Kaspersky Total Security

Käyttöopas

SOVELLUSVERSIO: 15.0 MAINTENANCE RELEASE 1

Arvoisa käyttäjä

Kiitos tuottemme valinnasta. Toivomme, että asiakirja auttaa sinua työssäsi ja tarjoaa vastauksia tähän ohjelmistotuotteeseen liittyen.

Asiakirjan muutospäivämäärä: 29.4.2015

http://www.kaspersky.fi
http://www.kaspersky.fi/support

SISÄLLYS

TIETOJA TÄSTÄ OPPAASTA

Tämä asiakirja on Kaspersky Total Security Maintenance Release 1:n (jäljempänä Kaspersky Total Security) käyttäjäopas.

Kaspersky Total Securityn oikea käyttö edellyttää, että tunnet käyttämäsi käyttöjärjestelmän käyttöliittymän, hallitset tärkeimmät järjestelmäkohtaiset tekniikat sekä osaat käyttää sähköpostia ja Internetiä.

Tämän oppaan tarkoituksena on:

- Auttaa sinua asentamaan, aktivoimaan ja käyttämään Kaspersky Total Security -ohjelmistoa.
- Auttaa sinua löytämään nopeasti tietoja Kaspersky Total Securityyn liittyvistä ongelmista.
- Kuvata, mistä saat lisätietoa sovelluksesta sekä siitä, miten voit olla yhteydessä tekniseen tukipalveluun.

TÄSSÄ OSIOSSA

TÄSSÄ OPPAASSA

Tämä asiakirja sisältää seuraavat osiot:

Sovellusta koskevien tietojen lähteet (katso sivulla 12)

Tässä osiossa kerrotaan tietolähteistä, jotka sisältävät tietoa sovelluksesta, sekä luetellaan verkkosivustoja, joissa voit keskustella sovelluksen käytöstä.

Kaspersky Total Security (katso sivulla 14)

Tämä osio kuvaa sovelluksen ominaisuudet ja tarjoaa tiivistä tietoa sovelluksen toiminnoista ja komponenteista. Saat tietää, mitä jakelupakettiin kuuluu, ja mitä palveluita sovelluksen rekisteröidyt käyttäjät voivat hyödyntää. Tässä osiossa on tietoja ohjelmisto- ja laitteistovaatimuksista, jotka tietokoneen on täytettävä sovelluksen asennusta varten.

Sovelluksen asentaminen ja poistaminen (katso sivulla 19)

Tämä osio sisältää vaiheittaiset ohjeet sovelluksen asentamiseksi ja poistamiseksi.

Sovelluksen käyttöoikeus (katso sivulla 28)

Tässä osiossa on tietoja sovelluksen aktivointiin liittyvistä avaintermeistä. Lukemalla tämän osion saat lisätietoja käyttöoikeussopimuksen tarkoituksesta sekä tavoista aktivoida sovellus ja uusia käyttöoikeutesi.

Sovelluksen ilmoitusten hallinta (katso sivulla 33)

Tässä osiossa on tietoja sovelluksen ilmoitusten hallinnasta.

Rajoitukset ja varoitukset (katso sivulla 106)

Tässä osiossa on tietoja rajoituksista, jotka eivät ole kriittisiä sovelluksen toiminnan kannalta.

Sanasto (katso sivulla 109)

Tämä osio sisältää luettelon termeistä, joita on käytetty tässä asiakirjassa, sekä niiden määritelmät.

Kaspersky Lab ZAO (katso sivulla 114)

Tämä osio sisältää tietoa Kaspersky Labista.

Tietoja kolmannen osapuolen koodista (katso sivulla 115)

Tämä osio sisältää tietoja sovelluksessa käytetystä kolmannen osapuolen ohjelmakoodista.

Tavaramerkki-ilmoitukset (katso sivulla 116)

Tämä osio sisältää luettelon kolmansien osapuolten tavaramerkeistä, joita on käytetty asiakirjassa.

Hakemisto

Tämän osion avulla voit nopeasti etsiä tarvittavat tiedot tästä asiakirjasta.

ASIAKIRJAMERKINNÄT

Tekstin ohella oppaassa on muutamia semanttisia elementtejä, joihin suosittelemme kiinnittämään erityistä huomiota. Ne sisältävät varoituksia, vinkkejä ja esimerkkejä.

Semanttisia elementtejä korostetaan asiakirjamerkinnöillä. Seuraava taulukko sisältää tietoja asiakirjan merkinnöistä ja esimerkkejä niiden käyttötarkoituksesta.

Taulukko 1. Asiakirjamerkinnät

ESIMERKKITEKSTI	ASIAKIRJAMERKINNÄN KUVAUS
Huomaa, että...	Varoitukset on korostettu punaisella värillä ja kehystetty. Varoitukset sisältävät tietoa mahdollisista ei-toivotuista toimenpiteistä, jotka voivat aiheuttaa tiedon häviämistä, laitteiden toimintahäiriöitä tai käyttöjärjestelmäongelmia.
Suosittelemme käyttämään...	Huomautukset on kehystetty. Huomautukset voivat sisältää hyödyllisiä vinkkejä, suosituksia, määrättyjä asetusarvoja tai sovelluksen käyttöön liittyviä erityistapauksia.
Esimerkki: ...	Esimerkit on annettu keltaisella taustalla ja otsikon "Esimerkki" alla.
Päivitys tarkoittaa... *Tietokannat ovat vanhentuneet* -tapahtuma esiintyy.	Seuraavat semanttiset elementit on merkitty tekstissä kursiivilla: • Uudet termit • Sovelluksen tilojen ja tapahtumien nimet
Paina **ENTER**. Paina **ALT+F4**.	Näppäimistön merkkien nimet on lihavoitu ja kirjoitettu isoilla kirjaimilla. Merkkien nimet yhdessä plus-merkin kanssa ilmaisevat näppäinyhdistelmän käyttöä. Näitä näppäimiä tulisi painaa samanaikaisesti.

ESIMERKKITEKSTI	ASIAKIRJAMERKINNÄN KUVAUS
Napsauta **OTA KÄYTTÖÖN** -painiketta.	Sovelluksen käyttöliittymäelementtien, kuten syötekenttien, valikkokohteiden ja painikkeiden nimet on esitetty lihavoituna.
Voit määrittää tehtäväaikataulun seuraavasti:	Ohjeiden johdanto-osat on kursivoitu ja niissä on nuolen merkki.
Kirjoita komentorivillä help. Tämän jälkeen näkyviin tulee seuraava viesti: Määritä päivämäärä muodossa pp:kk:vv.	Seuraavat tekstisisällöt esitetään erityisellä kirjasimella: • Komentorivin teksti • Viestin teksti, jonka sovellus tuo näytölle • Tiedot, jotka käyttäjän tulee syöttää
<Käyttäjänimi>	Muuttujat on merkitty kulmasulkeisiin. Kirjoita muuttujan sijaan vastaava arvo ilman kulmasulkeita.

SOVELLUSTA KOSKEVIEN TIETOJEN LÄHTEET

Tässä osiossa kerrotaan tietolähteistä, jotka sisältävät tietoa sovelluksesta, sekä luetellaan verkkosivustoja, joissa voit keskustella sovelluksen käytöstä.

Voit valita kysymyksen tärkeyden ja kiireellisyyden perusteella sopivimman tietolähteen.

TÄSSÄ OSIOSSA

TIETOLÄHTEITÄ ITSENÄISEEN TUTKIMUKSEEN

Voit tutkia asioita itse seuraavien tietolähteiden avulla:

- Sovellussivu Kaspersky Labin verkkosivustossa
- Sovellussivu teknisen tukipalvelun verkkosivuilla (tietokannassa)
- Online-ohje
- Dokumentaatio

Jos et löydä ratkaisua ongelmaasi, suosittelemme ottamaan yhteyttä Kaspersky Labin tekniseen tukeen (katso osiota "Tekninen puhelintuki" sivulla 99).

Kaspersky Labin verkkosivuston tietolähteiden käyttö edellyttää Internet-yhteyttä.

Sovellussivu Kaspersky Labin verkkosivustossa

Kaspersky Labin verkkosivustossa on erillinen sivu jokaiselle sovellukselle.

Tällä page (http://www.kaspersky.fi/total-security-multi-device) voit tarkastella yleistietoa sovelluksesta, sen toiminnoista ja ominaisuuksista.

Sivustossa on linkki eStore-verkkokauppaan. Sen kautta voit ostaa sovelluksen tai uusia sen käyttöoikeuden.

Sovellussivu teknisen tukipalvelun verkkosivuilla (tietokannassa)

Tietokanta on teknisen tuen verkkosivuston osa, joka sisältää Kaspersky Lab -sovellusten käyttöä koskevia ohjeita. Tietokanta sisältää aihealueittain ryhmiteltyjä lähdeartikkeleita.

Sovelluksen sivulta tietokannassa (http://support.kaspersky.com/kts) voit lukea hyödyllistä tietoa sisältäviä artikkeleita, suosituksia ja vastauksia usein kysyttyihin kysymyksiin liittyen sovelluksen ostamiseen, asennukseen ja käyttöön.

Artikkeleissa voi olla vastauksia kysymyksiin, jotka liittyvät sekä Kaspersky Total Securityyn että muihin Kaspersky Lab -sovelluksiin. Niissä voi olla myös teknisen tuen uutisia.

Online-ohje

Sovelluksen käytönaikainen ohje sisältää ohjetiedostoja.

Aihekohtainen ohje antaa tietoja sovelluksen jokaisesta ikkunasta ja luettelee sekä kuvaa vastaavat asetukset ja tehtäväluettelon.

Täysi ohje sisältää yksityiskohtaisia tietoja tietokoneen suojauksen hallinnasta, sovelluksen asetusten valinnasta ja käyttäjien tyypillisten tehtävien suorittamisesta.

Dokumentaatio

Sovelluksen käyttöopas antaa tietoja sovelluksen asennuksesta, aktivoinnista ja määrittämisestä sekä sovelluksen käyttötietoja. Asiakirja kuvaa myös sovelluksen käyttöliittymän ja tarjoaa ratkaisuja tilanteisiin, joita käyttäjä tyypillisesti kohtaa sovellusta käytettäessä.

KESKUSTELEMINEN KASPERSKY LAB -SOVELLUKSISTA FOORUMILLA

Jos kysymykseesi ei tarvita vastausta välittömästi, voit keskustella siitä Kaspersky Labin asiantuntijoiden sekä muiden käyttäjien kanssa foorumillamme (http://forum.kaspersky.com).

Tässä foorumissa voit tarkastella nykyisiä aiheita, jättää kommenttisi tai luoda uusia aiheita.

KASPERSKY TOTAL SECURITY

Tämä osio kuvaa sovelluksen ominaisuudet ja tarjoaa tiivistä tietoa sovelluksen toiminnoista ja komponenteista. Saat tietää, mitä jakelupakettiin kuuluu, ja mitä palveluita sovelluksen rekisteröidyt käyttäjät voivat hyödyntää. Tässä osiossa on tietoja ohjelmisto- ja laitteistovaatimuksista, jotka tietokoneen on täytettävä sovelluksen asennusta varten.

TÄSSÄ OSIOSSA

MITÄ UUTTA

Kaspersky Total Security sisältää seuraavat uudet ominaisuudet:

- Suosittujen verkkoselainten uusimmat versiot ovat tuettuja: suojauskomponentit (kuten virtuaalinen näppäimistö) tukevat selaimia Mozilla Firefox 32.x, 33.x, 34.x ja Google Chrome 37.x, 38.x.
- Tuki Google Chromen 64-bittisen käyttöjärjestelmän selainversiolle on lisätty.
- Sovelluksen suorituskykyä on parannettu, ja tietokoneen resurssien kulutusta on optimoitu.
- Sovellus käynnistyy nopeammin.
- Sovelluksen päivitysprosessia on parannettu.
- Järjestelmänvalvonta-komponentin toimintaa on parannettu: kryptaussuojaus on nyt käytettävissä. Jos kryptausohjelma yrittää salakirjoittaa tiedoston, Kaspersky Total Security luo tiedostosta automaattisesti varmuuskopion ennen kuin haitallinen kryptausohjelma salaa sen. Varmuuskopiot tallennetaan tilapäistiedostojen järjestelmäkansioon. Jos kryptausohjelma on salakirjoittanut tiedoston, Kaspersky Total Security palauttaa tiedoston automaattisesti varmuuskopiosta. Tietyt rajoitukset koskevat tätä toiminnallisuutta (katso osio "Rajoitukset ja varoitukset" sivulla page 106).
- Rahasuojaus-toimintoa on parannettu: Jos suojaus heikkenee Suojattua selainta käytettäessä, siitä kirjataan merkintä tapahtumalokiin. Sovellukseen on lisätty toiminto, joka tarkistaa varmenteiden avulla, että Kaspersky Lab -palveluihin sekä verkkopankkeihin ja maksupalveluihin muodostettavat yhteydet ovat turvallisia.

JAKELUPAKKAUS

Voit hankkia sovelluksen seuraavin tavoin:

- Laatikkoversiona. Jaellaan kumppaneidemme myymälöiden kautta.
- Verkkokaupasta. Kaspersky Labin ja kumppaneidemme verkkokaupoista (esim. http://www.kaspersky.fi, osio Online Shop).

Jos hankit sovelluksen laatikkoversion, jakelupakkaus sisältää seuraavat kohteet:

- Sinetöity kirjekuori, joka sisältää sovelluksen tiedostot ja dokumentaatiotiedostot
- Lyhyt käyttöopas ja aktivointikoodi
- Käyttöoikeussopimus, joka määrittelee ehdot sovelluksen käytölle

Jakelupakkauksen sisältö voi vaihdella riippuen alueesta, jossa sovellusta jaellaan.

Jos ostat Kaspersky Total Securityn verkkokaupasta, sovellus kopioidaan kaupan verkkosivustosta. Sovelluksen aktivointiin tarvittavat tiedot, aktivointikoodi mukaan lukien, lähetetään sinulle sähköpostitse, kun maksu on vastaanotettu.

TIETOJA KASPERSKY TOTAL SECURITY

Kaspersky Total Security antaa tietokoneelle kattavan suojauksen tunnettuja ja tuntemattomia uhkia, verkko- ja tietojenkalasteluhyökkäyksiä ja roskapostia vastaan. Kaspersky Total Securityyn on saatavana eri toimintoja ja suojauskomponentteja, joiden avulla tietokone voidaan suojata hyvin monipuolisesti.

Tietokoneen suojaus

Suojauskomponentit on suunniteltu suojaamaan tietokonetta tunnetuilta ja uusilta uhilta, verkkohyökkäyksiltä, huijauksilta ja roskapostilta. Kukin uhkatyyppi käsitellään yksittäisen suojauskomponentin toimesta (katso komponenttien kuvauksia jäljempänä tässä osiossa). Osat voidaan ottaa käyttöön tai poistaa käytöstä toisistaan riippumattomasti ja niiden asetukset ovat määritettävissä.

Turvallisuuskomponenttien antaman jatkuvan suojauksen lisäksi suosittelemme, että *tarkistat* tietokoneesi säännöllisesti virusten ja muiden haitallisten ohjelmien varalta. Näin toimimalla ehkäistään sellaisten haitallisten ohjelmien leviäminen, joita suojauskomponentit eivät ole havainneet esim. alhaiseksi asetetun turvallisuustason tai muun syyn vuoksi.

Sovelluksen käyttämät tietokannat ja sovellusmoduulit on *päivitettävä*, jotta Kaspersky Total Security pysyy ajan tasalla.

Määrätyt ja ajoittain suoritettavat tehtävät (kuten käyttäjän toimien jälkien poistaminen käyttöjärjestelmästä) suoritetaan käyttämällä *lisätyökaluja ja ohjattuja toimintoja*.

Seuraavat suojauskomponentit suojaavat tietokonettasi reaaliaikaisesti:

Alla on kuvaus logiikasta, jolla suojauskomponentit toimivat yhdessä silloin, kun Kaspersky Total Security on asetettu Kaspersky Labin asiantuntijoiden suosittelemaan tilaan (toisin sanoen silloin, kun käytetään sovelluksen oletusasetuksia).

Tiedoston virustorjunta

Tiedoston virustorjunta estää tietokoneen tiedostojärjestelmän tartunnan. Komponentti käynnistyy käyttöjärjestelmän käynnistyksen yhteydessä, pysyy jatkuvasti tietokoneen RAM-muistissa ja tarkistaa kaikki tietokoneesta tai kaikilta kytketyiltä asemilta avatut, tallennetut tai käynnistetyt tiedostot. Kaspersky Total Security keskeyttää kaikki yritykset päästä tiedostoon ja tarkistaa tiedoston tunnettujen virusten ja muiden haitallisten ohjelmien varalta. Pääsy tiedostoon sallitaan vain, jos tiedosto ei ole saanut tartuntaa tai jos sovellus on puhdistanut sen onnistuneesti. Jos tiedostoa ei voida jostain syystä puhdistaa, se poistetaan. Tällöin tiedoston kopio siirretään karanteeniin. Jos tartunnan saanut tiedosto on samassa sijainnissa kuin aiemmin poistettu samanniminen tiedosto, karanteeniin tallennetaan vain viimeisimmän tiedoston kopio. Kopiota aiemmasta samannimisestä tiedostosta ei tallenneta.

Sähköpostin virustorjunta

Sähköpostin virustorjunta tarkistaa tietokoneellesi tulevat ja siitä lähtevät sähköpostiviestit. Sähköposti on vastaanottajan käytettävissä vain, jos se ei sisällä vaarallisia objekteja.

Verkon virustorjunta

Verkon virustorjunta keskeyttää ja estää verkkosivujen komentosarjojen suorittamisen, jos ne uhkaavat tietokonetta. Verkon virustorjunta valvoo myös kaikkea verkkoliikennettä ja estää vaarallisten verkkosivustojen käytön.

Pikaviestinnän virustorjunta

Pikaviestinnän virustorjunta varmistaa pikaviestiohjelmien turvallisen käytön. Komponentti suojaa pikaviestintäprotokollien kautta tietokoneeseesi tulevia tietoja. Pikaviestinnän virustorjunta varmistaa pikaviestinnän eri sovellusten turvallisen käytön.

Sovellusten hallinta

Sovellusten hallinta kirjaa sovellusten suorittamat toiminnot käyttöjärjestelmässä ja hallinnoi sovellusten toimintoja niiden sovellusryhmän perusteella. Kullekin sovellusten ryhmälle on määritetty joukko sääntöjä. Nämä säännöt hallitsevat sovellusten pääsyä käyttöjärjestelmän eri resursseihin.

Palomuuri

Palomuuri varmistaa turvallisuutesi, kun käytät paikallisverkkoja ja Internetiä. Komponentti suodattaa kaikki verkkotoiminnot käyttäen kahdentyyppisiä sääntöjä: *sovellusten säännöt* ja *pakettisäännöt*.

Verkon valvonta

Verkon valvonta on suunniteltu valvomaan verkon toimintaa reaaliaikaisesti.

Järjestelmänvalvonta

Järjestelmänvalvonta-komponentilla voidaan palauttaa haittaohjelmien käyttöjärjestelmään tekemiä toimintoja.

Verkkohyökkäysten esto

Verkkohyökkäysten esto käynnistyy käyttöjärjestelmän käynnistyksen aikana ja seuraa saapuvaa verkkoliikennettä verkkohyökkäykselle tyypillisten ominaisuuksien osalta. Kun havaitaan hyökkäys tietokoneeseesi, Kaspersky Total Security estää kaiken hyökkääjän tietokoneeseesi kohdistaman verkkotoiminnan.

Roskapostin esto

Roskapostin esto integroituu tietokoneellesi asennettuun sähköpostiohjelmaan ja tarkistaa kaikki tulevat sähköpostit roskapostin varalta. Kaikki roskapostia sisältävät viestit merkitään erityisotsikolla. Voit määrittää Roskapostin eston käsittelemään roskapostit määrätyllä tavalla (esimerkiksi poistamaan ne automaattisesti tai siirtämään ne määrättyyn kansioon).

Verkkohuijausten esto

Verkkohuijausten eston avulla voit tarkistaa, onko URL-osoite tietojen kalasteluun käytettyjen URL-osoitteiden luettelossa. Komponentti sisältyy Verkon virustorjuntaan, Roskapostin estoon ja Pikaviestinnän virustorjuntaan.

Bannereiden esto

Bannereiden esto estää verkkosivustojen ja sovellusten käyttöliittymien mainosbannerit.

Rahasuojaus

Rahasuojaus suojaa luottamukselliset tiedot, kun käytät verkkopankki- ja maksupalveluja, ja se estää omaisuusrikokset verkkomaksuja suoritettaessa.

Suojattu näppäimistön syöttötila

Suojattu näppäimistön syöttötila suojaa näppäinpainallusten tallentajilta ja estää niitä kaappaamasta verkkosivuille syötettyjä henkilökohtaisia tietoja. Virtuaalinäppäimistö estää laitenäppäimistöllä syötettyjen tietojen kaappaamisen ja suojaa henkilökohtaisia tietoja kuvankaappauksien avulla tapahtuvilta kaappausyrityksiltä.

Luotetut sovellukset -tila

Luotetut sovellukset -tila suojaa tietokonetta sovelluksilta, jotka voivat olla vaarallisia. Kun Luotetut sovellukset -tila on käytössä, Kaspersky Total Security sallii vain sellaisten sovellusten suorittamisen, jotka on tunnistettu luotettaviksi (esimerkiksi Kaspersky Security Network -palvelusta saatujen tietojen tai luotetun digitaalisen allekirjoituksen perusteella).

Käytönvalvonta

Käytönvalvonta on suunniteltu suojaamaan lapsia ja teini-ikäisiä tietokoneen käyttöön ja verkkoselailuun liittyviltä uhkilta.

Käytönvalvonnalla voit asettaa joustavia rajoituksia verkkoresursseihin ja sovelluksiin pääsyyn eri käyttäjille riippuen heidän iästään. Lisäksi Käytönvalvonnan avulla voi katsella tilastollisia raportteja valvottujen käyttäjien toimista.

Varmuuskopiointi ja tietojen palautus

Varmuuskopiointi ja tietojen palautus -toiminnallisuus on suunniteltu suojaamaan tietojasi laitteistovikojen aiheuttamalta katoamiselta. Kaspersky Total Security voi varmuuskopioida tietoja ajastetusti siirrettäville levyille sekä verkko- ja Internet-taltioihin. Voit kopioida tiedostoja luokittain ja määrittää, kuinka monta versiota yksittäisestä tiedostosta tallennetaan.

Tietojen salaus

Tietojen salaus on suunniteltu suojaamaan luottamuksellisia tietoja luvattomalta käytöltä. Turvasäilön lukituksen avaaminen ja säilön sisällön tarkastelu vaatii salasanan.

Tietokoneen suojauksen etähallinta

Jos tietokoneellesi on asennettu Kaspersky Total Security ja sinulla on tili My Kaspersky -portaalissa, voit hallita tietokoneen suojausta etäyhteyden kautta.

PALVELU KÄYTTÄJILLE

Kun hankit sovelluksen käyttöoikeuden, saat käyttöösi seuraavat palvelut koko käyttöoikeuden voimassaolojakson ajan:

- Tietokantapäivitykset ja sovelluksen uusien versioiden käyttö
- Puhelin- ja sähköpostineuvonta liittyen sovelluksen asennus-, määritys- ja käyttökysymyksiin
- Tiedotuksia uusien Kaspersky Lab -sovellusten julkaisusta ja uusista viruksista sekä virusepidemioista. Voit käyttää tätä palvelua tilaamalla Kaspersky Labin uutiset teknisen tukipalvelun verkkosivuilla.

Neuvontaa ei tarjota liittyen käyttöjärjestelmien tai ulkopuolisten ohjelmistojen ja tekniikoiden toimintaan.

LAITTEISTO- JA OHJELMISTOVAATIMUKSET

Yleiset vaatimukset:

- 480 Mt vapaata kiintolevytilaa
- CD-/DVD-ROM (ohjelmiston asentamiseen asennuslevyltä)
- Internet-yhteys (sovelluksen aktivointiin sekä tietokantojen ja ohjelmamoduulien päivitykseen)
- Internet Explorer® 8.0 tai uudempi
- Microsoft® Windows® Installer 3.0 tai uudempi
- Microsoft .NET Framework 4 tai uudempi
- Verkkokameran käytön suojaus tukee vain yhteensopivia verkkokameramalleja http://support.kaspersky.com/10978.

Vaatimukset käyttöjärjestelmille Microsoft Windows XP Home Edition (Service Pack 3 tai uudempi), Microsoft Windows XP Professional (Service Pack 3 tai uudempi) ja Microsoft Windows XP Professional x64 Edition (Service Pack 2 tai uudempi):

- Vähintään 1 GHz:n suoritin
- 512 Mt vapaata RAM-muistia

Vaatimukset järjestelmille Microsoft Windows Vista® Home Basic (Service Pack 1 tai uudempi), Microsoft Windows Vista Home Premium (Service Pack 1 tai uudempi), Microsoft Windows Vista Business (Service Pack 1 tai uudempi), Microsoft Windows Vista Enterprise (Service Pack 1 tai uudempi), Microsoft Windows Vista Ultimate (Service Pack 1 tai uudempi), Microsoft Windows 7 Starter (Service Pack 1 tai uudempi), Microsoft Windows 7 Home Basic (Service Pack 1 tai uudempi), Microsoft Windows 7 Home Premium (Service Pack 1 tai uudempi), Microsoft Windows 7 Professional (Service Pack 1 tai uudempi), Microsoft Windows 7 Ultimate (Service Pack 1 tai uudempi), Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Microsoft Windows 8.1 Pro (Windows 8.1 Update), Microsoft Windows 8.1 Enterprise (Windows 8.1 Update) ja Microsoft Windows 10:

- Vähintään 1 GHz:n suoritin
- 1 Gt vapaata RAM-muistia (32-bittisille järjestelmille); 2 Gt vapaata RAM-muistia (64-bittisille järjestelmille)

Tablettien vaatimukset:

- Microsoft Tablet PC
- Vähintään 1,66 GHz:n Intel® Celeron® -suoritin
- 1 000 Mt vapaata RAM-muistia

Vaatimukset minikannettaville:

- Vähintään 1,60 GHz:n Intel Atom -suoritin
- 1 024 Mt vapaata RAM-muistia
- 10,1 tuuman näyttö tarkkuudella 1024×600
- Intel GMA 950 -näytönohjain

SOVELLUKSEN ASENTAMINEN JA POISTAMINEN

Tämä osio sisältää vaiheittaiset ohjeet sovelluksen asentamiseksi ja poistamiseksi.

TÄSSÄ OSIOSSA

NORMAALI ASENNUSMENETTELY

Kaspersky Total Security asennetaan tietokoneeseesi interaktiivisessa tilassa ohjatun asennustoiminnon avulla.

Ohjattu toiminto koostuu ikkunoista (vaiheista), joissa liikutaan painikkeilla **Takaisin** ja **Seuraava**. Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta. Voit pysäyttää ohjatun toiminnon missä tahansa asennusvaiheessa sulkemalla ohjatun toiminnon ikkunan.

Jos sovelluksen on tarkoitus suojata useampaa kuin yhtä tietokonetta (tietokoneiden enimmäismäärä määräytyy käyttäjän käyttöoikeussopimuksen ehtojen mukaisesti), se on asennettava identtisesti jokaiselle tietokoneelle.

- *Voit asentaa Kaspersky Total Securityn seuraavasti:*

  Suorita asennuspaketti asennus-CD:ltä (tiedosto, jonka pääte on .exe).

Voit asentaa Kaspersky Total Securityn myös käyttämällä Internetistä ladattua jakelupakettia. Tässä tapauksessa ohjattu asennustoiminto näyttää useita lisäasennusvaiheita joillekin kielivaihtoehdoille.

Sovelluksen mukana asennetaan verkkoselainlaajennukset, joilla turvataan Internetin selailu.

TÄSSÄ OSIOSSA

VAIHE 1. SOVELLUKSEN UUDEMMAN VERSION LÖYTÄMINEN

Ennen asennusta asennusohjelma tarkistaa Kaspersky Labin päivityspalvelimilta, onko Kaspersky Total Securityn uudempi versio saatavana.

Jos ohjattu asennustoiminto ei löydä uudempaa versiota sovelluksesta Kaspersky Labin päivityspalvelimilta, se aloittaa nykyisen version asennuksen.

Jos ohjattu toiminto löytää Kaspersky Labin päivityspalvelimilta uudemman version Kaspersky Total Securitysta, se ehdottaa uuden version lataamista ja asennusta tietokoneellesi. Suosittelemme asentamaan sovelluksen uuden version, sillä uudemmissa versioissa on enemmän parannuksia, jotka varmistavat tietokoneesi luotettavamman suojauksen. Jos estät uuden version asennuksen, ohjattu toiminto alkaa asentaa sovelluksen nykyistä versiota. Jos hyväksyt sovelluksen uuden version asennuksen, ohjattu asennustoiminto kopioi asennuspaketin tiedostot tietokoneellesi ja aloittaa uuden version asennuksen.

VAIHE 2. SOVELLUKSEN ASENNUKSEN ALOITTAMINEN

Tässä vaiheessa ohjattu asennustoiminto antaa sinulle mahdollisuuden asentaa sovellus.

Jatka asennusta napsauttamalla **Asenna**-painiketta.

Asennustyypistä ja kielivaihtoehdosta riippuen ohjattu toiminto tarjoaa tässä vaiheessa nähtäväksesi sinun ja Kaspersky Labin välillä solmittavan käyttöoikeussopimuksen sekä mahdollisuuden liittyä Kaspersky Security Network -verkostoon.

VAIHE 3. TUTUSTUMINEN KÄYTTÖOIKEUSSOPIMUKSEEN

Ohjatun asennustoiminnon tämä vaihe näytetään määrätyille kielivaihtoehdoille, kun Kaspersky Total Security asennetaan Internetistä ladatusta asennuspaketista.

Tässä vaiheessa ohjattu asennustoiminto tarjoaa sinulle mahdollisuuden tarkastella sinun ja Kaspersky Labin välillä solmittua käyttöoikeussopimusta.

Lue käyttöoikeussopimus huolellisesti, ja jos hyväksyt kaikki sen ehdot, napsauta **Hyväksy**-painiketta. Sitten sovelluksen asentaminen tietokoneellesi jatkuu.

Jos käyttöoikeussopimuksen ehtoja ei hyväksytä, sovelluksen asennus keskeytyy.

VAIHE 4. KASPERSKY SECURITY NETWORK (KSN) -TIEDONKERUULAUSEKE

Tässä vaiheessa ohjattu asennustoiminto pyytää sinua osallistumaan Kaspersky Security Network -verkostoon. Ohjelmaan osallistuminen tarkoittaa, että tietoa tietokoneessasi havaituista uusista uhista, suoritettavana olevista sovelluksista ja ladatuista allekirjoitetuista sovelluksista lähetetään Kaspersky Labille yhdessä käyttöjärjestelmän tietojen kanssa. Sinulta saatuja yksityisiä tietoja ei kerätä, käsitellä eikä tallenneta.

Tarkista Kaspersky Security Network -tiedonkeruulauseke. Jos hyväksyt kaikki ehdot, napsauta **Hyväksy**-painiketta ohjatun asennustoiminnon ikkunassa.

Jos et haluat osallistua Kaspersky Security Network -verkostoon, napsauta **Hylkää**-painiketta.

Sovelluksen asennus jatkuu, kun olet hyväksynyt tai hylännyt osallistumisen Kaspersky Security Network -verkostoon.

VAIHE 5. ASENNUS

Joissakin Kaspersky Total Securityn tilauksiin perustuvissa jakeluversioissa on annettava palveluntarjoajalta saatu salasana ennen asennusta.

Sovelluksen asennus käynnistyy, kun olet syöttänyt salasanan.

Sovelluksen asentaminen vie jonkin aikaa. Odota, kunnes asennus on valmis.

Kun toimenpide on valmis, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Kaspersky Total Security suorittaa joitakin tarkistuksia asennuksen aikana. Nämä tarkistukset saattavat havaita seuraavia ongelmia:

- *Käyttöjärjestelmä ei vastaa ohjelmistovaatimuksia*. Asennuksen aikana ohjattu toiminto tarkistaa, että seuraavat ehdot täyttyvät:
    - Täyttävätkö käyttöjärjestelmä ja korjauspaketit ohjelmistovaatimukset
    - Ovatko kaikki tarvittavat sovellukset käytettävissä
    - Riittääkö vapaa levytila asennukseen

    Jos jokin edellä luetelluista vaatimuksista ei täyty, ohjattu toiminto näyttää asianmukaisen huomautuksen.
- *Yhteensopimattomia sovelluksia tietokoneessa*. Jos epäyhteensopivia sovelluksia havaitaan, ne esitetään luettelona ja sinulle tarjotaan mahdollisuus poistaa ne. Suosittelemme poistamaan manuaalisesti kaikki sovellukset, joita Kaspersky Total Security ei pysty poistamaan automaattisesti. Epäyhteensopivien sovellusten poistamisen jälkeen käyttöjärjestelmä on käynnistettävä uudelleen. Tämän jälkeen Kaspersky Total Securityn asennusta jatketaan automaattisesti.
- *Haitallisia ohjelmia tietokoneessa*. Jos tietokoneelta havaitaan virustorjunnan asentamista haittaavia ohjelmia, ohjattu toiminto kehottaa sinua lataamaan *Kaspersky Virus Removal Toolin*, tartuntojen neutralointiin tarkoitetun erikoistyökalun.

    Jos sallit apuohjelman asentamisen, ohjattu asennustoiminto lataa sen automaattisesti Kaspersky Labin palvelimista. Apuohjelma asennetaan tämän jälkeen automaattisesti. Jos ohjattu toiminto ei pysty lataamaan apuohjelmaa, sinua kehotetaan lataamaan se itse napsauttamalla annettua linkkiä.

VAIHE 6. ASENNUKSEN VIIMEISTELY

Tässä vaiheessa ohjattu toiminto ilmoittaa sinulle sovelluksen asennuksen onnistumisesta. Jos haluat käynnistää Kaspersky Total Securityn välittömästi, varmista, että **Suorita Kaspersky Total Security** -ruutu on valittuna ja paina **Lopeta**-painiketta.

Jos olet poistanut valinnan **Suorita Kaspersky Total Security** -ruudusta ennen ohjatun toiminnon sulkemista, sovellus on käynnistettävä manuaalisesti.

Joissakin tapauksissa käyttöjärjestelmä on käynnistettävä uudelleen asennuksen viimeistelemiseksi.

VAIHE 7. SOVELLUKSEN AKTIVOINTI

Tässä vaiheessa ohjattu asennustoiminto antaa sinulle mahdollisuuden aktivoida sovellus.

Aktivointi on prosessi, jossa sovelluksen täysi toiminnallisuus otetaan käyttöön tietyksi ajaksi.

Jos olet ostanut Kaspersky Total Securityn käyttöoikeuden ja ladannut sovelluksen verkkokaupasta, sovellus voidaan aktivoida automaattisesti asennuksen aikana.

Kaspersky Total Securityn aktivointiin tarjotaan seuraavat vaihtoehdot:

- **Aktivoi sovellus**. Valitse tämä vaihtoehto ja anna aktivointikoodi, jos olet ostanut sovelluksen käyttöoikeuden.

  Jos kirjoitat tekstikenttään aktivointikoodin Kaspersky Internet Security- tai Kaspersky Anti-Virus -sovellusta varten, siirtyminen Kaspersky Internet Security- tai Kaspersky Anti-Virus -sovellukseen käynnistyy, kun aktivointi on suoritettu loppuun.

- **Aktivoi sovelluksen kokeiluversio**. Valitse tämä aktivointivaihtoehto, jos haluat asentaa sovelluksen kokeiluversion ennen kuin teet päätöksen käyttöoikeuden ostamisesta. Voit käyttää sovellusta ja kaikkia sen ominaisuuksia lyhyen kokeilujakson ajan. Kun kokeiluversion käyttöoikeus päättyy, kokeiluversiota ei ole mahdollista aktivoida uudelleen.

