F-Secure Anti-Virus 2013

Sisukord

Peatükk1: Installimine.....5

Enne esmakordset installimist.....6
Toote esimene installimine.....6
Rakenduste installimine ja uuendamine.....6
Abi ja tugi.....7

Peatükk2: Alustamine.....9

Kuidas kasutada automaatvärskendusi?.....10
Värskenduste oleku kontrollimine.....10
Internetiühenduse sätete muutmine.....10
Kontrollige funktsiooni Real-time Protection Network olekut.....11
Kuidas näha, mida toode on teinud?.....11
Kuva teadete ajalugu.....11
Muuda teavitamise sätteid.....11
Real-time Protection Network.....12
Mida kujutab endast Reaalajas toimiv kaitsevõrk?.....12
Reaalajas toimiva kaitsevõrgu eelised.....12
Milliseid andmeid te panustate?.....13
Kuidas me kaitseme teie privaatsust?.....14
Reaalajas kaitsevõrgustikku panustajaks saamine.....14
Küsimused Reaalajas toimiva kaitsevõrgu kohta.....14
Kuidas ma tean, kas minu tellimus kehtib?.....15
Tegevuskeskus.....15
Tellimuse aktiveerimine.....15

Peatükk3: Tutvustus.....17

Kaitse üldise oleku vaatamine.....18
Toote statistika kuvamine.....18
Tootevärskenduste käsitsemine.....19
Kuva andmebaasi versioonid.....19
Mobiilse lairibaühenduse sätete muutmine.....19
Mis on viirused ja muu õelvara?.....20
Viirused.....20
Nuhkvara.....20
Rootkitid.....21
Riskvara.....21

Peatükk4: Arvuti kaitsmine õelvara vastu.....23
Arvuti skannimine.....24
Failide skannimine automaatselt.....24
Failide käsitsi skannimine.....26
Meilide skannimine.....29
Skannimistulemuste kuvamine.....29
Failide välistamine skannimisest.....30
Failitüüpide välja arvamine.....30
Jäta välja faile asukoha alusel.....30
Välja jäetud rakenduste kuvamine.....31
Kuidas kasutada karantiini?.....32
Karantiinis üksuste kuvamine.....32
Karantiinis üksuste taastamine.....32
Mis on DeepGuard?.....33
DeepGuardi sisse- või väljalülitamine.....33
DeepGuardi blokeeritud rakenduste lubamine.....33
Kasutage DeepGuardi ühilduvusrežiimis.....34
Mida teha hoiatustega kahtlase käitumise kohta?.....34

Peatükk

1

Installimine

Teemad:

- *Enne esmakordset installimist*
- *Toote esimene installimine*
- *Rakenduste installimine ja uuendamine*
- *Abi ja tugi*

Enne esmakordset installimist

Täname, et valisite F-Secure'i.

Toote installimiseks vajate järgmist.

- Installi-CD või installi pakett. Kui kasutate CD-lugejata minisülearvutit, saate installipaketi alla laadida aadressilt *www.f-secure.com/netbook*.
- Teie registreerimisvõti.
- Interneti-ühendus.

Kui kasutate teise tarnija toodet, proovib installer seda automaatselt eemaldada. Kui see ei õnnestub eemaldage see käsitsi.

Märkus: Kui teil on arvutis rohkem kui üks konto, logige installimiseks sisse administraatorina.

Toote esimene installimine

Juhised toote installimiseks.

Järgige toote installimiseks järgmisi juhiseid.

1. Sisestage CD või topeltklõpsake allalaaditud installeril.

   Kui CD automaatselt ei käivitu , minge Windows Explorerisse, topeltklõpsake CD-ROMi ikoonil ja topeltklõpsake installimise käivitamiseks installifailil.

2. Järgige ekraanil olevaid juhiseid.

   - Kui soetasite toote CD-l kauplusest, leiate tellimuskoodi kiirinstallimise juhendi kaanelt.
   - Kui laadisite toote alla F-Secure'i e-poest, leiate tellimuskoodi ostutellimuse kinnitavast meilisõnumist.

   Enne registreerimise kinnitamist ja uusimate värskenduste allalaadimist Internetist võib arvuti vajada taaskäivitamist. Kui installite CD-lt, ärge unustage enne arvuti taaskäivitamist eemaldada installi-CDd.

Rakenduste installimine ja uuendamine

Juhised uue tellimuse aktiveerimiseks.

Uue tellimuse aktiveerimiseks või uue rakenduse installimiseks valimisklahvistiku abil järgige neid juhiseid.

Märkus: Valimisklahvistiku ikooni leiate Windowsi süsteemisalvest.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Avaneb hüpikmenüü.
2. Tehke valik **Kuva minu tellimused**
3. Valikus **Minu tellimused** minge lehele **Registreerimise olek** ja klõpsake käsul **Aktiveeri tellimus**.
   Avaneb aken **Aktiveeri tellimus**.
4. Sisestage rakenduse registreerimisvõti ja klõpsake **OK**.
5. Kui registreerimine on kinnitatud ja tellimus aktiveeritud, klõpsake käsul **Sulge**.
6. Valikus **Minu tellimused** minge lehele **Installi olek**. Kui install automaatselt ei käivitu, järgige neid juhiseid.
   a) Klõpsake käsul **Installi**.

Avaneb installi aken.

b) Klõpsake **Järgmine**.
Rakendus laaditakse alla ja installimine algab.

c) Kui installimine on lõpetatud, klõpsake käsul **Sulge**.

Uus tellimus on aktiveeritud.

Abi ja tugi

Toote veebiabisse pääsete, klõpsatesikoonil Abi või vajutades klahvi F1 toote mis tahes kuval olles.

Pärast litsentsi registreerimist on teil õigus saada täiendavaid teenuseid, nagu tasuta toote allalaadimised ja toote tugi. Registreerida saate lehel *www.f-secure.com/register*.

Peatükk

2

Alustamine

Teemad:

- *Kuidas kasutada automaatvärskendusi?*
- *Kuidas näha, mida toode on teinud?*
- *Real-time Protection Network*
- *Kuidas ma tean, kas minu tellimus kehtib?*

Teave toote kasutamise alustamise kohta.

See jaotis kirjeldab, kuidas muuta üldsätteid ja hallata oma tellimusi käivitusriba kaudu.

Käivitusriba üldsätted on sätted, mis kohalduvad kõigile käivitusribale installitud programmidele. Iga programmi sätete eraldi muutmise asemel saate lihtsalt muuta üldsätteid, mida seejärel kasutatakse kõigi installitud programmide puhul.

Käivitusriba üldsätete hulka kuuluvad järgmised sätted.

- Allalaadimised, kus saate vaadata teavet allalaaditud värskenduste kohta ja saate käsitsi kontrollida, kas on saadaval uusi värskendusi.
- Ühenduse sätted, kus saate muuta seda, kuidas arvuti loob Interneti-ühenduse.
- Teated, kus saate vaadata varasemaid teateid ja seada, milliseid teateid soovite näha.
- Privaatsussätted, kus saate valida, kas teie arvutil on või pole luba luua ühendus kaitsevõrguga reaalajas.

Samuti saate käivitusriba kaudu hallata oma installitud programmide tellimusi.

Kuidas kasutada automaatvärskendusi?

Automaatvärskendused tagavad teie arvutile ajakohase kaitse.

Näete flaieriteavitust, kui uued värskendused on saadaval. Kui te ei soovi kohe värskendust alla laadida, ei pea te midagi tegema. Saate värskenduse alla laadida pärast järgmist taaskäivitamist või kui uus värskendus on saadaval.

Värskenduste oleku kontrollimine

Saate vaadata viimase värskendamise kuupäeva ja kellaaega.

Kui automaatvärskendused on aktiveeritud, laadib tarkvara internetiühenduse olemasolul viimased värskendused alla automaatselt.

Kontrollimaks, kas arvutis on viimased värskendused, toimige järgmiselt.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Ava üldsätted**.
3. Valige **Automaatsed värskendused** > **Allalaadimised**.
4. Klõpsake **Kontrolli nüüd**.
   Tarkvara kontrollib internetiühenduse abil uute värskenduste olemasolu. Kui kaitse pole ajakohane, toob rakendus serverist uusimad värskendused.

   Märkus: Kui kasutate Internetti pääsemiseks modemit või ISDN-ühendust, peab see ühendus värskenduste otsimiseks olema aktiivne.

Internetiühenduse sätete muutmine

Tavaliselt pole vaikesätteid muuta tarvis, kuid saate konfigureerida serveri Interneti-ühenduse variandi, et saaksite värskendused automaatselt.

