa paremmin kuin vakiomallinen UEFI-tyyppinen BIOS.

Eristetyn tallennuksen lisäksi HP Sure Start käyttää AES-laitteistolohkoa (Advanced Encryption Standard) HP ESC:in AES-256-salauksen suorittamiseksi kaikille HP Sure Startin säilyvässä muistissa tallennetuille luottamuksellisille tiedoille näiden elementtien tietojen eheysmittauksen ohella. Käytettävä salausavain on yksilöllinen jokaiselle HP ESC:ille eikä se poistu koskaan ESC-ohjaimesta, joten yksittäisen HP ESC:in salaamien tietojen salauksen voi purkaa vain sama HP ESC.

Käynnistysavainten suojaus

HP Sure Start mahdollistaa laiteohjelmiston tallentamien UEFIn suojattujen käynnistysavainten tietokantojen tehokkaamman suojauksen verrattuna toimialan standardin mukaiseen suojattuun UEFI-käynnistykseen. Nämä muuttujat ovat kriittisiä UEFIn suojatun käynnistyksen ominaisuudelle, joka varmistaa käyttöjärjestelmän käynnistysohjelman eheyden ja aitouden ennen käyttöjärjestelmän käynnistämisen sallimista.

HP Sure Start suojaa UEFIn käynnistysavainten tietokannat säilyttämällä niistä varmennetun kappaleen HP Sure Startin suojatussa tallennuksessa. HP Sure Start havaitsee käyttöjärjestelmän tekemät valtuutetut muutokset UEFIn käynnistysavainten tietokantaan, ja HP ESC tallentaa nämä muutokset varmennettuun kappaleeseen. HP Sure Start käyttää sitten HP Sure Startin suojatussa tallennuksessa sijaitsevaa varmennettua kappaletta UEFIn käynnistysavainten tietokantojen valtuuttamattomien muutosten havaitsemiseksi ja estämiseksi.

Tämä oletuksena käytössä oleva ominaisuus kattaa seuraavat tietokannat:

- Allekirjoitustietokanta (db)
- Hylättyjen allekirjoitusten tietokanta (dbx)
- Key Enrollment Key -avain (KEK)
- Platform Key -avain (PEK), jota käyttöjärjestelmä päivittää dynaamisesti käytön aikana

Käytön aikainen Runtime Intrusion Detection -havainnointi (RTID)

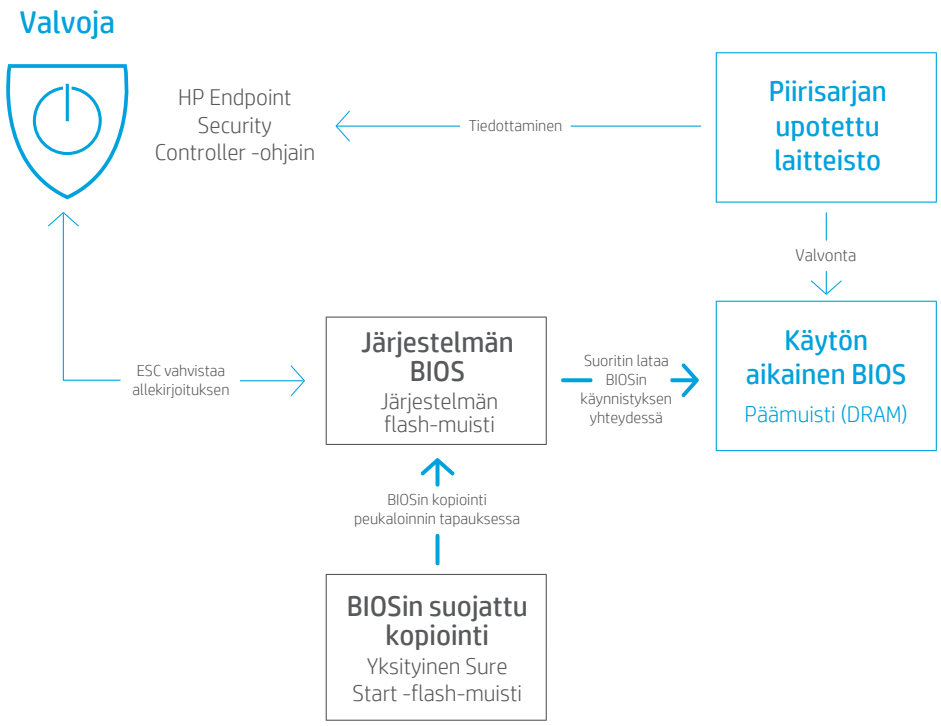
BIOS-koodin suoritus alkaa jokaisen käynnistyksen yhteydessä kiinteästä osoitteesta. Tämä BIOS-käynnistyskoodi mahdollistaa ennen käyttöjärjestelmän käynnistystä vaadittavat toimenpiteet. Siksi DRAMissa säilytetään BIOSin osa, jota tarvitaan kehittyneitä virranhallintatoimintoja, käyttöjärjestelmän palveluita ja muita käyttöjärjestelmästä riippumattomia toimintoja varten käyttöjärjestelmän ollessa päällä. Tämä BIOS-koodi, jota kutsutaan System Management Mode (SMM) -koodiksi, sijaitsee käyttöjärjestelmältä piilotetulla erityisellä DRAMin alueella. Tätä koodia kutsutaan myös "Runtime"-BIOS-koodiksi HP Sure Startin käytön aikaisen havainnoinnin (RTID) ominaisuuden kontekstissa. (Katso lisätietoja SMM:stä ja sen toiminnasta liitteestä B sivulla 12).