Internet-yhteys tarvitaan sovelluksen aktivointiin.

Rekisteröityminen My Kaspersky -portaaliin voi olla tarpeen sovelluksen aktivoinnin aikana.

VAIHE 8. KÄYTTÄJÄN REKISTERÖINTI

Tämä vaihe ei ole valittavissa Kaspersky Total Securityn kaikissa versioissa.

Rekisteröityneet käyttäjät voivat lähettää pyyntöjä tekniseen tukeen ja viruslaboratorioon My Kaspersky -portaalin kautta, ja he voivat myös hallita aktivointikoodeja ja vastaanottaa Kaspersky Labilta tietoja uusista sovelluksista ja erikoistarjouksista.

Jos hyväksyt rekisteröitymisen, määritä rekisteröitymistä varten vaadittavat tiedot oheisissa kentissä ja napsauta **Seuraava**-painiketta lähettääksesi tiedot Kaspersky Labiin.

Joissain tapauksissa sovelluksen käytön aloittaminen edellyttää käyttäjärekisteröintiä.

VAIHE 9. AKTIVOINNIN VIIMEISTELY

Ohjattu toiminto ilmoittaa, että Kaspersky Total Securityn aktivointi onnistui. Tämä ikkuna sisältää myös tietoja voimassaolevasta käyttöoikeudesta, käyttöoikeuden vanhenemispäivästä sekä käyttöoikeuden kattamasta isäntäkoneiden määrästä.

Jos olet hankkinut tilauksen, sen tila esitetään käyttöoikeuden voimassaolon päättymispäivän sijasta.

Sulje ohjattu toiminto napsauttamalla **Lopeta**-painiketta.

SOVELLUKSEN ASENTAMINEN KOMENTORIVILTÄ

Voit asentaa Kaspersky Total Securityn komentoriviltä.

Komentorivin rakenne:

```
<asennuspaketin polku> [parametrit]
```

Teknisen tuen verkkosivusto (http://support.kaspersky.com/11355) sisältää yksityiskohtaiset ohjeet ja asennusasetukset.

AIEMMAN SOVELLUSVERSION PÄIVITYS

Kaspersky Total Securityn asentaminen Kaspersky PUREn päälle

Jos Kaspersky PURE on jo asennettu tietokoneellesi, voit päivittää sen Kaspersky Total Securityksi. Jos sinulla on voimassaoleva Kaspersky PURE -käyttöoikeus, sovellusta ei tarvitse aktivoida: Ohjattu asennustoiminto saa automaattisesti käyttöoikeuden tiedot ja käyttää niitä Kaspersky Total Securityn asennuksen aikana.

Kaspersky Total Securityn asentaminen Kaspersky Internet Securityn päälle

Jos asennat Kaspersky Total Securityn tietokoneelle, jolle on jo asennettu kyseisellä hetkellä voimassaolevaa käyttöoikeutta käyttävä Kaspersky Internet Security, ohjattu aktivointitoiminto kehottaa sinua valitsemaan yhden seuraavista vaihtoehdoista:

- Jatka Kaspersky Internet Securityn käyttöä nykyisellä käyttöoikeudella. Tässä tapauksessa ohjattu siirtotoiminto käynnistyy. Kun ohjattu siirtotoiminto on suoritettu, Kaspersky Internet Security asennetaan tietokoneellesi. Voit käyttää Kaspersky Internet Securityä, kunnes Kaspersky Internet Security -käyttöoikeus vanhenee.

- Jatka Kaspersky Total Securityn uuden version asennusta. Tässä tapauksessa sovellus asennetaan ja aktivoidaan tavallisen asennusmenettelyn mukaisesti.

Kaspersky Total Security asennetaan tietokoneeseesi interaktiivisessa tilassa ohjatun asennustoiminnon avulla.

Ohjattu toiminto koostuu ikkunoista (vaiheista), joissa liikutaan painikkeilla **Takaisin** ja **Seuraava**. Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta. Voit pysäyttää ohjatun toiminnon missä tahansa asennusvaiheessa sulkemalla ohjatun toiminnon ikkunan.

Jos sovelluksen on tarkoitus suojata useampaa kuin yhtä tietokonetta (tietokoneiden enimmäismäärä määräytyy käyttäjän käyttöoikeussopimuksen ehtojen mukaisesti), se on asennettava identtisesti jokaiselle tietokoneelle.

➧ *Voit asentaa Kaspersky Total Securityn seuraavasti:*

Suorita asennuspaketti asennus-CD:ltä (tiedosto, jonka pääte on .exe).

Voit asentaa Kaspersky Total Securityn myös käyttämällä Internetistä ladattua jakelupakettia. Tässä tapauksessa ohjattu asennustoiminto näyttää useita lisäasennusvaiheita joillekin kielivaihtoehdoille.

Sovelluksen mukana asennetaan verkkoselainlaajennukset, joilla turvataan Internetin selailu.

Tietyt rajoitukset koskevat sovelluksen päivittämistä aiemmasta versiosta (katso osio "Rajoitukset ja varoitukset" sivulla page 106).

TÄSSÄ OSIOSSA

VAIHE 1. SOVELLUKSEN UUDEMMAN VERSION LÖYTÄMINEN

Ennen asennusta asennusohjelma tarkistaa Kaspersky Labin päivityspalvelimilta, onko Kaspersky Total Securityn uudempi versio saatavana.

Jos ohjattu asennustoiminto ei löydä uudempaa versiota sovelluksesta Kaspersky Labin päivityspalvelimilta, se aloittaa nykyisen version asennuksen.

Jos ohjattu toiminto löytää Kaspersky Labin päivityspalvelimilta uudemman version Kaspersky Total Securitysta, se ehdottaa uuden version lataamista ja asennusta tietokoneellesi. Suosittelemme asentamaan sovelluksen uuden version, sillä uudemmissa versioissa on enemmän parannuksia, jotka varmistavat tietokoneesi luotettavamman suojauksen. Jos estät uuden version asennuksen, ohjattu toiminto alkaa asentaa sovelluksen nykyistä versiota. Jos hyväksyt sovelluksen uuden version asennuksen, ohjattu asennustoiminto kopioi asennuspaketin tiedostot tietokoneellesi ja aloittaa uuden version asennuksen.

VAIHE 2. SOVELLUKSEN ASENNUKSEN ALOITTAMINEN

Tässä vaiheessa ohjattu asennustoiminto antaa sinulle mahdollisuuden asentaa sovellus.

Jatka asennusta napsauttamalla **Asenna**-painiketta.

Asennustyypistä ja kielivaihtoehdosta riippuen ohjattu toiminto tarjoaa tässä vaiheessa nähtäväksesi sinun ja Kaspersky Labin välillä solmittavan käyttöoikeussopimuksen sekä mahdollisuuden liittyä Kaspersky Security Network -verkostoon.

VAIHE 3. TUTUSTUMINEN KÄYTTÖOIKEUSSOPIMUKSEEN

Ohjatun asennustoiminnon tämä vaihe näytetään määrätyille kielivaihtoehdoille, kun Kaspersky Total Security asennetaan Internetistä ladatusta asennuspaketista.

Tässä vaiheessa ohjattu asennustoiminto tarjoaa sinulle mahdollisuuden tarkastella sinun ja Kaspersky Labin välillä solmittua käyttöoikeussopimusta.

Lue käyttöoikeussopimus huolellisesti, ja jos hyväksyt kaikki sen ehdot, napsauta **Hyväksy**-painiketta. Sitten sovelluksen asentaminen tietokoneellesi jatkuu.

Jos käyttöoikeussopimuksen ehtoja ei hyväksytä, sovelluksen asennus keskeytyy.

VAIHE 4. KASPERSKY SECURITY NETWORK (KSN) - TIEDONKERUULAUSEKE

Tässä vaiheessa ohjattu asennustoiminto pyytää sinua osallistumaan Kaspersky Security Network -verkostoon. Ohjelmaan osallistuminen tarkoittaa, että tietoa tietokoneessasi havaituista uusista uhista, suoritettavana olevista sovelluksista ja ladatuista allekirjoitetuista sovelluksista lähetetään Kaspersky Labille yhdessä käyttöjärjestelmän tietojen kanssa. Sinulta saatuja yksityisiä tietoja ei kerätä, käsitellä eikä tallenneta.

Tarkista Kaspersky Security Network -tiedonkeruulauseke. Jos hyväksyt kaikki ehdot, napsauta **Hyväksy**-painiketta ohjatun asennustoiminnon ikkunassa.

Jos et haluat osallistua Kaspersky Security Network -verkostoon, napsauta **Hylkää**-painiketta.

Sovelluksen asennus jatkuu, kun olet hyväksynyt tai hylännyt osallistumisen Kaspersky Security Network -verkostoon.

VAIHE 5. ASENNUS

Joissakin Kaspersky Total Securityn tilauksiin perustuvissa jakeluversioissa on annettava palveluntarjoajalta saatu salasana ennen asennusta.

Sovelluksen asennus käynnistyy, kun olet syöttänyt salasanan.

Sovelluksen asentaminen vie jonkin aikaa. Odota, kunnes asennus on valmis.

Kun toimenpide on valmis, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Kaspersky Total Security suorittaa joitakin tarkistuksia asennuksen aikana. Nämä tarkistukset saattavat havaita seuraavia ongelmia:

- *Käyttöjärjestelmä ei vastaa ohjelmistovaatimuksia*. Asennuksen aikana ohjattu toiminto tarkistaa, että seuraavat ehdot täyttyvät:
    - Täyttävätkö käyttöjärjestelmä ja korjauspaketit ohjelmistovaatimukset
    - Ovatko kaikki tarvittavat sovellukset käytettävissä
    - Riittääkö vapaa levytila asennukseen

    Jos jokin edellä luetelluista vaatimuksista ei täyty, ohjattu toiminto näyttää asianmukaisen huomautuksen.

- *Yhteensopimattomia sovelluksia tietokoneessa*. Jos epäyhteensopivia sovelluksia havaitaan, ne esitetään luettelona ja sinulle tarjotaan mahdollisuus poistaa ne. Suosittelemme poistamaan manuaalisesti kaikki sovellukset, joita Kaspersky Total Security ei pysty poistamaan automaattisesti. Epäyhteensopivien sovellusten poistamisen jälkeen käyttöjärjestelmä on käynnistettävä uudelleen. Tämän jälkeen Kaspersky Total Securityn asennusta jatketaan automaattisesti.

- *Haitallisia ohjelmia tietokoneessa*. Jos tietokoneelta havaitaan virustorjunnan asentamista haittaavia ohjelmia, ohjattu toiminto kehottaa sinua lataamaan *Kaspersky Virus Removal Toolin*, tartuntojen neutralointiin tarkoitetun erikoistyökalun.

    Jos sallit apuohjelman asentamisen, ohjattu asennustoiminto lataa sen automaattisesti Kaspersky Labin palvelimista. Apuohjelma asennetaan tämän jälkeen automaattisesti. Jos ohjattu toiminto ei pysty lataamaan apuohjelmaa, sinua kehotetaan lataamaan se itse napsauttamalla annettua linkkiä.

VAIHE 6. ASENNUKSEN VIIMEISTELY

Ohjatun toiminnon tämä ikkuna ilmoittaa sinulle sovelluksen asennuksen onnistumisesta.

Käynnistä käyttöjärjestelmä uudelleen sovelluksen asennuksen jälkeen.

Jos **Suorita Kaspersky Total Security** -ruutu on valittuna, sovellus käynnistetään automaattisesti, kun käynnistät käyttöjärjestelmän uudelleen.

Jos olet poistanut valinnan **Suorita Kaspersky Total Security** -ruudusta ennen ohjatun toiminnon sulkemista, sovellus on käynnistettävä manuaalisesti.

SOVELLUKSEN POISTO

Kaspersky Total Securityn poiston jälkeen tietokoneesi ja henkilökohtaiset tietosi ovat suojaamattomia.

Kaspersky Total Security poistetaan ohjatun asennustoiminnon avulla.

- *Voit käynnistää ohjatun toiminnon seuraavasti:*

  Valitse **Käynnistä**-valikosta **Kaikki ohjelmat** → **Kaspersky Total Security** → **Poista Kaspersky Total Security**.

TÄSSÄ OSIOSSA

VAIHE 1. SALASANAN ANTAMINEN SOVELLUKSEN POISTAMISEKSI

Kaspersky Total Securityn poistaminen edellyttää sovellusasetusten suojaussalasanan syöttämistä. Jos et jostain syystä pysty syöttämään salasanaa, sovelluksen poistaminen ei ole mahdollista.

Tämä vaihe tulee näkyviin vain, jos sovelluksen poistaminen on suojattu salasanalla.

VAIHE 2. TIETOJEN TALLENNUS MYÖHEMPÄÄ KÄYTTÖÄ VARTEN

Tässä vaiheessa voit määrittää, mitkä sovelluksen käyttämät tiedot haluat säilyttää myöhempää käyttöä varten sovelluksen seuraavan asennuksen aikana (esim. asennettaessa sovelluksen uudempaa versiota).

Oletusarvoisesti sovellus tarjoutuu tallentamaan käyttöoikeutta koskevia tietoja.

- *Tallenna tietoja tulevaa käyttöä varten valitsemalla ruudut niiden tietojen vieressä, jotka haluat tallentaa:*

  - **Käyttöoikeustiedot** – tietoja, jotka poistavat uuden sovelluksen aktivointitarpeen ja antavat sinun käyttää sovellusta voimassaolevan käyttöoikeuden ajan, ellei käyttöoikeus vanhene ennen kuin aloitat asennuksen.
  - **Karanteenissa olevat tiedostot** – sovelluksen tarkistamat ja karanteeniin asettamat tiedostot.

    Karanteeniin asetetut tiedostot eivät enää ole käytettävissä sen jälkeen, kun Kaspersky Total Security on poistettu tietokoneelta. Kaspersky Total Security tulee olla asennettuna, jotta voit suorittaa toimenpiteitä näille tiedostoille.

- **Sovelluksen käyttöasetukset** – asetusten määrityksen yhteydessä valitut sovelluksen asetusarvot.

  Kaspersky Lab ei takaa tukea aiempien sovellusversioiden asetuksille. Uuden version asennuksen jälkeen suosittelemme tarkistamaan, että sovelluksen asetukset ovat oikeat.

  Voit myös viedä suojausasetukset komentokehotteesta seuraavalla komennolla:

  avp.com EXPORT <tiedostonimi>

- **iChecker-tiedot** ovat tiedostoja, jotka sisältävät tietoja objekteista, jotka on jo tarkistettu käyttäen iChecker-teknologiaa.
- **Roskapostin eston tietokannat** – Tietokannat, jotka sisältävät esimerkkejä käyttäjän lisäämistä roskaposteista.
- **Tietojen salaus** -osio sisältää tiedostoja, jotka on tallennettu taltioon Tietojen salaus -toiminnolla.

VAIHE 3. SOVELLUKSEN POISTON VAHVISTAMINEN

Koska sovelluksen poisto uhkaa tietokoneesi turvallisuutta ja henkilökohtaisia tietojasi, sinua pyydetään vahvistamaan aikomuksesi poistaa sovellus. Suorita vahvistus napsauttamalla **Poista**-painiketta.

VAIHE 4. SOVELLUKSEN POISTO. POISTON VIIMEISTELY

Tässä vaiheessa ohjattu toiminto poistaa sovelluksen tietokoneeltasi. Odota, kunnes poisto on valmis.

Kun olet poistanut Kaspersky Total Securityn, voit jättää Kaspersky Labin verkkosivustolle kommentin ja kertoa meille, miksi päädyit poistamaan sovelluksen. Tämä edellyttää Kaspersky Labin verkkosivustolle siirtymistä napsauttamalla **Täytä lomake** -painiketta.

Tämä toiminto ei välttämättä ole käytettävissä kaikilla alueilla.

Sinun täytyy käynnistää käyttöjärjestelmä uudelleen sovelluksen poistamisen aikana. Jos peruutat välittömän uudelleenkäynnistyksen, sovelluksen poiston suorittamista loppuun viivytetään, kunnes käyttöjärjestelmä käynnistetään uudestaan, tai kunnes tietokone sammutetaan ja käynnistetään uudestaan.

SOVELLUKSEN KÄYTTÖOIKEUS

Tässä osiossa on tietoja sovelluksen aktivointiin liittyvistä avaintermeistä. Lukemalla tämän osion saat lisätietoja käyttöoikeussopimuksen tarkoituksesta sekä tavoista aktivoida sovellus ja uusia käyttöoikeutesi.

TÄSSÄ OSIOSSA

TIETOJA KÄYTTÄJÄN KÄYTTÖOIKEUSSOPIMUKSESTA

Käyttöoikeussopimus on sinun ja Kaspersky Lab ZAO:n välinen sitova sopimus, joka määrittää sovelluksen käyttöä koskevat ehdot.

Lue käyttöoikeussopimuksen ehdot huolellisesti ennen kuin aloitat sovelluksen käytön.

Käyttöoikeussopimuksen hyväksyminen asennuksen yhteydessä tarkoittaa, että olet hyväksynyt käyttöoikeussopimuksen ehdot. Jos et hyväksy käyttöoikeussopimuksen ehtoja, sinun on keskeytettävä sovelluksen asennus ja lopetettava sovelluksen käyttö.

TIETOJA KÄYTTÖOIKEUDESTA

Käyttöoikeus on aikarajoitteinen oikeus käyttää sovellusta, ja se myönnetään käyttöoikeussopimuksen puitteissa. Käyttöoikeus on yhteydessä uniikkiin koodiin, joka sinulla on Kaspersky Total Security -kopiosi aktivointia varten.

Voimassaoleva käyttöoikeus antaa sinulle luvan käyttää seuraavia palveluja:

- Oikeus käyttää sovellusta yhdellä tai useammalla laitteella

  Sallittu käytettävien laitteiden lukumäärä on määritetty käyttöoikeussopimuksessa.

- Kaspersky Labin teknisen tuen tarjoama apu
- Muut palvelut Kaspersky Labilta tai sen kumppaneilta käyttöoikeuden voimassaoloaikana (ks. "Palvelu käyttäjille" sivulla 17)

Sovellusten hallinta edellyttää käyttöoikeuden hankintaa sovelluksen käyttöä varten.

Käyttöoikeusjakso on rajattu. Kun käyttöoikeus vanhenee, sovellus jatkaa toimintaansa rajoitetun toiminnan tilassa (esimerkiksi sovelluksen päivitys ja Kaspersky Security Networkin käyttö ei ole mahdollista). Voit edelleen käyttää sovelluksen kaikkia komponentteja ja suorittaa tarkistuksia virusten ja haittaohjelmien varalta, mutta käytössäsi ovat vain ne tietokannat, jotka asennettiin ennen käyttöoikeuden vanhenemista. Jos haluat jatkaa Kaspersky Total Security käyttöä täyden toiminnallisuuden tilassa, sinun on uusittava käyttöoikeus.

Suosittelemme uusimaan käyttöoikeuden ennen sen vanhenemista, jotta varmistetaan tietokoneen paras mahdollinen suojaus kaikkia turvauhkia vastaan.

Voit hankkia Kaspersky Total Securityn kokeiluversion ennen käyttöoikeuden ostamista. Kaspersky Total Securityn kokeiluversio on käytettävissä lyhyen kokeilujakson ajan. Kun kokeilujakso on umpeutunut, Kaspersky Total Securityn kaikki ominaisuudet kytkeytyvät pois käytöstä. Jos haluat jatkaa sovelluksen käyttöä, sinun on ostettava käyttöoikeus.

TIETOJA AKTIVOINTIKOODISTA

Aktivointikoodi on koodi, jonka saat ostaessasi Kaspersky Total Securityn käyttöoikeuden. Tämä koodi tarvitaan sovelluksen aktivointiin.

Aktivointikoodi on uniikki merkkijono, joka koostuu kahdestakymmenestä numerosta ja latinalaisista kirjaimista, ja se on muotoa xxxxx-xxxxx-xxxxx-xxxxx.

Voit hankkia aktivointikoodin yhdellä seuraavista tavoista riippuen siitä, miten ostit sovelluksen:

- Jos ostat Kaspersky Total Securityn myyntipakettiversion, aktivointikoodi sijaitsee käyttöoppaassa tai asennus-CD:n sisältävässä myyntipaketissa.
- Jos ostat Kaspersky Total Securityn verkkokaupasta, aktivointikoodi lähetetään sähköpostiosoitteeseen, jonka määrität tilatessasi tuotetta.

Käyttöoikeuden voimassaolojakso alkaa sinä päivänä, kun aktivoit sovelluksen. Jos olet hankkinut käyttöoikeuden, jolla Kaspersky Total Security voidaan asentaa useisiin laitteisiin, käyttöoikeuden voimassaolokausi alkaa silloin, kun käytät aktivointikoodia ensimmäisen kerran.

Jos olet kadottanut tai vahingossa poistanut aktivointikoodisi sovelluksen aktivoinnin jälkeen, ota yhteys Kaspersky Labin tekniseen tukipalveluun aktivointikoodin palauttamiseksi (http://www.kaspersky.fi/support).

TIETOJA TILAUKSESTA

Kaspersky Total Security -tilaus mahdollistaa sovelluksen käytön valittujen parametrien mukaisesti (vanhenemispäivämäärä ja suojattujen laitteiden määrä). Voit hankkia Kaspersky Total Securityn tilauksen palveluntarjoajalta (esimerkiksi Internet-palveluntarjoajaltasi). Voit keskeyttää tai jatkaa tilaustasi, uusia sen automaattitilassa tai peruuttaa sen. Voit hallinnoida tilausta henkilökohtaisella sivullasi palveluntarjoajan verkkosivustossa.

Myyjiltä on saatavana kahta eri tilaustyyppiä Kaspersky Total Securityn käyttöön: päivitystilaus ja päivitys- sekä suojaustilaus.

Tilaus voi olla rajoitettu (esim. yksi vuosi) tai rajoittamaton (ei vanhenemispäivämäärää). Jos haluat jatkaa Kaspersky Total Securityn käyttöä rajoitetun tilauksen vanhennuttua, sinun tulee uusia se. Rajoittamattomat tilaukset uusitaan automaattisesti, jos ennakkomaksu on suoritettu palveluntarjoajalle ajallaan.

Kun rajoitettu tilaus vanhenee, sinulle myönnetään jatkoaikaa, jolloin voit vielä uusia tilauksesi. Sovelluksen toiminnallisuus pysyy vielä tällöin muuttumattomana.

Jos tilausta ei uusita ennen jatkoajan loppumista, Kaspersky Total Security lakkaa päivittämästä sovelluksen tietokantoja (päivitystilauksen tapauksessa), vaihtamasta tietoja Kaspersky Security Networkin kanssa tai suojaamasta tietokonetta ja suorittamasta tarkistuksia (päivitys- ja suojaustilauksien tapauksessa).

Jos haluat käyttää Kaspersky Total Securitya tilausversiona, sinun on annettava palveluntarjoajaltasi saama aktivointikoodi. Joissain tapauksissa aktivointikoodi voidaan ladata ja ottaa käyttöön automaattisesti. Jos sovellusta käytetään tilausversiona, et voi käyttää toista aktivointikoodia käyttöoikeuden uusimiseen. Voit syöttää toisen aktivointikoodin vasta tilausjakson päätyttyä.

Jos Kaspersky Total Security on jo käytössä nykyisellä käyttöoikeudella, kun rekisteröit tilauksesi, Kaspersky Total Securitya käytetään tilausversiona rekisteröinnin jälkeen. Aktivointikoodia, jolla aktivoit sovelluksen, voidaan käyttää toisessa tietokoneessa.

Voit peruuttaa tilauksen ottamalla yhteyden palveluntarjoajaan, jolta ostit Kaspersky Total Securityn.

Käytettävissä olevat tilauksenhallintavaihtoehdot voivat vaihdella riippuen palveluntarjoajasta. Lisäksi et ehkä saa käyttöösi jatkoaikaa, jolloin voit uusia tilauksen.

LISÄTIETOA TIETOJEN TOIMITTAMISESTA

Suojaustason parantamiseksi hyväksyt seuraavien tietojen automaattisen lähettämisen Kaspersky Labille samalla, kun hyväksyt käyttöoikeussopimuksen ehdot:

- Tietoja käsiteltyjen tiedostojen tarkistussummista (MD5)
- Tietoja, joita tarvitaan URL-osoitteiden maineen tarkastamiseen
- Sovelluksen ilmoitusten käyttötilastot
- Roskapostin estoon liittyvää tilastotietoa
- Tietoja aktivoinnista ja käytössä olevasta Kaspersky Total Securityn versiosta
- Tietoja Kaspersky Total Securityn asennetun version käyttöoikeudesta
- Tietoja havaittujen uhkien tyypeistä
- Tietoja käytössä olevista digitaalisista varmenteista sekä tietoja, joita tarvitaan niiden varmentamiseksi
- Tietoja sovelluksen toiminnasta ja käyttöoikeuksista, joita tarvitaan luotettujen verkkosivustojen sisällön näyttämiseen

Jos tietokone on varustettu TPM:llä (Trusted Platform Module), hyväksyt myös, että Kaspersky Labille lähetetään käyttöjärjestelmän käynnistystä koskeva TPM-raportti sekä sen varmentamisessa tarvittavia tietoja. Jos Kaspersky Total Securityn asennuksen yhteydessä tapahtuu virhe, hyväksyt, että Kaspersky Labille lähetetään automaattisesti tietoja virhekoodista, käytössä olevasta jakelupaketista sekä tietokoneestasi.

Jos osallistut Kaspersky Security Networkiin (ks. "Osallistuminen Kaspersky Security Networkiin (KSN)" sivulla 96), hyväksyt, että seuraavat Kaspersky Total Securityn käyttöön liittyvät tiedot lähetetään automaattisesti tietokoneestasi Kaspersky Labiin:

- Tietoja tietokoneen laitteistosta ja asennetuista ohjelmista
- Tietoja tietokoneen virustentorjunnan suojaustilasta sekä kaikista todennäköisesti tartunnan saaneista objekteista ja kyseisiin objekteihin liittyvistä päätöksistä
- Tietoja ladatuista ja käynnistetyistä sovelluksista
- Tietoja käyttöliittymän virheistä sekä Kaspersky Total Securityn käyttöliittymän käytöstä
- Sovelluksen tiedot, mukaan lukien sovelluksen versio, ladattujen ohjelmistomoduulien tiedostoja koskevat tiedot sekä nykyisten sovellustietokantojen versiot
- Tilastotietoja päivityksistä sekä yhteyksistä Kaspersky Labin palvelimille
- Tietoja käytössä olevasta langattomasta yhteydestä
- Tilastotietoja Kaspersky Total Securityn aiheuttamista viivästyksistä silloin, kun käyttäjä käyttää tietokoneelle asennettuja sovelluksia
- Tiedostot, joiden avulla rikolliset voivat vahingoittaa tietokonettasi, tai tällaisten tiedostojen osat, mukaan lukien haitallisten linkkien viittaamat tiedostot

Kaspersky Labille lähetettävät tiedot voidaan säilyttää tietokoneellasi enintään 30 päivän ajan niiden luomisesta. Tiedot säilytetään sisäisessä suojatussa tallennuspaikassa. Tallennettavan tiedon enimmäismäärä on 30 Mt.

Lisäksi hyväksyt, että Kaspersky Labille lähetetään automaattisesti ylimääräistä tarkistusta varten tiedostoja (tai tiedostojen osia), joita tunkeutujat saattavat todennäköisemmin käyttää hyväksi tarkoituksenaan vahingoittaa käyttäjän tietokonetta.

Kaspersky Lab suojaa kaikkia vastaanottamiaan tietoja sovellettavien lakien edellyttämällä tavalla. Kaspersky Lab käyttää kaikkia vastaanotettuja tietoja vain yleisinä tilastotietoina. Yleiset tilastotiedot luodaan automaattisesti käyttäen alkuperäisiä vastaanotettuja tietoja. Ne eivät sisällä yksityisiä tai muita luottamuksellisia tietoja. Alkuperäiset vastaanotetut tiedot säilytetään salattuina. Tietoa poistetaan sen kerääntyessä (kahdesti vuodessa). Yleiset tilastotiedot tallennetaan pysyvästi.

KÄYTTÖOIKEUDEN OSTAMINEN

Jos olet asentanut Kaspersky Total Securityn, etkä ole vielä ostanut käyttöoikeutta, voit tehdä sen asennuksen jälkeen. Kun ostat käyttöoikeuden, saat aktivointikoodin, jolla voit aktivoida sovelluksen (ks. "Sovelluksen aktivointi" sivulla 31).

Voit hankkia käyttöoikeuden seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa sijaitsevaa **Käyttöoikeus**-linkkiä, jolloin **Käyttöoikeudet**-ikkuna avautuu.
3. Napsauta avautuvassa ikkunassa **Osta aktivointikoodi** -painiketta.

Näkyviin tulee Kaspersky Lab eStoren tai kumppaniyrityksen verkkosivu, josta voit ostaa käyttöoikeuden.

SOVELLUKSEN AKTIVOINTI

Sovelluksen ominaisuuksien ja lisäpalveluiden hyödyntäminen edellyttää aktivointia.

Jos et aktivoinut sovellusta asennuksen yhteydessä, voit tehdä sen myöhemmin. Kaspersky Total Security muistuttaa sinua aktivoinnin tarpeellisuudesta tehtäväpalkin ilmoitusalueella näkyvillä viesteillä.

Aktivoi Kaspersky Total Security seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Kirjoita aktivointikoodi** -linkkiä. **Aktivointi**-ikkuna avautuu.
3. Syötä **Aktivointi**-ikkunassa aktivointikoodi asianmukaiseen kenttään ja napsauta **Aktivoi**-painiketta.

   Sovelluksen aktivointipyyntö luodaan.
4. Syötä käyttäjän rekisteröintitiedot.

   Käyttöehdoista riippuen sovellus voi kehottaa sinua kirjautumaan sisään My Kaspersky -portaaliin. Jos et ole rekisteröitynyt käyttäjä, saat käyttöösi lisätoimintoja täyttämällä rekisteröintilomakkeen.

   Rekisteröidyt käyttäjät voivat suorittaa seuraavia toimintoja:

   - Ottaa yhteyttä tukipalveluun ja viruslaboratorioon.
   - Aktivointikoodien hallinnointi.
   - Uusista sovelluksia ja erikoistarjouksia koskevien tietojen vastaanottaminen Kaspersky Labilta.

   Tämä vaihe ei ole valittavissa Kaspersky Total Securityn kaikissa versioissa.
5. Suorita rekisteröinti loppuun napsauttamalla **Lopeta**-painiketta **Aktivointi**-ikkunassa.

KÄYTTÖOIKEUDEN UUSIMINEN

Voit uusia käyttöoikeuden, kun se on vanhentumassa. Voit tehdä sen antamalla uuden aktivointikoodin ennen nykyisen käyttöoikeuden vanhenemista. Kun nykyinen käyttöoikeus vanhenee, Kaspersky Total Security aktivoidaan automaattisesti ylimääräisellä aktivointikoodilla.

Ylimääräisen aktivointikoodin määrittäminen käyttöoikeuden automaattista uusimista varten:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa sijaitsevaa **Käyttöoikeus**-linkkiä, jolloin **Käyttöoikeudet**-ikkuna avautuu.
3. Napsauta avautuvan ikkunan **Uusi aktivointikoodi** -osiossa **Kirjoita aktivointikoodi** -painiketta.
4. Kirjoita aktivointikoodi oikeisiin kenttiin ja napsauta **Lisää**-painiketta.

   Sitten Kaspersky Total Security lähettää tiedot Kaspersky Labin aktivointipalvelimelle varmennusta varten.
5. Napsauta **Lopeta**-painiketta.

Uusi aktivointikoodi näkyy **Käyttöoikeudet**-ikkunassa.

Sovellus aktivoidaan automaattisesti uudella aktivointikoodilla, kun käyttöoikeus vanhenee. Voit myös aktivoida sovelluksen uudella aktivointikoodilla manuaalisesti napsauttamalla **Aktivoi nyt** -painiketta. Tämä painike on käytettävissä, jos sovellusta ei ole aktivoitu automaattisesti. Tämä painike tulee käytettäväksi vasta, kun käyttöoikeus vanhenee.

Jos määrittämääsi aktivointikoodia on jo käytetty tällä tai toisella tietokoneella, käyttöoikeuden uusimisen osalta aktivointipäiväksi merkitään päivämäärä, jolloin sovellus aktivoitiin kyseisellä koodilla ensimmäisen kerran.

SOVELLUKSEN ILMOITUSTEN HALLINTA

Tehtäväpalkin ilmoitusalueelle tulevat ilmoitukset kertovat sinulle sovelluksen tapahtumista, jotka vaativat huomiotasi. Riippuen tapahtuman kriittisyydestä saatat saada seuraavantyyppisiä ilmoituksia:

- *Kriittiset ilmoitukset* tiedottavat tapahtumista, jotka ovat tärkeitä tietoturvan näkökulmasta, esim. haitallisen objektin tai vaarallisen toiminnan havaitseminen käyttöjärjestelmässä. Kriittisten ilmoitusten ja ponnahdusviestien käyttämät ikkunat ovat punaisia.

- *Tärkeät ilmoitukset* tiedottavat tapahtumista, jotka ovat mahdollisesti tärkeitä tietoturvan näkökulmasta, esim. todennäköisesti tartunnan saaneen objektin tai epäilyttävän toiminnan havaitseminen käyttöjärjestelmässä. Tärkeiden ilmoitusten ja ponnahdusviestien käyttämät ikkunat ovat keltaisia.

- *Tietoilmoitukset* ilmoittavat tapahtumista, joilla ei ole kriittistä merkitystä tietokoneen turvallisuudelle. Tietoilmoitusten ja ponnahdusviestien käyttämät ikkunat ovat vihreitä.

