F-Secure Anti-Virus 2013

Sisällys

Luku 1:Asennus.....5

Ennen ensimmäistä asennuskertaa.....6
Tuotteen asentaminen ensimmäisen kerran.....6
Sovellusten asentaminen ja päivittäminen.....6
Ohje ja tuki.....7

Luku 2:Aloittaminen.....9

Automaattisten päivitysten käyttäminen.....10
Päivityksen tilan tarkastaminen.....10
Internet-yhteysasetusten muuttaminen.....10
Reaaliaikaisen suojauksen verkon tilan tarkistaminen.....11
Tuotteen tekemien toimien tarkasteleminen.....11
Ilmoitushistorian näyttäminen.....11
Ilmoitusasetusten muuttaminen.....11
Reaaliaikainen suojausverkko.....12
Tietoja reaaliaikaisesta suojausverkosta.....12
Reaaliaikaisen suojausverkon käytön edut.....12
Lähetettävät tiedot.....13
Tietoja siitä, kuinka suojaamme yksityisyytesi.....14
Reaaliaikaiseen suojausverkkoon osallistuminen.....14
Reaaliaikaiseen suojausverkkoon liittyviä kysymyksiä.....14
Tilauksen voimassaolon tarkastaminen.....15
Toimenpidekeskus.....15
Aktivoi tilaus.....16

Luku 3:Johdanto.....17

Suojauksen yleistilan tarkastaminen.....18
Näytä tuotetilastot.....18
Käsittele tuotepäivitykset.....19
Näytä tietokantaversiot.....19
Muuta mobiililaajakaistan asetuksia.....19
Mitä virukset ja muut haittaohjelmat ovat?.....20
Virukset.....20
Vakoiluohjelmat.....20
Rootkit-ohjelmat.....21
Riskiohjelmat.....21

Luku 4:Tietokoneen suojaaminen haittaohjelmilta.....23
Tietokoneen tarkistaminen.....24
Tiedostojen automaattinen tarkistus.....24
Tiedostojen manuaalinen tarkistus.....26
Sähköpostin tarkistus.....29
Tarkistustulosten tarkasteleminen.....30
Tiedostojen jättäminen pois tarkistuksesta.....30
Tiedostotyyppien ohittaminen.....30
Tiedostojen ohittaminen sijainnin mukaan.....31
Ohitettujen sovellusten tarkasteleminen.....31
Eristyksen käyttäminen.....32
Eristettyjen kohteiden tarkasteleminen.....32
Eristettyjen kohteiden palauttaminen.....33
Mikä on DeepGuard?.....33
DeepGuardin ottaminen käyttöön tai poistaminen käytöstä.....33
Salli DeepGuardin torjumia sovelluksia.....34
DeepGuardin käyttäminen yhteensopivuustilassa.....34
Toimenpiteet epäilyttävän toiminnan varoituksen tullessa näkyviin.....34

Luku

1

Asennus

Aiheet:

- *Ennen ensimmäistä asennuskertaa*
- *Tuotteen asentaminen ensimmäisen kerran*
- *Sovellusten asentaminen ja päivittäminen*
- *Ohje ja tuki*

Ennen ensimmäistä asennuskertaa

Kiitos, että valitsit F-Securen.

Tuotteen asentamiseen tarvitaan seuraavaa:

- CD-asennuslevy tai asennuspaketti. Jos käytät kannettavaa tietokonetta, jossa ei ole CD-asemaa, voit ladata asennuspaketin osoitteesta *www.f-secure.com/netbook*.
- Tilauskoodi.
- Internet-yhteys.

Jos käytät jonkin toisen toimittajan tietoturvatuotetta, asennusohjelma yrittää poistaa sen automaattisesti. Jos tämä ei onnistu, poista se manuaalisesti.

Huomautus: Jos tietokoneessa on useita tilejä, kirjaudu järjestelmänvalvojan oikeuksilla, kun teet asennuksen.

Tuotteen asentaminen ensimmäisen kerran

Tuotteen asennusohjeet.

Voit asentaa tuotteen seuraavia ohjeita noudattamalla:

1. Aseta CD-levy asemaan tai kaksoisnapsauta lataamaasi asennusohjelmaa.

   Jos CD-levy ei käynnisty automaattisesti, siirry Windowsin Resurssienhallintaan, kaksoisnapsauta CD-levyn kuvaketta ja aloita asennus kaksoisnapsauttamalla asennustiedostoa.

2. Noudata näyttöön tulevia ohjeita.

   - Jos olet ostanut tuotteen CD-levynä liikkeestä, tilauskoodi on pika-asennusoppaan kannessa.
   - Jos olet ladannut tuotteen F-Secure eStore -myymälästä, tilauskoodi on ostotilauksen vahvistussähköpostissa.

   Tietokone on ehkä käynnistettävä uudelleen, ennen kuin tilauksen voi vahvistaa ja uusimmat päivitykset voi ladata Internetistä. Jos asennat CD-levyltä, muista poistaa CD-asennuslevy ennen tietokoneen uudelleenkäynnistystä.

Sovellusten asentaminen ja päivittäminen

Uuden tilauksen aktivointiohjeet.

Aktivoi uusi tilaus tai asenna uusi sovellus käynnistysalustan avulla näiden ohjeiden mukaisesti:

Huomautus: Käynnistysalustan kuvake löytyy Windowsin ilmaisinalueelta.

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Näytä omat tilaukset**
3. Siirry **Omat tilaukset** -kohdassa **Tilauksen tila** -sivulle ja valitse **Aktivoi tilaus**. **Aktivoi tilaus** -ikkuna tulee näkyviin.
4. Anna sovelluksen tilauskoodi ja valitse **OK**.

5. Kun tilaus on vahvistettu ja aktivoitu, valitse **Sulje**.
6. Siirry **Omat tilaukset** -kohdassa **Asennuksen tila** -sivulle. Jos asennus ei ala automaattisesti, noudata näitä ohjeita:
   a) Valitse **Asenna**.
      Asennusikkuna tulee näkyviin.
   b) Valitse **Seuraava**.
      Sovellus ladataan, ja asennus alkaa.
   c) Kun asennus on valmis, valitse **Sulje**.

Uusi tilaus on aktivoitu.

Ohje ja tuki

Voit avata tuotteen online-ohjeen napsauttamalla Ohje-kuvaketta tai painamalla F1-näppäintä missä tahansa tuotteen näytössä.

Kun olet rekisteröinyt käyttöoikeuden, voit käyttää lisäpalveluja, kuten maksuttomia tuotepäivityksiä ja tuotetukea. Voit tehdä rekisteröinnin osoitteessa *www.f-secure.com/register*.

Luku

2

Aloittaminen

Aiheet:

- *Automaattisten päivitysten käyttäminen*
- *Tuotteen tekemien toimien tarkasteleminen*
- *Reaaliaikainen suojausverkko*
- *Tilauksen voimassaolon tarkastaminen*

Tietoja tuotteen käytön aloittamisesta.

Tässä osiossa kerrotaan, miten yleisiä asetuksia voi muuttaa ja miten tilauksia voi hallita käynnistysalustan kautta.

Käynnistysalustan yleiset asetukset ovat asetuksia, jotka koskevat kaikkia käynnistysalustaan asennettuja ohjelmia. Asetuksia ei tarvitse muuttaa erikseen kussakin ohjelmassa, vaan voit muokata yleisiä asetuksia, joita käytetään sitten kaikissa asennetuissa ohjelmissa.

Käynnistysalustan yleisiä asetuksia ovat muun muassa seuraavat:

- Lataukset, jossa voit tarkastella tietoja ladatuista päivityksistä ja tarkistaa manuaalisesti, onko uusia päivityksiä saatavilla.
- Yhteysasetukset, jossa voit muuttaa tietokoneen Internet-yhteyttä.
- Ilmoitukset, jossa voit tarkastella aiempia ilmoituksia ja määrittää näytettävät ilmoitukset.
- Tietosuoja-asetukset, jossa voit valita, voiko tietokone muodostaa yhteyden reaaliaikaiseen suojausverkkoon.

Käynnistysalustan kautta voit myös hallita asennettujen ohjelmien tilauksia.

Automaattisten päivitysten käyttäminen

Automaattiset päivitykset pitävät tietokoneen suojauksen päivitettynä.

Tuote noutaa uusimmat päivitykset tietokoneeseesi, kun käytössä on Internet-yhteys. Se havaitsee verkkoliikenteen eikä häiritse muuta Internetin käyttöä, vaikka verkkoyhteys olisi hidas.

Päivityksen tilan tarkastaminen

Voit tarkistaa edellisen päivityksen päivämäärän ja kellonajan.

Kun automaattiset päivitykset ovat käytössä, tuote vastaanottaa uusimmat päivitykset automaattisesti, kun Internet-yhteys on muodostettu.

Varmista seuraavasti, että uusimmat päivitykset ovat käytössä:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Avaa yleisasetukset**.
3. Valitse **Automaattiset päivitykset** > **Lataukset**.
4. Valitse **Tarkista nyt**.
   Tuote muodostaa Internet-yhteyden ja tarkistaa uusimpien päivitysten saatavuuden. Jos suojaus ei ole ajan tasalla, ohjelma noutaa viimeisimmät päivitykset.

   Huomautus: Jos muodostat Internet-yhteyden modeemin tai ISDN-liittymän kautta, yhteyden on oltava käytössä, kun aloitat päivitystarkistuksen.

Internet-yhteysasetusten muuttaminen

Yleensä oletusasetuksia ei tarvitse muuttaa, mutta voit määrittää, miten palvelin muodostaa Internet-yhteyden, jotta saat päivitykset automaattisesti.

Internet-yhteyden asetusten muuttaminen:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Avaa yleisasetukset**.
3. Valitse **Automaattiset päivitykset** > **Yhteys**.
4. Valitse **Internet-yhteys** -luettelosta tapa, jolla tietokoneesi muodostaa yhteyden Internetiin.
   - Valitse **Oleta yhteyden olevan päällä jatkuvasti**, jos sinulla on kiinteä verkkoyhteys.