SMM-koodin eheys on kriittistä asiakaslaitteen tietoturvalle. HP Sure Start tarkistaa käyttöjärjestelmän käynnistyksen yhteydessä HP SMM BIOS -koodin eheyden. Käytön aikainen tunkeutumisen havainnointi sisältää mekanismeja, jotka varmistavat SMM:n BIOS-koodin eheyden käyttöjärjestelmän ollessa päällä lisäämällä uusia suojausominaisuuksia ja/tai menetelmän koodiin kohdistuvien hyökkäysten havaitsemiseksi.

Käytön aikaisen tunkeutumisen havainnoinnin arkkitehtuuri

RTID-ominaisuus käyttää alustan piirisarjan erityislaitteistoa käytön aikaisen HP SMM BIOSin häiriöiden havaitsemiksi. Jos havaitaan häiriöitä, ilmoitus annetaan HP Endpoint Security Controller -ohjaimelle, joka voi suorittaa käytännön mukaiset toimet suorittimesta riippumattomasti.

Kuva 2. Käytön aikainen tunkeutumisen havainnointi käyttää alustan piirisarjan erityislaitteistoa SMM-koodin muutosten havaitsemiseksi.



Käyttäjäilmoitukset, tapahtumien kirjaus lokiin ja käytäntöjen hallinta

Loppukäyttäjän HP Sure Start -ilmoitukset

HP Sure Start on normaalisti käyttäjälle näkymätön. Kun HP Sure Start havaitsee ongelman, palautustoiminnot ovat oletusasetuksilla automaattisia, eivätkä ne yleensä vaadi loppukäyttäjän tai IT-osaston toimia.

Käyttäjille saatetaan antaa käytön aikaisia ilmoituksia, jos HP Sure Startin dynaaminen suojaus tai käytön aikainen tunkeutumisen havaintotoiminto huomaa BIOSin eheyden ongelman käyttöjärjestelmän ollessa päällä. Jos havaitaan merkittävä tapahtuma tai ryhdytään toimiin, HP Sure Start antaa Windowsin® ilmoitusten kautta varoituksen seuraavan käynnistyksen aikana. HP Notifications-ohjelmisto tarvitaan näiden Windows-ilmoitusten näkemiseen.

Tapahtumien kirjaus lokiin HP Sure Startilla

HP Endpoint Security Controller -ohjain tallentaa HP Sure Startin valvoman laiteohjelmiston/BIOSin koodiin ja tietoihin liittyvät kriittiset tapahtumat. Nämä tapahtumat tallennetaan Sure Startin säilyvään tallennukseen. Nämä tapahtumat kopioidaan HP ESC:istä Windowsin Tapahtumienvalvontaan, kun tapahtumien lukemisen mahdollistava HP Notifications -ohjelmisto on asennettuna käyttäjän tai tämän hallinta-agentin toimesta.