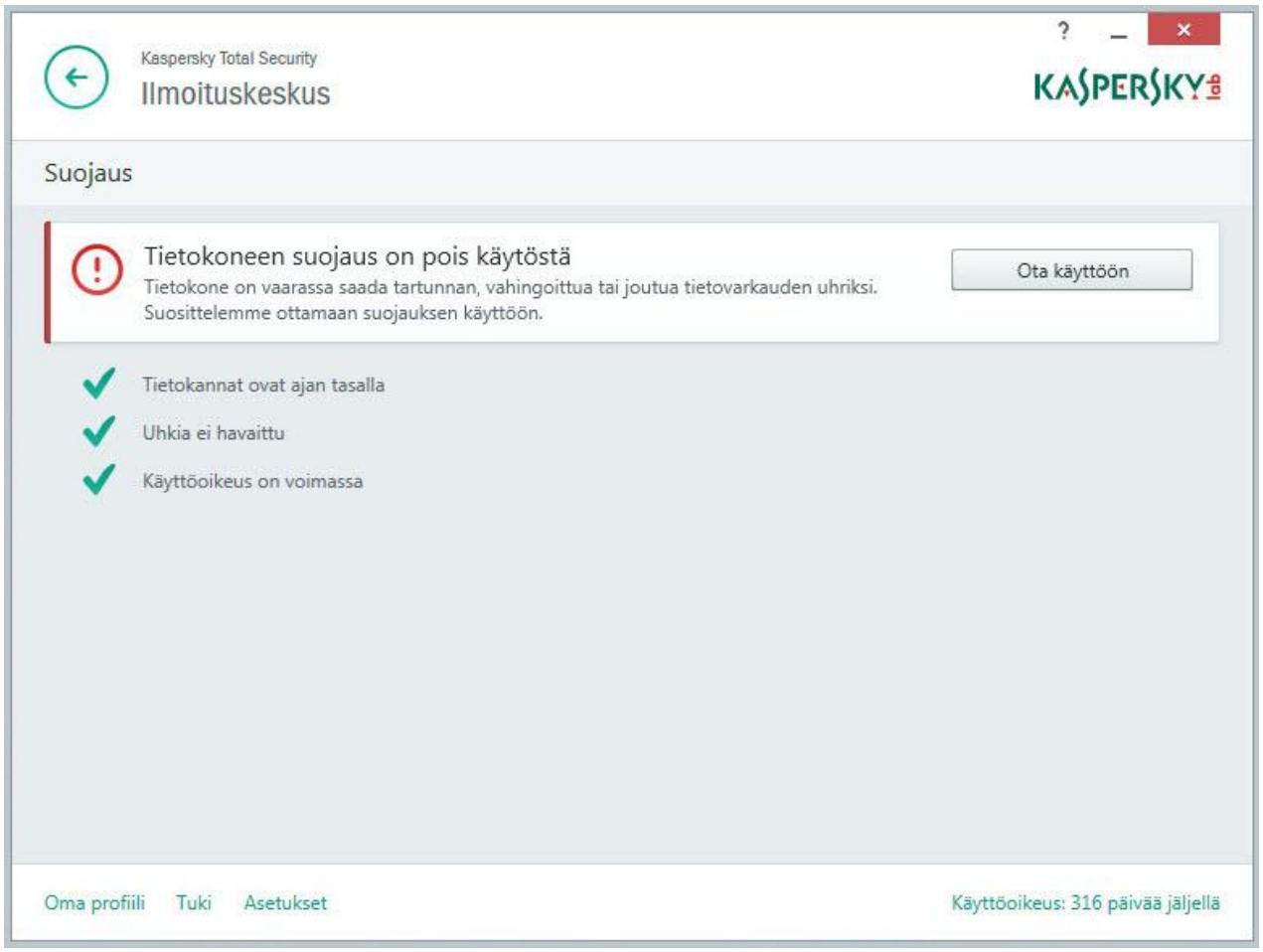
Jos tällainen ilmoitus näytetään, sinun tulee valita yksi siinä ehdotetuista vaihtoehdoista. Optimivaihtoehto on Kaspersky Labin asiantuntijoiden suosittelema vaihtoehto. Ilmoitus saatetaan sulkea automaattisesti, kun tietokone käynnistetään uudelleen, kun Kaspersky Total Security suljetaan, tai jos Microsoft Windows 8 -käyttöjärjestelmän Yhdistetty valmiustila -tila on käytössä. Kun ilmoitus suljetaan automaattisesti, Kaspersky Total Security suorittaa oletusarvoisesti suositellun toiminnon.

Ilmoituksia ei näytetä sovelluksen toiminnan ensimmäisen tunnin aikana, jos olet ostanut tietokoneen, jossa on esiasennettu Kaspersky Total Security (OEM-jakelu). Sovellus käsittelee havaitut objektit suositeltujen toimintojen mukaisesti. Käsittelyn tulokset tallennetaan raporttiin.

TIETOKONEEN SUOJAUSTILAN ARVIOINTI JA TIETOTURVAONGELMIEN RATKAISEMINEN

Tietokoneen suojauksen ongelmat ilmaistaan sovelluksen pääikkunan yläosassa sijaitsevalla ilmaisimella. Vihreä väri ilmaisee, että tietokoneesi on suojattu. Keltainen väri ilmaisee, että suojausongelmia on havaittu. Punainen väri ilmaisee, että tietokoneesi turvallisuus on vakavasti uhattuna. Ongelmat ja tietoturvauhat tulee korjata välittömästi.

Ilmaisimen napsauttaminen sovelluksen pääikkunassa avaa **Ilmoituskeskus**-ikkunan (katso seuraava kuva), joka sisältää tietoja tietokoneen suojauksen tilasta sekä viankorjausehdotuksia havaittuja ongelmia ja uhkia varten.



Kuva 1. Ilmoituskeskus -ikkuna

Suojauksen ongelmat on ryhmitelty luokkiin. Jokaista ongelmaa kohden näytetään luettelo toimenpiteistä, joiden avulla voit ratkaista ongelman.

TIETOKANTOJEN JA SOVELLUKSEN OHJELMISTOMODUULIEN PÄIVITYS

Oletusasetuksena on, että Kaspersky Total Security tarkistaa automaattisesti, onko Kaspersky Labin päivityspalvelimien kautta saatavilla uusia päivityksiä. Jos palvelimella on uusi päivityspaketti, Kaspersky Total Security lataa ja asentaa sen taustalla. Voit suorittaa Kaspersky Total Security -päivityksen manuaalisesti milloin tahansa sovelluksen pääikkunasta tai tehtäväpalkin ilmoitusalueella olevan sovelluskuvakkeen pikavalikosta.

Päivityspaketin lataaminen Kaspersky Labin palvelimilta edellyttää, että käytössäsi on Internet-yhteys.

Microsoft Windows 8 -käyttöjärjestelmällä varustetussa tietokoneessa päivityspaketteja ei ladata, jos Internet-laajakaistayhteys on muodostettu ja tämän yhteystyypin datansiirtomäärää on rajoitettu. Jotta voit ladata päivityspaketin, sinun täytyy poistaa rajoitus Sovellusasetukset-ikkunan **Verkko**-aliosiossa.

- *Voit suorittaa päivityksen tehtäväpalkin sovelluskuvakkeen pikavalikosta seuraavasti:*

  Valitse sovelluskuvakkeen pikavalikosta **Päivitys**-kohta.

- *Voit suorittaa päivityksen sovelluksen pääikkunasta seuraavasti:*

  1. Avaa sovelluksen pääikkuna ja napsauta **Päivitys**-painiketta.

     Päivitys-ikkuna avautuu.

  2. Napsauta **Päivitys**-ikkunassa **Päivitys**-painiketta.

TIETOKONEEN TARKISTAMINEN

Tämä osio sisältää tietoja siitä, miten tarkistaa tietokone virusten ja muiden uhkien varalta.

TÄSSÄ OSIOSSA

TÄYDELLINEN TARKISTUS

Täyden tarkistuksen aikana Kaspersky Total Security tarkistaa oletuksena seuraavat objektit:

- Järjestelmän muisti
- Järjestelmän käynnistyksen yhteydessä ladatut objektit
- Taltio
- Kiintolevyt ja siirrettävät levyt

Suosittelemme, että suoritat täydellisen tarkistuksen välittömästi, kun olet asentanut Kaspersky Total Securityn tietokoneellesi.

Voit aloittaa täydellisen tarkistuksen seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Tarkista**-painiketta.

   Tarkista-ikkuna avautuu.
3. Valitse **Tarkista**-ikkunassa oleva **Täydellinen tarkistus** -osio.
4. Napsauta **Täydellinen tarkistus** -osiossa **Suorita tarkistus**-painiketta.

Kaspersky Total Security aloittaa tietokoneen täydellisen tarkistuksen.

MUKAUTETTU TARKISTUS

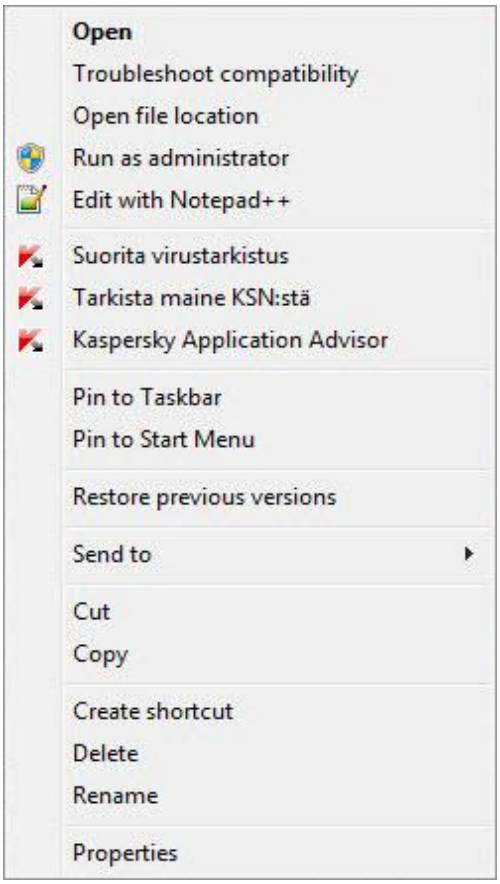
Mukautetun tarkistuksen avulla voit tarkistaa tiedoston, kansion tai aseman viruksien ja muiden uhkien varalta.

Voit aloittaa mukautetun tarkistuksen seuraavasti:

- Objektin pikavalikosta
- Pääsovellusikkunasta

Voit aloittaa mukautetun tarkistuksen objektin pikavalikosta seuraavasti:

1. Avaa Microsoft Windowsin Resurssienhallinta ja siirry kansioon, joka sisältää tarkistettavan objektin.
2. Avaa objektin pikavalikko (katso seuraava kuva) napsauttamalla hiiren kakkospainikkeella ja valitse **Suorita virustarkistus**.



Kuva 2. Objektin pikavalikko

Voit aloittaa mukautetun tarkistuksen sovelluksen pääikkunasta seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Tarkista**-painiketta.

   Tarkista-ikkuna avautuu.
3. Valitse **Tarkista**-ikkunassa oleva **Mukautettu tarkistus** -osio.
4. Määritä tarkistettavat objektit käyttäen jotain seuraavista menetelmistä:
   - Vedä objektit **Mukautettu tarkistus** -ikkunaan.
   - Napsauta **Lisää**-painiketta ja määritä objekti avautuvassa tiedoston tai kansion valintaikkunassa.
5. Napsauta **Suorita tarkistus** -painiketta.

PIKATARKISTUS

Pikatarkistuksen aikana Kaspersky Total Security tarkistaa oletuksena seuraavat objektit:

- Käyttöjärjestelmän käynnistyksen yhteydessä ladattavat objektit
- Järjestelmän muisti
- Levyn käynnistyssektorit

Voit aloittaa pikatarkistuksen seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Tarkista**-painiketta.

   Tarkista-ikkuna avautuu.
3. Valitse **Tarkista**-ikkunassa oleva **Pikatarkistus** -osio.
4. Napsauta **Pikatarkistus**-osiossa **Suorita tarkistus** -painiketta.

Kaspersky Total Security aloittaa tietokoneen pikatarkistuksen.

HEIKKOUSTARKISTUS

Heikkoudet ovat ohjelmistokoodin suojaamattomia osia, joita tunkeilijat voivat tarkoituksellisesti käyttää omiin tarkoituksiinsa, esimerkiksi suojaamattomissa sovelluksissa käytettyjen tietojen kopiointiin. Tietokoneesi heikkoustarkistus auttaa sinua paljastamaan tällaiset heikot kohdat tietokoneesi suojauksessa. Suosittelemme korjaamaan kaikki löytyvät heikkoudet.

Voit aloittaa heikkoustarkistuksen seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa **Heikkoustarkistus**-ikkuna napsauttamalla **Työkalut**-ikkunan vasemmassa reunassa olevaa **Heikkoustarkistus**-linkkiä.
4. Napsauta **Heikkoustarkistus**-ikkunassa **Suorita tarkistus** -painiketta.

Kaspersky Total Security aloittaa tietokoneen tarkistuksen heikkouksien varalta.

SOVELLUKSEN POISTAMAN TAI PUHDISTAMAN OBJEKTIN PALAUTTAMINEN

Kaspersky Lab suosittelee välttämään poistettujen tai puhdistettujen objektien palauttamista, koska ne saattavat olla uhka tietokoneellesi.

Voit palauttaa poistetun tai puhdistetun objektin käyttämällä varmuuskopiota, jonka sovellus on luonut objektin tarkistuksen yhteydessä.

Kaspersky Total Security ei puhdista Windows-kaupasta ladattuja sovelluksia. Jos tarkistuksen tulokset osoittavat sellaisen sovelluksen olevan vaarallinen, se poistetaan tietokoneeltasi.

Kun Windows-kaupasta ladattu sovellus poistetaan, Kaspersky Total Security ei luo siitä varmuuskopiota. Tällaisten objektien palauttaminen edellyttää käyttöjärjestelmän palautustyökalujen käyttöä (katso lisätietoja tietokoneesi käyttöjärjestelmän dokumentaatiosta) tai sovellusten päivittämistä Windows-kaupan kautta.

Voit palauttaa sovelluksen poistaman tai puhdistaman tiedoston seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Napsauta **Työkalut**-ikkunan vasemmassa reunassa olevaa **Karanteeni**-linkkiä avataksesi **Karanteeni**-ikkunan.
4. Valitse avautuvassa **Karanteeni**-ikkunassa olevasta luettelosta määrätty tiedosto ja napsauta sitten **Palauta**-painiketta.

KÄYTTÖJÄRJESTELMÄN VIANMÄÄRITYS TARTUNNAN JÄLKEEN

Tämä osio sisältää tietoja siitä, miten palauttaa käyttöjärjestelmä sen jälkeen, kun se on saanut virustartunnan.

TÄSSÄ OSIOSSA

KÄYTTÖJÄRJESTELMÄN PALAUTTAMINEN TARTUNNAN JÄLKEEN

Jos epäilet, että tietokoneesi käyttöjärjestelmä on vaurioitunut tai muuttunut haittaohjelman toiminnan tai järjestelmävian seurauksena, käytä *ohjattua Microsoft Windows -vianmääritystoimintoa*, joka puhdistaa järjestelmästä haitallisten objektien jättämät jäljet. Kaspersky Lab suosittelee, että suoritat ohjatun toiminnon sen jälkeen, kun tartunta on poistettu tietokoneestasi. Näin voit varmistaa, että kaikki uhkat ja tartuntojen aiheuttama vahinko on korjattu.

Ohjattu toiminto tarkistaa, onko järjestelmään tehty muutoksia kuten verkkoyhteyden käytön estäminen, tunnettujen tiedostomuotojen tiedostopäätteiden muuttaminen tai Ohjauspaneelin käytön estäminen. Erilaisille vaurioille on erilaisia syitä. Tällaisia syitä ovat esimerkiksi haittaohjelmien toiminta, virheelliset järjestelmämääritykset, järjestelmävirheet tai järjestelmän optimointitoimintojen virheellinen toiminta.

Kun tarkistus on tehty loppuun, ohjattu toiminto analysoi tiedot arvioidakseen, onko järjestelmässä vaurioita, jotka vaativat välitöntä huomiota. Ohjattu toiminto luo tarkistuksen perusteella luettelon toiminnoista, jotka täytyy tehdä vaurioiden korjaamiseksi. Ohjattu toiminto luokittelee nämä toiminnot sen perusteella, miten vakavia havaitut ongelmat ovat.

KÄYTTÖJÄRJESTELMÄN VIANMÄÄRITYKSEN SUORITTAMINEN MICROSOFT WINDOWSIN OHJATUN VIANMÄÄRITYSTOIMINNON AVULLA

- *Voit suorittaa Microsoft Windowsin ohjatun vianmääritystoiminnon seuraavasti:*

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Käynnistä Microsoft Windowsin ohjattu vianmääritystoiminto napsauttamalla **Työkalut**-ikkunan vasemmassa reunassa olevaa **Microsoft Windows -vianetsintä** -linkkiä.

Microsoft Windowsin ohjattu vianmääritystoiminto -ikkuna avautuu.

Ohjattu toiminto koostuu ikkunoista (vaiheista), joissa liikutaan painikkeilla **Takaisin** ja **Seuraava**. Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta. Voit keskeyttää ohjatun toiminnon milloin tahansa napsauttamalla **Peruuta**-painiketta.

Alla on tarkempia tietoja ohjatusta toiminnosta.

Vaihe 1. Käyttöjärjestelmän palautuksen aloittaminen

Varmista, että ohjatun toiminnon asetus **Hae haittaohjelmien toiminnan aiheuttamia vaurioita** on valittuna, ja napsauta **Seuraava**-painiketta.

Vaihe 2. Ongelmien haku

Ohjattu toiminto etsii ongelmia ja vaurioita, jotka tulisi korjata. Kun haku on valmis, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Vaihe 3. Valitse toimenpiteet vaurioiden korjaamiseksi

Kaikki aiemman vaiheen aikana löydetyt vauriot ryhmitellään niiden aiheuttaman vaaran mukaan. Kunkin vaurioryhmän kohdalla Kaspersky Lab suosittelee tiettyä toimintosarjaa vahinkojen korjaamiseksi. Toimenpiteet on jaettu kolmeen ryhmään:

- *Vahvasti suositellut toiminnot* poistavat ongelmia, jotka aiheuttavat vakavan turvallisuusuhan. Suosittelemme, että suoritat kaikki tämän ryhmän toimenpiteet.
- *Suositellut toiminnot* auttavat poistamaan mahdollisesti uhan aiheuttavia ongelmia. Suosittelemme, että suoritat myös kaikki tämän ryhmän toimenpiteet.
- *Lisätoiminnot* korjaavat järjestelmän vahinkoja, jotka eivät aiheuta uhkaa nyt, mutta voivat vaarantaa tietokoneen turvallisuuden tulevaisuudessa.

Voit tarkastella tietyn ryhmän sisältämiä toimintoja napsauttamalla (plusmerkki) -kuvaketta ryhmän nimen vasemmalla puolella.

Jos haluat ohjatun toiminnon suorittavan jonkin toimenpiteen, valitse toimenpiteen vasemmalla puolella oleva valintaruutu. Oletusasetuksena on, että ohjattu toiminto suorittaa kaikki suositellut ja vahvasti suositellut toiminnot. Jos et halua suorittaa jotakin tiettyä toimintoa, poista valinta sen vieressä olevasta valintaruudusta.

Suosittelemme, että et poista valintaa oletuksena valituista ruuduista, sillä tämä voi tehdä tietokoneesta haavoittuvan uhille.

Kun olet määrittänyt toimenpiteet ohjatun toiminnon suoritusta varten, napsauta **Seuraava**-painiketta.

Vaihe 4. Vaurioiden korjaaminen

Ohjattu toiminto suorittaa edellisen vaiheen aikana valitut toiminnot. Vaurioiden korjaamisessa voi kestää jonkin aikaa. Kun vaurioiden korjaaminen on valmis, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Vaihe 5. Ohjatun toiminnon viimeistely

Sulje ohjattu toiminto napsauttamalla **Lopeta**-painiketta.

SÄHKÖPOSTIVIESTIEN SUOJAAMINEN

Tämä osio sisältää tietoja siitä, miten suojata sähköposti roskapostilta, viruksilta ja muilta uhkilta.

TÄSSÄ OSIOSSA

SÄHKÖPOSTIN VIRUSTORJUNNAN MÄÄRITTÄMINEN

Kaspersky Total Security voi tarkistaa sähköpostiviestejä vaarallisten objektien varalta käyttämällä Sähköpostin virustorjuntaa. Sähköpostin virustorjunta käynnistyy käyttöjärjestelmän käynnistyessä ja pysyy keskusmuistissa jatkuvasti. Se tarkistaa kaikki POP3-, SMTP-, IMAP-, MAPI- ja NNTP-yhteydellä sekä salatulla (SSL) POP3-, SMTP- ja IMAP-yhteydellä lähetetyt ja vastaanotetut viestit.

Oletuksena Sähköpostin virustorjunta tarkistaa sekä saapuvat että lähtevät viestit. Tarvittaessa voit ottaa käyttöön vain saapuvien viestien tarkistuksen.

Voit määrittää Sähköpostin virustorjunnan asetukset seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä.
3. Valitse ikkunan vasemmalla puolella olevasta **Suojaus**-osiosta **Sähköpostin virustorjunta** -komponentti.

   Sähköpostin virustorjunnan asetukset näkyvät ikkunassa.
4. Varmista, että ikkunan yläosassa oleva valitsin, joka ottaa käyttöön / poistaa käytöstä Sähköpostin virustorjunnan, on käytössä.
5. Valitse turvallisuustaso:
   - **Suositellaan**. Jos valitset tämän turvallisuustason, Sähköpostin virustorjunta tarkistaa sekä saapuvat että lähtevät viestit ja tarkistaa liitetyt arkistot.
   - **Alhainen**. Jos valitset tämän turvallisuustason, Sähköpostin virustorjunta tarkistaa vain saapuvat viestit eikä se tarkista liitettyjä arkistoja.
   - **Korkea**. Jos valitset tämän turvallisuustason, Sähköpostin virustorjunta tarkistaa sekä saapuvat että lähtevät viestit ja tarkistaa liitetyt arkistot. Kun valitset korkean turvallisuustason, syvä heuristinen analyysi kytketään päälle.
6. Valitse **Toimenpide havaittaessa uhka** -pudotusluettelosta toiminto, jonka Sähköpostin virustorjunta suorittaa havaitessaan tartunnan saaneen objektin (esimerkiksi poista tartunta).

Jos uhkia ei ole havaittu sähköpostiviestissä tai jos kaikkien tartunnan saaneiden objektien tartunnan poisto onnistuu, viesti vapautuu muita toimenpiteitä varten. Jos komponentti epäonnistuu tartunnan saaneen objektin tartunnan poistamisessa, Sähköpostin virustorjunta nimeää uudelleen tai poistaa objektin viestistä ja lisää viestin aiheeseen huomautuksen siitä, että Kaspersky Total Security on käsitellyt viestin. Ennen objektin poistamista Kaspersky Total Security luo siitä varmuuskopion ja asettaa kopion Karanteeniin (ks. "Sovelluksen poistaman tai puhdistaman objektin palauttaminen" sivulla 39).

EI-HALUTTUJEN SÄHKÖPOSTIEN (ROSKAPOSTIN) ESTÄMINEN

Jos saat suuren määrän roskapostia, ota käyttöön Roskapostin esto -komponentti ja aseta suositeltu turvallisuustaso.

Voit ottaa Roskapostin eston käyttöön ja asettaa sen suositellulle turvallisuustasolle seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä. Siirry **Asetukset**-osioon.
3. Valitse ikkunan vasemmassa reunassa oleva **Suojaus**-osio.
4. Valitse **Suojaus**-osion oikeasta reunasta **Roskapostin esto** -komponentti.

   Näyttöön tulevat Roskapostin eston asetukset.
5. Ikkunan oikeanpuoleisessa osassa voit ottaa Roskapostin eston käyttöön valitsimella.
6. Varmista, että **Tietoturvataso**-osiossa on valittuna **Suositeltu** turvallisuustaso.

YKSITYISTEN TIETOJEN SUOJAAMINEN INTERNETISSÄ

Tämä osio sisältää tietoja siitä, miten tehdä Internetin selaamisesta turvallista ja kuinka suojata tietosi varkaudelta.

TÄSSÄ OSIOSSA

YKSITYISTEN TIETOJEN SUOJAAMINEN INTERNETISSÄ

Kaspersky Total Security auttaa sinua suojaamaan yksityiset tietosi varkauksien varalta:

- Salasanat, käyttäjänimet ja muut rekisteröintitiedot
- Tilinumerot ja pankkikorttien numerot

Kaspersky Total Security sisältää osia ja työkaluja, joilla voit suojata yksityiset tietosi varkausyrityksiltä, joissa hyödynnetään sellaisia menetelmiä kuin verkkohuijaukset tai näppäimistöllä annettujen tietojen sieppaaminen.

Suojaus verkkohuijauksia vastaan varmistetaan Verkkohuijausten estolla, joka on asennettu Verkon virustorjunta-, Roskapostin esto- ja Pikaviestinnän virustorjunta -komponentteihin. Ottamalla nämä komponentit käyttöön varmistat kattavan suojauksen verkkohuijauksia vastaan.

Tietokoneen näppäimistöllä syötettyjen tietojen suojaus tapahtuu virtuaalisen näppäimistön ja suojatun näppäimistön syöttötilan avulla.

Yksityisten tietojen ohjattu poistamistoiminto tyhjentää tietokoneen kaikista käyttäjän toimiin liittyvistä tiedoista.

Rahasuojaus suojaa tiedot, kun käytät verkkopankkeja ja teet ostoksia verkkokaupoissa.

Yksityisten tietojen siirtäminen internetin kautta on estetty Käytönvalvonnan työkalun avulla (ks. "Käytönvalvonnan käyttö" sivulla 60).

TIETOJA VIRTUAALISESTA NÄPPÄIMISTÖSTÄ

Verkossa on usein tarpeen syöttää yksityisiä tietoja tai käyttäjänimiä ja salasanoja. Tämä tapahtuu esimerkiksi silloin, kun kirjaudut sisään sivustoihin, teet ostoksia tai käytät verkkopankkia.

On olemassa uhka, että syöttämäsi henkilökohtaiset tiedot kaapataan ja kopioidaan näppäinpainallusten tallentajan (eli keylogger-ohjelman) avulla. Virtuaalinen näppäimistö estää näppäimistön kautta syötettyjen tietojen kaappaamisen.

Monet vakoiluohjelmiksi luokitellut sovellukset pystyvät ottamaan näyttökaappauksia, jotka sitten siirretään luvattomien käyttäjien haltuun analysointia ja henkilökohtaisten tietojen varastamista varten. Virtuaalinen näppäimistö suojaa sillä syötettyjä henkilökohtaisia tietoja näyttökaappauksien avulla tapahtuvilta kaappausyrityksiltä.

Virtuaalisessa näppäimistössä on seuraavat ominaisuudet:

- Voit painaa virtuaalisen näppäimistön näppäimiä hiirtä käyttämällä.
- Toisin kuin laitenäppäimistöä käytettäessä, kahden näppäimen painaminen samanaikaisesti ei ole mahdollista virtuaalisessa näppäimistössä. Siksi näppäinyhdistelmät (kuten **ALT**+**F4**),on tehtävä napsauttamalla ensimmäistä näppäintä (esim. **ALT**), sitten toista näppäintä (esim. **F4**), ja lopuksi uudelleen ensimmäistä näppäintä. Toinen näppäimen napsautus vastaa näppäimen vapauttamista laitenäppäimistössä.
- Virtuaalisen näppäimistön kieltä voidaan vaihtaa samasta pikakuvakkeesta kuin laitenäppäimistön asetuksia käyttöjärjestelmässä. Napsauta toista näppäintä hiiren oikealla painikkeella (jos esimerkiksi näppäinyhdistelmä **VASEN ALT**+**VAIHTO** on määritetty käyttöjärjestelmässä näppäimistökielen vaihtamista varten, napsauta hiiren vasemmalla painikkeella **VASEN ALT** -näppäintä ja sitten hiiren oikealla painikkeella **VAIHTO**-näppäintä).

Varmista virtuaalisella näppäimistöllä syötettyjen tietojen suojaus käynnistämällä tietokone uudelleen sen jälkeen, kun Kaspersky Total Security on asennettu.

Virtuaalisen näppäimistön käyttöä koskevat seuraavat rajoitukset:

- Virtuaalinen näppäimistö estää yksityisten tietojen kaappaamisen vain silloin, kun käytettävä selain on Microsoft Internet Explorer, Mozilla Firefox tai Google Chrome. Jos käytössä on muu selain, virtuaalinen näppäimistö ei suojaa henkilötietojasi tietojen sieppaamisen varalta.
- Virtuaalinen näppäimistö ei ole käytettävissä Microsoft Internet Explorer 10:ssä tai 11:ssä, jotka käyttävät Windows 8 -tyyliä, tai Microsoft Internet Explorer 10:ssä tai 11:ssä, jos **Ota tehostettu suojaustila käyttöön** -valintaruutu on valittu selainasetuksissa. Tässä tapauksessa suosittelemme käyttämään virtuaalista näppäimistöä Kaspersky Total Securityn käyttöliittymän kautta.
- Virtuaalinen näppäimistö ei pysty suojaamaan henkilökohtaisia tietojasi, jos kyseisiä tietoja vaativaan sivustoon on murtauduttu - tässä tapauksessa asiattomat käyttäjät saavat tiedot käsiinsä suoraan sivustosta.
- Virtuaalinen näppäimistö ei estä näyttökuvien ottamista **PRINT SCREEN** -näppäimellä tai muilla käyttöjärjestelmässä toimivilla näppäinyhdistelmillä.
- Virtuaalista näppäimistöä käytettäessä Microsoft Internet Explorerin automaattinen täydennystoiminto ei enää toimi, sillä rikolliset voivat kaapata tietoja automaattisen syöttötavan kautta.
- Kaspersky Total Security ei estä luvattomien näyttökuvien tallentamista Microsoft Windows 8- ja 8.1-käyttöjärjestelmissä (vain 64-bittiset versiot), jos virtuaalinen näppäimistö on käytössä, mutta Suojattu selain -prosessia ei ole käynnistetty.
- Joissakin selaimissa (kuten Google Chromessa), syötetyn tiedon suojaus ei ehkä toimi kaikille tietotyypeille (kuten sähköpostiosoitteille tai numeroille).

Edellä olevassa luettelossa on kuvattu tiedon syöttämisen suojauksen olennaiset rajoitukset. Täydellinen luettelo rajoituksista on Kaspersky Labin teknisen tuen verkkosivuston artikkelissa http://support.kaspersky.com/11048.

VIRTUAALISEN NÄPPÄIMISTÖN KÄYNNISTÄMINEN

Voit avata virtuaalisen näppäimistön seuraavilla tavoilla:

- Tehtäväpalkin ilmoitusalueen sovelluskuvakkeen pikavalikosta
- Pääsovellusikkunasta
- Napsauttamalla virtuaalisen näppäimistön käyttökuvaketta Microsoft Internet Explorerista, Mozilla Firefoxista tai Google Chromesta
- Käyttämällä verkkosivustojen syötekentissä olevaa virtuaalisen näppäimistön pikakäynnistyskuvaketta

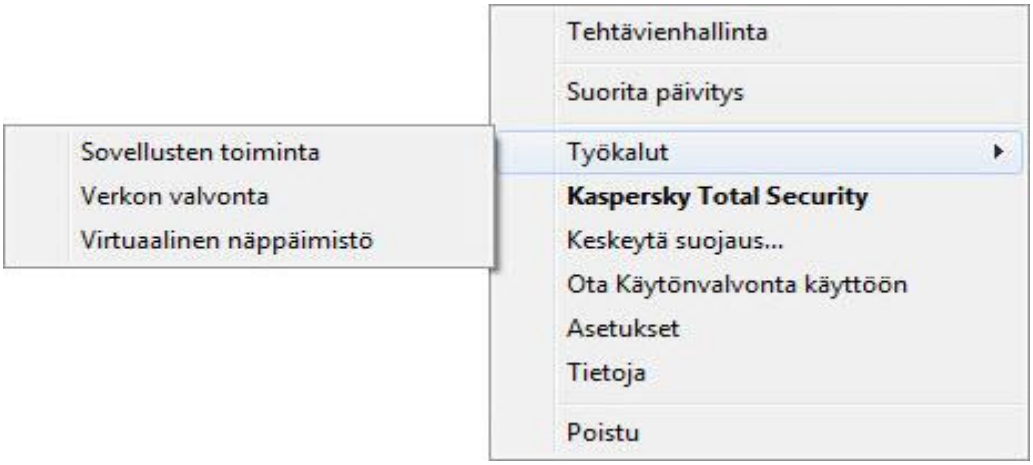
  Voit määrittää pikakäynnistyskuvakkeen näkymisen verkkosivustojen syöttökentissä (katso osiota "Virtuaalisen näppäimistön kuvakkeen näkyvyysasetuksien määrittäminen" sivulla 47).

  Kun käytät virtuaalista näppäimistöä, Kaspersky Total Security kytkee verkkosivustojen tekstikenttien automaattisen täytön pois päältä.

- Painamalla näppäinyhdistelmää.

Voit avata virtuaalisen näppäimistön tehtäväpalkin ilmoitusalueen sovelluskuvakkeen pikavalikosta seuraavasti:

Valitse sovelluskuvakkeen pikavalikosta (katso seuraava kuva) **Työkalut** → **Virtuaalinen näppäimistö**.



Kuva 3. Kaspersky Total Securityn pikavalikko

Voit avata virtuaalisen näppäimistön sovelluksen pääikkunasta seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa virtuaalinen näppäimistö napsauttamalla **Työkalut**-ikkunan vasemmassa reunassa olevaa **Virtuaalinen näppäimistö** -linkkiä.

Voit avata virtuaalisen näppäimistön Microsoft Internet Explorer- tai Mozilla Firefox -selaimen ikkunassa

napsauttamalla selaimen työkalupalkissa sijaitsevaa  **Virtuaalinen näppäimistö** -painiketta.

- *Voit avata virtuaalisen näppäimistön Google Chrome -selaimen ikkunassa*

  1. napsauttamalla selaimen työkalupalkissa sijaitsevaa **Kaspersky Protection** -painiketta.
  2. Valitse avautuvassa valikossa kohde **Virtuaalinen näppäimistö**.

- *Voit avata virtuaalisen näppäimistön laitenäppäimistön avulla seuraavasti:*

  Käytä seuraavaa näppäinyhdistelmää: **CTRL**+**ALT**+**VAIHTO**+**P**.

VIRTUAALISEN NÄPPÄIMISTÖN KUVAKKEEN NÄKYVYYSASETUKSIEN MÄÄRITTÄMINEN

- *Voit määrittää virtuaalisen näppäimistön pikakäynnistyskuvakkeen näkyvyyden verkkosivustojen syötekentissä seuraavasti:*

  1. Avaa sovelluksen pääikkuna.
  2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä.
  3. Näyttöön avautuvassa **Asetukset**-ikkunassa valitse **Lisäasetukset**-osiosta **Suojattu syöttötila**.

     Näyttöön tulevat tietojen suojatun syötön asetukset.
  4. Valitse tarvittaessa **Virtuaalinen näppäimistö** -osiossa **Avaa virtuaalinen näppäimistö painettaessa CTRL+ALT+VAIHTO+P** -valintaruutu.
  5. Jos haluat, että virtuaalisen näppäimistön pikakäynnistyskuvake näkyy syötekentissä, valitse **Näytä pikakäynnistyskuvake syötekentissä** -valintaruutu.
  6. Jos haluat, että virtuaalisen näppäimistön pikakäynnistyskuvake näkyy vain määrätyillä verkkosivustoilla, toimi seuraavasti:
     a. Napsauta **Virtuaalinen näppäimistö** -osion **Muokkaa luokkia** -linkkiä, jolloin **Suojatun syöttötilan asetukset** -ikkuna avautuu.
     b. Valitse niiden verkkosivustojen luokkien valintaruudut, joiden syötekentissä haluat pikakäynnistyskuvakkeen näkyvän.

        Virtuaalisen näppäimistön pikakäynnistyskuvake tulee näkyviin avattaessa verkkosivustoa, joka kuuluu mihin tahansa valituista luokista.
     c. Jos haluat kytkeä virtuaalisen näppäimistön pikakäynnistyskuvakkeen näkyviin tai pois näkyvistä määrätyllä verkkosivustolla:
        a. Napsauttamalla **Määritä poissulkemiset** -linkkiä voit avata **Virtuaalisen näppäimistön poissulkemiset** -ikkunan.
        b. Napsauta **Lisää**-painiketta ikkunan alaosassa.

           Näyttöön avautuu ikkuna virtuaalisen näppäimistön poissulkemisen lisäämistä varten.
        c. Syötä verkkosivuston verkko-osoite **URL-peite**-kenttään.
        d. Jos haluat, että virtuaalisen näppäimistön pikakäynnistyskuvake näkyy (tai ei näy) vain määrätyllä verkkosivustolla, valitse **Laajuus**-osiossa **Ota käyttöön määritetyllä sivulla**.
        e. Määritä **Virtuaalisen näppäimistön kuvake** -osiossa, näytetäänkö virtuaalisen näppäimistön pikakäynnistyskuvake määrätyllä verkkosivulla.
        f. Napsauta **Lisää**-painiketta.

           Määritetty verkkosivusto tulee näkyviin luetteloon **Virtuaalisen näppäimistön poissulkemiset** -ikkunassa.

  Kun avaat määritetyn verkkosivuston, virtuaalisen näppäimistön pikakäynnistyskuvake tulee määritettyjen asetusten mukaisesti näkyviin sivuston syötekenttiin.

TIETOKONEEN NÄPPÄIMISTÖLLÄ SYÖTETTYJEN TIETOJEN SUOJAAMINEN

Tietokoneen näppäimistöllä syötettyjen tietojen suojaamisella ehkäistään näppäimistöllä syötettyjen tietojen varastaminen.