     Huomautus: Jos tietokoneen verkkoyhteys ei ole kiinteä vaan tarvittaessa muodostettava puhelinverkkoyhteys, **Oleta yhteyden olevan päällä jatkuvasti** -vaihtoehdon valitseminen saattaa aiheuttaa useita puhelinverkkoyhteyksiä.
   - Valitse **Havaitse yhteys**, jos haluat noutaa päivityksiä vain, kun tuote havaitsee, että verkkoyhteys on käytettävissä.
   - Valitse **Havaitse tietoliikenne**, jos haluat noutaa päivityksiä vain, kun tuote havaitsee muuta verkkoliikennettä.

     Vihje: Jos laitteistoasetukset ovat epätavalliset ja ne käyttävät **Havaitse yhteys** -asetusta havaitsemaan käytettävää verkkoyhteyttä (vaikka sellaista ei olisi), valitse sen sijaan **Havaitse tietoliikenne** -asetus.

5. Valitse **HTTP-välityspalvelin** -luettelosta, käyttääkö tietokone *välityspalvelinta* Internet-yhteyden muodostamiseen.
   - Valitse **Ei HTTP-välityspalvelinta**, jos tietokone ei muodosta Internet-yhteyttä suoraan.
   - Valitse **Määritä HTTP-välityspalvelin manuaalisesti**, jos haluat määrittää *HTTP-välityspalvelin* asetukset.
   - Valitse **Käytä selaimen HTTP-välityspalvelinta**, jos haluat käyttää Web-selaimeen määritettyjä *HTTP-välityspalvelinasetuksia*.

Reaaliaikaisen suojauksen verkon tilan tarkistaminen

Useiden tuoteominaisuuksien asianmukainen toimiminen edellyttää yhteyttä reaaliaikaisen suojauksen verkkoon.

Jos verkko-ongelmia ilmenee, tai palomuuri estää reaaliaikaisen suojauksen verkon liikenteen, tila on "katkaistu". Jos reaaliaikaisen suojauksen verkon käyttöä edellyttäviä tuoteominaisuuksia ei ole asennettu, tila on "ei käytössä".

Voit tarkistaa tilan seuraavasti:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Avaa yleisasetukset**.
3. Valitse **Automaattiset päivitykset** > **Yhteys**.

Reaaliaikaisen suojauksen verkko -kohdassa näkyy reaaliaikaisen suojauksen verkon senhetkinen tila.

Tuotteen tekemien toimien tarkasteleminen

Ilmoitukset-sivulla näet, mitä tuote on tehnyt tietokoneen suojaamiseksi.

Tuote näyttää ilmoituksen, kun se tekee jotain, kuten löytää estettävän viruksen. Myös palveluntarjoaja saattaa lähettää joitakin ilmoituksia esimerkiksi ilmoituksena uusista palveluista.

Ilmoitushistorian näyttäminen

Voit tarkastella näytettyjä ilmoituksia ilmoitushistoriassa

Ilmoitushistorian tarkasteleminen:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Avaa yleisasetukset**.
3. Valitse **Muu** > **Ilmoitukset**.
4. Valitse **Näytä ilmoitushistoria**.
   Ilmoitushistorialuettelo tulee näkyviin.

Ilmoitusasetusten muuttaminen

Voit valita, millaisia ilmoituksia haluat tuotteen näyttävän.

Voit muuttaa ilmoitusasetuksia seuraavasti:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.

2. Valitse **Avaa yleisasetukset**.
3. Valitse **Muu** > **Ilmoitukset**.
4. Valitse **Salli ohjelmaviestit** -vaihtoehto tai poista sen valinta, jos haluat ottaa ohjelmaviestit käyttöön tai poistaa ne käytöstä.

   Kun tämä asetus on otettu käyttöön, tuote näyttää asennettujen ohjelmien ilmoitukset.
5. Valitse **Salli kampanjaviestit** -vaihtoehto tai poista sen valinta, jos haluat ottaa kampanjaviestit käyttöön tai poistaa ne käytöstä.
6. Valitse **OK**.

Reaaliaikainen suojausverkko

Tässä asiakirjassa on kuvaus reaaliaikaisesta suojausverkosta. Se on F-Secure Corporationin verkkopalvelu, joka tunnistaa vaarattomat sovellukset ja Web-sivustot ja tarjoaa samalla suojaa haittaohjelmia ja Web-sivustojen heikkouksien hyödyntämistä vastaan.

Tietoja reaaliaikaisesta suojausverkosta

Reaaliaikainen suojausverkko on verkkopalvelu, joka tarjoaa nopean mahdollisuuden päivittää suojaus uusimpia Internet-pohjaisia uhkia vastaan.

Reaaliaikaiseen suojausverkkoon osallistumalla voit auttaa meitä vahvistamaan suojausta uusia uhkia vastaan. Reaaliaikainen suojausverkko kerää tiettyjen tuntemattomien, haitallisten tai epäilyttävien sovellusten tilastotietoja sekä tietoja siitä, mitä ne tekevät laitteessasi. Nämä tiedot kerätään nimettömästi ja lähetetään F-Secure Corporationille yhdistettyä data-analyysia varten. Analysoitujen tietojen perusteella parannamme laitteesi suojausta uusimpia uhkia ja haitallisia tiedostoja vastaan.

Reaaliaikaisen suojausverkon toiminta

Reaaliaikaiseen suojausverkkoon osallistuminen tarkoittaa, että toimitat tuntemattomia sovelluksia ja Web-sivustoja sekä haitallisia sovelluksia ja Web-sivustojen heikkouksia koskevia tietoja. Reaaliaikainen suojausverkko ei jäljitä Web-toimia eikä kerää jo analysoitujen Web-sivustojen tietoja, eikä se kerää tietokoneeseen asennettujen puhtaiden sovellusten tietoja.

Jos et halua lähettää näitä tietoja, reaaliaikainen suojausverkko ei kerää asennettujen sovellusten tai avattujen Web-sivustojen tietoja. Tuotteen on kuitenkin lähetettävä sovellusten, Web-sivustojen, viestien ja muiden objektien mainetta koskeva kysely F-Secure-palvelimille. Kysely tehdään kryptografista tarkistussummaa käyttämällä. Tällä menetelmällä kyselyn kohteena olevaa objektia ei lähetetä F-Securelle. Emme jäljitä tietoja käyttäjäkohtaisesti, vaan vain tiedoston tai Web-sivuston käyttölaskurin määrä muuttuu.

Kaikkea verkon tietoliikennettä reaaliaikaiseen suojausverkkoon ei voi pysäyttää, koska ominaisuus on oleellinen osa tuotteen tarjoamaa suojaa.

Reaaliaikaisen suojausverkon käytön edut

Reaaliaikaisen suojausverkon avulla saat nopeamman ja tarkemman suojauksen uusimpia uhkia vastaan ja vältyt tarpeettomilta hälytyksiltä epäilyttävistä sovelluksista, jotka eivät ole haitallisia.

Reaaliaikaiseen suojausverkkoon osallistumalla voit auttaa meitä löytämään uusia, aiemmin havaitsemattomia haittaohjelmia ja poistaamaan mahdolliset väärät hälytykset virusmääritystietokannastamme.

Kaikki reaaliaikaisen suojausverkon osallistujat auttavat toisiaan. Kun reaaliaikainen suojausverkko löytää epäilyttävän sovelluksen laitteestasi, hyödyt analyysituloksista, jos sama sovellus on löydetty jo aiemmin muista laitteista. Reaaliaikainen suojausverkko parantaa laitteen yleistä suorituskykyä, koska sen ansiosta asennetun suojausohjelman ei tarvitse tarkistaa uudelleen sovelluksia, jotka reaaliaikainen suojausverkko on jo aiemmin analysoinut ja havainnut turvallisiksi. Vastaavasti haitallisia Web-sivustoja ja ei-toivottuja

roskaposteja käsittelevät tiedot jaetaan reaaliaikaisen suojausverkon kautta. Näimme voimme tarjota asiakkaillemme entistä tarkempaa suojausta Web-sivuston haavoittuvuuksien hyödyntämisyrityksiä ja roskapostiviestejä vastaan.

Mitä enemmän käyttäjiä reaaliaikaiseen suojausverkkoon osallistuu, sitä paremmin yksittäisiä käyttäjiä voidaan suojata.

Lähetettävät tiedot

Reaaliaikaiseen suojausverkkoon osallistuminen tarkoittaa, että toimitat laitteeseen tallennettuja sovelluksia ja avaamiasi Web-sivustoja koskevia tietoja, jotta reaaliaikainen suojausverkko voi suojata käyttäjiä uusimmilta haittasovelluksilta ja epäilyttäviltä Web-sivustoilta.

Tiedostojen maineen analysoiminen

Reaaliaikainen suojausverkko kerää tietoja vain sovelluksista, joita ei tunneta, ja tiedostoista, jotka ovat epäilyttäviä tai joiden tiedetään olevan haittaohjelmia.

Real-time Protection Network kerää nimettömiä tietoja laitteessa olevista puhtaista ja epäilyttävistä sovelluksista. Real-time Protection Network kerää tietoja vain ohjelmatiedostoista (kuten Windowsin PE-tiedostoista, joiden tiedostotunnisteita voivat olla .cpl, .exe, .dll, .ocx, .sys, .scr ja .drv).

Kerättyjä tietoja ovat:

- sovellustiedoston polku laitteessasi
- tiedoston koko ja sen luonti- tai muokkausajankohta
- tiedostomääritteet ja oikeudet,
- tiedoston allekirjoitustiedot
- tiedoston nykyinen versio ja tieto yrityksestä, joka on luonut sen
- tiedoston alkuperä tai sen latauksen URL-osoite
- F-Secure DeepGuard ja tarkistettujen tiedostojen virustorjunta-analyysin tulokset sekä
- muut vastaavat tiedot.

