HP TamperLockin käyttöopas

YHTEENVETO

HP TamperLock suojaa tietokonetta tilanteissa, joissa hyökkääjä yrittää avata sen kotelon ja tehdä laitteistoon haitallisia muokkauksia.

Ensimmäinen painos: syyskuu 2020

Asiakirjan osanumero: M11669-351

Sisällysluettelo

1 Yleiskatsaus 1

2 Käyttö 2

3 Toimintosarja 3

4 Käytäntöasetukset 4

5 Tila 6

Tapahtumien valvontaloki 6

1 Yleiskatsaus

HP TamperLock suojaa tietokonetta tilanteissa, joissa hyökkääjä yrittää avata sen kotelon ja tehdä laitteistoon haitallisia muokkauksia. HP TamperLock sisältää antureita, joiden avulla se voi havaita, onko kotelo avattu, ja käytäntöjä, joilla voidaan määrittää, miten tällaisiin tapahtumiin reagoidaan.

HP TamperLockin käytännöt sisältävät valinnaisena mahdollisuutena järjestelmän käynnistyksen estämisen BIOS-tasolla siihen asti, että BIOS-järjestelmänvalvojan kirjautumistiedot annetaan, HP Trusted Platform Module (TPM) -turvapiirin käyttäjäavainten nollaamisen (kun esimerkiksi BitLocker-avaimet nollataan, paikalliselle asemalle tallennettujen tietojen käyttöön tarvitaan muualla säilytettävä BitLocker-palautusavain) sekä mahdollisuuden sammuttaa järjestelmä välittömästi, kun kotelo avataan. Kotelon avaustapahtumat ja -historia tallennetaan alustalaitteistoon, ja järjestelmänvalvoja voi tehdä niitä koskevia kyselyitä etäyhteydellä.

HP TamperLock -käytäntöjä suojataan muokkauksilta suojatussa tallennustilassa HP Endpoint Security Controller -laitteiston avulla. Suojattu tallennustila suojaa fyysisiltä hyökkäyksiltä BIOS- ja laiteohjelmistotietoja sekä HP TamperLockin asetuksiin liittyviä flash-muistiin tallennettuja asetuksia. Tämä ominaisuus on aina käytössä järjestelmissä, jotka tukevat HP TamperLockia, eikä sitä voi poistaa käytöstä.

2 Käyttö

HP TamperLock on määritetty lukitsemaan järjestelmä luvattoman käytön vuoksi. Se tunnistaa kotelon luvattoman avaamisen riippumatta järjestelmän virtatilasta. HP TamperLock tunnistaa tarkalleen ottaen kotelon avaustapahtuman kaikissa seuraavissa järjestelmän virtatiloissa, kun HP TamperLockiin on määritetty HP:n suosittelemat asetukset.

- **Järjestelmä käynnissä** (käyttöjärjestelmä käynnissä)
- **Järjestelmä sammutettuna** (käyttöjärjestelmä sammutettuna tai horrostilassa)
- **Järjestelmä lepotilassa**

TÄRKEÄÄ: Saat tässä asiakirjassa kuvatut parhaat tulokset määrittämällä HP TamperLockiin HP:n suosittelemat asetukset, jotka on esitetty taulukossa 4-1.

Lisäksi HP TamperLockin kotelon avauksen tunnistin aktivoituu myös tilanteessa, jossa kotelon ollessa avattuna irrotetaan kaikki virtalähteet, kuten sisäinen akku ja reaaliaikakellon nappiparisto.

HUOMAUTUS: Reaaliaikakellon virranmenetys aktivoi automaattisesti HP TamperLockin kotelon avauksen tunnistimen. Tämän vuoksi HP TamperLockin kotelon avauksen tunnistin aktivoituu järjestelmissä, joita säilytetään yli kahden vuoden ajan niin, ettei niitä ole kytketty virtalähteeseen, vaikka koteloa ei olisikaan avattu.

Kun HP TamperLock havaitsee kotelon avaamisen järjestelmän ollessa käynnissä tai lepotilassa, järjestelmä sammutetaan välittömästi ja kaikki tallentamattomat tiedot menetetään. Jos valinnainen käytäntö, jonka mukaan TPM-turvapiirin tila nollataan kotelon avauksen tunnistuksen yhteydessä, on **käytössä**, BIOS nollaa TPM-turvapiirin. BIOS ei käynnistä käyttöjärjestelmää kotelon avaamisen tunnistuksen jälkeen, vaan se kehottaa paikallista käyttäjää syöttämään BIOS-järjestelmänvalvojan salasanan tai (Sure Admin -tilassa) kertaluontoisen PIN-koodin, jolla voidaan avata järjestelmän lukitus ja käynnistää se normaalisti.