Näppäimistöllä syötettyjen tietojen suojauksella on seuraavat rajoitukset:

- Tietokoneen näppäimistöllä syötettyjen tietojen suojaaminen on käytössä vain Microsoft Internet Explorer-, Mozilla Firefox- ja Google Chrome -selaimissa. Muita verkkoselaimia käytettäessä tietokoneen näppäimistöllä syötettyjä tietoja ei ole suojattu varkauksien varalta.
- Suojattu näppäimistön syöttötila ei ole saatavilla Windows-kaupasta ladatulle Microsoft Internet Explorerille.
- Tietokoneen näppäimistöllä syötettyjen tietojen suojaaminen ei suojaa henkilötietojasi, jos tällaisten tietojen syöttämistä edellyttävä verkkosivusto on hakkeroitu, koska tällöin tunkeutujat saavat tiedot suoraan verkkosivustolta.
- Joissakin selaimissa (kuten Google Chromessa), syötetyn tiedon suojaus ei ehkä toimi kaikille tietotyypeille (kuten sähköpostiosoitteille tai numeroille).

Edellä olevassa luettelossa on kuvattu tiedon syöttämisen suojauksen olennaiset rajoitukset. Täydellinen luettelo rajoituksista on Kaspersky Labin teknisen tuen verkkosivuston artikkelissa http://support.kaspersky.com/11048.

Voit määrittää tietokoneen näppäimistöllä syötettyjen tietojen suojaamisen eri verkkosivustoille. Kun tietokoneen näppäimistöllä syötettyjen tietojen suojaus on määritetty, sinun ei tarvitse tehdä muita toimenpiteitä tietoja syöttäessäsi.

Määritä tietokoneen näppäimistöllä syötettävien tietojen suojaaminen seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä. Siirry **Asetukset**-osioon.
3. Näyttöön avautuvassa **Lisäasetukset**-osiossa valitse **Suojattu syöttötila** -aliosio.

   Näyttöön tulevat tietojen suojatun syötön asetukset.
4. Ikkunan alaosassa olevassa **Suojattu näppäimistön syöttötila** -osiossa valitse **Ota käyttöön Suojattu näppäimistön syöttötila** -valintaruutu.
5. Määritä laitenäppäimistöllä syötettävien tietojen suojauksen laajuus:
   a. Avaa **Suojatun syöttötilan asetukset** -ikkuna napsauttamalla **Muokkaa luokkia** -linkkiä **Suojattu näppäimistön syöttötila** -osion alaosassa.
   b. Valitse niiden verkkosivustoluokkien valintaruudut, joissa näppäimistöllä syötettävät tiedot tulisi suojata.
   c. Jos haluat suojata näppäimistöllä syötetyt tiedot määrätyllä verkkosivustolla:
      a. Avaa **Suojatun näppäimistön syöttötilan poissulkemiset** -ikkuna napsauttamalla **Määritä poissulkemiset** -linkkiä.
      b. Napsauta avautuvassa ikkunassa **Lisää**-painiketta.

         Näyttöön avautuu ikkuna, jossa voi lisätä poissulkemisen Suojattuun näppäimistön syöttötilaan.
      c. Kirjoita verkkosivuston verkko-osoite avautuvan ikkunan **URL-peite**-kenttään.
      d. Valitse yksi vaihtoehtoisista Suojatun syöttötilan menetelmistä tälle sivustolle (**Ota käyttöön määritetyllä verkkosivulla** tai **Ota käyttöön koko verkkosivustolla**).
      e. Valitse toiminto, jonka Suojattu syöttötila suorittaa tällä verkkosivustolla (**Suojaa** tai **Älä suojaa**).
      f. Napsauta **Lisää**-painiketta.

Määritetty verkkosivusto tulee näkyviin luetteloon **Suojatun näppäimistön syöttötilan poissulkemiset** -ikkunassa. Kun tämä verkkosivusto avataan, Suojattu syöttötila aktivoituu ja toimii määrittämiesi asetusten mukaan.

WI-FI-VERKOISSA OLEVIA HEIKKOUKSIA KOSKEVIEN ILMOITUSTEN MÄÄRITTÄMINEN

Kun olet yhteydessä heikosti suojattuun Wi-Fi-verkkoon, luottamukselliset tietosi voidaan varastaa. Kaspersky Total Security tarkastaa Wi-Fi-verkot aina, kun liityt sellaiseen. Jos Wi-Fi-verkko on turvaton (jos esimerkiksi käytössä on heikko salausprotokolla tai jos verkon nimi (SSID) on hyvin yleinen), sovellus ilmoittaa, että yhteyttä ollaan muodostamassa turvattomaan Wi-Fi-verkkoon. Napsauttamalla ilmoitusikkunassa näkyvää linkkiä saat lisätietoja Wi-Fi-verkkojen turvallisesta käytöstä.

Jos haluat määrittää Wi-Fi-verkkojen heikkousilmoitukset, toimi seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä. Siirry **Asetukset**-osioon.
3. Valitse ikkunan vasemmassa reunassa oleva **Suojaus**-osio.
4. Valitse **Suojaus**-osion oikeasta reunasta **Palomuuri**-komponentti.

   Näyttöön tulevat Palomuuri-komponentin asetukset.
5. Valitse **Ilmoita Wi-Fi-verkkojen heikkouksista** -valintaruutu, jos se ei ole valittuna. Poista valinta ruudusta, jos et halua nähdä ilmoituksia. Valinta on oletuksena valittuna.
6. Jos **Ilmoita Wi-Fi-verkkojen heikkouksista** -valintaruutu on valittuna, voit muokata ilmoitusten näyttämistä koskevia lisäasetuksia:

   - Valitsemalla **Estä suojaamattoman salasanan välittäminen Internetissä ja anna siitä varoitus** -valintaruudun voit estää salasanojen lähettämisen salaamattomana tietona täyttäessäsi Internet-lomakkeiden **Salasana**-kenttiä. Valinta ei oletuksena ole valittuna.
   - Napsauttamalla **Nollaa piilotetut ilmoitukset** -linkkiä voit palauttaa salaamattomien salasanojen lähettämistä koskevat ilmoitukset oletusarvoihinsa. Jos olet aiemmin estänyt ilmoitukset salasanojen lähettämisestä salaamattomassa muodossa, ilmoitusten näyttäminen jatkuu.

RAHATAPAHTUMIEN JA VERKKO-OSTOSTEN SUOJAAMINEN

Kaspersky Total Security tarjoaa mahdollisuuden suojata pankkien ja maksujärjestelmien verkkosivustoille syöttämäsi luottamukselliset tiedot (kuten pankkikorttien numerot sekä pankkipalvelujen salasanat) ja estää rahavarkaudet verkkomaksuissa avaamalla tällaiset sivustot suojatussa selaimessa.

Suojattu selain on erityinen selaimen tila, joka on suunniteltu suojaamaan tietojasi käyttäessäsi pankkien tai maksujärjestelmien verkkosivustoja. Suojattu selain käynnistetään eristetyssä ympäristössä, mikä estää muita sovelluksia lisäämästä omaa koodiaan Suojatun selaimen prosessiin.

Suojattu selain -tilassa sovellus suojaa seuraavilta uhkatyypeiltä:

- Ei-luotetut moduulit. Aina kun käytät pankin tai maksujärjestelmän verkkosivustoa, sovellus tarkistaa sen ei-luotettujen moduulien varalta.
- Rootkitit. Sovellus suorittaa rootkit-tarkistuksen Suojatun selaimen käynnistyksen yhteydessä.
- Tunnetut käyttöjärjestelmän heikkoudet. Sovellus suorittaa käyttöjärjestelmän heikkouksien tarkistuksen Suojatun selaimen käynnistyksen yhteydessä.
- Pankkien tai maksujärjestelmien verkkosivustojen virheelliset varmenteet. Kun käytät pankin tai maksujärjestelmän verkkosivustoa, sovellus tarkistaa sen varmenteet. Tarkistuksessa käytetään riskialttiiden varmenteiden tietokantaa.

Kun sivusto avataan suojatussa selaimessa, selainikkunan reunoilla näytetään kehykset. Kehyksien väri ilmaisee suojauksen tilan.

Selainikkunan kehykset voivat käyttää seuraavia merkitysvärejä:

- Vihreä kehys. Tarkoittaa, että kaikki tarkistukset on suoritettu onnistuneesti. Voit jatkaa Suojatun selaimen käyttämistä.
- Keltainen kehys. Tarkoittaa, että tarkistuksissa on havaittu tietoturvaongelmia, jotka täytyy ratkaista.

  Sovellus voi havaita seuraavat uhkat ja tietoturvaongelmat:

  - Ei-luotettu moduuli. Tietokoneen tarkistus ja tartunnan poisto vaaditaan.
  - Rootkit. Tietokoneen tarkistus ja tartunnan poisto vaaditaan.
  - Käyttöjärjestelmän heikkous. Käyttöjärjestelmään täytyy asentaa päivityksiä.
  - Pankin tai maksujärjestelmän verkkosivuston virheellinen varmenne.

  Jos havaittuja uhkia ei eliminoida, pankin tai maksujärjestelmän verkkosivustoon muodostettavan yhteyden turvallisuutta ei taata. Tapahtumat, jotka liittyvät Suojatun selaimen käynnistämiseen ja käyttämiseen alennetussa suojaustilassa kirjataan Windowsin tapahtumalokiin.

  Kehyksen keltainen väri voi myös ilmaista, että Suojattua selainta ei voida käynnistää teknisten rajoituksien vuoksi. Esimerkiksi käynnissä voi olla kolmannen osapuolen valmistama hypervisor-ohjelma, tai tietokoneesi ei tue laitteiston virtualisointia.

Jotta suojattu selain toimii oikein, varmista, että Rahasuojaus-liitännäiset ovat käytössä. Selain ottaa liitännäiset automaattisesti käyttöön, kun se käynnistetään ensimmäisen kerran uudelleen Kaspersky Total Securityn asennuksen jälkeen. Jos et ole sulkenut selainta ja käynnistänyt sitä uudelleen Kaspersky Total Securityn asennuksen jälkeen, liitännäiset eivät ole käytössä.

Liitännäisten automaattista käyttöönottoa koskevat seuraavat rajoitukset:

- Liitännäiset integroidaan ja otetaan käyttöön vain sovelluksen tukemissa selaimissa.

  Seuraavat selaimet tukevat Rahasuojaus-liitännäisiä:

  - Internet Explorer 8.0, 9.0, 10.0 ja 11.0.

    Modern UI -tyyliä käyttävää Internet Explorer 10- ja Windows 8 -tyyliä käyttävää Internet Explorer 11 -selainta ei tueta.

  - Mozilla Firefox 19.x, 20.x, 21.x, 22.x, 23.x, 24.x, 25.x, 26.x, 27.x, 28.x, 29.x, 30.x, 31.x, 32.x, 33.x, ja 34.x.
  - Google Chrome 33.x, 34.x, 35.x, 36.x, 37.x, ja 38.x.

    Kaspersky Total Security tukee Google Chromen versioita 37.x ja 38.x sekä 32-bittisissä että 64-bittisissä käyttöjärjestelmissä.

    Mozilla Firefoxin liitännäisiä ei oteta automaattisesti käyttöön, jos selaimeen ei ole luotu käyttäjäprofiilia. Luo käyttäjäprofiili sulkemalla selain ja käynnistämällä se uudelleen.

    Kun Google Chrome käynnistetään ensimmäisen suojatussa tilassa, verkkoselain pyytää asentamaan laajennuksen nimeltä Kaspersky Protection Plugin; se aktivoi Rahasuojaus-komponentin. Jos hylkäät Kaspersky Protection Plugin -asennuksen, voit asentaa sen myöhemmin napsauttamalla tätä linkkiä: http://support.kaspersky.com/interactive/google/en/kisplugin.

- Kun selain päivitetään, liitännäiset otetaan käyttöön automaattisesti vain, jos selaimen uusi versio tukee samaa liitännäisten käyttöönoton menetelmää kuin edellinen versio. Jos selaimen uusi versio tukee samaa liitännäisten käyttöönoton menetelmää kuin sen edellinen versio, liitännäiset otetaan käyttöön automaattisesti.

Jos liitännäisiä ei oteta käyttöön automaattisesti selaimen käynnistyessä uudelleen, ne täytyy ottaa käyttöön käsin. Voit tarkistaa, onko liitännäiset otettu käyttöön ja ottaa ne käyttöön käsin selaimen asetuksissa. Voit hakea lisää tietoja liitännäisten käyttöönotosta nykyisen selaimesi apujärjestelmästä.

Voit ottaa käyttöön tai poistaa käytöstä liitännäisten automaattisen aktivoinnin (ks. "Rahasuojaus-liitännäisten automaattisen aktivoinnin käyttöönotto" sivulla 52) sovelluksen asetusikkunassa.

Suojattua selainta ei voi käynnistää, jos **Ota itsepuolustus käyttöön** -valintaruutu ei ole valittuna sovelluksen asetusikkunan **Lisäasetukset**-osion kohdassa **Itsepuolustus**.

TÄSSÄ OSIOSSA

RAHASUOJAUKSEN ASETUSTEN MÄÄRITYS

Määritä Rahasuojauksen asetukset seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Asetukset**-linkkiä siirtyäksesi **Asetukset**-osioon.
3. Valitse ikkunan vasemmassa reunassa oleva **Suojaus**-osio.
4. Valitse **Rahasuojaus**-osio **Suojaus**-aliosion oikeasta reunasta.

   Näyttöön tulevat Rahasuojaus-komponentin asetukset.
5. Ota käyttöön Rahasuojaus ikkunan yläosassa olevalla valitsimella.
6. Jos haluat ottaa käyttöön ilmoitukset käyttöjärjestelmässä havaituista heikkouksista ennen suojatun selaimen käynnistämistä, valitse **Ota käyttöön ilmoitukset käyttöjärjestelmän heikkouksista** -valintaruutu.

RAHASUOJAUKSEN MÄÄRITTÄMINEN MÄÄRÄTYLLE VERKKOSIVUSTOLLE

Voit määrittää Rahasuojauksen määrätylle verkkosivustolle seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa **Rahasuojaus**-painiketta.

   Näyttöön avautuu **Rahasuojaus**-ikkuna.
3. Napsauta **Lisää verkkosivusto Rahasuojaukseen** -painiketta.

   Ikkunan oikeaan reunaan tulee kenttiä verkkosivustojen tietojen syöttämistä varten.
4. Kirjoita **Rahasuojauksen verkkosivusto** -kenttään sen verkkosivuston URL-osoite, jonka haluat avata suojatussa selaimessa.

   Verkkosivuston osoitteessa on oltava HTTPS-protokollan etuliite https://, jota suojattu selain käyttää oletusarvoisesti.
5. Kirjoita tarvittaessa kyseisen verkkosivuston nimi tai kuvaus **Kuvaus**-kenttään.
6. Valitse toiminto, jonka haluat suojatun selaimen suorittavan, kun avaat verkkosivuston:
   - Jos haluat, että verkkosivusto avautuu aina suojatussa selaimessa, valitse **Käynnistä suojattu selain**.
   - Jos haluat, että Kaspersky Total Security kysyy toimenpidettä verkkosivustoa avattaessa, valitse **Kysy toimenpidettä**.
   - Jos haluat poistaa Rahasuojauksen käytöstä verkkosivustolla, valitse **Älä käynnistä suojattua selainta**.
7. Napsauta **Lisää**-painiketta ikkunan oikeassa reunassa.

Verkkosivusto näytetään ikkunan vasemmassa reunassa olevassa luettelossa.

RAHASUOJAUS-LIITÄNNÄISTEN AUTOMAATTISEN AKTIVOINNIN KÄYTTÖÖNOTTO

Voit ottaa käyttöön Rahasuojaus-laajennusten käynnistyksen verkkoselaimissa seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Asetukset**-linkkiä siirtyäksesi **Asetukset**-osioon.
3. Valitse ikkunan vasemmassa reunassa oleva **Suojaus**-osio.
4. Valitse **Verkon virustorjunta**-osio **Suojaus**-osion oikeasta reunasta.
5. Napsauta avautuvassa **Verkon virustorjunnan asetukset** -ikkunassa **Lisäasetukset** -linkkiä, jolloin **Verkon virustorjunnan lisäasetukset** -ikkuna avautuu.
6. Valitse **Verkkoselainlaajennukset**-osiossa **Aktivoi sovelluslaajennukset kaikissa verkkoselaimissa automaattisesti** -valintaruutu.

TIETOJA NÄYTTÖKAAPPAUKSILTA SUOJAUTUMISESTA

Kaspersky Total Security suojaa tietojasi estämällä vakoiluohjelmia ottamasta luvattomia näyttökaappauksia, kun käytät suojattuja verkkosivustoja. Suojaus näyttökaappauksilta on oletusarvoisesti käytössä. Jos suojaus on poistettu käytöstä manuaalisesti, voit ottaa sen käyttöön sovelluksen asetusikkunassa (ks. "Näyttökaappauksilta suojautumisen ottaminen käyttöön" sivulla 53).

Kaspersky Total Security käyttää hypervisor-teknologiaa näyttökaappauksilta suojautumiseen. Microsoft Windows 8 x64 -käyttöjärjestelmää käyttävissä tietokoneissa Kaspersky Total Securityn hypervisorin antamaa suojausta näyttökaappauksilta koskevat seuraavat rajoitukset:

- Toiminto ei ole käytettävissä, jos suoritettavana on ulkopuolisen kehittäjän hypervisor, kuten esimerkiksi VMware® virtualization hypervisor. Kun suljet ulkopuolisen kehittäjän hypervisorin, suojaus näyttökaappauksilta palautuu käytettäväksi.
- Toiminto ei ole käytettävissä, jos tietokoneesi suoritin ei tue laitteiston virtualisointia. Katso lisätietoja siitä, tukeeko suorittimesi laitteiston virtualisointia tietokoneesi mukana toimitetusta dokumentaatiosta, tai käy suorittimen valmistajan verkkosivustolla.
- Toiminto ei ole käytettävissä, jos jokin ulkopuolisen kehittäjän hypervisor (kuten VMwaren hypervisor) on suoritettavana suojatun selaimen käynnistyessä.

NÄYTTÖKAAPPAUKSILTA SUOJAUTUMISEN OTTAMINEN KÄYTTÖÖN

Voit ottaa näyttökaappauksilta suojautumisen käyttöön seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä. Siirry **Asetukset**-osioon.
3. Valitse ikkunan vasemmassa reunassa oleva **Suojaus**-osio.
4. Valitse **Suojaus**-osiossa **Rahasuojaus**-aliosio ja varmista, että Rahasuojaus-valintakytkin on aktivoituna.

   Näyttöön avautuu **Rahasuojauksen asetukset** -ikkuna.
5. Valitse **Lisäasetukset**-osiossa **Estä näyttökaappausten ottaminen suojatussa selaimessa** -valintaruutu.

TIETOJA LEIKEPÖYDÄN TIETOJEN SUOJAUKSESTA

Kaspersky Total Security estää sovellusten luvattoman pääsyn leikepöydälle tehdessäsi verkko-ostoksia, mikä estää rikollisia varastamasta tietoja. Esto on käytettävissä vain, jos ei-luotettu sovellus yrittää saada luvattoman pääsyn leikepöydälle. Jos kopioit tiedon manuaalisesti sovellusikkunasta toiseen (esim. Muistiosta tekstinkäsittelyohjelmaan), pääsy leikepöydälle sallitaan. Jos kopioitavien tietojen lähteenä on tavallisessa tilassa avattu Internet Explorer® -selain, vain selaimen osoitekentästä peräisin olevien tietojen kopiointi leikepöydälle on mahdollista.

KASPERSKY PASSWORD MANAGERIN KÄYNNISTÄMINEN

Kaspersky Password Manager on suunniteltu tallentamaan ja synkronoimaan salasanat turvallisesti kaikkien laitteiden välillä. Kaspersky Password Manager asennetaan Kaspersky Total Securitystä erikseen. Kun Kaspersky Password Manager on asennettu, voit käynnistää sen **Käynnistä**-valikosta tai Kaspersky Total Securityn ikkunasta.

Voit käynnistää jo asennetun Kaspersky Password Managerin seuraavasti:

1. Avaa Kaspersky Total Securityn pääikkuna.
2. Napsauta **Salasanojen hallintatoiminto** -painiketta.

Kaspersky Password Manager -ikkuna avautuu.

Voit ladata Kaspersky Password Managerin, jota ei ole vielä asennettu, seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Salasanojen hallintatoiminto** -painiketta.

   Salasanojen hallintatoiminto -ikkuna avautuu.
3. Napsauta **Lataa**-painiketta.

   Siirryt Kaspersky Labin verkkosivustolle, jolta voit ladata Kaspersky Password Managerin asennuspaketin.

Voit lukea ohjeita Kaspersky Password Managerin käyttöön *Kaspersky Password Managerin käyttöoppaasta*.

VERKKOSIVUSTON TURVALLISUUDEN TARKISTUS

Kaspersky Total Security sallii verkkosivuston turvallisuuden tarkistamisen ennen kuin napsautat sen avaavaa linkkiä. Sivustot tarkistetaan käyttämällä *Kaspersky URL Advisoria*, joka on integroitu Verkon virustorjunta -komponenttiin.

Kaspersky URL Advisor ei ole saatavilla Microsoft Internet Explorer 10- ja 11 -selaimille, jotka käyttävät Windows 8 -tyyliä.

Kaspersky URL Advisor on integroitu Microsoft Internet Explorer-, Google Chrome- ja Mozilla Firefox -selaimiin, ja se tarkistaa selaimessa avatut verkkosivujen linkit. Kaspersky Total Security näyttää yhden seuraavista kuvakkeista jokaisen linkin vieressä:

- – jos linkitetty verkkosivu on Kaspersky Labin mukaan turvallinen
- – jos linkitetyn verkkosivun turvallisuustilanteesta ei ole tietoa
- – jos linkitetty verkkosivu on Kaspersky Labin mukaan vaarallinen

Voit tarkastella ponnahdusikkunaa, joka sisältää lisätietoja linkistä viemällä hiiren kohdistimen vastaavan kuvakkeen päälle.

Oletusarvoisesti Kaspersky Total Security tarkistaa linkit vain hakutuloksista. Voit ottaa käyttöön linkkien tarkistuksen jokaisella verkkosivustolla.

Ota käyttöön linkkien tarkistus verkkosivustoilla seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Avaa **Asetukset**-ikkuna napsauttamalla pääikkunan alaosassa olevaa **Asetukset**-linkkiä.
3. Valitse **Suojaus**-osiossa **Verkon virustorjunta** -aliosa.

   Näyttöön tulee Verkon virustorjunta -asetukset.
4. Napsauta ikkunan alaosassa olevaa **Lisäasetukset**-linkkiä. Verkon virustorjunnan lisäasetukset -ikkuna avautuu.
5. Valitse **Kaspersky URL Advisor** -osiossa **Tarkista URL-osoitteet** -valintaruutu.
6. Jos haluat, että Verkon virustorjunta tarkistaa kaikkien verkkosivustojen sisällön, valitse **Kaikilla paitsi määritetyillä verkkosivustoilla**.

   Määritä tarvittaessa verkkosivut, joihin luotat napsauttamalla **Määritä poissulkemiset** -linkkiä. Verkon virustorjunta ei tarkista määritettyjen verkkosivujen sisältöä eikä salattuja yhteyksiä määritettyihin verkkosivustoihin.

7. Jos haluat, että Verkon virustorjunta tarkistaa vain määritettyjen verkkosivujen sisällön, toimi seuraavasti:

    a. Valitse **Vain määritetyillä verkkosivustoilla**.

    b. Napsauta **Määritä tarkistettavat verkkosivustot** -linkkiä.

    c. Napsauta avautuvassa **Määritä tarkistettavat verkkosivustot** -ikkunassa **Lisää**-painiketta.

    d. Kirjoita avautuvassa **Lisää URL-osoite** -ikkunassa sen verkkosivun URL-osoite, jonka sisällön haluat tarkistaa.

    e. Valitse verkkosivun tarkistuksen tila (jos tila on *Aktiivinen*, Verkon virustorjunta tarkistaa verkkosivun sisällön).

    f. Napsauta **Lisää**-painiketta.

    Määritetty verkkosivu tulee näkyviin luetteloon **Tarkistettavat verkkosivustot** -ikkunassa. Verkon virustorjunta tarkistaa tämän verkkosivun URL-osoitteet.

8. Jos haluat muokata URL-tarkistuksen lisäasetuksia, napsauta **Verkon virustorjunnan lisäasetukset** -ikkunan **Kaspersky URL Advisor** -osiossa **Määritä Kaspersky URL Advisor** -linkkiä.

    Määritä Kaspersky URL Advisor -ikkuna avautuu.

9. Jos haluat, että Verkon virustorjunta ilmoittaa sinulle linkkien turvallisuuden kaikilla verkkosivuilla, valitse **Tarkista URL-osoitteet** -osiossa **Kaikki URL-osoitteet**.

10. Jos haluat, että Verkon virustorjunta näyttää tietoja siitä, kuuluuko linkki määrättyyn verkkosivustojen sisältöluokkaan (esimerkiksi *Rienaava, alatyylinen*), toimi seuraavasti:

    a. Valitse **Näytä verkkosivustojen sisältöluokkia koskevia tietoja** -valintaruutu.

    b. Valitse valintaruudut niiden verkkosivustojen sisältöluokkien vierestä, joiden tietoja haluat näkyvän kommenteissa.

Verkon virustorjunta tarkistaa linkit määritetyiltä verkkosivuilta ja näyttää tietoja linkkien luokista nykyisten asetusten mukaisesti.

BANNERIEN ESTO SELATTAESSA VERKKOSIVUSTOJA

Bannerien esto -komponentti on suunniteltu suojaamaan käyttäjää verkkosivustoilla olevilta bannereilta. Jos komponentti on käytössä, voit estää bannerien näyttämisen suoraan verkkosivustossa. Voit myös määrittää Kaspersky Total Securityn asetuksissa verkkosivuston osoitteen ja osoitepeitteen, joiden perusteella kyseisen verkkosivuston bannerit estetään. Oletusarvoisesti Kaspersky Total Security suojaa käyttäjää yleisimmiltä bannerityypeiltä.

TÄSSÄ OSIOSSA

BANNERIEN ESTO -KOMPONENTIN KÄYTTÖÖNOTTO

Voit ottaa Bannerien esto -komponentin käyttöön seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Asetukset**-linkkiä, jolloin **Asetukset**-ikkuna avautuu.
3. Valitse **Suojaus**-osio.
4. Ota **Bannerien esto** -komponentti käyttöön.

VERKKOSIVUSTOJEN BANNERIEN ESTÄMINEN

Voit estää verkkosivustojen näyttämät bannerit seuraavasti:

1. Osoita hiirellä verkkosivustolla olevaa banneria, jonka haluat piilottaa.
2. Paina näppäimistön **CTRL**-näppäintä.
3. Valitse avautuvassa valikossa **Lisää Bannerien estoon**.

   Estetyt URL-osoitteet -ikkuna avautuu.
4. Napsauta **Estetyt URL-osoitteet** -ikkunassa **Lisää**-painiketta.

   Bannerin URL-osoite lisätään estettävien URL-osoitteiden luetteloon.
5. Päivitä verkkosivu selaimessa, ja bannerin näyttäminen estetään.

Banneria ei näytetä, kun käytät verkkosivua myöhemmin.

VERKKOSIVUSTOJEN KAIKKIEN BANNERIEN ESTÄMINEN

Voit estää kaikki tietyn verkkosivuston näyttämät bannerit. Voit tehdä sen lisäämällä verkkosivuston osoitepeitteen estettävien verkko-osoitteiden luetteloon.

Voit estää kaikki verkkosivuston bannerit seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Asetukset**-linkkiä, jolloin **Asetukset**-ikkuna avautuu.
3. Valitse **Suojaus**-osio.
4. Valitse **Bannerien esto** -komponentti.

   Näyttöön avautuu **Bannerien eston asetukset** -ikkuna.
5. Napsauta **Bannerien eston asetukset** -ikkunassa **Määritä estetyt URL-osoitteet** -linkkiä, jolloin **Estetyt URL-osoitteet** -ikkuna avautuu.
6. Napsauta **Estetyt URL-osoitteet** -ikkunassa **Lisää**-painiketta.
7. Lisää avautuvan ikkunan **Verkko-osoitteen peite (URL)** -kenttään sen verkkosivuston osoitepeite, jonka näyttämät bannerit haluat estää. Esimerkiksi: http://esimerkki.com*.
8. Valitse verkkosivuston tilaksi **Aktiivinen**.
9. Napsauta **Lisää**-painiketta.

Kaspersky Total Security estää nyt sivuston http://esimerkki.com bannerit.

TIETOKONEELLA JA VERKOSSA OLEVIEN TOIMINNAN JÄLKIEN POISTAMINEN

Käyttäjän tietokoneella suorittamat toimenpiteet tallennetaan käyttöjärjestelmään. Seuraavat tiedot tallennetaan:

- Tiedot käyttäjien määrittämistä hakusanoista ja vierailluista verkkosivustoista
- Tiedot käynnistetyistä sovelluksista sekä avatuista ja tallennetuista tiedostoista
- Microsoft Windows -tapahtumalokin tapahtumat
- Muita tietoja käyttäjän toiminnasta

Tunkeutujat ja luvattomat henkilöt voivat saada pääsyn henkilökohtaisiin tietoihin, joita on säilötty tietoihin käyttäjän aiemmista toimenpiteistä.

Kaspersky Total Security sisältää yksityisten tietojen ohjatun poistamistoiminnon, joka puhdistaa käyttäjän toimintaan liittyvät jäljet käyttöjärjestelmästä.

Voit käynnistää yksityisten tietojen ohjatun poistamistoiminnon seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Käynnistä yksityisten tietojen ohjattu poistamistoiminto napsauttamalla **Työkalut**-ikkunan vasemmassa reunassa olevaa **Yksityisten tietojen poistaja** -linkkiä.

Ohjattu toiminto koostuu ikkunoista (vaiheista), joissa liikutaan painikkeilla **Takaisin** ja **Seuraava**. Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta. Voit keskeyttää ohjatun toiminnon milloin tahansa napsauttamalla **Peruuta**-painiketta.

Alla on tarkempia tietoja ohjatusta toiminnosta.

Vaihe 1. Ohjatun toiminnon käynnistäminen

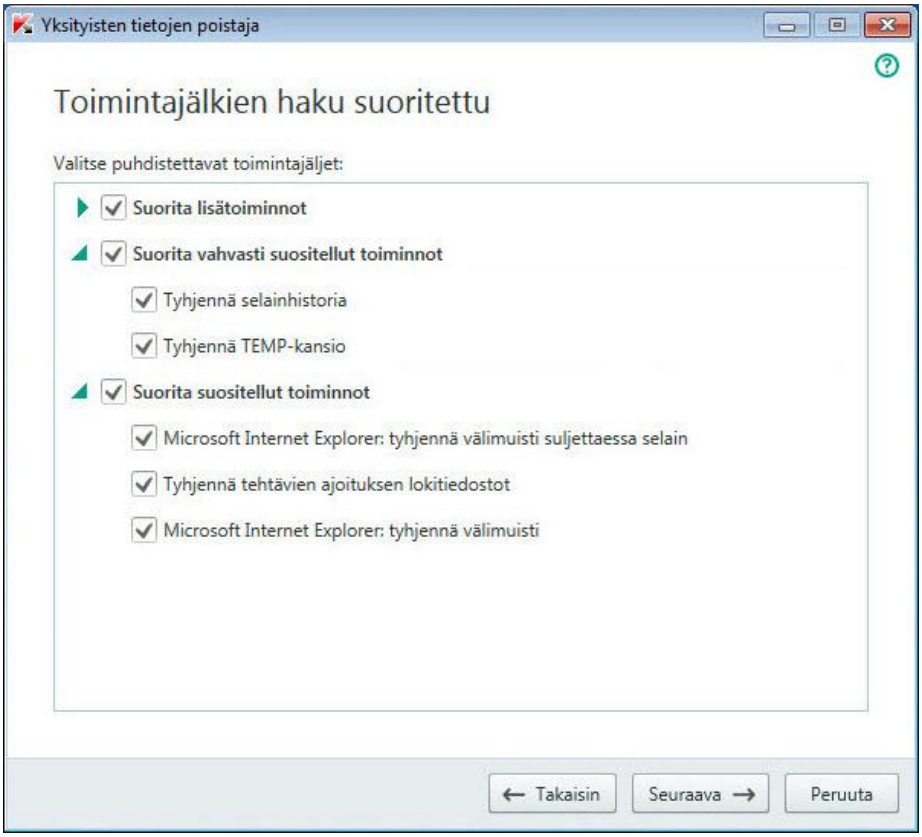
Varmista, että **Etsi jälkiä käyttäjän toimista** -valintaruutu on valittuna. Käynnistä ohjattu toiminto napsauttamalla **Seuraava**-painiketta.

Vaihe 2. Toiminnan jälkien etsintä

Tämä ohjattu toiminto etsii tietokoneesta toiminnan jälkiä. Haku voi kestää jonkin aikaa. Kun haku on valmis, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Vaihe 3. Yksityisten tietojen poiston toimintojen valitseminen

Kun haku on valmis, ohjattu toiminto ilmoittaa sinulle havaituista toiminnan jäljistä ja kysyy, mitä toimintoja suoritetaan niiden poistamiseksi (katso seuraava kuva).



Kuva 4. Havaitut toimintajäljet ja niiden poistamista koskevat suositukset

Voit tarkastella tietyn ryhmän sisältämiä toimintoja napsauttamalla (plusmerkki) -kuvaketta ryhmän nimen vasemmalla puolella.

Jos haluat ohjatun toiminnon suorittavan jonkin toimenpiteen, valitse toimenpiteen vasemmalla puolella oleva valintaruutu. Oletusasetuksena on, että ohjattu toiminto suorittaa kaikki suositellut ja vahvasti suositellut toiminnot. Jos et halua suorittaa jotakin tiettyä toimintoa, poista valinta sen vieressä olevasta valintaruudusta.

Suosittelemme, että et poista valintaa oletuksena valituista ruuduista, sillä tämä voi tehdä tietokoneesta haavoittuvan uhille.

Kun olet määrittänyt toimenpiteet ohjatun toiminnon suoritusta varten, napsauta **Seuraava**-painiketta.

Vaihe 4. Yksityisten tietojen poistaja

Ohjattu toiminto suorittaa edellisen vaiheen aikana valitut toiminnot. Toiminnan jättämien jälkien poistaminen saattaa kestää jonkin aikaa. Tietokoneen uudelleenkäynnistys saattaa olla tarpeen tiettyjen toiminnan jälkien poistamiseksi. Ohjattu toiminto ilmoittaa tästä tarvittaessa.

Kun puhdistaminen on suoritettu, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Vaihe 5. Ohjatun toiminnon viimeistely

Sulje ohjattu toiminto napsauttamalla **Lopeta**-painiketta.

KÄYTTÄJIEN TOIMINNAN HALLINTA TIETOKONEELLA JA INTERNETISSÄ

Tämä osio sisältää tietoja siitä, miten hallita käyttäjien toimintoja tietokoneella ja Internetissä Kaspersky Total Securityn avulla.

TÄSSÄ OSIOSSA

KÄYTÖNVALVONNAN KÄYTTÖ

Käytönvalvonta mahdollistaa käyttäjien toiminnan valvonnan paikallisella tietokoneella ja verkossa. Käytönvalvonnan avulla voit rajoittaa Internet-resurssien ja sovellusten käyttöä sekä tarkastella raportteja käyttäjien toimista.