Internetiühenduse sätete muutmiseks toimige järgmiselt.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Ava üldsätted**.
3. Valige **Automaatsed värskendused** > **Ühendus**.
4. Loendis **Interneti-ühendus** valige arvutile Interneti-ühenduse loomise viis.
   - Märkige ruut **Eelda püsiühendust** juhul, kui arvuti kasutab Interneti püsiühendust.

     Märkus: Kui teie arvutil pole tegelikult Interneti püsiühendust, vaid hoopis sissehelistusühendus, võidakse ruudu **Eelda püsiühendust** märkimisel luua mitu sissehelistusühendust.
   - Märkige ruut **Tuvasta ühendus**, et tuua värskendusi vaid siis, kui toode on tuvastanud aktiivse võrguühenduse.
   - Märkige ruut **Tuvasta liiklus**, et tuua värskendusi vaid siis, kui toode on tuvastanud muu võrguliikluse.

     Nõuanne: Kui teie arvutil on ebatavaline riistvarakonfiguratsioon, mille korral säte **Tuvasta ühendus** tuvastab aktiivse võrguühenduse ka siis, kui seda tegelikult pole, valige hoopis **Tuvasta liiklus**.
5. **HTTP-puhverserveris** loendit ja valige, kas teie arvuti kasutab *puhverserverit* Interneti-ühenduse loomiseks või mitte.

- Kui teie arvuti on Internetti ühendatu otse, valige **Mitte HTTP-puhverserver**.
- Valige suvand **Konfigureeri HTTP-puhverserver käsitsi**, konfigureerimaks *HTTP-puhverserveri* sätteid.
- Valige **Kasuta minu brauseri HTTP-puhverserverit**, kui soovite kasutada samu *HTTP-puhverserveri* sätteid, mis te olete konfigureerinud veebibrauseris.

Kontrollige funktsiooni Real-time Protection Network olekut

Korralikult toimimiseks sõltuvad paljud tooted funktsiooni Real-time Protection Network ühenduvusest.

Kui esineb võrguühenduse probleeme või kui teie tulemüür blokeerib reaalajas toimiv kaitsevõrk liikluse, siis on olekuks „ühendus katkestatud“. Kui pole installitud ühtegi toote funktsiooni, mis vajavad juurdepääsu reaalajas toimiv kaitsevõrku, on olekuks „pole kasutusel“.

Oleku kontrollimiseks tehke järgmist.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Ava üldsätted**.
3. Valige **Automaatsed värskendused** > **Ühendus**.

Reaalajas toimivas kaitsevõrgus olles saate vaadata reaalajas toimiva kaitsevõrgu praegust olekut.

Kuidas näha, mida toode on teinud?

Lehel **Teated** saate vaadata, milliseid toiminguid on toode teinud teie arvuti kaitsmiseks.

Toode kuvab toimingu sooritamisel teate, nt leides viiruse, mille ta blokeerib. Mõned teated võib saata ka teie teenusepakkuja, nt teavet uute saadaolevate teenuste kohta.

Kuva teadete ajalugu

Saate vaadata, millised teated on teadete ajaloos kuvatud

Teadete ajaloo kuvamiseks tehke järgmist.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Ava üldsätted**.
3. Valige **Muu** > **Teated**.
4. Klõpsake **Kuva teadete ajalugu**.
   Avaneb teadete ajaloo loend.

Muuda teavitamise sätteid

Saate valida, mis tüüpi teateid soovite, et toode kuvaks.

Teavitamise sätete muutmiseks tehke järgmist.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Ava üldsätted**.
3. Valige **Muu** > **Teated**.
4. Valige või loobuge valikust **Luba programmi sõnumid**, et lülitada programmi sõnumid sisse või välja.

Kui säte on aktiivne, kuvab toode installitud programmide teated.

5. Valige või loobuge valikust **Luba reklaamisõnumid**, et lülitada reklaamisõnumid sisse või välja.
6. Klõpsake **OK**.

Real-time Protection Network

Käesolev dokument kirjeldab Reaalajas toimivat kaitsevõrku, F-Secure Corporationi võrguteenust, mis tuvastab puhtaid rakendusi ja veebisaite, pakkudes samal ajal kaitset ründevara ja veebisaitide vallutuste vastu.

Mida kujutab endast Reaalajas toimiv kaitsevõrk?

Reaalajas toimiv kaitsevõrk on võrguteenus, mis tagab kiire reageerimise uusimate Interneti-põhiste ohtude korral.

Reaalajas kaitsevõrgustikku panustajana saate aidata meil tugevdada kaitset uute esilekerkivate ohtude vastu. Reaalajas kaitsevõrgustik kogub statistilisi andmeid teatud tundmatute, ründavate või kahtlaste rakenduste ja nende tegevuse kohta teie arvutis. See teave on anonüümne ja saadetakse F-Secure Corporationile kombineeritud andmete analüüsimiseks. Analüüsitud teavet kasutame teie arvuti turvalisuse parandamiseks uusimate ohtude ja ründefailide vastu.

Kuidas Reaalajas toimiv kaitsevõrk töötab?

Reaalajas kaitsevõrgustikku panustajana saate anda teavet tundmatute rakenduste ja veebisaitide, samuti ründerakenduste ja vallutuste kohta veebisaitidel, mida on juba analüüsitud, ning see ei kogu teavet teie arvutisse installitud puhaste rakenduste kohta.

Kui te selliseid andmeid ei soovi edastada, ei kogu Reaalajas kaitsevõrgustik installitud rakenduste ja külastatavate veebisaitide kohta. Toode peab siiski esitama päringu F-Secure'i serveritele rakenduste, veebisaitide, sõnumite jm maine kohta. Päring tehakse kasutades krüptograafilist kontrollsummat, kus päringuobjekti ennast F-Secure'ile ei saadeta. Me ei jälita andmeid kasutajapõhiselt, vaid ainult siis, kui faili või veebisaidi külastusloenduri näit kasvab.

Kogu võrguliiklust Reaalajas toimivasse kaitsevõrku pole võimalik peatada, kuna see on lahutamatu osa toote pakutavast kaitsest.

Reaalajas toimiva kaitsevõrgu eelised

Reaalajas toimiv kaitsevõrk annab teile kiirema ja täpsema kaitse uusimate ohtude vastu ning te ei saa mittevajalikke kahtlaste rakenduste kohta, mis ei ole pahatahtlikud.

Reaalajas kaitsevõrgustikku panustajana saate meil aidata avastada uut ja tuvastamata ründevara ning eemaldada võimalikud valepositiivsed tulemused meie viirusmääratluste andmebaasist.

Kõik Reaalajas toimiva kaitsevõrku kasutajad aitavad üksteist. Kui Reaalajas toimiv kaitsevõrk leiab teie seadmest kahtlase rakenduse, on teil kasu analüüsitulemustest, mis on juba tehtud sellesama rakenduse teistest seadmetest leidmise järel. Reaalajas toimiv kaitsevõrk parandab teie seadme üldist toimivust, sest kui Reaalajas toimiv kaitsevõrk on rakendust juba analüüsinud ja leidnud selle puhta olevat ei pea installitud turbetoode seda enam skannima. Samuti jagatakse Reaalajas toimiva kaitsevõrku kaudu teavet pahatahtlike veebisaitide ja soovimatute hulgisõnumite kohta ning me suudame tagada teile täpsema kaitse veebisaitide vallutuste ja rämpsposti vastu.

Mida rohkem inimesi panustab reaalajas kaitsevõrgustikku, seda paremini on individuaalsed kasutajad kaitstud.

Milliseid andmeid te panustate?

Reaalajas kaitsevõrgustikku panustajana annate teavet rakenduste kohta, mis on teie seadmes talletatud, ja veebisaitide kohta, mida külastate, et reaalajas kaitsevõrgustik saaks pakkuda kaitset uusimate ründerakenduste ja kahtlaste veebisaitide vastu.

Faili maine analüüsimine

Reaalajas toimiv kaitsevõrk kogub teavet ainult rakenduste kohta, mille maine pole teada ja failide kohta, mis on kahtlased ja millest on teada, et tegemist on ründevaraga.

Reaalajas toimiva kaitsevõrk kogub anonüümset teavet teie seadme puhaste ja kahtlaste rakenduste kohta. Reaalajas toimiva kaitsevõrk kogub teavet ainult täitmisfailide kohta (nt Windowsi platvormi Portable Executable failid, millel on faililaiendid cpl, exe, dll, ocx, sys, scr ja drv).

Kogutud teabe hulka kuulub:

- Faili tee, kohta, kus rakendus seadmes asub.
- Faili suurus ja selle loomise ja muutmise aeg.
- faili atribuudid ja õigused,
- Faili signatuuri teave.
- Faili praegune versioon ja selle loonud ettevõte.
- Faili päritolu või selle allalaadimise URL.
- F-Secure DeepGuard ja skannitud failide viirusetõrje analüüsi tulemused ning
- Muu sarnane teave.

