bitdefender
ANTIVIRUS v10

10th anniversary

Käyttöopas

Virustorjunta

Vakoilunesto

bitdefender
secure your every bit

BitDefender Antivirus v10

Käyttöopas

BitDefender

Julkaistu 2007.05.25
Version 10.2

Laillisuustiedote

Varoitus ja vastuuvapauslauseke. Tämä tuote ja sen kirjallinen aineisto ovat suojattu tekijänoikeuslailla. Tässä dokumentissa olevat tiedot ovat siinä “kuten ovat”-perusteella, eikä niillä ole takuuta. Vaikka kaikki mahdolliset varotoimet on otettu huomioon valmistettaessa tätä dokumenttia, kirjoittajilla ei ole mitään velvollisuuksia yhtäkään henkilöä tai ryhmää kohtaan mitä tulee menetyksiin ja vahinkoihin, jotka ovat aiheutuneet tai joiden väitetään aiheutuneen suoraan tai epäsuorasti tämän työn sisältämistä tiedoista.

Tämä kirja sisältää linkkejä kolmansien osapuolien verkkosivuille, jotka eivät ole SOFTWIN-yhtiön valvonnassa, eikä SOFTWIN ole vastuussa minkään linkitetyn sivuston sisällöstä. Jos käyt tässä oppaassa mainituilla kolmansien osapuolten verkkosivuilla, teet sen omalla vastuullasi. SOFTWIN on ilmoittanut nämä verkko-osoitteet vain mukavuussyistä, eikä linkkien sisällyttäminen tarkoita sitä, että SOFTWIN tukee tai ottaa mitään vastuuta näistä kolmansien osapuolten sivustojen sisällöistä.

Tavaramerkit. Tässä kirjassa voi olla tavaramerkkien nimiä. Kaikki mainitut rekisteröidyt ja rekisteröimättömät tavaramerkit ovat yksinomaan kunkin omistajansa omaisuutta.


bitdefender
secure your every bit

Sisällys

Lisenssi ja takuu

JOS ET HYVÄKSY SEURAAVIA EHTOJA, ÄLÄ ASENNA OHJELMISTOA. VALITSEMALLA "HYVÄKSYN", "OK", "JATKA", "KYLLÄ" TAI ASENTAMALLA TAI KÄYTTÄMÄLLÄ OHJELMISTOA MILLÄÄN TAVALLA, ILMAISET YMMÄRTÄVÄSI JA HYVÄKSYVÄSI TÄMÄN SOPIMUKSEN EHDOT KOKONAISUUDESSAAN.

Nämä ehdot kattavat BitDefender sovellukset ja palvelut kotikäyttäjille lisensoituna sinulle, sisältäen niihin liittyvän dokumentaation ja mitkä tahansa ostamasi lisenssin alaisuudessa sinulle toimitetut ohjelmistopäivitykset tai mitkä tahansa ohjelmistoon liittyvät palvelut jotka on määritelty dokumentaatiossa ja kaikkien näiden kopiot.

Tämä lisenssisopimus on laillinen sopimus sinun (loppukäyttäjänä joko yksityishenkilö tai yksittäinen yritys) ja SOFTWIN-yhtiön välillä ja se oikeuttaa käyttämään SOFTWINin ohjelmistotuotetta, joka on edellä tarkemmin määritelty ja joka sisältää tietokoneohjelman ja voi sisältää myös siihen liittyviä viestivälineitä, painettua aineistoa, sekä verkosta saatavaa tai elektronisessa muodossa olevia dokumentaatioita (BitDefender). Nämä kaikki on suojattu Yhdysvaltalaisilla ja kansainvälisillä tekijänoikeuslaeilla sekä kansainvälisillä sopimuksilla. Asentamalla koneeseen, kopioimalla tai muuten käyttämällä BitDefenderiä sitoudut noudattamaan tämän sopimuksen ehtoja. Älä asenna tai muuten käytä BitDefenderiä, ellet hyväksy tämän sopimuksen ehtoja. Tässä tapauksessa voit palauttaa tuotteen 30 päivän kuluessa ostamisesta siihen liikkeeseen, josta ostit sen ja saat maksamasi hinnan takaisin. Ostokuitti pitää kuitenkin esittää palautuksen yhteydessä.

Jos et hyväksy näitä ehtoja, älä asenna tai käytä BitDefenderiä.

BitDefender Lisenssi. BitDefender on suojattu tekijänoikeuslaeilla ja kansainvälisillä tekijänoikeussopimuksilla sekä muilla aineettoman omaisuuden suojaavilla laeilla ja sopimuksilla (immateriaalioikeudet). BitDefender on lisensoitu, sitä ei myydä.

LISENSSIN MYÖNTÄMINEN. Täten SOFTWIN yhtiö myöntää sinulle ja vain sinulle seuraavan ei-yksinoikeudellisen luvan käyttää BitDefenderiä:

OHJELMISTOSOVELLUS. Voit asentaa ja käyttää BitDefenderiä niin monessa tietokoneessa kuin on tarpeen, hankittujen lisenssien kokonaismäärän sallimissa rajoissa. Voit tehdä asennusmediasta yhden kopion varmuuskopioksi.

TYÖASEMA KÄYTTÄJÄLISENSSI. Tämä lisenssi pätee BitDefender ohjelmistoon joka voidaan asentaa yhteen tietokoneeseen josta ei jaeta verkkopalveluita. Jokainen ensisijainen käyttäjä voi asentaa tämän ohjelmiston yhteen tietokoneeseen ja tehdä yhden varmuuskopion eri laitteeseen. Ensisijaisten käyttäjien enin sallittu lukumäärä on lisenssissä mainittu lukumäärä.

LISENSSIEHDOT: Myönnetyn lisenssin voimassaolo alkaa siitä päivästä kun asennat, kopioit tai muuten ensimmäisen kerran käytät BitDefenderiä ja se pysyy voimassa vain sille koneelle, johon se alunperin asennettiin.

PÄIVITYKSET. Jos kyseessä on tuote, joka on merkitty BitDefenderin päivitykseksi, sinulla pitää olla asianmukainen lisenssi alkuperäiseen tuotteeseen, jonka SOFTWIN tunnistaa versioksi, jolla on oikeus päivitykseen. BitDefender, joka on merkitty päivitykseksi korvaa ja / tai täydentää tuotetta, joka muodosti perustan oikeudelliseen päivitykseen. Voit käyttää päivityksen tuloksena saamaasi tuotetta vain tässä lisenssi-sopimuksessa määriteltyjen ehtojen mukaisesti. Jos BitDefender on ohjelmistopakettiin kuuluvan komponentin päivitys, jonka paketin olet lisensoinut yhtenä tuotteena, BitDefenderiä voidaan käyttää ja siirtää vain osana tätä yksittäistä tuotepakettia, eikä sitä voi erottaa käytettäväksi useammalle kuin yhdelle koneelle.

TEKIJÄNOIKEUDET. Kaikki oikeudet, nimi ja osuus BitDefenderiin ja kaikki tekijänoikeudet BitDefenderiin (sisältäen, mutta ei rajoittuen kaikki kuvat, valokuvat, logot, animaatiot, videot, audiotiedostot, musiikki, teksti ja apletit, jotka kuuluvat kiinteästi BitDefenderiin), siihen liittyvät painotuotteet ja kaikki BitDefenderin kopiot omistaa SOFTWIN. BitDefender on suojattu tekijänoikeuslaeilla ja kansainvälisillä sopimuksilla ja säännöksillä. Tästä syystä sinun pitää kohdella BitDefenderiä kuten mitä tahansa tekijänoikeuslailla suojattua materiaalia, paitsi että saat asentaa BitDefenderin yhteen omaan tietokoneeseesi edellyttäen, että säilytät alkuperäinen yksinomaan arkistokäytössä tai varmistuskappaleena. Sinulla ei ole oikeutta kopioida BitDefenderin mukana tulevia painotuotteita. Sinun pitää liittää kopioiden mukaan kaikki tekijänoikeutta koskevat tiedotteet niiden alkuperäisessä muodossaan riippumatta siitä missä muodossa tai mille tallennusvälineelle ne on tehty. Sinulla ei ole oikeutta siirtää lisenssiä, vuokrata, myydä, tai liisata BitDefenderiä. Et saa muokata, purkaa, kääntää konekielelle tai muuttaa millään tapaa ohjelmaydintä, etkä saa yrittää ottaa selville BitDefenderin lähdekoodia.

RAJOITETTU TAKUU. SOFTWIN antaa toimitetun tietovälineen toimivuudesta takuun, joka on voimassa 30 päivää siitä päivästä, kun BitDefender toimitetaan loppukäyttäjälle. SOFTWIN vastaanotettuaan viallisen välineen voi harkintansa mukaan korvata sen uudella vastaavalla tai palauttaa tuotteesta maksetun hinnan. SOFTWIN ei takaa sitä että BitDefender toimisi keskeytymättömästi tai virheettömästi tai että virheet korjattaisiin. SOFTWIN ei takaa sitä, että BitDefender täyttää vaatimuksesi. Täten softwin kieltäytyy kaikista muista takuuvastuista, jotka koskevat bitdefenderiä, joko ilmenevistä tai epäsuorista. Edellä mainittu takuu on poissulkeva ja toimii muiden takuiden sijasta, joko ilmenevissä tai epäsuorissa tapauksissa, mukaan lukien kauppaan liittyvät epäsuorat takuut, jotka ovat tiettyyn tarkoitukseen sopivia tai eivät loukkaa oikeuksia. TÄMÄ TAKUU ANTAA SINULLE TIETTYJÄ RAJOITETTUJA LAILLISIA OIKEUKSIA. SINULLA VOI OLLA MUITA OIKEUKSIA, JOTKA OVAT ERILAISIA ERI VALTIOISSA.

LUKUUNOTTAMATTA ERITYISESTI TÄSSÄ SOPIMUKSESSA ESITETTYÄ, SOFTWIN KIISTÄÄ KAIKKI MUUT TAKUUT, SUORAT TAI EPÄSUORAT, KUNNIOITTAEN TUOTTEISIIN, LAAJENNUKSIIN, YLLÄPITOON TAI TUKEEN LIITTYVÄÄ, TAI MITÄ TAHANSA MATERIAALIA (AINEETONTA TAI AINEELLISTA) TAI MUITA TUOTETTUJA PALVELUITA. SOFTWIN TÄTEN ERITYISESTI KIISTÄÄ MITKÄ TAHANSA EPÄSUORAT TAKUUT JA EHDOT SISÄLTÄEN RAJOITUKSETTA EPÄSUORAT KAUPALLISET TAKUUT, AINEISTON OIKEELLISUUDEN, TIEDOTTAVAN SISÄLLÖN OIKEELLISUUDEN, JÄRJESTELMÄINTEGROINNIN JA KOLMANSIEN OSAPUOLIEN OIKEUKSIEN LOUKKAAMATTOMUUDEN SUODATTAMALLA, ESTÄMÄLLÄ TAI POISTAMALLA TÄLLAISIA KOLMANSIEN OSAPUOLIEN OHJELMISTOJA, VAKOILUOHJELMISTOJA, MAINOSOHJELMISTOJA, EVÄSTEITÄ, SÄHKÖPOSTEJA, DOKUMENTTEJA, MAINOKSIA TAI VASTAAVIA JOHTUVATPA NE ASETUKSISTA, LAINSÄÄDÄNNÖSTÄ, SOPIMUSKILPAILUSTA, KÄYTÄNNÖISTÄ JA MENETTELYISTÄ TAI KAUPPATAVASTA.

VAHINKOVASTUIDEN IRTISANOMINEN. Jokainen, joka testaa tai arvioi BitDefenderiä, kantaa kaiken vastuun BitDefenderin laadusta ja suorituskyvystä. SOFTWIN ei ole vastuussa minkäänlaisista vahingoista; olivatpa vahingot aiheutuneet suoraan tai epäsuorasti tuotteen käytöstä, suorituskyvystä, BitDefenderin toimittamisesta tilaajalle, vaikka SOFTWIN- yhtiölle olisi annettu tieto sellaisten vahinkojen olemassaolosta tai niiden mahdollisuudesta. JOTKIN VALTIOT EIVÄT SALLI RAJOITUKSIA TAI VASTUUN POISTAMISTA KOSKIEN SATUNNAISIA TAI VÄLILLISIÄ VAHINKOJA, JOLLOIN YLLÄ OLEVAA RAJOITUSTA TAI POISSULKEMISTA EI SOVELLETA. MISSÄÄN TAPAUKSESSA SOFTWININ VASTUU EI YLITÄ TUOTTEESTA MAKSETTUA HINTAA. Yllä olevia vastuunvapautuslausekkeita ja rajoituksia sovelletaan riippumatta siitä hyväksytkö tai käytätkö, arvioit tai testaat BitDefenderiä.

TÄRKEÄ TIEDOTUS KÄYTTÄJILLE. TÄMÄ OHJELMISTO EI OLE VIKASIETOINEN EIKÄ SITÄ OLE SUUNNITELTU TAI TARKOITETTU KÄYTETTÄVÄKSI MINKÄÄNLAISESSA VAARALLISESSA YMPÄRISTÖSSÄ, JOSSA TARVITTAISIIN VIANKESTÄVÄÄ SUORITUSKYKYÄ TAI TOIMINTAA. TÄTÄ OHJELMISTOA EI OLE TARKOITETTU KÄYTETTÄVÄKSI LENTOKONEIDEN SUUNNISTUSKÄYTÖSSÄ, YDINVOIMALAITOKSILLA EIKÄ TIETOLIIKENNEJÄRJESTELMISSÄ, ASEJÄRJESTELMISSÄ, SUORISSA TAI EPÄSUORISSSA HENGENPELASTUSJÄRJESTELMISSÄ, ILMAILULIIKENTEEN VALVONNASSA, EIKÄ MISSÄÄN SELLAISISSA SOVELLUTUKSISSA, TAI ASENNUKSISSA, JOISSA VIKAANTUMINEN VOISI AIHEUTTAA KUOLEMAN, VAKAVIA FYYSISIÄ VAMMOJA TAI OMAISUUSVAHINKOJA.

YLEISTÄ. Tässä sopimuksessa sovelletaan Romanian valtion lakeja ja kansainvälisiä tekijänoikeusasetuksia ja -sopimuksia. Kaikki tästä lisenssisopimuksesta aiheutuvat oikeudelliset kiistat käsitellään Romanian valtion oikeuslaitoksissa.

BitDefenderin käytöstä aiheutuvia hintoja, maksuja ja kuluja voidaan muuttaa ilman eri ilmoitusta.

Siinä tapauksessa, että tämän sopimuksen jokin kohta tulee pätemättömäksi, se ei vaikuta muiden tämän sopimuksen kohtien pätevyyteen.

BitDefender ja BitDefender logot ovat SOFTWIN-yhtiön tavaramerkkejä. Kaikki muut tässä tuotteessa käytetyt tavaramerkit ovat niiden omistajien omaisuutta.

Tämä lisenssi päättyy välittömästi ilman eri ilmoitusta jos rikot mitä tahansa sen ehdoista. Et ole oikeutettu mihinkään korvaukseen SOFTWIN-yhtiön tai BitDefender tuotteiden jälleenmyyjien taholta lisenssin päättyessä. Luottamuksellisuuteen ja rajoituksiin liittyvät ehdot jäävät voimaan lisenssin päättyessäkin.

SOFTWIN voi muuttaa näitä ehtoja milloin tahansa ja muutetut ehdot astuvat voimaan välittömästi niihin liittyvissä ohjelmistoissa. Jos jokin osa näistä ehdoista havaitaan mitättömäksi tai täytäntöönpanokelvottomaksi, se ei vaikuta muihin ehtoihin, jotka pysyvät voimassa ja täytäntöönpanokelpoisia.

Jos näiden ehtojen käännöksissä eri kielille näyttää olevan ristiriitaisuuksia tai epäjohdonmukaisuutta, SOFTWIN-yhtiön toimittama englanninkielinen versio on pätevin.

SOFTWIN yhteystiedot:5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, tai puhelin 40-21-2330780 tai Fax:40-21-2330763, sähköposti: <office@bitdefender.com>.

Johdanto

Tämä opas on tarkoitettu kaikille käyttäjille, jotka ovat valinneet **BitDefender Antivirus v10** tietokoneensa tietoturvaratkaisuksi. Oppaassa olevat tiedot soveltuvat ei vain tietokonealan asiantuntijoille, vaan myös kaikille, jotka käyttävät koneissaan Windows-käyttöjärjestelmää.

Tässä oppaassa selostetaan **BitDefender Antivirus v10**, sekä esitellään yhtiö ja työryhmä, joka sen on rakentanut, se opastaa sinua asennuksessa ja ohjelmiston asetusten määrittelyssä. Opit käyttämään **BitDefender Antivirus v10**:ntä, päivittämään, testaamaan ja tekemään käyttöösi soveltuvat asetukset. Opit myös kuinka saat BitDefenderistä suurimman hyödyn.

Toivotamme sinulle miellyttäviä ja hyödyllisiä opiskeluhetkiä.

1. Kirjan käytännöt

1.1. Painoasuun liittyviä käytäntöjä

Kirjassa käytetään erilaisia kirjoitustyylejä luettavuuden parantamiseksi. Niiden merkitys on esitetty alla olevassa taulukossa.

Ulkoasu	Kuvaus
`sample syntax`	Näytesyntaksit on painettu `kiinteävälisillä` merkeillä.
http://www.bitdefender.com	URL-linkit osoittavat johonkin ulkopuoliseen osoitteeseen http tai ftp palvelimille.
`<support@bitdefender.com>`	Sähköpostiosoitteet ovat tekstin seassa yhteydenottotietoja varten.
“Johdanto” (p. xiii)	Tämä on sisäinen viite johonkin kohtaan dokumentin sisällä.
`filename`	Tiedostot ja kansiot/hakemistot on painettu `tasavälisillä` merkeillä.
option	Kaikki tuotevaihtoehdot on painettu **lihavoiduilla** merkeillä.

Ulkoasu	Kuvaus
`sample code listing`	Koodilistaus on painettu `kiinteävälisillä` merkeillä.

1.2. Huomautukset

Huomautukset ovat tekstissä merkitty graafisesti ja niiden tarkoitus on tiedottaa aiheeseen liittyvästä lisätiedosta.

Huomaa

Huomaa-kappale on lyhyt huomautus. Sen voi ohittaakin, mutta siinä voi kuitenkin olla arvokasta lisätietoa, kuten erityispiirteitä tai viite johonkin samansisältöiseen aiheeseen.

Tärkeää

Tämä pitäisi ottaa huomioon, eikä saisi ohittaa lukematta. Yleensä kyseessä ei ole kriittisiä tietoa, mutta kuitenkin merkitykseltään tärkeää.

Varoitus

Varoitus sisältää kriittistä tietoa, joka pitäisi ottaa huomioon erityisen huolellisesti. Mitään vakavaa ei pääse tapahtumaan, jos vain otat varoitusviitteet huomioon. Sinun kannattaa lukea ja ymmärtää varoitukset, koska niissä selvitetään joitain erittäin riskialttiita seikkoja.

2. Kirjan rakenne

Kirja koostuu seitsemästä osasta, sisältäen seuraavat pääaiheet: Yleistä BitDefenderistä, Tuotteen asentaminen, Tuotteen kuvaus ja ominaisuudet, Hallintakonsoli, Parhaat toimintatavat, BitDefender käynnistys CD ja Ohjeiden saaminen. Lisäksi kirjassa on sanasto joidenkin teknisten termien selventämiseksi.

Tietoa BitDefenderistä. Lyhyt opastus BitDefenderiin.

Tuotteen asennus. Askel askeleelta ohjeet BitDefenderin asentamiseksi tietokoneeseen. Tämä on kattava opas **BitDefender Antivirus 10** asennukseen. Alkaen onnistuneen asennuksen perus edellytyksistä, saat ohjeet läpi koko asennusprosessin läpiviemiseen. Lopuksi myös asennuksen poisto selostetaan sen varalta, että joutuisit poistamaan BitDefender asennuksen.

Kuvaus ja ominaisuudet. BitDefender Antivirus v10, tuotteen ominaisuudet ja osat.

Hallintakonsoli. Kuvaus BitDefenderin hallinnan ja ylläpidon perusteista. Tässä luvussa käydään läpi yksityiskohtaisesti **BitDefender Antivirus v10**, kuinka rekisteröidä

tuote, tarkistaa tietokone, suorittaa päivitykset. Sinulle opetetaan, kuinka konfiguroida ja käyttää kaikkia BitDefenderin osia.

Parhaat toimintavat. Seuraa näitä ohjeita tehdäksesi BitDefenderistäsi paras mahdollinen

BitDefender Korjaus CD. Tietoja BitDefender käynnistys CD:stä. Ohjeita tämän käynnistävän CD:n ominaisuuksien ymmärtämiseksi ja käyttämiseksi.

Avun saaminen. Mistä etsiä ja kysyä neuvoja, jos jotain odottamatonta ilmaantuu.

Sanasto. Sanastossa yritetään selostaa joitakin teknisiä ja muuten epätavallisia kirjassa olevia ilmaisuja, termejä ja oppisanoja.

3. Kommenttipyyntö

Haastamme teidät auttamaan meitä parantamaan tätä kirjaa. Olemme testanneet ja varmistaneet parhaan kykymme mukaan tämän kirjan tiedot. Olkaa hyvä ja kirjoittakaa meille, jos havaitsette virheitä ja puutteita tässä kirjassa tai jos teillä on muita parannusehdotuksia. Teidän avullanne saamme parhaan mahdollisen ohjekirjan käyttöönne.

Kommentit ovat tervetulleita osoitteeseen <documentation@bitdefender.com>.

Tärkeää

Ole hyvä ja kirjoita kaikki tähän käyttöopppaaseen liittyvät sähköpostit englannin kielellä jotta voimme käsitellä ne mahdollisimman nopeasti.

Tietoa BitDefenderistä

Luku 1. Mikä on BitDefender?

BitDefender on johtava maailmanlaajuinen tietoturvatarkaisujen toimittaja joka täyttää tämän päivän tietojärjestelmien turvavaatimukset. Yhtiö tarjoaa yhden nopeimmista ja tehokkaimmista tietoturvaohjelmistoista, asettaen uudet standardit uhkien hallintaan, nopeaan havaitsemiseen ja haittojen lieventämiseen. BitDefender toimittaa tuotteita ja palveluita yli 41 miljoonalle koti- ja yrityskäyttäjälle yli 180 maassa. BitDefenderin toimipaikat sijaitsevat **Yhdysvalloissa**, **Isossa Britanniassa**, **Saksassa**, **Espanjassa** ja **Romaniassa**.

- Virustorjunta, palomuuri, vakoiluohjelmaesto, roskapostin esto ja lapsilukko yritys- ja kotikäyttäjille;
- BitDefenderin tuoteperhe on tarkoitettu osaksi monimutkaisia IT-järjestelmiä (työasemat, tiedostopalvelimet, sähköpostipalvelimet ja yhdyskäytävät), Windows, Linux ja FreeBSD alustoille;
- Maailmanlaajuinen jakelu, tuotteita saatavilla 18 eri kielellä;
- Helppokäyttöisyys yhdessä ohjatun asennuksen kanssa opastaa käyttäjän asennusvaiheen läpi vain muutaman kysymyksen avulla;
- Kansainvälisesti sertifioidut tuotteet: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, ym;
- Asiakaspalvelua kellon ympäri - asiakaspalvelu on käytössä 24 tuntia, 7 päivää viikossa;
- Salamannopea reaktioaika uusien hyökkäysten ilmaantuessa;
- Paras tunnistusaste;
- Tunnin välein saatavilla olevat virustunnisteet - automaattiset tai ajastetut toiminnot tarjoavat suojan uusimpia viruksia vastaan.

1.1. Miksi BitDefender?

Todistetusti aktiivisin virustorjunnan tuottaja. BitDefenderin nopea reagointi tietokonevirusepidemioihin (hyökkäyksiin) vahvistettiin alkaen viimeisten CodeRed-, Nimda ja Sircam sekä Badtrans.B-virusten ja muiden vaarallisten, nopeasti leviävien ja ilkivaltaisten koodien torjunnassa. BitDefender oli ensimmäinen, joka antoi vastamyrkkyä näitä koodeja vastaan ja antoi myös tämän torjuntakeinon vapaasti kaikkien tarvitsevien käyttöön Internetin välityksellä. Nyt kun Klez-virus leviää jatkuvasti

erilaisina versioina, on välitön suojaustarve tullut jälleen kriittisen tärkeäksi kaikille tietokonejärjestelmille.

Uudistuskykyinen. Euroopan komissio ja EuroCase palkinnot merkittävistä uutuuksista. BitDefender on julistettu European IST-palkinnon voittajaksi, jonka myöntävät Euroopan komissio ja 18 akatemian edustajat Euroopassa. Nyt, sen kahdeksantena vuotena, European IST-palkinto on palkkio edistyksellisistä tuotteista, jotka edustavat parhaita eurooppalaisia innovaatioita informaatioteknologian alalla.

Kattava ja monipuolinen. Hoitaa verkon jokaisen yksittäisen pisteen taaten täydellisen turvan. BitDefenderin antamat suojausratkaisut yritysympäristöön tyydyttävät nykyaikaisen yritysympäristön suojausvaatimukset ja mahdollistavat kaikkien monimutkaisten uhkien hallinnan. Tuote poistaa kaikki uhkatekijät, jotka vaarantavat verkon toiminnan, alkaen pienistä paikallisverkoista ja kattaen suuret monipalvelinjärjestelmät sekä monialustaiset WAN-verkot.

Järjestelmäsi täydellinen suoja. Kestävä rintama kaikkia mahdollisia uhkia vastaan. Viruksen tunnistus, joka perustuu koodin analysointiin, ei ole aina antanut hyviä tuloksia. BitDefender soveltaa käyttäytymisperustaista tunnistusta ja kykenee antamaan suojan myös uusia haittaohjelmia vastaan.

Seuraavia ongelmia tietokoneiden käyttäjät haluavat välttää ja niitä varten suojaustuotteet on suunniteltu:

- Matojen hyökkäykset
- Tiedonsiirtokatkokset saastuneiden sähköpostiviestien vuoksi
- Sähköpostiliikenteen katkokset
- Järjestelmien palautukset ja puhdistus
- Tuotantomenetykset, kun järjestelmät ovat pois käytöstä
- Hakkerointi ja asiattomien pääsy järjestelmiin, josta voi aiheutua vahinkoja

Useat samanaikaiset **kehitys- ja etunäkökohdat** voidaan toteuttaa käyttämällä BitDefenderin suojavalikoimaa:

- Turvataan verkon korkea käyttöaste pysäyttämällä ilkivaltaisten koodien hyökkäykset ja leviäminen (esim. Nimda, Trojan horses, DDoS).
- Suojaa etäkäyttäjät hyökkäyksiltä.
- Pienentää hallintokuluja ja BitDefenderin Enterprisen avulla saadaan yrityksen tietojärjestelmät nopeasti hallintaan.
- Sähköpostin kautta leviävät haittaohjelmat pysäytetään käytettäessä BitDefenderin suojauksia yrityksen yhdyskäytävissä. Estää tilapäisesti tai pysyvästi asiattomien, vahingollisten ja kalliiksi käyvien sovellusten yhteydet.

Lisätietoja BitDefenderistä voit saada vierailemalla osoitteessa: http://www.bitdefender.com.

Tuotteen asennus

Luku 2. BitDefender Antivirus v10 asennus

BitDefender Antivirus v10 asennus osio tässä käyttöoppaassa sisältää seuraavat aiheet:

- Järjestelmävaatimukset
- Asennuksen vaiheet
- Ohjattu asennus
- Ohjelman päivitys
- BitDefenderin poistaminen, korjaaminen tai mukauttaminen

2.1. Järjestelmävaatimukset

Tuotteen kunnollinen toiminnan varmistamiseksi, tarkista ennen asennusta että jokin seuraavista käyttöjärjestelmistä on asennettu tietokoneeseesi, ja että vastaavat järjestelmävaatimukset täyttyvät.