Nykyisin yhä useammat lapset ja teini-ikäiset saavat käyttöönsä tietokoneita ja verkkoresursseja. Tietokoneet ja Internet altistavat lapset useille eri vaaroille:

- Ajan ja/tai rahan menettäminen keskusteluryhmissä, peliresursseissa, verkkokaupoissa ja huutokaupoissa
- Pääsy vain aikuisille tarkoitetuille verkkosivuille, jotka voivat sisältää mm. pornoa, ääriliikkeitä, tuliaseita, huumeiden käyttöä ja raakaa väkivaltaa
- Haittaohjelmia sisältävien tiedostojen lataaminen
- Tietokoneen liiallisen käytön aiheuttamat terveyshaitat
- Yhteydet tuntemattomien ihmisten kanssa, jotka voivat esiintyä ystävinä saadakseen alaikäiseltä käyttäjältä henkilökohtaisia tietoja kuten todellinen nimi ja osoite sekä aika, jolloin ketään ei ole kotona

Käytönvalvonnalla voit vähentää tietokoneen ja Internetin aiheuttamia riskejä. Tämä saavutetaan seuraavilla toiminnoilla:

- Tietokoneen ja Internetin käyttöajan rajoittaminen.
- Sallittujen ja estettyjen pelien ja sovellusten luettelojen luominen sekä sallittujen sovellusten käytön väliaikainen rajoittaminen.
- Sallittujen ja estettyjen verkkosivujen luetteloiden luominen sekä sopimatonta sisältöä sisältävien verkkosivuluokkien valikoiva estäminen.

- Hakukoneiden turvallisen haun ottaminen käyttöön (linkkejä verkkosivuille, joissa on epäilyttävää sisältöä, ei näytetä hakutuloksissa).
- Tiedostojen Internetistä lataamisen rajoittaminen.
- Pikaviestintäohjelmien ja yhteisöverkostojen sallittujen ja estettyjen yhteyshenkilöiden luetteloiden luominen.
- Pikaviestintäohjelmien ja yhteisöverkostojen viestilokien tarkastelu.
- Määrättyjen henkilökohtaisten tietojen lähettämisen esto.
- Määritettyjen avainsanojen etsintä viestilokeista.

Voit määrittää Käytönvalvonnan asetukset tietokoneen kullekin käyttäjätilille erikseen. Voit myös tarkastella Käytönvalvonnan raportteja valvottavien käyttäjien toiminnasta.

KÄYTÖNVALVONNAN ASETUKSIIN SIIRTYMINEN

Voit siirtyä Käytönvalvonnan asetuksiin seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta sovelluksen pääikkunassa **Käytönvalvonta**-painiketta.
3. Kun avaat **Käytönvalvonta**-ikkunan ensimmäistä kertaa, sovellus kehottaa sinua asettamaan Käytönvalvonnan asetuksia suojaavan salasanan. Valitse yksi seuraavista vaihtoehdoista:
   - Jos haluat suojata Käytönvalvonnan asetukset salasanalla, täytä **Salasana**- ja **Vahvista**- kentät ja napsauta sitten **Jatka**-painiketta.
   - Jos et halua suojata Käytönvalvonnan asetuksia salasanalla, etene Käytönvalvonnan asetuksiin napsauttamalla **Ohita**-linkkiä.

   Käytönvalvonta-ikkuna avautuu.
4. Valitse käyttäjätili ja napsauta **Määritä rajoitukset** -linkkiä, jolloin Käytönvalvonnan asetusikkuna avautuu.

TIETOKONEEN KÄYTÖN HALLINTA

Käytönvalvonnan avulla voit rajoittaa käyttäjän tietokoneen käyttöaikaa. Voit määrittää aikavälin, jonka aikana Käytönvalvonta estää tietokoneen käytön (uniaika) sekä kokonaiskäyttöaikarajoituksen tietokoneen päivittäiselle käytölle. Voit määrittää eri aikarajoitukset arkipäiville ja viikonlopuille.

Voit määrittää aikarajoja tietokoneen käytölle seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Tietokone**-osio.
3. Voit määrittää aikavälin, jolloin Käytönvalvonta estää tietokoneen käytön siirtymällä **Arkipäivisin**- tai **Viikonloppuisin**-osioon ja valitsemalla **Estä käyttö klo** -valintaruudun.
4. Määritä eston aloitusaika **Estä käyttö klo** -valintaruudun vieressä olevasta pudotusluetteloon.
5. Määritä eston päättymisaika **Päättymisaika**-pudotusluetteloon.

   Voit myös asettaa tietokoneen käyttöaikataulun taulukon avulla. Voit tarkastella taulukkoa napsauttamalla painiketta  .

   Käytönvalvonta estää käyttäjän pääsyn tietokoneelle määritetyllä aikavälillä.

6. Jos haluat asettaa aikarajan tietokoneen käytön kokonaismäärälle päivän aikana, valitse **Arkipäivisin**- ja **Viikonloppuisin**-osioissa **Salli käyttö enintään** -valintaruutu ja valitse sitten aikavälin pituus valintaruudun vieressä olevasta pudotusluettelosta.

   Käytönvalvonta estää käyttäjän pääsyn tietokoneelle, kun tietokoneen kokonaiskäyttöaika ylittää määritetyn päivittäisen rajan.

7. Voit asettaa taukoja käyttäjän tietokoneen käyttöön valitsemalla **Tauot**-osiossa olevan **Pidä tauko joka** -valintaruudun ja valitsemalla sitten valintaruudun vieressä olevista pudotusluetteloista haluamasi taukojen tiheyden (esimerkiksi kerran tunnissa) ja niiden pituuden (esimerkiksi 10 minuuttia).

8. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta estää käyttäjän pääsyn tietokoneelle nykyisten asetusten mukaan.

INTERNETIN KÄYTÖN HALLINTA

Käytönvalvonnan avulla voit rajoittaa Internetin käyttöaikaa ja estää käyttäjiltä määrättyyn luokkaan kuuluvien verkkosivustojen tai määritettyjen verkkosivustojen käytön. Lisäksi voit estää käyttäjää lataamasta määrätyn tyyppisiä tiedostoja (kuten arkistot tai videot) Internetistä.

- *Voit määrittää aikarajoja Internetin käytölle seuraavasti:*

  1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).

  2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Internet**-osio.

  3. Jos haluat rajoittaa Internetin kokonaiskäyttöaikaa arkipäivisin, valitse **Internetin käytön aikarajoitus** -osiossa oleva **Rajoita käyttöä arkipäivisin <HH:MM> tuntiin päivässä** -valintaruutu. Valitse sitten aikarajan pituus valintaruudun vieressä olevasta pudotusluettelosta.

  4. Jos haluat rajoittaa Internetin kokonaiskäyttöaikaa viikonloppuisin, valitse **Rajoita käyttöä viikonloppuisin <HH:MM> tuntiin päivässä** -valintaruutu. Valitse sitten aikarajan pituus valintaruudun vieressä olevasta pudotusluettelosta.

  5. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

  Käytönvalvonta rajoittaa käyttäjän Internetin kokonaiskäyttöaikaa määrittämiesi arvojen mukaisesti.

- *Voit rajoittaa määrättyjen verkkosivustojen käyttöä seuraavasti:*

  1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
  2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Internet**-osio.
  3. Voit estää aikuissisällön näkymisen hakutuloksissa valitsemalla **Hallinnoi verkkoselausta** -osiossa **Ota turvallinen haku käyttöön** -valintaruudun.

     Kun etsit tietoa verkkosivustoilla kuten Google, YouTube (vain käyttäjät, jotka eivät ole kirjautuneet tilillään youtube.com-verkkosivustolle) Bing®, Yahoo!, Mail.ru, VKontakte ja Yandex, hakutuloksissa ei näytetä aikuissisältöä.

  4. Voit estää pääsyn määrätyn luokan verkkosivustoille seuraavasti:

     a. Valitse **Hallinnoi verkkoselausta** -osiossa **Estä pääsy seuraaville verkkosivustoille** -valintaruutu.

     b. Valitse **Aikuisviihdesivustot** ja napsauta **Valitse verkkosivustojen luokat** -linkkiä, jolloin**Verkkosivustojen käytön eston luokat** -ikkuna avautuu.

     c. Valitse valintaruudut estettävien verkkosivustoluokkien vierestä.

        Käytönvalvonta estää kaikki käyttäjän yritykset avata verkkosivusto, jos sen sisältö luokitellaan jonkin estetyn luokan mukaiseksi.

5. Voit estää pääsyn määrätyille verkkosivustoille seuraavasti:

   a. Valitse **Hallinnoi verkkoselausta** -osiossa **Estä pääsy seuraaville verkkosivustoille** -valintaruutu.

   b. Valitse **Kaikki verkkosivustot paitsi luettelossa sallitut poikkeukset** ja napsauta **Lisää poissulkemisia** -linkkiä avataksesi **Poissulkemiset**-ikkunan.

   c. Napsauta **Lisää**-painiketta ikkunan alaosassa.

      Näyttöön tulee **Lisää uusi verkkosivusto** -ikkuna.

   d. Syötä estettävän verkkosivuston osoite **URL-peite**-kenttään.

   e. Määritä **Laajuus**-osiossa haluamasi eston laajuus: koko verkkosivusto tai pelkästään määritetty verkkosivu.

   f. Jos haluat estää määritetyn verkkosivuston, valitse **Toiminto**-osiossa **Estä**.

   g. Napsauta **Lisää**-painiketta.

   Määritetty verkkosivusto tulee näkyviin luetteloon **Poissulkemiset**-ikkunassa.

6. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta estää kaikki käyttäjän yritykset avata mikä tahansa luettelossa oleva verkkosivusto käytössä olevien asetusten mukaisesti.

Voit estää tietyntyyppisten tiedostojen lataamisen Internetistä seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Internet**-osio.
3. Valitse **Estä tiedostojen lataus** -osiossa valintaruudut niiden tiedostotyyppien vierestä, joiden lataus halutaan estää.
4. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta estää määrätyn tyyppisten tiedostojen lataamisen Internetistä.

PELIEN JA SOVELLUSTEN KÄYNNISTÄMISEN HALLINTA

Käytönvalvonnan avulla voit sallia tai estää käyttäjältä pelien käynnistämisen ikärajoitusten mukaan. Voit myös estää käyttäjää käynnistämästä määrättyjä sovelluksia (kuten pelejä tai pikaviestintäohjelmia) tai rajoittaa niiden käyttöä aikarajoilla.

Voit estää sopimatonta sisältöä sisältävien pelien käytön seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Sovellukset**-osio.
3. **Estä pelejä sisällön mukaan** -osiossa voit estää sellaisten pelien käynnistämisen, jotka eivät sovellu käyttäjälle hänen ikänsä vuoksi ja/tai pelien sisällön vuoksi:

   a. Jos haluat estää kaikkien käyttäjän iän takia sopimattomien pelien käynnistämisen, valitse **Estä pelejä ikäluokituksen mukaan** -valintaruutu. Valitse sitten ikärajoitusvaihtoehto valintaruudun vieressä olevasta pudotusluettelosta.

   b. Jos haluat estää pelit, joiden sisältö kuuluu määrättyyn luokkaan:

      a. Valitse **Estä aikuisten luokkiin kuuluvat pelit** -valintaruutu.

      b. Napsauta **Valitse peliluokat** -linkkiä ja avaa **Estä pelit luokkien mukaan** -ikkuna.

      c. Valitse sisältöluokkien vieressä olevat valintaruudut, jotka vastaavat estettäviä pelejä.

4. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Voit rajoittaa määrätyn sovelluksen käynnistyksen seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Sovellukset**-osio.
3. Napsauta ikkunan alaosassa **Lisää sovellus luetteloon** -linkkiä, ja valitse sitten avautuvassa **Avaa**-ikkunassa halutun sovelluksen käynnistystiedosto.

   Valittu sovellus tulee näkyviin **Estä määritetyt sovellukset** -osion luetteloon. Kaspersky Total Security lisää sovelluksen automaattisesti määritettyyn luokkaan, esimerkiksi *Pelit*.
4. Jos haluat estää sovelluksen, valitse luettelossa olevan nimen vieressä oleva valintaruutu. Voit myös estää kaikki sovellukset, jotka kuuluvat määrättyyn luokkaan valitsemalla luettelossa luokan nimen vieressä olevan valintaruudun (voit esimerkiksi estää *Pelit*-luokan).
5. Jos halut rajoittaa sovelluksen käyttöaikaa, valitse sovellus tai sovellusluokka luettelosta ja napsauta **Määritä säännöt** -linkkiä ja avaa **Sovelluksen käyttörajoitus** -ikkuna.
6. Jos haluat asettaa sovelluksen käytöllä aikarajan arkipäivinä ja viikonloppuina, valitse **Arkipäivisin**- ja **Viikonloppuisin**-osioissa **Salli käyttö enintään** -valintaruutu ja määritä pudotusluettelosta, montako tuntia päivässä käyttäjä voi käyttää sovellusta. Voit myös määrittää ajan, jolloin käyttäjä saa / ei saa käyttää sovellusta taulukon avulla. Voit tarkastella taulukkoa napsauttamalla painiketta  .
7. Jos haluat määrittää taukoja sovelluksen käyttöön, valitse **Tauot**-osiossa **Pidä tauko joka** -valintaruutu ja valitse tauon taajuus ja pituus pudotusluettelosta.
8. Napsauta **Tallenna**-painiketta.
9. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta soveltaa määritettyjä rajoituksia, kun käyttäjä käyttää sovellusta.

YHTEISÖVERKOSTOJEN VIESTINNÄN HALLINTA

Käytönvalvonnan avulla voit tarkkailla käyttäjän viestintää yhteisöverkostoissa ja pikaviestintäohjelmissa sekä estää viestinnän määrättyjen yhteyshenkilöiden kanssa.

Voit määrittää käyttäjän viestinnän valvonnan seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Viestintä**-osio.
3. Voit tarkastella viestilokeja ja tarvittaessa estää määrätyt yhteyshenkilöt seuraavasti:
   a. Valitse **Estä viestintä kaikkien yhteystietojen kanssa, pois lukien sallitut yhteystiedot**.
   b. Napsauta **Tunnetut yhteyshenkilöt** -linkkiä, jolloin **Viestintäraportti**-ikkuna avautuu.
   c. Tarkastele yhteyshenkilöitä, joiden kanssa käyttäjä on viestinyt. Voit tuoda määrättyjä yhteyshenkilöitä ikkunaan yhdellä seuraavista tavoista:
      - Voit tarkastella käyttäjän viestintää määrätyssä yhteisöverkostossa tai määrätyllä pikaviestimellä valitsemalla haluamasi kohdan ikkunan vasemmassa reunassa olevasta pudotusluettelosta.
      - Voit tarkastella yhteyshenkilöitä, joille käyttäjä on kirjoittanut eniten valitsemalla **Viestien lukumäärän mukaan** -kohdan ikkunan oikeassa reunassa olevasta pudotusluettelosta.
      - Voit tarkastella yhteyshenkilöitä, joille käyttäjä on kirjoittanut tiettynä päivänä valitsemalla **Viestintäpäivän mukaan** -kohdan ikkunan oikeassa reunassa olevasta pudotusluettelosta.
   d. Jos haluat tarkastella käyttäjän viestintää määrätyn yhteyshenkilön kanssa, napsauta haluamaasi kohdetta luettelossa.

      Viestiloki-ikkuna avautuu.
   e. Jos haluat estää käyttäjän viestinnän valitun yhteyshenkilön kanssa, napsauta **Estä viestintä** -painiketta.
4. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta estää viestinnän käyttäjän ja valitun yhteyshenkilön välillä.

VIESTIEN SISÄLLÖN VALVONTA

Käytönvalvonnan avulla voit valvoa ja estää käyttäjän yritykset lisätä viesteihin määrättyjä yksityisiä tietoja (kuten nimet, puhelinnumerot, pankkikorttien numerot) ja avainsanoja (kuten alatyyliset sanat).

Voit määrittää yksityisten tietojen lähettämisen hallinta-asetukset seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Sisällönvalvonta**-osio.
3. Valitse **Yksityisten tietojen siirron hallinta** -osiossa **Estä yksityisten tietojen siirto kolmansille osapuolille** -valintaruutu.
4. Napsauta **Muokkaa yksityisten tietojen luetteloa** -linkkiä, jolloin **Yksityisten tietojen luettelo** -ikkuna avautuu.
5. Napsauta **Lisää**-painiketta ikkunan alaosassa.

   Näyttöön avautuu ikkuna yksityisten tietojen lisäämistä varten.
6. Voit lisätä kuvauksen yksityiseen tietoon (esimerkiksi "puhelinnumero") napsauttamalla asianomaista linkkiä kirjoittamalla kuvauksen **Kentän nimi** -kenttään.
7. Kirjoita yksityiset tiedot (kuten sukunimesi tai puhelinnumerosi) **Arvo**-kenttään.
8. Napsauta **Lisää**-painiketta.

   Yksityiset tiedot tulevat näkyviin **Yksityisten tietojen luettelo** -ikkunassa.
9. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta valvoo ja estää käyttäjän yritykset käyttää määritettyä yksityistä tietoa pikaviestintäohjelmien ja verkkosivustojen kautta tapahtuvassa viestinnässä.

Voit määrittää viestien avainsanojen hallinnan seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse Käytönvalvonnan asetukset -ikkunassa oleva **Sisällönvalvonta**-osio.
3. Valitse **Avainsanojen hallinta** -osiossa **Ota käyttöön avainsanojen hallinta** -valintaruutu.
4. Napsauta **Muokkaa avainsanojen luetteloa** -linkkiä, jolloin **Avainsanojen hallinta** -ikkuna avautuu.
5. Napsauta **Lisää**-painiketta ikkunan alaosassa.

   Näyttöön avautuu ikkuna avainsanan lisäämistä varten.
6. Kirjoita avainlause **Arvo**-kenttään ja napsauta **Lisää**-painiketta.

   Määritetty avainlause tulee näkyviin avainsanaluettelossa **Avainsanojen hallinta** -ikkunassa.
7. Ota **Käytönvalvonta**-ikkunassa käyttöön **Käytönvalvonta**-kytkin, joka sijaitsee käyttäjätilin vieressä.

Käytönvalvonta estää sellaisten viestien lähetyksen, jotka sisältävät määritetyn avainlauseen riippumatta siitä, tapahtuuko viestin lähetys Internetissä vai pikaviestintäohjelmissa.

KÄYTTÄJÄN TOIMIIN LIITTYVÄN RAPORTIN TARKASTELEMINEN

Voit tarkastella jokaisen Käytönvalvonnan alaisen käyttäjätilin toimintaraportteja, joissa voit tarkastella valvottujen tapahtumien jokaista luokkaa yksitellen.

Voit tarkastella raporttia valvotun käyttäjätilin toiminnasta seuraavasti:

1. Siirry Käytönvalvonnan asetusikkunaan (ks. "Siirtyminen Käytönvalvonnan asetuksiin" sivulla 61).
2. Valitse käyttäjätili ja siirry raportti-ikkunaan napsauttamalla **Näytä raportti** -linkkiä.
3. Kun olet halutun rajoitustyypin osiossa (esimerkiksi **Internet** tai **Viestintä**), avaa valvottujen toimintojen raportti napsauttamalla **Lisätiedot**-linkkiä.

Ikkunaan tulee raportti käyttäjän valvotuista toiminnoista.

TIETOKONEEN SUOJAUKSEN ETÄHALLINTA

Tässä osiossa on tietoja siitä, miten voit hallita etäyhteyden kautta sellaisten tietokoneiden suojausta, joihin on asennettu Kaspersky Total Security.

TÄSSÄ OSIOSSA

TIETOJA TIETOKONEEN SUOJAUKSEN ETÄHALLINNASTA

Jos tietokoneeseen on asennettu Kaspersky Total Security, voit hallita kyseisen tietokoneen suojausta etäyhteyden kautta. Tietokoneen suojausta voi hallita etäyhteyden kautta My Kaspersky -portaalin avulla. Jos haluat hallita tietokoneen suojausta etäyhteyden kautta, rekisteröidy My Kaspersky -portaaliin, kirjaudu sisään My Kaspersky -tilillesi ja siirry **Laitteet**-osioon.

My Kaspersky -portaalissa voit suorittaa seuraavat tietokoneen suojaukseen liittyvät tehtävät:

- Tarkastella tietokoneen tietoturvaongelmien luetteloa ja korjata ongelmia etäyhteyden kautta
- Tarkistaa tietokoneen virusten ja muiden uhkien varalta
- Päivittää tietokantoja ja sovellusmoduuleja
- Määrittää Kaspersky Total Securityn komponentteja

Jos tietokoneen tarkistus käynnistetään My Kaspersky -portaalin kautta, Kaspersky Total Security käsittelee havaitsemansa objektit automaattisesti ilman käyttäjän toimenpiteitä. Jos Kaspersky Total Security havaitsee viruksen tai muun uhkan, se yrittää poistaa tartunnan käynnistämättä tietokonetta uudelleen. Jos tartuntaa ei voida poistaa ilman tietokoneen uudelleenkäynnistystä, asiaa koskeva ilmoitus näytetään My Kaspersky -portaalin tietoturvaongelmaluettelossa.

SIIRTYMINEN TIETOKONEEN SUOJAUKSEN ETÄHALLINTAAN

Voit siirtyä tietokoneen suojauksen etähallintaan seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Verkkohallinta**-painiketta.
3. Napsauta **Verkkohallinta**-ikkunassa **Yhdistä tietokone My Kasperskyyn** -painiketta.

   Jos et ole vielä kirjautunut sisään My Kaspersky -portaaliin, kirjautumiskaavake avautuu **Verkkohallinta**-ikkunaan. Täytä kentät ja kirjaudu My Kaspersky -portaaliin.

My Kaspersky -portaalin osio **Laitteet** avautuu selainikkunassa oletusarvoisesti.

KÄYTTÖJÄRJESTELMÄN RESURSSIEN VARAAMINEN TIETOKONEPELIEN KÄYTTÖÖN

Jos Kaspersky Total Security on käynnissä koko näytön tilassa samanaikaisesti tiettyjen sovellusten kanssa (erityisesti tietokonepelit), seuraavia haittavaikutuksia voi ilmetä:

- Sovelluksen tai pelin suorituskyky laskee puutteellisten käyttöjärjestelmäresurssien takia.
- Kaspersky Total Security ilmoitusikkunat häiritsevät käyttäjän pelaamista.

Jos et haluat muuttaa Kaspersky Total Securityn asetuksia manuaalisesti aina, kun siirryt käyttämään täyden näytön tilaa, voit käyttää Peliprofiilia. Kun Peliprofiili otetaan käyttöön, täyden näytön tilaan siirtyminen muuttaa Kaspersky Total Securityn komponenttien asetuksia automaattisesti. Näin varmistetaan järjestelmän optimaalinen toiminta. Kun poistut täyden näytön tilasta, sovelluksen asetukset palautuvat täyden näytön tilan käyttöönottoa edeltäneisiin lähtöarvoihinsa.

Voit ottaa Peliprofiilin käyttöön seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Asetukset**-linkkiä siirtyäksesi **Asetukset**-osioon.
3. Valitse ikkunan vasemmalta puolelta **Suorituskyky**-osio.

   Ikkunassa näytetään Kaspersky Total Securityn suorituskykyasetukset.
4. Valitse **Peliprofiili**-osiossa **Käytä Peliprofiilia** -valintaruutu.

TUNTEMATTOMIEN SOVELLUSTEN KÄSITTELY

Kaspersky Total Security auttaa pienentämään tuntemattomien sovellusten käytössä ilmeneviä riskejä (kuten virusten ja muiden haittaohjelmien tartuntavaara ja ei-halutut muutokset käyttöjärjestelmän asetuksissa).

Kaspersky Total Security sisältää komponentteja ja työkaluja, joiden avulla voidaan tarkistaa sovelluksen maine ja hallita sovelluksen suorittamia toimenpiteitä tietokoneessasi.

TÄSSÄ OSIOSSA

SOVELLUKSEN MAINEEN TARKISTAMINEN

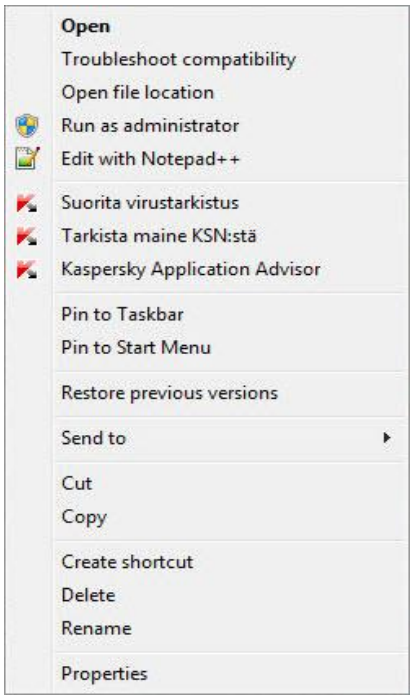
Kaspersky Total Securityn avulla voit tarkistaa sovellusten maineen käyttäjiltä eri puolilla maailmaa. Sovelluksen maine koostuu seuraavista ehdoista:

- Toimittajan nimi
- Tiedot digitaalisesta allekirjoituksesta (jos sovelluksella on digitaalinen allekirjoitus)
- Tiedot ryhmästä, johon Sovellusten hallinta tai suurin osa Kaspersky Security Network -käyttäjistä on sovelluksen asettanut
- Sovellusta käyttävien Kaspersky Security Network -käyttäjien määrä (käytettävissä, jos sovellus on sisällytetty Kaspersky Security Network -tietokannan Luotettu-ryhmään)
- Aika, jolloin sovellus on tullut tunnetuksi Kaspersky Security Network -verkostossa
- Maat, joissa sovellus on levinnyt laajimmalle

Sovelluksen maineen tarkistus on saatavana, jos olet osallistunut Kaspersky Security Network -verkostoon.

Voit tarkistaa sovelluksen maineen seuraavasti:

Avaa sovelluksen käynnistystiedoston pikavalikko ja valitse **Tarkista maine KSN:stä** (katso seuraava kuva).



Kuva 5. Objektin pikavalikko

Näyttöön avautuu ikkuna, joka sisältää tietoja sovelluksen maineesta KSN:ssä.

KATSO MYÖS:

Osallistuminen Kaspersky Security Network (KSN) -verkostoon..... 96

SOVELLUSTEN TOIMINNAN HALLINTA TIETOKONEELLA JA VERKOSSA

Sovellusten hallinta estää sovelluksia tekemästä toimia, jotka voivat vaarantaa käyttöjärjestelmän toiminnan, ja varmistaa, että pääsy käyttöjärjestelmäresursseihin ja yksityisiin tietoihisi on valvottua.

Sovellusten hallinta seuraa tietokoneeseen asennettujen sovellusten toimintaa käyttöjärjestelmässä ja säätelee sovelluksia sääntöjen perusteella. Nämä säännöt rajoittavat sovellusten epäilyttävää toimintaa, kuten sovellusten suojattujen resurssien käyttöä. Näitä resursseja ovat mm. tiedostot ja kansiot, rekisteriavaimet sekä verkko-osoitteet:

- Sovellusten oikeuksia seuraaviin toimintoihin ei voi määrittää 64-bittistä käyttöjärjestelmää käyttävässä tietokoneessa.
- Fyysisen muistin suora käyttö
- Tulostinajureiden hallinta
- Palvelun luonti
- Palvelun luku

- Palvelun muokkaus
- Palvelun uudelleenmääritys
- Palvelun hallinta
- Palvelun käynnistys
- Palvelun poisto
- Käyttöoikeus sisäiseen selaintietoon
- Käyttöjärjestelmän kriittisten objektien käyttö
- Käyttöoikeus salasanataltioon
- Virheenkorjauksen oikeuksien asetus
- Käyttöjärjestelmän ohjelmaliittymien käyttö
- Käyttöjärjestelmän ohjelmaliittymien käyttö (DNS)
- Sovellusten oikeuksia seuraaviin toimintoihin ei voi määrittää 64-bittistä Microsoft Windows 8 -käyttöjärjestelmää käyttävässä tietokoneessa.
- Ikkunaviestien lähettäminen toisiin prosesseihin
- Epäilyttävät toimenpiteet
- Kaappaajien asennus
- Saapuvien virtatapahtumien kaappaus
- Näyttökaappausten ottaminen

Palomuuri-komponentti hallinnoi sovellusten verkkotoimintaa.

Kun sovellus käynnistetään tietokoneella ensimmäisen kerran, Sovellusten hallinta tarkistaa sovelluksen turvallisuuden ja sijoittaa sen ryhmään (Luotettu, Ei-luotettu, Paljon rajoitettu tai Vähän rajoitettu). Ryhmä määrittää säännöt, joiden mukaan Kaspersky Total Security hallitsee sovelluksen toimintaa.

Kaspersky Total Security lajittelee sovellukset luottamusryhmiin (Luotettu, Vähän rajoitettu, Paljon rajoitettu tai Ei-luotettu) vain, jos käytössä on joko Sovellusten hallinta tai Palomuuri tai molemmat komponentit yhtäaikaa. Jos molemmat komponentit on poistettu käytöstä, sovelluksien luottamusryhmät määrittävä toiminto ei ole käytössä.

Voit muokata sovelluksen hallintasääntöjä manuaalisesti.

SOVELLUKSEN HALLINNAN MÄÄRITTÄMINEN

Voit määrittää Sovelluksen hallinnan seuraavasti:

1. Avaa Kaspersky Total Securityn pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa **Sovellusten hallinta** -ikkuna napsauttamalla **Työkalut**-ikkunassa **Sovellusten hallinta** -linkkiä.

4. Napsauta **Sovellusten hallinta** -ikkunan **Sovellukset**-osiossa **Hallitse sovelluksia** -linkkiä, jolloin **Hallitse sovelluksia** -ikkuna avautuu.

5. Valitse luettelosta haluamasi sovellus ja kaksoisnapsauta sitä, jolloin **Sovellussäännöt** -ikkuna avautuu.

   Sovellussäännöt-ikkuna avautuu.

6. Määritä sovelluksen hallinnan säännöt:

   - Voit määrittää säännöt sovellusten pääsylle käyttöjärjestelmäresursseihin seuraavasti:

     a. Valitse **Tiedostot ja järjestelmärekisteri** -välilehdellä haluamasi resurssiluokka.

     b. Napsauta hiiren oikealla painikkeella saraketta, jossa on resurssiin käytettävissä oleva toiminto (**Lukeminen**, **Kirjoittaminen**, **Poista** tai **Luominen**) avataksesi pikavalikon. Valitse pikavalikosta haluamasi kohde (**Salli**, **Estä**, **Toiminto** tai **Peri**).

   - Voit muokata sovelluksen oikeuksia suorittaa eri toimenpiteitä käyttöjärjestelmässä seuraavasti:

     a. Valitse haluamasi oikeusluokka **Oikeudet**-välilehdeltä.

     b. Avaa pikavalikko napsauttamalla **Oikeus**-saraketta hiiren oikealla painikkeella. Valitse pikavalikosta haluamasi kohde (**Salli**, **Estä**, **Kysy toimenpidettä** tai **Peri**).

   - Voit muokata sovelluksen oikeuksia suorittaa eri toimenpiteitä verkossa seuraavasti:

     a. Napsauta **Verkkosäännöt**-välilehdessä **Lisää**-painiketta.

        Verkkosääntö-ikkuna avautuu.

     b. Määritä vaaditut sääntöasetukset avautuvassa ikkunassa ja napsauta **Tallenna**-painiketta.

     c. Määritä uudelle säännölle prioriteetti siirtämällä sitä luettelossa **Ylös**- ja **Alas**-painikkeilla.

   - Jos haluat rajata ulos määrätyt toimenpiteet Sovellusten hallinta -komponentista, valitse toimenpiteet, joita ei säädellä **Poissulkemiset**-välilehdellä.

7. Napsauta **Tallenna**-painiketta.

   Sovellusten valvonnan poissulkemiselle luodut säännöt ovat nähtävissä Kaspersky Total Securityn asetusikkunan osiossa **Uhkat ja poissulkemiset**.

Sovellusten hallinta valvoo ja rajoittaa sovelluksen toimintaa määritettyjen asetusten mukaisesti.

TIETOJA SOVELLUSTEN OIKEUDESTA KÄYTTÄÄ VERKKOKAMERAA

Rikolliset voivat yrittää saada verkkokameran luvattomasti käyttöön erityisen ohjelmiston avulla. Kaspersky Total Security estää verkkokameran luvattoman käytön ja ilmoittaa, kun käyttö on estetty. Oletusarvoisesti Kaspersky Total Security estää verkkokameran käytön niiltä sovelluksilta, jotka on sisällytetty ryhmiin Paljon rajoitettu tai Ei-luotettu.

Sovellusten hallinnan asetusikunasta voit sallia verkkokameran käytön sovelluksille (ks. "Verkkokameran käyttöoikeuden myöntäminen sovellukselle" sivulla 73), jotka ovat Korkea rajoitettu- ja Ei-luotettu-ryhmissä. Jos Vähän rajoitettu -luottamusryhmään kuuluva sovellus yrittää muodostaa yhteyden verkkokameraan, Kaspersky Total Security näyttää ilmoituksen ja kysyy, sallitaanko verkkokameran käyttö kyseiselle sovellukselle.

Jos verkkokameraa yrittää käyttää sovellus, jolta verkkokameran käyttö on oletusarvoisesti estetty, Kaspersky Total Security näyttää asiaa koskevan ilmoituksen. Ilmoitus voi esimerkiksi kertoa, että tietokoneelle asennettu sovellus (kuten Skype) vastaanottaa tällä hetkellä videotietoja verkkokamerasta. Ilmoitusten pudotusvalikossa voit estää sovellusta käyttämästä verkkokameraa tai siirtyä määrittämään sovelluksien verkkokameran käyttöoikeuden asetuksia (katso osio "Verkkokameran käyttöoikeuden asetuksien määrittäminen" sivulla 73). Ilmoitusta ei näytetä, jos jokin sovellus on jo käynnissä koko näytön tilassa.

Sovelluksen vastaanottamaa videotietoa käsittelevän ilmoituksen pudotusluettelosta voit myös piilottaa ilmoituksen valitsemalla kohteen **Piilota ilmoitus** tai siirtyä Asetukset-osioon määrittämään ilmoitusten näyttöasetuksia (katso osio "Verkkokameran käyttöoikeuden asetuksien määrittäminen" sivulla 73).

Oletuksena Kaspersky Total Security sallii verkkokameran käytön sovelluksille, jotka kysyvät lupaasi, jos sovelluksen käyttöliittymää ladataan tai poistetaan muistista tai sovellus ei vastaa etkä voi sallia käyttöä manuaalisesti.

Verkkokameran suojausta koskevat seuraavat toiminnot ja rajoitukset:

- Sovellus rajoittaa verkkokameran tietojen käsittelystä saatavien video- ja still-kuvien käyttöä.
- Kaspersky Total Security ohjaa vain USB- ja IEEE1394-väylien kautta liitettyjä verkkokameroita, jotka näkyvät Windowsin Laitehallinnassa Kuvanmuodostuslaitteina.

Luettelo tuetuista verkkokameroista on tässä linkissä http://support.kaspersky.com/10978.

Sovellusten hallinta -komponentin on oltava käytössä, jotta verkkokameran luvattomalta käytöltä voidaan suojautua.

VERKKOKAMERAN KÄYTTÖOIKEUDEN ASETUKSIEN MÄÄRITTÄMINEN

Voit määrittää verkkokameran käyttöoikeuden asetukset seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Avaa **Asetukset**-ikkuna napsauttamalla pääikkunan alaosassa olevaa **Asetukset**-linkkiä.
3. Valitse **Suojaus**-osion oikeassa alakulmassa sijaitseva **Verkkokameran käyttöoikeus** -komponentti.
4. Määritä tietokoneeseen liitetyn verkkokameran käyttöoikeuden asetukset:
   - Jos haluat estää verkkokameran käytön kaikilta sovelluksilta, valitse **Estä verkkokameran käyttöoikeus kaikilta sovelluksilta** -valintaruutu.
   - Jos haluat saada ilmoituksen, kun jokin sovellus käyttää verkkokameraa luvallisesti, valitse **Näytä ilmoitus, kun verkkokamera on sellaisen sovelluksen käytössä, jolla on oikeus käyttää verkkokameraa** -valintaruutu.
   - Jos haluat myöntää verkkokameran käyttöoikeuden kaikille sovelluksille, siirry **Asetukset**-ikkunassa **Suojaus**-välilehdelle ja poista käytöstä **Verkkokameran käyttöoikeus**.