Reaalajas toimiva kaitsevõrk ei kogu kunagi teavet teie isiklike dokumentide kohta, v.a kui neis tuvastatakse nakkus. Kõikide pahatahtlike failide puhul kogub rakendus nakkuse nime ja faili nakkuse eemaldamise oleku.

Reaalajas toimiva kaitsevõrguga saate esitada analüüsimiseks ka kahtlased rakendused. Teie esitatud rakendused hõlmavad ainult kaasaskantavaid täitefaile. Reaalajas toimiv kaitsevõrk ei kogu kunagi mingit teavet teie isiklike dokumentide kohta ja neid ei laadita analüüsimiseks kunagi automaatselt üles.

Failide esitamine analüüsimiseks

Reaalajas kaitsevõrgustikuga saate ka esitada kahtlasi rakendusi analüüsimiseks.

Üksikuid kahtlasi rakendusi saate esitada käsitsi, kui toode teile seda võimalust pakub. Esitada saate ainult Portable Executable tüüpi faile. Reaalajas kaitsevõrgustik ei laadi kunagi kunagi üles isiklikke dokumente.

Veebisaidi maine analüüsimine

Real-time Protection Network ei jälita teie veebitoiminguid ega kogu teavet veebisaitide kohta, mida on juba analüüsitud. Rakendus kontrollib teie veebi sirvimise ajal, kas külastatud veebisaidid on turvalised. Kui külastate veebisaiti, kontrollib Real-time Protection Network selle turvalisust ja teavitab teid, kui saiti hinnatakse kahtlaseks või kahjulikuks.

Kui külastatav veebisait sisaldab pahatahtlikku või kahtlast sisu või teadaolevat vallutust, kogub Real-time Protection Network saidi tervikliku URL-i nii, et selle veebisaidi sisu saab analüüsida.

Kui külastate saiti, mida pole veel hinnatud, KOGUB Real-time Protection Network domeeni ja alamdomeenide nimed ning teatud juhtudel tee külastatud lehele, et saiti saaks analüüsida ja hinnata. Kõik URL-i parameetrid, mis võivad sisaldada teavet, mida saab teiega seostada isiklikult tuvastavas vormingus, eemaldatakse teie privaatsuse kaitsmise eesmärgil.

Märkus: Real-time Protection Network ei hinda ega analüüsi privaatvõrgu veebilehti, seega ei kogu see kunagi mingit teavet privaatvõrkude IP-aadresside kohta (nt ettevõttesiseste võrkude kohta).

Süsteemiteabe analüüsimine

Real-time Protection Network kogub teie operatsioonisüsteemi nime ja versiooni, teabe Interneti-ühenduse ja Real-time Protection Networki kasutusstatistika kohta (nt veebisaidi maine kohta tehtud päringute arvu ja päringule vastuse saamise keskmise aja kohta), et saaksime teenust jälgida ja parandada.

Kuidas me kaitseme teie privaatsust?

Edastame teabe turvaliselt ja eemaldame automaatselt kõik isikuandmed, mida andmed võivad sisaldada.

Reaalajas kaitsevõrgustik eemaldab tuvastusandmed enne nende saatmist F-Secure'ile ja krüpteerib edastamiseks kogu kogutud teabe, et kaitsta seda volitamata juurdepääsu eest. Kogutud teavet ei töödelda individuaalselt; see rühmitatakse teabega teistelt reaalajas kaitsevõrgustikku andmete edastajatelt. Kõik andmed analüüsitakse statistiliselt ja anonüümselt, mis tähendab, et teiega ei seostata mingeid andmeid ühelgi viisil.

Mingit teave, mille järgi saaks teid isiklikult tuvastada, ei ole kogutud andmetesse kaasatud. Reaalajas toimiv kaitsevõrk ei kogu privaatseid IP-aadresse ega teie isiklikke andmeid nagu e-posti aadressid, kasutajanimed ja paroolid. Ehkki teeme kõikmõeldavaid jõupingutusi kõigi isikuandmete eemaldamiseks, võib juhtuda, et kogutud teabesse jäävad mõned tuvastusandmed. Sellisel juhul ei proovi me selliseid tahtmatult kogutud andmeid kasutada teie tuvastamiseks.

Rakendame rangeid turvameetmeid ning füüsilisi, administratiivseid ja tehnilisi turbevahendeid, et kaitsta kogutud andmeid edastamise, talletamise ja töötlemise ajal. Teave talletatakse meie kontrolli all olevatesse turvapaikadesse ja serveritesse, mis asuvad meie või meie alltöövõtjate kontorites. Kogutud teabele on juurdepääs ainult volitatud isikutel.

F-Secure võib kogutud teavet jagada oma filiaalide, alltöövõtjate, edasimüüjate ja partneritega, kuid ainult mitte-tuvastatavas vormingus.

Reaalajas kaitsevõrgustikku panustajaks saamine

Aitate meil parandada Reaalajas toimiva kaitsevõrku kaitset, andes teavet pahatahtlike programmide ja veebisaitide kohta.

Reaalajas kaitsevõrgustikku panustajaks võite otsustada saada installimise ajal. Installi vaikeseadete alusel panustate te reaalajas kaitsevõrgustikku. Saate selle seadistuse hiljem tootes muuta.

Reaalajas kaitsevõrgustiku seadete muutmiseks järgige neid juhiseid.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Ava üldsätted**.
3. Valige **Muu** > **Privaatsus**.
4. Reaalajas kaitsevõrgustikku panustajaks saamiseks märkige osalusruut.

Küsimused Reaalajas toimiva kaitsevõrgu kohta

Kontaktteave Reaalajas toimiva kaitsevõrgu kohta küsimuste esitamiseks.

Kui teil on täiendavaid küsimusi Reaalajas toimiva kaitsevõrgu kohta, võtke ühendust järgmisel aadressil:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

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

Meie veebisaidil on alati saadaval nende põhimõtete uusim versioon.

Kuidas ma tean, kas minu tellimus kehtib?

Teie tellimuse tüüp ja olek kuvatakse lehel **Tellimuse olek**.

Kui teie tellimus hakkab aeguma või on juba aegunud, siis vastaval käivitusriba ikoonil olev programmi kaitseolek muutub.

Tellimuse kehtivuse kontrollimiseks tehke järgmist.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Kuva minu tellimused**.
3. Valige **Tellimuse olek**, et vaadata teavet oma installitud programmide tellimuste kohta.
4. Valige **Installi olek**, et näha, millised programmid on installimiseks saadaval.

Teie tellimuse olek ja aegumiskuupäev kuvatakse ka programmi **Statistika** lehel. Kui teie tellimus on aegunud, peate toote kasutamiseks ja värskenduste saamise jätkumiseks oma tellimuse uuendama.

Märkus: Kui tellimuse kehtivus on lõppenud, hakkab toote olekuikoon süsteemisalves vilkuma.

Tegevuskeskus

Tegevuskeskuses näidatakse kõiki tähtsaid teatisi, mis vajavad teie tähelepanu.

Kui teie tellimus on aegunud või hakkab aeguma, siis teavitab tegevuskeskus teid sellest. Tegevuskeskuse sõnumi taustavärv ja sisu sõltuvad teie tellimuse tüübist ja olekust.

- Kui tellimus hakkab aeguma ja saadaval on tasuta tellimusi, on sõnumi taust valge ja sellel on nupp **Aktiveeri**.
- Kui tellimus hakkab aeguma ja tasuta tellimusi saadaval pole, on sõnumi taust kollaneja sellel on nupud **Osta** ja **Sisesta võti**. Kui olete uue tellimuse juba ostnud, saate registreerimisvõtme sisestamiseks klõpsata käsul **Sisesta võti** ja uue tellimuse aktiveerida.
- Kui tellimus on aegunud jasaadaval on tasuta tellimusi, on sõnumi taust punane ja sellel on nupp **Aktiveeri**.
- Kui tellimus on aegunud ja tasuta tellimusi saadaval pole, on sõnumi taust punane ja sellel on nupud **Osta** ja **Sisesta võti**. Kui olete uue tellimuse juba ostnud, saate registreerimisvõtme sisestamiseks klõpsata käsul **Sisesta võti** ja uue tellimuse aktiveerida.

Märkus: Link **Näita teavituste ajalugu** tegevuskeskuses kuvab toote teavitussõnumite, mitte tegevuskeskuse varasemate sõnumite loendi.

Tellimuse aktiveerimine

Kui teil on toote jaoks uus tellimusvõti või kampaaniakood, tuleb see aktiveerida.

Tellimuse aktiveerimiseks tehke järgmist.