2.1.1. Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit / Vista

- Pentium II 350 MHz tai nopeampi
- Minimum 128 MB RAM muistia (256 MB suositeltava määrä)
- Vähintään 60 MB vapaata kiintolevytilaa
- Internet Explorer 5.5 tai uudempi

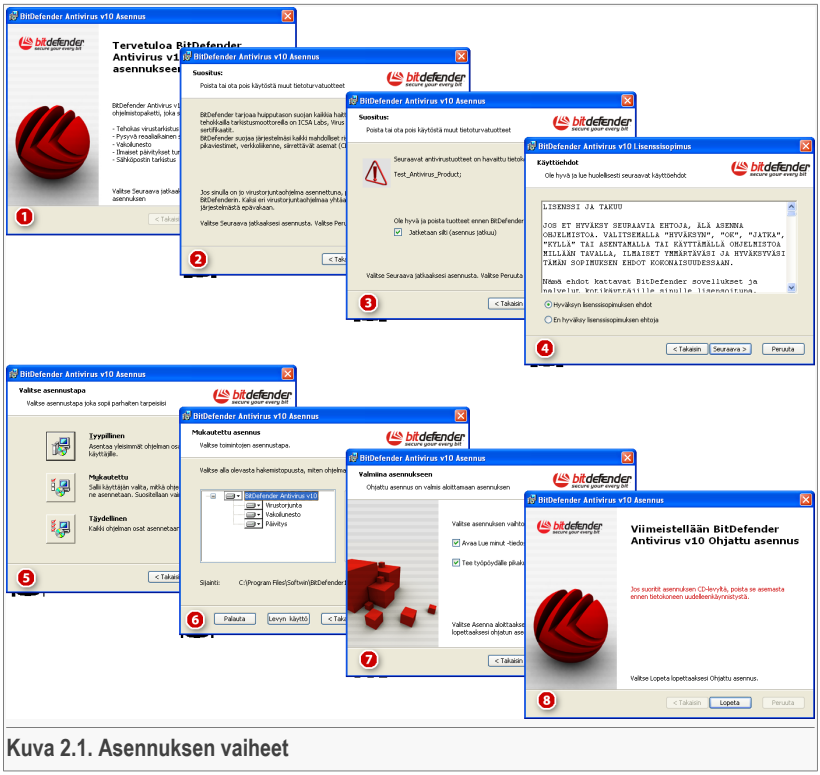
2.1.2. Microsoft Windows Vista 32-bit

- 800 MHz prosessori tai nopeampi
- Vähintään 512 MB RAM muistia (1 GB suositus)
- Vähintään 60 MB vapaata kiintolevytilaa

BitDefender Antivirus v10 kokeiluverio on ladattavissa osoitteessahttp://www.bitdefender.com.

2.2. Asennuksen vaiheet

Kaksoisklikkaa setup.exe -tiedostoa. Tämä käynnistää ohjatun asennuksen, joka opastaa sinut asennusprosessin läpi.



Kuva 2.1. Asennuksen vaiheet

1. Valitse **Seuraava** jatkaaksesi asennusta tai **Peruuta**, jos haluat lopettaa asennuksen.
2. Valitse **Seuraava** jatkaaksesi tai **Takaisin**, palataksesi ensimmäiseen vaiheeseen.
3. BitDefender Antivirus v10 varoittaa, jos tietokoneessasi on asennettuna jokin muu antivirustuote.

Varoitus

On erittäin suositeltavaa poistaa muut havaitut antivirustuotteet ennen BitDefenderin asennusta._ Kahden tai useamman antivirustuotteen käyttäminen tietokoneessa yhtäaikaa tekee useimmiten tietokoneen käytön mahdottomaksi.

Valitse **Takaisin** palataksesi edelliseen vaiheeseen tai **Peruuta** poistuaksesi asennuksesta. Jos haluat jatkaa, valitse **Seuraava**.

Huomaa

Jos BitDefender Antivirus v10 ei löydä järjestelmästä muita antivirustuotteita, tämä vaihe ohitetaan.

4. Lue Lisenssisopimus ja valitse **Hyväksyn lisenssisopimuksen ehdot** ja sen jälkeen valitse **Seuraava**. Jos et hyväksy ehtoja, valitse **Peruuta**. Asennusprosessi keskeytetään ja lopetetaan.
5. Voit valita minkä tyyppisen asennuksen haluat: tyypillinen, asiakasvalintainen, tai täydellinen.

   Tyypillinen
   Ohjelma asennetaan tavallisimmilla asetuksilla. Tämä on suositeltava tapa useimmille käyttäjille.

   Mukautettu
   Voit valita, mitkä osat haluat asentaa. Tämä on suositeltava tapa kokeneimmille käyttäjille.

   Täysi
   Tuotteen täydellinen asentaminen. Kaikki BitDefenderin osat asennetaan.

   Jos valitset **Tyypillinen** tai **Täysi**, vaihe 6 ohitetaan.
6. Jos olet valinnut **Valinnainen**, uusi ikkuna ilmestyy näytölle, jossa on luettelo kaikista BitDefenderin komponenteista, joista voit valita ne, jotka haluat asentaa.

   Jos klikkaat osan nimeä, lyhyt kuvaus ilmestyy oikeaan reunaan (sisältäen asennuksen tarvitseman minimimäärän kovalevytilaa). Jos klikkaat jonkin oan kuvaketta, näytölle tulee ikkuna, josta voit valita, asennetaanko valittu osa vai ei.

   Voit valita kansion, mihin tuote asennetaan. Oletuskansio on `C:\Program Files\Softwin\BitDefender 10`.

   Jos haluat asentaa tuotteen ei kansioon, valitse **Selaa** ja valitse avautuvasta ikkunasta haluamasi kansio, mihin haluat BitDefender Antivurs v10 asennettavan. Valitse **Seuraava**.
7. Kaksi vaihtoehtoa ovat valittuina oletuksena:

- **Avaa lue minut–tiedosto**, jolloin ”Lue minut”-tiedosto avautuu asennuksen lopussa.
- **Tee pikakuvake työpöydälle** - tekee pikakuvakkeen BitDefender Antivirus v10:lle työpöydälle asennuksen lopussa.
- **Ota Windows Defender pois käytöstä** -ottaa Windows Defenderin pois käytöstä; tämä valinta on näkyvissä vain Windows Vistassa.

Valitse **Asenna** aloittaaksesi tuotteen asennuksen.

Tärkeää

Asennuksen aikana käynnistyy ohjattu asennu. Se auttaa sinua rekisteröimään **BitDefender Antivirus v10** tuotteen, luomaan BitDefender tilin ja määrittää BitDefenderin suorittamaan turvallisuuden kannalta tärkeitä tehtäviä.
Suorita ohjattu asennus loppuun jatkaaksesi seuraavaan vaiheeseen.

8. Valitse **Lopeta** viimeistelläksesi tuotteen asennuksen. Jos hyväksyit oletusasennuspolun, uusi kansio nimeltään `Softwin` on luotu `Program Files` -kansioon, jossa on alikansio nimeltä `BitDefender 10`.

Huomaa

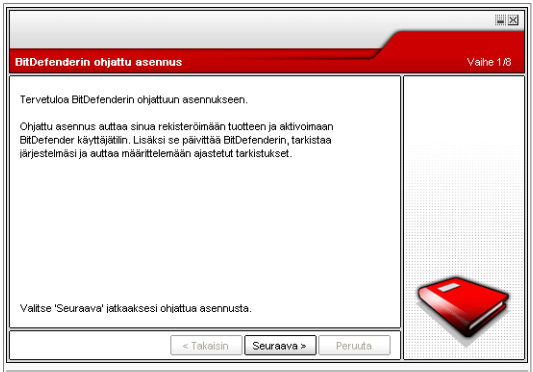
Sinua pyydetään uudelleenkäynnistämään kone, jonka jälkeen ohjattu asennus viimeistelee asennusprosessin.

2.3. Ohjattu ensiasennus

Asennuksen aikana käynnistyy ohjattu asennus. Se auttaa sinua rekisteröimään **BitDefender Antivirus v10** tuotteen, luomaan BitDefender tilin ja määrittää BitDefenderin suorittamaan tärkeitä turvallisuuteen liittyviä tehtäviä.

Tämän ohjatun asennuksen suorittaminen loppuun ei ole välttämätöntä; suosittelemme kuitenkin tekemään niin säästääksesi aikaa ja varmistaaksesi, että järjestelmäsi on suojattu jo ennen kuin BitDefender Antivirus v10 on asennettu.

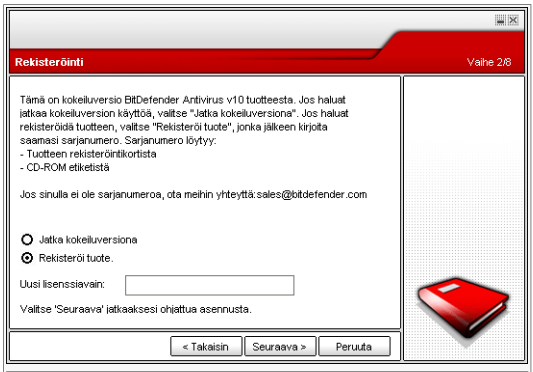
2.3.1. Vaihe 1/8 - BitDefender ohjattu ensiasennus



Kuva 2.2. Tervetuloa –ikkuna

Valitse **Seuraava**.

2.3.2. Vaihe 2/8 - Rekisteröi BitDefender Antivirus v10



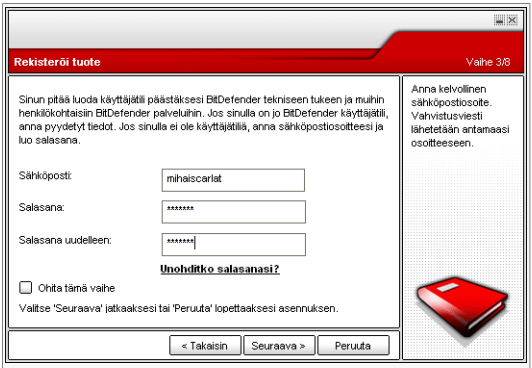
Kuva 2.3. Rekisteröinti

Valitse **Rekisteröi tuote** rekisteröidäksesi **BitDefender Antivirus v10**:n. Kirjoita lisenssiavain **Uusi lisenssiavain** kenttään.

Jatkaaksesi tuotteen kokeilua, valitse **Jatka tuotteen kokeilua**.

Valitse **Seuraava**.

2.3.3. Vaihe 3/8 - Luo BitDefender tili



Kuva 2.4. Tilin luominen

Minulla ei ole BitDefender tiliä

Saadaksesi hyödyn BitDefenderin ilmaisesta teknisestä tuesta ja muista ilmaisista palveluista, sinun täytyy luoda tili.

Kirjoita kelvollinen sähköpostiosoite **Sähköposti** kenttään. Keksi salasana ja kirjoita se **Salasana** kenttään. Vahvista salasana kirjoittamalla se uudelleen **Vahvista salasana** kenttään. Käytä sähköpostiosoitetta ja salasanaa kun kirjaudut tilillesi osoitteessa http://myaccount.bitdefender.com.

Huomaa

Salasanan on oltava vähintään neljä merkkiä pitkä.

Voidaksesi aktivoida tilisi, sinun on ensin aktivoitava sähköpostiosoitteesi._ Tarkista sähköpostisi ja seuraa BitDefender rekisteröintipalvelun sinulle lähetettämässä viestissä olevia ohjeita.

Tärkeää

Ole hyvä ja aktivoi tilisi ennen siirtymistä seuraavaan vaiheeseen.

Jos et halua luoda BitDefender tiliä, valitse **Ohita tämä vaihe**. Myös seuraava ohjatun asennuksen vaihe ohitetaan.

Valitse **Seuraava** asennuksen jatkamiseksi tai **Peruuta** lopettaaksesi ohjatun asennuksen.

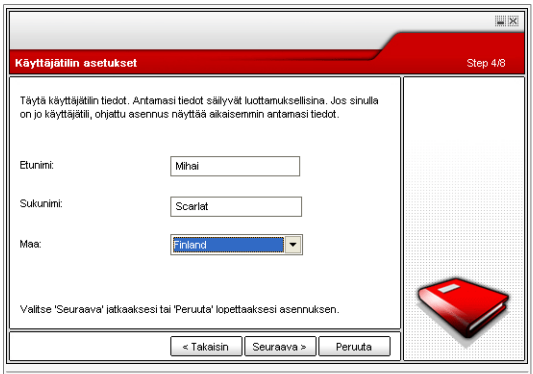
Minulla on jo BitDefender tili

Jos sinulla on jo aktiivinen tili, anna sähköpostiosoitteesi ja salasana. Jos annat väärän salasanan, saat kehoituksen kirjoittaa se uudelleen kun valitset **Seuraava**. Valitse **Ok** kirjoittaaksesi salasanan uudelleen tai **Peruuta** lopettaaksesi ohjatun asennuksen.

Jos olet unohtanut salasanasi, valitse **Unohditko salasanasi?** ja seuraa ohjeita.

Valitse **Seuraava** asennuksen jatkamiseksi tai **Peruuta** lopettaaksesi ohjatun asennuksen.

2.3.4. Vaihe 4/8 - Kirjoita tilin tiedot



Kuva 2.5. Tilin tiedot

Huomaa

Sinun ei tarvitse käydä läpi tätä vaihetta jos valitsit **Ohita tämä vaihe** ohjatun asennuksen kolmannessa vaiheessa.

Kirjoita etu- ja sukunimesi ja valitse maa jossa asut.

Jos sinulla on jo tili, ohjattu asennus näyttää aikaisemmin antamasi tiedot._ Halutessasi voit muokata tietoja tässä.

Tärkeää

Antamasi tiedot pysyvät luottamuksellisena.

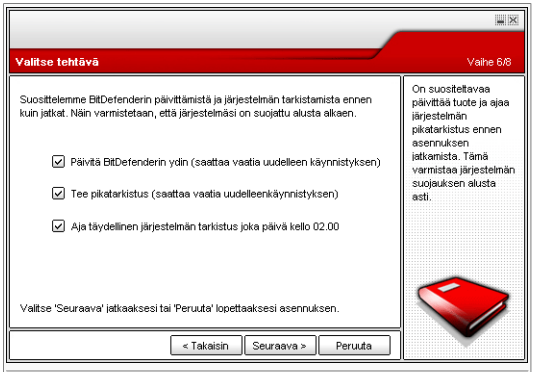
Valitse **Seuraava** asennuksen jatkamiseksi tai **Peruuta** lopettaaksesi ohjatun asennuksen.

2.3.5. Vaihe 5/8 - Tietoja RTVR:stä

Kuva 2.6. RTVR tietoa (Reaaliaikainen virusraportointi)

Valitse **Seuraava** asennuksen jatkamiseksi tai **Peruuta** lopettaaksesi ohjatun asennuksen.

2.3.6. Vaihe 6/8 – Valitse suoritettavat tehtävät



Kuva 2.7. Tehtävävalinta

Määrittele BitDefender Antivirus v10 suorittamaan järjestelmäsi turvallisuuden kannalta tärkeitä tehtäviä.

Seuraavat vaihtoehdot ovat käytettävissä:

- **Päivitä BitDefender Antivirus v10 ytimet (voi vaatia uudelleenkäynnistämisen)** - seuraavassa vaiheessa suoritetaan BitDefender Antivirus v10 ytimien päivitys tietokoneesi suojaamiseksi viimeisimpiä uhkia vastaan.
- **Suorita järjestelmän pikatarkistus (voi vaatia uudelleenkäynnistyksen)** - seuraavassa vaiheessa BitDefender Antivirus v10 suorittaa järjestelmän pikatarkistuksen varmistaakseen ettei tiedostot kansioissa `Windows` ja `Ohjelmatiedostot` sisällä haittaohjelmia.
- **Tee järjestelmän täydellinen tarkistus joka päivä klo 14:00** - tekee järjestelmän täydellisen tarkistuksen joka päivä klo 14:00.

Tärkeää

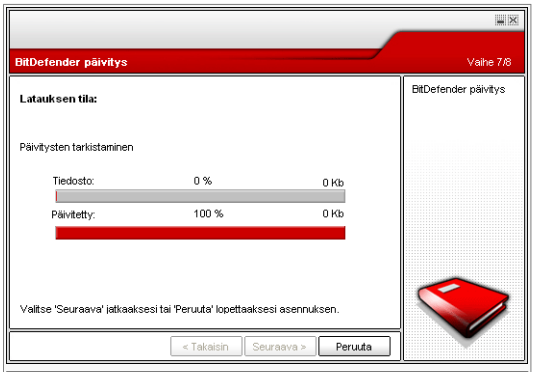
Suosittelemme, että jätät nämä vaihtoehdot valituiksi ennen kuin jatkat seuraavaan vaiheeseen, varmistaaksesi järjestelmän turvallisuuden.

Jos valitset vain viimeisen vaihtoehdon tai jätät kaikki valitsematta, seuraava vaihe ohitetaan.

Voit vaihtaa mitä tahansa asetuksia palaamalla edellisiin vaiheisiin valitsemalla **Takaisin**). Myöhemmin näitä asetuksia ei voi enää muuttaa: jos jatkat, et voi palata aikaisempiin vaiheisiin.

Valitse **Seuraava** asennuksen jatkamiseksi tai **Peruuta** lopettaaksesi ohjatun asennuksen.

2.3.7. Vaihe 7/8 - Odota tehtävien suorittamista loppuun

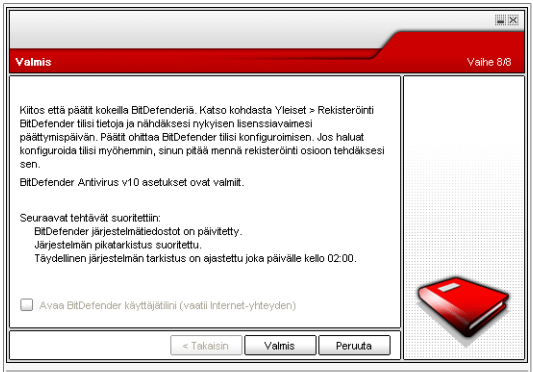


Kuva 2.8. Tehtävän tila

Odota tehtävien suorittamista loppuun. Voit nähdä valittujen tehtävien tilan edellisessä vaiheessa.

Valitse **Seuraava** asennuksen jatkamiseksi tai **Peruuta** lopettaaksesi ohjatun asennuksen.

2.3.8. Vaihe 8/8 – Näytä yhteenveto



Kuva 2.9. Valmis

Tämä on ohjatun asennukset viimeinen vaihe.

Valitse **Avaa BitDefender tilini** kirjautuaksesi BitDefender tilillesi. Tähän tarvitaan Internet-yhteys.

Valitse **Lopeta** viedäksesi ohjatun asennuksen loppuun ja jatkaaksesi asennusprosessia.

2.4. Ohjelman päivitys

Päivitys voidaan tehdä seuraavilla tavoilla:

- **Asenna poistamatta aikaisempaa versiota - v8 tai uudempi, Internet Security poissuljettuna**

  Kaksoisklikkaa asennustiedostoa ja seuraa ohjatun asennuksen ohjeita "*Asennuksen vaiheet*" (p. 10) -osiossa.

  Tärkeää

  Asennuksen aikana tulee esiin virheilmoitus, jonka aiheuttaa `Filespy -palvelu`. Valitse **OK** jatkaaksesi asennusta.

- **Poista edelliset versiot ja asenna uusi - kaikki BitDefender versiot**

Enismmäiseksi sinun täytyy poistaa edelliset versiot, sen jälkeen käynnistä tietokone uudelleen ja asenna uusi versio ohjeiden mukaisesti, jotka löytyvät "*Asennuksen vaiheet*" (p. 10) osiosta.

Tärkeää

Jos päivität BitDefender v8 tai uudemmasta suosittelemme, että tallennat BitDefender asetukset. Päivityksen jälkeen voit ladata asetukset uuteen versioon.

2.5. BitDefenderin poistaminen, korjaaminen tai mukauttaminen

Jos haluat mukauttaa, korjata tai poistaa **BitDefender Antivirus v10:n**, valitse Windowsista: **Käynnistä** -> **Ohjelmat** -> **BitDefender 10** -> **Muokauta, Korjaa tai Poista**.

Sinua pyydetään vahvistamaan valintasi valitsemalla **Seuraava**. Näytölle avautuu uusi ikkuna, josta voit valita:

- **Muokkaa** - valitaksesi uusia ohjelman osia lisättäväksi tai jo asennettuja osia poistettavaksi.

  Huomaa

  Oppiaksesi kuinka viedä asennusprosessi loppuun asti, katso kohtaa kuudes vaihe "*Asennuksen vaiheet*" (p. 10) osiossa.

- **Korjaa** - kaikkien viimeksi asennettujen ohjelman osien uudelleen asentamiseksi.

  Tärkeää

  Ennen tuotteen korjausta suosittelemme, että tallennatBitDefender asetukset. Korjauksen jälkeen voit ladata asetukset uudelleen.

- **Poista** - poista kaikki asennetut komponentit.

  Jos poistat BitDefenderin asennuksen, tietokoneesi ei ole enää suojassa viruksia, vakoiluohjelmia ja tunkeutujia vastaan. Jos haluat, että Windows Palomuuri ja Windows Defender otetaan käyttöön BitDefenderin poistamisen jälkeen, valitse niihin liittyvät kohdat seuraavassa vaiheessa.

  Arvostaisimme jos voisit käyttää hetken aikaa kertoaksesi meille, miksi halusit poistaa BitDefenderin Valitse **Lähetä palautetta** ja täytä online lomake lähettääksesi meille mielipiteesi ja parannusehdotuksesi.

Asennus jatkuu, kun valitset yhden yllä mainituista vaihtoehdoista. Suosittelemme, että valitset **Poista** -vaihtoehdon, niin saat puhtaan uudelleen asennuksen. Asennuksen poiston jälkeen on suositeltavaa poistaa myöskin `Softwin` kansio `Program Files`-kansiosta.

Kuvaus ja ominaisuudet

Luku 3. BitDefender Antivirus v10

Virustorunta- ja vakoilunesto-ohjelmisto tietokoneellesi!

BitDefender Antivirus v10 on tehokas virustorjunta- ja vakoilunestotyökalu ominaisuuksilla, jotka parhaiten täyttävät tietoturvatarpeesi. Helppokäyttöisyys ja automaattiset päivitykset tekevät **BitDefender Antivirusksesta** 'asenna ja unohda' -tuotteen.

3.1. Virustorjunta

Virustorjunnan tehtävä on varmistaa kaikkien mahdollisten virusten tunnistus ja poistaminen. BitDefender Virustorjunta käyttää tehokkaita tarkistusmoottoreita, jotka ovat sertifioineet ICSA Labs, Virus Bulletin, Checkmark, CheckVir ja TÜV.

Ennakoiva tunnistus. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) emuloi virtuaalista tietokonetta tietokoneen sisällä, missä ohjelman osat suoritetaan ja tarkistetaan mahdollisen haittaohjelmalle tyypillisen käyttäytymisen varalta. Tämä BitDefenderin patentoima teknologia edustaa uutta turvatasoa, joka pitää käyttöjärjestelmän suojassa tuntemattomilta viruksilta tunnistamalla haitalliset ohjelmakoodin osat, vaikka niiden tunnistetta ei vielä olisikaan julkaistu.

Pysyvä virussuoja. Uudet ja parannetut BitDefenderin tarkistusmoottorit etsivät ja puhdistavat saastuneita tiedostoja niitä käytettäessä, minimoiden tietojen menetystä. Saastuneet tiedostot voidaan nyt puhdistaa ja palauttaa niitä tuhoamatta.

Rootkit havaitseminen ja poistaminen. Uusi BitDefender osa, joka etsii rootkit ohjelmia (haitallisia piilotettuja ohjelmia, jotka on suunniteltu ottamaan tietokone hallintaan) ja löydettäessä poistaa ne.

Internet tarkistus. Internet liikenne suodatetaan nyt reaaliajassa, jo ennen kuin mitään pääsee selaimeen asti. Tämä varmistaa turvallisen ja nautittavan internetin käytön.

Vertaisverkko- ja pikaviestiohjelmasuojaus. Suodattimet viruksia vastaan, jotka leviävät pikaviestien kautta ja tiedostojen jakamisessa ohjelmasovelluksissa.

Täydellinen sähköpostisuoja. BitDefender toimii POP3/SMTP protokollatasolla, suodattaen tulevat ja lähtevät sähköpostiviestit riippumatta käytetystä sähköpostiohjelmasta (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, jne.) ilman erillistä määrittelyä.

3.2. Vakoilunesto

BitDefender tarkkailee ja estää mahdollisia vakoilu-uhkia reeaaliajassa, ennen kuin ne ehtivät vahingoittaa järjestelmääsi. Käyttäen tekemäänsä laajaa tietokantaa vakoiluohjelmatunnisteista, se pitää tietokoneesi suojassa vakoiluohjelmilta.

Tosiaikainen vakoilunesto. BitDefender tunnistaa kymmeniä mahdollisia järjestelmässäsi olevia riskikohtia, joissa vakoiluohjelma voisi toimia, se tarkistaa myös kaikki muutokset, joita järjestelmään ja ohjelmiin on tehty. Kaikki tunnetut vakoiluohjelmien uhat torjutaan tosiaikaisesti.

Vakoiluohjelmatarkistus ja poisto. BitDefender voi tarkistaa järjestelmäsi tai sen osan etsien tunnettuja vakoiluohjelmia. Tarkistus käyttää jatkuvasti päivittyvää vakoiluohjelmatietokantaa.

Yksityisyydensuoja. Yksityisyyden suoja tarkkailee tietokoneeltasi lähtevää HTTP (Internet) ja SMTP (sähköposti) liikennettä, joka voisi sisältää henkilökohtaisia tietoja - kuten luottokorttien numerot, henkilötunnukset, ja muut käyttäjän määrittelemät tiedot (esim. salasanan osat).

Soitonesto. Luvattomia yhteyksiä valvova yhteysesto-ohjelma (anti-dialer) voidaan konfiguroida, niin etteivät ilkivaltaiset sovellukset kykene ottamaan luvattomia, kalliiksi käyviä modeemiyhteyksiä.

Evästevalvonta. Vakoilunesto suodattaa tulevat ja lähtevät evästetyyppiset tiedostot, pitäen henkilöllisyytesi ja mieltymyksesi luottamuksellisina Internetiä käytettäessä.

Aktiivinen sisällön välvonta. Estää aktiivisesti kaikki mahdolliset haitalliset sovelluskoodit, kuten ActiveX, Java Applets tai Java Scripts.

3.3. Muut ominaisuudet

Käyttöönotto. Ohjattu asetusten mukauttaminen käynnistyy automaattisesti ohjelman asennuksen jälkeen, auttaen käyttäjää valitsemaan sopivimmat päivitysasetukset, ottamaan käyttöön ajastetun tarkistuksen sekä opastaa tuotteen rekisteröinnissä ja aktivoinnissa.

Käyttömukavuus. BitDefender suunnitteli käyttöliittymän uudelleen, korostaen käytettävyyttä ja välttäen sekavuutta. Tuloksena monet BitDefender Antivirus v10:n osat tarvitsevat käyttäjältä vähemmän toimenpiteitä, automaattisten ja itseoppivien toimintojen ansiosta.

Päivitys kerran tunnissa. BitDefender päivitetään Internetin välityksellä 24 kertaa vuorokaudessa, suoraan tai välityspalvelimen kautta. Tuote kykenee tarvittaessa

korjaamaan itsensä lataamalla vioittuneet tai puuttuvat tiedostot BitDefenderin palvelimilta.

24/7-tuki. Online-palvelumme tarjoaa käyttöösi ammattitaitoiset tukihenkilöt sekä tietokannan, jossa on vastauksia usein esitettyihin kysymyksiin.

Korjauslevy. BitDefender Antivirus v10 toimitetaan käynnistävällä CD-levyllä. Tätä CD-levyä voidaan käyttää järjestelmän tutkimiseen, korjaamiseen ja puhdistamiseen, kun tietokoneen käyttöjärjestelmää ei voida käynnistää.

Luku 4. BitDefenderin osat

BitDefender Antivirus 10 sisältää seuraavat osat: **Yleiset**, **Virustorjunta**, **Vakoilunesto** ja **Päivitys**.

4.1. Yleiset -osa

BitDefender asentuu täysin konfiguroituna maksimaaliseen suojaukseen.