VERKKOKAMERAN KÄYTTÖOIKEUDEN MYÖNTÄMINEN SOVELLUKSELLE

Voit myöntää verkkokameran käyttöoikeuden sovellukselle seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa **Sovellusten hallinta** -ikkuna napsauttamalla **Työkalut**-ikkunassa **Sovellusten hallinta** -linkkiä.
4. Napsauta **Sovellusten hallinta** -ikkunan **Sovellukset**-osiossa **Hallitse sovelluksia** -linkkiä, jolloin **Hallitse sovelluksia** -ikkuna avautuu.

5. Valitse luettelosta sovellus, jolle haluat myöntää verkkokameran käyttöoikeuden. Avaa **Sovellussäännöt** -ikkuna kaksoisnapsauttamalla sovellusta.

6. Siirry **Sovellussäännöt** -ikkunassa **Oikeudet**-välilehdelle.

7. Valitse oikeusluokkien luettelosta **Järjestelmän muutos** → **Epäilyttävät järjestelmän muutokset** → **Käytä verkkokameraa**.

8. Avaa pikavalikko napsauttamalla **Oikeus**-saraketta hiiren oikealla painikkeella ja valitse sitten **Salli**.

9. Napsauta **Tallenna**-painiketta.

Valitulle sovellukselle myönnetään verkkokameran käyttöoikeus.

LUOTETUT SOVELLUKSET -TILA

Tässä osiossa on tietoja Luotetut sovellukset -tilasta.

TÄSSÄ OSIOSSA

TIETOJA LUOTETUT SOVELLUKSET -TILASTA

Kaspersky Total Securityn avulla voit luoda tietokoneellesi turvallisen käyttöympäristön eli Luotetut sovellukset -tilan, jossa vain luotetut sovellukset saavat luvan käynnistyä. Luotetut sovellukset -tila on hyödyllinen, jos käytät tiettyjä tunnettuja sovelluksia eikä sinun tarvitse usein suorittaa uusia tuntemattomia tiedostoja Internetistä. Luotetut sovellukset -tilassa Kaspersky Total Security estää kaikki sovellukset, joita Kaspersky Lab ei ole luokitellut luotetuksi. Päätös siitä, luotetaanko sovellukseen, voi syntyä perustuen Kaspersky Security Networkista saatuihin tietoihin, sovelluksen digitaalisen allekirjoituksen tietoihin, asentajan luottamustasoon sekä sovelluksen latauksen lähteeseen.

Luotetut sovellukset -tilassa on seuraavat ominaisuudet ja rajoitukset:

- Luotetut sovellukset -tilan käyttö edellyttää, että seuraavat suojauskomponentit ovat toiminnassa: Sovellusten hallinta, Tiedostojen virustorjunta ja Järjestelmän tarkkailu. Jos jokin näistä komponenteista lopettaa toiminnan, Luotetut sovellukset -tila otetaan pois käytöstä.

- Luotetut sovellukset -tila ei välttämättä ole käytettävissä, jos järjestelmätiedostot sijaitsevat kiintolevyn osiossa, jonka tiedostojärjestelmä on muu kuin NTFS.

- Luotetut sovellukset -tila voi puuttua tai se ei ehkä ole valittavissa Kaspersky Total Securityn nykyisessä sovellusversiossa. Luotetut sovellukset -tilan saatavuus Kaspersky Total Securityssa riippuu alueestasi ja palveluntarjoajastasi. Jos tarvitset Luotetut sovellukset -tilaa, muista kysyä siitä ostaessasi sovellusta.

- Jos Kaspersky Total Security -versio tukee Luotetut sovellukset tilaa - mutta se ei ole juuri nyt käytettävissä, se saattaa tulla käyttöön kun tietokannat ja sovelluksen ohjelmistomoduulit päivitetään (ks. "Tietokantojen ja sovelluksen ohjelmistomoduulien päivittäminen" sivulla 35). Kun tietokannat ja sovelluksen sovellusmoduulit on päivitetty, voit määrittää tuntemattomien sovellusten ja moduulien käynnistystilan.

Ennen Luotetut sovellukset -tilan käyttöönottoa Kaspersky Total Security analysoi käyttöjärjestelmäsi ja tietokoneellesi asennetut sovellukset. Analyysi voi kestää pitkään (jopa muutamia tunteja). Jos analyysi havaitsee ohjelmia, joita ei voida luokitella luotetuiksi, Luotetut sovellukset -tilan käyttöönottoa ei suositella. Kun Luotetut sovellukset -tila on käytössä, Kaspersky Total Security saattaa estää sovelluksia, joita ei ole tunnistettu luotetuiksi. Voit sallia tällaisten sovellusten käytön (ks. "Sovellusten toiminnan hallinta tietokoneella ja verkossa" sivulla 70) jos sinulla on niitä käytössäsi ja ottaa sitten Luotetut sovellukset -tilan käyttöön.

Kaspersky Total Security voi suorittaa käyttöjärjestelmän ja asennettujen sovellusten analyysin automaattisesti taustalla. Jos Kaspersky Total Securityn tekemä analyysi osoittaa, että tietokoneessa käytetään lähinnä luotettuja sovelluksia, Luotetut sovellukset -tila voidaan ottaa automaattisesti käyttöön.

LUOTETUT SOVELLUKSET -TILAN OTTAMINEN KÄYTTÖÖN

Ota Luotetut sovellukset -tila käyttöön seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa **Sovellusten hallinta** -ikkuna napsauttamalla **Työkalut**-ikkunassa **Sovellusten hallinta** -linkkiä.
4. Napsauta **Sovellusten hallinta** -ikkunan alaosassa olevassa **Luotetut sovellukset -tila on pois käytöstä** -osiossa **Ota käyttöön** -linkkiä.

   Jos kaikki tarvittavat suojauskomponentit eivät ole käytössä, näyttöön avautuu ikkuna. Se sisältää lisätietoja suojauskomponenteista, jotka on otettava käyttöön ennen Luotetut sovellukset -tilan käyttöä.
5. Napsauta **Jatka**-painiketta.

   Tämä suorittaa analyysin käyttöjärjestelmästä ja asennetuita sovelluksista, lukuun ottamatta suoritettavaa koodia sisältäviä tilapäisiä tiedostoja sekä resurssien dynaamisia linkityskirjastoja. Analyysin eteneminen näkyy avautuvassa **Asennettujen sovellusten analyysi** -ikkunassa.

   Odota, kunnes käyttöjärjestelmän ja asennettujen sovellusten analyysi on valmis. Voit pienentää **Asennettujen sovellusten analyysi** -ikkunan. Silloin analyysi suoritetaan taustalla. Voit tarkastella analyysin etenemistä napsauttamalla **Asennettujen sovellusten analyysi (<N> %)** -linkkiä **Sovellusten hallinta** -ikkunassa.
6. Voit tarkastella analyysitulosten tietoja **Asennettujen sovellusten ja suoritettavien tiedostojen analysointi on valmis** -ikkunassa.

   Jos analyysin yhteydessä havaitaan järjestelmätiedostoja, joiden ominaisuuksia ei tunnisteta, suosittelemme välttämään Luotetut sovellukset -tilan käyttöönottoa. Suosittelemme välttämään Luotetut sovellukset -tilan käyttöönottoa myös silloin, kun on havaittu paljon sovelluksia, joista on saatavana niin vähän tietoa, ettei Kaspersky Total Security voi luokitella niitä täysin turvalliseksi.

   Voit tarkastella ei-luotettujen järjestelmätiedostojen tietoja napsauttamalla **Siirry tuntemattomien järjestelmätiedostojen luetteloon** -linkkiä. Ei-luotettujen järjestelmätiedostojen luettelo tulee näkyviin **Tuntemattomat järjestelmätiedostot** -ikkunassa. Voit myös peruuttaa Luotetut sovellukset -tilan käytön napsauttamalla **Älä ota käyttöön Luotetut sovellukset -tilaa** -painiketta.
7. Jos haluat sallia ei-luotettujen sovellusten ja järjestelmätiedostojen suorittamisen, napsauta **Asennettujen sovellusten ja suoritettavien tiedostojen analysointi on valmis** -ikkunassa **Salli tuntemattomien järjestelmätiedostojen suorittaminen ja jatka** -linkkiä.
8. Napsauta **Ota käyttöön Luotetut sovellukset -tila oletusarvoisesti** -painiketta.

Luotetut sovellukset -tila on nyt käytössä. Kaspersky Total Security estää kaikki sovellukset ja järjestelmätiedostot, joita ei ole luokiteltu luotetuiksi. Sovellus siirtyy **Sovellusten hallinta** -ikkunaan.

Kun otat Luotetut sovellukset -tilan käyttöön ja käynnistät käyttöjärjestelmän uudelleen ensimmäistä kertaa, tuntemattomien sovellusten käynnistyminen sallitaan, kunnes Kaspersky Total Security käynnistyy. Kun käyttöjärjestelmä käynnistetään myöhemmin uudelleen, Kaspersky Total Security estää tuntemattomien sovellusten käynnistymisen välittömästi.

LUOTETUT SOVELLUKSET -TILAN OTTAMINEN POIS KÄYTÖSTÄ

Voit ottaa Luotetut sovellukset -tilan pois käytöstä seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa **Sovellusten hallinta** -ikkuna napsauttamalla **Työkalut**-ikkunassa **Sovellusten hallinta** -linkkiä.
4. Napsauta ikkunan alaosassa olevassa **Luotetut sovellukset -tila on käytössä** -osiossa **Poista käytöstä** -linkkiä.

Luotetut sovellukset -tila on nyt pois käytöstä.

TIEDOSTOSILPPURI

Henkilötietojen lisäturvallisuus varmistetaan suojaamalla poistettuja tietoja niin, etteivät hakkerit voi luvattomasti palauttaa niitä.

Kaspersky Total Security sisältää pysyvän tietojen poistotyökalun, joka tekee tietojen palauttamisesta mahdotonta normaaleilla ohjelmistoilla.

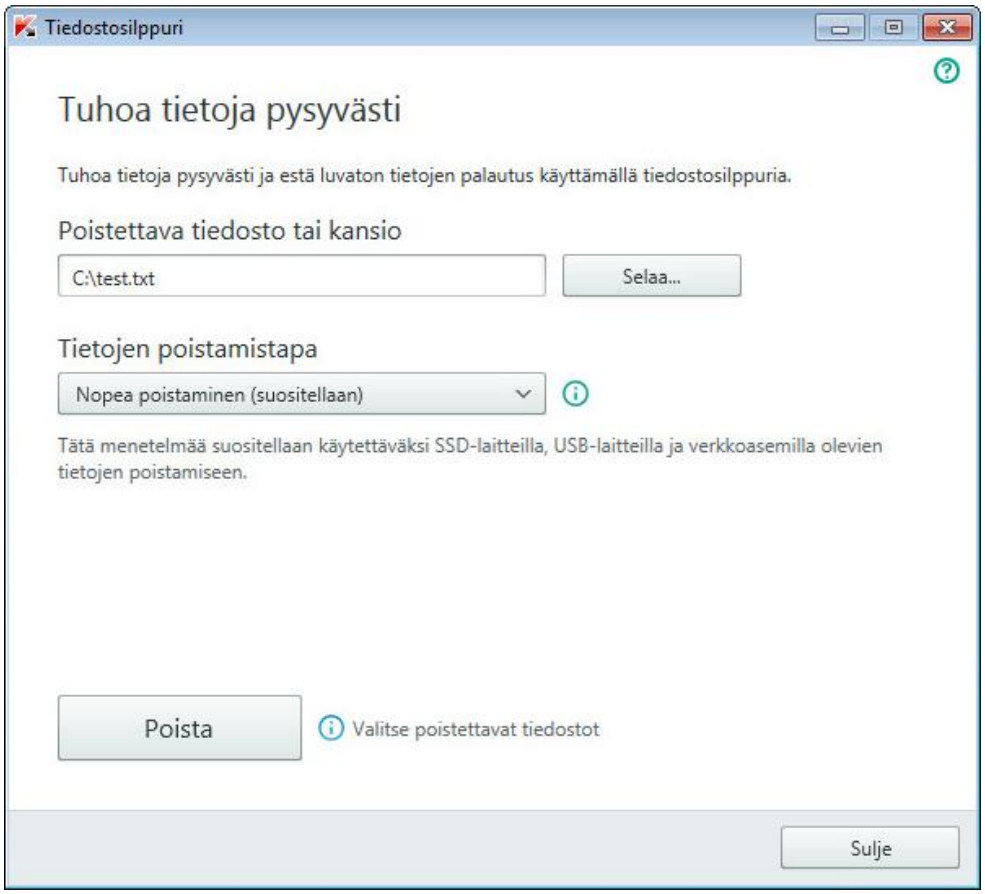
Kaspersky Total Security mahdollistaa tietojen poistamisen ilman palautusmahdollisuutta seuraavilta tietovälineiltä:

- paikalliset asemat ja verkkoasemat. Poisto on mahdollista, jos käyttäjällä on oikeudet tiedon kirjoittamiseen ja poistamiseen.
- Siirrettävät asemat tai muut laitteet, jotka tunnistetaan siirrettävinä asemina (kuten levykkeet, muistikortit, USB-levyt ja matkapuhelimet). Tiedot voidaan poistaa muistikortilta, jos sen mekaaninen kirjoitussuojaus ei ole käytössä.

Voit poistaa tiedot, joita voit käyttää henkilökohtaisella tililläsi. Varmista ennen tietojen poistoa, että käynnissä olevat sovellukset eivät käytä niitä.

Tiedon poistaminen pysyvästi:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Napsauta **Työkalut**-ikkunassa **Tiedostosilppuri**-linkkiä avataksesi **Tiedostosilppuri**-ikkunan (katso kuva alla).



*Kuva 6. **Tiedostosilppuri**-ikkuna*

4. Napsauta **Selaa**-painiketta ja valitse pysyvästi poistettava kansio tai tiedosto avautuvassa **Valitse kansio** -ikkunassa.

   Järjestelmätiedostojen ja -kansioiden poisto voi aiheuttaa käyttöjärjestelmän toimintahäiriöitä.

5. Valitse haluttu tietojen poistoalgoritmi **Tietojen poistamistapa** -pudotusluettelosta.

   Jos haluat poistaa tietoja SSD- ja USB-laitteista sekä verkkoasemista, suosittelemme käyttämään **Nopea poistaminen**- tai **GOST R 50739-95** -menetelmää. Muut poistomenetelmät voivat vaurioittaa SSD- tai USB-laitetta tai verkkoasemaa.

6. Napsauta **Poista**-painiketta.

7. Valitse **Kyllä** avautuvassa poiston vahvistusikkunassa. Jos joitakin tiedostoja ei poisteta, yritä poistaa ne uudelleen napsauttamalla avautuvassa ikkunassa **Yritä uudelleen** -painiketta. Voit valita toisen poistettavan kansion napsauttamalla **Lopeta**-painiketta.

TARPEETTOMIEN TIETOJEN POISTAJA

Tässä osiossa on ohjeita väliaikaisten ja tarpeettomien tiedostojen poistamiseen.

TÄSSÄ OSIOSSA

TIETOJA TARPEETTOMIEN TIETOJEN POISTAMISESTA

Käyttöjärjestelmän kansioihin kertyy ajan kuluessa väliaikaisia tai tarpeettomia tiedostoja. Nämä tiedostot saattavat käyttää paljon levytilaa, mikä heikentää järjestelmän tehokkuutta. Lisäksi haittaohjelmat saattavat hyödyntää niitä.

Sovellukset ja käyttöjärjestelmä luovat väliaikaisia tiedostoja käynnistyessään. Kaikkia väliaikaisia tiedostoja ei kuitenkaan poisteta, kun käyttöjärjestelmä tai ne luonut sovellus suljetaan. Kaspersky Total Security sisältää tarpeettomien tietojen poistotoiminnon.

Tarpeettomien tietojen poistaja havaitsee ja poistaa seuraavia tiedostoja:

- Järjestelmän lokitiedostot, joihin tallennetaan kaikkien aktiivisten sovelluksien nimet
- Eri sovelluksien ja päivitystyökalujen (kuten Windows Update) tapahtumalokit
- Järjestelmän yhteyslokit
- Internet-selaimien väliaikaiset tiedostot (evästeet)
- Väliaikaiset tiedostot, joita ei poistettu sovelluksen asennuksen tai poistamisen yhteydessä
- Roskakorin sisältö
- Temp-kansiossa säilytettävät väliaikaistiedostot, jotka saattavat käyttää jopa useita gigatavuja tallennustilaa.

Tarpeettomien tiedostojen lisäksi ohjattu toiminto poistaa tiedostoja, jotka saattavat sisältää luottamuksellisia tietoja kuten salasanoja, käyttäjätunnuksia tai rekisteröintilomakkeiden tietoja. Näiden tietojen lopulliseen poistamiseen suosittelemme kuitenkin ohjattua yksityisten tietojen poistotoimintoa.

TARPEETTOMIEN TIETOJEN POISTAMINEN

Voit käynnistää ohjatun tarpeettomien tietojen poistotoiminnon seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Napsauta avautuvassa ikkunassa **Tarpeettomien tietojen poistaja** -linkkiä, jolloin ohjattu tarpeettomien tietojen poistotoiminto käynnistyy.

Ohjattu toiminto koostuu ikkunoista (vaiheista), joissa liikutaan painikkeilla **Takaisin** ja **Seuraava**. Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta. Voit keskeyttää ohjatun toiminnon milloin tahansa napsauttamalla **Peruuta**-painiketta.

Alla on tarkempia tietoja ohjatusta toiminnosta.

Vaihe 1. Ohjatun toiminnon käynnistäminen

Ohjatun toiminnon ensimmäinen sivu sisältää tietoja tarpeettomien tietojen poistamisesta.

Käynnistä ohjattu toiminto napsauttamalla **Seuraava**-painiketta.

Vaihe 2. Tarpeettomien tietojen haku

Ohjattu toiminto etsii tietokoneesta tarpeettomia tietoja. Haku voi kestää jonkin aikaa. Kun haku on valmis, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Vaihe 3. Toimenpiteen valinta tarpeettomien tietojen poistamiseksi

Kun tarpeettomien tietojen haku on suoritettu, näyttöön avautuu toimenpideluettelon sisältävä ikkuna.

Jos haluat ohjatun toiminnon suorittavan jonkin toimenpiteen, valitse toimenpiteen vasemmalla puolella oleva valintaruutu. Oletusasetuksena on, että ohjattu toiminto suorittaa kaikki suositellut ja vahvasti suositellut toiminnot. Jos et halua suorittaa jotakin tiettyä toimintoa, poista valinta sen vieressä olevasta valintaruudusta.

Oletuksena valittujen valintaruutujen valinnan poistamista ei suositella. Tämä voi heikentää tietokoneen turvallisuutta.

Kun olet määrittänyt toimenpiteet ohjatun toiminnon suoritusta varten, napsauta **Seuraava**-painiketta.

Vaihe 4. Tarpeettomien tietojen poistaminen

Ohjattu toiminto suorittaa edellisen vaiheen aikana valitut toiminnot. Tarpeettomien tietojen poistamisessa voi kestää jonkin aikaa.

Kun tarpeettomat tiedot on poistettu, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Käyttöjärjestelmä saattaa käyttää joitakin tiedostoja (kuten Microsoft Windowsin lokitiedostoja ja Microsoft Office tapahtumalokia) ohjatun toiminnon ollessa käynnissä. Ohjattu toiminto kehottaa käynnistämään tietokoneen uudelleen, jotta nämä tiedostot voidaan poistaa.

Vaihe 5. Ohjatun toiminnon viimeistely

Sulje ohjattu toiminto napsauttamalla **Lopeta**-painiketta.

VARMUUSKOPIOINTI JA TIETOJEN PALAUTUS

Tämä osio sisältää tietoa tietojen varmuuskopioinnista.

TÄSSÄ OSIOSSA

TIETOJA VARMUUSKOPIOINNISTA JA TIETOJEN PALAUTUKSESTA

Tietojen varmuuskopiointi on tarpeen kun sinun on suojattava tietosi katoamiselta, jos tietokoneesi menee rikki tai varastetaan, tai jos tiedot poistetaan vahingossa tai hakkerit tuhoavat ne.

Varmuuskopioi tietoja luomalla (katso osio "Varmuuskopiointitehtävän luominen" sivulla 83) ja käynnistämällä (katso osio "Varmuuskopiointitehtävän käynnistäminen" sivulla 85) varmuuskopiointitehtävä. Tehtävä voidaan käynnistää automaattisesti aikataulun mukaan tai manuaalisesti. Voit myös tarkastella tietoja suoritetuista varmuuskopiointitehtävistä sovelluksella.

Suosittelemme varmuuskopioimaan siirrettävällä asemalla tai verkkotaltiossa olevat tiedot.

Kaspersky Total Securityn avulla voit luoda varmuuskopioita käyttämällä seuraavia taltiotyyppejä:

- Paikallinen asema
- Siirrettävä asema (esim. ulkoinen kiintolevy)
- Verkkoasema
- FTP-palvelin
- Verkkotaltio (katso osio "Tietoja verkkotaltiosta" sivulla 86).

VARMUUSKOPIOINTITEHTÄVÄN LUOMINEN

Varmuuskopiointitehtävän luominen:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Varmuuskopiointi ja tietojen palautus** -painiketta.
3. Tee seuraavat toimet avautuvassa **Varmuuskopiointi ja tietojen palautus** -ikkunassa:

   - Napsauta **Valitse varmuuskopioitavat tiedostot** -painiketta, jos varmuuskopiointitehtävää ei ole vielä luotu.
   - Napsauta **Luo varmuuskopioita toisista tiedostoista** -painiketta, jos sinulla on jo olemassa oleva varmuuskopiointitehtävä ja haluat luoda uuden.

   Varmuuskopiointitehtävän ohjattu luontitoiminto avautuu.

   Ohjattu toiminto koostuu ikkunoista (vaiheista), joissa liikutaan painikkeilla **Takaisin** ja **Seuraava**. Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta. Voit keskeyttää ohjatun toiminnon milloin tahansa napsauttamalla **Peruuta**-painiketta.

   Alla on tarkempia tietoja ohjatusta toiminnosta.

Valitse tiedostot

Valitse ohjatun toiminnon tässä vaiheessa varmuuskopioitavat tiedostotyypit tai kansiot:

- Suorita nopea asetusten määritys valitsemalla jokin esiasetetuista tiedostotyypeistä (Omat tiedostot- ja Työpöytä-kansioissa olevat tiedostot, valokuvat sekä kuvat, elokuvat ja videot tai musiikkitiedostot). Jos vahvistat valinnan, ohjattu toiminto etenee suoraan **Valitse varmuuskopiointitaltio** -vaiheeseen.
- Valitse **Luo varmuuskopiot määritetyissä kansioissa olevista tiedostoista**, jos haluat määrittää varmuuskopioitavat kansiot manuaalisesti.

Valitse varmuuskopioitavat kansiot

Jos olet valinnut **Luo varmuuskopiot määritetyissä kansioissa olevista tiedostoista** -valinnan ohjatun toiminnon edellisessä vaiheessa, napsauta **Lisää kansio** -painiketta ja valitse kansio avautuvassa **Valitse kansio** -ikkunassa tai vedä kansio sovelluksen ikkunaan.

Valitse **Rajoita varmuuskopiointia tiedostotyyppien perusteella** -ruutu, jos haluat määrittää valittujen kansioiden varmuuskopioitavat tiedostoluokat.

Valitse varmuuskopioitavat tiedostotyypit

Jos valitsit **Rajoita varmuuskopiointia tiedostotyyppien perusteella** -ruudun ohjatun toiminnon edellisessä vaiheessa, valitse seuraavassa ikkunassa valintaruudut vastapäätä tiedostotyyppejä, jotka haluat varmuuskopioida.

Valitse varmuuskopiointitaltio

Valitse tässä vaiheessa varmuuskopiotaltio:

- **Verkkotaltio**. Valitse tämä asetus, jos haluat tallentaa varmuuskopiot Dropbox-verkkotaltioon. Ennen verkkotaltion käyttämistä sinun tulee aktivoida verkkotaltio (katso osio "Verkkotaltion aktivointi" sivulla 86). Kun varmuuskopioit tietoja verkkotaltioon, Kaspersky Total Security ei luo varmuuskopioita tietotyypeistä, jotka sisältyvät Dropboxin käyttöehtojen rajoituksiin.
- **Paikallinen asema**. Jos haluat tallentaa varmuuskopiot paikalliselle asemalle, valitse haluamasi paikallinen asema luettelosta.
- **Verkkotaltio**. Jos haluat tallentaa varmuuskopiot verkkotaltioon, valitse haluamasi verkkotaltio luettelosta.
- **Siirrettävä asema**. Jos haluat tallentaa varmuuskopiot siirrettävälle asemalle, valitse haluamasi siirrettävä asema luettelosta.

Tietojen turvallisuuden varmistamiseksi suosittelemme käyttämään verkkotaltiota tai luomaan varmuuskopiotaltiot siirrettäville asemille.

Verkkotaltion lisääminen:

1. Napsauta **Lisää verkkotaltio** -linkkiä, niin **Lisää verkkotaltio** -ikkuna avautuu ja voit valita verkkotaltion tyypin: verkkoasema tai FTP-palvelin.
2. Määritä verkkotaltioon yhdistämiseen vaadittavat tiedot.
3. Napsauta **OK**.

Siirrettävän aseman lisääminen varmuuskopiotaltioksi:

1. Napsauta **Yhdistä olemassa oleva taltio** -linkkiä, niin **Yhdistä taltio** -ikkuna avautuu.
2. Valitse **Siirrettävä asema** -osio.
3. Napsauta **Selaa**-painiketta ja määritä avautuvassa ikkunassa siirrettävä asema, jonne haluat tallentaa tiedostojen varmuuskopiot.

Valitse **Käytä lisäasetuksia taltioissa** -valintaruutu, jos haluat määrittää tiedostotaltioiden asetuksia kuten säilytettävien varmuuskopioversioiden lukumäärä ja varmuuskopioiden säilytysajan kesto.

Varmuuskopiointiaikataulun luominen

Tee jokin seuraavista tässä ohjatun toiminnon vaiheessa:

- Määritä varmuuskopiointitehtävän aikataulu, jos haluat että varmuuskopiointi aloitetaan automaattisesti.
- Valitse **Suorita varmuuskopiointi** -luettelossa **manuaalisesti**-vaihtoehto, jos haluat aloittaa tehtävän manuaalisesti.

Salasanan määrittäminen varmuuskopioiden suojaamista varten

Suojaa varmuuskopioiden käyttö salasanalla valitsemalla **Ota salasanasuojaus käyttöön** -valintaruutu ja täyttämällä **Varmuuskopioiden käytön salasana**- ja **Vahvista salasana** -kentät.

Tiedostoversioiden tallennusasetukset

Tämä vaihe on käytettävissä, jos valitsit **Käytä lisäasetuksia taltioissa** -ruudun edellisessä vaiheessa.

Määritä tiedostotaltion asetukset:

- Valitse **Rajoita varmuuskopioiden versioiden lukumäärää** -ruutu ja määritä **Tallennettavien varmuuskopioversioiden määrä** -luettelossa, kuinka monta varmuuskopioversiota yksittäisestä tiedostosta säilytetään.

- Valitse **Rajoita varmuuskopioiden versioiden säilytysaikaa** -ruutu ja määritä **Varmuuskopioiden vanhojen versioiden säilytysaika** -luettelossa, kuinka monta päivää kutakin varmuuskopioversiota säilytetään.

Varmuuskopiointitehtävän nimen syöttäminen

Suorita tässä vaiheessa seuraavat toimenpiteet:

1. Anna varmuuskopiointitehtävän nimi.

2. Valitse **Suorita varmuuskopiointi**, **kun ohjattu toiminto on suoritettu** -valintaruutu, ja varmuuskopiointi käynnistyy automaattisesti, kun ohjattu toiminto on suoritettu loppuun.

Ohjatun toiminnon viimeistely

Napsauta **Lopeta**-painiketta.

Varmuuskopiointitehtävä luodaan. Luomasi tehtävä näkyy **Varmuuskopiointi ja tietojen palautus** -ikkunassa.

VARMUUSKOPIOINTITEHTÄVÄN KÄYNNISTÄMINEN

Varmuuskopiointitehtävän käynnistäminen:

1. Avaa sovelluksen pääikkuna.

2. Napsauta **Varmuuskopiointi ja tietojen palautus** -painiketta.

3. Valitse varmuuskopiointitehtävä **Varmuuskopiointi ja tietojen palautus** -ikkunassa ja napsauta **Suorita varmuuskopiointi** -painiketta.

Varmuuskopiointitehtävä käynnistetään.

TIETOJEN PALAUTUS VARMUUSKOPIOSTA

Voit palauttaa tiedot varmuuskopiosta seuraavasti:

1. Avaa sovelluksen pääikkuna.

2. Napsauta **Varmuuskopiointi ja tietojen palautus** -painiketta.

3. Tee jokin seuraavista:

   - Napsauta haluamasi varmuuskopiointitehtävää vastapäätä olevaa **Palauta tiedostot** -painiketta.

   - Avaa ikkuna napsauttamalla **Hallitse taltioita** -painiketta ja napsauta haluamaasi varmuuskopiotaltiota vastapäätä olevaa **Palauta tiedostot** -painiketta.

4. Jos varmuuskopion luomisen yhteydessä määritettiin salasana, syötä kyseinen salasana **Anna salasana käyttääksesi taltiota** -ikkunassa.

5. Valitse **Varmuuskopioinnin päivä/aika** -pudotusluettelosta varmuuskopion luomisen päiväys ja aika.

6. Valitse palautettavien kansioiden vastapäätä olevat ruudut.
7. Jos haluat palauttaa vain tietyntyyppisiä tiedostoja, valitse haluamasi tyypit **Tiedostotyyppi**-pudotusluettelosta.
8. Napsauta **Palauta valitut tiedostot** -painiketta.

   Palauta tiedostot varmuuskopiosta -ikkuna avautuu.
9. Valitse yksi seuraavista kahdesta vaihtoehdosta:
   - **Alkuperäinen kansio**. Jos tämä vaihtoehto on valittu, sovellus palauttaa tiedot niiden alkuperäiseen kansioon.
   - **Määritetty kansio**. Jos tämä vaihtoehto on valittu, sovellus palauttaa tiedot määritettyyn kansioon. Valitse kansio, jonne haluat palauttaa tiedot napsauttamalla **Selaa**-painiketta.
10. Valitse **Jos havaitaan samannimisiä tiedostoja,** -pudotusluettelosta sovelluksen suorittama toiminto, kun palautettavan tiedoston nimi vastaa kohdekansiossa jo olevaa tiedoston nimeä.
11. Napsauta **Palauta**-painiketta.

    Palautettavaksi valitut tiedostot palautetaan varmuuskopiosta ja tallennetaan määritettyyn kansioon.

TIETOJA VERKKOTALTIOSTA

Kaspersky Total Securityn avulla voit tallentaa varmuuskopioita tiedoistasi verkkotaltioon etäpalvelimelle Dropbox-palvelun kautta.

Verkkotaltion käyttö:

- Varmista, että tietokone on yhdistetty Internetiin.
- Luo tili verkkotaltion palveluntarjoajan verkkosivustossa.
- Aktivoi verkkotaltio.

Voit varmuuskopioida tietoja kaikilta Kaspersky Total Securityn sisältäviltä laitteiltasi yhdelle ja samalle Dropbox-tilille, etkä näin ollen tarvitse useita eri verkkotaltioita.

Verkkotaltion koon määrittää verkkotaltiopalvelujen tarjoaja, Dropbox-verkkopalvelu. Katso lisätietoja palveluehdoista Dropbox-verkkosivustolta osoitteessa https://www.dropbox.com.

VERKKOTALTION AKTIVOINTI

Aktivoi verkkotaltio seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Varmuuskopiointi ja tietojen palautus** -painiketta.
3. Tee seuraavat toimet avautuvassa **Varmuuskopiointi ja tietojen palautus** -ikkunassa:
   - Napsauta **Valitse varmuuskopioitavat tiedostot** -painiketta, jos varmuuskopiointitehtävää ei ole vielä luotu.
   - Napsauta **Luo varmuuskopioita toisista tiedostoista** -painiketta, jos olet jo luonut varmuuskopiointitehtävän.

   Varmuuskopiointitehtävän ohjattu luontitoiminto (katso osio "Varmuuskopiointitehtävän luominen" sivulla 83) käynnistyy.

4. Määritä varmuuskopioitavien tiedostojen tietoluokka tai valitse tiedostot manuaalisesti tietotyyppien valintaikkunassa.

5. Valitse verkkotaltio taltioiden valintaikkunassa ja napsauta **Aktivoi**-painiketta.

   Verkkotaltion luonti edellyttää Internet-yhteyttä.

   Näyttöön tulee Dropbox-tilin kirjautumisikkuna.

6. Tee jokin seuraavista toimista avautuvassa ikkunassa:

   - Suorita rekisteröinti, jos et ole vielä rekisteröitynyt Dropbox-käyttäjäksi.
   - Jos sinulla on jo Dropbox-tili, kirjaudu sisään Dropbox-tilillesi.

7. Viimeistele verkkotaltion aktivointi vahvistamalla, että Kaspersky Total Security saa käyttää Dropbox-tiliäsi tietojen varmuuskopiointiin ja palauttamiseen. Kaspersky Total Security sijoittaa tallennettujen tietojen varmuuskopiot erilliseen kansioon, joka luodaan Dropbox-taltioon sovelluksia varten.

   Kun verkkotaltion aktivointi on valmis, taltion valintaikkuna avautuu. Se sisältää eri verkkotaltioita, joista voit valita haluamasi. Aktivoitujen verkkotaltioiden osalta sovellus näyttää käytetyn tilan ja tietojen tallennusta varten vapaana olevan tilan.

TIETOJEN TALLENTAMINEN TURVASÄILÖIHIN

Tässä osiossa on tietoja tietojen suojaamisesta tietosäiliöitä käyttämällä.

TÄSSÄ OSIOSSA

TIETOJA TURVASÄILÖSTÄ

Turvasäilöt on suunniteltu suojaamaan luottamuksellisia tietoja luvattomalta käytöltä. *Turvasäilö* on tiedon taltio tietokoneellasi. Voit lukita säilön tai avata sen lukituksen käyttämällä vain sinun tiedossasi olevaa salasanaa. Sinun on annettava salasana, jotta voit muokata lukitun turvasäilön tiedostoja.

Jos kadotat tai unohdat salasanan, et voi palauttaa tietoja.

Kaspersky Total Security käyttää turvasäilöjen luomiseen seuraavaa algoritmia: AES XTS 256, jonka avaimen tehokas pituus on 56-bittinen.

TIEDOSTOJEN SIIRTÄMINEN TURVASÄILÖÖN

Tiedostojen siirtäminen turvasäilöön:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Tietojen salaus** -painiketta.
3. Tee jokin seuraavista toimista avautuvassa **Tietojen salaus** -ikkunassa:
   - Valitse **Luo uusi turvasäilö**, jos sinulla ei vielä ole turvasäilöä.
   - Napsauta **Luo turvasäilö** -painiketta, jos olet aiemmin luonut turvasäilön.
4. Napsauta **Lisää tiedostoja ja kansioita turvasäilöön** -painiketta, niin Resurssienhallinta avataan ja voit määrittää, mitkä tiedostot siirretään turvasäilöön.

   Valitut tiedostot tulevat näkyviin **Tietojen salaus** -ikkunassa.
5. Napsauta **Jatka**-painiketta.
6. Kirjoita turvasäilön nimi ja määritä sen sijainti tai käytä oletusasetuksia.
7. Voit käyttää turvasäilöä nopeasti valitsemalla **Luo turvasäilön pikakuvake työpöydälle** -valintaruudun.
8. Napsauta **Jatka**-painiketta.