1. Paremklõpsake käivitusklahvistikul kõige parempoolsemal ikoonil.
   Ilmub hüpikmenüü.
2. Valige **Kuva minu tellimused**.
3. Võimalik on toimida kahel viisil.

- Klõpsake käsul **Aktiveeri tellimus**.
- Klõpsake käsul **Aktiveeri kampaaniakood**.

4. Sisestage avanenud dialoogiboksi oma uus tellimuse võti või kampaaniakood ja klõpsake **OK**.

> **Nõuanne:** Kui saate tellimuskoodi meili teel, kopeerige kood meilisõnumist ja kleepige see vastavale väljale.

Pärast uue tellimusvõtme sisestamist kuvatakse lehel **Tellimuse olek** uue tellimuse kehtivuskuupäev.

Peatükk

3

Tutvustus

Teemad:

- *Kaitse üldise oleku vaatamine*
- *Toote statistika kuvamine*
- *Tootevärskenduste käsitsemine*
- *Mis on viirused ja muu õelvara?*

Toode kaitseb teie arvutit viiruste ja muude kahjulike rakenduste vastu.

Toode skannib faile, analüüsib rakendusi ja teeb automaatseid värskendusi. Te ei pea ise midagi tegema.

Kaitse üldise oleku vaatamine

Lehel **Olek** kuvatakse installitud toote funktsioonide lühiülevaade ja nende hetke olek.

Lehe **Olek** avamine.

Klõpsake pealehe suvandil **Olek**.

Avaneb leht **Olek**.

Ikoonil kuvatakse programmi olek ja selle turbefunktsioonid.

Olekuikoon	Oleku nimi	Kirjeldus
	OK	Teie arvuti on kaitstud. Funktsioon on sisse lülitatud ja töötab korrektselt.
	Teave	Toode teavitab teid funktsiooni erilisest olekust. Näiteks: funktsiooni värskendatakse.
	Hoiatus	Teie arvuti pole täielikult kaitstud. Näiteks: toodet pole kaua aega värskendatud või vajab funktsiooni olek tähelepanu.
	Tõrge	Teie arvuti pole kaitstud. Näiteks: teie tellimus on aegunud või on oluline funktsioon välja lülitatud.
	Väljas	Ebaoluline funktsioon on välja lülitatud.

Toote statistika kuvamine

Lehel **Statistika** saate näha, mida toode alates installimisest teinud on.

Lehe **Statistika** avamine

Klõpsake pealehe suvandil **Statistika**.

Avaneb leht **Statistika**.

- Suvandil **Viimane edukas värskenduskontroll** kuvatakse viimase värskenduse kellaaeg.
- Suvandil **Viiruse ja nuhkvara skannimine** kuvatakse installimisest alates skannitud ja puhastatud failide arv.
- **Rakendused** näitavad, mitu programmi on DeepGuard pärast installimist lubanud või blokeerinud.
- **Tulemüüri ühendused** näitab lubatud ja blokeeritud ühenduste arvu installimisest saadik.

- **Rämpsposti ja andmepüügi filtreerimine** näitab, mitu meilisõnumit on toode tuvastanud kehtiva meilisõnumi ja rämpsposti sõnumina.

Tootevärskenduste käsitsemine

Toode värskendab kaitset automaatselt.

Kuva andmebaasi versioonid

Lehel **Andmebaasi värskendused** näete viimaste värskenduste aegu ja versiooni numbreid.

Lehe **Andmebaasi värskendused** avamiseks tehke järgmist.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Muud sätted** > **Andmebaasi versioonid**.

Lehel **Andmebaasi versioonid** kuvatakse viimane kuupäev, millal värskendati viiruste ja nuhkvara määratlusi, DeepGuardi ning rämpsposti ja andmepüügi filtreerimist ja nende versiooninumbreid.

Mobiilse lairibaühenduse sätete muutmine

Valige, kas soovite mobiilse lairibaühenduse kasutamise ajal turvavärskendusi alla laadida.

Märkus: See funktsioon on saadaval ainult operatsioonisüsteemis Microsoft Windows 7.

Vaikimisi laaditakse turvavärskendused alla, kui olete koduses operaatorivõrgus. Värskendused aga peatatakse, kui satute teise operaatorivõrku. Selle põhjuseks on võimalikud hinnaerinevused erinevate operaatorite vahel, nt erinevates riikides. Võite kaaluda selle sätte muutmata jätmist, kui soovite külastuse ajal säilitada ribalaiust ja võib-olla ka hinda.

Märkus: See säte kehtib ainult mobiilsete lairibaühenduste puhul. Kui arvuti on ühendatud fiks- või traadita võrku, värskendatakse toodet automaatselt.

Sätete muutmiseks tehke järgmist.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Muud sätted** > **Mobiil-lairiba** > **Laadi alla turvavärskendused**.
3. Valige värskendus, mida mobiilsete ühenduste puhul eelistate:
   - **Ainult minu koduses operaatorivõrgus**

     Värskendused laaditakse alati alla teie koduses operaatorivõrgus. Kui viibite teise operaatori võrgus, siis värskendused peatatakse. Soovitame seda valikut, et hoida oma turvatoode ajakohane kindla hinna eest.
   - **Mitte kunagi**

     Värskendusi ei laadita alla, kui kasutate mobiil-lairiba.
   - **Alati**

     Värskendused laaditakse alla alati, olenemata sellest, millist võrku kasutate. Tehke see valik, kui soovite olla kindel, et teie arvuti turvalisus on hinnast olenemata alati ajakohane.

4. Kui soovite operaatori võrgu iga kord kodust väljudes uuesti valida, tehke valik **Küsi alati, kui lahkun kodusest operaatorivõrgust**.

Peatatud turvavärskendused

Turvavärskendused võib peatada, kui kasutate väljaspool kodust operaatorivõrku mobiilset lairibaühendust.

Sellisel juhul näete teavitusflaierit **Peatatud** ekraani alumises paremas nurgas. Värskendused peatatakse, kuna operaatoritel, nt erinevates riikides, on erinevad ühenduste hinnad. Võite jätta selle seade muutmata, kui soovite külastuse jooksul säilitada ribalaiuse ja võimalik, et ka hinna. Kui te siiski soovite seadeid muuta, klõpsake lingil **Muuda**.

Märkus:

See funktsioon on saadaval ainult operatsioonisüsteemis Microsoft Windows 7.

Mis on viirused ja muu õelvara?

Õelvara on programmid, mis on loodud teie arvutit kahjustama, seda teie teadmata illegaalsel otstarbel kasutama või teie arvutist teavet varastama.

Õelvara võib:

- võtta teie veebibrauseri enda kontrolli alla;
- suunata ümber teie otsingukatsed;
- näidata soovimatut reklaami;
- jälgida, milliseid veebisaite külastate;
- varastada isiklikke andmeid (nt teie pangateavet);
- kasutada teie arvutit rämpsposti saatmiseks ja
- kasutada teie arvutit teiste arvutite ründamiseks.

Õelvaraprogrammid võivad muuta teie arvuti töö aeglaseks ja ebastabiilseks. Teil on alust kahtlustada, et teie arvutis leidub *õelvara*, kui arvuti muutub ootamatult väga aeglaseks ja jookseb sageli kokku.

Viirused

Viirus on enamasti programm, mis võib end kinnitada teiste failide külge ja end korduvalt paljundada. Viirused võivad teiste failide sisu muuta ja asendada viisil, mis võib teie arvutit kahjustada.

Viirus on programm, mis installitakse teie arvutisse tavaliselt teie teadmata. Installitud viirus proovib end paljundada. Viirus:

- kasutab osa teie arvuti süsteemiressurssidest;
- võib muuta või kahjustada teie arvutis leiduvaid faile;
- proovib arvatavasti kasutada teie arvutit teiste arvutite nakatamiseks;
- võib lubada teie arvuti kasutamist ebaseaduslikuks otstarbeks.

Nuhkvara

Nuhkvaraks nimetatakse programme, mis koguvad teie isiklikku teavet.

Nuhkvara võib koguda näiteks järgmist teavet:

- Interneti-saidid, mida olete sirvinud,
- teie arvutis leiduvad meiliaadressid,
- paroolid või
- krediitkaardinumbrid.

Nuhkvara installitakse peaaegu alati ilma teie selgesõnalise loata. Nuhkvara võidakse installida koos kasuliku programmiga või meelitades teid klõpsama teatud valikule eksitavas hüpikaknas.

Rootkitid

Rootkitid on programmid, mis muudavad muu *õelvara* raskesti ülesleitavaks.