Seuraavien tapahtumien seurauksena HP Notifications -ohjelmisto lukee kaikki HP Sure Start -alijärjestelmän tapahtumat ja varmistaa, että Windowsin Tapahtumienhallintaan lisätään kaikki tapahtumat, joita ei ole vielä tallennettu siihen:

- Windowsin käynnistys
- Windowsin palauttaminen valmius-/lepotilasta
- HP Sure Startin dynaamiset käytön aikaiset ilmoitukset
- HP Sure Startin käytön aikainen tunkeutumisen havaitseminen (Runtime Intrusion Detection, RTID)

HP Notifications -ohjelmisto tallentaa HP Sure Start -tapahtumat erityiseen "HP Sure Start" -sovellustapahtumalokiin. Tähän lokiin sisällytetään vain HP Sure Start -tapahtumat. Windowsin Tapahtumienvalvonnan polku HP Sure Start -tapahtumiin on seuraava: Järjestelmätyökalut/Tapahtumienvalvonta/Sovellus- ja palvelulokit/HP Sure Start.

Windowsin Tapahtumienvalvonnan HP Sure Startiin liittyvät ilmoitustasot on määritelty jäljempänä olevassa taulukossa.

Tapahtumat lisätään Windowsin Tapahtumienvalvontaan siinä järjestyksessä, missä HP Sure Start on luonut ne. HP Sure Start -alijärjestelmän vanhin tapahtuma lisätään Windowsin Tapahtumienvalvontaan ensin ja uusin tapahtuma viimeiseksi.

Windowsin Tapahtumienvalvonnan tapahtumien aikaleimat näyttävät ajan, jolloin tapahtuma on lisätty lokiin EIVÄTKÄ tapahtumisaikaa. Jokainen Windowsin Tapahtumienvalvonnan Sure Start -tapahtuma sisältää yksityiskohtaisia tietoja, kuten varsinaisen tapahtumisajan aikaleiman.

Huomautus: Tapahtumat säilyvät HP Endpoint Security Controller -ohjaimessa senkin jälkeen, kun ne on kopioitu Windowsin Tapahtumienvalvontaan. Jos Windowsin Tapahtumienvalvonta tyhjennetään, HP Notifications -ohjelmisto lisää kaikki HP Sure Start -tapahtumat uudelleen seuraavan kerran, kun jokin tapahtuma laukaisee HP Sure Start -tapahtumalokin tarkistamisen.

HP Sure Startin Windowsin Tapahtumienvalvonnan tapahtumatyypit

Tapahtuman taso	Määritelmä
Tieto	Tapahtumat, joita odotetaan normaalissa käytössä (esim. BIOSin päivittäminen).
Varoitus	Odottamattomat tapahtumat, joista HP Sure Start on palautunut täysin ja joiden tapauksessa alustan täyttä toimintakykyä varten ei vaadita käyttäjän/järjestelmänvalvojan toimia. Nämä tapahtumat ovat epätavallisia toimintoja, joita käyttäjän/järjestelmänvalvojan voi olla syytä tutkia tarkemmin, erityisesti, jos näitä tapahtumia tuntuu esiintyvän useilla tietokoneilla.
Virhe	Tapahtumat, jotka vaativat järjestelmänvalvojan/HP-tuen toimia alustan täyttä palautusta varten.

HP Sure Startin käytäntöjen ohjaus

HP:n järjestelmä-BIOS on heti käyttövalmiina HP Sure Start -käytäntöjen käyttöönottoa ja optimointia varten peruskäyttäjälle. Koska HP Sure Start on oletuksena käytössä, tyypillisen käyttäjän ei tarvitse muokata HP Sure Startin asetuksien suojausta. Järjestelmän BIOS tarjoaa edistyneelle käyttäjälle joitain tapoja ohjata HP Sure Startin toimintaa BIOSin käytäntöasetusruudulla (F10). Jos muuta ei ilmoiteta, nämä asetukset ja toiminnot sijaitsevat valikossa Security/BIOS Sure Start.

Huomautus: Käytännöt tallennetaan HP ESC:in säilyvään muistiin, jota suoritin ei voi suoraan käsitellä. Siksi Sure Start -asetusten voimaan tulemiseksi vaaditaan tietokoneen uudelleenkäynnistys.