9. Täytä **Salasana**- ja **Vahvista salasana** -kentät ja napsauta **Jatka**.
10. Valitse, miten turvasäilön ulkopuolella olevien tiedostojen lähdekopioita käsitellään:
    - Poista turvasäilön ulkopuolella olevien tiedostojen lähdekopioita napsauttamalla **Poista**.
    - Säilytä turvasäilön ulkopuolella olevien tiedostojen lähdekopiot napsauttamalla **Ohita**.
11. Napsauta **Lopeta**-painiketta.

    Luomasi turvasäilö näkyy **Omat turvasäilöt** -luettelossa.
12. Lukitse turvasäilö napsauttamalla **Lukitse turvasäilö** -painiketta.

    Lukitun turvasäilön tietoja voidaan käyttää salasanan syöttämisen jälkeen.

TURVASÄILÖN TIEDOSTOJEN KÄYTTÄMINEN

Turvasäilön tietojen käyttäminen:

1. Avaa sovelluksen pääikkuna.
2. Napsauta **Tietojen salaus** -painiketta.
3. Napsauta avautuvassa **Tietojen salaus** -ikkunassa haluamasi turvasäilön vieressä olevaa **Avaa turvasäilö** -painiketta.
4. Anna salasana ja napsauta **Avaa turvasäilö Resurssienhallinnassa** -painiketta.

Turvasäilöön tallennetut tiedostot näkyvät Rersurssienhallinta-ikkunassa. Voit tehdä muutoksia tiedostoihin ja lukita turvasäilön uudelleen.

Jos haluat avata aiemmalla sovellusversiolla luotuja turvasäilöjä, muunna vanha turvasäilö uuteen muotoon. Sovellus kehottaa suorittamaan muuntamisen, kun turvasäilöä yritetään avata Kaspersky Total Securityllä.

Jos turvasäilö sisältää paljon tietoja, sen muuntamisessa uuteen muotoon voi kestää kauan aikaa.

KASPERSKY TOTAL SECURITY - OHJELMISTON HALLINTATOIMINTOJEN KÄYTÖN RAJOITTAMINEN SALASANALLA

Tietokone saattaa olla useiden käyttäjien käytössä, ja heidän tietokoneen käyttötaitonsa ja -kokemuksensa voivat vaihdella huomattavasti. Tietokoneen turvallisuus voi vaarantua, jos eri käyttäjät pääsevät rajoituksetta käyttämään Kaspersky Total Securitya ja sen asetuksia.

Voit rajoittaa pääsyä sovellukseen asettamalla järjestelmänvalvojan salasanan ja määrittämällä toimet, jotka vaativat kyseisen salasanan syöttämistä:

- Sovelluksen asetusten muokkaus.
- Sovelluksen sulkeminen.
- Sovelluksen poisto.

Voit suojata Kaspersky Total Securityn hallinnan salasanalla seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Asetukset**-linkkiä siirtyäksesi **Asetukset**-osioon.
3. Valitse ikkunan vasemmalla puolella oleva **Yleinen**-osio ja napsauta **Määritä salasanasuojaus** -linkkiä, jolloin näyttöön avautuu **Salasanasuojaus**-ikkuna.
4. Täytä avautuvassa ikkunassa **Uusi salasana**- ja **Vahvista salasana** -kentät.
5. Määritä **Salasanan laajuus** -asetusryhmässä sovelluksen toimet, joiden suorittamista haluat rajoittaa salasanalla.

Unohtunutta salasanaa ei voi palauttaa. Jos olet unohtanut salasanasi, ota yhteys tekniseen tukeen voidaksesi jälleen muokata Kaspersky Total Securityn asetuksia.

TIETOKONEEN SUOJAUKSEN KESKEYTTÄMINEN JA JATKAMINEN

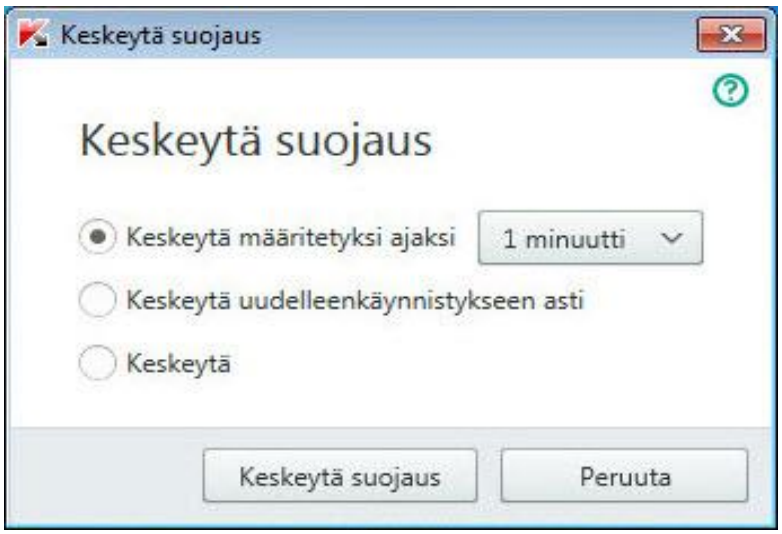
Suojauksen keskeyttäminen tarkoittaa, että kaikki suojauskomponentit poistetaan tilapäisesti käytöstä määrätyn ajanjakson ajaksi.

Kun suojaus on keskeytetty tai Kaspersky Total Security ei ole käynnissä, tietokoneessasi käynnissä olevien sovellusten toimintaa tarkkaillaan. Tiedot sovellusten toiminnan tarkkailun tuloksista tallennetaan käyttöjärjestelmään. Kun Kaspersky Total Security käynnistetään uudelleen tai suojausta jatketaan, Kaspersky Total Security käyttää tätä tietoa suojatakseen tietokonetta haitalliselta toiminnalta, jota on voitu suorittaa kun suojaus on ollut keskeytettynä tai Kaspersky Total Security on ollut pois käytöstä. Tietoja sovellusten toiminnan valvonnan tuloksista säilytetään toistaiseksi. Tiedot poistetaan, jos Kaspersky Total Security poistetaan tietokoneesta.

Tietokoneen suojauksen keskeyttäminen:

1. Valitse **Keskeytä suojaus** tehtäväpalkin sovelluskuvakkeen pikavalikosta.

   Näyttöön tulee **Keskeytä suojaus** -ikkuna (katso seuraava kuva).



Kuva 7. Keskeytä suojaus -ikkuna

2. Valitse **Keskeytä suojaus** -ikkunassa aika, jonka jälkeen suojausta jatketaan:

   - **Keskeytä määritetyksi ajaksi**: suojaus otetaan käyttöön, kun alla olevasta pudotusluettelosta valittu aika päättyy.
   - **Keskeytä uudelleenkäynnistykseen asti**: suojaus otetaan käyttöön sen jälkeen, kun sovellus tai käyttöjärjestelmä on käynnistetty uudelleen (edellyttäen, että sovellus käynnistyy automaattisesti käyttöjärjestelmän käynnistyessä).
   - **Keskeytä**: suojausta jatketaan vasta silloin, kun päätät jatkaa sitä.

Kun haluat jatkaa tietokoneen suojausta:

Valitse **Jatka suojausta** tehtäväpalkin sovelluskuvakkeen pikavalikosta.

SOVELLUKSEN OLETUSASETUSTEN PALAUTTAMINEN

Voit milloin tahansa palauttaa käyttöön Kaspersky Labin suosittelemat Kaspersky Total Securityn oletusarvoiset sovellusasetukset. Oletusasetukset voidaan palauttaa käyttämällä *sovelluksen ohjattua määritystoimintoa*.

Kun toiminto on valmis, jokainen suojauskomponentti palaa *Suositeltu*-suojaustasolle. Kun palautat käyttöön suositeltua turvallisuustasoa, voit tallentaa aiemmin määritetyt sovelluskomponenttien asetusarvot.

Voit käynnistää sovelluksen ohjatun määritystoiminnon seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Asetukset**-linkkiä.

   Näyttöön tulee **Asetukset**-osio.
3. Valitse **Yleinen**-osio.

   Ikkunassa näytetään Kaspersky Total Securityn asetukset.
4. Valitse ikkunan alaosassa olevasta **Hallinnoi asetuksia** -pudotusluettelosta **Palauta asetukset**.

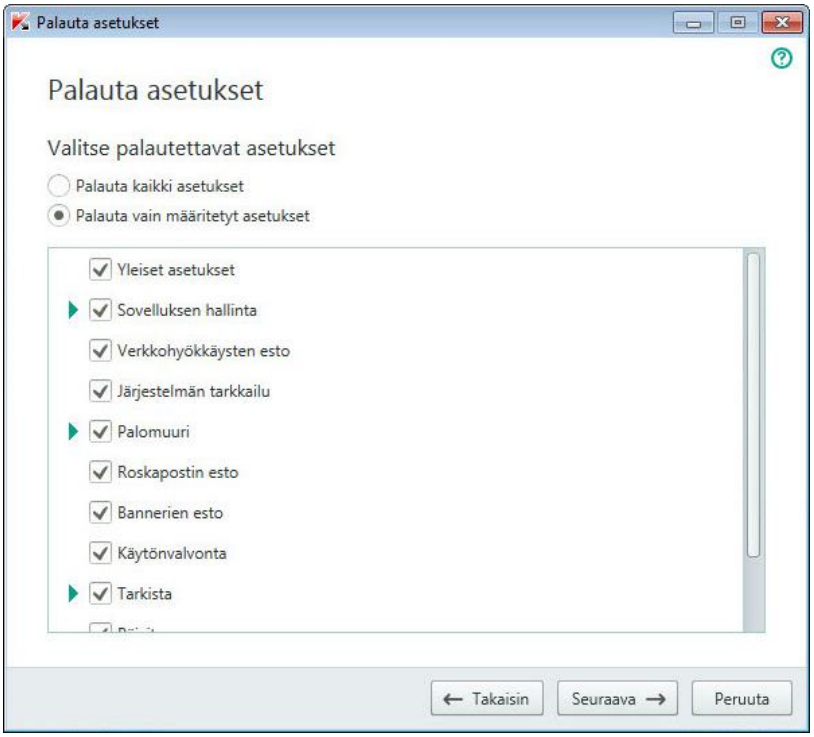
Alla on tarkempia tietoja ohjatusta toiminnosta.

Vaihe 1. Ohjatun toiminnon käynnistäminen

Jatka ohjattua asennusta napsauttamalla **Seuraava**-painiketta.

Vaihe 2. Palauta asetukset

Tässä ohjatun toiminnon ikkunassa näkyy, millä Kaspersky Total Securityn komponenteilla on oletusarvoista eroavia asetuksia. Asetukset voivat poiketa, koska niitä on muutettu käyttäjän toimesta, tai ne ovat muuttuneet Kaspersky Total Securityn (Palomuurin tai Roskapostin eston) koulutuksen takia. Jos joillekin komponenteille on luotu erityisiä asetuksia, myös ne näkyvät ikkunassa (katso seuraava kuva).



Kuva 8. Palauta asetukset -ikkuna

Erityisasetukset käsittävät Roskapostin eston sallittujen ja estettyjen lauseiden sekä osoitteiden luettelon, luotettujen verkko-osoitteiden ja palveluntarjoajien puhelinnumeroiden luettelon, sovelluskomponenteille luodut poissulkemissäännöt sekä Palomuurin paketti- ja sovellussuodatussäännöt.

Erityiset asetukset luodaan Kaspersky Total Security -sovelluksessa yksittäisten tehtävien ja tietoturvavaatimusten mukaisesti. Kaspersky Lab suosittelee, että tallennat erityisasetukset palauttaessasi sovelluksen oletusasetuksia.

Valitse tallennettavaksi haluamiesi asetusten ruudut ja napsauta **Seuraava**-painiketta.

Vaihe 3. Käyttöjärjestelmän analysointi

Tässä vaiheessa kerätään tietoja Microsoft Windows -sovelluksista. Nämä sovellukset lisätään luotettujen sovellusten luetteloon. Luotettujen sovellusten toimintaa käyttöjärjestelmässä ei rajoiteta.

Kun analyysi on suoritettu loppuun, ohjattu toiminto siirtyy automaattisesti seuraavaan vaiheeseen.

Vaihe 4. Palauttamisen viimeistely

Voit sulkea ohjatun toiminnon valmistumisen jälkeen napsauttamalla **Lopeta**-painiketta.

SOVELLUKSEN TOIMINTARAPORTIN TARKASTELU

Kaspersky Total Security ylläpitää toimintaraportteja kullekin suojauskomponentille. Raportin avulla voit saada tilastotietoa sovelluksen toiminnasta (esim. katsoa, kuinka monta haittaobjektia on havaittu ja neutraloitu tietyllä ajanjaksolla, kuinka monesti sovellus on päivitetty ko. ajanjaksolla, kuinka monta roskapostiviestiä on havaittu ja paljon muuta). Raportit säilytetään salatussa muodossa.

Voit tarkastella sovelluksen toimintaraporttia seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Näytä Lisätyökalut** -linkkiä. **Työkalut**-ikkuna avautuu.
3. Avaa **Raportit**-ikkuna napsauttamalla **Työkalut**-ikkunassa **Raportti**-linkkiä.

   Raportit-ikkuna sisältää raportteja sovelluksen toiminnasta nykyisen päivän aikana (ikkunan vasemmalla puolella) ja määrätyn ajanjakson aikana (ikkunan oikealla puolella).
4. Jos haluat tarkastella yksityiskohtaista raporttia sovelluksen toiminnasta, napsauta **Raportit**-ikkunan yläosassa olevaa **Yksityiskohtaiset raportit** -linkkiä. **Yksityiskohtaiset raportit** -ikkuna avautuu.

Yksityiskohtaiset raportit -ikkuna näyttää tiedot taulukkomuodossa. Voit valita useita eri lajittelutapoja, jotka helpottavat raporttien tarkastelua.

SOVELLUKSEN ASETUSTEN OTTAMINEN KÄYTTÖÖN TOISELLA TIETOKONEELLA

Kun olet määrittänyt sovelluksen, voit soveltaa sen asetuksia toiselle tietokoneelle asennettuun Kaspersky Total Securityn kopioon. Näin sovellus käyttää identtisiä asetuksia molemmilla tietokoneilla.

Sovelluksen asetukset tallennetaan määritystiedostoon, jonka voit siirtää toiselle tietokoneelle.

Kaspersky Total Security asetuksien siirtämisessä toiselle tietokoneelle on kolme vaihetta:

1. Tallenna sovelluksen asetukset määritystiedostoon.
2. Siirrä määritystiedosto toiselle tietokoneelle (esimerkiksi sähköpostitse tai siirrettävää asemaa käyttämällä).
3. Tuo määritystiedostossa olevat asetukset sovelluksen toiselle tietokoneelle asennettuun kopioon.

Voit viedä sovelluksen asetukset seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Avaa **Asetukset**-ikkuna napsauttamalla ikkunan alaosassa olevaa **Asetukset**-linkkiä.
3. Valitse **Asetukset**-ikkunassa oleva **Yleinen**-osio.
4. Valitse **Hallinnoi asetuksia** -pudotusluettelosta kohde **Vie asetukset**.

   Näyttöön avautuu **Tallenna nimellä** -ikkuna.
5. Määrittele määritystiedoston nimi ja napsauta **Tallenna**-painiketta.

Sovelluksen asetukset on nyt tallennettu määritystiedostoon.

Voit myös viedä sovelluksen asetukset komentokehotteesta seuraavalla komennolla: avp.com EXPORT <tiedostonimi>.

Voit tuoda asetukset sovelluksen toiselle tietokoneelle asennettuun kopioon seuraavasti:

1. Avaa Kaspersky Total Securityn pääikkuna toisella tietokoneella.
2. Avaa **Asetukset**-ikkuna napsauttamalla ikkunan alaosassa olevaa **Asetukset**-linkkiä.
3. Valitse **Asetukset**-ikkunassa oleva **Yleinen**-osio.
4. Valitse **Hallinnoi asetuksia** -pudotusluettelosta kohde **Tuo asetukset**.

   Avaa-ikkuna avautuu.
5. Valitse määritystiedosto ja napsauta **Avaa**-painiketta.

Asetukset tuodaan toiselle tietokoneelle asennettuun sovellukseen.

OSALLISTUMINEN KASPERSKY SECURITY NETWORK (KSN) -VERKOSTOON

Kaspersky Total Security käyttää pilvisuojausta, mikä parantaa tietokoneesi suojausta. Pilvisuojaus toteutetaan Kaspersky Security Network -infrastruktuurin avulla. Se hyödyntää eri puolilla maailmaa sijaitsevilta käyttäjiltä kerättyjä tietoja.

Kaspersky Security Network (KSN) on verkkopalveluinfrastruktuuri, joka tarjoaa pääsyn Kaspersky Labin verkkotietopankkiin. Se sisältää jatkuvasti päivittyvää tietoa tiedostojen, verkkoresurssien ja ohjelmistojen maineesta. Kaspersky Security Networkin tuottaman tiedon ansiosta Kaspersky Total Security voi tarjota suojaa tuntemattomilta uhkilta nopeammin, minkä lisäksi verkosto parantaa määrättyjen suojauskomponenttien tehoa ja vähentää virhehälytysten riskiä.

Kaspersky Security Network -verkostoon osallistuvien käyttäjien ansiosta Kaspersky Lab voi vastaanottaa nopeasti tietoja uusien uhkien tyypeistä ja lähteistä, kehittää ratkaisuja niiden neutraloimiseksi ja pienentää virhehälytysten määrän mahdollisimman alhaiseksi. Osallistumalla Kaspersky Security Network -verkostoon voit tarkastella sovellusten ja verkkosivustojen mainetilastoja.

Jos osallistut Kaspersky Security Network -verkostoon, tietoja käyttöjärjestelmäsi määrityksestä sekä Kaspersky Total Securityn prosessien aloitus- ja lopetusajasta lähetetään automaattisesti Kaspersky Labille (ks. "Lisätietoja tietojen toimittamisesta" sivulla 30).

TÄSSÄ OSIOSSA

KASPERSKY SECURITY NETWORK -OSALLISTUMISEN OTTAMINEN KÄYTTÖÖN TAI POISTAMINEN KÄYTÖSTÄ

Osallistuminen Kaspersky Security Networkiin on vapaaehtoista. Voit ottaa käyttöön tai poistaa käytöstä Kaspersky Security Networkin, kun asennat Kaspersky Total Securityn ja/tai milloin tahansa sen jälkeen, kun sovellus on asennettu.

Kaspersky Security Network -osallistumisen ottaminen käyttöön tai poistaminen käytöstä:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Asetukset**-linkkiä avataksesi **Asetukset**-ikkunan.
3. Valitse **Lisäasetukset**-osiossa **Palaute**-aliosio.

   Ikkunassa näkyy tietoja Kaspersky Security Networkista (KSN) ja KSN:n osallistumisasetuksista.
4. Voit ottaa käyttöön tai poistaa käytöstä osallistumisen Kaspersky Security Networkiin **Ota käyttöön**- tai **Poista käytöstä** -painikkeilla:

   - Jos haluat osallistua KSN-verkostoon, napsauta **Ota käyttöön** -painiketta.
   - Jos et halua osallistua KSN-verkostoon, napsauta **Poista käytöstä** -painiketta.

KASPERSKY SECURITY NETWORK -YHTEYDEN TARKISTAMINEN

Yhteys Kaspersky Security Networkiin voi katketa seuraavista syistä:

- Et osallistu Kaspersky Security Network -verkostoon.
- Tietokoneesi ei ole yhteydessä Internetiin.
- Avaimen nykyinen tila ei salli yhteyden muodostamista Kaspersky Security Networkiin.

Avaimen nykyinen tila näkyy **Käyttöoikeudet**-ikkunassa.

Voit kokeilla Kaspersky Security Network -yhteyttä seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta pääikkunan alaosassa olevaa **Asetukset**-linkkiä avataksesi **Asetukset**-ikkunan.
3. Valitse **Lisäasetukset**-osiossa **Palaute**-aliosio.

Ikkunassa näkyy Kaspersky Security Networkin yhteyden tila.

SOVELLUKSEN KÄYTTÖ KOMENTORIVILTÄ

Voit käyttää Kaspersky Total Securitya komentoriviltä.

Komentorivin rakenne:

```
avp.com <komento> [settings]
```

Voit katsoa ohjeita komentorivin rakenteesta kirjoittamalla seuraavan komennon:

```
avp.com [ /? | HELP ]
```

Tällä komennolla saat täydellisen luettelon komennoita, jotka ovat käytettävissä Kaspersky Total Securityn hallintaan komentoriviltä.

Jos haluat ohjeita tietyn komennon rakenteesta, voit antaa jonkin seuraavista komennoista:

```
avp.com <komento> /?
avp.com HELP <komento>
```

Komentorivillä voit viitata sovellukseen joko sen asennuskansiosta tai määrittämällä täydellisen polun avp.comiin.

YHTEYDENOTTO TEKNISEEN TUKEEN

Tämä osio sisältää tietoja siitä, miten voit saada teknistä tukea ja mitä se edellyttää.

TÄSSÄ OSIOSSA

MITEN TEKNISTÄ TUKEA SAADAAN

Jos et löydä ratkaisua ongelmaasi sovelluksen dokumentaatiosta tai jostakin sovellusta koskevasta tietolähteestä (ks. "Sovellusta koskevan tiedon lähteet" sivulla 12), suosittelemme ottamaan yhteyttä Kaspersky Labin tekniseen tukeen. Teknisen tuen asiantuntijat vastaavat kysymyksiisi, jotka liittyvät sovelluksen asennukseen ja käyttöön.

Ennen kuin otat yhteyttä tekniseen tukipalveluun, lue tukisäännöt (http://support.kaspersky.com/support/rules).

Voit ottaa yhteyttä tekniseen tukipalveluun seuraavasti:

- Puhelimitse. Tällä tavoin voit keskustella venäjänkielisen tai kansainvälisen teknisen tukipalvelumme asiantuntijoiden kanssa.
- Lähetä pyyntö My Kaspersky -portaalista. Tällä tavoin voit ottaa yhteyttä asiantuntijoihimme kyselylomakkeella.

Tekninen tuki on vain sovelluksen käyttöoikeuden ostaneiden käyttäjien käytettävissä. Kokeiluversion käyttäjille ei tarjota teknistä tukea.

TEKNINEN TUKI PUHELIMITSE

Hätätilanteessa voit soittaa venäjänkieliseen tai kansainväliseen tekniseen tukeen (http://support2.kaspersky.com/us/support/contacts) puhelimitse.

Ennen kuin otat yhteyttä tekniseen tukipalveluun, lue tukisäännöt (http://support.kaspersky.com/support/rules). Tämä auttaa asiantuntijoitamme auttamaan sinua nopeammin.

TEKNISEN TUEN SAAMINEN MY KASPERSKY -PORTAALISSA

My Kaspersky (https://my.kaspersky.com) on palvelu, jossa voit lähettää pyyntöjä tekniseen tukeen ja hallinnoida Kaspersky Lab -sovelluksien aktivointikoodeja.

Saat My Kaspersky -portaalin käyttöoikeuden rekisteröitymällä rekisteröintisivulla (https://my.kaspersky.com). Kirjaudu My Kaspersky -portaaliin antamalla sähköpostiosoitteesi ja salasanasi.

My Kaspersky -portaalissa voit suorittaa seuraavat toimenpiteet:

- Ottaa yhteyttä tukipalveluun ja viruslaboratorioon.
- Ottaa yhteyttä tekniseen tukipalveluun käyttämättä sähköpostia.
- Seurata pyyntösi tilaa reaaliajassa.
- Tarkastella yksityiskohtaisia historiatietoja tekniseen tukeen lähettämistäsi pyynnöistä.
- Saada kopion avaintiedostosta, jos se on kadonnut tai poistettu.

Tekninen tukipalvelu sähköpostitse

Voit lähettää pyynnön tekniseen tukipalveluun englanniksi, venäjäksi, saksaksi, ranskaksi tai espanjaksi.

Määritä verkon tukipyyntölomakkeeseen seuraavat tiedot:

- Pyynnön tyyppi
- Sovelluksen nimi ja versionumero
- Pyynnön kuvaus
- Asiakastunnus ja salasana
- Sähköpostiosoite

Teknisen tukipalvelun asiantuntija lähettää vastauksen kysymykseesi My Kaspersky -portaalin kautta sekä verkkopyynnössä määrittämääsi sähköpostiosoitteeseen.

Verkkopyyntö viruslaboratorioon

Tietyt pyynnöt tulee lähettää teknisen tukipalvelun sijaan Viruslaboratorioon.

Voit lähettää viruslaboratorioon epäilyttävien tiedostojen ja verkkoresurssien tutkimuspyyntöjä. Voit myös ottaa yhteyttä viruslaboratorioon, mikäli Kaspersky Total Security antaa vääriä hälytyksiä tiedostoista ja verkkoresursseista, joita et pidä vaarallisina.

TIEDON KERÄÄMINEN TEKNISTÄ TUKEA VARTEN

Kun ilmoitat teknisen tuen asiantuntijoille havaitusta ongelmasta, he saattavat pyytää sinua luomaan raportin, joka sisältää tietoa käyttöjärjestelmästäsi, ja lähettämään sen tekniseen tukeen. Teknisen tuen asiantuntijat voivat myös pyytää sinua luomaan jäljitystiedoston. Jäljitystiedoston avulla voit jäljittää sovellusten komentojen prosesseja vaihe kerrallaan ja tunnistaa sovelluksen toiminnan vaiheen, jossa virhe tapahtuu.

Kun teknisen tuen asiantuntijat ovat analysoineet lähettämäsi tiedot, he voivat luoda AVZ-komentosarjan ja lähettää sen sinulle. AVZ-komentosarjoja suorittamalla voit analysoida aktiivisia prosesseja haitallisen koodin varalta, tarkistaa järjestelmän haitallisen koodin varalta, poistaa tartunnan tai poistaa tartunnan saaneita tiedostoja sekä luoda raportteja järjestelmän tarkistuksesta.

Voidakseen tarjota parempaa tukea sovelluksen toimintaan liittyvissä ongelmissa teknisen tuen asiantuntijat voivat pyytää sinua muuttamaan tilapäisesti sovelluksen asetuksia samalla kun vianmääritystä tehdään. Tätä varten sinun voi olla tarpeen tehdä seuraavia toimia:

- Aktivoida laajennetun vianetsintätiedon kerääminen.
- Määrittää yksittäiset sovelluskomponentit muuttamalla erityisiä asetuksia, jotka eivät ole käytettävissä normaalin käyttöliittymän kautta.
- Määrittää kerätyn vianmääritystiedon tallennus ja lähettäminen uudelleen.
- Määrittää verkkoliikenteen kaappaus ja verkkoliikenteen tallennus tiedostoon.

Teknisen tuen asiantuntijat antavat sinulle kaikki tarvittavat tiedot näiden toimenpiteiden suorittamiseen (vaiheittaiset ohjeet, muutettavat asetukset, komentosarjat, komentorivin lisäominaisuudet, vianetsintämoduulit, erityisapuohjelmat jne.) ja ilmoittavat, mitä tietoa kerätään vianetsintätarkoituksiin. Kun laajennetut diagnostiikkatiedot on kerätty, ne tallennetaan käyttäjän tietokoneeseen. Kerättyjä tietoja ei lähetetä Kaspersky Labille automaattisesti.

Suosittelemme, että teet edellä kuvatut toimenpiteet vain teknisen tuen asiantuntijan valvonnassa ja saatuasi ohjeet niiden suorittamiseen. Jos muutat sovelluksen asetuksia itse tavoilla, joita ei ole kuvattu ylläpitäjän oppaassa tai joita teknisen tuen asiantuntijat eivät suosittele, seurauksena voi olla käyttöjärjestelmän hidastuminen ja kaatuminen, tietokoneen suojaustason aleneminen sekä käsitellyn tiedon saatavuuden ja eheyden vaurioituminen.

TÄSSÄ OSIOSSA

JÄRJESTELMÄN TILARAPORTIN LUOMINEN

Järjestelmän tilaraportin luominen:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Tuki**-linkkiä avataksesi **Tuki**-ikkunan.
3. Napsauta avautuvassa ikkunassa **Tukityökalut**-linkkiä.

   Tukityökalut-ikkuna avautuu.
4. Napsauta avautuvassa ikkunassa **Luo käyttöjärjestelmän tilaraportti** -linkkiä.

Järjestelmän tilaraportti luodaan HTML- ja XML-muodoissa ja tallennetaan sysinfo.zip-arkistoon. Voit tarkastella raporttia sen jälkeen, kun tiedot käyttöjärjestelmästä on kerätty.

Voit tarkastella raporttia seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Tuki**-linkkiä avataksesi **Tuki**-ikkunan.
3. Napsauta avautuvassa ikkunassa **Tukityökalut**-linkkiä.

   Tukityökalut-ikkuna avautuu.
4. Napsauta avautuvassa ikkunassa **Näytä raportti** -linkkiä.

   Microsoft Windowsin Resurssienhallinta-ikkuna avautuu.
5. Avaa avautuvasta ikkunasta arkisto, jonka nimi on sysinfo.zip. Se sisältää raporttitiedostot.

TIEDOSTOJEN LÄHETTÄMINEN

Kun olet luonut jälkitiedostot ja järjestelmän tilaraportin, ne on lähetettävä Kaspersky Labin teknisen tuen asiantuntijoille.

Datatiedostojen lataamiseksi teknisen tuen palvelimeen tarvitaan pyyntönumero. Tämä numero on saatavilla My Kaspersky -portaalista, kun lähettämäsi pyyntö on aktiivinen.

Voit ladata datatiedostoja teknisen tuen palvelimeen seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Tuki**-linkkiä avataksesi **Tuki**-ikkunan.
3. Napsauta avautuvassa ikkunassa **Tukityökalut**-linkkiä.

   Tukityökalut-ikkuna avautuu.
4. Napsauta avautuvassa ikkunassa **Lähetä raportti tekniseen tukeen** -linkkiä.

   Lähetä raportti -ikkuna avautuu.
5. Valitse valintaruudut niiden tietojen vieressä, jotka haluat lähettää tekniseen tukipalveluun.
6. Napsauta **Lähetä raportti** -painiketta.

Valitut datatiedostot pakataan ja lähetetään teknisen tuen palvelimeen.

Jos yhteyden ottaminen tekniseen tukeen ei jostakin syystä ole mahdollista, datatiedostoja voidaan säilyttää tietokoneessasi, jolloin ne voidaan lähettää myöhemmin My Kaspersky -portaalin kautta.

Voit tallentaa datatiedostoja levylle seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Tuki**-linkkiä avataksesi **Tuki**-ikkunan.
3. Napsauta avautuvassa ikkunassa **Tukityökalut**-linkkiä.
4. **Tukityökalut**-ikkuna avautuu.
5. Napsauta avautuvassa ikkunassa **Lähetä raportti tekniseen tukeen** -linkkiä.

   Lähetä raportti -ikkuna avautuu.
6. Valitse, millaisia tietoja haluat lähettää:

   - **Käyttöjärjestelmän tiedot**. Valitse tämä valintaruutu, jos haluat lähettää tekniselle tuelle tietoja tietokoneesi käyttöjärjestelmästä.
   - **Analyysia varten kerätyt tiedot**. Valitse tämä valintaruutu, jos haluat lähettää tekniselle tuelle sovelluksien toiminnan jälkiä sisältäviä jälkitiedostoja. Napsauta **<tiedostojen lukumäärä>, <tietomäärä>** -linkkiä, jolloin **Analyysia varten kerätyt tiedot** -ikkuna avautuu. Valitse lähetettäviä jälkitiedostoja vastapäätä olevat ruudut.
7. Napsauta **Tallenna raportti** -linkkiä.

   Näyttöön avautuu ikkuna arkiston tallennusta varten.
8. Määritä arkiston nimi ja vahvista tallennus.

Luotu arkisto voidaan lähettää tekniseen tukeen My Kaspersky -portaalin kautta.

JÄLKITIEDOSTOJEN SISÄLTÖ JA TALLENTAMINEN

Jälkitiedostoja säilytetään tietokoneella salatussa muodossa niin kauan, kun sovellus on käytössä. Kun sovellus poistetaan, jälkitiedostot poistetaan pysyvästi.

Jälkitiedostot tallennetaan kansioon ProgramData\Kaspersky Lab.

Jälkitiedostojen nimien muoto on seuraavanlainen: KAV<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1.

Kaikki jälkitiedostot sisältävät seuraavat yleiset tiedot:

- Tapahtuman ajankohta.
- Suoritussäikeen numero.
- Tapahtuman aiheuttanut sovelluskomponentti.
- Tapahtuman vakavuusaste (tietotapahtuma, varoitus, kriittinen tapahtuma, virhe).
- Tapahtuman kuvaus, joka liittyy sovelluskomponentin suorittamaan komentoon ja komennon suorittamisen lopputulokseen.

SRV.log-, GUI.log- ja ALL.log-jälkitiedostojen sisältö

SRV.log- ja GUI.log-jälkitiedostot saattavat sisältää seuraavia tietoja:

- Henkilötietoja kuten sukunimi, etunimi ja patronyymi, mikäli kyseiset tiedot sisältyvät tiedoston polkuun paikallisella tietokoneella.
- Käyttäjänimi ja salasana, jos niitä on siirretty avoimesti. Nämä tiedot saattavat tallentua jälkitiedostoihin Internet-liikenteen tarkistuksen aikana. Liikenne tallennetaan vain trafmon2.ppl:n jälkitiedostoihin.
- Käyttäjänimi, salasana ja evästeet, jos ne sisältyvät HTTP-ylätunnisteisiin.
- Microsoft Windows -tilin nimi, jos tilin nimi sisältyy tiedoston nimeen.
- Tilisi nimen ja salasanan sisältävä verkko-osoite tai sähköpostiosoitteesi, jos ne sisältyvät havaitun objektin nimeen.
- Käyttämäsi verkkosivustot sekä uudelleenohjaukset näiltä verkkosivustoilta. Tiedot tallennetaan jälkitiedostoihin, kun sovellus tarkistaa verkkosivustoja.
- Välityspalvelimen osoite, tietokoneen nimi, portti, IP-osoite ja käyttäjänimi, jolla kirjauduttiin sisään välityspalvelimelle. Nämä tiedot tallennetaan jälkitiedostoihin, jos sovellus käyttää välityspalvelinta.
- Etä-IP-osoitteet, joihin tietokoneesi on muodostanut yhteyden.
- Viestin aihe, tunniste, lähettäjän nimi ja viestin lähettäjän verkkosivun osoite yhteisöverkostossa. Nämä tiedot tallennetaan jälkitiedostoihin, jos Käytönvalvonta-komponentti on otettu käyttöön.
- Tietoja sovelluksen aktivoinnista, mihin voivat sisältyä nykyiset ja aiemmat aktivointikoodit, sovelluksen lokalisointitiedot, sovelluksen tai tuotteen tai muokkauksen tunnukset, sovellusversio, jokaisen sovelluksen asennuskerran yhteydessä luotu ainutlaatuinen tunnus, käyttäjän tietokoneen tunnus ja päivämäärä ja aika aktivointihetkellä (UTC).

HST.log-, BL.log- ja Dumpwriter.log-jälkitiedostojen sisältö

HST-jälkitiedosto sisältää tietokantojen ja sovellusmoduulien päivityksiin liittyviä tietoja.

BL-jälkitiedosto sisältää sovelluksen suorittamisen aikana tapahtuviin tapahtumiin liittyviä tietoja. Se sisältää myös tietoja, joita tarvitaan sovelluksen virheiden korjaamiseen. Tämä tiedosto luodaan, jos sovellus käynnistetään käyttämällä parametriä avp.exe –bl. BL-tiedosto voi sisältää tietoja sovelluksen aktivoinnista, mihin voivat sisältyä nykyiset ja aiemmat aktivointikoodit, sovelluksen lokalisointitiedot, sovelluksen tai tuotteen tai muokkauksen tunnukset, sovellusversio, jokaisen sovelluksen asennuskerran yhteydessä luotu ainutlaatuinen tunnus, käyttäjän tietokoneen tunnus ja päivämäärä ja aika aktivointihetkellä (UTC).