Yleistä -osassa voit mukauttaa tietoturvatasoa ja suorittaa tärkeitä tietoturvatehtäviä. Tässä osassa voit myös rekisteröidä tuotteesi ja asettaa BitDefenderin yleiset toimintatavat.

4.2. Virustorjunta

BitDefender suojaa koneesi viruksilta, vakoiluohjelmilta ja muilta haittaohjelmilta tarkistamalla tiedostot, sähköpostiviestit, lataukset ja muun sisällön niiden tullessa järjestelmääsi.

BitDefenderi tarjoama suojaus on jaettu kahteen luokkaan:

- Käytönaikainen tarkistus - estää uusia viruksia, vakoiluohjelmia ja muita haittaohjelmia pääsemästä järjestelmääsi. Tätä kutsutaan myös reaaliaikaiseksi suojaukseksi – tiedostot tarkistetaan niitä käytettäessä. BitDefender hakee esim. Word-dokumentista tunnettuja uhkia silloin, kun avaat sen ja sähköpostiviestistä silloin, kun vastaanotat sen. BitDefender tarkistaa tiedostot ”silloin kun käytät niitä” - käytönaikaisesti.
- Manuaalinen tarkistus - Havaitsee järjestelmääsi jo päässeet virukset, vakoiluohjelmat ja muut haittaohjelmat. Tämä on perinteinen, käyttäjän käynnistämä virustarkistus - sinä valitset, mitkä levyt, kansiot tai tiedostot tarkistetaan ja BitDefender tekee sen.

4.3. Vakoilunesto

BitDefender tarkkailee lukuisia mahdollisia "riskikohtia" järjestelmässäsi, joissa vakoiluohjelmat voisivat toimia ja se tarkistaa myös kaikki muutokset, joita järjestelmässä ja ohjelmistoissa tapahtuu. Se torjuu tehokkaasti Troijalaiset ja muut hakkereiden asentamat työkalut, jotka yrittävät vaarantaa yksityisyytesi ja lähettää yksityistä tietoa tietokoneeltasi hakkerille, esim. luottokorttien numeroita.

4.4. Päivitys

Uusia haittaohjelmia löydetään ja tunnistetaan joka päivä. Tämän vuoksi on hyvin tärkeää pitää BitDefender päivitettynä uusimpien virustunnisteiden avulla. Oletusarvoisesti BitDefender tarkistaa automaattisesti tunnin välein, onko uusia päivityksiä saatavilla.

Päivitykset tulevat seuraavilla tavoilla:

- **Päivitykset virustorjunta-ytimille** - kun uusia uhkia ilmaantuu, tiedostot, jotka sisältävät virustunnisteita, pitää päivittää, jotta varmistetaan pysyvä, ajan tasalla oleva suojaus niitä vastaan. Tämän tyyppinen päivitys tunnetaan myös nimellä **Virustunnisteiden päivitys**.
- **Päivitykset vakoilunesto-ytimille** - uusi vakoiluohjelman tunnus lisätään tietokantaan. Tämä päivitys tunnetaan nimellä **Vakoiluneston päivitys**.
- **Tuotepäivitykset** - kun uusi tuoteversio julkaistaan, uudet ominaisuudet ja hakutekniikat otetaan käyttöön, jotta tuotteen suorituskyky tulisi entistä paremmaksi. Tätä toimenpidettä kusutaan **Tuotepäivitykseksi**.

Lisäksi käyttäjän näkökulmasta voimme ottaa huomioon:

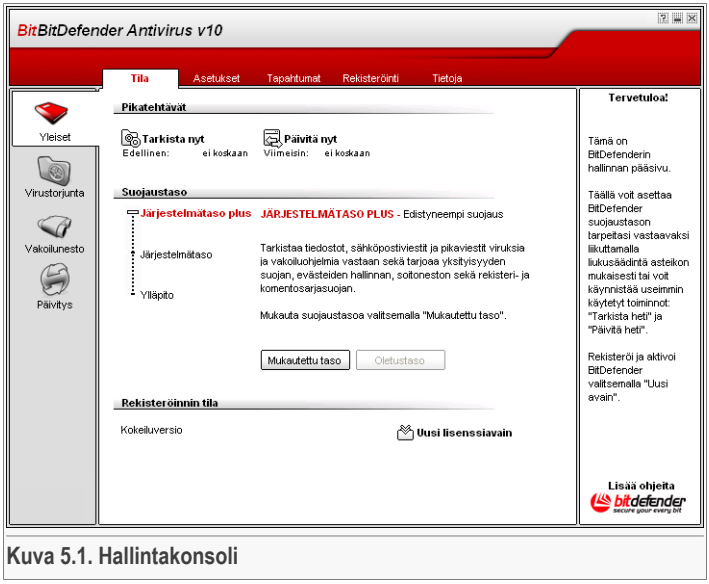
- Automaattinen päivitys - BitDefender muodostaa automaattisesti yhteyden päivityspalvelimeen tarkistaakseen, onko uusia päivityksiä julkaistu. Jos on, BitDefender päivitetään automaattisesti. Automaattinen päivitys voidaan halutessasi tehdä milloin tahansa valitsemalla **Päivitä nyt** kohdassa Päivitys.
- Manuaalinen päivitys - viimeisimmät tunnisteet pitää ladata ja asentaa manuaalisesti.

Hallintakonsoli

Luku 5. Yleiskatsaus

BitDefender Antivirus v10 sisältää keskitetyn hallintakonsolin, josta voidaan konfiguroida kaikkien BitDefender osien suojausasetukset. Sinun tarvitsee avata vain hallintakonsoli, josta pääset käsiksi hallitsemaan kaikkia osia: **Virustorjunta**, **Vakoilunesto** ja **Päivitys**.

Päästäksesi hallintakonsoliin, käytä Windowsin käynnistä -valikkoa ja valitse **Käynnistä → Kaikki ohjelmat → BitDefender 10 → BitDefender Antivirus v10** tai klikkaa **BitDefender kuvaketta** ilmaisinalueella.



Kuva 5.1. Hallintakonsoli

BitDefenderin osien valikko sijaitsee hallintakonsolin vasemmassa reunassa:

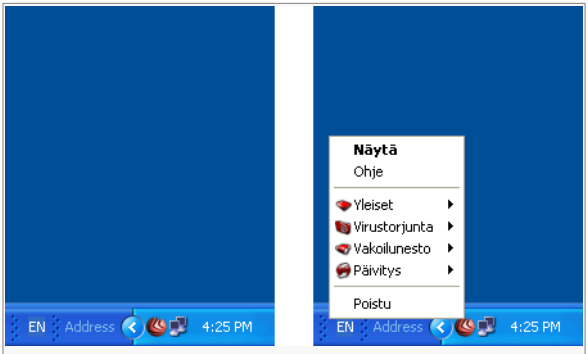
- Yleistä - tässä osiossa voit asettaa yleisen turvatason ja suorittaa keskeisiä tietoturvatehtäviä. Täällä voit myös rekisteröidä tuotteen ja nähdä yhteenvedon kaikista BitDefenderin pääasetuksista, tiedot tuotteesta ja yhteystiedot.
- Virustorjunta - voit konfiguroida **Virustorjunta** -osan toimintoja.
- Vakoilunesto - voit konfiguroida **Vakoilunesto** -osan toimintoja.
- Päivitys - voit konfiguroida **Päivitys** -osan toimintoja.

Hallintakonsolin oikeassa reunassa näet tietoja valitusta osiosta. **Lisää** -painike, joka sijaitsee alhaalla oikealla, avaa **Ohje** tiedoston.

5.1. Ilmaisinalue

Kun konsoli-ikkuna on pienennetty, ohjelman kuvake ilmestyy ilmaisinalueelle.

Jos kaksoisklikkaat tätä kuvaketta, hallintakonsoli avautuu. Jos klikkaat sitä hiiren oikealla painikkeella, avautuu pikavalikko. Tätä kautta voit päästä nopeasti BitDefenderiin hallintaan.



Kuva 5.2. BitDefender kuvake ilmaisinalueella

- **Näytä / Sulje** - avaa hallintakonsolin tai pienentää sen ilmaisinalueelle.
- **Ohje** - Avaa ohjevalikon.
- **Yleinen** - Yleinen osan hallinta.
  - **Uusi lisenssiavain** - aloittaa ohjatun rekisteröinnin, joka opastaa sinua rekisteröintiprosessissa.
  - **Muokkaa käyttäjätiliä** - käynnistää ohjatun toiminnon, joka auttaa sinua luomaan BitDefender tilin.
- **Virustorjunta** - Antivirus osan hallinta.
  - **Reaaliaikainen suojaus on käytössä / pois käytöstä** - näyttää reaaliaikaisen suojauksen tilan (käytössä / pois käytöstä). Valitse tämä ottaaksesi reaaliaikaisen suojauksen pois käytöstä tai käyttöön.
  - **Tarkista** - avaa alavalikon, josta voit suorittaa jonkin Tarkista osassa olevista tarkistustehtävistä.
- **Vakoilunesto** - Vakoilunesto osan hallinta.
  - **Vakoilunesto on käytössä / pois käytöstä** - näyttää vakoiluohjelmasuojauksen tilan (käytössä / pois käytöstä). Valitse tämä ottaaksesi vakoiluneston pois käytöstä tai käyttöön.
  - Valitse **Lisäasetukset** - vakoiluneston lisäasetusten mukauttaminen.
- **Päivitys** - Päivitys osan hallinta.
  - **Päivitä nyt** - suorittaa päivityksen välittömästi.

- **Automaattinen päivitys on käytössä / pois käytöstä** - näyttää automaattisen päivityksen tilan (käytössä / pois käytöstä). Valitse tämä ottaaksesi automaattisen päivityksen pois käytöstä tai käyttöön.
- **Poistu** - Lopettaa sovelluksen kokonaan. Kun valitset tämän, ilmaisinalueella oleva kuvake poistuu näkyvistä ja jotta saisit hallintakonsolin uudelleen auki, pitää se käynnistää jälleen Windowsin Käynnistä-valikosta.

Huomaa

Ikoni muuttuu mustaksi, jos poistat käytöstä yhden tai useamman BitDefenderin osan. Näin tiedät hallintakonsolia avaamatta, jos jotkin osat ovat pois käytöstä.
Ikoni vilkkuu silloin kun päivitys on saatavissa.

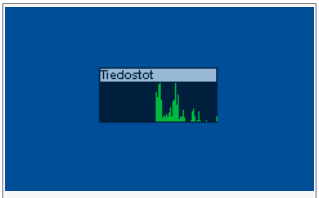
5.2. Toimintapalkki

Toimintapalkki on pieni kaksiosainen ikkuna, joka kuvaa järjestelmän tarkistustoimintoja.

Vihreät palkit (**Tiedostot**) näyttävät tarkistettujen tiedostojen määrän per sekunti, asteikolla 0 -50.

Huomaa

Toimintapalkki ilmoittaa, jos virussuojaus on pois päältä, näyttämällä punaisen ristin alueen päällä (**Tiedostot** tai **Verkko**) Näin tiedät, onko koneesi suojattu, avaamatta hallintakonsolia.



Kuva 5.3. Toimintapalkki

Jos et halua pitää toimintapalkkia näkyvillä, klikkaa hiiren oikealla painikkeella sen päällä ja valitse **Piilota**.

Huomaa

Poistaaksesi toimintapalkin näkyvistä kokonaan, poista **Näytä Toimintapalkki (tuotteen toiminta näytöllä graafisesti) -valinta** (**Yleiset** -osan Asetukset-osiossa).

Luku 6. Yleiset -osa

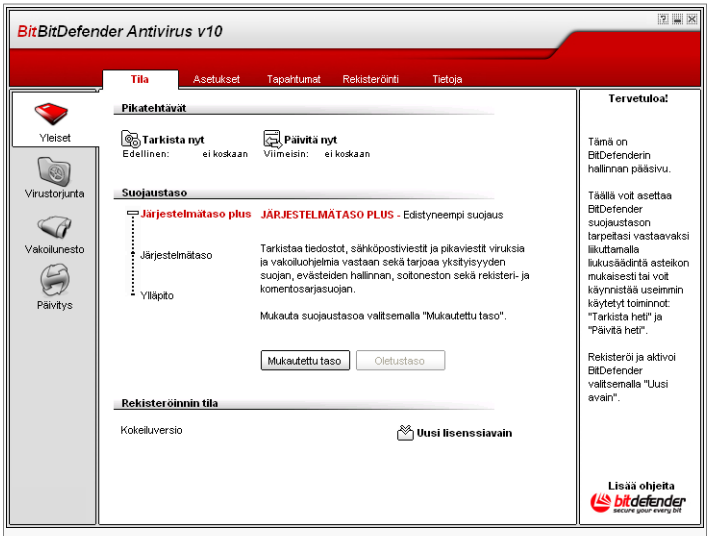
Tämän käyttöoppaan **Yleiset**-osio sisältää seuraavia aiheita:

- Päähallinta
- Hallintakonsolin asetukset
- Tapahtumat
- Tuotteen rekisteröinti
- Tietoja ohjelmasta

Huomaa

Lisätietoja **Yleistä** -osasta löytyy kohdasta "*Yleiset -osa*" (p. 29).

6.1. Päähallinta



Kuva 6.1. Päähallinta

Tässä osassa voit mukauttaa yleistä tietoturvatasoa ja suorittaa tärkeitä BitDefenderin tehtäviä. Voit myös rekisteröidä tuotteen ja nähdä lisenssin päättymispäivän.

6.1.1. Pikatehtävät

BitDefender mahdollistaa nopean pääsyn tärkeisiin tietoturvatehtäviin. Käyttämällä näitä tehtäviä, voit pitää BitDefenderin ajan tasalla, tarkistaa järjestelmäsi tai estää verkkoliikenteen.

Tarkistaaksesi koko järjestelmän, valitse **Tarkista nyt**. Tarkistusikkuna [70] tulee esiin ja järjestelmän täydellinen tarkistus käynnistyy.

Tärkeää

Suosittelemme täyden järjestelmätarkistuksen tekemistä vähintään kerran viikossa. Saadaksesi lisätietoja tarkistustehtävistä ja -prosesseista, katso tämän käyttöoppaanManuaalinen tarkistus osaa.

Suosittelemme BitDefenderin päivittämistä ennen järjestelmän tarkistusta, jotta se voisi havaita viimeisimmät tietoturvauhat. Päivittääksesi BitDefenderin, valitse **Päivitä nyt**. Odota muutama sekunti päivitysprosessin valmistumista tai siirry Päivitys osaan nähdäksesi päivityksen tilan.

Huomaa

Lisää tietoa päivitysprosessista löydät tämän käyttöoppaan Automaattinen päivitys osasta.

6.1.2. Turvataso

Voit valita tarpeisiisi parhaiten sopivan tietoturvatason. Siirrä liukusäädintä asteikolla asettaaksesi sopivan turvatason.

Valittavissa on kolme turvatasoa:

Turvataso	Kuvaus
Ylläpito	Ei suojausta. Ainoastaan**Automaattinen päivitys** on käytössä. Ainoastaan BitDefenderin päivitys on käytössä. Vaikkakaan tämä ei tarjoa minkäänlaista suojaa, se voi olla hyödyllinen taso järjestelmän ylläpitäjille.
Järjestelmätaso	Suojaa viruksilta. Suositellaan erityisesti tietokoneille, joissa ei ole verkko- tai internetyhteyttä. Resurssienkulutus on hyvin vähäinen. Tiedostot tarkistetaan viruksia vastaan käytönaikaisesti.

Turvataso	Kuvaus
Järjestelmätaso Plus	Suojaa viruksilta ja vakoiluohjelmilta. Suositellaan erityisesti tietokoneille, joissa ei ole verkko- tai Internetyhteyttä. Resurssienkulutus on hyvin vähäinen. Tiedostot tarkistetaan viruksia ja vakoiluohjelmia vastaan käytönaikaisesti.

BitDefender Antivirus v10 on suositeltava versio tietokoneille, joissa ei ole verkko- tai Internetyhteyttä.

Voit mukauttaa turvatasoa valitsemalla **Mukautettu taso**. Valitse esiin tulevasta ikkunasta haluamasi suojausvaihtoehdot ja valitse **OK**.

Valitse **Oletustaso**-ottaaksesi käyttöön oletusasetukset.

6.1.3. Rekisteröinnin tila

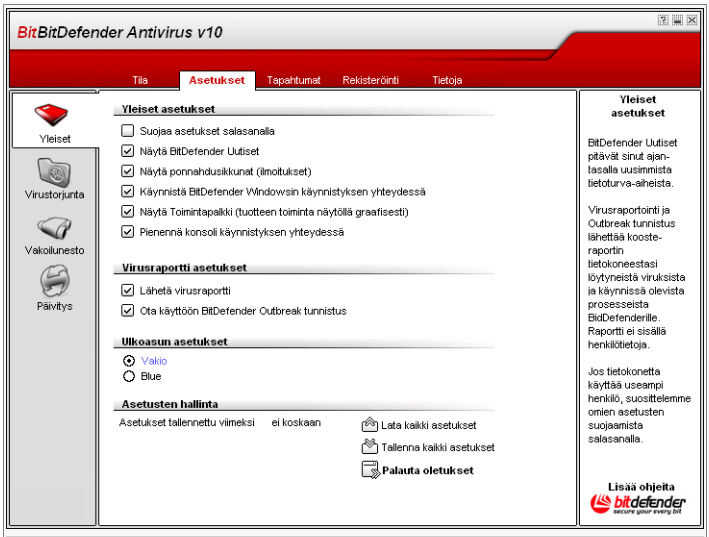
Tässä osiossa on tietoja BitDefender lisenssin tilasta. Tässä osiossa voit myös rekisteröidä tuotteen ja nähdä lisenssin päättymispäivän.

Antaaksesi uuden lisennsiavaimen, valitse **Uusi lisenssiavain**. Suorita ohjattu rekisteröinti loppuun, jotta BitDefenderin rekisteröinti onnistuisi.

Huomaa

Lisätietoja rekisteröintiprosessista löydät tämän käyttöoppaan Rekisteröinti -osiosta.

6.2. Hallintakonsolin asetukset



Kuva 6.2. Hallintakonsolin asetukset

Tässä voit tehdä BitDefenderin yleisimmät asetukset. Oletusarvoisesti BitDefender ladataan Windowsin käynnistyksen yhteydessä ja pienennetään kuvakkeeksi ilmaisinalueelle.

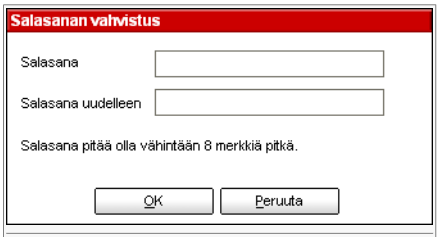
6.2.1. Asetukset

- **Suojaa asetukset salasanalla** - mahdollistaa salasanan määrittämisen hallintakonsolin asetusten suojaamiseksi.

  Huomaa

  Jos et ole ainoa, jolla on järjestelmänvalvojan oikeudet tähän tietokoneeseen, on suositeltavaa suojata BitDefenderin asetukset salasanalla.

  Jos valitset tämän vaihtoehdon, näytölle ilmestyy seuraava ikkuna:



Kuva 6.3. Anna salasana

Kirjoita salasana **Salasana** -kenttään ja kirjoita se uudelleen **Salasana uudelleen** –kenttään ja valitse **OK**.

Tästä eteenpäin sinulta kysytään salasanaa, jos haluat muuttaa BitDefenderin asetuksia.

Tärkeää

Jos unohdat salasanan, sinun pitää korjata tuotetta, jotta voisit muuttaa BitDefenderin konfiguraatiota.

- **Näytä BitDefender uutiset (tietoturva-aiheisia ilmoituksia)** - näyttää aika-ajoin tietoturvaan liittyviä ilmoituksia, jotka koskevat uusia virusuhkia.
- **Näytä ponnahdusikkunat (ilmoitukset näytöllä)** - näyttää ponnahdusikkunat, jotka koskevat tuotteen tilaa.
- **Käynnistä BitDefender Windowsin käynnistyksen yhteydessä** - käynnistää BitDefenderin automaattisesti, kun järjestelmä käynnistetään.

Huomaa

Suosittelemme että pidät tämän vaihtoehdon valittuna.

- **Näytä toimintapalkki (tuotteen toiminta näytöllä graafisesti** - ottaa käyttöön/pois käytöstä Toimintapalkin.
- **Pienennä konsoli käynnistyksen yhteydessä** - pienentää BitDefenderin hallintakonsolin sen lataamisen jälkeen ilmaisinalueelle. Vain BitDefender ikoni jää näkyviin ilmaisinalueelle.

6.2.2. Virusraportoinnin asetukset

- **Lähetä virusraportit** - lähettää BitDefenderille raportteja tietokoneestasi löytyneistä viruksista. Tämä auttaa meitä jäljittämään virusten leviämisiä.

Raportit eivät sisälllä luottamuksellisia tietoja, kuten nimesi, IP-osoite tai muuta sellaista, eikä tietoja käytetä kaupallisiin tarkoituksiin. Kerätyt tiedot sisältävät vain viruksen nimen ja niitä käytetään vain tilastollisiin tarkoituksiin.

- **Ota käyttöön BitDefender Outbreak tunnistus** - lähettää BitDefenderille raportteja, jotka liittyvät mahdollisten virushyökkäysten syntymisiin.

  Raportit eivät sisälllä luottamuksellisia tietoja, kuten nimeäsi, IP-osoitetta tai muuta sellaista tietoa, eikä tietoja käytetä mihinkään kaupallisiin tarkoituksiin. Kerätyt tiedot sisältävät vain mahdollisen viruksen nimen ja niitä käytetään vain uusien virusten tunnistamiseksi.

6.2.3. Ulkoasun asetukset

Mahdollistaa hallintakonsolin värityksen valitsemisen. Ulkoasulla tarkoitetaan käyttöliittymän taustaväriä. Voit vaihtaa ulkoasun väritystä niitä kuvaavista valinnoista.

6.2.4. Asetusten hallinta

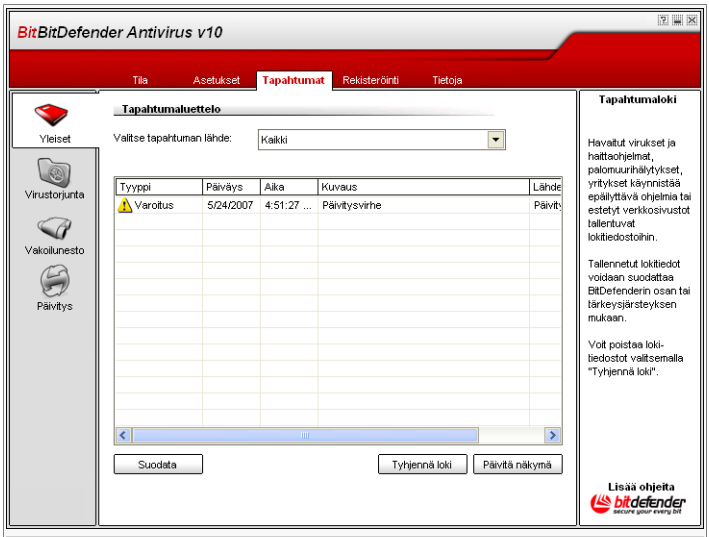
Valitse **Tallenna kaikki asetukset** tai **Lataa kaikki asetukset** tallentaaksesi tai ladataksesi BitDefenderin asetukset haluamaasi sijaintiin. Näin voit käyttää samoja asetuksia BitDefenderin uudelleenasennuksen tai korjaavan asennuksen jälkeen.

Tärkeää

Vain käyttäjät, joilla on järjestelmänvalvojan oikeudet, voivat tallentaa ja ladata asetuksia.

Ladataksesi oletusasetukset, valitse **Oletustaso**.

6.3. Tapahtumat



Kuva 6.4. Tapahtumat

Tässä osiossa esitetään kaikki BitDefenderin muodostamat tapahtumat.

On kolmen tyyppisiä tapahtumia: **Ilmoitus**, **Varoitus** ja **Kriittinen**.

Esimerkkejä tapahtumista:

- **Ilmoitus** - kun sähköposti on tarkistettu;
- **Varoitus** - kun on huomattu epäilyttävä tiedosto;
- **Hälytys** - kun on löydetty saastunut tiedosto.

Jokainen tapahtuma saa seuraavat tiedot: tapahtuman päiväys ja kellonaika, lyhyt kuvaus ja sen lähde (**Virustorjunta**, **Palomuuri**, **Vakoilunesto** tai **Päivitys**). Kaksoisklikkaamalla tapahtumaa näet sen ominaisuudet.

Voit suodattaa näitä tapahtumia kahdella tavalla (tyypin tai lähteen mukaan):

- Valitse **Suodatin** valitaksesi minkä tyyppiset tapahtumat näytetään.
- Valitse tapahtuman lähde pudotusvalikosta.

Jos hallintakonsolin **Tapahtumat** osio on avoinna ja jotain tapahtuu samaan aikaan, sinun pitää valita **Päivitä**, nähdäksesi tapahtuman.

Poistaaksesi kaikki tapahtumat, valitse **Tyhjennä loki** ja sen jälkeen **Kyllä** vahvistaaksesi toiminnon.

6.4. Tuotteen rekisteröinti

Kuva 6.5. Tuotteen rekisteröinti

Tässä osiossa on tietoja BitDefender lisenssin tilasta (rekisteröinnin tila, tuotetiedot, päättymispäivä) ja BitDefender tilistä. Täällä voit myös rekisteröidä tuotteen ja mukauttaa BitDefender tiliäsi.

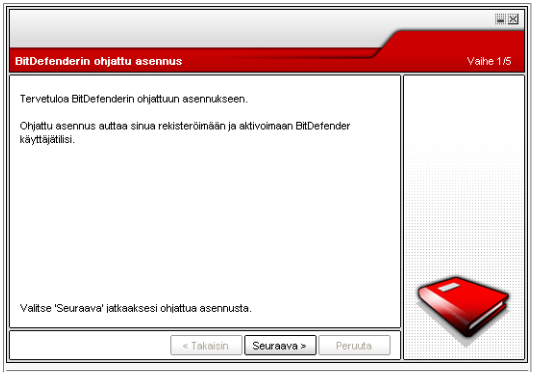
Valitse **Osta nyt** hankkiaksesi uuden lisenssiavaimen BitDefenderin online kaupasta.

Valitsemalla **Uusi lisenssiavain** voit rekisteröidä tuotteen, muuttaa lisenssiavainta tai tilitietoja. Mukauttaaksesi BitDefender tiliäsi, valitse **Muokkaa käyttäjätiliäsi**. Kummassakin tapauksessa ohjattu rekisteröinti käynnistyy.

6.4.1. Ohjattu rekisteröinti

Ohjatussa rekisteröinnissä on viisi vaihetta.

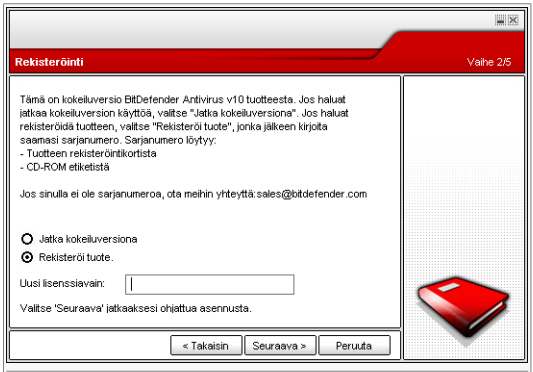
Vaihe 1/5 - Tervetuloa BitDefenderin ohjattuun rekisteröintiin



Kuva 6.6. Tervetuloa –ikkuna

Valitse **Seuraava**.