Rootkitid peidavad faile ja protsesse. Üldjuhul teevad nad seda teie arvutis toimuva pahatahtliku tegevuse peitmiseks. Kui rootkit *õelvara* peidab, pole lihtne kindlaks teha, et teie arvutis leidub õelvara.

See toode sisaldab rootkitikontrolli funktsiooni, mis otsib arvutist just rootkitte, et *õelvara* poleks lihtne peita.

Riskvara

Riskvara ei ole konkreetselt loodud teie arvutit kahjustama, kuid valel kasutamisel võib seda siiski teha.

Riskvara ei ole lihtsalt õelvara. Riskvara täidab kasulikke, kuid vahel ka ohtlikke funktsioone.

Riskvara programmide näited on:

- sõnumsideprogrammid (nt IRC, jututoad),
- failide Interneti kaudu ühest arvutist teise edastamiseks mõeldud programmid
- või Interneti-telefoniprogrammid (VoIP (*IP-kõne (Voice over Internet Protocol)*).
- Kaugjuurdepääsu tarkvara, nt VNC,
- Petuvara, mis võib inimesi hirmutada või petta võltsturbetarkvara soetama.
- tarkvara, mis on loodud vältima CD-kontrolle või kopeerimise kaitseid.

Kui olete programmi teadlikult ise installinud ja õigesti seadistanud, ei pruugi see olla ohtlik.

Kui aga riskvara on installitud teie teadmata, on see tõenäoliselt installitud pahatahtlikul otstarbel ja tuleks eemaldada.

Peatükk

4

Arvuti kaitsmine õelvara vastu

Teemad:

- *Arvuti skannimine*
- *Failide välistamine skannimisest*
- *Kuidas kasutada karantiini?*
- *Mis on DeepGuard?*

Viiruse- ja nuhkvaratõrje kaitseb teie arvutit programmide eest, mis võivad varastada isiklikku teavet, arvutit kahjustada või seda illegaalsetel eesmärkidel kasutada.

Vaikimisi tegeletakse kõigi ründevara tüüpidega nende leidmisel, nii et need ei saa kahju tekitada.

Vaikimisi skannib viiruse- ja nuhkvaratõrje teie kohalikke kõvakettaid, mis tahes eemaldatavaid meediume (nt kaasaskantavaid draive või CD-sid) ja allalaaditud sisu automaatselt. Samuti saate seada selle automaatselt skannima meilisõnumeid.

Viiruste ja nuhkvara skannimine jälgib ka igasuguseid muutusi teie arvutis, mis võivad viidata *ründevarale*. Mis tahes ohtlike süsteemimuudatuste puhul, nt süsteemiseadete või tähtsate süsteemiprotsesside muudatuste leidmisel peatab DeepGuard sellise programmi käitamise, sest see võib suure tõenäosusega olla *ründevara*.

Arvuti skannimine

Kui viiruste ja nuhkvara skannimine on sisse lülitatud, skannib see teie arvutit kahjulike failide osas automaatselt. Samuti saate faile käsitsi skannida ja seada plaanilised skannimised.

Soovitame viiruste ja nuhkvara skannimise kogu aeg sees hoida. Skannige oma faile käsitsi, kui soovite kindlaks teha, et teie arvutis pole kahjulikke faile või kui soovite skannida faile, mille olete reaalajas skannimisest välistanud.

Kui olete seadistanud plaanilise skannimise, eemaldab viiruste ja nuhkvara skannimine kahjulikud failid teie arvutist määratud aegadel.

Failide skannimine automaatselt

Reaalajas skannimine kaitseb teie arvutit, skannides kõiki faile nende avamisel ja blokeerides juurdepääsu neile failidele, mis sisaldavad *õelvara*.

Kui arvuti proovib failile ligi pääseda, skannib reaalajas skannimine faili ründevara osas enne, kui lubab teie arvutile juurdepääsu sellele failile. Kui reaalajas skannimine leiab kahjulikku sisu, paneb see faili karantiini, enne kui see saab kahju tekitada.

Kas reaalajas skannimine mõjutab arvuti jõudlust?

Enamasti ei pane te kontrolliprotsessi tähelegi, kuna see kulutab üsna vähe aega ja süsteemiressursse. See, kui palju aega ja süsteemiressursse reaalajas skannimine nõuab, sõltub näiteks faili sisust, asukohast ja tüübist.

Failid, mille kontrollimine võtab rohkem aega:

- Teisaldatavatel andmekandjatel (nt CD, DVD, teisaldatav USB-draiv) olevad failid.
- tihendatud failid, näiteks *.zip* failid.

  Märkus: Tihendatud faile vaikimisi ei skannita.

Reaalajas saknnimine võib teie arvuti tööd aeglustada, kui:

- teil on arvuti, mis ei vasta süsteeminõuetele või
- proovite pääseda paljude failide juurde samaaegselt. Näiteks kui avate kataloogi, mis sisaldab palju faile, mis vajavad skannimist.

Reaalajas skannimise sisselülitamine

Hoidke reaalajas skannimine sees, et peatada *ründevara* enne, kui see jõuab teie arvutit kahjustada.

Reaalajas skannimise sisse- või väljalülitamiseks tehke järgmist.

1. Klõpsake pealehe suvandil **Olek**.
2. Klõpsake **Muuda sellel lehel olevaid seadeid**.

   Märkus: Turvafunktsioonide väljalülitamiseks vajate administraatori õigusi.

3. **Viiruste ja nuhkvara skannimise** sisse- või väljalülitamine.
4. Klõpsake **Sulge**.

Kahjulike failide automaatne käsitsemine

Reaalajas skannimine käsitseb kahjulikke faile automaatselt, küsimusi esitamata.

Reaalajas skannimisel kahjulike failide automaatse käsitsemise lubamiseks tehke järgmist.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Arvuti turvalisus** > **Viiruste ja nuhkvara skannimine**.
3. Valige käsk **Käsitse kahjulikke faile automaatselt**.

Kui otsustate kahjulikke faile automaatselt mitte käsitseda, küsib reaalajas skannimine kahjuliku faili leidmise korral, mida soovite sellega teha.

Nuhkvara käsitsemine

Viiruste ja nuhkvara skannimine blokeerib nuhkvara kohe kui see proovib käivituda.

Enne kui nuhkvara rakendus saab käivituda, blokeerib toode selle ja laseb teil otsustada, mida soovite sellega teha.

Nuhkvara leidmisel valige üks järgnevatest toimingutest.

Ettevõetav tegevus	Mis juhtub nuhkvaraga?
Automaatne tegutsemine	Laske tootel leitud nuhkvara põhjal otsustada, milline on parim toiming.
Nuhkvara karantiini panemine	Teisaldage nuhkvara karantiini, kus see ei saa teie arvutit kahjustada.
Kustutage nuhkvara.	Eemaldage kõik nuhkvaraga seotud failid oma arvutist.
Ainult nuhkvara blokeerimine	Blokeerige juurdepääs nuhkvarale, kuid jätke see arvutisse alles.
Nuhkvara skannimisest välistamine	Lubage nuhkvaral töötada ja välistage see edaspidisest skannimisest.

Riskvara käsitsemine

Viiruste ja nuhkvara skannimine blokeerib riskvara kohe kui see proovib tööle hakata.

Enne kui riskvararakendus saab käivituda, blokeerib toode toode selle ja laseb teil otsustada, mida soovite sellega teha.

Riskvara leidmisel valige üks alltoodud toimingutest.

Ettevõetav tegevus	Mis juhtub riskvaraga?
Ainult riskvara blokeerimine	Blokeerige juurdepääs riskvarale, kuid jätke see arvutisse alles.
Riskvara karantiini panemine	Teisaldage riskvara karantiini, kus see ei saa teie arvutit kahjustada.
Riskvara kustutamine	Eemaldage kõik riskvaraga seotud failid arvutist.
Riskvara skannimisest välistamine	Lubage riskvaral töötada ja välistage see edaspidisest skannimisest.

Jälgimisküpsiste automaatne eemaldamine

Jälgimisküpsiste eemaldamisega peatate veebisaitide võimaluse jälgida saite, mida Internetis külastate.

Jälgimisküpsised on väiksed failid, mis lubavad veebisaitidel salvestada, milliseid veebisaite te külastate. Järgige neid juhiseid, et hoida jälgimisküpsised oma arvutist eemal.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Arvuti turvalisus** > **Viiruste ja nuhkvara skannimine**.
3. Valige käsk **Eemalda jälgimisküpsised**.
4. Klõpsake **OK**.

Failide käsitsi skannimine

Saate skannida faile käsitsi, näiteks välise seadmega arvutiühenduse loomisel, tagamaks, et need ei sisalda mingit ründevara.