Käytettävissä on seuraavat HP Sure Start -asetukset ja -toiminnot:

- Käynnistyslohkon varmistaminen jokaisen käynnistyksen yhteydessä
- BIOS-tietojen palautuskäytäntö
- Verkko-ohjaimen konfiguraation palautus (vain Intel)
- Ilmoitus verkko-ohjaimen konfiguraation muutoksesta (vain Intel)
- Käynnistyslohkon dynaaminen skannaus käytön aikana (vain Intel)
- HP Sure Start BIOSin asetusten suojaus
- Käynnistysavainten HP Sure Start -suojaus
- Kehittynyt HP-laiteohjelmiston käytön aikainen tunkeutumisen estäminen ja havainnointi (vain Intel)
- HP-laiteohjelmiston käytön aikainen tunkeutumisen havainnointi (vain AMD)
- HP Sure Start -tietoturvatapahtumien käytäntö
- HP Sure Start -tietoturvatapahtumien ilmoittaminen käynnistyksen yhteydessä
- BIOS-version lukitus
- Järjestelmäkiintolevyn MBR:n tallennus/palautus
- Järjestelmäkiintolevyn GPT:n tallennus/palautus
- Käynnistyssektorin (MBR/GPT) palautuskäytäntö

Käynnistyslohkon varmistaminen jokaisen käynnistyksen yhteydessä (Verify Boot Block on Every Boot)

HP Sure Start varmistaa aina BIOSin käynnistyslohkon eheyden, kun tietokone käynnistetään tai palautetaan valmius- tai lepotilasta. Kun käytössä on valinta **enable**, HP Sure Start varmistaa käynnistyslohkon eheyden myös jokaisen lämminkäynnistyksen (Windowsin uudelleenkäynnistyksen) yhteydessä. Tämä valinta parantaa tietoturvaa, mutta hidastaa käynnistystä. Tämän ominaisuuden oletusasetus on **disable**.

BIOS-tietojen palautuskäytäntö (BIOS Data Recovery Policy)

Kun käytössä on valinta **Automatic**, HP Sure Start korjaa tarvittaessa automaattisesti BIOSin tai tietokonekohtaiset tiedot. Kun käytössä on valinta **Manual**, HP Sure Start vaatii erityisen näppäinyhdistelmän korjausten aloittamiseksi. Jos käynnistyslohkon koodissa on ongelma, järjestelmä ei suostu käynnistymään ja järjestelmän LED-valo vilkkuu erityisellä tavalla. Jos tietokonekohtaisissa tiedoissa on ongelma, järjestelmä näyttää ruudulla viestin. Vaadittu näppäinyhdistelmä ja LED-valon vilkkumisen tapa vaihtelevat riippuen siitä, onko järjestelmä kannettava, työpöytäkone vai tabletti. Manual-tila on hyödyllinen käyttäjille, jotka voivat tutkia järjestelmän flash-muistin sisältöä ennen korjausta. Tyypillisille käyttäjille ei suositella Manual-tilaa. Tämän ominaisuuden oletusasetus on **Automatic**.

Verkko-ohjaimen konfiguraation palautus (Network Controller Configuration Restore) (vain Intel)

Tämä toiminto on käytettävissä vain Intel-järjestelmissä. Kun tämä on valittuna, HP Sure Start palauttaa välittömästi verkko-ohjaimen konfiguraation tehdasasetuksiin.

Ilmoitus verkko-ohjaimen konfiguraation muutoksesta (Prompt on Network Controller Configuration Change) (vain Intel)

Tämä asetus on käytettävissä vain Intel-järjestelmissä. HP tarjoaa tehtaalla määritetyn verkko-ohjaimen konfiguraation, johon kuuluu MAC-osoite. Kun käytössä on valinta **enable**, järjestelmä valvoo verkko-ohjaimen konfiguraation tilaa ja ilmoittaa käyttäjälle, jos tehdasasetuksiin on tehty muutos. Tämän ominaisuuden oletusasetus on **disable**.

Käynnistyslohkon dynaaminen skannaus käytön aikana (Dynamic Runtime Scanning of Boot Block) (vain Intel)

Tämä asetus on käytettävissä vain Intel-järjestelmissä. Kun käytössä on oletusasetus **enable**, HP Sure Start tarkistaa säännöllisesti BIOS-käynnistyslohkon eheyden käyttöjärjestelmän ollessa päällä. Kun käytössä on asetus **disable**, HP Sure Start tarkistaa eheyden vain ennen käynnistystä tai palautumista valmius- tai lepotilasta.

BIOS-asetusten suojaus (HP Sure Start BIOS Setting Protection)

BIOS-asetusten suojauskäytännön oletusasetus on **disable**. Tämän ominaisuuden käyttöönottamista varten asiakaslaitteen omistajan/järjestelmänvalvojan tulee ensin määrittää kaikki BIOS-käytännöt haluamikseen. Omistajan/järjestelmänvalvojan tarvitsee myös määrittää BIOSin järjestelmänvalvojan salasana HP Sure Startin BIOS-asetusten suojauksen käyttämiseksi.