Real-time Protection Network ei kerää koskaan tietoja henkilökohtaisista asiakirjoista, ellei niissä ole havaittu tartuntaa. Jos kyseessä on haitallinen tiedosto, se kerää tartunnan nimen ja tartunnan poistamisen tilan.

Reaaliaikaisen suojausverkon avulla voit myös lähettää epäilyttäviä sovelluksia analysoitavaksi. Voit lähettää vain PE (Portable Executable) -tiedostoja. Reaaliaikainen suojausverkko ei koskaan kerää mitään tietoja henkilökohtaisista asiakirjoistasi eikä koskaan lähetä niitä analysoitaviksi.

Tiedostojen lähettäminen analysoitaviksi

Reaaliaikaisen suojausverkon avulla voit myös lähettää epäilyttäviä sovelluksia analysoitavaksi.

Voit lähettää erillisiä epäilyttäviä sovelluksia manuaalisesti, kun tuote kehottaa tekemään niin. Voit lähettää vain Portable Executable -tiedostoja. Reaaliaikainen suojausverkko ei koskaan lataa henkilökohtaisia asiakirjoja.

Web-sivuston maineen analysoiminen

Reaaliaikainen suojausverkko ei seuraa Internetin käyttöäsi tai kerää tietoja Web-sivustoista, jotka on jo analysoitu. Se varmistaa, että Internetin selaamisesi aikana käyttämäsi Web-sivustot ovat turvallisia. Kun käyt sivustossa, reaaliaikainen suojausverkko tarkistaa sen turvallisuuden ja ilmoittaa sinulle, jos sivusto on arvioitu epäilyttäväksi tai haitalliseksi.

Jos Web-sivusto, jossa vierailet, sisältää haitallista tai epäilyttävää sisältöä tai tunnetun heikkoutta hyödyntävän ongelman, reaaliaikainen suojausverkko kerää sivuston koko URL-osoitteen, jotta Web-sivun sisältö voidaan analysoida.

Jos käyt sivustossa, jota ei ole vielä arvioitu, reaaliaikainen suojausverkko kerää toimialueen ja alitoimialueen nimet ja joissakin tapauksissa käyttämäsi sivun polun, jotta sivusto voidaan analysoida ja sen vaarallisuus

arvioida. Kaikki tietoja luultavasti sisältävät URL-parametrit, jotka voidaan liittää sinuun henkilöllisyytesi paljastavalla tavalla, poistetaan yksityisyytesi varjelemiseksi.

Huomautus: Reaaliaikainen suojausverkko ei arvioi tai analysoi yksityisten verkkojen Web-sivuja. Tästä syystä se ei koskaan kerää mitään tietoja yksityisten IP-verkkojen osoitteista (esimerkiksi yritysverkoista).

Järjestelmätietojen analysoiminen

Reaaliaikainen suojausverkko kerää käyttöjärjestelmän nimen ja version, tietoja Internet-suojauksesta ja reaaliaikaisen verkon käyttötiedoista (esimerkiksi siitä, kuinka monta kertaa Web-sivuston mainetta on kyselty ja kuinka kauan kyselyyn vastaaminen keskimäärin kestää), jotta voimme valvoa ja parantaa palvelua.

Tietoja siitä, kuinka suojaamme yksityisyytesi

Siirrämme tiedot turvallisesti ja poistamme niistä automaattisesti kaikki niiden mahdollisesti sisältämät henkilötiedot.

Reaaliaikainen suojausverkko poistaa henkilötiedot ennen tietojen lähettämistä F-Securelle ja salaa kaikki kerätyt tiedot siirron aikana suojatakseen niitä luvattomalta käytöltä. Kerättyjä tietoja ei käsitellä yksitellen, vaan ne ryhmitellään muiden reaaliaikaiseen suojausverkkoon osallistuvien tietojen kanssa. Kaikki tiedot analysoidaan tilastotietoina ja nimettömästi, mikä tarkoittaa, että mitään tietoja ei yhdistetä sinuun millään tavalla.

Kerättyihin tietoihin ei sisällytetä mitään tietoja, joiden avulla henkilöllisyytesi voitaisiin selvittää. Reaaliaikainen suojausverkko ei kerää yksityisiä IP-osoitteita tai henkilökohtaisia tietojasi, kuten sähköpostiosoitteita, käyttäjänimiä ja salasanoja. Teemme parhaamme kaikkien henkilötietojen poistamiseksi, mutta on mahdollista, että kerättyihin tietoihin jää silti henkilötietoja. Jos näin käy, emme käytä tällaisia tahattomasti kerättyjä tietoja henkilöllisyytesi selvittämiseen.

Käytämme tiukkoja suojausmenetelmiä ja fyysisiä, hallinnollisia ja teknisiä suojauskeinoja kerättyjen tietojen suojaamiseksi niiden siirtämisen, tallentamisen ja käsittelemisen aikana. Tiedot tallennetaan turvattuun sijaintiin ja hallinnassamme oleviin palvelimiin, jotka sijaitsevat joko toimipisteessämme tai alihankkijoidemme toimipisteessä. Vain valtuutetut henkillöt voivat käsitellä kerättyjä tietoja.

F-Secure saattaa jakaa kerättyjä tietoja yhteyskumppaniensa, alihankkijoidensa, jakelijoidensa ja kumppaniensa kanssa, mutta tiedot jaetaan aina nimettöminä siten, ettei niiden perusteella voi tunnistaa kenenkään henkilöllisyyttä.

Reaaliaikaiseen suojausverkkoon osallistuminen

Voit auttaa meitä parantamaan reaaliaikaisen suojausverkon suojaa lähettämällä tietoja haitallisista ohjelmista ja Web-sivustoista.

Voit valita reaaliaikaiseen suojausverkkoon osallistumisen asennuksen aikana. Kun asennuksen oletusasetukset valitaan, tietoja toimitetaan reaaliaikaiseen suojausverkkoon. Voit muuttaa tätä asetusta myöhemmin tuotteessa.

Voit muuttaa reaaliaikaisen suojausverkon asetuksia seuraavasti:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Avaa yleisasetukset**.
3. Valitse **Muu** > **Tietosuoja**.
4. Valitse osallistumisvalintaruutu, jotta osallistut reaaliaikaiseen suojausverkkoon.

Reaaliaikaiseen suojausverkkoon liittyviä kysymyksiä

Yhteystiedot reaaliaikaista suojausverkkoa koskevia kysymyksiä varten:

Jos sinulla on lisää kysymyksiä reaaliaikaisesta suojausverkosta, ota yhteyttä:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

Tämän tietosuojakäytännön uusin versio on aina luettavissa Web-sivustossamme.

Tilauksen voimassaolon tarkastaminen

Tilauksen tyyppi ja tila näkyvät **Tilauksen tila** -sivulla.

Kun tilaus on umpeutumassa tai jos tilaus on umpeutunut, koko ohjelman suojaustila vastaavassa käynnistysalustan kuvakkeessa muuttuu.

Tilauksen voimassaolon tarkistaminen:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Näytä omat tilaukset**.
3. Valitse **Tilauksen tila**, jos haluat tarkastella asennettujen ohjelmien tilausten tietoja.
4. Valitse **Asennuksen tila**, jos haluat tarkastella, mitkä ohjelmat ovat asennettavissa.

Tilauksen tila ja umpeutumispäivämäärä näkyvät myös ohjelman **Tilastot**-sivulla. Jos tilaus on umpeutunut, sinun on uusittava tilaus, jotta voit jatkaa päivitysten vastaanottamista ja tuotteen käyttämistä.

Huomautus: Jos tilaus on päättynyt, tilarivillä oleva tuotteen tilakuva vilkkuu.

Toimenpidekeskus

Toimenpidekeskuksessa näkyvät kaikki huomiotasi edellyttävät tärkeät ilmoitukset.

Jos tilaus on umpeutunut tai umpeutumassa, toimenpidekeskus ilmoittaa tästä. Toimenpidekeskusviestin taustaväri ja sisältö määräytyvät tilauksen tyypin ja tilan mukaan:

- Jos tilaus on umpeutumassa, ja vapaita tilauksia on käytettävissä, viestin taustaväri on valkoinen ja siinä on **Aktivoi**-painike.
- Jos tilaus on umpeutumassa, eikä vapaita tilauksia ole käytettävissä, viestin taustaväri on keltainen ja siinä on **Osta**- ja **Anna koodi** -painikkeet. Jos olet jo ostanut uuden tilauksen, voit napsauttaa **Anna koodi** -painiketta ja aktivoida uuden tilauksen antamalla tilauskoodin.
- Jos tilaus on umpeutunut, ja vapaita tilauksia on käytettävissä, viestin taustaväri on punainen ja siinä on **Aktivoi**-painike.
- Jos tilaus on umpeutunut, eikä vapaita tilauksia ole käytettävissä, viestin taustaväri on punainen ja siinä on **Osta**- ja **Anna koodi** -painikkeet. Jos olet jo ostanut uuden tilauksen, voit napsauttaa **Anna koodi** -painiketta ja aktivoida uuden tilauksen antamalla tilauskoodin.

Huomautus: Toimenpidekeskuksen **Näytä ilmoitushistoria** -linkki sisältää luettelon tuoteilmoitusviesteistä, mutta ei aiempia toimintokeskusviestejä.

Aktivoi tilaus

Kun sinulla on tuotteen uusi tilauskoodi tai kampanjakoodi, se on aktivoitava.

Voit aktivoida tilauksen seuraavasti:

1. Napsauta käynnistysalustassa äärimmäisenä oikealla olevaa kuvaketta hiiren kakkospainikkeella. Ponnahdusvalikko tulee näkyviin.
2. Valitse **Näytä omat tilaukset**.
3. Valitse jompikumpi seuraavista vaihtoehdoista:
   - Valitse **Aktivoi tilaus**.
   - Valitse **Aktivoi kampanjakoodi**.
4. Kirjoita uusi tilaus- tai kampanjakoodi näkyviin tulevaan valintaikkunaan ja valitse **OK**.