Vaihe 2/5 - Rekisteröinti



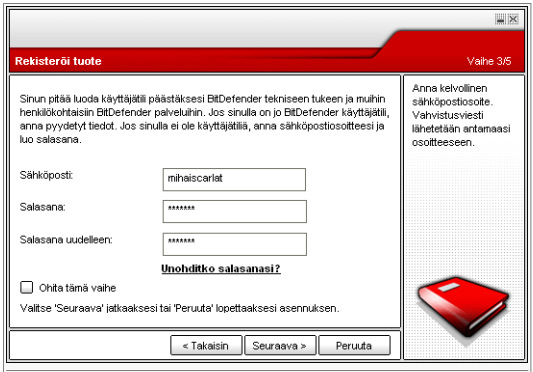
Kuva 6.7. Rekisteröinti

Valitse **Rekisteröi tuote** rekisteröidäksesi **BitDefender Antivirus v10**:n. Kirjoita lisenssiavain **Uusi lisenssiavain** kenttään.

Jatkaaksesi tuotteen kokeilua, valitse **Jatka tuotteen kokeilua**.

Valitse **Seuraava**.

Vaihe 3/5 - Luo BitDefender tili



Kuva 6.8. Tilin luominen

Minulla ei ole BitDefender tiliä

Saadaksesi hyödyn BitDefenderin ilmaisesta teknisestä tuesta ja muista ilmaisista palveluista, sinun täytyy luoda tili.

Kirjoita kelvollinen sähköpostiosoite **Sähköposti** kenttään. Keksi salasana ja kirjoita se **Salasana** kenttään. Vahvista salasana kirjoittamalla se uudelleen **Vahvista salasana** kenttään. Käytä sähköpostiosoitetta ja salasanaa kun kirjaudut tilillesi osoitteessa http://myaccount.bitdefender.com.

Huomaa

Salasanan on oltava vähintään neljä merkkiä pitkä.

Voidaksesi aktivoida tilisi, sinun on ensin aktivoitava sähköpostiosoitteesi._ Tarkista sähköpostisi ja seuraa BitDefender rekisteröintipalvelun sinulle lähetettämässä viestissä olevia ohjeita.

Tärkeää

Ole hyvä ja aktivoi tilisi ennen siirtymistä seuraavaan vaiheeseen.

Jos et halua luoda BitDefender tiliä, valitse **Ohita tämä vaihe**. Myös seuraava ohjatun asennuksen vaihe ohitetaan.

Valitse **Seuraava** jatkaaksesi.

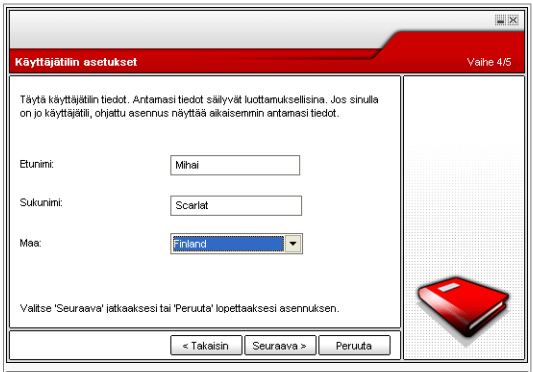
Minulla on jo BitDefender tili

Jos sinulla on jo aktiivinen tili, anna sähköpostiosoitteesi ja salasana. Jos annat väärän salasanan, saat kehoituksen kirjoittaa se uudelleen kun valitset **Seuraava**. Valitse **Ok** kirjoittaaksesi salasanan uudelleen tai **Peruuta** lopettaaksesi ohjatun asennuksen.

Jos olet unohtanut salasanasi, valitse **Unohditko salasanasi?** ja seuraa ohjeita.

Valitse **Seuraava** jatkaaksesi.

Vaihe 4/5 - Kirjoita tilin tiedot



Kuva 6.9. Tilin tiedot

Huomaa

Sinun ei tarvitse käydä läpi tätä vaihetta jos valitsit **Ohita tämä vaihe** ohjatun asennuksen kolmannessa vaiheessa.

Kirjoita etu- ja sukunimesi ja valitse maa jossa asut.

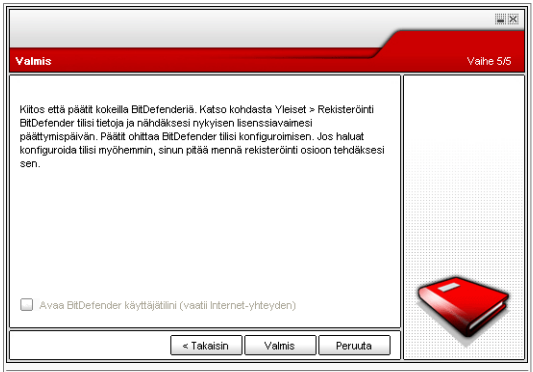
Jos sinulla on jo tili, ohjattu asennus näyttää aikaisemmin antamasi tiedot. Tässä voit halutessasi myös muokata tietojasi.

Tärkeää

Antamasi tiedot pysyvät luottamuksellisena.

Valitse **Seuraava**.

Vaihe 5/5 – Näytä yhteenveto



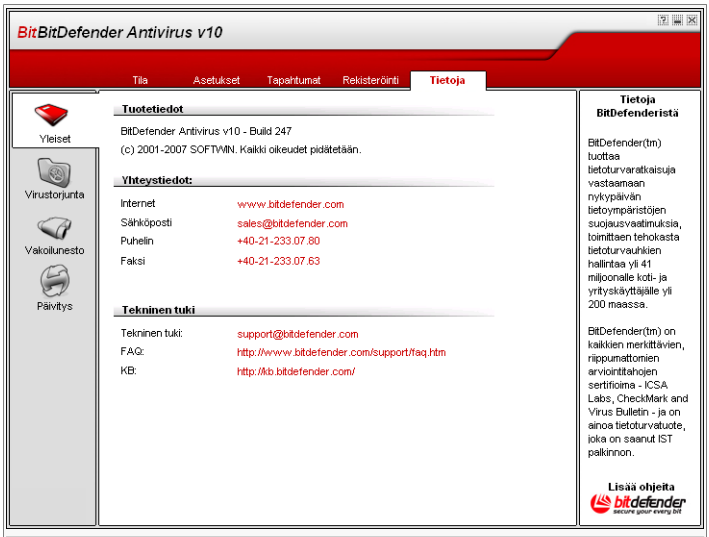
Kuva 6.10. Valmis

Tämä on opastetun asetusten määrittelyn viimeinen vaihe. Voit tehdä vielä muutoksia palaamalla aikaisempiin vaiheisiin valitsemalla **Takaisin**.

Jos et halua muuttaa enää mitään, valitse **Valmis** lopettaaksesi ohjatun asennuksen.

Valitse **Avaa BitDefender tilini** kirjautuaksesi BitDefender tilillesi. Tähän tarvitaan Internet-yhteys.

6.5. Tietoja ohjelmasta



Kuva 6.11. Yleistä tietoa

Tästä osiosta löydät yhteystiedot ja tuotteen tiedot.

BitDefender™ on johtava maailmanlaajuinen tietoturvatarkaisujen toimittaja, joka täyttää nykyajan tietojärjestelmien turvavaatimukset. Yhtiö tarjoaa yhden nopeimmista ja tehokkaimmista tietoturvaohjelmistoista, asettaen uudet standardit uhkien hallintaan, nopeaan havaitsemiseen ja haittojen lieventämiseen. BitDefender toimittaa tuotteita ja palveluita yli 40 miljoonalle koti- ja yrityskäyttäjälle yli 180 maassa.

BitDefender™ on kaikkien merkittävien, riippumattomien tuotearvostelijoiden sertifioima - **ICSA Labs**, **CheckMark** ja **Virus Bulletin**, ja on ainoa tietoturvatuote, joka on saanut **IST Prize** palkinnon.

Lisätietoja BitDefenderistä voit saada vierailemalla osoitteessa: http://www.bitdefender.com.

Luku 7. Virustorjunta

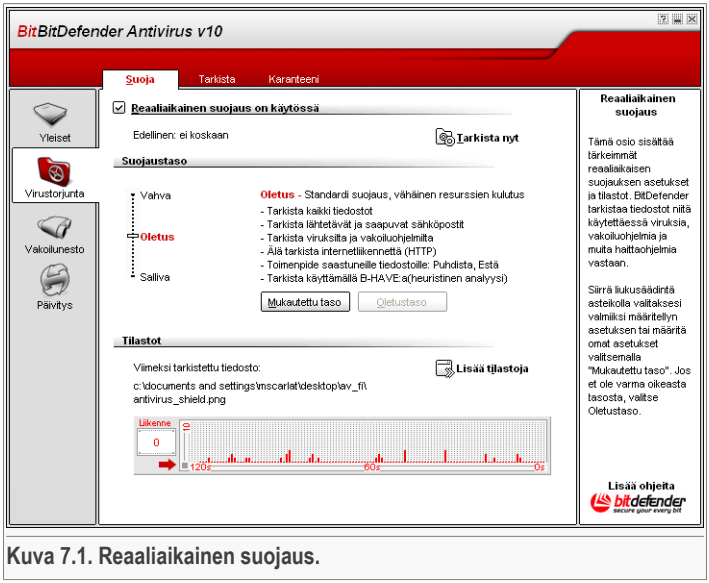
Tämän käyttöoppaan **Virustorjunta** -osio sisältää seuraavat aiheet:

- Käytönaikainen tarkistus
- Manuaalinen tarkistus
- Karanteeni

Huomaa

Saat tarkempia tietoja **Virustorjunta** -osasta lukemalla selostuksen kohdasta "*Virustorjunta*" (p. 29).

7.1. Manuaalinen tarkistus



Kuva 7.1. Reaaliaikainen suojaus.

Tässä osiossa voit konfiguroida **Reaaliaikaisen suojauksen** ja nähdä sen toimintaan liittyviä tietoja. **Reaaliaikainen suojaus** suojaa tietokoneesi tarkistamalla sähköpostiviestit, tiedostolataukset ja käytettävät tiedostot.

Tärkeää

Estääksesi viruksia saastuttamasta tietokonettasi, pidä **Reaaliaikainen suojaus** käytössä.

Osion alareunassa voit nähdä **Reaaliaikaista suojaa** koskevia tilastoja tarkistetuista tiedostoista ja sähköpostiviesteistä. Valitse **Lisää tilastoja**, jos haluat tarkastella tarkempia tietoja näistä tilastoista.

7.1.1. Suojaustaso

Voit valita tarpeisiisi parhaiten sopivan suojaustason. Siirrä liukukytkintä asteikolla asettaaksesi sopivan suojaustason.

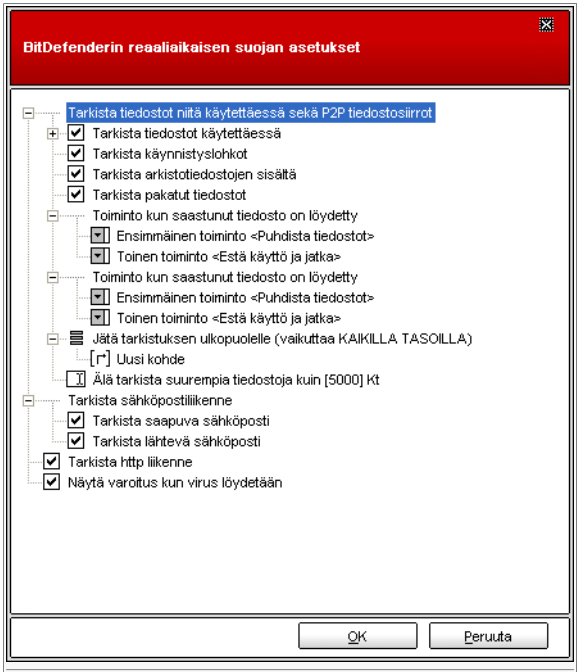
Valittavana on kolme erilaista suojaustasoa:

Suojaustaso	Kuvaus
Salliva	Täyttää perusturvatarpeet. Resurssien kulutus on erittäin alhainen. Ohjelmat ja tuleva sähköposti tarkistetaan vain virusten varalta. Käytössö on sekä perinteinen, tunnisteisiin perustuva tunnistus, että heuristinen tarkistus. Saastuneille tiedostoille tehdään seuraavat toimenpiteet: puhdistus / käytön esto.
Oletus	Tarjoaa normaalisuojauksen. Resurssien kulutus on alhainen. Kaikki tiedostot ja tuleva/lähtevä sähköposti tarkistetaan viruksia ja vakoiluohjelmia vastaan. Käytössä on sekä perinteinen, tunnisteisiin perustuva tunnistus, että heuristinen tarkistus. Saastuneille tiedostoille tehdään seuraavat toimenpiteen: puhdistus / käytön esto.
Vahva	Tarjoaa korkean suoajustason. Resurssien kulutus on kohtuullinen. Kaikki tiedostot, tuleva ja lähtevä sähköposti ja Internet-liikenne tarkistetaan viruksia ja vakoiluohjelmia vastaan. Käytössä on sekä perinteinen, tunnisteisiin perustuva tunnistus, että heuristinen tarkistus. Saastuneille tiedostoille tehdään seuraavat toimenpiteen: puhdistus / käytön esto.

Reaaliaikaisen suojauksen oletusasetukset otetaan käyttöön valitsemalla **Oletus**.

Kokeneet käyttäjät voivat hyödyntää BitDefenderin tarjoamia tarkistusasetuksia. Tarkistus voidaan määritellä ohittamaan tiettyjä tiedostopäätteitä, hakemistoja tai arkistoja jotka tiedetään harmittomiksi. Tämä voi nopeuttaa tarkistusta merkittävästi ja parantaa tietokoneen käytettävyyttä tarkistuksen aikana.

Jos haluat muokata voimassa olevaa lisenssiavainta valitse **Uusi lisenssiavain**. Näytölle avautuu seuraava ikkuna:



Kuva 7.2. Suojausasetukset

Virustarkistuksen vaihtoehdot on järjestetty laajenevaksi valikoksi, samaan tapaan kuin Windowsin resurssienhallinnassa.

Klikkaa ”+” niin valinta avautuu tai ”-” , niin valinta sulkeutuu.

Voit huomata, että joitakin vaihtoehtoja ei voi avata, vaikka niissä onkin ”+” merkki. Syy tähän on se, ettei niitä ole vielä valittu. Voit todeta, että jos valitset ne, voidaan ne avatakin.

- **Tarkista avattavat tiedostot ja P2P-siirtovaihtoehdot** - tarkistaa avattavat tiedostot ja vertaisverkko- tiedonsiirron (Instant Messaging Software-sovellukset kuten: ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Valitse myös tarkistettavat tiedostotyypit.

Valinnat		Kuvaus
Tarkista tiedostot käytettäessä	**Tarkista kaikki tiedostot**	Virukset tarkastetaan kaikista avatuista tiedostoista tyypistä riippumatta.
	Tarkista vain ohjelmatiedostot	Vain ohjelmatiedostot tarkistetaan. Tämä tarkoittaa vain niitä tiedostoja, joissa on seuraava pääte: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`;

Valinnat		Kuvaus
		.cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml ja .nws.
	Tarkista tiedostot määritellyllä päätteellä	Vain ne tiedostot tarkistetaan, joissa on käyttäjän määrittelemä pääte eli tiedostotunniste. Nämä päätteet pitää erottaa ”;” –merkillä.
	Jätä tarkistamatta tiedostot joiden pääte on: []	Tiedostoja, joissa on käyttäjän määrittelemät päätteet eli tunnisteet ei tarkisteta. Nämä päätteet pitää erottaa ”;” –merkillä.
	Tarkista riskiohjelmilta	Tarkistaa riskiohjelmistoilta. Tällaiset tiedostot luokitellaan saastuneiksi. Ohjelmistot, jotka sisältävät mainoskomponentteja voivat lakata toimimasta, jos tämä valinta on käytössä. Valitse **Jätä pois modeemiyhteysohjelmat ja sovellukset tarkistuksesta**, jos et halua tarkistaa tällaisia tiedostoja.
Tarkista levykeasema sitä käytettäessä		Tarkistaa levykeaseman sitä käytettäessä.
Tarkista arkistojen sisältä		Avatut arkistot tarkistetaan. Kun tämä vaihtoehto on valittuna, tietokoneen toiminta hidastuu.
Tarkista pakatut tiedostot		Kaikki pakatut tiedostot tarkistetaan.
Ensimmäinen toiminto		Valitse pudotusvalikosta ensimmäinen toiminto, joka suoritetaan saastuneille tai epäilyttäville tiedostoille.
	Estä avaaminen ja jatka	Saastuneen tiedoston löytyessä sen avaaminen estetään.
	Puhdista tiedosto	Saastunut tiedosto puhdistetaan.
	Tuhoa tiedosto	Saastuneet tiedostot tuhotaan välittömästi ilman varoitusta.

Valinnat		Kuvaus
	Siirrä tiedosto karanteeniin	Siirtää saastuneet tiedostot karanteeniin.
Toinen toiminto		Valitse pudotusvalikosta toinen toiminto, joka suoritetaan saastuneille tiedostoille, jos ensimmäinen toiminto epäonnistuu.
	Estä avaaminen ja jatka	Saastuneen tiedoston löytyessä sen avaaminen estetään.
	Tuhoa tiedosto	Saastuneet tiedostot tuhotaan välittömästi ilman varoitusta.
	Siirrä tiedosto karanteeniin	Siirtää saastuneet tiedostot karanteeniin.
Älä tarkista tiedostoja joiden koko on suurempi kuin [x] Kt		Kirjoita tarkistettavien tiedostojen enimmäiskoko. Jos arvo on 0 Kt, kaikki tiedostot tarkistetaan riippumatta niiden koosta.
Jätä tarkistuksen ulkopuolelle (vaikuttaa KAIKILLA TASOILLA)		Klikkaa "+" merkkiä tämän valinnan kohdalla määritelläksesi kansiot, jotka jätetään tarkistuksen ulkopuolelle. Esiin tulee valinta `Uusi kohde`, jonka valitsemalla avautuu selausnäkymä, josta voit hakea tarkistuksen ulkopuolelle jätettävän kohteen. Tässä valitut kohteet jätetään tarkistuksen ulkopuolelle, riippumatta valitusta turvatasosta (ei ainoastaan **Mukautettu taso**).

- **Tarkista sähköpostiliikenne** - tarkistaa sähköpostiliikenteen.

  Seuraavat vaihtoehdot ovat käytettävissä:

Valinnat	Kuvaus
Tarkista saapuva sähköposti	Tarkistaa kaiken saapuvan sähköpostin.
Tarkista lähtevä sähköposti	Tarkistaa kaiken lähtevän sähköpostin.

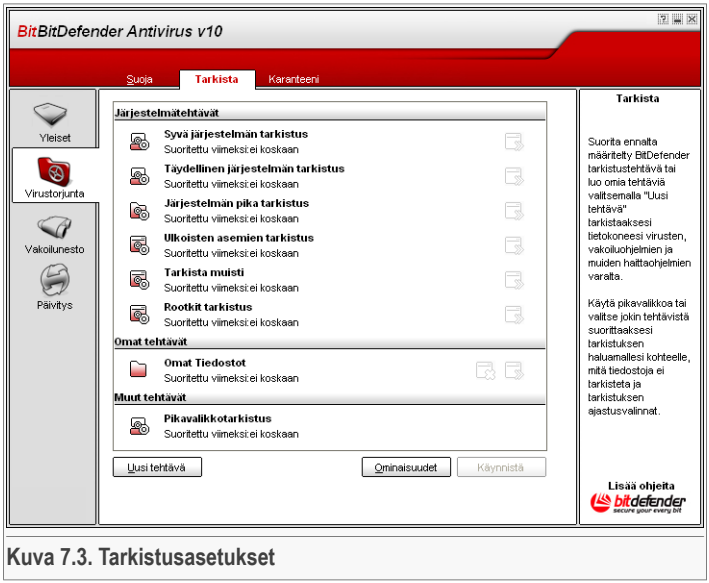
- **Tarkista http liikenne** - tarkistaa http liikenteen.
- **Näytä varoitus, kun virus löydetään** - avaa varoitusikkunan, kun virus löydetään tiedostosta tai sähköpostiviestistä.

Varoitusikkunassa näytetään tiedoston saastuttaneen viruksen nimi, tiedoston polku, BitDefenderin tekemät toimenpiteet sekä linkki BitDefenderin verkkosivulle, josta voit löytää virusta koskevia lisätietoja. Saastuneesta sähköpostista varoitusikkunassa näytetään lisäksi tiedot lähettäjästä ja vastaanottajasta.

Epäilyttävän tiedoston löytyessä, voit käynnistää varoitusikkunasta ohjatun toiminnon, joka opastaa sinua lähettämään tiedoston BitDefenderille tutkittavaksi. Voit liittää mukaan oman sähköpostiosoitteesi, jolloin saat lähettämääsi raporttia koskevia tietoja BitDefenderiltä.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan.

7.2. Manuaalinen tarkistus



Kuva 7.3. Tarkistusasetukset

Tässä osiossa voit konfiguroida BitDefenderin tarkistamaan tietokoneesi.

BitDefenderin tärkein tavoite on pitää koneesi puhtaana viruksista. Tämä toteutuu etupäässä siten, että se pitää uudet virukset poissa koneestasi ja tarkistamalla sähköpostit ja kaikki tietokoneellesi ladatut uudet tiedostot.

On mahdollista, että tietokoneessasi on virus jo ennen kuin olet asentanut BitDefenderin siihen. Tämän vuoksi on oikein hyvä, että teet täydellisen tietokoneen tarkistuksen

heti BitDefenderin asennuksen jälkeen. On myös hyvä tarkistaa tietokone säännöllisesti viruksia vastaan.

7.2.1. Tarkistusasetukset

Manuaalinen tarkistus perustuu tarkistustehtäviin. Käyttäjä voi tarkistaa tietokoneen käyttäen valmiiksi määriteltyjä tarkistustehtäviä tai itse luomiaan tarkistustehtäviä (käyttäjän määrittelemät tehtävät).

Tarkistustehtävissä on kolme eri luokkaa:

- **Järjestelmätehtävät** - sisältää luettelon valmiiksi määritellyistä järjestelmätarkistustehtävistä. Seuraavat tehtävät ovat käytettävissä:

Oletustehtävä	Kuvaus
Järjestelmän syvätarkistus	Tarkistaa koko järjestelmän, mukaanlukien arkistot, viruksia ja vakoiluohjelmia vastaan.
Täydellinen järjestelmän tarkistus	Tarkistaa koko järjestelmän, paitsi arkistot, viruksia ja vakoiluohjelmia vastaan.
Järjestelmän pikatarkistus	Tarkistaa kaikki ohjelmat viruksia ja vakoiluohjelmia vastaan.
Ulkoisten asemien tarkistus	Tarkistaa ulkoiset aseman viruksia ja vakoiluohjelmia vastaan.
Tarkista muisti	Tarkistaa muistin tunnettuja vakoiluohjelmia vastaan.
Rootkit tarkistus	Tarkistaa muistin näkymättömiä haittaohjelmia vastaan.

- **Omat tehtävät** - näyttää käyttäjän luomat tehtävät.

  Tehtävä nimeltä `Omat tiedostot` luodaan. Käytä tätä tehtävää tarkistaaksesi tiedostot `Omat tiedostot` kansiosta.

- **Muut tehtävät** - sisältää luettelon muista tehtävistä. Nämä tarkistustehtävät viittaavat vaihtoehtoisiin tarkisustehtäviin, joita ei voida suorittaa tästä valikosta. Tässä voit vain muokata näiden asetuksia tai tarkastella niihin liittyviä tarkistusraportteja.

Jokaisen tehtävän oikealla puolella on käytettävissä kolme painiketta:

- **Ajastettu tehtävä** - osoittaa, että valittu tehtävä on ajastettu suoritettavaksi myöhemmin. Valitse tämä siirtyäksesi Ajastus osioon **Asetukset** ikkunassa, muokataksesi tehtävän asetuksia.

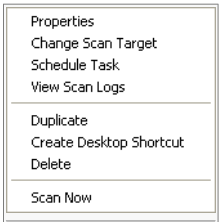
- **Poista** - poistaa valitun tehtävän.

Huomaa
Ei saatavilla järjestelmän tehtäviin. Et voi poistaa järjestelmän tehtävää.

- **Tarkista nyt** - suorittaa valitun tarkistustehtävän välittömästi.

7.2.2. Pikavalikko

Pikavalikko on käytettävissä jokaiselle tehtävälle. Klikkaa hiiren oikealla painikkeella tehtävän kohdalla sen avaamiseksi.



Kuva 7.4. Pikavalikko

Seuraavat vaihtoehdot ovat käytettävissä pikavalikoissa:

- **Tarkista nyt** - Suorittaa valitun tehtävän välittömästi.
- **Vaihda tarkistuksen kohde** - avaa **Ominaisuudet** -ikkunan **Tarkistuspolku** -välilehden, josta voit vaihtaa valitun tehtävän tarkistuskohdetta.
- **Ajastus** - avaa **Ominaisuudet** -ikkunan **Ajastus** -välilehden, jossa voit määritellä valitun tehtävän ajastuksen.
- **Tarkistusloki** - avaa **Ominaisuudet** -ikkunan **Tarkistusloki** -välilehden, josta voit nähdä valitun tehtävän suorittamisen jälkeen luodun raportin.
- **Kopioi** - tekee valitusta tehtävästä kopion.

Huomaa
Tämä on käytännöllinen tapa luoda uusia tehtäviä, koska voit muokata kopioidun tehtävän asetuksia.

- **Luo pikakuvake työpöydälle** - luo valitusta tehtävästä pikakuvakkeen työpöydälle.
- **Poista** - poistaa valitun tehtävän.

Huomaa
Ei saatavilla järjestelmän tehtäviin. Et voi poistaa järjestelmän tehtävää.

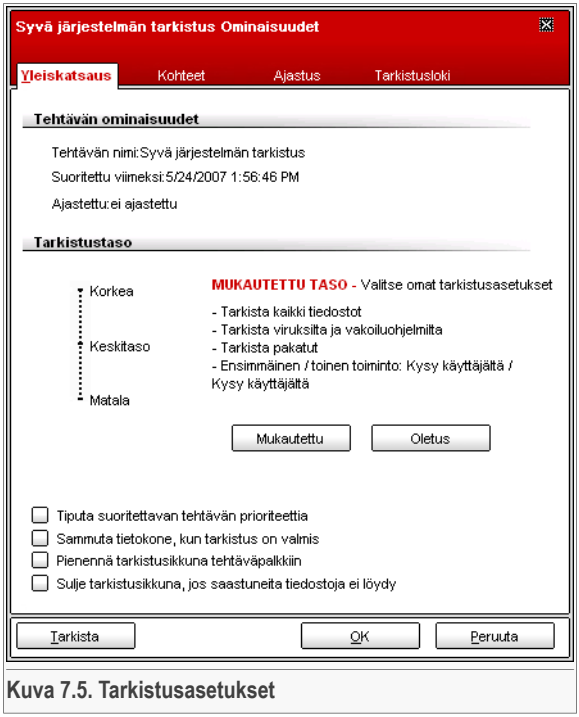
- **Ominaisuudet** - avaa **Ominaisuudet** -ikkunan **Yleiskatsaus** -välilehden, josta voit vaihtaa valitun tehtävän asetuksia.

Tärkeää
Johtuen niiden erityisestä luonteesta, **Ominaisuudet** ja **Tarkistusloki** valinnat eivät ole käytettävissä **Sekalaiset tehtävät** luokassa.

7.2.3. Tehtävän ominaisuudet

Jokaisella tarkistustehtävällä on oma **Ominaisuudet** -ikkuna, jossa voit määritellä tarkistusasetukset, tarkistuskohteen, ajastaa tehtävän tai tarkastalle tarkistusraportteja. Siirtyäksesi tähän ikkunaan, valitse **Ominaisuudet** (tai klikkaa hiiren oikealla painikkeella tehtävän kohdalla ja valitse **Ominaisuudet**).

Tarkistusasetukset



Kuva 7.5. Tarkistusasetukset

Tästä voit nähdä tietoja tehtävästä (nimi, suoritettu viimeksi ja ajastuksen tilan) ja muokata tarkistusasetuksia.

Tarkistustaso

Ensimmäiseksi sinun pitää valita tarkistustaso. Siirrä liukukytkintä asteikolla valitaksesi sopivan tason.