Kun tämä on valmis, BIOS-asetusten suojauskäytännön pitäisi vaihtua tilaan "enable". Tässä vaiheessa luodaan varmuuskopio kaikista BIOS-asetuksista HP Sure Startin suojattuun tallennukseen. Tästä eteenpäin mitään näistä BIOS-asetuksista ei voida muokata paikallisesti tai etänä. Jokaisen käynnistyksen yhteydessä varmistetaan, että BIOS-käytäntöasetukset ovat halutussa tilassa. Jos näissä esiintyy poikkeama, BIOS-asetukset palautetaan HP Sure Startin suojatusta tallennuksesta.

BIOS-asetusten muokkaamiseksi täytyy syöttää BIOSin järjestelmänvalvojan salasana ja BIOS-asetusten suojaus tulee poistaa käytöstä. Tämän jälkeen BIOS-asetuksia voi muuttaa.

Käynnistysavainten HP Sure Start -suojaus (Secure Boot Keys Protection)

Tämän asetuksen tehdasarvo on **enable**, jolloin HP Sure Start mahdollistaa BIOSin käyttämien turvattujen käynnistystietokantojen ja -avainten parannetun suojauksen ja käyttöjärjestelmän käynnistysohjelman aitouden tarkistamisen ennen kuin se käynnistyy. Kun asetukselle annetaan arvo **disable**, käytössä on vain vakiomallinen suojattu UEFI-käynnistys, eikä HP Sure Start -alijärjestelmä säilytä varmuuskopiota.

Kehittynyt HP-laiteohjelmiston käytön aikainen tunkeutumisen estäminen ja havainnointi (Enhanced HP Firmware Runtime Intrusion Prevention and Detection) (vain Intel) sekä HP-laiteohjelmiston käytön aikainen tunkeutumisen havainnointi (HP Firmware Runtime Intrusion Detection) (vain AMD)

Käytön aikaisen RTID-suojausominaisuuden tehdasasetus on **enable** kaikilla HP:n toimittamilla alustoilla. Loppukäyttäjän/järjestelmänvalvojan ei tarvitse kytkeä tätä ominaisuutta päälle tai ottaa sitä käyttöön HP Sure Start RTID:n käyttöä varten.

Alustan omistaja/järjestelmänvalvoja voi asettaa RTID-ominaisuudelle valinnaisesti asetuksen **disable**.

HP Sure Start -tietoturvatapahtumien käytäntö (HP Sure Start Security Event Policy)

Tämä BIOS-käytäntö määrittää, mihin toimiin ryhdytään, kun HP Sure Start havaitsee hyökkäyksen tai sen yrityksen käyttöjärjestelmän ollessa päällä. Tälle käytännölle on kolme asetusvaihtoehtoa:

- **Vain tapahtuman kirjaus (Log event only)**: Kun tämä asetus on valittuna, HP ESC kirjaa havaintotapahtumat lokiin, jota voidaan tarkastella Windowsin Tapahtumienhallinnan polulla Sovellus- ja palvelulokit/HP Sure Start.[3]
- **Tapahtuman kirjaus ja ilmoitus käyttäjälle (Log event and notify user)**: Tämä on oletusasetus. Kun tämä asetus on valittuna, HP ESC kirjaa havaintotapahtumat lokiin, jota voidaan tarkastella Windowsin Tapahtumienhallinnan polulla Sovellus- ja palvelulokit/HP Sure Start. Lisäksi käyttäjä saa Windowsissa ilmoituksen tapahtumasta.[4]
- **Tapahtuman kirjaus ja järjestelmän sammutus (Log event and power off system)**: Kun tämä asetus on valittuna, HP ESC kirjaa havaintotapahtumat lokiin, jota voidaan tarkastella Windowsin Tapahtumienhallinnan polulla Sovellus- ja palvelulokit/HP Sure Start. Lisäksi käyttäjä saa Windowsissa ilmoituksen tapahtumasta ja siitä, että järjestelmä sammutetaan pian.