Käsitsi skannimise käivitamine

Vastavalt vajadusele saate kontrollida nii tervet arvutit kui ka otsida ainult teatud kindlat tüüpi *õelvara* või kontrollida mõnda kindlat asukohta.

Kui kahtlustate, et arvutis võib leiduda kindlat tüüpi *õelvara*, võite otsida ainult seda tüüpi. Kui arvate, et arvutis võib probleeme olla mõnes kindlas kohas, võite kontrollida ainult seda asukohta. Selline kontroll võtab palju vähem aega kui terve arvuti kontrollimine.

Arvuti käsitsi kontrollimiseks toimige järgmiselt.

1. Klõpsake pealehel suvandi **Skannimine** all oleval noolel.

   Kuvatakse skannimise suvandid.
2. Valige kontrolli tüüp.

   Muutmaks arvutis viiruste ja muude kahjulike rakenduste käsitsi skannimist optimaalseks valige käsk **Skannimisseadete muutmine**.
3. Suvandi **Vali, mida skannida** valimisel avaneb aken, milles saate valida skannitava asukoha. Avaneb **Kontrollimisviisard**.

Kontrolli tüübid

Vastavalt vajadusele saate kontrollida nii tervet arvutit kui ka otsida ainult teatud kindlat tüüpi õelvara või kontrollida mõnda kindlat asukohta.

Järgnevalt on ära toodud eri tüüpi kontrollid.

Kontrollitüüp	Mida kontrollitakse	Millal seda tüüpi kasutada
Viiruste ja nuhkvara skannimine	arvuti osi viiruste, nuhkvara ja riskvara suhtes	See kontrollitüüp on palju kiirem kui täielik kontroll. See otsib läbi ainult need süsteemiosad, mis sisaldavad installitud programmifaile. Seda tüüpi soovitatakse siis, kui soovite kiiresti kontrollida, kas arvuti on puhas, sest see leiab ja eemaldab efektiivselt teie arvutist aktiivse õelvara.
Täisskann arvutile	Tervet arvutit (siseseid ja väliseid kõvakettaid) viiruste, nuhkvara ja riskvara suhtes	Kui soovite olla täiesti kindel, et teie arvutis pole õelvara ega riskvara. Seda tüüpi kontroll võtab kõige kauem aega. See kombineerib kiire õelvarakontrolli ja kõvaketta kontrolli. Otsitakse ka võimalikke rootkiti peidetud üksusi.
Valige, mida skannida	Kindel fail, kaust või ketas viiruste, nuhkvara ja riskvara jaoks	Kui teil on alust arvata, et mõni kindel koht teie arvutis võib sisaldada õelvara (nt sisaldab see koht potentsiaalselt ohtlikest allikatest, näiteks võrdõiguslikest failijagamisvõrkudest, alla laaditud faile). Skannimise aeg sõltub skannitava suurusest ja objektist. Skannimine viiakse kiiresti lõpule, kui kontrollite näiteks kausta, mis sisaldab vaid mõnda väikest faili.

Kontrollitüüp	Mida kontrollitakse	Millal seda tüüpi kasutada
Juurkomplekti skannimine	Olulisi süsteemikohti, kus kahtlane üksus võib tähendada turbeprobleemi. Skannib peidetud faile, kaustu, kettaid või protsesse	Kui kahtlustate, et arvutisse võib olla installitud juurkomplekt. Näiteks kui arvutist leiti hiljuti õelvara ja te soovite veenduda, et see ei installinud juurkomplekti.

Windows Exploreris skannimine

Kettaid, kaustu ja faile saab *viiruste*, *nuhkvara* ja *riskvara* suhtes skannida Windows Exploreris.

Ketta, kausta või faili kontrollimiseks tehke järgmist.

1. Asetage oma hiirekursor selle ketta, kausta või faili kohale, mida soovite kontrollida, ja paremklõpsake sellel.
2. Klõpsake paremklõpsamisel avanevas menüüs käsul **Skanni kaustu viiruste suhtes**. (Selle suvandi nimi sõltub sellest, kas kontrollite ketast, kausta või faili.)
   Avatakse aken **Kontrollimisviisard** ja skannimine algab.

Kui leitakse mõni *viirus* või *nuhkvara*, juhendab **Kontrollimisviisard** teid puhastamisprotsessis.

Skannimiseks failide valimine

Valige failitüübid, mida soovite käsitsi või ajastatud kontrollimiste käigus *viiruste* ja *nuhkvara* osas kontrollida.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Muud sätted** > **Käsitsi skannimine**.
3. Valikus **Skannimisvalikud** valige üks järgmistest seadetest.

Ainult teadaolevate failitüüpide skannimine	Ainult nende failitüüpide (nt täitmisfailide) skannimine, mis võivad kõige tõenäolisemalt nakkust kanda. Selle valiku tegemine muudab skannimise ühtlasi ka kiiremaks. Skannitakse järgmiste laienditega faile: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` ja `.hqx`.
Skannimine tihendatud failide sees	Arhiveeritud failide ja kaustade skannimine.
Täpsema heuristika kasutamine	Skannimise ajal olemasoleva heuristika kasutamine uue või tundmatu õelvara lihtsamaks leidmseks. **Märkus:** Selle suvandi valimisel võtab skannimine rohkem aega ja võib anda rohkem valesid tulemusi (võib ohutud faile kahtlastena tuvastada).

4. Klõpsake **OK**.

Märkus: Välistatud üksuste loendis olevaid välistatud faile ei skannita isegi siis, kui teete siin valiku nende skannimiseks.

Mida teha kahjulike failide leidmise korral

Valige leitud kahjulikke failide käsitsemisviis.

Kui leiate käsitsi skannimisel kahjulikku sisu, tehke sobiva toimingu valimiseks järgmist.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Muud sätted** > **Käsitsi skannimine**.
3. Tehke valikus **Viiruse või nuhkvara leidmisel** järgmised valikud.

Suvand	Kirjeldus
Küsi minult (vaikeseade)	Saate valida toimingu, mida teha iga käsitsi skannimisel leitud üksusega.
Failide eemaldamine	Toode proovib automaatselt puhastada käsitsi skannimisel leitud nakatunud faile. **Märkus:** Kui toode ei saa nakatunud faili puhastada, paneb see faili karantiini (v.a juhul, kui see on leitud võrgust või eemaldatavalt seadmelt), nii et see ei saa arvutit kahjustada.
Pane failid karantiini	Toode teisaldab kõik käsitsi skannimisel leitud kahjulikud failid karantiini, kus need ei saa arvutit kahjustada.
Kustuta failid	Toode kustutab kõik käsitsi skannimisel leitud kahjulikud failid.
Ainult teavita	Toode jätab kõik käsitsi skannimisel leitud failid nii, nagu need on ja salvestab tuvastamise tulemused skannimise aruandesse. **Märkus:** Kui reaalajas skannimine on välja lülitatud, saab mis tahes ründevara selle valiku korral arvutit kahjustada.

Märkus: Kui plaanilise skannimise käigus leitakse kahjulikke faile, eemaldatakse need automaatselt.

Skannimise plaanimine

Seadke arvuti skannima ja eemaldage viirused ja muud kahjulikud rakendused automaatselt, kui te seda ei kasuta, või seadke skannimine töötama regulaarselt, tagamaks, et teie arvuti on puhas.

Skannimise plaanimiseks tehke nii.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Muud sätted** > **Plaaniline skannimine**.
3. Lülitage **Plaaniline skannimine** sisse.
4. Valige, millal soovite skannimist alustada.

Suvand	Kirjeldus
Iga päev	Skannige arvutit iga päev.
Iga nädal	Skannige arvutit valitud nädalapäevadel. Valige päevad loendist.
Iga kuu	Skannige arvutit valitud päevadel kuus. Päevade valimiseks tehke järgmist. 1. Valige soovitud **Päev** suvandid. 2. Valige soovitud kuupäev valitud päeva kõrval asuvast loendist.

5. Valige, millal soovite valitud päevadel skanni alustada.

Suvand	Kirjeldus
Alguse aeg	Käivitage skannimine määratud ajal.
Pärast seda, kui arvutit pole kasutatud	Käivitage skannimine pärast seda, kui te pole arvutit kasutanud määratud ajavahemiku vältel.

Plaanitud skannimine kasutab arvuti skannimisel käsitsi skannimise seadeid, välja arvatud juhul, kui see skannib iga kord arhiive ja eemaldab kahjulikud failid automaatselt.

Meilide skannimine

Meilide skannimine kaitseb teid teile saadetud kahjulike meilide vastu.

Meilide viiruste osas skannimiseks peab viiruste ja nuhkvara skannimine olema sisse lülitatud.

E-posti skannimise sisse lülitamiseks tehke järgmist.