   Vihje: Jos olet saanut tilauskoodin sähköpostissa, voit kopioida koodin sähköpostiviestistä ja liittää sen kenttään.

Kun olet antanut uuden tilauskoodin, uusi tilauksen voimassaolopäivä tulee näkyviin **Tilauksen tila** -sivulle.

Luku

3

Johdanto

Aiheet:

- *Suojauksen yleistilan tarkastaminen*
- *Näytä tuotetilastot*
- *Käsittele tuotepäivitykset*
- *Mitä virukset ja muut haittaohjelmat ovat?*

Tämä tuote suojaa tietokonetta viruksilta ja muilta haitallisilta sovelluksilta.

Tuote tarkistaa tiedostoja, analysoi sovelluksia ja päivittää automaattisesti. Se ei edellytä sinulta mitään toimia.

Suojauksen yleistilan tarkastaminen

Tila-sivulla on pikakatsaus asennetuista tuoteominaisuuksista ja niiden senhetkisestä tilasta.

Voit avata Tila-sivun seuraavasti:

Valitse pääsivulta Tila.

Tila-sivu tulee näkyviin.

Kuvakkeet ilmaisevat ohjelman ja sen suojausominaisuuksien tilan.

Tilakuvake	Tilan nimi	Kuvaus
	OK	Tietokone on suojattu. Ominaisuus on käytössä ja toimii oikein.
	Tiedot	Tuote ilmoittaa ominaisuuden erikoistilasta. Ominaisuutta saatetaan esimerkiksi päivittää.
	Varoitus	Tietokonetta ei ole suojattu täysin. Tuote ei ole esimerkiksi saanut päivityksiä pitkään aikaan tai ominaisuuden tila edellyttää toimia.
	Virhe	Tietokonetta ei ole suojattu Tilauksesi on voinut vanhentua tai tärkeä ominaisuus on poistettu käytöstä.
	Ei käytössä	Muu kuin kriittinen ominaisuus on poistettu käytöstä.

Näytä tuotetilastot

Voit tarkastaa, mitä tuote on tehnyt sen asennuksen jälkeen Tilastot-sivulta.

Voit avata Tilastot-sivun seuraavasti:

Valitse pääsivulta Tilastot.

Tilastot-sivu tulee näkyviin.

- **Edellinen onnistunut päivitystarkistus** näyttää edellisen päivityksen ajankohdan.
- **Virus- ja vakoiluohjelmatarkistus** näyttää, kuinka monta tiedostoa tuote on tarkistanut ja puhdistanut asennuksen jälkeen.
- **Sovellukset** ilmaisee, kuinka monta ohjelmaa DeepGuard on sallinnut tai estänyt asennuksen jälkeen.

- **Palomuurin yhteydet** näyttää asennuksen jälkeisten sallittujen ja estettyjen yhteyksien määrän.
- **Roskaposti- ja tietokalastussuodatus** näyttää, kuinka monta sähköpostiviestiä tuote on havainnut kelvollisiksi sähköpostiviesteiksi ja roskapostiviesteiksi.

Käsittele tuotepäivitykset

Tuote pitää suojauksen päivitettynä automaattisesti.

Näytä tietokantaversiot

Viimeisimpien päivitysten kellonajat ja versionumerot näytetään **Tietokannan päivitykset** -sivulla.

Tietokannan päivitykset -sivun avaaminen:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Muut asetukset** > **Tietokantaversiot**.

Tietokantaversiot-sivulla näkyy uusin päivämäärä, jolloin virus- ja vakoiluohjelmien tunnistetiedot, DeepGuard ja roskaposti- ja tietokalastelu-suodatuksen tiedot on päivitetty, sekä näiden toimintojen versionumerot.

Muuta mobiililaajakaistan asetuksia

Valitse, haluatko ladata suojauspäivitykset, kun käytät mobiililaajakaistaa.

Huomautus: Tämä toiminto on käytettävissä vain Microsoft Windows 7:ssä.

Suojauspäivitykset ladataan oletusarvoisesti aina, kun olet kotioperaattorin verkossa. Päivitykset kuitenkin keskeytetään, kun vierailet toisen operaattorin verkossa. Tämä johtuu siitä, että yhteyshinnat saattavat vaihdella esimerkiksi operaattorikohtaisesti eri maissa. Tätä asetusta ei kannata muuttaa, jos haluat säästää kaistanleveyttä ja mahdollisesti myös rahaa vierailun aikana.

Huomautus: Tämä asetus koskee vain mobiililaajakaistayhteyksiä. Kun tietokone on liitetty kiinteään tai langattomaan verkkoon, tuote päivitetään automaattisesti.

Voit muuttaa asetusta seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Muut asetukset** > **Mobiililaajakaista** > **Lataa suojauspäivitykset**.
3. Valitse haluamasi mobiiliyhteyksien päivitysvaihtoehto:
   - **Vain kotioperaattorin verkossa**

     Päivitykset ladataan aina kotioperaattorin verkossa. Kun vierailet jonkin toisen operaattorin verkossa, päivitykset keskeytetään. Suosittelemme, että valitset tämän vaihtoehdon, jotta suojaustuote pysyy ajantasaisena ja kulut odotetun kaltaisina.
   - **Ei koskaan**

     Päivityksiä ei ladata, kun mobiililaajakaista on käytössä.
   - **Aina**

     Päivitykset ladataan aina käytössä olevasta verkosta riippumatta. Valitse tämä vaihtoehto, jos haluat varmistaa, että tietokoneen suojaus on aina ajan tasalla kuluista huolimatta.

4. Jos haluat päättää erikseen joka kerta, kun poistut kotioperaattorin verkosta, valitse **Kysy minulta aina, kun poistun kotioperaattorin verkosta**.

Keskeytetyt suojauspäivitykset

Suojauspäivitykset voi keskeyttää, kun käytät mobiililaajakaistaa kotioperaattorisi verkon ulkopuolella.

Tässä tapauksessa **Keskeytetty**-ilmoitus tulee näkyviin näytön oikeaan alakulmaan. Päivitykset keskeytetään, koska yhteyksien hinnat saattavat vaihdella operaattorikohtaisesti esimerkiksi eri maissa. Tätä asetusta ei ehkä kannata muuttaa, jos haluat säästää kaistanleveyttä ja mahdollisesti myös kustannuksia käyntisi aikana. Jos kuitenkin haluat muuttaa asetuksia, napsauta **Muuta**-linkkiä.

Huomautus:

Tämä toiminto on käytettävissä vain Microsoft Windows 7:ssä.

Mitä virukset ja muut haittaohjelmat ovat?

Haittaohjelmat on suunniteltu vahingoittamaan tietokonetta, käyttämään tietokonetta laittomiin tarkoituksiin huomaamattasi tai varastamaan tietoja tietokoneesta.

Haittaohjelmat voivat:

- vallata Web-selaimen,
- suunnata hakuja uudelleen,
- näyttää ei-toivottuja mainoksia,
- pitää kirjaa käytettävistä Web-sivustoista,
- anastaa henkilökohtaisia tietoja, kuten pankkitietoja,
- käyttää tietokonetta roskapostin lähettämiseen ja
- käyttää tietokonetta hyökkäyksiin toisia tietokoneita vastaan.

Haittaohjelmat voivat myös hidastaa ja epävakauttaa tietokonetta. On ehkä syytä epäillä, että tietokoneessa on *haittaohjelma*, jos tietokoneesta tulee yhtäkkiä erittäin hidas tai se kaatuu usein.

Virukset

Virukset ovat yleensä ohjelmia, jotka voivat liittää itsensä tiedostoihin ja monistaa itsensä toistuvasti. Ne voivat muuttaa ja korvata toisten tiedostojen sisältöä tavalla, joka voi vahingoittaa tietokonetta.

Virus on ohjelma, joka asentuu yleensä tietokoneeseen tietämättäsi. Tietokoneessa oleva virus yrittää monistaa itsensä. Virus:

- käyttää tietokoneen järjestelmäresursseja
- saattaa muuttaa tai vahingoittaa tietokoneen tiedostoja
- yrittää luultavasti käyttää tietokonetta muiden tietokoneiden saastuttamiseen
- saattaa aiheuttaa sen, että tietokonetta käytetään laittomiin tarkoituksiin.

Vakoiluohjelmat

Vakoiluohjelmat ovat henkilökohtaisia tietoja kerääviä ohjelmia.

Vakoiluohjelmat voivat kerätä henkilökohtaisia tietoja mukaan lukien:

- Internet-sivustoja, joita olet selannut,
- tietokoneen sähköpostiosoitteita,
- salasanoja tai
- luottokorttinumeroita.

Vakoiluohjelma asentuu melkein aina ilman lupaasi. Vakoiluohjelma saatetaan asentaa yhdessä hyödyllisen ohjelman kanssa tai siten, että sinut huijataan napsauttamaan harhaanjohtavaan ponnahdusikkunaan tulevaa vaihtoehtoa.

Rootkit-ohjelmat

Rootkit-ohjelmat ovat ohjelmia, jotka hankaloittavat muiden *haittaohjelmien* löytämistä.

Rootkit-ohjelmat piilottavat tiedostoja ja prosesseja. Yleensä ne tekevät näin piilottaakseen haitallista toimintaa tietokoneessa. Kun rootkit-ohjelma piilottaa *haittaohjelman*, ei ole helppoa huomata, että tietokoneessa on haittaohjelma.

Tässä tuotteessa on rootkit-tarkistusohjelma, joka etsii erityisesti rootkit-ohjelmia, jotta *haittaohjelma*t eivät voi piiloutua helposti.

Riskiohjelmat

Riskiohjelmia ei ole suunniteltu erityisesti tietokoneen vahingoittamiseen, mutta ne saattavat olla haitallisia väärinkäytettyinä.

Riskiohjelma ei ole suoranaisesti haittaohjelma. Riskiohjelmat suorittavat joitakin hyödyllisiä mutta mahdollisesti vaarallisia toimintoja.