HP Sure Start -tietoturvatapahtumien ilmoittaminen käynnistyksen yhteydessä (HP Sure Start Security Event Boot Notification)

Tämä BIOS-käytäntö määrittää, täytyykö käyttäjän hyväksyä HP Sure Startin järjestelmän käynnistyksen aikana antamat varoitukset ja virheviestit ennen kuin käynnistystä voidaan jatkaa. Oletusasetuksella **Require Acknowledgement** (hyväksyntä vaaditaan) järjestelmä pysähtyy virheviestin näyttämisen ajaksi. Paikallisen käyttäjän täytyy painaa jotain painiketta käynnistyksen jatkamiseksi. Jos asetukseksi vaihdetaan **Time out after 15 seconds** (aikakatkaisu 15 sekunnin jälkeen), käynnistys jatkuu automaattisesti, kun viesti on näkynyt ruudulla 15 sekunnin ajan.

BIOS-version lukitus (Lock BIOS Version)

Tämä asetus sijaitsee BIOS-valikon (F10) kohdassa Main/Update System BIOS.

Kun käytössä on asetus **disable**, BIOS voidaan päivittää tuetuilla prosesseilla. Kun HP ESC havaitsee järjestelmä flash-muistissa kelvollisen käynnistyslohkon päivityksen, se päivittää käynnistyslohkon varmuuskopion.

Kun käytössä on asetus **enable**, mikään HP:n BIOS-päivitystyökalu ei pysty päivittämään BIOSia. Lisäksi HP Sure Start suojaa BIOS-versiota muutoksilta estämällä valtuuttamattomia menetelmiä poistamasta järjestelmän flash-muistia. HP ESC tallentaa BIOSin lukitun version. Kun HP ESC havaitsee järjestelmän flash-muistin sisältämän BIOSin muutoksen, HP ESC kirjoittaa BIOS-käynnistyslohkon päälle HP ESC:in version käynnistyslohkosta. HP ESC:in versio käynnistyslohkosta suoritetaan ja BIOSin oikea versio palautetaan. Tämän ominaisuuden oletusasetus on **disable**.

Järjestelmäkiintolevyn MBR:n tallennus/palautus (Save/Restore MBR of System Hard Drive) ja Järjestelmäkiintolevyn GPT:n tallennus/palautus (Save/Restore GPT of System Hard Drive)

Tämä asetus sijaitsee BIOS-valikon (F10) kohdassa Security/Hard Drive Utilities. Riippuen HP Sure Startin havaitseman ensisijaisen levyn osiointityypistä (GPT tai MBR), vain toinen näistä ominaisuuksista on tarjolla.

Kun käytössä on asetus **enable**, HP Sure Start säilyttää suojatun varmuuskopion ensisijaisen aseman MBR-/GPT-osiotaulukosta ja vertaa varmuuskopiota levyn osiotaulukkoon jokaisen käynnistyksen yhteydessä. Jos havaitaan eroavuus, käyttäjää pyydetään valitsemaan osiotaulukon palauttaminen varmuuskopiosta tai varmuuskopion päivittäminen muutosten mukaisesti. **Käynnistyssektorin (MBR/GPT) palautuskäytäntöä** voidaan valinnaisesti käyttää poistamaan käyttäjän valinta suoritettavalle toimenpiteelle, kun HP Sure Start havaitsee poikkeavuuden.

Kun käytössä on oletusasetus **disable** HP Sure Start ei tarjoa MBR-/GPT-suojausta.

Käynnistyssektorin (MBR/GPT) palautuskäytäntö (Boot Sector (MBR/GPT) Recovery Policy)

Kun käytössä on oletusasetus **Local User Control** (paikallisen käyttäjän ohjaama), käyttäjää pyydetään valitsemaan toimenpide, kun HP Sure Start havaitsee MBR-/GPT-osiotaulukon muutoksen. Kun käytössä on asetus **Recover in the event of corruption (palauttaminen korruption tapauksessa)**, HP Sure Start palauttaa MBR:n/GPT:n automaattisesti tallennettuun tilaan aina, kun havaitaan eroavuus.

HP Sure Startin käytäntöohjauksen etähallinta

HP Sure Startin käytännöt on oletuksena optimoitu tyypilliselle käyttäjälle. Koska HP Sure Start on oletuksena käytössä, etäjärjestelmänvalvojan ei tarvitse ryhtyä toimiin HP Sure Startin ottamiseksi käyttöön. Jos etäjärjestelmänvalvoja haluaa muokata HP Sure Startin käytäntöasetuksia, hän voi käyttää siihen samoja Windows Management Instrumentation (WMI) -rajapintoja ja HP BIOS Configuration Utilityn komentosarjoja kuin joita käytetään muiden alustan BIOS-käytäntöjen hallintaan. Lisäksi järjestelmänvalvojat voivat hallita HP Sure Startin ominaisuuksia Microsoft System Center Configuration Managerin (SCCM) Manageability Integration Kit (MIK) -laajennuksella.