1. Klõpsake peamisel lehel Sätted.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige Arvuti turvalisus > Viiruste ja nuhkvara skannimine.
3. Valige käsk Eemalda kahjulikud meilimanused.
4. Klõpsake OK.

Millal meilisõnumeid ja manuseid kontrollitakse?

Viiruste ja nuhkvara skannimine eemaldab kahjuliku sisu teile saadetud meilidest.

Viiruste ja nuhkvara skannimine eemaldab kahjulikud meilid, mida saavad sellised meiliprogrammid nagu Microsoft Outlook ja Outlook Express, Microsoft Mail või Mozilla Thunderbird. See skannib krüpteerimata meilisõnumid ja manused iga kord kui teie meiliprogramm saab neid meiliserverist POP3 protokolli kasutades.

Viiruste ja nuhkvara skannimine ei saa skannida meilisõnumeid veebimeilides, mis sisaldavad teie veebibrauserit käitavaid meilirakendusi, nt Hotmail, Yahoo! mail või Gmail. Olete *viiruste* vastu siiski kaitstud, isegi kui te ei eemalda kahjulikke manuseid või kasutate veebimeili. Kui avate meilimanuse, eemaldab reaalajas skannimine mis tahes kahjulikud manused enne, kui need saavad kahju tekitada.

Märkus: Reaalajas skannimine kaitseb ainult teie arvutit, mitte teie sõprade omi. Reaalajas skannimine ei skanni manustatud faile muidu, kui manuste avamisel. See tähendab, et kui kasutate veebimeili ja edastate sõnumi enne selles sisalduva manuse avamist, võite saata sõpradele nakatatud meile.

Skannimistulemuste kuvamine

Viiruste ja nuhkvara ajaloos kuvatakse kõik kahjulikud failid, mis toode on leidnud.

Mõnikord ei saa toode millegi kahjuliku leidmisel valitud toimingut teha. Näiteks kui valite failide puhastamise ja neid ei saa puhastada, teisaldab toode need karantiini. Seda teavet saate vaadata viiruste ja nuhkvara ajaloos.

Ajaloo vaatamiseks toimige nii.

1. Klõpsake peamisel lehel Sätted.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige Arvuti turvalisus > Viiruste ja nuhkvara skannimine.
3. Klõpsake käsul Kuva eemaldamiste ajalugu.

Viiruste ja nuhkvara ajaloos kuvatakse järgmine teave:

- kahjuliku faili leidmise kuupäev ja kellaaeg,
- ründevara nimi ja selle asukoht arvutis ja
- tehtud toiming.

Failide välistamine skannimisest

Mõnikord võite soovida mõned failid või rakendused skannimisest välistada. Välistatud üksusi ei skannita, välja arvatud juhul, kui eemaldate need välistatud üksuste loendist.

Märkus: Reaalajas ja käsitsi skannimiseks on eraldi välistatud üksuste loendid. Näiteks kui välistate faili reaalajas skannimisest, skannitakse see käsitsi skannimise ajal, välja arvatud juhul, kui välistate selle ka käsitsi skannimisest.

Failitüüpide välja arvamine

Kui välistate failid tüübi alusel, siis määratud laiendiga faile kahjuliku sisu osas ei skannita.

Välistatava failitüübi lisamiseks või eemaldamiseks tehke järgmist.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige, kas soovite välistada failitüübi reaalajas või käsitsi skannimisest.
   - Failitüübi reaalajas skannimisest välistamiseks valige **Arvuti turvalisus** > **Viiruste ja nuhkvara skannimine**.
   - Failitüübi käsitsi skannimisest välistamiseks valige **Muud sätted** > **Käsitsi skannimine**.
3. Klõpsake käsul **Välista failid skannimisest**.
4. Failitüübi välja arvamiseks.
   a) Valige vahekaart **Failitüübid**.
   b) Valige **Jäta välja nende laienditega failid**.
   c) Tippige nupu **Lisa** kõrval asuvale väljale faili laiend, mis määrab väljajäetavate failide tüübid.

      Ilma laiendita failide määramiseks tippige '.'. Te saate kasutada metamärki '?', et üksikut tähte esindada või '*', et esindada suvalist hulka tähti.

      Kui te soovite näiteks välja jätta käivitatavaid faile, tippige väljale `exe`.
   d) Klõpsake **Lisa**.
5. Korrake eelmisi samme kõigi laienditega, mida soovite viiruste osas kontrollimisest välja jätta.
6. Klõpsake **OK**, et sulgeda dialoogiaken **Jäta kontrollimisel välja**.
7. Uute sätete rakendamiseks klõpsake **OK**.

Valitud failitüübid välistatakse edaspidisest skannimisest.

Jäta välja faile asukoha alusel

Kui välistate failid asukoha alusel, siis määratud ketastel või kaustades olevaid faile kahjuliku sisu osas ei skannita.

Failiasukohtade välistamisse lisamiseks või sealt eemaldamiseks tehke järgmist.

1. Klõpsake peamisel lehel **Sätted**.

Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige, kas soovite välistada asukoha reaalajas skannimisest või käsitsi skannimisest.
   - Valige **Arvuti** > **Viiruste ja nuhkvara skannimine**, et välistada asukoht reaalajas skannimisest.
   - Valige **Arvuti** > **Käsitsi skannimine**, et välistada asukoht käsitsi skannimisest.
3. Klõpsake käsul **Välista failid skannimisest**.
4. Faili, ketta või kausta välja arvamiseks:
   a) Valige vahekaart **Objektid**.
   b) Valige **Jäta välja objektid (failid, kaustad, ...)**.
   c) Klõpsake **Lisa**.
   d) Valige fail, ketas või kaust, mille soovite viirusekontrollist välja jätta.

   Märkus: Osad kettad võivad olla eemaldatavad, nagu näiteks CD-, DVD- või võrgukettad. Võrgukettaid ja tühje eemaldatavaid kettaid ei saa välja jätta.

   e) Klõpsake **OK**.
5. Korrake eelmist sammu, et muud failid, kettad või kaustad viirusekontrollist välja jätta.
6. Klõpsake **OK**, et sulgeda dialoogiaken **Jäta kontrollimisel välja**.
7. Uute sätete rakendamiseks klõpsake **OK**.

Valitud failid, kettad või kaustad välistatakse edaspidistest skannimistest.

Välja jäetud rakenduste kuvamine

Saate vaadata rakendusi, mille olete skannimisest välistanud, ja eemaldada need välistatud üksuste loendist, kui soovite neid edaspidi skannida.

Kui reaalajas skannimine või käsitsi skannimine tuvastab rakenduse, mis käitud nagu nuhk- või riskvara, kuid te teate, et see on ohutu, saate selle skannimisest välistada, nii et toode ei hoiata teid enam selle osas.

Märkus: Kui rakendus käitub nagu viirus või muu kahjulik tarkvara, ei saa seda välistada.

Rakendusi ei saa otse välistada. Uued rakendused ilmuvad välistusloendis ainult juhul, kui välistate need skannimise ajal.

Skannimisest välja jäetud rakenduste kuvamiseks.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige, kas soovite vaadata rakendusi, mis on reaalajas või käsitsi skannimisest välistatud.
   - Valige **Arvuti** > **Viiruste ja nuhkvara skannimine**, et vaadata rakendusi, mis on välistatud reaalajas skannimisest.
   - Valige **Arvuti** > **Käsitsi skannimine**, et vaadata rakendusi, mis on välistatud käsitsi skannimisest.
3. Klõpsake käsul **Välista failid skannimisest**.
4. Klõpsake vahekaarti **Rakendused**.

   Märkus: Välja arvata saab ainult nuhkvara ja riskvara, mitte viiruseid.

5. Kui soovite välistatud rakendusi uuesti skannida, tehke järgmist.
   a) Valige rakendus, mida soovite skannimisse kaasata.
   b) Klõpsake käsul **Eemalda**.

6. Klõpsake **OK**, et sulgeda dialoogiaken **Jäta kontrollimisel välja**.
7. Väljumiseks klõpsake **OK**.

Kuidas kasutada karantiini?

Karantiiniks nimetatakse turvalist hoidlat potentsiaalselt ohtlike failide jaoks.

Karantiini pandud failid ei saa edasi levida ega teie arvutit kahjustada.

Karantiini saate panna *õelvara*, *nuhkvara* ja *riskvara*, et need kahjutuks teha. Kui juhtute neid faile või rakendusi hiljem siiski vajama, saate need karantiinist taastada.

Kui teil pole karantiini pandud üksust vaja, võite selle kustutada. Karantiini pandud üksuse kustutamisel eemaldatakse see teie arvutist jäädavalt.