Riskiohjelmia ovat esimerkiksi seuraavat:

- pikaviestinohjelmat (kuten IRC-keskusteluohjelma),
- ohjelmat, joita käytetään tiedostojen siirtämiseen tietokoneesta toiseen Internetin kautta,
- Internet-puhelinohjelmat (VoIP, *Voice Over IP -sovellukset*).
- etäkäyttöohjelmat, kuten VNC,
- pelotteluohjelmat, jotka saattavat pelotella tai huijata ostamaan väärennettyjä tietoturvaohjelmistoja, tai
- CD-tarkistukset ja kopiointisuojaukset ohittamaan suunnitellut ohjelmistot.

Jos olet tarkoituksellisesti asentanut ohjelman ja määrittänyt sen oikein, siitä ei todennäköisesti ole haittaa.

Jos riskiohjelma asennetaan tietämättäsi, sen mukana asentuu todennäköisesti haitallista sisältöä. Silloin ohjelma täytyy poistaa.

Luku

4

Tietokoneen suojaaminen haittaohjelmilta

Aiheet:

- *Tietokoneen tarkistaminen*
- *Tiedostojen jättäminen pois tarkistuksesta*
- *Eristyksen käyttäminen*
- *Mikä on DeepGuard?*

Virusten ja vakoiluohjelmien tarkistus suojaa tietokonetta ohjelmilta, jotka saattavat anastaa henkilötietoja, vioittaa tietokonetta tai käyttää sitä laittomiin tarkoituksiin.

Oletusarvon mukaan kaikki haittaohjelmatyypit käsitellään heti, kun ne löytyvät, jotta ne eivät voi aiheuttaa harmia.

Virus- ja vakoiluohjelmantarkistus tarkistaa oletusarvoisesti paikalliset kiintolevyt, kaikki siirrettävät tietovälineet (kuten kannettavat asemat ja CD-levyt) ja ladatun sisällön automaattisesti. Voit määrittää sen tarkistamaan myös sähköpostit automaattisesti.

Virus- ja vakoiluohjelmantarkistus myös tarkkailee tietokonetta sellaisten muutosten varalta, jotka saattavat olla merkki *haittaohjelmasta*. Jos vaarallisia järjestelmämuutoksia, kuten järjestelmäasetusten tai tärkeiden järjestelmäprosessien muutosyrityksiä, ilmenee, DeepGuard pysäyttää tämän ohjelman suorittamisen, sillä se on todennäköisesti *haittaohjelma*.

Tietokoneen tarkistaminen

Kun virus- ja vakoiluohjelmatarkistus on käytössä, se etsii tietokoneestasi haitallisia tiedostoja automaattisesti. Voit myös tarkistaa tiedostoja manuaalisesti ja määrittää ajoitettuja tarkistuksia.

On suositeltavaa pitää virus- ja vakoiluohjelmatarkistus käytössä koko ajan. Tarkista tiedostot manuaalisesti, kun haluat varmistaa, että tietokoneessasi ei ole haitallisia tiedostoja, tai haluat tarkistaa tosiaikaisesta tarkistuksesta pois jätettyjä tiedostoja.

Kun määrität ajoitetun tarkistuksen, virus- ja vakoiluohjelmatarkistus poistaa haitalliset tiedostot tietokoneeltasi määritettyinä aikoina.

Tiedostojen automaattinen tarkistus

Käytönaikainen tarkistus suojaa tietokonetta tarkistamalla kaikki tiedostot, kun niitä otetaan käyttöön, ja estämällä sellaisten tiedostojen käytön, jotka sisältävät *haittaohjelmia*.

Kun tietokoneesi yrittää käyttää tiedostoa, tosiaikainen tarkistus tarkistaa tiedoston haittaohjelmien varalta ennen kuin tietokone saa luvan käyttää tiedostoa. Jos tosiaikainen tarkistus havaitsee haitallista sisältöä, se asettaa tiedoston karanteenin, jotta se ei ehdi aiheuttaa haittaa.

Vaikuttaako tosiaikainen tarkistus tietokoneen suorituskykyyn?

Yleensä tarkistusprosessia ei huomaa, koska se vie vain vähän aikaa ja järjestelmäresursseja. Käytönaikaiseen tarkistukseen kuluva aika ja järjestelmäresurssien määrä riippuu esimerkiksi tiedoston sisällöstä, sijainnista ja tyypistä.

Tiedostot, joiden tarkistamiseen menee kauemmin:

- Siirrettävillä tallennusvälineillä, kuten CD-levyillä, DVD-levyillä ja kannettavilla USB-asemilla, olevat tiedostot.
- Pakatut tiedostot, kuten *.zip* -tiedostot.

  Huomautus: Pakattuja tiedostoja ei oletusarvoisesti tarkisteta.

Käytönaikainen tarkistus voi hidastaa tietokonetta, jos:

- tietokoneesi ei ole järjestelmävaatimusten mukainen
- käytät useita tiedostoja samanaikaisesti. Kun esimerkiksi avaat hakemiston, jossa on paljon tiedostoja, jotka on tarkistettava.

Käytönaikaisen tarkistuksen ottaminen käyttöön ja poistaminen käytöstä

Pidä tosiaikainen tarkistus päällä, jotta *haittaohjelmat* voidaan pysäyttää, ennen kuin ne vahingoittavat tietokonetta.

Voit ottaa tosiaikaisen tarkistuksen käyttöön tai poistaa sen käytöstä seuraavasti:

1. Valitse pääsivulta **Tila**.
2. Valitse **Muuta asetuksia tällä sivulla**.

   Huomautus: Suojausominaisuuksien sammuttaminen edellyttää järjestelmänvalvojan oikeuksia.

3. Ota **Virus- ja vakoiluohjelmatarkistus** käyttöön tai poista se käytöstä.
4. Valitse **Sulje**.

Haitallisten tiedostojen automaattinen käsittely

Tosiaikainen tarkistus voi käsitellä haitalliset tiedostot automaattisesti ilman käyttäjälle esitettäviä kysymyksiä.

Voit määrittää tosiaikaisen tarkistuksen käsittelemään haitalliset tiedostot automaattisesti seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Tietokoneen suojaus** > **Virus- ja vakoiluohjelmatarkistus**.
3. Valitse **Käsittele haitalliset tiedostot automaattisesti**.

Jos et valitse haitallisten tiedostojen automaattista käsittelyvaihtoehtoa, tosiaikainen tarkistus kysyy aina erikseen toimintoa, joka sen löytämille haitallisille tiedostoille tehdään.

Vakoiluohjelmien käsitteleminen

Virus- ja vakoiluohjelmatarkistus estää vakoiluohjelman suorittamisen heti, kun sitä yritetään käynnistää.

Tuote estää vakoiluohjelman ennen sen käynnistymistä ja kysyy käyttäjältä, mitä vakoiluohjelmalla pitäisi tehdä.

Kun vakoiluohjelma havaitaan, valitse jokin seuraavista toiminnosta:

Suoritettava toiminto	Mitä vakoiluohjelmalle tapahtuu
Käsittele automaattisesti	Tuote päättää suoritettavan toiminnon automaattisesti havaitun vakoiluohjelman perusteella.
Aseta vakoiluohjelma karanteeniin	Vakoiluohjelma siirretään karanteeniin, jossa se ei voi vahingoittaa tietokonetta.
Poista vakoiluohjelma	Kaikki vakoiluohjelmaan liittyvät tiedostot poistetaan tietokoneelta.
Estä vain vakoiluohjelma	Vakoiluohjelman käyttö estetään, mutta se jää tietokoneeseen.
Jätä vakoiluohjelma pois tarkistuksesta	Salli vakoiluohjelman suoritus ja jätä se jatkossa pois tarkistuksista.

Käsittele riskiohjelma

Virus- ja vakoiluohjelmatarkistus estää riskiohjelman heti, kun sitä yritetään käynnistää.

Ennen riskiohjelman käynnistymistä tuote torjuu sen ja kysyy sinulta, miten haluat käsitellä ohjelmaa.

Valitse jokin seuraavista toiminnoista, kun riskiohjelma löydetään:

Suoritettava toiminto	Mitä Riskiohjelmallelle tapahtuu
Estä vain riskiohjelma	Riskiohjelman käyttö estetään, mutta se jää tietokoneelle.
Eristä riskiohjelma	Riskiohjelma siirretään karanteeniin, jossa se ei voi vahingoittaa tietokonetta.
Poista riskiohjelma	Kaikki riskiohjelmaan liittyvät tiedostot poistetaan tietokoneelta.
Jätä riskiohjelma pois tarkistuksesta	Salli riskiohjelman suoritus ja jätä se jatkossa pois tarkistuksista.

Poista seurantaevästeet automaattisesti

Poistamalla seurantaevästeet estät Web-sivustoja selvittämästä, mitä Internet-sivustoja käytät.

Seurantaevästeet ovat pienikokoisia tiedostoja, joihin Web-sivustot voivat tallentaa käyttämäsi Internet-sivustot. Voit estää evästeiden tallentamisen tietokoneellesi toimimalla seuraavien ohjeiden mukaan.

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Tietokoneen suojaus** > **Virus- ja vakoiluohjelmatarkistus**.
3. Valitse **Poista seurantaevästeet**.
4. Valitse **OK**.

Tiedostojen manuaalinen tarkistus

Voit tarkistaa tiedostoja manuaalisesti esimerkiksi, kun kytket tietokoneeseen ulkoisen laitteen ja haluat varmistaa, ettei siinä ole haittaohjelmia.

Manuaalisen tarkistuksen käynnistäminen

Voit tarkistaa koko tietokoneen, etsiä tietyntyyppistä *haittaohjelmaa* tai tarkistaa tietyn sijainnin.

Jos epäilet, että tietokoneessa on tietyntyyppinen *haittaohjelma*, voit etsiä vain kyseisen tyyppistä ohjelmaa. Jos epäilet, että tietokoneen tietyssä sijainnissa on haittaohjelmia, voit tarkistaa vain kyseisen osan. Nämä tarkistukset ovat huomattavasti nopeampia kuin koko tietokoneen tarkistus.