Valittavana on kolme tarkistustasoa:

Suojaustaso	Kuvaus
Matala	Tarjoaa perustason tunnistustarkkuuden. Resurssien kulutus on hyvin alhainen. Ohjelmat tarkistetaan vain virusten varalta. Tunnisteisiin perustuvan tarkistuksen lisäksi, käytössä on myös heuristinen tarkistus. Saastuneille kohteille suoritetaan seuraavat toimenpiteen: puhdistus / siirto karanteeniin.
Keskitaso	Tarjoaa hyvän tunnistustarkkuuden. Resurssien kulutus on kohtuullinen. Kaikki tiedostot tarkistetaan viruksien ja vakoiluohjelmien varalta. Tunnisteisiin perustuvan tarkistuksen lisäksi käytössä on myös heuristinen tarkistus. Saastuneille kohteille suoritetaan seuraavat toimenpiteen: puhdistus / siirto karanteeniin.
Korkea	Tarjoaa korkean tunnistustarkkuuden. Resurssien kulutus on suuri. Kaikki tiedostot ja arkistot tarkistetaan viruksien ja vakoiluohjelmien varalta. Tunnisteisiin perustuvan tarkistuksen lisäksi käytössä on myös heuristinen tarkistus. Saastuneille kohteille suoritetaan seuraavat toimenpiteen: puhdistus / siirto karanteeniin.

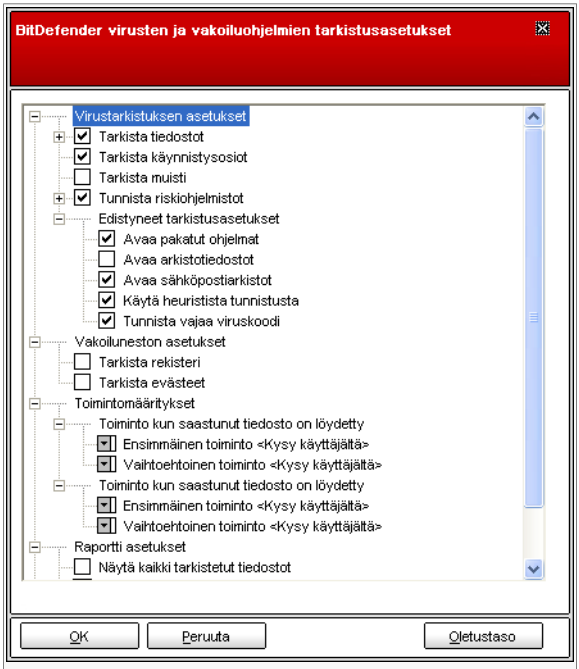
Tärkeää

Rootkit tarkistus sisältää samat tarkistustasot, mutta erilaiset valinnat:

- **Matala** - Vain prosessit tarkistetaan. Havaituille kohteille ei suoriteta mitään toimenpiteitä.
- **Keskitaso** - tiedostot ja prosessit tarkistetaan piilotettujen kohteiden varalta. Havaituille kohteille ei suoriteta mitään toimenpiteitä.
- **Korkea** - tiedostot ja prosessit tarkistetaan piilotettujen kohteiden varalta. Havaitut kohteet nimetään uudelleen.

Kokeneet käyttäjät voivat haluta hyötyä hakuasetusten eduista, joita BitDefender tarjoaa. Tarkistustoiminto voidaan asettaa ohittamaan harmittomiksi tietämiesi tiedostopäätteiden, kansioiden tai arkistojen yli. Tämä nopeuttaa virustarkistusta ja parantaa koneesi toimintakykyä virustarkistuksen aikana.

Valitse **Mukautettu** tehdäksesi omat tarkistuasetukset.



Kuva 7.6. Tarkistusasetukset

Virustarkistuksen vaihtoehdot on järjestetty laajenevaksi valikoksi, samaan tapaan kuin Windowsin resurssienhallinnassa.

Tarkistusvalinnat on jaettu viiteen luokkaan:

- **Virustarkistuksen asetukset**
- **Vakoiluneston asetukset**
- **Toimintomääritykset**
- **Raporttiasetukset**
- **Muut valinnat**

Klikkaa ”+” niin valinta avautuu tai ”-” , niin valinta sulkeutuu.

Tärkeää

Rootkit tarkistus -tehtävässä on vain kolme luokkaa: **Rootkit tarkistus**, **Raportointi** ja **Muut valinnat**. Ensimmäisessä luokasta voit valita, mitä tarkistetaan (tiedosot vai muisti, tai molemmat) ja voit määritellä mitä havaituille kohteille tehdään (**Ei mitään**

(kirjoittaa lokiin)/Nimeä uudelleen). Kaksi muuta luokkaa ovat samanlaisia kuin on kuvattu seuraavassa.

- Määrittele tarkistettavat kohdetyypit (arkistot, sähköpostit, jne) ja muut valinnat. Tämä tehdään kohdassa **Virustarkistuksen asetukset**.

Valinnat		Kuvaus
Tarkista tiedostot	**Tarkista kaikki tiedostot**	Virukset tarkastetaan kaikista avatuista tiedostoista tyypistä riippumatta.
	Tarkista vain ohjelmatiedostot	Viruksia haetaan vain ohjelmatiedostoista. Tämä tarkoittaa sitä, että vain ne tiedostot tutkitaan, joiden pääte on seuraavan luettelon mukainen: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` ja `nws`.
	Tarkista tiedostot määritellyllä päätteellä	Vain ne tiedostot tarkistetaan, joissa on käyttäjän määrittelemä pääte eli tiedostotunniste. Nämä päätteet pitää erottaa ”;” –merkillä.
	Takistuksen ulkopuolelle jätettävät tiedostotyypit	Tiedostoja, joissa on käyttäjän määrittelemät päätteet eli tunnisteet ei tarkisteta. Nämä päätteet pitää erottaa ”;” –merkillä.
Tarkista käynnistyssektorit		Hakee virukset järjestelmän käynnistyssektorilta.
Tarkista muisti		Tarkistaa tietokoneen muistin viruksien ja muiden haittaohjelmien varalta.
Tunnista riskitiedostot		Etsii muita kuin viruksia, kuten soitto- ja mainosohjelmia. Näitä tiedostoja voidaan käsitellä kuten saastuneita tiedostoja. Ohjelmistot, jotka sisältävät mainoskomponentteja, saattavat lakata toimimasta, jos tätä valintaa käytetään.

Valinnat		Kuvaus
		Valitse **Ohita sovellukset ja soitto-ohjelmat**, jos haluat jättää nämä tarkistuksen ulkopuolelle.
Toimintomääritykset	**Tarkista pakatut ohjelmat**	Tarkistaa pakatut tiedostojen sisällön.
	Avaa arkistot	Hakee virukset arkistojen sisällöstä.
	Avaa sähköpostiarkistot	Hakee virukset postiarkistojen sisällöstä.
	Käytä heuristista tunnistusta	Käyttää heuristista menetelmää virusten hakuun tiedostoista. Heuristisen hakumenetelmän tarkoituksena on tunnistaa uudet virukset perustuen tiettyihin malleihin ja algoritmeihin, ennen kuin viruksen määrittely löytyy. Vääriä hälytysviestejäkin voi ilmetä. Kun sellainen tiedosto on tunnistettu, se luokitellaan epäillyksi. Tällaisissa tapauksissa suosittelemme, että lähetät tiedoston BitDefenderille tutkittavaksi.
	Tunnista vajaa viruskoodi	Tunnistaa vajaat haittaohjelmat, jotka eivät täysin vastaa tunnistemäärittelyjä.

- Määrittele kohteet, jotka tarkistetaan vakoiluohjelmien varalta(rekisteri, evästeet). Tämä tehdään kohdassa **Vakoiluneston asetukset**.

Valinnat	Kuvaus
Tarkista rekisteri	Tarkistaa rekisterimerkinnät.
Tarkista evästeet	Tarkistaa evästetiedostot.

- Määrittele toiminto saastuneille tai epäilyttäville tiedostoille. Avaa **Toimintomääritykset** -luokka nähdäksesi kaikki näitä tiedostoja koskevat toiminnot.

  Valitse toiminnot, jotka suoritetaan kun saastunut tai epäilyttävä tiedosto havaitaan. Voit määritellä erilaisia toimintoja saastuneille ja epäilyttäville tiedostoille. Voit valita myös vaihtoehtoisen toiminnon, jos ensimmäinen epäonnistuu.

Toimenpide	Kuvaus
Ei mitään (kirjaa lokiin)	Saastuneille tiedostoille ei tehdä mitään. Nämä tiedostot näkyvät raporttitiedostossa.
Kysy käyttäjältä	Kun saastunut tiedosto havaitaan, esiin tulee ikkuna, jossa käyttäjää kehotetaan valitsemaan tiedostolle suoritettava toiminto. Riippuen tiedoston tärkeydestä voit valita puhdistetaanko, eristetäänkö se karanteeniin vai tuhotaanko tiedosto.
Puhdista tiedostot	Saastunut tiedosto puhdistetaan.
Tuhoa tiedostot	Saastuneet tiedostot tuhotaan välittömästi ilman varoitusta.
Siirrä tiedostot Karanteeniin	Siirtää saastuneet tiedostot karanteeniin.
Nimeä tiedostot uudelleen	Vaihtaa saastuneiden tiedostojen tunnisteen. Saastuneiden tiedostojen uusi pääte eli tunniste on `.vir`. Nimeämällä saastuneet tiedostot uudelleen estetään niiden mahdollinen suorittaminen ja siten myös tartunnan leviäminen tai muu haitanteko. Samalla ne voidan tallentaa myöhempää tutkimusta ja analysointia varten.

Tärkeää

Nimeä tiedostot uudelleen tekee saman toiminnon kuin tehdään piilotetuille tiedostoille (rootkit). Havaittujen tiedostojen uusi pääte on muotoa `.bd.ren`. Nimeämällä havaitut tiedostot uudelleen, estetään haittaohjelmien suorittaminen ja niiden leviäminen. Samalla ne voidaan tallentaa myöhempää analyysia varten.

- Määrittele vaihtoehdot raporttitiedostoille. Avaa **Raporttivaihtoehdot** nähdäksesi kaikki mahdolliset vaihtoehdot.

Valinnat	Kuvaus
Näytä kaikki tarkistetut tiedostot	Tekee raporttitiedostoon luettelon kaikista tarkistetuista tiedostoista ja niiden tilasta (saastunut tai ei-saastunut). Kun tämä vaihtoehto on valittu, tietokoneen toiminta hidastuu.
Poista vanhemmat kuin [x] päivää vanhat lokitiedostot	Tässä kohdassa voidaan määritellä, kuinka kauan raportteja säilytetään Tarkistusloki -osiossa. Valitse

Valinnat	Kuvaus
	tämä ja kirjoita uusi aikaväli. Oletusaikaväli on 180 päivää.

Huomaa

Raporttitiedostot voidaan nähdä Tarkistusloki -osiossa, **Ominaisuudet** -ikkunassa.

- Määrittele muut valinnat. Avaa **Muut valinnat** -luokka, josta voit valita seuraavat vaihtoehdot:

Valinnat	Kuvaus
Lähetä epäilyttävät tiedostot BitDefenderille	Sinua kehotetaan lähettämään kaikki epäilyttävät tiedostot BitDefenderille tarkistuksen päätyttyä.

Jos valitset **Oletustaso**, oletusasetukset ladataan käyttöön.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan.

Muut asetukset

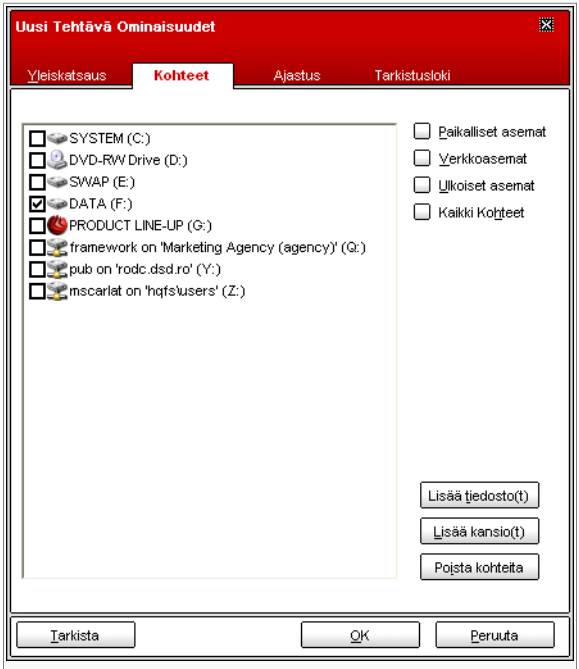
Tarksitusprosesseissa on käytettävissäsä myös joukko yleisiä asetuksia:

Valinnat	Kuvaus
Tiputa suoritettavan tehtävän prioriteettiä	Alentaa tarkistusprosessin prioriteettia. Tämä nopeuttaa muita ohjelmia ja pidentää tarkistusprosessiin kuluvaa aikaa.
Sulje tietokone tarkistuksen päätyttyä	Sammuttaa tietokoneen tarkistusprosessin päätyttyä.
Lähetä epäilyttävät tiedostot BitDefenderille	Sinua kehotetaan lähettämään kaikki epäilyttävät tiedostot BitDefenderille tarkistuksen päätyttyä.
Pienennä tarkistusikkuna ilmaisinalueelle käynnistyksen yhteydessä	Pienentää tarkistusikkunan käynnistyksen jälkeen ilmaisinalueelle. Avataksesi sen, kaksoisklikkaa BitDefender kuvaketta.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan. Suorittaaksesi tehtävän, valitse **Tarkista**.

Kohteet

Valitse tehtävä, jonka jälkeen valitse **Ominaisuudet** ja **Kohteet** –välilehti.



Kuva 7.7. Kohteet

Tässä voit valita tarkistuksen kohteen.

Osio sisältää seuraavat painikkeet:

- **Lisää tiedosto(t)** - avaa selausikkunan, jossa voit valita tarkistettavat tiedostot.
- **Lisää kansio(t)** - samoin kuin edellä, mutta voit valita kansiot, jotka haluat BitDefenderin tarkistavan yksittäisten tiedostojen sijasta.

Huomaa

Voit myös käyttää vedä ja pudota menetelmää lisätäksesi tiedostoja / kansioita luetteloon.

- **Poista kohteita** - poistaa tiedostot / kansiot, jotka on aikaisemmin valittu luettelosta tarkistuksen kohteiksi.

Huomaa

Vain ne tiedostot / kansiot jotka lisättiin jälkeenpäin voidaan poistaa, mutta ei niitä, jotka BitDefender ”näkee” automaattisesti.

Edellisten määritelmien lisäksi on myös olemassa vaihtoehto, joka mahdollistaa hakukohteiden nopean valinnan.

- **Paikalliset asemat** - paikallisten levyasemien tarkistamiseksi.
- **Verkkoasemat** - kaikkien verkkoasemien tarkistamiseksi.
- **Ulkoiset asemat** - ulkoisten asemien tarkistamiseksi (CD-ROM, levykeasema).
- **Kaikki kohteet** - tarkistus suoritetaan kaikille asemille, riippumatta siitä ovatko ne verkossa, paikallisia tai ulkoisia.

Huomaa

Jos haluat BitDefenderin tarkistavan koko tietokoneesi viruksia vastaan, valitse **Kaikki kohteet**.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan. Suorittaaksesi tehtävän, valitse **Tarkista**.

Ajastus

Valitse tehtävä, jonka jälkeen valitse **Ominaisuudet** ja **Ajastus** –välilehti.

Kuva 7.8. Ajastus

Tässä voit nähdä onko tehtävä on ajastettu sekä muokata ajastuksen asetuksia.

Tärkeää

Tarkistusprosessi kestää jonkin aikaa ja toimii parhaiten jos suljet kaikki muut ohjelmat. On siksi hyvä ajastaa tarkistustehtävät sellaiseen ajankohtaan, jolloin et käytä tietokonetta aktiivisesti.

Tehtävän ajastuksen yhteydessä on valittava yksi seuraavista vaihtoehdoista:

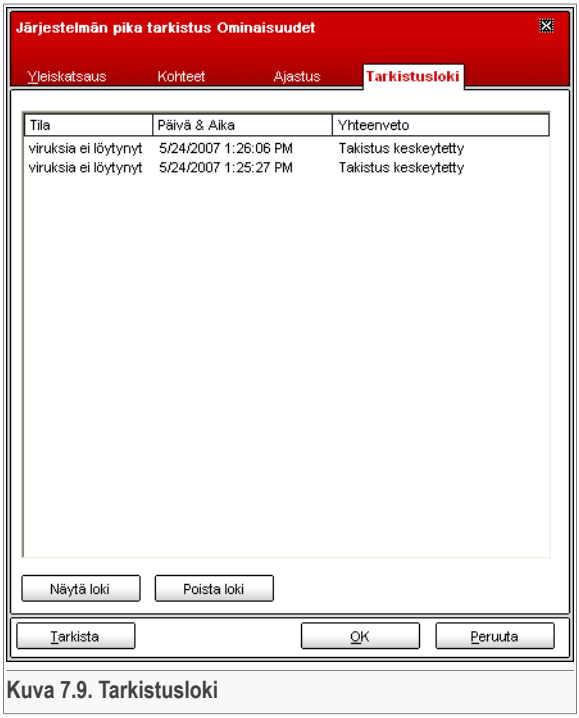
- **Ei ajastettu** - käynnistää tarkistuksen vain käyttäjän toimesta.
- **Kerran** - käynnistää tarkistuksen vain keran, tiettynä ajakohtana. Määritä tarkistuksen ajankohta kohdassa **Aloitus pvm / Aloitusaika**.
- **Säännöllisesti** - käynnistää tarkistuksen toistuvasti tietyin aikavälein (tunnit, päivät, viikot, kuukaudet, vuodet) alkaen määriteltynä päivänä ja kellonaikana.

Jos haluat, että tarkistus toistuu säännöllisin aikavälein, valitse **Säännöllisesti** kirjoita kohtaan **Joka** arvo minuutteina/tunteina/päivinä/kuukausina/vuosina osoittamaan tehtävän toistumisvälin. Myös aloituspäivä ja kellonaika pitää määritellä kohtaan **Aloitus pvm / Aloitusaika**.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan. Suorittaaksesi tehtävän, valitse **Tarkista**.

Tarkistusloki

Valitse tehtävä, jonka jälkeen valitse **Ominaisuudet** ja **Tarkistusloki** –välilehti.



Kuva 7.9. Tarkistusloki

Tässä voit nähdä raportit, jotka luodaan joka kerta kun tarkistustehtävä on suoritettu. Jokainen tiedosto sisältää tietoja tarkistustuloksista (puhdas/saastunut), päivä ja kellonaika jolloin tarkistus suoritettiin ja yhteenvedon.

Käytettävissä on kaksi painiketta:

- **Näytä loki** - avaa valitun raportin.
- **Poista loki** - poistaa valitun lokitiedoston.

Samat toiminnot ovat käytettävissä pikavalikossa, joka avautuu kun klikkaat lokitiedostoa hiiren oikealla painikkeella.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan. Suorittaaksesi tehtävän, valitse **Tarkista**.

7.2.4. Manuaalisen tarkistuksen mallit

BitDefenderissä on mahdollista suorittaa kolmentyyppisiä manuaalisia tarkistuksia:

- Välitön tarkistus - suorita tehtävä kohdasta järjestelmätehtävät;
- Pikavalikkotarkistus - klikkaa hiiren oikealla painikkeella tiedostoa tai kansiota ja valitse BitDefender Antivirus v10;
- Vedä ja pudota haku - vedä ja pudota tiedosto tai kansio toimintopalkin päälle;

Välitön tarkistus

Tarkistaakesi tietokoneesi tai osan siitä, voit käyttää valmiita tarkistutehtäviä tai voit luoda omia tehtäviä. Tehtävien luomiseksi on kaksi tapaa:

- Kopioi olemassa oleva tehtävä, nimeä se uudelleen ja tee tarvittavat muutokset Ominaisuudet ikkunassa;
- Valitse **Uusi tehtävä** luodaksesi uuden tehtävän ja konfiguroi sitä.

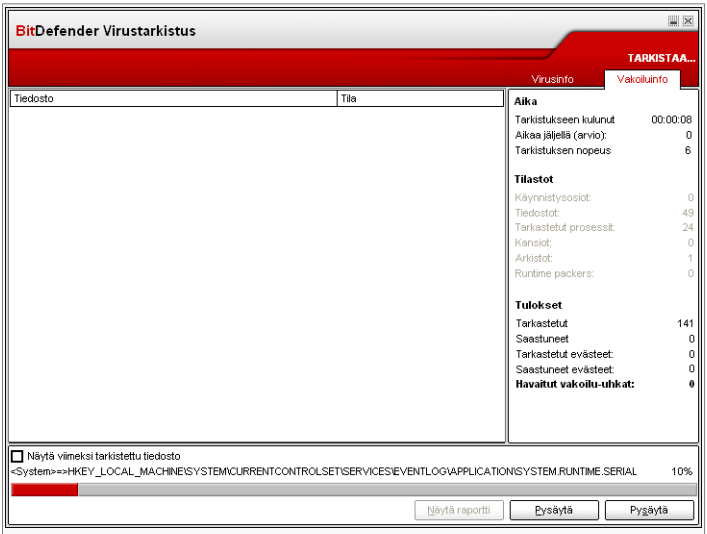
Jotta BitDefender voisi suorittaa täydellisen virustarkistuksen, pitää kaikki avoimet ohjelmat sulkea. Erityisesti sähköpostiohjelman (esim. Outlook, Outlook Express, Eudora) sulkeminen on tärkeää.

Ennen kuin annat BitDefenderin käynnistää tarkistuksen, varmista, että BitDefenderin virustunnisteet ovat ajan tasalla, koska uusia viruksia löytyy ja tunnistetaan joka päivä. Voit tarkistaa viimeisimmän päivityksen Päivitys -osan yläosasta.

Aloittaaksesi tarkistuksen, käytä jotakin seuraavista menetelmistä:

- kaksoisklikkaa luettelosta haluamaasi tarkistustehtävää.
- valitse **Tarkista** tehtävän ominaisuusikkunassa.
- valitse tehtävä ja sen jälkeen valitse **Tarkista NYT**.

Esiin tulee tarkistusikkuna.



Kuva 7.10. Tarkistusikkuna

Ilmaisinalueelle ilmestyy kuvake, kun tarkistusprosessi on käynnissä.

Tarkistuksen aikana BitDefender näyttää tarkistuksen edistymisen ja varoittaa, jos uhkia löydetään. Oikeassa reunassa näet tarkistusprosessin tilastotietoja. Tarkistuskohteesta riippuen, näytetään vakoiluohjelma- ja/tai virustietoja. Jos molempia tietoja on näkyvissä, valitse välilehdistä nähdäksesi lisätietoja vakoiluohjelma- tai virustarkistusprosessista.

Valitse **Näytä viimeksi tarkistettu tiedosto**, niin vain viimeksi tarkistettua tiedostoa koskevat tiedot ovat näkyvissä.

Huomaa

Tarkistuprosessi voi kestää jonkin aikaa, riippuen tarkistuksen valinnoista.

Käytettävissä on kolme painiketta:

- **Stop** - avaa uuden ikkunan, josta voit lopettaa tarkistusprosessin. Valitse **Kyllä**&**Sulje** lopettaaksesi tarkistuksen.

Huomaa

Jos tarkistuksen aikana löydetään epäilyttäviä tietoja, sinua pyydetään lähettämään ne BitDefenderille.

- **Pysäytä** - pysäyttää väliaikaisesti tarkistusprosessin – voit jatkaa sitä valitsemalla **Jatka**-painiketta.
- **Näytä raportti** - avaa virustarkistusraportin.

Huomaa

Jos klikkaat tehtävää oikealla hiiren painikkeella, pikavalikko tarkistusikkunan hallintaan avautuu. Valinnat (**Pysäytä / Jatka**, **Lopeta** and **Lopeta&Sulje**) ovat samanlaisia kuin tarkistusikkunan painikkeissa.

Jos **Kysy käyttäjältä** valinta on käytössä Ominaisuudet ikkunassa, saastuneen tiedoston löytyessä ilmaantuu ikkuna, jossa sinulta kysytään saastuneelle tiedostolle suoritettava toimenpide.

Nyt voit nähdä tiedoston nimen ja viruksen nimen.

Valitse yksi seuraavista toiminnoista, jota sovelletaan saastuneelle tiedostolle:

- **Puhdista** - puhdistaa saastuneen tiedoston;
- **Tuhoa** - tuhoaa saastuneen tiedoston;
- **Siirrä karanteeniin** - siirtää saastuneen tiedoston karanteeniin;
- **Hylkää** - jättää tartunnan ilman toimenpiteitä, saastuneelle tiedostolle ei tehdä mitään.

Jos tarkistat kansion ja haluat, että sama toiminto suoritetaan kaikille saastuneille tiedostoille, valitse **Käytä kaikkiin**.

Kuva 7.11. Toiminnon valinta

Huomaa

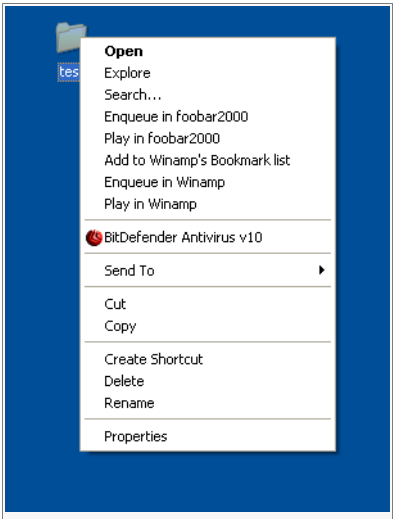
Ellei **Puhdista** vaihtoehto ole käytössä, tiedostoa ei voida puhdistaa. Tällöin paras valinta on eristää se karanteenivyöhykkeelle ja lähettää BitDefenderille analysoitavaksi tai sen voi myös tuhota.

Valitse **OK**.

Huomaa

Raporttitiedosto tallennetaan automaattisesti suoritettavan tehtävän Tarkistusloki osioon **Ominaisuudet** ikkunassa.

Pikavalikko tarkistus



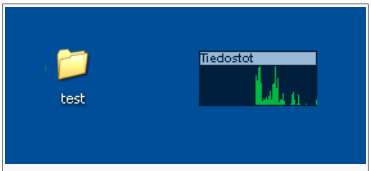
Kuva 7.12. Pikavalikko tarkistus

Klikkaa hiiren oikealla painikkeella tiedostoa tai kansiota, jonka haluat tarkistaa ja valitse **BitDefender Antivirus v10**.

Voit muokata tarkistusvalintoja ja tarkastella raporttitiedostoja valitsemalla Ominaisuudet, tehtävän **Pikavalikkotarkitus** kohdalla.

Vedä ja pudota tarkistus

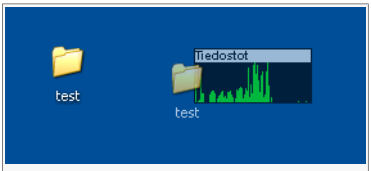
Vedä tiedosto tai kansio, jonka haluat tarkistaa **Aktiviteetti ikkunaan** kuten alla näytetään.



Kuva 7.13. Vedä tiedosto

Jos saastunut tiedosto havaitaan Varkoitus ikkuna Ilmestyy ja kysyy mikä toiminto suoritetaan saastuneelle tiedostolle.

Molemmissa vaihtoehtoisissa tarkistuksissa (Pikavalikkotarkistus ja Vedä&pudota tarkistus), tarkistusikkuna [70] aukeaa.



Kuva 7.14. Pudota tiedosto

7.2.5. Rootkit tarkistus

BitDefender tulee ratkaisemaan uusimmatkin tietoturvauhat esittelemällä Rootkit tunnistuksen tehokkaassa virustorjunta ja vakoiluohjelma hakumoottorissa. BitDefender pystyy nyt tunnistamaan Rootkit ohjelmat etsimällä piiloitettuja tiedostoja, kansioita ja prosesseja. BitDefender pystyy suojaamaan järjestelmän uudelleen nimeämällä haittaohjelmat, joita rootkitit käyttävät.

Kun haluat tarkistaa järjestelmän rootkittien varalta, niin suorita **Rootkit Tarkistus** tehtävä, niin tarkistusikkuna ilmestyy näkyville.