Lisäksi järjestelmänvalvojat voivat hallita HP Sure Startin ominaisuuksia ja tarkastella sen ilmoituksia Microsoft System Center Configuration Managerin (SCCM) Manageability Integration Kit (MIK) -laajennuksella.

Johtopäätös

HP Sure Start tarjoaa nämä merkittävät hyödyt:

- **Keskeytyksetön tuottavuus** – HP Sure Start varmistaa liiketoiminnan jatkuvuuden hyökkäyksen tai vahingossa tapahtuvan korruption tapauksessa poistamalla tarpeen odottaa IT-osaston palvelua.
- **Kustannussäästöt** – HP Sure Startin automaattinen palautuminen vähentää IT-osaston palveluiden tarvetta ja parantaa tuottavuutta, mikä alentaa alustan huoltokustannuksia.
- **Mielenrauha** – HP Sure Start sisältää useita tietoturvaominaisuuksia, jotka kattavat useita ohjelmisto- ja laitteistoalustoja.

HP Sure Start mahdollistaa kriittisen BIOS-laiteohjelmiston suojaamisen haittaohjelmilta alan johtavalla laiteohjelmistohyökkäyksen havainnoinnilla ja automaattisella korjauksella. Nämä ominaisuudet ovat saatavilla valikoiduille HP Elite -tietokoneille.

Liite A – HP Sure Startin sukupolvet

HP lanseerasi Sure Startin vuonna 2014. HP on sen jälkeen parantanut Sure Startia ja laajentanut sen tukemaa laitevalikoimaa. Jäljempänä olevassa taulukossa on yhteenveto eri sukupolvien yhteydessä lisätyistä ominaisuuksista.

Sukupolvi	Julkaisuaika	Lisätyt ominaisuudet
HP Sure Start	2014	• Laiteohjelmiston ja BIOSin aitouden valvonta ja itsepalautuva korjaus • Laiteohjelmiston valvonta ja vaatimustenmukaisuus
HP Sure Start with Dynamic Protection	2015	• Windowsin Tapahtumienhallinnan tuki • Dynaaminen suojaus (valikoidut Intel-tuotteet)
HP Sure Start Gen3 (valikoidut Intel-tuotteet)[5] HP Sure Start with Runtime Intrusion Detection (valikoidut AMD-tuotteet)[6]	2017	• Käytön aikainen tunkeutumisen havaitseminen • BIOS-asetusten suojaus • Microsoft SCCM:n Manageability Integration Kit (MIK) -laajennus
HP Sure Start Gen4[7]	2018	• Suojattu tallennus – vahvat kryptografiset menetelmät BIOS-asetusten, käyttäjien tunnistetietojen ja muiden asetusten tallentamiseen HP Endpoint Security Controller -ohjainlaitteessa eheyden suojaamista, peukaloinnin havaitsemista ja tietojen luottamuksellista suojausta varten • Käynnistystietokannan suojaaminen – vakiomallista UEFI-suojausta tehokkaampi BIOSin tallentamien tietokantojen ja avainten suojaus käyttöjärjestelmän turvallista käynnistystä varten • Intel-alustoilla Intel Management Engine -laiteohjelmiston parannettu suojaus ja palautus • HP Endpoint Security Controller -ohjaimella on kolmannen osapuolen tietoturvasertifikaatti – itsenäisen ja valtuutetun laboratorion vahvistus julkisesti saatavilla kriteereillä, menetelmillä ja prosesseilla siitä, että HP ESC:in ydintoiminnot toimivat kuvatulla tavalla[1] • HP Sure Startilla varustetut HP-yritystietokoneet ylittävät NIST Platform Firmware Resiliency -ohjeiden vaatimukset (Special Publication -julkaisu 800-193)

Liite B – System Management Mode -hallintatilan (SMM) yleiskatsaus

System Management Mode -hallintatila (SMM) on alan vakiomenetelmä, jolla ohjataan tietokoneiden virranhallintaominaisuuksia ja muita käyttöjärjestelmästä itsenäisiä ominaisuuksia käyttöjärjestelmän ollessa päällä. SMM-termi ja sen käyttöönotto koskevat x86-arkkitehtuureja, mutta useat nykyaikaiset arkkitehtuurit käyttävät samankaltaista konseptia.