HP TamperLockin tila voidaan selvittää siihen liittyvän BIOS-asetuksen kyselyllä taikka Windowsin Tapahtumienvalvonnan kautta, kun HP Notifications -ohjelmisto on asennettu.

3 Toimintosarja

HP TamperLockin toimintosarja on esitetty tässä.

1. HP TamperLock tunnistaa, että kotelo on avattu.
2. Jos järjestelmä on käynnissä tai lepotilassa, HP TamperLock pakottaa sammutuksen, jota ei voi peruuttaa.
3. Kotelon avaustapahtuma aiheuttaa sen, että tietokonelaitteisto siirtyy lukittuun tilaan.
4. Kun kotelo taas suljetaan, järjestelmä voidaan käynnistää uudelleen. Kun järjestelmä käynnistetään uudelleen, seuraavat tapahtumat toteutuvat:
    1. Jos TPM-turvapiirin nollaamiskäytäntö on käytössä, BIOS nollaa TPM:n.
    2. Paikallinen käyttäjä saa ilmoituksen kotelon avaamisesta.
    3. BIOS-järjestelmänvalvojan kirjautumistietoja pyydetään:
        - Jos kirjautumistiedot annetaan, järjestelmä käynnistyy normaalisti.
        - Jos kirjautumistietoja ei anneta, järjestelmä ei käynnisty käyttöjärjestelmään.
5. Valvontalokin merkintä synkronoidaan Windowsin® tapahtumalokin kanssa, jos HP Notifications -ohjelmisto on asennettu.

4 Käytäntöasetukset

HP Client Management -työkalujen avulla voit tarkastella ja määrittää HP TamperLockin käytäntöjä BIOS-asetuksina. Asetuksilla ohjataan HP TamperLockin toimintojen käyttöä sekä kotelon avaamisen yhteydessä toteutettavia toimenpiteitä.

Taulukko 4-1 TamperLockin käytäntöasetukset

Asetukset	Kuvaus	Oletus	HP:n suositus
Kotelon avauksen tunnistin	• **Disabled** (Poistettu käytöstä) – Mitään toimenpiteitä ei toteuteta, kun kotelo avataan. • **Notify the user** (Ilmoita käyttäjälle) – Näyttää varoitusviestin seuraavan käynnistyksen yhteydessä, kun kotelo on ollut avattuna. • **Administrator Credential** (Järjestelmänvalvojan kirjautumistiedot) – Tämä asetus vaatii järjestelmänvalvojan salasanan tai (kun HP Sure Admin on käytössä) kertaluontoisen PIN-koodin syöttämisen ennen käynnistyksen jatkamista, kun kotelo on ollut avattuna. Tämän asetuksen käyttöönotto edellyttää salasanan asettamista tai HP Sure Admin Enhanced BIOS Authentication Mode -ominaisuuden käyttöönottoa sekä paikallisen käyttöavaimen määritystä. • **Administrator Password** (Järjestelmänvalvojan salasana) – Sama toiminnallisuus kuin Administrator Credential -vaihtoehdolla (tämän asetuksen käytöllä toteutetaan yhteensopivuus aikaisemman kotelon avauksen tunnistinta tukevan asetustenhallintaohjelmiston kanssa).	Ei käytössä	Administrator Credential (Järjestelmänvalvojan kirjautumistiedot) tai Administrator Password (Järjestelmänvalvojan salasana)
Virran katkaisu kotelon avaamisen yhteydessä	Käytettävissä vain, kun kotelon avauksen tunnistinta ei ole poistettu käytöstä. **Disabled** (Poistettu käytöstä) – Jos järjestelmä on käynnissä tai lepotilassa, kun kotelo avataan, sen tilaa ei muuteta. **Enabled** (Käytössä) – Järjestelmä sammutetaan välittömästi, kun kotelo avataan, jos järjestelmä on käynnissä tai lepotilassa (S3 tai moderni valmiustila).	Ei käytössä	Käytössä
TPM:n nollaus käynnistyksen yhteydessä kotelon avaamisen jälkeen	Käytettävissä vain, kun kotelon avauksen tunnistinta ei ole poistettu käytöstä. • **Disabled** (Poistettu käytöstä) – TPM:n tilaa ei muuteta, kun kotelo avataan. • **Enabled** (Käytössä) – TPM nollataan seuraavan käynnistyksen yhteydessä, kun	Ei käytössä	Riippuu asiakkaan vaatimuksista.