Tärkeää

Kun suoritat rootkit tarkistusta, on suositeltavaa, että asetat BitDefenderin niin, että se ei tee mitään toimintoa piiloitetuille tiedostoille.

Tarkistuksen päätteeksi näet tulokset. Jos piiloitettuja tiedostoja on tunnistettu, tarkista ne varovasti: tunnistetut piilotiedostot saattavat aiheuttaa mahdollisen tunkeutumisen järjestelmään.

Jos olet varma, että havaitut tiedostot ovat osa haittaohjelmaa, suosittelemme, että asetat toiminnoksi **Nimeä uudelleen** ja suoritat **Rootkit tarkistus** tehtävän uudelleen. Näin toimimalla piilotettujen tiedostojen toiminta estetään.

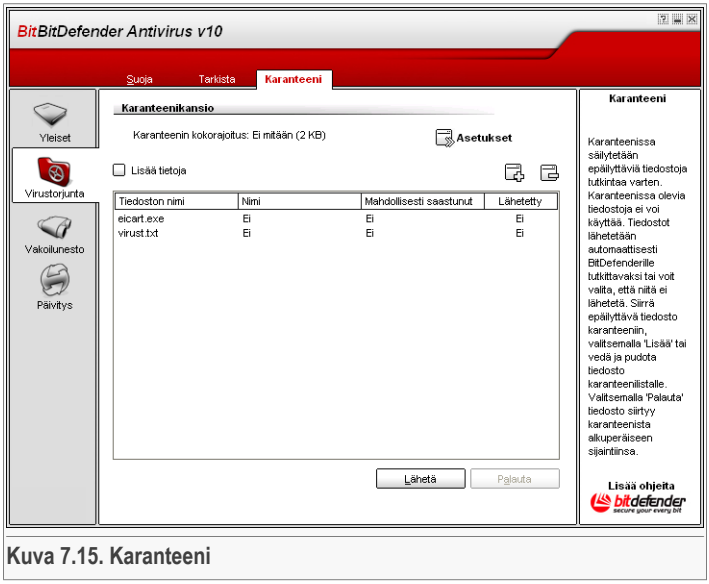
Varoitus

KAIKKI PIILOTETU TIEDOSTOT EIVÄT OLE HAITTAOHJELMIA! Ennen kuin nimeät piilotetut tiedostot uudelleen, varmista etteivät ne ole osa järjestelmätiedostoja tai jonkin luotettavan sovelluksen osia. Tällaisten tiedostojen nimeäminen uudelleen voisi tehdä järjestelmästäsi epävakaan.

Tärkeää

Jos järjestelmäsi on joutunut hakkeroinnin kohteeksi, on vain yksi täysin varma keino päästä eroon tunkeutujasta; järjestelmän uudelleen asentaminen.

7.3. Karanteeni



Kuva 7.15. Karanteeni

BitDefender mahdollistaa saastuneiden tai epäilyttävien tiedostojen eristämisen turvalliselle alueelle, jota kutsutaan Karanteeniksi. Eristämällä tällaiset tiedostot karanteeniin, riski tietokoneen saastumisesta poistuu ja samalla saat mahdollisuuden lähettää tällaiset tiedostot edelleen tarkistettaviksi BitDefenderille.

Antivirusohjelman komponentti, joka varmistaa eristettyjen tiedostojen hallinnan on **Karanteeni**. Tämä osa on suunniteltu lähettämään saastuneet tiedostot automaattisesti BitDefenderille.

Kuten ehkä olet huomannut, **Karanteeni** -osio sisältää luettelon kaikista tähän mennessä eristetyistä tiedostoista. Jokaisesta tiedostosta on ilmoitettu sen nimi, koko, eristyspäiväys ja tarkistettavaksi lähetyksen päiväys. Lisätietoja karanteenitiedostoista saat valitsemalla **Lisää tietoja**.

Huomaa

Kun virus on karanteenissa, se ei voi aiheuttaa mitään harmia, koska se ei voi käynnistyä eikä sitä voi lukea.

Valitse **Lisää**, lisätäksesi karanteeniin tiedoston, jota epäilet saastuneeksi. Tämä avaa ikkunan, josta voit hakea ja valita kyseisen tiedoston. Näin toimimalla tiedosto kopioidaan karanteeniin. Jos haluat siirtää tiedoston karanteeniin, sinun täytyy valita kohta **Poista alkuperäisestä sijainnista**. Nopeampi tapa lisätä epäilyttäviä tiedostoja karanteeniin on käyttää vedä&pudota toimintoa.

Poistaaksesi valitun tiedoston karanteenista, valitse **Poista**. Jos haluat palauttaa tiedoston alkuperäiseen sijaintiinsa, valitse **Palauta**.

Voit lähettää minkä tahansa tiedoston karanteenista BitDefenderille valitsemalla **Lähetä**.

Tärkeää

Ennen lähettämistä sinun täytyy määritellä joitakin tietoja. Valitse **Asetukset** ja täydennä kentät **Lähetysasetukset** -osiossa seuraavaksi kuvatulla tavalla.

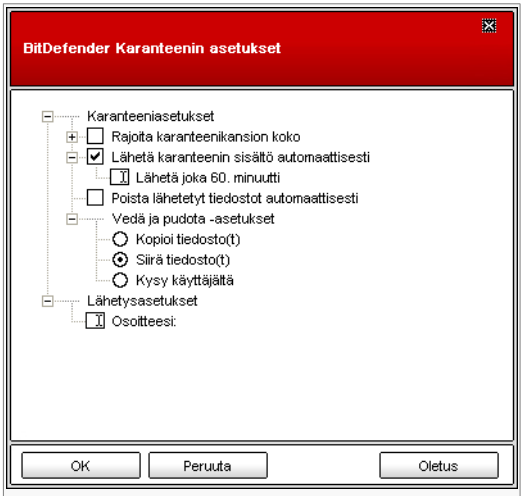
Valitse **Asetukset** jos haluat muokata karanteenin lisäasetuksia. Tämä avaa uuden ikkunan.

Karanteeniasetukset on jaettu kahteen ryhmään:

- **Karanteeniasetukset**
- **Lähetysasetukset**

Huomaa

Klikkaa ”+” niin valinta avautuu tai ”-” , niin valinta sulkeutuu.



Kuva 7.16. Karanteeniasetukset

Karanteeniasetukset

- **Rajoita karanteenikansion koko** - tarkkailee karanteenikansion kokoa. Oletuskoko on 12000kt. Jos haluat muuttaa kokoa, kirjoita uusi koko kenttään.

  Jos valitset **Poista automaattisesti vanhat tiedostot**, karanteenin ollessa täynnä ja uutta tiedostoa lisättäessä, vanhimmat tiedostot karanteenissa poistetaan automaattisesti tilan vapauttamiseksi uusille tiedostoille.

Huomaa

Oletusasetuksena karanteenikansiolla ei ole kokorajoitusta.

- **Lähetä karanteenin sisältö automaattisesti** - lähettää karanteenitiedostot automaattisesti BitDefenderille tarkempaan analyysiin. Kahden peräkkäisen lähetyksen väli voidaan määritellä syöttämällä arvo minuutteina **Lähetä joka x minuutti** -kenttään.
- **Automaattinen poisto** - poistaa automaattisesti karanteenitiedoston, kun lähetys BitDefenderille on tapahtunut.
- **Vedä & pudota asetukset** - jos käytät vedä & pudota-menetelmää tiedostojen lisäämiseksi karanteeniin, voit valita käsittelyn: kopioi, siirrä tai kehota.

Lähetysasetukset

- **Osoite** - lisää sähköpostiosoitteesi, jos haluat asiantuntijoiltamme palautetta lähettästäsi epäillystä tiedostosta.

Valitse **OK** tallentaaksesi muutokset. Jos valitset **Oletus**, oletusvalinnat ladataan käyttöön.

Luku 8. Vakoilunesto

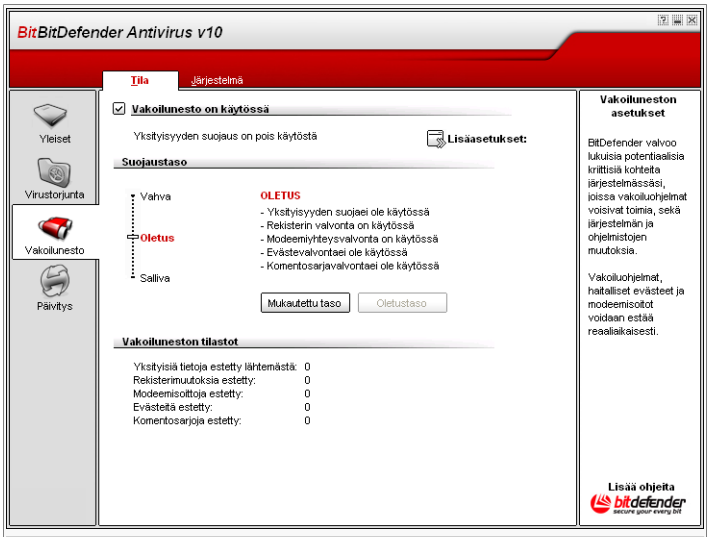
Tämän käyttöoppaan **Vakoilunesto**-osiossa ovat seuraavat aiheet:

- Vakoiluneston tila
- Lisäasetukset - Yksityisyys
- Lisäasetukset - Rekisterit
- Lisäasetukset - Soitto
- Lisäasetukset - Evästeet
- Lisäasetukset - Script
- Järjestelmätiedot

Huomaa

Lisätietoja **Vakoilunestosta** saat lukemalla selostuksen kohdassa "*Vakoilunesto*" (p. 29).

8.1. Vakoiluneston tila



Kuva 8.1. Vakoiluneston tila

Tässä osiossa voit määritellä **Vakoilunesto** -osan toimintoja ja saat tietoja sen toiminnasta.

Tärkeää

Pidä aina **Vakoilunesto** käytössä, jotta vakoiluohjelmat eivät pääsisi saastuttamaan konettasi.

Ikkunan alareunassa voit nähdä **Vakoilunestoa** koskevia tilastotietoja.

Vakoilunesto suojaa koneesi vakoiluohjelmia vastaan viiden tärkeän suojattavan toiminnon kautta:

- Yksityisyydensuoja - suojaa luottamuksellista tietoa suodattamalla HTTP ja SMTP liikennettä luomiesi sääntöjen perusteella. Nämä säännöt luodaan Yksityisyys -osiossa.
- Rekisterin valvonta - kysyy vahvistusta, kun jokin ohjelma yrittää muuttaa rekisteriasetuksia, joita suoritetaan Windowsin käynnistyksen yhteydessä.

- Modeemiyhteyksen valvonta - kysyy vahvistusta, kun jokin ohjelma yrittää muodostaa yheyden tietokoneen modeemia käyttämällä.
- Evästevalvonta - kysyy vahvistusta, kun uusi verkkosivusto yrittää tallentaa evästeen.
- Komentosarjavalvonta - kysyy vahvistusta, kun jokin verkkosivusto yrittää aktivoida komentosarjan tai muuta aktiivista sisältöä.

Mukauttaaksesi näiden toimintojen asetuksia, valitse Lisäasetukset.

8.1.1. Suojaustaso

Voit valita tarpeisiisi parhaiten sopivan suojaustason. Siirrä liukukytkintä asteikolla asettaaksesi sopivan suojaustason.

Valittavana on kolme erilaista suojaustasoa:

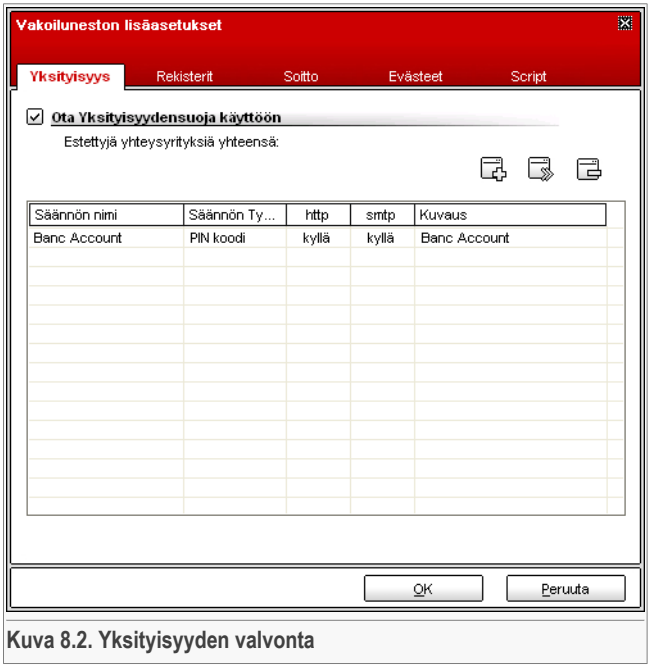
Suojaustaso	Kuvaus
Salliva	Vain **Rekisterin valvonta** on käytössä.
Oletus	**Rekisterin valvonta** ja **Modeemiyhteyksien valvonta** ovat käytössä.
Vahva	**Rekisterin valvonta**, **Modeemiyhteyksien valvonta** ja **Yksityisyyden suoja** ovat käytössä.

Voit mukauttaa suojaustasoa valitsemalla **Mukautettu taso**. Valitse avautuvasta ikkunasta haluamasi Vakoiluneston asetukset ja valitse **OK**.

Valitse **Oletustaso** asettaaksesi liukukytkimen oletustasolle.

8.2. Lisäasetukset - Yksityisyys

Päästäksesi tähän osioon, valitse osio **Lisäasetukset Antispyware** -osan Tila osiossa.



Kuva 8.2. Yksityisyyden valvonta

Luottamuksellisten tietojen pitäminen turvassa on tärkeä asia, joka koskee meitä kaikkia. Tietojen varastaminen on vallannut alaa Internet-kommunikoinnin kehittymisen myötä ja jatkuvasti kehitetään uusia keinoja ihmisten huijaamiseksi antamaan yksityistä tietoa.

On kyseessä sitten sähköpostiosoitteesi tai luottokorttisi numero, väärissä käsissä tällaiset tiedot voivat aiheuttaa paljon vahinkoa: voit hukkua roskapostiviesteihin tai voit huomata luottotilisi tyhjennetyn.

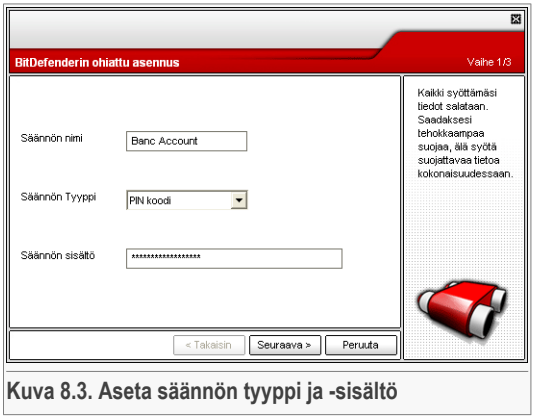
Yksityisyyden suoja autta sinua pitämään luottamukselliset tiedot turvassa. Se tarkistaa HTTP ja SMTP -liikenteen, määrittelemiesi astusten mukaan. Jos luottamukselliseksi määriteltyä tietoa löytyy, siihen liittyvä verkkosivu tai sähköpostiviesti estetään.

Säännöt täytyy luoda manuaalisesti (valitse **Lisää** ja valitse säännön parametrit). Ohjattu asetusten luominen käynnistyy.

8.2.1. Ohjattu sääntöjen luominen

Ohjattu sääntöjen luominen on kolmivaiheinen prosessi.

Vaihe 1/3 – Aseta säännön tyyppi ja -sisältö



Kuva 8.3. Aseta säännön tyyppi ja -sisältö

Kirjoita säännön nimi sille varattuun kenttään.

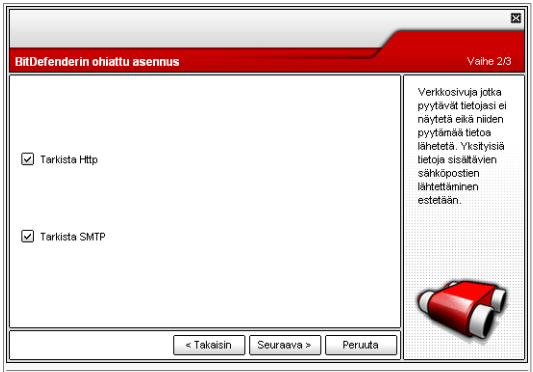
Seuraavat parametrit pitää asettaa:

- **Säännön tyyppi** - valitse säännön tyyppi (osoite, nimi, luottokortti, PIN, henkilötunnus, jne).
- **Säännön sisältö** - kirjoita säännön sisältö.

Kaikki kirjoittamasi tiedot salataan. Saadaksesi tehokkaampaa suojaa, älä kirjoita salattavaa tietoa kokonaisuudessaan.

Valitse **Seuraava**.

Vaihe 2/3 – Valitse liikenne



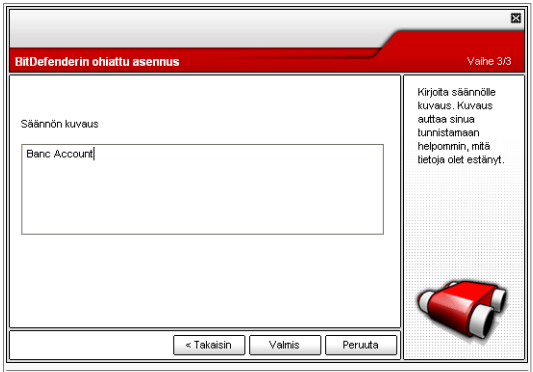
Kuva 8.4. Valitse liikenne

Valitse liikenne, jonka haluat BitDefenderin tarkistavan. Seuraavat valinnat ovat käytettävissä:

- **Tarkista Http** - tarkistaa HTTP (Internet) -liikenteen ja estää sellaisten tietojen lähettämisen, jotka vastaavat luotuja sääntöjä.
- **Tarkista SMTP** - tarkistaa SMTP (sähköposti) -liikenteen ja estää sellaisten tietojen lähettämisen, jotka vastaavat luotuja sääntöjä.

Valitse **Seuraava**.

Vaihe 3/3 – Säännön kuvaus



Kuva 8.5. Säännön kuvaus

Kirjoita lyhyt kuvaus säännöstä.

Valitse **Valmis**.

8.2.2. Sääntöjen hallinta

Voit tarkastella taulukossa luetteloituja sääntöjä.

Poistaaksesi säännön, valitse sääntö ja sen jälkeen valitse **Poista**. Ottaaksesi säännön tilapäisesti pois käytöstä poistamatta sitä, ota rastit pois http ja smtp -kohdista.

Muokataksesi sääntöä, valitse sääntö ja sen jälkeen valitse **Muokkaa** tai kaksoisklikkaa sääntöä. Uusi ikkuna avautuu.

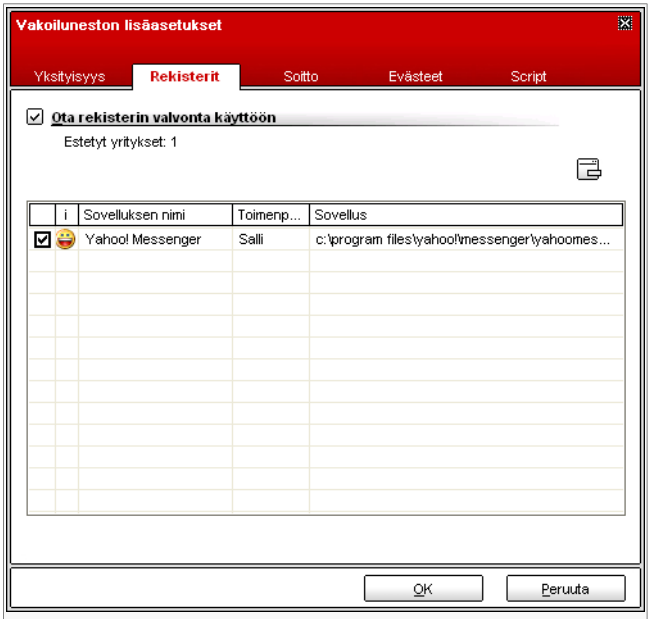
Kuva 8.6. Muokkaa sääntöä

Tässä voit muuttaa säännön nimeä, kuvausta ja parametreja (tyyppi, sisältö ja liikenne). Valitse **OK** tallentaaksesi muutokset.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan.

8.3. Lisäasetukset - Rekisterit

Päästäksesi tähän osioon, siirry **Vakoiluneston lisäasetukset** ikkunaan (siirry **Vakoilunesto** -osan, Tila -osioon ja valitse **Lisäasetukset**) ja valitse **Rekisterit** -välilehti.



Kuva 8.7. Rekisterikontrolli

Erittäin tärkeä osa Windowsia on nimeltään **Rekisteri**. Se on paikka, missä Windows pitää asetuksiaan, asennettujen ohjelmien ja laitteiden tietoja, tietoja käyttäjistä jne.

Rekisteriä käytetään myös määrittelemään mitkä ohjelmat käynnistetään automaattisesti kun Windows käynnistyy. Virukset käyttävät usein tätä mahdollisuutta ja ne aktivoituvat, kun tietokone käynnistetään.

Rekisterikontrolli valvoo rekisterin toimintaa – tämä on hyödyllistä ns. Troijalaisten toteamiseksi. Se varoittaa, kun jokin ohjelma yrittää muuttaa Windowsin käynnistykseen liittyviä rekisterinasetuksia.

Kuva 8.8. Rekisterihälytys

Voit estää tämän muutoksen valitsemalla **Ei** tai sallia valitsemalla **Kyllä**.

Jos haluat BitDefenderin muistavan valintasi, sinun täytyy laittaa rasti kohtaan **Muista tämä vastaus**.

Huomaa

Antamasi vastaukset muodostavat säännöstön perustan.

Poistaaksesi rekisterimerkinnän, valitse merkintä ja sen jälkeen valitse **Poista**. Ottaaksesi rekisterimerkinnän tilapäisesti pois käytöstä, ota rasti pois merkinnän kohdalla olevasta ruudusta.

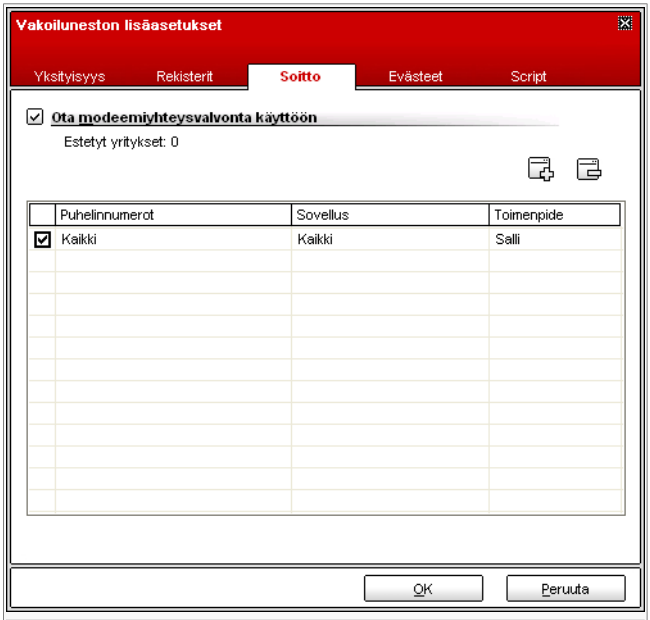
Huomaa

BitDefender hälyttää joka kerran, kun asennat uusia ohjelmia, jotka aktivoituvat käynnistyksessä. Nämä ohjelmat ovat yleensä luotettavia ja käynnistys voidaan hyväksyä.

Valitse **OK** sulkeaksi ikkunan.

8.4. Lisäasetukset - Soitto

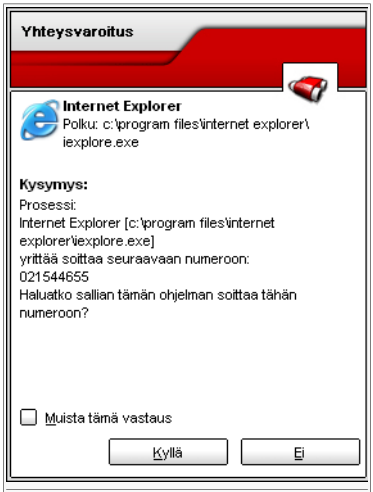
Päästäksesi tähän osioon, siirry **Vakoiluneston lisäasetukset** -ikkunaan (siirry **Vakoilunesto** -osan, Tila -osioon ja valitse **Lisäasetukset**) ja valitse **Soitto** -välilehti.



Kuva 8.9. Yhteysvalvonta

Numeronvalitsimet ovat sovelluksia, jotka käyttävät tietokoneen modemia yhteyden ottamiseen erilaisiin puhelinnumeroihin. Tavallisesti numeronvalitsimia käytetään, jotta voitaisiin muodostaa yhteys erilaisiin numeroihin. Lisäksi tämä tapahtuu avaamalla yhteys erittäin kalliisiin puhelinnumeroihin.

Käyttämällä **Yhteysvalvonta**–menetelmää voit itse päättää mihin numeroihin koneen sallitaan muodostaa yhteys ja mihin numeroihin yhetydenotto estetään. Tämä toiminto valvoo kaikkia numeronvalitsimia, jotka yrittävät käyttää tietokoneen modemia, ja se myös varoittaa käyttäjää sekä kehoittaa häntä valitsemaan sallitaanko, vai estetäänkö sellaiset yritykset:



Kuva 8.10. Modeemiyhteysvaroitus

Voit nähdä sovelluksen nimen sekä puhelinnumeron.

Valitse **Muista tämä vastaus** -valinta ja sen jälkeen **Kyllä** tai **Ei**, jolloin sääntö luodaan ja sitä otetaan käyttöön, ja se lisätään myös sääntöluetteloon. Tämän jälkeen et saa enää ilmoitusta, kun sovellus yrittää valita tämän saman puhelinnumeron.

Jokainen sääntö, joka on tallennettu, saadaan esille **Yhteys**–osiossa myöhempää hienosäätöä varten.

Tärkeää

Säännöt ovat luettelossa tärkeysjärjestyksessä alkaen ylhäältä ja tämä tarkoittaa, että ensimmäinen sääntö on kaikista tärkein. Sääntöjen järjestystä voi muuttaa vetämällä ja pudottamalla ne uuteen paikkaan.

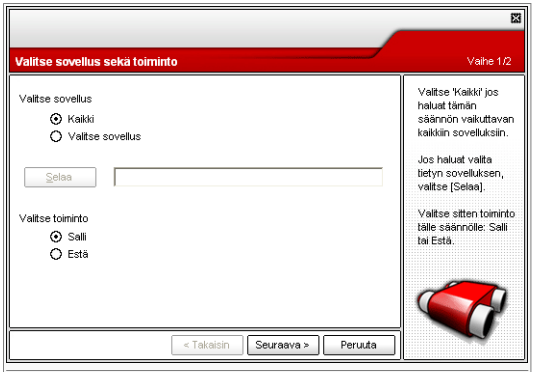
Poistaaksesi säännön, valitse sääntö ja sen jälkeen valitse **Poista**. Muuttaaksesi säännön parametreja, kaksoisklikkaa sääntöä ja tee tarvittavat muutokset. Ottaaksesi säännön väliaikaisesti pois käytöstä, ota rasti pois säännön kohdalla olevasta ruudusta.

Sännöt voidaa asettaa automaattisesti (hälytysikkunan kautta) tai manuaalisesti (valitse **Lisää** ja aseta säännön parametrit). Ohjattu asetusten luominen käynnistyy.

8.4.1. Ohjattu sääntöjen luominen

Ohjattu asetusten luominen on kaksivaiheinen prosessi.

Vaihe 1/2 - Valitse sovellus ja toiminto



Kuva 8.11. Valitse sovellus ja toiminto

Voit asettaa seuraavat parametrit:

- **Sovellus** - valitse sovellus jolle tehdään sääntö. Voit valita vain yhden sovelluksen (**Valitse sovellus**, sitten **Selaa** ja valitse sovellus) tai kaikki sovellukset (valitse **Mikä tahansa**).
- **Toiminta** - valitse säännön toiminta.

Toimenpide	Kuvaus
Salli	Toiminto sallitaan.
Estä	Toiminto estetään.