BIOS määrittää SMM:n käynnistyksen aikana. SMM-koodi lisätään päämuistiin (DRAM), ja BIOS käyttää sitten erityisiä (lukittavia) piirisarjan sisäisiä konfiguraatiorekistereitä tämän alueen käytön estämiseksi, kun suoritinta ei käytetä SMM-kontekstissa. SMM-tilan suorittaminen on käytön aikana tapahtumapohjainen. Piirisarja on ohjelmoitu tunnistamaan erinäisiä tapahtumia ja aikakatkaisuja. Kun tällainen tapahtuma ilmenee, piirisarjan laitteisto aktivoi System Management Interrupt -syöttösignaalin (SMI). Suoritin tallentaa koko tilansa seuraavalla ohjerajalla ja käynnistää SMM-tilan.

Kun suoritin siirtyy SMM-tilaan, se käynnistää laitteiston SMI Active -tuotossignaalin (SMIACT). Tämä pistoke toimii ilmoituksena piirisarjan laitteistolle, että suoritin siirtyy SMM-tilaan. SMI voidaan käynnistää milloin tahansa missä tahansa toimintatilassa, paitsi itse SMM:n kautta. Piirisarjan laitteisto tunnistaa SMIACT-signaalin ja ohjaa kaikki seuraavat muistisyklit SMM:lle varatulle suojatulle muistialueelle (jota kutsutaan joskus SMRAM-alueeksi). Heti SMI-syötteen saamisen ja SMIACT-tuotoksen aktivoinnin jälkeen suoritin alkaa tallentamaan koko sisäistä tilaansa tälle suojatulle muistialueelle.

Kun suorittimen tila on tallennettu SMRAM-muistiin, erityinen SMRAM:issa sijaitseva SMM-käsittelykoodi (jonka BIOS sijoittaa SMRAM:iin käynnistyksen aikana) alkaa toimia erityisessä SMM-tilassa. Tässä toimintatilassa useimmat laitteiston ja muistin eristysmekanismit keskeytetään ja suoritin voi käyttää lähes kaikkia alustan resursseja, jotta se voi suorittaa vaaditut tehtävät. SMM-koodi suorittaa vaaditun tehtävän, ja sitten on aika palauttaa suoritin aiempaan toimintatilaan. Tässä vaiheessa SMM-koodi suorittaa Return from System Management Mode -ohjeen (RSM) SMM:stä poistumiseksi. RSM-ohjeen seurauksena suoritin palautuu aiempaan tilaansa, joka palautetaan SMM:n käynnistämisen aikana SMRAM:iin tallennetusta kopiosta. Kun RSM:n suoritus on valmis, koko suorittimen tila on palautettu SMI-tapahtumaa edeltävään tilaan ja edellinen ohjelma (käyttöjärjestelmä, sovellukset, hypervisor jne.) jatkaa suorittamista siitä, mihin se jäi.

[1] HP Sure Start Controller -ohjainlaitteisto on saanut CSPN-sertifikaattikehyksen mukaisen sertifikaatin.

[2] HP Sure Start with Dynamic Protection on saatavilla HP Elite -tuotteille, joissa on 6. sukupolven Intel Core -suoritin tai uudempi.

[3] HP Notification -ohjelmiston täytyy olla asennettuna, jotta HP Sure Start -tapahtumia voidaan nähdä Windowsin Tapahtumienhallinnassa.

[4] HP Notification -ohjelmiston täytyy olla asennettuna ilmoitusten saamiseksi.

[5] 3. sukupolven HP Sure Start on saatavilla HP Elite -tuotteille, joissa on Intelin 7. sukupolven suoritin.

[6] HP Sure Start with Runtime Intrusion Detection on saatavilla HP Elite -tuotteille, joissa on AMD:n 7. sukupolven suoritin.

[7] 4. sukupolven HP Sure Start on saatavilla HP Elite- ja HP Pro 600 -tuotteille, joissa on 8. sukupolven Intel- tai AMD-suoritin.

Lisätietoja on osoitteessa
hp.com/go/computersecurity

4AA7-3172FICI, Toukokuu 2018