Dumpwriter.log-jälkitiedosto sisältää palvelutietoja, joita tarvitaan korjattaessa sovelluksen muistivedoksen kirjoittamisesta aiheutuvia virheitä.

Sovelluslaajennusten jälkitiedostojen sisältö

Sovelluslaajennusten jälkitiedostot sisältävät seuraavia tietoja:

- VirtualKeyboard (VKB.log) sisältää laajennuksen toimintaan liittyviä palvelutietoja. Se sisältää myös tietoja, joita tarvitaan korjattaessa laajennusten virheitä.
- Online Banking (OB.log) sisältää laajennusten toimintaan liittyviä palvelutietoja kuten verkkosivustojen tarkistustapahtumat ja tarkistustulokset, yhteydet etä-IP-osoitteisiin, välityspalvelimen asetukset ja evästeet. Tiedosto sisältää myös tietoja, joita tarvitaan laajennusvirheiden korjaamisessa.
- ContentBlocker (CB.log) sisältää laajennusten toimintaan liittyviä tietoja kuten verkko-osoitteiden tarkistustapahtumat ja tarkistustulokset, yhteydet etä-IP-osoitteisiin ja välityspalvelimen asetukset. Tiedosto sisältää myös tietoja, joita tarvitaan laajennusvirheiden korjaamisessa.
- Office Anti-Virus (OA.log) sisältää Microsoft Office -tiedostojen tarkistuksiin liittyviä tietoja. Tämä tiedosto voi myös sisältää tietoja tiedoston täydellisestä polusta tai verkkosivustosta, jolta tiedosto ladattiin.
- Jälkitiedosto laajennukselle, jota käytetään tarkistustehtävän käynnistämiseen pikavalikosta (shellex.dll.log). Sisältää tietoja tarkistustehtävien suorittamisesta sekä laajennusvirheiden korjaamiseen tarvittavia tietoja.
- Microsoft Outlook® -laajennuksen jälkitiedostot:
  - mcouas.OUTLOOK.EXE. Roskapostin esto -laajennus
  - mcou.OUTLOOK.EXE. Sähköpostin virustorjunta -laajennus.

  Tiedostot saattavat sisältää viestien osia, ja myös osoitteita.
- Jälkitiedosto laajennukselle, jota käytetään Google Chrome -laajennuksen rekisteröintiin (NativeMessagingHost.log). Sisältää laajennuksen toimintaan liittyviä palvelutietoja.

AVZ-KOMENTOSARJOJEN SUORITTAMINEN

On suositeltavaa, että et tee muutoksia Kaspersky Labin asiantuntijoilta saamasi AVZ-komentosarjan tekstiin. Jos komentosarjan suorituksen aikana ilmenee ongelmia ota yhteyttä tekniseen tukeen.

Voit suorittaa AVZ-komentosarjan seuraavasti:

1. Avaa sovelluksen pääikkuna.
2. Napsauta ikkunan alaosassa olevaa **Tuki**-linkkiä avataksesi **Tuki**-ikkunan.
3. Napsauta avautuvassa ikkunassa **Tukityökalut**-linkkiä.

   Tukityökalut-ikkuna avautuu.
4. Napsauta avautuvassa ikkunassa **Suorita komentosarja** -linkkiä.

   Suorita komentosarja -ikkuna avautuu.
5. Kopioi teksti komentosarjasta, jonka teknisen tuen asiantuntijat ovat lähettäneet, liitä se avautuvan ikkunan syötekenttään ja napsauta sitten **Suorita**-painiketta.

Komentosarja suoritetaan.

Jos komentosarjan suorittaminen onnistuu, ohjattu toiminto sulkeutuu automaattisesti. Jos komentosarjan suorituksen aikana tapahtuu virhe, ohjattu toiminto näyttää asianmukaisen viestin.

RAJOITUKSET JA VAROITUKSET

Kaspersky Total Securityllä on joitakin rajoituksia, jotka eivät ole kriittisiä sovelluksen toiminnan kannalta.

Sovelluksen päivittämistä uudempaan versioon koskevat rajoitukset

- Kun päivität aiemman Kaspersky Total Security -sovellusversion, seuraavat sovellusasetukset korvataan oletusasetuksilla: päivityslähteet, sallittujen URL-osoitteiden luettelo ja Kaspersky URL Advisor -asetukset.

- Kun uusi Kaspersky Total Security -versio asennetaan 2.0-versiota vanhemman Kaspersky PUREn päälle, tiedostojen varmuuskopiot ja karanteenissa olevat objektit katoavat: Niiden muotoa ei enää tueta, eikä niiden muuntaminen uuden sovellusversion käyttämään muotoon ole mahdollista. Kun Kaspersky PUREn versio 2.0 päivitetään, tiedostojen varmuuskopiot ja karanteenissa olevat objektit voidaan muuntaa uuteen muotoon. Kaspersky PURE 3.0 -sovellusversion käyttämää varmuuskopiotaltioiden muotoa tuetaan edelleen, eikä sitä tarvitse muuntaa uuteen muotoon.

Tiettyjä komponentteja ja tiedostojen automaattista käsittelyä koskevat rajoitukset

Virustartunnan saaneet tiedostot käsitellään automaattisesti Kaspersky Labin asiantuntijoiden määrittämien sääntöjen perusteella. Näitä sääntöjä ei voi muokata manuaalisesti. Sääntöjä voidaan päivittää tietokantapäivityksen ja sovellusmoduulien päivityksen yhteydessä. Myös Palomuurin, Sovelluksen hallinnan ja Luotetut sovellukset -tilan säännöt päivitetään automaattisesti.

Verkkosivustojen varmenteiden tarkistusta ja tiedostojen tarkistusta koskevat rajoitukset

Kun verkkosivuston varmenteita tai tiedostoja tarkistetaan, sovellus saattaa ottaa yhteyttä Kaspersky Security Networkiin tietojen noutamista varten. Jos tietojen noutaminen Kaspersky Security Networkista ei onnistu, sovellus määrittää paikallisten virustorjuntatietokantojen perusteella, onko tiedosto saanut tartunnan tai onko varmenne ei-luotettu.

Järjestelmän tarkkailu -toiminnon rajoitukset

Kryptausohjelmien (haittaohjelmat, jotka salakirjoittavat käyttäjän tiedostoja) estoa koskevat seuraavat rajoitukset:

- Toiminto hyödyntää tilapäisten tiedostojen säilyttämiseen käytettävää Temp-järjestelmäkansiota. Jos Temp-kansion sisältävällä järjestelmälevyllä ei ole riittävästi tallennustilaa väliaikaistiedostojen luomiseen, kryptausohjelmien esto ei ole käytössä. Tällaisessa tapauksessa sovellus ei näytä ilmoitusta siitä, että tiedostoja ei ole varmuuskopioitu (niitä ei ole suojattu).

- Tilapäiset tiedostot poistetaan automaattisesti, kun suljet Kaspersky Total Securityn tai poistat Järjestelmän tarkkailu -komponentin käytöstä.

- Jos Kaspersky Total Security suljetaan äkillisesti, väliaikaistiedostoja ei poisteta. Voit poistaa väliaikaiset tiedostot tyhjentämällä Temp-kansion manuaalisesti. Voit tehdä sen avaamalla **Suorita**-ikkunan (**Suorita** -komento Windows XP:ssä) ja kirjoittamalla **Avaa**-kenttään komennon %TEMP%. Napsauta **OK**.

Kerättyjä diagnostiikkatietoja koskeva varoitus

Teknistä tukea varten kerättävät, sovelluksen toimintaa koskevat diagnostiikkatiedot ovat keräämisen aikana salattuja. Voit tarvittaessa poistaa salauksen käytöstä.

Salatut yhteydet -toiminnon rajoitukset

Algoritmien tarkistuksen toteutukseen liittyvistä teknisistä rajoituksista johtuen salattujen yhteyden tarkistaminen ei tue tiettyjä TLS 1.0 -protokollan ja sen myöhempien versioiden laajennuksia (erityisesti NPN ja ALPN). Näitä protokollia käyttävät yhteydet voivat olla rajoitettuja. SPDY-protokollaa tukevat verkkoselaimet käyttävät HTTP over TLS (HTTPS) -protokollaa SPDY:n sijaan myös silloin, kun palvelin, johon yhteys muodostetaan tukee SPDY-protokollaa. Tämä ei vaikuta yhteyden tietoturvatasoon.

Roskapostin esto -komponentin toimintaa koskeva varoitus

Roskapostin eston toiminnallisuus voidaan määrittää muokkaamalla Roskapostin esto -komponentin asetustiedostoa.

Varmuuskopioinnin rajoitukset

Varmuuskopiointia koskevat seuraavat rajoitukset:

- Varmuuskopioiden säilyttäminen verkkotaltiossa poistuu käytöstä, kun kiintolevy tai tietokone vaihdetaan. Voit lukea tietoja verkkotaltioyhteyden palauttamisesta laitteiston vaihtamisen jälkeen Kaspersky Labin teknisen tuen verkkosivustolta.
- Verkkotaltion palvelutiedostojen muokkaaminen voi aiheuttaa verkkotaltion käyttöoikeuden menettämisen ja estää tietojen palauttamisen.

Tiedon suojaus -toiminnallisuuden rajoitukset

Kun turvasäilö luodaan FAT32-tiedostojärjestelmään, asemalla olevan turvasäilötiedoston koko saa olla enintään 4 Gt.

Suojattu selain -tilassa suoritettavien, rootkitien varalta tehtävien ydinmuistitarkistuksien erityispiirteitä

Kun ei-luotettu moduuli havaitaan Suojattu selain -tilassa, selaimeen avautuu uusi, haittaohjelmahavainnosta ilmoittava välilehti. Tässä tapauksessa on suositeltavaa sulkea selain ja suorittaa tietokoneen täydellinen tarkistus.

Leikepöydän tietojen suojauksen erityispiirteitä

Kaspersky Total Security sallii sovelluksien käyttää leikepöytää seuraavissa tapauksissa:

- Sovellus, jonka ikkuna on aktiivinen yrittää sijoittaa tietoja leikepöydälle. Aktiivinen ikkuna on kullakin hetkellä käytössäsi oleva ikkuna.
- Sovelluksen luotettu prosessi yrittää sijoittaa tietoja leikepöydälle.
- Sovelluksen luotettu prosessi tai prosessi, jonka ikkuna on aktiivinen yrittää vastaanottaa tietoja leikepöydältä.
- Sovellusprosessi, joka sijoitti aiemmin tietoja leikepöydälle, yrittää vastaanottaa kyseisiä tietoja leikepöydältä.

Kaspersky Lab -sovelluksien yhteensopivuutta koskeva varoitus

Kaspersky Total Security on yhteensopiva seuraavien Kaspersky Lab -sovelluksien kanssa:

- Kaspersky Fraud Prevention 2.0
- Kaspersky Fraud Prevention 2.5
- Kaspersky Fraud Prevention 3.0
- Kaspersky Fraud Prevention 3.5
- Kaspersky Password Manager 2.0
- Kaspersky Password Manager 5.0
- Kaspersky Password Manager 7.0

Sovelluskomponenttien suorittaman haitallisten objektien käsittelyn erikoispiirteitä

Oletusarvoisesti sovellus voi poistaa tiedostoja, joiden tartuntaa ei voida poistaa. Oletusarvoisen poiston voivat suorittaa tiedostojen käsittelyn yhteydessä komponentit kuten Sovellusten hallinta, Sähköpostin virustorjunta, Tiedostojen virustorjunta (tarkistustehtävän aikana) sekä Järjestelmän tarkkailu, jos se havaitsee haitallista sovellustoimintaa.

Tiettyihin komponentteihin kohdistuvat rajoitukset, kun sovellus asennetaan yhdessä Kaspersky Fraud Prevention for Endpointin kanssa

Seuraavien Kaspersky Total Securityn komponenttien toimintaa rajoitetaan Suojattu selain -tilassa, jos sovellus on asennettu yhdessä Kaspersky Fraud Prevention for Endpointin kanssa:

- Verkon virustorjunta (pois lukien Verkkohuijauksen esto)
- Käytönvalvonta
- Kaspersky URL Advisor
- Bannereiden esto

Kaspersky Total Security -ohjelmiston rajoitukset Microsoft Windows 10 -käyttöjärjestelmässä

Seuraava toiminto ei ole käytettävissä sovelluksessa, joka on asennettu Microsoft Windows 10 -käyttöjärjestelmään:

- Näyttökaappauksilta suojautuminen
- Leikepöydän tietojen suojaaminen
- Verkkokameran käytön suojaaminen
- Kehittynyt tartunnan poisto

Seuraavan sovellustoiminnon käyttöä on myös osittain rajoitettu Microsoft Windows 10 -käyttöjärjestelmässä:

- Sovelluksen käyttöliittymän itsepuolustus ei toimi, vaikka se olisikin otettu käyttöön.
- Järjestelmänvalvonta
- Suojaus kryptaus- ja näytön lukitusohjelmilta. Sovellus havaitsee vain kaikkein tavallisimmat kryptaus- ja näytön lukitusohjelmat.

Sovellusten hallinnan mukautussovellus ei toimi. Sovelluksen luokittelu uudessa Windows-käyttöliittymässä ei toimi oikein.

SANASTO

A

AKTIVOINTIKOODI

Koodi, jonka saat ostaessasi Kaspersky Total Securityn käyttöoikeuden. Tämä koodi tarvitaan sovelluksen aktivointiin.

Aktivointikoodi on uniikki merkkijono, joka koostuu kahdestakymmenestä aakkosnumeerisesta merkistä, ja se on muotoa xxxxx-xxxxx-xxxxx-xxxxx.

D

DIGITAALINEN ALLEKIRJOITUS

Asiakirjaan tai sovellukseen upotettu, salattu data. Digitaalista allekirjoitusta käytetään asiakirjan tai sovelluksen tekijän varmentamiseen. Digitaalisen allekirjoituksen luominen edellyttää, että asiakirjan tai sovelluksen tekijällä on digitaalinen varmenne, joka todistaa tekijän henkilöllisyyden.

Digitaalisen allekirjoituksen avulla voit varmentaa tiedonlähteen ja tiedon eheyden sekä suojata itsesi väärennöksiltä.

H

HAITALLISTEN VERKKO-OSOITTEIDEN TIETOKANTA

Luettelo verkko-osoitteista, joiden sisältöä voidaan pitää mahdollisesti vaarallisena. Luettelo on Kaspersky Labin asiantuntijoiden luoma. Sitä päivitetään säännöllisesti, ja se sisältyy Kaspersky Lab -sovelluspakettiin.

HEIKKOUS

Käyttöjärjestelmässä tai sovelluksessa oleva vika, jota haittaohjelmien tekijät voivat hyödyntää päästäkseen sisään käyttöjärjestelmään tai sovellukseen ja rikkoakseen sen eheyden. Jos käyttöjärjestelmässä esiintyy paljon heikkouksia, se on epäluotettava, sillä käyttöjärjestelmään murtautuvat virukset voivat haitata käyttöjärjestelmän ja asennettujen sovellusten toimintaa.

HEURISTINEN ANALYSOIJA

Teknologia, jota käytetään tunnistamaan uhkia, joiden tietoja ei ole vielä lisätty Kaspersky Labin tietokantoihin. Heuristinen analysoija havaitsee objektit, joiden toiminta käyttöjärjestelmässä voi aiheuttaa tietoturvauhan. Heuristisen analysoijan havaitsemat objektit ovat todennäköisesti saaneet tartunnan. Objektia voidaan esimerkiksi pitää todennäköisesti tartunnan saaneena, jos se sisältää komentojonoja, jotka ovat tyypillisiä haitallisille objekteille (avaa tiedosto, kirjoita tiedostoon).

HYPERVISOR

Sovellus, joka tukee useiden käyttöjärjestelmien rinnakkaista käyttöä samalla tietokoneella.

I

ICHECKER-TEKNIIKKA

Tekniikka, joka lisää virustarkistusten nopeutta jättämällä pois objektit, jotka eivät ole muuttuneet edellisen tarkistuksen jälkeen, olettaen, että tarkistuksen parametrit (tietokannat ja asetukset) eivät ole muuttuneet. Jokaisen tiedoston tiedot tallennetaan erityiseen tietokantaan. Tätä tekniikkaa käytetään sekä reaaliaikaisessa suojauksessa että tarvittaessa tehtävissä tarkistuksissa.

Oletetaan esimerkiksi, että Kaspersky Lab -sovellus tarkistaa arkiston ja antaa sille tilan ei tartuntaa. Seuraavalla kerralla sovellus ohittaa tämän arkiston, jos sitä ei ole muutettu tai jos tarkistuksen asetuksia ei ole vaihdettu. Jos muutit arkiston sisältöä lisäämällä siihen uuden objektin, muokkasit tarkistuksen asetuksia tai päivitit sovelluksen tietokannat, arkisto tarkistetaan uudelleen.

iChecker-tekniikan rajoitukset:

- Tekniikka ei toimi suurten tiedostojen kanssa, sillä on nopeampaa tarkistaa tiedosto kuin tarkistaa, onko sitä muokattu edellisen tarkistuksen jälkeen.
- Tekniikka tukee rajallista määrää tiedostomuotoja.

J

JÄLJET

Sovelluksen suoritus virheenkorjaustilassa; kunkin komennon suorituksen jälkeen sovellus pysäytetään ja ko. vaiheen tulos näytetään.

K

KARANTEENI

Erillinen tallennussijainti, johon sovellus tallentaa tartunnan poiston aikana muutettujen tai poistettujen tiedostojen varmuuskopiot. Tiedostoista tallennetaan kopiot erityisessä tallennusmuodossa, joka ei uhkaa tietokonetta.

KASPERSKY LAB -PÄIVITYSPALVELIMET

Kaspersky Labin HTTP-palvelimet, joilta tietokantojen ja sovellusmoduulien päivitykset ladataan.

KASPERSKY SECURITY NETWORK (KSN)

Verkkopalveluinfrastruktuuri, joka tarjoaa pääsyn Kaspersky Labin verkkotietopankkiin. Se sisältää tietoa tiedostojen, verkkoresurssien ja ohjelmistojen maineesta. Kaspersky Security Networkin tuottaman tiedon ansiosta Kaspersky Internet Security voi tarjota suojaa tuntemattomilta uhkilta nopeammin, minkä lisäksi verkosto parantaa määrättyjen suojauskomponenttien tehoa ja vähentää väärien hälytysten riskiä.

KÄYNNISTYSOBJEKTIT

Ohjelmat, jotka tarvitaan käyttöjärjestelmän ja tietokoneeseen asennetun ohjelmiston käynnistykseen ja oikeaan toimintaan. Nämä objektit suoritetaan aina käyttöjärjestelmän käynnistyksen yhteydessä. Tietyt virukset voivat tartuttaa erityisesti automaattisesti käynnistyviä objekteja, mikä voi johtaa esim. siihen, ettet voi käyttää käyttöjärjestelmää.

KÄYTTÖOIKEUSAIKA

Ajanjakso, jonka sisällä voit käyttää sovelluksen toimintoja ja lisäpalveluja.

KOMENTOSARJA

Pieni tietokoneohjelma tai itsenäinen ohjelman (toiminnon) osa, joka on yleensä kehitetty tiettyä tehtävää varten. Käytetään useimmiten hypertekstiin upotetuissa ohjelmissa. Komentosarjoja suoritetaan esimerkiksi silloin, kun avaat määrättyjä verkkosivustoja.

Jos reaaliaikainen suojaus on käytössä, sovellus seuraa komentosarjojen suoritusta, keskeyttää ne ja tarkistaa ne virusten varalta. Riippuen tarkistuksen tuloksista voit estää tai sallia komentosarjan suorituksen.

L

LEVYN KÄYNNISTYSLOHKO

Käynnistyslohko on erityinen alue tietokoneen kiintolevyllä, levykkeellä tai muulla tallennusvälineellä. Se sisältää tietoa levyn tiedostojärjestelmästä sekä latausohjelman, joka vastaa käyttöjärjestelmän käynnistämisestä.

Useat virukset tarttuvat käynnistyslohkoon ja niitä kutsutaan siksi käynnistysviruksiksi. Kaspersky Lab -sovelluksella voidaan tarkistaa käynnistyslohkot virusten varalta ja poistaa virustartunta, jos sellainen löydetään.

LIIKENTEEN TARKISTUS

Reaaliaikainen tarkistus, joka käyttää uusimpien (voimassaolevien) tietokantaversioiden tietoja kaikkien protokollien (esim. HTTP, FTP) kautta siirretyille objekteille.

LUOTETTU PROSESSI

Sovellusprosessi, jonka tiedostotoimenpiteitä Kaspersky Lab -sovellus ei rajoita reaaliaikaisessa suojaustilassa. Kun luotetun prosessin toiminnassa havaitaan epäilyttäviä piirteitä, Kaspersky Total Security poistaa sen luotettujen prosessien luettelosta ja estää sen toiminnan.

LUOTTAMUSRYHMÄ

Ryhmä, johon Kaspersky Total Security sijoittaa sovelluksen tai prosessin seuraavien ehtojen mukaan: digitaalisen allekirjoituksen olemassaolo, maine Kaspersky Security Network -verkostossa, sovelluslähteen luottamustaso ja sovelluksen tai prosessin suorittamien toimintojen potentiaalinen vaarallisuus. Kaspersky Total Security voi rajoittaa sovelluksen käyttöjärjestelmässä suorittamia toimenpiteitä sovelluksen luottamusryhmästä riippuen.

Kaspersky Total Securityssä sovellukset kuuluvat johonkin seuraavista luottamusryhmistä: Luotettu, Vähän rajoitettu, Paljon rajoitettu tai Ei-luotettu.

N

NÄPPÄINPAINALLUSTEN TALLENTAJA

Ohjelma, joka on suunniteltu tallentamaan piilotettuun lokiin käyttäjän näppäinpainallukset. Näppäinpainallusten tallentajat sieppaavat näppäinten painallukset.

O

OBJEKTIN ESTÄMINEN

Ulkoisten sovellusten pääsyn estäminen objektiin. Estettyä objektia ei voi lukea, suorittaa, muokata tai poistaa.

P

PAKATTU TIEDOSTO

Arkisto, joka sisältää purkuohjelman sekä ohjeet sen suoritukseen käyttöjärjestelmälle.

PÄIVITYS

Menettely, jossa korvataan tai lisätään uusia tiedostoja (tietokantoja tai sovellusmoduuleja), jotka on haettu Kaspersky Labin päivityspalvelimilta.

PÄIVITYSPAKETTI

Tiedostopaketti tietokantojen ja sovellusmoduulien päivittämiseen. Kaspersky Lab -sovellus kopioi päivityspaketit Kaspersky Labin päivityspalvelimilta, ja asentaa ja käyttää niitä automaattisesti.

PROTOKOLLA

Tarkasti määritetty ja standardisoitu sääntövalikoima, joka ohjaa vuorovaikutusta asiakkaan ja palvelimen välillä. Tunnettuja protokollia ja niihin liittyviä palveluita ovat HTTP, FTP ja NNTP.

R

ROOTKIT

Ohjelma tai ohjelmavalikoima, joka on kehitetty piilottamaan tunkeutujan tai haittaohjelmiston jäljet käyttöjärjestelmässä.

Windows-pohjaisissa käyttöjärjestelmissä rootkit tarkoittaa yleensä ohjelmaa, joka tunkeutuu käyttöjärjestelmään ja kaappaa järjestelmän toimintoja (Windowsin API:t). Kaappaamalla ja muokkaamalla alhaisen tason API-toimintoja sovellukset voivat piiloutua huomaamattomasti käyttöjärjestelmään. Tavallisesti rootkit myös peittää kiintolevylle tallennettujen tiedostojen, kansioiden ja prosessien olemassaolon sekä rekisteriavaimet, jos sellaisia on kuvattu rootkitin asetuksissa. Monet rootkitit asentavat käyttöjärjestelmään omia ajureita ja palveluita (ne ovat myös "näkymättömiä").

ROSKAPOSTI

Ei toivottuja massapostituksia, jotka useimmiten sisältävät mainoksia.

S

SOVELLUKSEN AKTIVOINTI

Sovelluksen kytkeminen täyden toiminnallisuuden tilaan. Käyttäjä voi suorittaa aktivoinnin sovelluksen asennuksen aikana tai sen jälkeen. Aktivointi vaatii, että käyttäjällä on käytössään aktivointikoodi.

SOVELLUSMODUULIT

Kaspersky Lab -asennuspaketissa olevat tiedostot, joilla sovelluksen tärkeimpiä tehtäviä suoritetaan. Kukin sovellusmoduuli vastaa yhtä sovelluksen tehtävätyyppiä (suojaus, tarkistus, tietokantojen ja sovellusmoduulien päivitys).

SUOJATTU SELAIN

Vakioselaimen erityinen toimintatila, joka on suunniteltu raha-asioiden ja ostosten hoitamiseen verkossa. Suojatun selaimen käyttö varmistaa pankkien ja maksujärjestelmien verkkosivustoille syötettyjen luottamuksellisten tietojen (kuten pankkikorttien numero tai salasanat, joita tarvitaan verkkopankkeihin kirjautuessa) turvallisuuden. Se myös estää omaisuuden varastamisen verkossa tapahtuvien rahasiirtojen yhteydessä. Vakioselain, jolla sivusto yritettiin avata, näyttää suojatun selaimen käynnistystä koskevan viestin.

SUOJAUSKOMPONENTIT

Kaspersky Total Securityn toiminnan kannalta keskeisiä osia, jotka on suunniteltu suojaamaan tietyntyyppisiltä uhkilta (esimerkiksi Roskapostin esto, Verkkohuijauksen esto). Jokainen komponenteista on suhteellisen itsenäinen, joten ne voidaan poistaa käytöstä tai niiden asetuksia voidaan muokata yksitellen.

T

TARTUNNAN SAANUT OBJEKTI

Objekti, jonka koodista osa vastaa täysin tunnetun haittaohjelman koodia. Kaspersky Lab ei suosittele tällaisten objektien käyttöä.

TEHTÄVÄ

Kaspersky Lab -sovelluksen toiminnot toteutetaan tehtävinä, kuten Täydellinen tarkistus -tehtävä tai päivitystehtävä.

TEHTÄVÄN ASETUKSET

Tehtävätyyppikohtaiset sovellusasetukset.

TIEDOSTOPEITE

Tiedoston nimen esittäminen jokerimerkein. Tiedostopeitteissä käytetyt yleiset jokerimerkit ovat * ja ?, jossa * korvaa minkä tahansa määrän merkkejä ja ? yhden merkin.

TIETOJEN KALASTELU

Internet-petoksen tyyppi, jossa pyritään saamaan luvattomasti käyttöön käyttäjän luottamuksellista tietoa.

TIETOJENKALASTELUOSOITTEIDEN TIETOKANTA

Luettelo verkko-osoitteista, jotka Kaspersky Labin asiantuntijat ovat määrittäneet verkkohuijausosoitteiksi. Tietokantoja päivitetään säännöllisesti, ja ne ovat osa Kaspersky Lab -sovelluspakettia.

TIETOTURVATASO

Tietoturvataso määritetään sovelluskomponenttikohtaisesti valmiiksi määritetyllä asetusjoukolla.

TODENNÄKÖINEN ROSKAPOSTI

Viesti, jota ei voida yksiselitteisesti pitää roskapostina, mutta joka sisältää useita roskapostin piirteitä (esim. tietyn tyyppiset postitukset ja mainostusviestit).

TODENNÄKÖISESTI TARTUNNAN SAANUT OBJEKTI

Objekti, jonka koodissa on osia tunnetun uhkan muokatusta koodista, tai objekti, joka muistuttaa käytökseltään tunnettua uhkaa.

TUNTEMATON VIRUS

Uusi virus, josta ei ole tietoa tietokannoissa. Yleensä sovellus tunnistaa objekteissa olevat tuntemattomat virukset heuristisen analysoijan avulla. Nämä objektit luokitellaan todennäköisesti tartunnan saaneiksi.

TURVASÄILÖ

Turvasäilö on erityinen taltio, jossa tiedostot säilytetään salatussa muodossa. Tiedostojen käyttö vaatii salasanan. Turvasäilöjen tarkoitus on estää käyttäjätietojen luvaton käyttö.

U

UHKATASO

Indeksi, joka osoittaa sovelluksen käyttöjärjestelmälle muodostaman uhkan todennäköisyyden. Heuristinen analyysi laskee uhkatason perustuen kahteen erityyppiseen ehtoon:

- Staattiset (kuten tiedot sovelluksen käynnistystiedostosta: koko, luontipäivä jne.)
- Dynaamiset, joita käytetään simuloitaessa sovelluksen toimintaa virtuaalisessa ympäristössä (analyysi sovelluksen kutsuista järjestelmätoimintoihin)

Uhkatason avulla voidaan havaita haittaohjelmalle tyypillinen käytös. Mitä matalampi uhkataso on, sitä useampia toimia sovellus saa tehdä käyttöjärjestelmässä.

V

VÄÄRÄ HÄLYTYS

Tilanne, jossa Kaspersky Lab -sovellus pitää puhdasta objektia tartunnan saaneena, koska sen koodi muistuttaa viruksen koodia.

VARMUUSKOPIOINTI JA TIETOJEN PALAUTUS

Luo varmuuskopioita tietokoneelle tallennetuista tiedoista. Varmuuskopioiden avulla estetään tietojen katoaminen varkauden, laitevian tai hakkerien hyökkäyksen johdosta.

VIRUS

Ohjelma, joka tartuttaa muita ohjelmia lisäämällä niihin omaa koodiansa tarkoituksena kaapata hallinta, kun tartunnan saaneita tiedostoja suoritetaan. Tämän yksinkertaisen määritelmän avulla voidaan tunnistaa minkä tahansa viruksen suorittama päätoimenpide: tartuttaminen.

VIRUSTORJUNTATIETOKANNAT

Tietokannat, jotka sisältävät tietoja Kaspersky Labin tuntemista tietoturvauhista virustietokantojen julkaisuhetkellä. Virustietokannoissa olevien tietueiden avulla voidaan havaita haittakoodi tarkistetuissa objekteissa. Virustorjuntatietokannat ovat Kaspersky Labin asiantuntijoiden luomia ja ne päivitetään tunnin välein.

Y

YHTEENSOPIMATON SOVELLUS

Ulkopuolisen kehittäjän virustorjuntasovellus tai Kaspersky Lab -sovellus, jota ei voi hallita Kaspersky Total Securityn kautta.

KASPERSKY LAB ZAO

Kaspersky Lab on saanut kansainvälistä tunnustusta tarjoamastaan suojasta viruksia, haittaohjelmia, roskapostia, verkko- ja hakkerihyökkäyksiä sekä muita uhkia vastaan.

Vuonna 2008 Kaspersky Lab arvioitiin maailman neljän johtavan loppukäyttäjien tietoturvaratkaisuja toimittavan yrityksen joukkoon (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab on venäläisten kotikäyttäjien ensisijainen tietokoneen turvajärjestelmien toimittaja (lähde: COMCON-tutkimus "TGI-Russia 2009").

Kaspersky Lab perustettiin vuonna 1997. Nykyisin Kaspersky Lab on kansainvälinen konserni, jonka pääkonttori on Moskovassa. Sen viisi alueellista divisioonaa hallinnoivat yhtiön toimintaa Venäjällä, Länsi- ja Itä-Euroopassa, Lähi-idässä, Afrikassa, Etelä- ja Pohjois-Amerikassa, Japanissa, Kiinassa ja muissa Tyynenmeren Aasian maissa. Yhtiö työllistää yli 2 000 pätevää asiantuntijaa.

TUOTTEET. Kaspersky Labin tuotteet suojaavat kaikkia järjestelmiä kotitietokoneista suuriin yritysverkkoihin.

Yksityiskäyttöön tarkoitettuihin tuotteisiin sisältyy virustorjuntasovelluksia kaikille nykypäivän digitaalisessa elämässä käytetyille laitteille kotitietokoneista kannettaviin tietokoneisiin, älypuhelimiin, tabletteihin ja muihin mobiililaitteisiin.

Kaspersky Lab toimittaa sovelluksia ja palveluita suojaamaan työasemia, tiedosto- ja verkkopalvelimia, postiyhdyskäytäviä sekä palomuureja. Yhdessä Kaspersky Labin keskitetyn hallintajärjestelmän kanssa käytettyinä nämä ratkaisut varmistavat yrityksille ja organisaatioille tehokkaan, automaattisen suojan tietokoneuhkia vastaan. Kaspersky Labin tuotteet ovat suurten koelaboratorioiden varmentamia, yhteensopivia monien toimittajien ohjelmistojen kanssa ja optimoituja toimimaan monilla laitteistoalustoilla.

Kaspersky Labin virusanalyytikot työskentelevät kellon ympäri. He löytävät joka päivä sadoittain uusia tietokoneuhkia, luovat työkaluja niiden havaitsemiseen ja tartunnan poistoon ja sisällyttävät ne Kaspersky Lab -sovellusten käyttämiin tietokantoihin. *Kaspersky Labin virustorjuntatietokanta päivitetään kerran tunnissa ja Roskapostin eston tietokanta päivitetään joka viides minuutti.*

TEKNIIKAT. Kaspersky Lab on alun perin kehittänyt useita tekniikoita, jotka ovat nykyisin modernien virustorjuntaohjelmistojen vakio-ominaisuuksia. Esimerkiksi tämän takia monet ulkoiset ohjelmistokehittäjät ovat päättäneet käyttää Kasperskyn virustorjuntamoottoria omissa sovelluksissaan. Tällaisia yrityksiä ovat mm. Safenet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Iso-Britannia), Communigate Systems (USA), Openwave Messaging (Irlanti), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (Ranska), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Monet yhtiön innovatiivisista tekniikoista on patentoitu.

SAAVUTUKSET. Vuosien varrella Kaspersky Lab on voittanut satoja palkintoja työstään tietokoneuhkien torjumiseksi. Esimerkiksi vuonna 2010 Kaspersky Anti-Virus palkittiin usealla korkean tason Advanced+ -palkinnolla arvostetun itävaltalaisen AV-Comparatives-virustorjuntalaboratorion testeissä. Mutta Kaspersky Labin tärkein saavutus on kuitenkin käyttäjien uskollisuus. Yhtiön tuotteet ja tekniikat suojaavat yli 300 miljoonaa käyttäjää ja sillä on yli 200 000 yritysasiakasta.

Kaspersky Labin verkkosivusto:	http://www.kaspersky.fi
Virus Encyclopedia:	http://www.securelist.com
Virus Lab:	newvirus@kaspersky.com (vain todennäköisesti tartunnan saaneiden tiedostojen lähettämiseen arkistomuodossa)
Kaspersky Lab -verkkofoorumi:	http://forum.kaspersky.com/

TIETOJA KOLMANNEN OSAPUOLEN KOODISTA

Tiedot kolmannen osapuolen koodista on tallennettu sovelluksen asennuskansioon tiedostoon legal_notices.txt.

TAVARAMERKKI-ILMOITUKSET

Rekisteröidyt tavaramerkit ja palvelumerkit ovat niiden omistajiensa omaisuutta.

Dropbox on Dropbox, Inc:n tavaramerkki.

Google, Google Chrome ja YouTube ovat Google, Inc:n tavaramerkkejä.

Intel, Celeron ja Atom ovat Intel Corporationin tavaramerkkejä Yhdysvalloissa ja/tai muissa maissa.

Internet Explorer, Microsoft, Windows, Bing, Outlook ja Windows Vista ovat Microsoft Corporationin rekisteröityjä tavaramerkkejä Yhdysvalloissa ja muissa maissa.

Mozilla, Firefox ovat Mozilla Foundationin tavaramerkkejä.

Skype on Skypen tavaramerkki.

VMware on VMware, Inc:n tavaramerkki, tai VMware, Inc:n Yhdysvalloissa tai muilla alueilla rekisteröimä tavaramerkki.

Mail.ru on Mail.ru LLC:n tavaramerkki.

HAKEMISTO

P

R

S

T

V

Y