Valitse **Seuraava**.

Vaihe 2/2 – Valitse puhelinnumerot

Kuva 8.12. Valitse puhelinnumerot

Valitse **Määritä puhelinnumero**, kirjoita puhelinnumero, johon sääntöä tullaan soveltamaan ja valitse **Lisää**.

Huomaa

Voit käyttää jokerimerkkejä kiellettyjen puhelinnumeroiden luettelossasi, esim. 1900* tarkoittaa, että kaikki numerot, jotka alkavat numerosarjalla 1900, tullaan estämään.

Valitse **Kaikki**, jos haluat, että tätä sääntöä sovelletaan kaikkiin puhelinnumeroihin. Kun haluat poistaa jonkin puhelinnumeron, valitse numero ja sen jälkeen **Poista**.

Huomaa

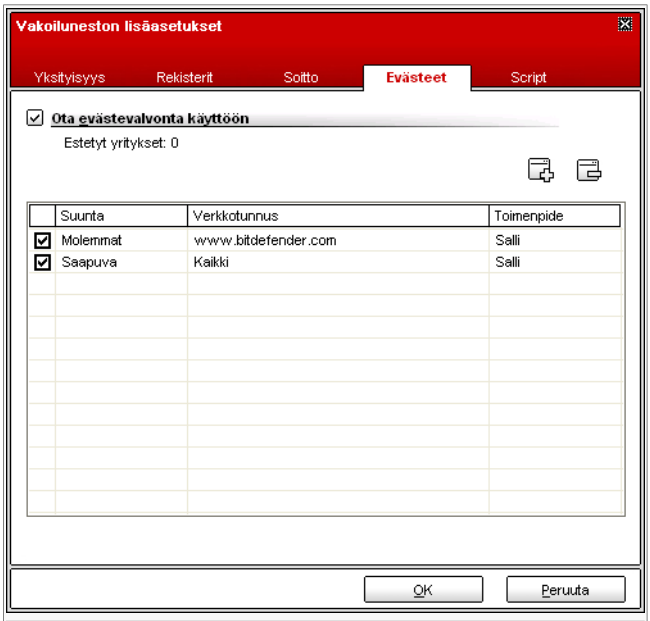
Voit myös luoda säännön, joka sallii tietyn ohjelman valita vain tiettyjä numeroita (kuten esim. Internetpalvelun tarjoajasi numeron tai telefaksi uutispalvelun numeron).

Valitse **Valmis**.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan.

8.5. Lisäasetukset - Evästeet

Päästäksesi tähän osioon, siirry **Vakoiluneston lisäasetukset** -ikkunaan (siirry **Vakoilunesto** -osan Tila -osioon, ja valitse **Lisäasetukset**) ja valitse **Evästeet** -välilehti.



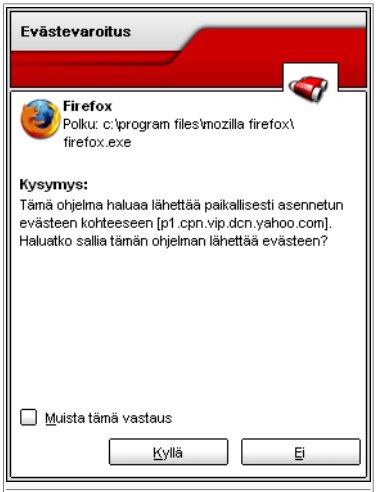
Kuva 8.13. Evästevalvonta

Evästeitä eli pipareita (cookies) esiintyy erittäin yleisesti Internetissä. Ne ovat pieniä tiedostoja, jotka tallentuvat tietokoneeseesi. Verkkoyhteydet lähettävät näitä evästeitä siksi, että pystyisivät hankkimaan sinusta yksityiskohtaisia tietoja (niitä tietoja, jotka liittyvät Internet-yhteyksiisi sekä valintoihin, joita olet tehnyt sivustoilla).

Yleisesti ottaen evästeiden tarkoituksena on helpottaa koneesi käyttöä. Ne voivat esim. auttaa verkkosivustoa muistamaan nimesi ja tekemäsi valinnat, ettei sinun tarvitse kirjoittaa niitä joka kerta uudelleen, kun vierailet uudelleen k.o. osoitteessa.

Mutta evästeitä voidaan käyttää myös yksityisyytesi vaarantamiseen, koska ne keräävät tietoja siitä, missä osoitteissa olet vieraillut käyttäessäsi Internetiä.

Tässä **Evästevalvonta** auttaa. Kun **Evästevalvonta** on otettu käyttöön, se kysyy sinulta luvan aina, kun uusi Internet-sivusto yrittää asentaa evästeen koneellesi:



Kuva 8.14. Evästevaroitus

Voit nähdä sen sovelluksen nimen, joka yrittää lähettää evästetiedostoa.

Valitse **Muista tämä vastaus** ja sen jälkeen **Kyllä** tai **Ei**, jolloin sääntö luodaan ja otetaan käyttöön, ja se lisätään myös sääntöluetteloon. Et saa tämän jälkeen enää ilmoitusta, kun otat otat yhteyden samaan sivustoon.

Tämä auttaa sinua valitsemaan mihin verkkosivustoihin luotat ja mihin et luota.

Huomaa

Koska Internetissä käytetään nykyisin hyvin paljon evästeitä, voi **Evästevalvonta** tuntua ensi alkuun melko rasittavalta. Aluksi se tekee monia kysymyksiä niistä osoitteista, jotka yrittävät asentaa evästeitä koneellesi. Heti kun lisäät tavanomaiset osoitteesi säännöstöön, muuttuu Internetin käyttö yhtä helpoksi kuin ennenkin.

Jokaista sääntöä, joka on tallennettu, voidaan tarkastella **Evästeet** -osiossa myöhempää hienosäätöä varten.

Tärkeää

Säännöt ovat luettelossa tärkeysjärjestyksessä alkaen ylhäältä ja tämä tarkoittaa, että ensimmäinen sääntö on kaikista tärkein. Sääntöjen järjestystä voi muuttaa vetämällä ja pudottamalla ne uuteen paikkaan.

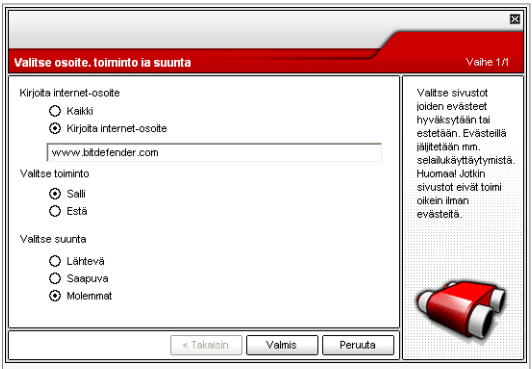
Poistaaksesi säännön, valitse sääntö ja sen jälkeen valitse **Poista**. Muuttaaksesi säännön parametreja, kaksoisklikkaa sääntöä ja tee tarvittavat muutokset. Ottaaksesi säännön väliaikaisesti pois käytöstä, ota rasti pois säännön kohdalla olevasta ruudusta.

Sännöt voidaa asettaa automaattisesti (hälytysikkunan kautta) tai manuaalisesti (valitse **Lisää** ja aseta säännön parametrit). Ohjattu asetusten luominen käynnistyy.

8.5.1. Ohjattu sääntöjen luominen

Konfigurointiopasteikkuna on yksivaiheinen prosessi.

Vaihe 1/1 – Valitse osoite, toiminto ja suunta



Kuva 8.15. Valitse osoite, toiminto ja suunta

Voit asettaa seuraavat parametrit:

- **Verkko-osoite** - kirjoita osoite, johon sääntöä sovelletaan.
- **Toiminta** - valitse säännön toiminta.

Toimenpide	Kuvaus
Salli	Evästeet, jotka tämä osoite lähettää, saa suorittaa.
Estä	Evästeet, joita tämä osoite lähettää, ei saa suorittaa.

- **Suunta** - valitse liikenteen suunta.

Tyyppi	Kuvaus
Lähtevä	Sääntöä sovelletaan ainoastaan niihin evästeisiin, jotka lähetetään takaisin siihen osoitteeseen, johon tietokone on yhteydessä.

Tyyppi	Kuvaus
Tuleva	Sääntöä sovelletaan ainoastaan niihin evästeisiin, jotka vastaanotetaan siitä osoitteesta, johon tietokone on yhteydessä.
Molemmat	Sääntö koskee molempia liikennesuuntia.

Valitse **Valmis**.

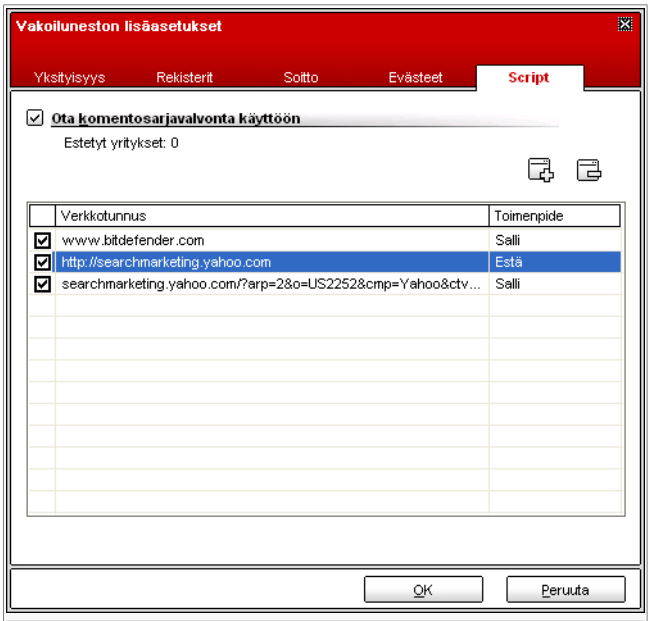
Huomaa

Voit ottaa vastaan evästeitä, mutta et voi koskaan palauttaa niitä asettamalla toimintoa **Estä**–tilaan ja suuntavalinnan **Lähtevä**–tilaan.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan.

8.6. Lisäasetukset - Script

Päästäkesi tähän osioon, siirry **Vakoiluneston lisäasetukset** -ikkunaan (siirry **Vakoilunesto** -osan Tila -osioon ja valitse **Lisäasetukset**) ja valitse **Script** -välilehti.



Kuva 8.16. Script-valvonta

Scriptit ja muut koodit, kuten ActiveX kontrollit ja Java appletit, joita käytetään vuorovaikutteisten Internetsivujen tekemiseen, voidaan ohjelmoida aiheuttamaan vahingollisia seurauksia. Esim. ActiveX ohjelmien avulla hakkerit voivat päästä koneellesi ja he voivat lukea siellä olevia tietoja ja myös tuhota tietoja ja varastaa salasanoja sekä siepata sanomia, kun koneesi on kytketty Internetiin. Olisi viisasta hyväksyä ainoastaan sellaiset aktiiviset sisällöt, jotka tulevat osoitteista, jotka täysin tunnet ja joihin varmasti luotat.

BitDefender antaa sinun valita itse annatko näiden koodien toimia, vai estätkö niiden toiminnan.

Script-valvonnan avulla voit itse päättää mihin Internetosoitteisiin luotat ja mihin et. BitDefender kysyy aina luvan, kun jokin internetsivusto yrittää aktivoida scriptin tai muuta aktiivista sisältöä:

Kuva 8.17. Script-varoitus

Voit nähdä resurssin nimen.

Valitse **Muista tämä vastaus** ja sen jälkeen **Kyllä** tai **Ei**, niin sääntö luodaan ja se otetaan käyttöön, ja se lisätään myös sääntöluetteloon. Et saa tämän jälkeen enää ilmoitusta, kun sama sivusto yrittää lähettää koneellesi aktiivista sisältöä.

Kaikki säännöt, jotka on tallennettu muistiin, voidaan ottaa uudelleen esille **Script**–osiossa myöhempää hienosäätöä varten.

Tärkeää

Säännöt ovat luettelossa tärkeysjärjestyksessä alkaen ylhäältä ja tämä tarkoittaa, että ensimmäinen sääntö on kaikista tärkein. Sääntöjen järjestystä voi muuttaa vetämällä ja pudottamalla ne uuteen paikkaan.

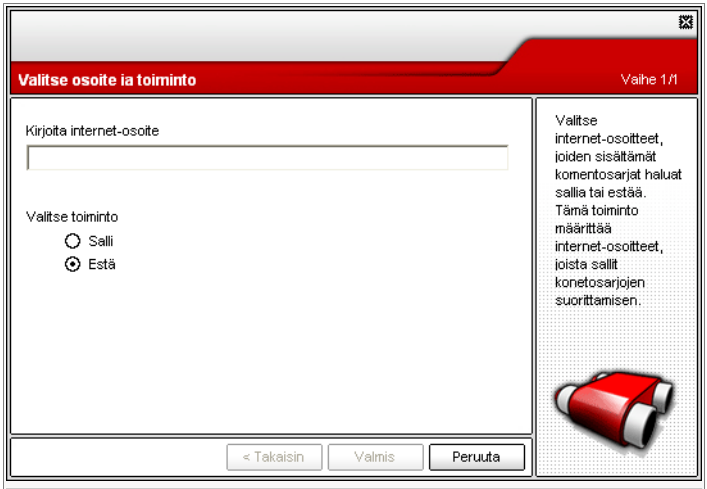
Poistaaksesi säännön, valitse sääntö ja sen jälkeen valitse **Poista**. Muuttaaksesi säännön parametreja, kaksoisklikkaa sääntöä ja tee tarvittavat muutokset. Ottaaksesi säännön väliaikaisesti pois käytöstä, ota rasti pois säännön kohdalla olevasta ruudusta.

Sännöt voidaa asettaa automaattisesti (hälytysikkunan kautta) tai manuaalisesti (valitse **Lisää** ja aseta säännön parametrit). Ohjattu asetusten luominen käynnistyy.

8.6.1. Ohjattu sääntöjen luominen

Konfigurointiopasteikkuna on yksivaiheinen prosessi.

Vaihe 1/1 - Valitse osoite ja toiminto



Kuva 8.18. Valitse osoite ja toiminto

Voit asettaa seuraavat parametrit:

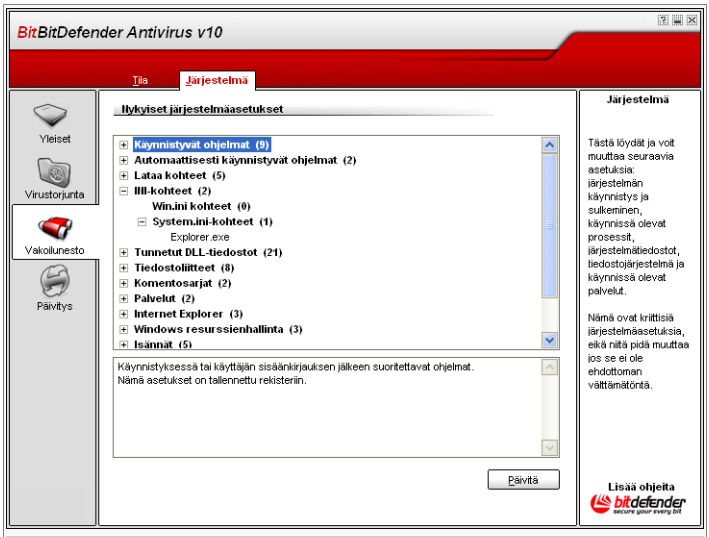
- **Verkko-osoite** - kirjoita osoite, johon sääntöä sovelletaan.
- **Toiminta** - valitse säännön toiminta.

Toimenpide	Kuvaus
Salli	Scriptit, jotka tämä osoite lähettää, saa suorittaa.
Estä	Scriptit joita tämä osoite lähettää, ei saa suorittaa.

Valitse **Valmis**.

Valitse **OK** tallentaaksesi muutokset ja sulkeaksesi ikkunan.

8.7. Järjestelmätiedot



Kuva 8.19. Järjestelmätiedot

Tässä ikkunassa näet ja voit muuttaa tärkeimpiä asetuksia.

Luettelo sisältää kaikki ne asetukset, jotka on ladattu silloin kun järjestelmä on käynnistetty ja luettelossa ovat myös kaikki ne asetukset, jotka eri sovellukset ovat ladanneet.

Käytettävissä on kolme painiketta:

- **Poista** - poistaa valitut asetukset.
- **Mene** - avaa ikkunan, jossa valittu astus sijaitsee (esim. **rekisteritiedostokansio**).
- **Uudista** - avaa uudelleen **Järjestelmätiedot**-osion.

Luku 9. Päivitys

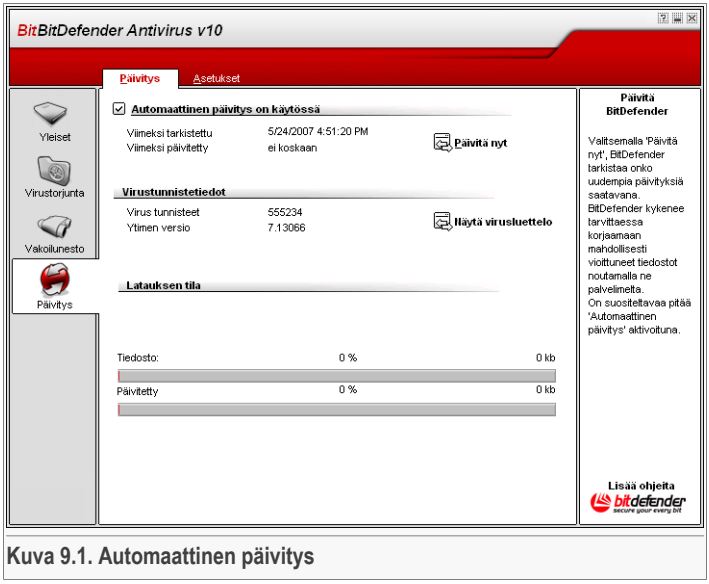
Tämän käyttöohjeen **Päivitys** -osio sisältää seuraavat aiheet:

- Automaattinen päivitys
- Manuaalinen päivitys
- Päivitysasetukset

Huomaa

Saat tarkempia tietoja **Päivitys** -osan toiminnasta kappaleesta "*Päivitys*" (p. 30).

9.1. Automaattinen päivitys



Kuva 9.1. Automaattinen päivitys

Tässä osiossa voit tarkastella päivityksiin liittyviä tietoja ja suorittaa päivityksiä.

Tärkeää

Pitääksesi järjestelmäsi suojattuna uusimpia uhkia vastaan, pidä **Automaattinen päivitys** käytössä.

Jos koneesi on kytketty Internetiin laajakaistayhteyden tai xDSL-yhteyden kautta, BitDefender huolehtii itse päivityksestään. Se tarkistaa uudet päivitykset heti, kun käynnistät tietokoneesi ja **tunneittain** sen jälkeen.

Jos päivitys on saatavilla, riippuen niistä valinnoista ja asetuksista, joita on tehty Automaattisen päivityksen asetukset-osiossa, käyttäjältä kysytään vahvistusta päivitykselle tai päivitys tapahtuu automaattisesti.

Automaattinen päivitys voidaan suorittaa milloin tahansa, valitsemalla **Päivitä nyt**. Tästä käytetään myös nimeä **Käyttäjän pyynnöstä -päivitys**.

Päivitys -osa ottaa yhteyden BitDefenderin päivityspalvelimelle ja tarkistaa onko päivityksiä saatavissa. Jos päivitys on saatavilla, riippuen Manuaalinen päivitys-osiossa tehdyistä valinnoista, käyttäjää pyydetään vahvistamaan päivitys tai päivitys tapahtuu automaattisesti.

Tärkeää
Voi olla tarpeellista, että sammutat ja käynnistät koneesi uudelleen päivityksen jälkeen. Suosittelemme, että teet sen kuitenkin niin pian kuin mahdollista.

Huomaa
Jos koneesi on kytketty Internetiin modemiyhteyden kautta, niin on hyvä ajatus, että päivität BitDefenderin säännöllisin välein käyttäen menetelmää Päivitä pyydettäessä.

Voit nähdä BitDefenderin sisältämät virustunnisteet, valitsemalla **Näytä virusluettelo**. Ohjelma luo HTML -tiedoston, joka sisältää kaikki käyettävissä olevat tunnisteen. Valitse **Näytä virusluettelo** uudelleen nähdäksesi luettelon. Voit etsiä tietokannasta tiettyä tunnistetta tai valita **BitDefender Virus List** siirtyäksesi BitDefenderin verkossa olevaan tunnistetietokantaan.

9.2. Manuaalinen päivitys

Tämä menetelmä tekee viimeisimpien virusmääritysten asennuksen. Kun asennat tuotepäivityksen viimeisimmän version, niin käytä menetelmää Automaattinen päivitys.

Tärkeää
Käytä manuaalista päivitystä silloin, kun automaattista päivitystä ei voida suorittaa tai kun tietokonetta ei ole kytketty internettiin.

Käytettävissä on kaksi menetelmää suorittaa manuaalinen päivitys:

- Käyttäen `weekly.exe` tiedostoa;
- Käyttäen `zip arkistoja`.

9.2.1. Manuaalinen päivitys käyttäen `weekly.exe` –tiedostoa

Päivityspaketti `weekly.exe` julkistetaan jokaisena perjantaina ja se sisältää kaikki virusmäärittelyt ja virustarkastusmoottorit, jotka ovat saatavilla päivityksen suorituspäivään mennessä.

Kun päivität BitDefenderin käyttäen `weekly.exe`-tiedostoa, niin toimi seuraavien ohjeiden mukaisesti:

1. Imuroi weekly.exe-tiedosto Internetistä ja talleta se koneesi kovalevylle.
2. Etsi ladattu tiedosto ja kaksoisklikkaa sitä, käynnistääksesi ohjatun päivityksen.
3. Valitse **Seuraava**.
4. Valitse **Hyväksyn lisenssin ehdot** ja valitse sen jälkeen **Seuraava**.
5. Valitse **Asenna**.
6. Valitse **Valmis**.

9.2.2. Manuaalinen päivitys käyttäen `zip -arkistoja`

Päivityspalvelimella on kaksi zip-arkistoa, jotka sisältävät virustarkistusmoottorien päivitykset sekä virustunnisteet: `cumulative.zip` sekä `daily.zip`.

- `cumulative.zip` julkaistaan kerran viikossa maanantaisin ja se sisältää kaikki virusmääritykset sekä virustarkastusmoottorien päivitykset päivityksen julkistamispäivään asti.
- `daily.zip` julkaistaan joka päivä ja se sisältää kaikki virusmääritykset sekä virustarkastusmoottorien päivitykset viimeisestä cumulative.zip tiedoston julkaisupäivästä alkaen tähän päivään asti.

BitDefender käyttää palvelu-perustaista arkkitehtuuria. Tästä johtuen se prosessi, joka korvaa virusmäärittelyt, on erilainen riippuen käyttöjärjestelmästä:

- Windows NT-SP6, Windows 2000, Windows XP, Windows Vista.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Toimi seuraavalla tavalla:

1. **Lataa asianmukainen päivitys.** Jos on maanantai, niin lataa cumulative.zip ja pyydettäessä tallenna se jonnekin kiintolevyllesi. Muina päivinä lataa daily.zip ja

tallenna myös se koneesi kiintolevylle. Jos tämä on ensimmäinen kerta kun teet manuaalista päivitystä, lataa molemmat tiedostot.

2. **Pysäytä BitDefender virustorjunta.**
   - **Poistu BitDefenderin hallintaikkunasta.** Klikkaa hiiren oikealla painikkeella BitDefender -kuvaketta Ilmaisinalueella ja valitse **Poistu**.
   - **Avoimet palvelut.** Valitse **Käynnistä** ja **Ohjauspaneeli**, ja sen jälkeen valitse **Valvontatyökalut** ja **Palvelut**.
   - **Pysäytä BitDefender Virus Shield -palvelu.** Valitse **BitDefender Virus Shiels** palvelu luettelosta ja sen jälkeen valitse **Lopeta**.
   - **Pysäytä BitDefender Scan Server -palvelu.** Valitse **BitDefender Scan Server** tehtävä luettelosta ja sen jälkeen valitse **Lopeta**.
3. **Pura arkiston sisältö.** Käynnistä `cumulative.zip` , kun molemmat päivitysarkistot on saatavissa. Pura sisältö kansioon `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` ja hyväksy olemassa olevien tiedostojen päällekirjoittaminen.
4. **Käynnistä uudelleen BitDefender virustorjuntasuoja.**
   - **Käynnistä BitDefender Scan Server -palvelu.** Valitse **BitDefender Scan Server** tehtäväluettelosta ja valitse sitten **Käynnistä**.
   - **Käynnistä BitDefender Virus Shield -palvelu.** Valitse **BitDefender Virus Shield** tehtäväluettelosta ja valitse sitten **Käynnistä**.
   - **Avaa BitDefenderin hallintakonsoli.**

Huomaa

Jos käytössäsi on Windows Vista, sinua pyydetään vahvistamaan suurin osa näistä toiminnoista.

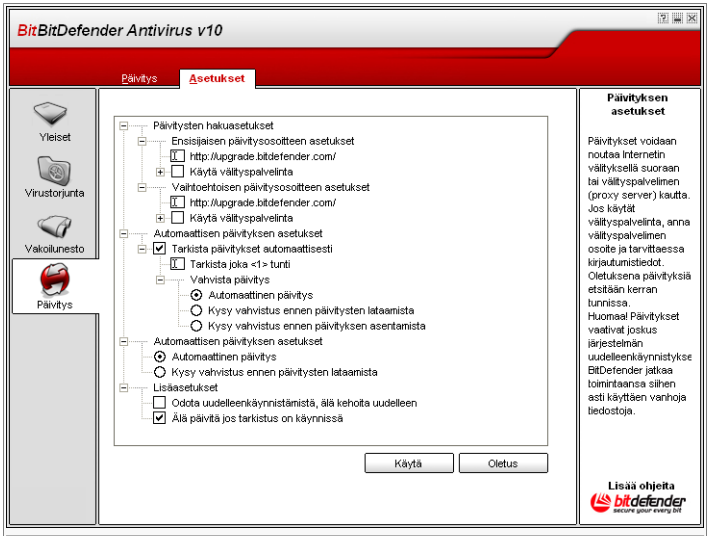
Windows 98, Windows Millennium

Toimi seuraavalla tavalla:

1. **Lataa asianmukainen päivitys.** Jos on maanantai, niin lataa cumulative.zip ja pyydettäessä tallenna se jonnekin kiintolevyllesi. Muina päivinä lataa daily.zip ja tallenna myös se koneesi kiintolevylle. Jos tämä on ensimmäinen kerta kun teet manuaalista päivitystä, lataa molemmat tiedostot.
2. **Pura arkiston sisältö.** Käynnistä `cumulative.zip` , kun molemmat päivitysarkistot on saatavissa. Pura sisältö kansioon `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` ja hyväksy olemassa olevien tiedostojen päällekirjoittaminen.

3. **Sammuta kone ja käynnistä se uudelleen.**

9.3. Päivitä asetukset



Kuva 9.2. Päivitä asetukset

Päivitykset voidaan noutaa verkosta suoraan Internetin kautta tai välityspalvelimen (proxy) kautta.

Päivitysasetusten ikkuna sisältää neljä valinnaista vaihtoehtoa (**Päivityskohteen asetukset**, **Automaattisen päivityksen asetukset**, **Manuaalisen päivityksen tyyppi** ja **Yhteysasetukaset**) järjestettyinä laajennettaviin Windows-tyyppisiin valikoihin.

Huomaa

Avaa kohde napauttamalla “+” tain sulje se napauttamalla “-“.

9.3.1. Päivitysosoitteen asetukset

Luotettavampaa ja nopeampaa päivitystä varten voit konfiguroida kahta päivityskohdetta: **Ensisijainen päivityskohde** ja **Vaihtoehtoinen päivityskohde**. Molempia varten täytyy lisäksi tehdä seuraavat määrittelyt:

- **Päivityskohde** - Jos olet liitetty paikallisverkkoon, jossa virustunnisteet ovat saatavana paikallisesti, voit vaihtaa päivityskohteen sinne. Oletuskohde on muuten: http://upgrade.bitdefender.com.
- **Käytä välityspalvelinta** - Jos yritys käyttää välityspalvelinta (proxy), käytä tätä valintaa. Seuraavat asetukset pitää määritellä:
  - **Välityspalvelimen asetukset** - kirjoita IP-osoite tai välityspalvelimen nimi, sekä yhteyden käyttämä portti.