- Karantiini pandud *õelvara* võite üldjuhul kustutada.
- Karantiini pandud *nuhkvara* võite üldjuhul kustutada. On aga võimalik, et karantiini pandud *nuhkvara* kuulub mõne soovitud tarkvaraprogrammi koosseisu ning selle eemaldamisel ei saa vastav programm õigesti töötada. Kui soovite seda programmi oma arvutis säilitada, võite karantiini pandud *nuhkvara* taastada.
- Karantiini pandud *riskvara* võib olla soovitud ja ohutu tarkvaraprogramm. Kui olete programmi ise installinud ja seadistanud, võite selle karantiinist taastada. Kui aga *riskvara* on installitud teie teadmata, on see tõenäoliselt installitud pahatahtlikul otstarbel ja tuleks kustutada.

Karantiinis üksuste kuvamine

Te saate karantiinis olevate üksuste kohta rohkem teavet kuvada.

Karantiinis olevate üksuste lisateabe vaatamiseks:

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Arvuti turvalisus** > **Viiruste ja nuhkvara skannimine**.
3. Klõpsake käsul **Kuva karantiin**.
   Lehel **Karantiin** kuvatakse karantiini talletatud üksuste koguarv.
4. Karantiinis olevate üksuste kohta üksikasjaliku teabe vaatamiseks klõpsake **Üksikasjad**.

   Sisu saate sortida ründevara nime või faili tee alusel.

   Kuvatakse esimese saja elemendi loend koos karantiini pandud elementide tüübi ja nimega ning teega sinna, kuhu failid olid installitud.
5. Karantiini pandud elemendi kohta lisateabe vaatamiseks klõpsake elemendi kõrval oleval ikoonil veerus **Olek**.

Karantiinis üksuste taastamine

Vajadusel saate karantiini pandud üksused taastada.

Vajadusel saate karantiini pandud rakendused või failid taastada. Taastage karantiini pandud üksused ainult juhul, kui olete kindel, et need ei kujuta endast ohtu. Taastatud üksused teisaldatakse tagasi nende algsesse asukohta teie arvutis.

Karantiinis üksuste taastamine

1. Klõpsake peamisel lehel **Sätted**.

Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Arvuti turvalisus** > **Viiruste ja nuhkvara skannimine**.
3. Klõpsake käsul **Kuva karantiin**.
4. Valige karantiini pandud elemendid, mida soovite taastada.
5. Klõpsake **Taasta**.

Mis on DeepGuard?

DeepGuard analüüsib failide sisu ja rakenduste käitumist ning jälgib mitteusaldusväärseid rakendusi.

DeepGuard blokeerib uued ja avastamata *viirused*, *ussid* ja muud kahjulikud rakendused, mis proovivad muuta teie arvutit, ning takistab kahtlastel rakendustel Internetist teie arvutisse pääseda.

Kui DeepGuard tuvastab uue rakenduse, mis proovib süsteemis teha potentsiaalselt kahjulikke muudatusi, lubab see rakendusel töötada turvatsoonis, nii et rakendus ei saa teie arvutit kahjustada. DeepGuard analüüsib, milliseid muudatusi proovis rakendus teha ja otsustab selle põhjal, kui tõenäoliselt on rakendus *ründevara*. Kui rakendus on arvatavasti *pahavara*, siis DeepGuard blokeerib selle.

DeepGuardi tuvastatud potentsiaalselt kahjulike süsteemimuudatuste hulka kuuluvad järgmised muudatused.

- süsteemisätete (Windowsi registri) muudatusi,
- katseid lülitada välja süsteemi tööks olulisi programme (nt turbeprogramme nagu see toode) ja
- katseid muuta olulisi süsteemifaile.

DeepGuardi sisse- või väljalülitamine

Hoidke DeepGuard sees, et takistada kahtlastel rakendustel teha teie arvutis potentsiaalselt ohtlikke süsteemimuudatusi.

Kui kasutate operatsioonisüsteemi Windows XP, kontrollige enne DeepGuardi sisselülitamist, et teil on installitud hoolduspakett Service Pack 2.

DeepGuardi sisse- või väljalülitamiseks tehke järgmist.

1. Klõpsake pealehe suvandil **Olek**.
2. Klõpsake **Muuda sellel lehel olevaid seadeid**.

   Märkus: Turvafunktsioonide väljalülitamiseks vajate administraatori õigusi.

3. **DeepGuardi** sisse- või väljalülitamine.
4. Klõpsake **Sulge**.

DeepGuardi blokeeritud rakenduste lubamine

Saate kontrollida, milliseid rakendusi DeepGuard lubab ja millised blokeerib.

Mõnikord võib DeepGuard blokeerida turvalise rakenduse töötamise, isegi juhul, kui soovite seda kasutada ja teate, et see on turvaline. Selle põhjuseks on asjaolu, et rakendus proovib teha süsteemimuudatusi, mis võivad olla potentsiaalselt kahjulikud. Võite olla rakenduse DeepGuardi hüpikakna kuvamisel ka tahtmatult blokeerinud.

DeepGuardi blokeeritud rakenduse lubamiseks tehke järgmist.

1. Klõspake pealehel valikul **Tööriistad**.
2. Klõpsake **Rakendused**.

Kuvatakse loend **Jälgitavad rakendused**.

3. Leidke rakendus, mida soovite lubada.

   Märkus: Loendi sortimiseks saate klõpsata veeru päistel. Näiteks klõpsake veerul **Luba**, et sortida loend lubatud ja keelatud programmide rühmadesse.

4. Valige veerus **Luba** käsk **Luba**.
5. Klõpsake **Sulge**.

DeepGuard lubab rakendusel süsteemimuudatusi teha.

Kasutage DeepGuardi ühilduvusrežiimis

Maksimaalse kaitse saamiseks muudab DeepGuard ajutiselt töötavaid programme. Mõned programmid kontrollivad, et need pole rikutud või muudetud ega pruugi selle funktsiooniga ühilduda. Näiteks kontrollivad petmisvastaseid tööriistu kasutavad veebimängud käitamisel, et neid poleks ühelgi moel muudetud. Sellistel puhkudel lülitage ühilduvusrežiim välja.

Ühilduvusrežiimi sisselülitamiseks tehke järgmist.

1. Klõpsake peamisel lehel **Sätted**.

   Märkus: Sätete muutmiseks peavad teil olema administraatoriõigused.

2. Valige **Arvuti turvalisus** > **DeepGuard**.
3. Valige käsk **Kasuta ühilduvusrežiimi**.
4. Klõpsake **OK**.

Mida teha hoiatustega kahtlase käitumise kohta?

DeepGuard jälgib rakendusi, mis pole usaldusväärsed. Kui jälgitav rakendus proovib pääseda Internetti, teha muudatusi teie süsteemis või käitub kahtlaselt, siis DeepGuard blokeerib selle.

Kui olete valinud DeepGuardi seadetes käsu **Hoiata mind kahtlase käitumise puhul**, teavitab DeepGuard teid, kui tuvastab potentsiaalselt kahjuliku rakenduse või kui käivitate rakenduse, mille maine on teadmata.

Otsustamaks, mida soovite teha DeepGuardi blokeeritud rakendusega, tehke järgmist.

1. Klõpsake valikul **Üksikasjad**, et kuvada lisateavet programmi kohta.
   Üksikasjade jaotises näete järgmist:

   - rakenduse asukohta,
   - rakenduse mainet reaalajas kaitsevõrgustikus ja
   - seda, kui levinud kasutuses rakendus on.

2. Otsustage, kas usaldate rakendust, mille DeepGuard on blokeerinud.

   - Kui te ei soovi rakendust blokeerida, valige **Usaldan rakendust. Luba sellel jätkata.**.

     Rakendus on turvaline tõenäolisemalt järgmistel puhkudel.

     - DeepGuard blokeeris rakenduse mõne teie toimingu tulemusena.
     - Te tunnete seda rakendust.
     - Saite rakenduse usaldusväärsest allikast.

   - Kui soovite rakendusele blokeeringu säilitada, valige **Ma ei usalda rakendust. Jäta see blokeerituks.**.

     Rakendus ei ole turvaline tõenäolisemalt järgmistel puhkudel.

     - Rakendus pole levinud kasutuses.

- Rakenduse maine pole teada.
- Te ei tunne seda rakendust.

3. Kui soovite edastada kahtlase rakenduse analüüsimiseks, tehke järgmist.

a) Klõpsake käsul **Teata rakendusest F-Secure'ile**.
Toode kuvab edastamise tingimused.

b) Kui nõustute tingimustega ja soovite näidise edastada, klõpsake käsul **Nõustu**.

Soovitame saata näidise järgmistel puhkudel.

- DeepGuard blokeerib rakenduse, mille teate olevat turvalise või
- kahtlustate, et rakendus võib olla *ründevara*.