Taulukko 4-1 TamperLockin käytäntöasetukset (jatkoa)

Asetukset	Kuvaus	Oletus	HP:n suositus
	kotelo on avattu. Kaikki TPM:n asiakasavaimet nollataan. **HUOMAUTUS:** Ota tämä asetus käyttöön vain, kun manuaalinen palautus etävarmuuskopioista on mahdollinen tai kun et halua käyttää palautusta. Jos BitLocker on käytössä, aseman salausta ei voi purkaa ilman BitLocker-palautusavainta.		
Käynnistystä edeltävä DMA-suojaus	**Thunderbolt only** (Vain Thunderbolt) – IOMMU-yksikön (Input-Output Memory Management Unit) laitteistopohjainen DMA-suojaus on käytössä BIOS-esikäynnistysympäristössä Thunderbolt-liitäntää käyttävillä PCI-e-laitteilla. **All PCIe devices** (Kaikki PCIe-laitteet) – IOMMU-yksikön (Input-Output Memory Management Unit) laitteistopohjainen DMA-suojaus on käytössä BIOS-esikäynnistysympäristössä kaikilla sisäisillä ja ulkoisilla PCI-e-laitteilla.	Thunderbolt Only (Vain Thunderbolt)	All PCI-Devices (Kaikki PCI-laitteet)
DMA-suojaus	**Disabled** (Poistettu käytöstä) – BIOS ei määritä IOMMU-yksikön (Input-Output Memory Management Unit) laitteistoa DMA-suojausta tukevien käyttöjärjestelmien käyttöön. **Enabled** (Käytössä) – BIOS määrittää IOMMU-yksikön (Input-Output Memory Management Unit) laitteiston DMA-suojausta tukevien käyttöjärjestelmien käyttöön.	Käytössä	Käytössä

5 Tila

Voit määrittää BIOS-asetuksen kyselyllä HP TamperLockin tilan käyttäen nykyisiä BIOS-asetusten hallintatyökaluja. Ainoa tapa nollata tämä asetus on antaa BIOS-järjestelmänvalvojan salasana tai BIOS-järjestelmänvalvojan kirjautumistiedot (Sure Admin -tila).

Taulukko 5-1

Asetus	Kuvaus
Kotelon viimeisin avaus ja lukumäärä	Kun kotelon avauksen tunnistinta ei ole otettu pois käytöstä, tämä asetus ilmoittaa, milloin kotelo on viimeksi avattu sekä kuinka monta kertaa se on avattu ja avaus on kuitattu sen jälkeen, kun BIOS-järjestelmänvalvoja on viimeksi nollannut tunnistimen. Syötteen muoto on KK/PP/VVVV TT:MM:SS. X kertaa. Järjestelmän olosuhteista riippuen (esim. tietokoneen ollessa sammutettuna) kotelon peräkkäiset avaukset eivät kasvata lukemaa. Päivämäärä ja kellonaika ilmoitetaan 0-arvoina tilanteissa, joissa arvoa ei voi määrittää, kuten reaaliaikakellon virranmenetyksen jälkeen.

Tapahtumien valvontaloki

Jos HP Notifications -ohjelmisto on asennettu, voit tarkastella seuraavia tapahtumalokeja Windowsin Tapahtumienvalvonnassa HP Sure Start -kansiossa.

Taulukko 5-2 Valvontaloki

Lähteen tunnus	Tapahtuman tunnus	Tapahtuma	Tapahtumalokin tyyppi
0x8A	0x1E	HP TamperLock – Järjestelmä havaitsi, että kotelo on avattu.	Varoitus
	0x1F	HP TamperLock – Käyttäjä kuittasi BIOS POST -ilmoituksen siitä, että kotelo oli avattu.	Tiedoksi
	0x20	HP TamperLock – TPM-turvapiiri nollattiin kotelon avaamisen vuoksi HP TamperLockin nykyisten käytäntöasetusten mukaan.	Tiedoksi