Voit aloittaa manuaalisen tarkistuksen seuraavasti:

1. Napsauta pääsivulla **Tarkista**-kohdan alla olevaa nuolta.

   Tarkistusasetukset ovat näkyvissä.
2. Valitse tarkistustyyppi.

   Valitsemalla **Muuta tarkistusasetuksia** voit optimoida sen, miten manuaalinen tarkistus etsii tietokoneesta viruksia ja haitallisia sovelluksia.
3. Jos olet valinnut **Valitse tarkistettavat kohteet** -vaihtoehdon, näkyviin tulee ikkuna, jossa voit valita tarkistettavan sijainnin.
   Näyttöön tulee **Ohjattu tarkistus** -ikkuna.

Tarkistustyypit

Voit tarkistaa koko tietokoneen, etsiä tietyntyyppistä haittaohjelma tai tarkistaa tietyn sijainnin.

Seuraavassa on luettelo erilaisista tarkistustyypeistä:

Tarkistustyyppi	Tarkistettavat kohteet	Milloin tyyppiä käytetään
Virus- ja vakoiluohjelmatarkistus	Tietokoneen osat virusten, vakoiluohjelmien ja riskiohjelmien varalta	Tällainen tarkistus on paljon nopeampi kuin täysi tarkistus. Se kohdistaa haun vain niihin järjestelmän osiin, jotka sisältävät asennettuja ohjelmatiedostoja. Tätä tarkistustyyppiä suositellaan, jos haluat tarkistaa nopeasti, onko tietokone puhdas, koska se pystyy löytämään ja poistamaan kaikki aktiiviset haittaohjelmat tietokoneesta tehokkaasti.
Täysi tietokoneen tarkistus	Koko tietokone (sisäiset ja ulkoiset kiintolevyt) virusten, vakoiluohjelmien ja riskiohjelmien varalta	Kun haluat olla täysin varma, ettei tietokoneessa ole haittaohjelmaa tai riskiohjelmaa. Tämän tarkistuksen tekeminen kestää pisimpään. Siinä yhdistyy nopea haittaohjelmien tarkistus ja kiintolevyn tarkistus. Se tarkistaa myös kohteet, jotka rootkit-ohjelma on mahdollisesti piilottanut.
Valitse tarkistettavat kohteet...	Tietty tiedosto, kansio tai asema virusten, vakoiluohjelmien ja riskiohjelmien varalta	Kun epäilet, että tietyssä sijainnissa voi olla haittaohjelma. Sijainnissa voi esimerkiksi olla mahdollisista vaarallisista lähteistä, kuten vertaisverkoista, ladattuja tiedostoja. Tarkistukseen käytettävä aika määräytyy tarkistettavan kohteen koon perusteella. Tarkistus tehdään nopeasti, jos

Tarkistustyyppi	Tarkistettavat kohteet	Milloin tyyppiä käytetään
		tarkistat esimerkiksi kansion, jossa on vain muutama pieni tiedosto.
Rootkit-ohjelmatarkistus	Tärkeät järjestelmäkohteet, joissa epäilyttävä kohde voi aiheuttaa tietoturvaongelmia. Tarkistaa piilotetut tiedostot, kansiot, asemat ja prosessit.	Kun epäilet, että tietokoneeseen on saatettu asentaa rootkit-ohjelma. Jos tietokoneessa on esimerkiksi havaittu äskettäin haittaohjelma ja haluat, varmistaa, että se ei asentanut rootkit-ohjelmaa.

Tarkistaminen Windowsin Resurssienhallinnassa

Voit tarkistaa levyjä, kansioita ja tiedostoja *virusten*, *vakoiluohjelmien* ja *riskiohjelmien* varalta Windowsin Resurssienhallinnassa.

Voit tarkistaa levyn, kansion tai tiedoston seuraavasti:

1. Siirrä hiiren osoitin tarkistettavan levyn, kansion tai tiedoston päälle ja napsauta hiiren oikeaa painiketta.
2. Valitse **Tarkista kansiot virusten varalta** -vaihtoehto valikosta, joka avautuu, kun napsautat hiiren kakkospainiketta. (Valinnan nimi riippuu siitä, tarkistatko levyn, kansion vai tiedoston.) **Ohjattu tarkistus**-ikkuna tulee näkyviin ja tarkistus alkaa.

Jos sovellus löytää *viruksen* tai *vakoiluohjelman*, **Ohjattu tarkistus** opastaa viruksen poistossa.

Tarkistettavien tiedostojen valitseminen

Voit valita tiedostotyypit, jotka haluat tarkistaa *virusten* ja *vakoiluohjelmien* varalta manuaalisissa ja ajoitetuissa tarkistuksissa.

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Muut asetukset** > **Manuaalinen tarkistus**.
3. Valitse **Tarkistusasetukset**-kohdassa jokin seuraavista asetuksista:

Tarkista vain tunnetut tiedostotyypit	Vain todennäköisimmin tartuntoja saaneiden tiedostotyyppien tarkistaminen. Tällaisia ovat esimerkiksi ohjelmatiedostot. Jos valitset tämän vaihtoehdon, tarkistus myös nopeutuu. Seuraavilla tiedostotunnisteilla merkityt tiedostot tarkistetaan: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` ja `.hqx`.
Tarkista pakatut tiedostot	Voit tarkistaa arkistotiedostot ja -kansiot seuraavasti.
Käytä kehittynyttä heuristiikkaa	Käyttää kaikkea käytettävissä olevaa heuristiikkaa tarkistuksen aikana, jotta uudet tai tuntemattomat haittaohjelmat löytyvät paremmin. **Huomautus:** Jos valitset tämän vaihtoehdon, tarkistus kestää pidempään ja voi aiheuttaa enemmän vääriä hälytyksiä (raportoi haitalliset tiedostot epäilyttäviksi).

4. Valitse **OK**.

Huomautus: Pois jätettävien kohteiden luettelossa olevia tiedostoja ei tarkisteta, vaikka valitsisit ne tarkistettavaksi tässä.

Toimintaohjeet haitallisten tiedostojen löytyessä

Voit valita, miten löydetyt haitalliset tiedostot käsitellään.

Voit valita manuaalisessa tarkistuksessa löydetyn haitallisen sisällön käsittelytavan seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Muut asetukset** > **Manuaalinen tarkistus**.
3. Valitse kohdassa **Kun virus tai vakoiluohjelma löytyy** jokin seuraavista asetuksista:

Valinta	Kuvaus
Kysy minulta (oletusasetus)	Voit valita aina erikseen toiminnon, joka manuaalisessa tarkistuksessa löydetylle kohteelle tehdään.
Puhdista tiedostot	Tuote yrittää puhdistaa automaattisessa tarkistuksessa havaitut tartunnan saaneet tiedostot automaattisesti. **Huomautus:** Jos tuote ei pysty puhdistamaan tartunnan saanutta tiedostoa, se asetetaan karanteeniin (paitsi, jos se sijaitsee verkossa tai siirrettävässä asemassa), jotta se ei pääse vahingoittamaan tietokonetta.
Eristä tiedostot	Tuota siirtää manuaalisessa tarkistuksessa havaitut haitalliset tiedostot karanteeniin, missä ne eivät voi vahingoittaa tietokonetta.
Poista tiedostot	Tuote poistaa kaikki manuaalisessa tarkistuksessa havaitut haitalliset tiedostot.
Vain raportti	Tuote jättää kaikki manuaalisessa tarkistuksessa havaitut haitalliset tiedostot ennalleen ja tallentaa vain tiedon niistä tarkistusraporttiin. **Huomautus:** Jos reaaliaikainen tarkistus on poistettu käytöstä, mikä tahansa haittaohjelma voi edelleen vahingoittaa tietokonetta, jos valitset tämän vaihtoehdon.

Huomautus: Ajoitetun tarkistuksen aikana havaitut haitalliset tiedostot puhdistetaan automaattisesti.

Tarkistuksen ajoittaminen

Voit varmistaa tietokoneen pysymisen puhtaana haittaohjelmista määrittämällä tietokoneen etsimään ja poistamaan virukset ja muut haitalliset sovellukset automaattisesti, kun et käytä tietokonetta, tai suorittamaan tarkistuksen säännöllisesti.

Voit ajoittaa tarkistuksen seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Muut asetukset** > **Ajoitettu tarkistus**.
3. Ota **Ajoitettu tarkistus** käyttöön.
4. Valitse, milloin haluat tarkistuksen alkavan.

Valinta	Kuvaus
Päivittäin	Tarkista tietokone joka päivä.
Viikoittain	Tarkista tietokone valittuina viikonpäivinä. Valitse päivät luettelosta.
Kuukausittain	Tarkista tietokone valittuina kuukaudenpäivinä. Voit valita päivät seuraavasti: 1. Valitse jokin Päivä -vaihtoehdoista. 2. Valitse kuukaudenpäivä luettelosta valitun päivän vierestä.

5. Valitse, milloin haluat tarkistuksen alkavan valittuina päivinä.

Valinta	Kuvaus
Aloitusaika	Aloita tarkistus määritettynä aikana.
Kun tietokone on käyttämättä	Aloita tarkistus, kun tietokone on ollut käyttämättä määritetyn ajan.

Ajoitetuissa tarkistuksissa käytetään manuaalisen tarkistuksen asetuksia. Ainoat poikkeukset ovat, että ajoitetussa tarkistuksessa tarkistetaan aina arkistot ja haitalliset tiedostot puhdistetaan automaattisesti.

Sähköpostin tarkistus

Sähköpostin tarkistus suojaa tietokonettasi vastaanottamiesi sähköpostiviestien sisältämiltä haitallisilta liitetiedostoilta .

Virus- ja vakoiluohjelmatarkistuksen on oltava käytössä, jotta sähköpostin virustarkistuksen voisi ottaa käyttöön.

Voit ottaa sähköpostin tarkistuksen käyttöön seuraavasti:

1. Valitse pääsivulta Asetukset.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse Tietokoneen suojaus > Virus- ja vakoiluohjelmatarkistus.
3. Valitse Poista haitalliset sähköpostiliitteet.
4. Valitse OK.

Milloin sähköpostiviestit ja liitteet tarkistetaan?

Virus- ja vakoiluohjelmatarkistus voi poistaa haitallista sisältöä myös vastaanottamistasi sähköposteista.

Virus- ja vakoiluohjelmatarkistus poistaa haitalliset sähköpostiviestit, joita vastaanotetaan sähköpostiohjelmilla, kuten Microsoft Outlookilla ja Outlook Expressillä, Microsoft Maililla tai Mozilla Thunderbirdillä. Se tarkistaa salaamattomat sähköpostiviestit ja liitteet aina, kun sähköpostiohjelma vastaanottaa ne postipalvelimelta, joka käyttää POP3-protokollaa.

Virus- ja vakoiluohjelmatarkistus ei voi tarkistaa sähköpostiviestejä Web-sähköpostijärjestelmistä tai selaimessa käytettävistä sähköpostisovelluksista, kuten Hotmailista, Yahoo! mailista tai Gmailista. Vaikka et määritä haitallisia liitteitä poistettavaksi tai käytät Web-sähköpostia, tietokoneesi on silti suojattu *viruksilta*. Kun avaat sähköpostiliitteen, tosiaikainen tarkistustoiminto poistaa kaikki haitalliset liitteet, ennen kuin ne ehtivät aiheuttaa vahinkoa.

Huomautus: Tosiaikainen tarkistus suojaa vain oman tietokoneesi, se ei suojaa ystäviäsi. Tosiaikainen tarkistus ei tarkiste liitetiedostoja, ellet avaa niitä. Jos siis käytät Web-sähköpostia ja välität viestin ystävällesi ennen viestin liitteiden avaamista, saatat ehkä välittää ystävällesi viruksen sisältävän viestin.

Tarkistustulosten tarkasteleminen

Virus- ja vakoiluohjelmahistoriassa näkyvät kaikki tuotteen löytämät haitalliset tiedostot.

Joskus tuote ei pysty tekemään valitsemaasi toimintoa haitalliselle kohteelle. Jos esimerkiksi valitset tiedostot puhdistettavaksi mutta tiedoston puhdistaminen ei onnistu, tuote siirtää sen karanteeniin. Näet tällaiset tapahtumat virus- ja vakoiluohjelmahistoriasta.

Voit tarkastella historiaa seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Tietokoneen suojaus** > **Virus- ja vakoiluohjelmatarkistus**.
3. Valitse **Näytä poistohistoria**.

Virus- ja vakoiluohjelmahistoriassa näkyy seuraavat tiedot:

- Haitallisen tiedoston löytymispäivämäärä ja -aika,
- Haittaohjelman nimi ja sijainti tietokoneella.
- Suoritettu toiminto.

Tiedostojen jättäminen pois tarkistuksesta

Osa tiedostoista ja sovelluksista voidaan joskus jättää pois tarkistuksesta. Pois jätettyjä kohteita ei tarkisteta, ellet poista niitä pois jätettävien kohteiden luettelosta

Huomautus: Tosiaikaisella ja manuaalisella tarkistuksella on omat pois jätettävien kohteiden luettelot. Jos esimerkiksi määrität tiedoston jätettäväksi pois tosiaikaisesta tarkistuksesta, se tarkistetaan silti manuaalisessa tarkistuksessa, ellet määritä sitä jätettäväksi pois erikseen.

Tiedostotyyppien ohittaminen

Kun jätät tiedostoja pois tarkistuksesta niiden tiedostotyypin perusteella, kyseisen tiedostotunnisteen tiedostoja ei tarkisteta haitallisen sisällön varalta.

Voit lisätä tai poistaa pois jätettävän tiedostotyypin seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse, haluatko jättää tiedostotyypin tiedostot pois tosiaikaisesta vai manuaalisesta tarkistuksesta:
   - Valitse **Tietokoneen suojaus** > **Virus- ja vakoiluohjelmatarkistus**, jos haluat jättää tiedostotyypin pois reaaliaikaisesta tarkistuksesta.
   - Valitse **Muut asetukset** > **Manuaalinen tarkistus**, jos haluat jättää tiedostotyypin pois manuaalisesta tarkistuksesta.
3. Valitse **Jätä tiedostot pois tarkistuksesta**.
4. Voit ohittaa tiedostotyypin seuraavasti:
   a) Valitse **Tiedostotyypit**-välilehti.
   b) Valitse **Älä tarkista tiedostoja, joiden pääte on**.
   c) Kirjoita tiedostotunniste, joka määrittää ohitettavien tiedostojen tyypin,**Lisää**-painikkeen vieressä olevaan kenttään.

Jos haluat määrittää tiedostot, joilla ei ole mitään tunnistetta, kirjoita ".". Käytä yleismerkkiä "?", jos haluat sen vastaavan mitä tahansa yhtä merkkiä, tai "*", jos haluat sen vastaavan mitä tahansa merkkejä.

Jos haluat ohittaa esimerkiksi suoritettavat tiedostot, kirjoita kenttään exe.

d) Valitse **Lisää**.

5. Toista edellinen vaihe muille tunnisteille, jotka haluat ohittaa virustarkistuksen aikana.
6. Valitse **OK,** jotta **Tarkistuksessa ohitettavat** -valintaikkuna suljetaan.
7. Valitse **OK**.

Valittujen tiedostotyyppien tiedostot jätetään pois tulevista tarkistuksista.

Tiedostojen ohittaminen sijainnin mukaan

Kun jätät tiedostoja pois tarkistuksesta niiden sijainnin perusteella, määrittämissäsi asemissa tai kansioissa olevia tiedostoja ei tarkisteta haitallisen sisällön varalta.

Voit lisätä tai poistaa pois jätettävän tiedostosijainnin seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse, haluatko jättää sijainnin tiedostot pois tosiaikaisesta vai manuaalisesta tarkistuksesta:
   - Valitse **Tietokone** > **Virus- ja vakoiluohjelmatarkistus**, jos haluat jättää sijainnin tiedostot pois tosiaikaisesta tarkistuksesta.
   - Valitse **Tietokone** > **Manuaalinen tarkistus**, jos haluat jättää sijainnin tiedostot pois manuaalisesta tarkistuksesta.
3. Valitse **Jätä tiedostot pois tarkistuksesta**.
4. Voit ohittaa tiedoston, aseman tai kansion seuraavasti:
   a) Valitse **Kohteet**-välilehti.
   b) Valitse **Älä tarkista kohteita (tiedostoja, kansioita...)**.
   c) Valitse **Lisää**.
   d) Valitse tiedosto, asema tai kansio, jonka haluat virustarkistuksen ohittavan.

      Huomautus: Jotkin asemat saattavat olla siirrettäviä asemia, esimerkiksi CD-, DVD- tai verkkoasemia. Verkkoasemia ja tyhjiä siirrettäviä asemia ei voi ohittaa.

   e) Valitse **OK**.
5. Jos haluat ohittaa muita tiedostoja, asemia tai kansioita virustarkistuksessa, toista edellä kerrotut toimet.
6. Valitse **OK,** jotta **Tarkistuksessa ohitettavat** -valintaikkuna suljetaan.
7. Valitse **OK**.

Valitut tiedostot, asemat ja kansiot jätetään pois tulevista tarkistuksista.

Ohitettujen sovellusten tarkasteleminen

Voit tarkastella sovelluksia, jotka on jätetty pois tarkistuksesta, ja poistaa pois jätettyjen kohteiden luettelosta ne kohteet, jotka haluat tarkistaa tulevaisuudessa.

Jos tosiaikaisessa tai manuaalisessa tarkistuksessa havaitaan vakoilu- tai riskiohjelman tavoin toimiva sovellus, mutta tiedät kyseisen sovelluksen olevan turvallinen, voit jättää sen pois tarkistuksesta, jolloin tuote ei enää varoita siitä.

Huomautus: Jos sovellus toimii viruksen tai muun haittaohjelman tavoin, sitä ei voi jättää pois tarkistuksesta.

Et voi määrittää pois jätettäviä sovelluksia suoraan. Voit lisätä uusia sovelluksia pois jätettävien kohteiden luetteloon vain määrittämällä ne pois jätettäväksi tarkistuksen yhteydessä.

Voit tarkastella tarkistuksessa ohitettavia sovelluksia seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse, haluatko tarkastella sovelluksia, jotka on jätetty pois tosiaikaisesta tarkistuksesta, vai sovelluksia, jotka on jätetty pois manuaalisesta tarkistuksesta:
   - Valitse **Tietokone** > **Virus- ja vakoiluohjelmatarkistus**, jos haluat tarkastella sovelluksia, jotka on jätetty pois tosiaikaisesta tarkistuksesta.
   - Valitse **Tietokone** > **Manuaalinen tarkistus**, jos haluat tarkastella sovelluksia, jotka on jätetty pois manuaalisesta tarkistuksesta.
3. Valitse **Jätä tiedostot pois tarkistuksesta**.
4. Valitse **Sovellukset** -välilehti.

   Huomautus: Vain vakoiluohjelma- ja riskiohjelmasovellukset voidaan ohittaa. Viruksia ei voi ohittaa.

5. Toimi seuraavasti, jos haluat tarkistaa pois jätetyn sovelluksen uudelleen:
   a) Valitse sovellus, jonka haluat sisällyttää tarkistukseen.
   b) Valitse **Poista**.
6. Valitse **OK,** jotta **Tarkistuksessa ohitettavat** -valintaikkuna suljetaan.
7. Valitse **OK**.

Eristyksen käyttäminen

Eristysvarasto on turvavarasto tiedostoille, jotka voivat olla haitallisia.

Eristetyt tiedostot eivät voi levitä tai vahingoittaa tietokonetta.

Voit eristää *haittaohjelmia*, *vakoiluohjelmia* ja *riskiohjelmia* ja tehdä siten niistä harmittomia. Voit myöhemmin palauttaa sovelluksia tai tiedostoja eristyksestä, jos tarvitset niitä.

Jos et tarvitse eristettyä kohdetta, voit poistaa sen. Kohteen poisto eristyksestä poistaa sen tietokoneesta pysyvästi.

- Voit poistaa eristetyt *haittaohjelma*t.
- Useimmissa tapauksissa voit poistaa eristetyt *vakoiluohjelma*t. Eristetty *vakoiluohjelma* voi joskus olla osa laillista tietokoneohjelmaa, ja sen poisto voi estää varsinaisen ohjelman toiminnan. Jos haluat säilyttää ohjelman tietokoneessa, voit palauttaa eristetyn *vakoiluohjelma*n.
- Eristetty *riskiohjelma* voi olla laillinen tietokoneohjelma. Jos olet asentanut ja määrittänyt ohjelman itse, voit palauttaa sen eristyksestä. Jos *riskiohjelma* on asennettu tietämättäsi, siinä on todennäköisesti haitallista sisältöä, ja se tulisi poistaa.

Eristettyjen kohteiden tarkasteleminen

Voit tarkastella lisätietoja eristetyistä kohteista.

Voit tarkastella eristettyjen kohteiden tietoja seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Tietokoneen suojaus** > **Virus- ja vakoiluohjelmatarkistus**.
3. Valitse **Näytä karanteeni**.
   Karanteeniin asetettujen kohteiden kokonaismäärä näkyy **Karanteeni**-sivulla.
4. Jos haluat tarkastella yksityiskohtaisia tietoja karanteeniin asetetuista kohteista, valitse **Tiedot**.

   Voit lajitella sisällön joko haittaohjelman nimen tai tiedostopolun mukaan.

   Näkyviin tulee luettelo ensimmäisistä 500 kohteesta. Luettelossa näkyvät eristetyt kohteet, niidet nimet ja polku, johon tiedostot on asennettu.
5. Voit tarkastella karanteeniin asetetun kohteen lisätietoja napsauttamalla ⓘ-kuvaketta kohteen vieressä **Tila**-sarakkeessa.

Eristettyjen kohteiden palauttaminen

Voit palauttaa tarvitsemasi eristetyt kohteet.

Voit palauttaa sovelluksia tai tiedostoja eristyksestä, jos tarvitset niitä. Älä palauta kohteita, jollet ole varma, että kohteet eivät ole vaarallisia. Palautetut kohteet palaavat alkuperäiseen sijaintiinsa tietokoneessa.

Eristettyjen kohteiden palauttaminen:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Tietokoneen suojaus** > **Virus- ja vakoiluohjelmatarkistus**.
3. Valitse **Näytä karanteeni**.
4. Valitse eristykseen asetetut kohteet, jotka haluat palauttaa.
5. Valitse **Palauta**.

Mikä on DeepGuard?

DeepGuard analysoi tiedostojen sisällön ja sovellusten toiminnan ja valvoo sovelluksia, joihin ei luoteta.

DeepGuard estää uudet ja tunnistamattomat *virukset*, *madot* ja muut haitalliset sovellukset, jotka yrittävät muuttaa tietokonetta, ja estää epäilyttäviä sovelluksia käyttämästä Internetiä.

Kun DeepGuard havaitsee uuden sovelluksen, joka yrittää tehdä mahdollisesti haitallisia muutoksia järjestelmään, se sallii sovelluksen suorituksen turvallisella vyöhykkeellä. Tällöin sovellus ei voi vahingoittaa tietokonetta. DeepGuard analysoi, mitä muutoksia sovellus yrittää tehdä, ja päättää sen perusteella, miten todennäköisesti kyseessä on *haittaohjelma*. Jos sovellus on todennäköisesti *haittaohjelma*, DeepGuard estää sen.

DeepGuard tunnistaa muun muassa seuraavat mahdollisesti haitalliset järjestelmämuutokset:

- järjestelmän asetusten (Windowsin rekisteritietojen) muutokset
- yritykset poistaa käytöstä tärkeitä järjestelmäohjelmia, kuten suojausohjelmia (esimerkiksi tämä tuote) ja
- yritykset muokata tärkeitä järjestelmätiedostoja.

DeepGuardin ottaminen käyttöön tai poistaminen käytöstä

Pidä DeepGuard käytössä, jotta epäilyttävät sovellukset eivät pääse tekemään mahdollisesti haitallisia muutoksia tietokoneeseen

Jos käyttöjärjestelmä on Windows XP, varmista, että siihen on asennettu Service Pack 2, ennen kuin otat DeepGuardin käyttöön.

Voit ottaa DeepGuardin käyttöön tai poistaa sen käytöstä seuraavasti:

1. Valitse pääsivulta **Tila**.
2. Valitse **Muuta asetuksia tällä sivulla**.

   Huomautus: Suojausominaisuuksien sammuttaminen edellyttää järjestelmänvalvojan oikeuksia.

3. Ota **DeepGuard** käyttöön tai poista se käytöstä.
4. Valitse **Sulje**.

Salli DeepGuardin torjumia sovelluksia

Voit määrittää, mitkä sovellukset DeepGuard sallii ja mitkä se estää.

DeepGuard saattaa estää myös turvallisen sovelluksen suorittamisen, vaikka tunnet sovelluksen ja tiedät sen turvalliseksi. Näin käy, kun sovellus yrittää tehdä järjestelmämuutoksia, jotka saattavat olla vahingollisia. Olet myös ehkä saattanut epähuomiossa estää sovelluksen suorittamisen, kun DeepGuard on kysynyt sitä kohoikkunassa.

Voit sallia DeepGuardin estämän sovelluksen suorittamisen seuraavasti:

1. Valitse pääsivulla **Työkalut**.
2. Valitse **Sovellukset**.
   Seuratut sovellukset -luettelo tulee näkyviin.
3. Etsi sovellus, jonka haluat sallia.

   Huomautus: Voit lajitella luettelon sarakeotsikoiden perusteella napsauttamalla niitä. Jos esimerkiksi haluat lajitella luettelon sallittuihin ja estettyihin ohjelmiin, napsauta **Lupa**-saraketta.

4. Valitse **Salli Lupa**-sarakkeesta.
5. Valitse **Sulje**.

DeepGuard sallii jälleen sovelluksen tehdä muutoksia järjestelmään.

DeepGuardin käyttäminen yhteensopivuustilassa

Parhaan mahdollisen suojauksen varmistamiseksi DeepGuard muokkaa suoritettavia ohjelmia tilapäisesti. Osa ohjelmista tarkistaa, ovatko ne vioittuneet tai onko niitä muokattu. Tällaiset ohjelmat eivät ehkä ole yhteensopivia tämän DeepGuardin ominaisuuden kanssa. Esimerkiksi huijausyritykset tunnistavat verkkopelit tarkistavat niitä käynnistettäessä, ettei niitä ole muokattu millään tavalla. Tällaisissa tilanteissa voit ottaa käyttöön yhteensopivuustilan.

Voit ottaa yhteensopivuustilan käyttöön seuraavasti:

1. Valitse pääsivulta **Asetukset**.

   Huomautus: Asetusten muuttaminen edellyttää järjestelmänvalvojan oikeuksia.

2. Valitse **Tietokoneen suojaus** > **DeepGuard**.
3. Valitse **Käytä yhteensopivuustilaa**.
4. Valitse **OK**.

Toimenpiteet epäilyttävän toiminnan varoituksen tullessa näkyviin

DeepGuard seuraa sovelluksia, joihin ei luoteta. Jos seurattu sovellus yrittää käyttää Internetiä, tehdä muutoksia järjestelmään tai toimii muuten epäilyttävästi, DeepGuard estää sen.

Jos valitset DeepGuard-asetukseksi **Varoita epäilyttävästä toiminnasta**, DeepGuard ilmoittaa käyttäjälle, kun se havaitsee mahdollisesti haitallisen sovelluksen tai kun käyttäjä käynnistää sovelluksen, joka on luokiteltu epäilyttäväksi sovellukseksi.

Voit päättää seuraavasti, mitä haluat tehdä DeepGuardin estämälle sovellukselle:

1. Katso lisätietoja ohjelmasta valitsemalla **Tiedot**.
   Tieto-osiosta näet
   - sovelluksen sijainnin
   - sovelluksen luokituksen Real-time Protection Network -verkossa
   - sovelluksen yleisyystiedot.
2. Päätä, haluatko määrittää DeepGuardin estämän sovelluksen luotetuksi:
   - Jos et halua estää sovellusta, valitse **Luotan sovellukseen. Anna sen jatkaa**.

     Sovellus on todennäköisesti turvallinen seuraavissa tilanteissa:
     - DeepGuard on estänyt sovelluksen jonkin itse tekemäsi toimen seurauksena.
     - Tunnistat sovelluksen.
     - Olet saanut sovelluksen luotetusta lähteestä.
   - Jos haluat pitää sovelluksen estettynä, valitse **En luota sovellukseen. Pidä se estettynä**.

     Sovellus on todennäköisesti haitallinen seuraavissa tilanteissa:
     - Sovellus ei ole yleisesti käytetty.
     - Sovelluksella ei ole tunnettua luokitusta.
     - Et tunnista sovellusta.
3. Voit lähettää epäilyttävän sovelluksen analysoitavaksi seuraavasti:
   a) Valitse **Ilmoita sovelluksesta F-Securelle**.
   Tuote näyttää lähetykseen liittyvät ehdot.
   b) Valitse **Hyväksy**, jos hyväksyt ehdot ja haluat lähettää näytetiedot.

   Suosittelemme, että lähetät näytteen seuraavissa tilanteissa:
   - DeepGuard estää sovelluksen, jonka tiedät luotettavaksi.
   - Epäilet, että sovellus on *haittaohjelma*.