    Tärkeää
    Syntaksi: `nimi:portti` tai `ip:portti`.

  - **Välityspalvelin käyttäjä** - kirjoita käyttäjänimi, jonka välityspalvelin tunnistaa.

    Tärkeää
    Syntaksi: `toimialue\käyttäjä`.

  - **Välityspalvelin salasana** - kirjoita kelvollinen salasana edellä määritellylle käyttäjälle.

9.3.2. Automaattisen päivityksen asetukset

- **Hae päivitykset automaattisesti** - BitDefender tarkistaa automaattisesti päivityspalvelimilta onko päivityksiä saatavana.
- **Hae joka x tunti** - Asettaa tarkastusvälin tunteina, oletusarvo 1 h.
- **Taustapäivitys** - BitDefender automaattisesti hakee ja toteuttaa päivityksen.
- **Kysy ennen hakua** - kun päivitys on saatavana, sen lataus varmistetaan.
- **Kysy ennen asennusta** - latauksen jälkeen varmistetaan asennus.

Tärkeää
Jos valitset **Kysy ennen hakua** ja/tai **Kysy ennen asennusta** , suljet ja poistut hallintakonsolista, automaattista päivitystä ei suoriteta.

9.3.3. Manuaalisen päivityksen asetukset

- **Taustapäivitys** - manuaalinen päivitys suoritetaan automaattisesti taustalla.

- **Kysy ennen hakua** - manuaalinen päivitys varmistaa latauksen ja asennuksen ennen suoritusta.

Tärkeää

Jos valitset **Kysy ennen hakua** ja suljet ja poistut hallintakonsolista manualista päivitystä ei suoriteta.

9.3.4. Lisäasetukset

- **Odota käynnistystä ilman kehottetta** - Vaikka päivitys vaatii uudelleenkäynnistyksen, toiminta jatkuu vanhoilla tiedostoilla kunnes uudelleenkäynnistys tapahtuu. Kehoteta ei kuitenkaan esitetä, eikä näin häiritä muuta toimintaa.
- **Älä päivitä jos tarkistus on käynnissä** - BitDefenderiä ei päivitetä, jos tarkistusprosessi on käynnissä. Tämä valinta estää BitDefenderin päivitystä keskeyttämästä tarkistutehtävää.

Huomaa

Jos BitDefender päivitetään tarkistuksen ollessa käynnissä, tarkistus lopetetaan.

Tallenna muutokset valitsemalla **Käytä** tai **Oletus**, oletusarvojen lataamiseksi.

Parhaat toimintavat

Luku 10. Parhaat toimintavat

Tämän käyttöohjeen **Parhaat käyttövinkit** -osio sisältää seuraavat aiheet:

- Kuinka suojata tietokoneesi haittaohjelmia vastaan
- Kuinka konfiguroida tarkistustehtävä

10.1. Kuinka suojata tietokoneesi haittaohjelmia vastaan

Seuraa näitä vaiheita suojataksesi tietokoneesi viruksia, vakoiluohjelmia ja muita haittaohjelmia vastaan:

1. **Ohjattu ensiasennus.** Asennuksen aikana käynnistyy ohjattu asennus. Se opastaa sinua BitDefenderin rekisteröinnissä ja luomaan BitDefender -tilin saadaksesi täyden hyödyn ilmaisesta teknisestä tuesta. Se opastaa sinua myös asettamaan BitDefenderin suorittamaan tärkeitä tietoturvatehtäviä.

   Tärkeää

   Jos sinulla on BitDefender Korjaus CD, tarkista järjestelmäsi ennen BitDefenderin asentamista varmistaaksesi, että järjestelmässäsi ei ole ennestään mitään haittaohjelmia.

2. **Päivitä BitDefender.** Jos et ole suorittanut ensiasennusta loppuun ohjelman asennuksen aikana, tee käyttäjän pyytämä päivitys (siirry **Päivitys** -osan, Päivitys -osioon ja valitse **Päivitä nyt**).
3. **Tee täydellinen järjestelmän tarkistus.** Siirry **Virustorjunta** -osan Suoja -osioon ja valitse **Tarkista nyt**.

   Huomaa

   Voit myös käynnistää täydellisen järjestelmän tarkistuksen Tarkista -osiosta. Valitse **Täydellinen järjestelmän tarkistus** -tehtävä ja sen jälkeen valitse **Käynnistä**.

4. **Ehkäise tartunnat ennalta.** Pidä **Suoja** -osiossa valinta reaaliaikainen suojaus käytössä suojautuaksesi viruksia, vakoiluohjelmia ja muita haittaohjelmia vastaan. Aseta suojaustaso joka vastaa parhaiten tarpeitasi. Voit mukauttaa [52] tasoa milloin tahansa valitsemalla **Mukautettu taso**.

Tärkeää

Ohjelmoi BitDefender Antivirus v10 tarkistamaan järjestelmäsi vähintään kerran viikossa ajastamalla **Täydellinen järjestelmän tarkistus** -tehtävä Tarkista -osiossa.

5. **Pidä BitDefender ajan tasalla.** Pidä **Päivitys** -osan Päivitys -osiossa **Automaattinen päivitys** käytössä, suojataksesi järjestelmäsi uusimpia uhkia vastaan.
6. **Ajasta täydellinen järjestelmän tarkistus.** Siirry **Tarkistus** -osioon ja ohjelmoi BitDefender tarkistamaan järjestelmäsi vähintään kerran viikossa, valitsemalla ajastamalla **Täydellinen järjestelmän tarkistus** -tehtävä.

10.2. Kuinka konfiguroida uusi tarkistustehtävä

Seuraa näitä vaiheita luodaksesi ja konfiguroidaksesi tarkistustehtävän:

1. **Luo uusi tehtävä.** Siirry Tarkistus -osioon ja valitse **Uusi tehtävä**. Ominaisuudet -ikkuna tulee esiin.

Huomaa

Voit luoda uuden tehtävän myös kopioimalla jonkin olemassa olevista tehtävistä. Tehdäksesi näin, klikkaa tehtävää hiiren oikealla painikkeella ja valitse **Kopioi** from pikavalikosta. Valitse kopioi ja sen jälkeen valitse **Ominaisuudet** avataksesi **Ominaisuudet** -ikkunan.

2. **Aseta suojaustaso.** Siirry **Yleiset** -osioon asettaaksesi tarkistustason. Halutessasi voit mukauttaa [60] tarkistusasetuksia valitsemalla **Mukauta**.
3. **Aseta tarkistuksen kohde:** Siirry **Kohteet** -osioon ja valitse kohteet, jotka haluat tarkistaa.
4. **Tehtävän ajastus.** Jos tarkistustehtävä on hyvin monimuotoinen, voi olla hyvä ajastaa se myöhemmin suoritettavaksi, kun tietokonetta ei käytetä aktiivisesti. Tämän auttaa BitDefenderiä tarkistamaan järjestelmäsi luotettavasti. Siirry **Ajastus** -osioon ajastaaksesi tehtävän.

BitDefender Korjaus CD

BitDefender Antivirus 10 toimitetaan käynnistävällä CD-levyllä (BitDefender Korjaus CD, perustana LinuxDefender), joka pystyy tarkistamaan ja puhdistamaan kiintolevyasemat ennen käyttöjärjestelmän käynnistymistä.

Pelaastus-CD:ä pitäisi käyttää aina, kun järjestelmä ei toimi kunnolla virussaastumisen takia.

Virustunnisteiden päivitys tapahtuu automaattisesti ilman käyttäjän toimia joka kerta, kun Korjaus CD käynnistetään.

LinuxDefender esivalmistettu Knoppix-jakelu, joka integroi viimeisimmän BitDefenderin Linuxin turvaratkaisuun GNU/Linux Knoppix Live CD tarjoten välittömän antivirus- / roskapostin esto-suojan, joka on kykenevä tarkistamaan ja puhdistamaan kaikki levyasemat (mukaan lukien Windows NTFS-osiot), etä- Samba/Windows-asemat tai NFS-asennuspisteet. Verkkopohjainen konfigurointiliittymä BitDefender-ratkaisuille on myös saatavana.

Luku 11. Yleiskatsaus

Erityisominaisuudet

- Välitön sähköpostisuoja (Virustorjunta & Roskapostin esto)
- AntiVirus ratkaisut kovalevylle
- NTFS-kirjoitustuki
- Saastuneiden tiedostojen puhdistus

11.1. Mitä on KNOPPIX?

Tiedustelu osoitteesta: http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

11.2. Järjestelmävaatimukset

Ennen kuin käynnistät LinuxDefenderin, varmista, että järjestelmäsi täyttää seuraavat vaatimukset.

Prosessorin tyyppi
x86 yhteensopiva, vähintään 166 MHz. Suosittelemme vähintään i686 prosessoria, 800MHz.

Muisti
Vähintään 64MB, suosittelemme 128MB paremman suorityskyvyn aikaansaamiseksi.

CD-ROM
LinuxDefender toimii CD-ROM -levyltä, joten CD-ROM -asema ja CD-ROM -käynnistystä tukeva BIOS ovat välttämättömiä.

Internet-yhteys
Vaikka LinuxDefender toimiikin ilman Internet-yhteyttä, päivitystoiminnot vaativat aktiivisen HTTP-linkin. Siksi ajantasaisen suojan takaamiseksi, Internet-yhteys on VÄLTTÄMÄTÖN.

Näytön resoluutio

Selainpohjaiseen hallintaan näytön resoluutioksi suositellaan vähintään 800x600.

11.3. Ohjelmistot

BitDefender Korjaus CD sisältää seuraavat ohjelmistot.

- BitDefender SMTP Proxy (Roskapostin esto & Virustorjunta)
- BitDefender Remote Admin (selainpohjainen konfigurointi)
- BitDefender Linux Edition (virustarkistus) + GTK käyttöliittymä
- BitDefender dokumentaatio (PDF & HTML formaateissa)
- BitDefender Extrat (kuvia, esitteitä)
- Linux-Kernel 2.6
- Sisäinen NTFS kirjoitussuojaus
- LUFS - Linux Userland File System
- Työkalut tietojen ja järjestelmän korjaamiseen, myös muiden käyttöjärjestelmien
- Verkko- ja tietoturva-analysointityökalut tietoverkon ylläpitäjille
- Amanda varmistusratkaisu
- thhtpd
- Ethereal verkkoliikenteen analysointityökalu, IPTraf IP LAN Monitor
- Nessus - verkon tietoturvatyökalu
- Parted, QTParted ja partimage, levyosioiden koon muutaminen, tallennus- & palautusratkaisu
- Adobe Acrobat Reader
- Mozilla Firefox selain

11.4. BitDefender Linux tietoturvaratkaisu

LinuxDefender CD sisältää BitDefender SMTP Proxy Antivirus/Antispam for Linux, BitDefender Remote Admin (selainpohjainen käyttöliittymä BitDefender SMTP Proxy:n hallintaan) ja BitDefender Linux Edition virustarkistustyökalun.

11.4.1. BitDefender SMTP Proxy

BitDefender for Linux Mail Servers - SMTP Proxy on turvallinen sisällön tarkistusratkaisu, joka tarjoaa virustorjunnan ja roskapostisuojan yhdyskäytävätasolla, tarkistamalla kaiken sähköpostiliikenteen tunnettuja ja tuntemattomia haittaohjelmia vastaan. Ainutlaatuisen, patentoidun teknologian ansiosta, BitDefender for Mail Servers on yhteensopiva kaikkien tunnettujen sähköposti-alustojen kanssa ja on "RedHat Ready" hyväksytty.

Tämä virustorjunta- ja roskapostin estoratkaisu tarkistaa, puhdistaa ja suodattaa sähköpostiliikenteen millä tahansa sähköpostipalvelimella, riippumatta alustasta ja käyttöjärjestelmästä. BitDefender SMTP Proxy käynnistyy järjestelmän käynnistyessä ja tarkistaan kaiken sisääntulevan sähköpostiliikenteen. Konfiguroidaksesi BitDefender SMTP Proxyn, käytä BitDefender Remote Admin -sovellusta noudattamalla seuraavia ohjeita.

11.4.2. BitDefender Remote Admin

Voit konfiguroida ja hallita BitDefender palveluita etänä (verkkoasetusten konfiguroinnin jälkeen) tai paikallisesti, noudattamalla seuraavia vaiheita:

1. Käynnistä Firefox -selain ja lataa BitDefender Remote Admin URL: https://localhost:8139 (tai kaksoisklikkaa BitDefender Remote Admin -kuvaketta työpöydällä)
2. Kirjaudu sisään tunnuksilla "bd" (käyttäjätunnus) ja "bd" (salasana)
3. Valitse "SMTP Proxy" vasemmalla olevasta valikosta
4. Aseta Real SMTP palvelin ja portti
5. Lisää sähköpostidomain
6. Lisää verkkodomain
7. Valitse "Roskaposti" vasemmalla olevasta valikosta ja konfiguroi roskapostin esto
8. Valitse "Antivirus" konfiguroidaksesi BitDefender Antivirus toiminnot (mitä tehdään kun virus löydetään, karanteenin sijainti)
9. Lisäksi voit konfigroida "Mail notifications" ja lokiasetukset ("Logger")

11.4.3. BitDefender Linux Edition

LinuxDefenderin mukana toimitettava virurtarkistustyökalu on integroitu työpöytään. Tämä versio käyttää GTK+ graafista käyttöliittymää.

Selaa kiintolevyäsi (tai asennetut etälevyt), klikkaa oikealla hiiren painikkeella jotain tiedostoa tai kansiota ja valitse Scan with BitDefender". BitDefender Linux Edition tarkistaa valitut kohteet ja näyttää tilaraportin. Muita vaihtoehtoja käyttääksesi katso BitDefender Linux Edition dokumentaatiota (Bitdefender Documentation kansiossa tai ohjekirjan sivuilla) ja **/opt/BitDefender/lib/bdc** ohjelmassa.

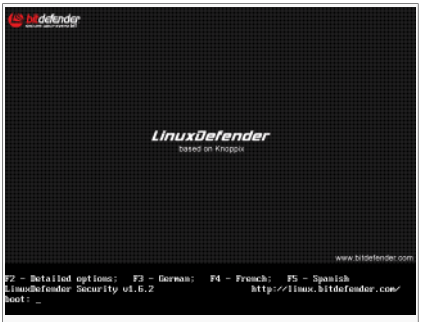
Luku 12. LinuxDefender - miten tehdä

12.1. Käynnistys ja lopettaminen

12.1.1. LinuxDefenderin käynnistäminen

Käynnistääksesi CD:ltä, muokkaa tietokoneesi BIOS -asetuksia niin. että se voi käynnistää CD:ltä, laita CD asemaan ja käynnistä tietokone uudelleen. Varmista, että tietokoneesi pystyy käynnistämään CD:ltä.

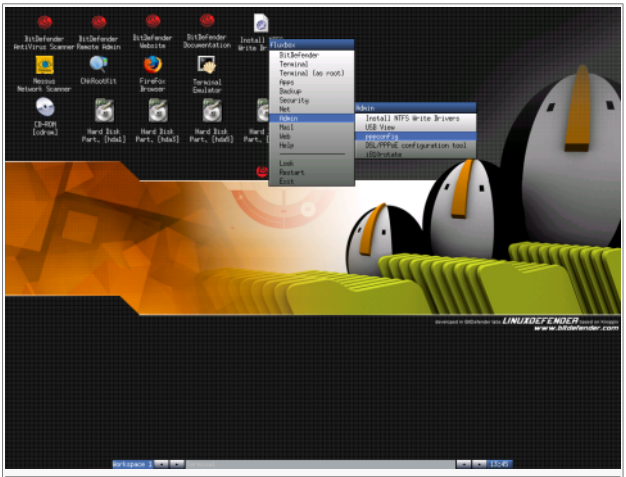
Odota, kunnes seuraava näkymä tulee esiin ja seuraa näytön ohjeita LinuxDefenderin käynnistämiseksi.



Kuva 12.1. Käynnistysnäkymä

Valitse F2 nähdäksesi yksityiskohtaiset vaihtoehdot. Valitse F3 nähdäksesi saksankieliset yksityiskohtaiset vaihtoehdot. Valitse F4 nähdäksesi ranskankieliset yksityiskohtaiset vaihtoehdot. Valitse F5 nähdäksesi espanjankieliset yksityiskohtaiset vaihtoehdot. Pikakäynnistys oletusasetuksilla, paina ENTER.

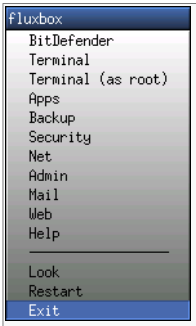
Kun käynnistysprosessi on valmis, työpöytä tulee näkyviin. Voit nyt käynnistää LinuxDefenderin.



Kuva 12.2. Työpöytä

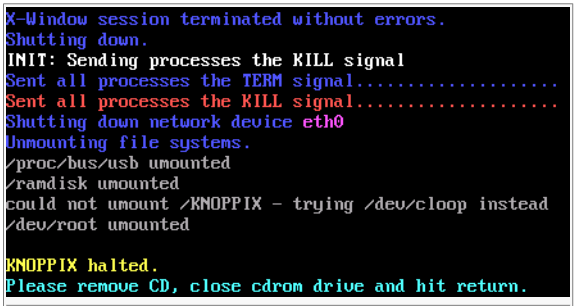
12.1.2. Lopeta LinuxDefender

LinuxDefenderin lopettamiseksi oikealla tavalla, on suositeltavaa ottaa pois käytöstä asennetut etälevyt (mounted) käyttämällä **umount** komentoa tai klikkaamalla oikealla hiiren painikkeella osion kuvaketta ja valitsemalla **Unmount**. Tämän jälkeen voit turvallisesti sammuttaa tietokoneen valitsemalla **Exit** LinuxDefender -valikossa (klikkaa oikealla hiiren painikkeella valikon avaamiseksi) tai kirjoittamlla komennon **halt** terminaali-ikkunassa.



Kuva 12.3. Valitse "EXIT"

Kun LinuxDefender on sulkenut kaikki ohjelmat onnistuneesti, seuraavanlainen kuva tulee näkyviin. Voit poistaa CD:n käynnistääksesi tietokoneen kiintolevyltä. Tämän jälkeen voit sammuttaa tietokoneen tai käynnistää sen uudelleen.



Kuva 12.4. Odota tätä viestiä ennen sammuttamista

12.2. Konfiguroi Internet-yhteys

Jos verkossa on käytettävissä DHCP palvelin ja sinulla on verkkokortti, Internet-yhteyden pitäisi olla valmiina käyttöön. Konfiguroidaksesi Internet-yhteyden manuaalisesti, noudata seuraavia vaiheita.

1. Avaa LinuxDefender -valikko (oikealla hiirenpainikkeella)ja valitse **Terminal** avataksesi konsolin.
2. Kirjoita **netcardconfig** konsolissa avataksesi verkon konfigurointityökalun.
3. Jos verkossasi käytetään DHCP:tä, valitse **yes** (jos et ole varma, kysy verkon ylläpitäjältä). Muussa tapauksessa, katso seuraavaa kohtaa.
4. Verkkoyhteys pitäisi muodostua automaattisesti. Voit nähdä IP-osoitteesi ja verkkokortin asetukset komennolla **ifconfig**.
5. Jos sinulla on kiinteä IP-osoite (DHCP ei ole käytössä), valitse **No** DHCP kysymyksessä.
6. Seuraa näytön ohjeita. Jos et ole varma, mitä tietoja pitäisi kirjoittaa, ota yhteys verkon ylläpitäjään tietojen saamiseksi.

Jos kaikki menee oikein, voit testata Internet-yhteyttäsi "pingaamalla" osoitetta `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Jos käytät modeemiyhteyttä, valitse **pppconfig** LinuxDefender / Admin -valikosta. Seuraa sen jälkeen näytön ohjeita asentaaksesi PPP Internet-yhteyden.

12.3. BitDefender päivitys

BitDefender paketit LinuxDefenderille käyttävät järjestelmän ramdisk -virtuaalilevyä päivitteville tiedostoille. Tämän ansiosta voit päivittää kaikki virustunnisteet, tarkistusmoottorit tai roskapostitietokannat, vaikka järjestelmää käytetäänkin "vain luku" -medialta, kuten LinuxDefender CD.

Varmista, että sinulla on toimiva Internet-yhteys. Avaa ensimmäiseksi BitDefender Remote Admin ja valitse **Live! Update** vasemmalla olevasta valikosta. Valitse Press **Update Now** tarkistaaksesi uusien päivitysten saatavuuden.

Voit vaihtoehtoisesti kirjoittaa seuraavan komennon konsolissa.

```
# /opt/BitDefender/bin/bd  update
```

Kaikista päivitysprosesseista kirjoitetaan automaattisesti merkinnät BitDefender lokiin. Voit tarkastella sitä seuraavalla komennolla.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Jos käytät välityspalvelinta ulkoisiin yhteyksiin, konfiguroi Proxy-asetukset **Live! Update** -valikossa, **Configuration** -välilehdellä.

12.4. Virustarkistus

12.4.1. Kuinka pääsen käsiksi Windows-tietoihini?

Tuki NTFS kirjoitukselle

Tuki NTFS kirjoitukselle on mahdollista käyttämällä toimintoa Captive NTFS write project. Tarvitset kaksi ajuritiedostoa Windows-asennuksesta: `ntoskrnl.exe` and `ntfs.sys`. Tällä hetkellä vain Windows XP ajurit ovat tuettuja. Voit kuitenkin käyttää samoja ajureita myös Windows 2000/NT/2003 osioille.

NTFS ajureiden asennus

Päästäksesi käsiksi NTFS Windows-osoihin ja voidaksesi kirjoittaa näihin osioihin, sinun pitää asentaa ensin NTFS ajurit. Jos et käytä NTFS:sää Windows-osioissa, vaan käytät FAT-muotoa tai tarvitset vain lukuoikeudet tietoihin, voit asentaa (mount) asemat ja päästä käsiksi Windows-asemiin kuten mihin tahansa Linux-asemaan.

NTFS tuen lisäämiseksi osioille, sinun pitää asentaa ensin NTFS ajurit kiintolevyltä, jaetuista resursseista, USB-tikulta tai Windows Update -sivustolta. On suositeltavaa käyttää ajureita tunnetusti turvallisesta sijainnista, koska paikalliset levyasemat Windows-tietokoneessa voivat olla virusten saastuttamia tai muutoin vahingoittuneita.

Kaksoisklikkaa **Install NTFS Write Drivers** kuvaketta työpöydällä suorittaaksesi **BitDefender Captive NTFS Installer** sovelluksen. Valitse ensimmäinen vaihtoehto, jos haluat asentaa ajurit tietokoneen kiintolevyltä.

Jos ajurit ovat tavanomaisessa paikassaan, käytä **Quick search** toimintoa ajureiden hakemiseksi.

Vaihtoehtoisesti voit määritellä mistä ajurit voidaan löytää. Voit myös ladata ajurit Windows Update SP1:stä.

Ajureita ei asenneta kiintolevylle, vaan LinuxDefender käyttää niitä väliaikaisesti päästäkseen käsiksi Windows NTFS osioihin. Jos ohjelma asentaa NTFS ajurit, voit kaksoisklikata NTFS osion työpöytäkuvaketta ja selata sen sisältöä. Käyttääksesi tehokkaampaa tiedostohallintaa, käytä Midnight Commander -sovellusta LinuxDefender -valikosta (tai kirjoita **mc** konsolissa.

12.4.2. Kuinka suoritan virustarkistuksen?

Selaa kansiota, klikkaa oikealla hiiren painikkeella tiedoston tai kansion päällä ja valitse **Send to**. Valitse sitten **BitDefender Scanner**.

Voit myös antaa seuraavan komennon konsolissa. **BitDefender Antivirus Scanner** käynnistyy valittu kansio tai tiedosto tarkistuskohteeksi valittuna.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Valitse sitten **Start Scan**.

Jos haluat konfiguroida virustorjunnan asetuksia, valitse **Configure Antivirus** -välilehti ohjelman vasemmassa reunassa.

12.5. Sisäänrakennettu Instant Mail Filtering Toaster

Voit käyttää LinuxDefeneriä luodaksesi sähköpostin esisuodatusratkaisun, ilman että sinun tarvitsee asentaa mitään ohjelmistoja tai tehdä muutoksia sähköpostipalvelimeen. Tämän tarkoitus on laittaa LinuxDefender -järjestelmä sähköpostipalvelimesi eteen, jolloin BitDefender pystyy tarkistamaan SMTP liikenteen roskapostia ja viruksia vastaan ja välittämään sen todelliselle sähköpostipalvelimelle.

12.5.1. Järjestelmävaatimukset

Tarvitset PC-tietokoneen Pentium III yhteensopivalla proserolilla tai uudemalla, vähintää 256MB RAM ja CD/DVD asema. LinuxDefender järjestelmä pitää määritellä vastaanottamaan SMTP-liikenne todellisen sähköpostipalvelimen sijasta. Asennuksen tekemiseen on muutamia vaihtoehtoja.

1. Vaihda oikean sähköpostipalvelimesi IP-osoite ja määritä sen nykyinen IP-osoite LinuxDefender järjestelmälle.
2. Vaihda DNS merkinnät niin, että domainiesi MX merkintä osoittaa LinuxDefender järjestelmään.
3. Määritä sähköpostiohjelmat käyttämään LinuxDefenderiä SMTP-palvelimena.
4. Vaihda palomuurisi asetukset ohjaamaan kaikki SMTP-yhteydet LinuxDefender järjestelmään oikean sähköpostipalvelimen sijasta.

LinuxDefender - kuinka tehdä -ohjeessa ei kuvailla mitään edellämainituista tehtävistä. Lisätietoja saat seuraavista linkeistä: Linux Networking guides and Netfilter documentation.

12.5.2. Email Toaster

Käynnistä tietokone LinuxDefender CD:llä ja odota, kunnes X Windows -järjestelmä on ladattu ja toimintavalmiina.

Konfiguroidaksesi BitDefender SMTP Proxy:n, kaksoisklikkaa **BitDefender Remote Admin** kuvaketta työpöydällä. Seuraavanlainen ikkuna aukeaa. Käytä `bd` käyttäjänimenä ja `bd` salasanana sisäänkirjautumiseksi.

Onnistuneen kirjautumisen jälkeen voit konfiguroida SMTP Proxyn.

Valitse **SMTP Proxy** konfiguroidaksesi todellisen sähköpostipalvelimen, jonka haluat suojata viruksia ja roskapostia vastaan.

Valitse **Email domains** -välilehti kirjoittaaksesi kaikki sähköpostidomainit, joilta haluat vastaanottaa sähköpostia.

Valitse **Add Email Domain** tai **Add Bulk Domains** ja seuraa näytön ohjeita asettaaksesi sähköpostidomainit.

Valitse **Net domains** -välilehti kirjoittaaksesi kaikki domainit joista haluat vastaanottaa sähköpostia.

Valitse **Add Net Domain** tai **Add Bulk Net Domains** ja seuraa näytön ohjeita asettaaksesi verkkodomainit.

Vaitse **Antivirus** vasemmanpuoleisesta valikosta valiteksasi, miten toimitaan viruken löytyessä ja konfiguroidaksesi muita virustorjunnan vaihtoehtoja.

Nyt kaikki SMTP-liikenne tarkistetaan ja suodatetaan BitDefenderin toimesta. Oletuksena, kaikki saastuneet viestit puhdistetaan tai estetään ja kaikki roskaposti, jonka BitDefender havaitsee, merkitään Aihe -kenttään sanalla `[SPAM]`. Sähköpostin ylätunniste (`X-BitDefender-Spam: Yes/No`) lisätään kaikkiin sähköposteihin helpottamaan sähköpostisovelluksen sisäistä suodatusta.

12.6. Tee verkon turvallisuustarkistus

Tietojen palauttamisen ja sähköpostin suodattamisen lisäksi LinuxDefender sisältää sarjan työkaluja, joilla voidaan suorittaa syvälle meneviä tietokoneen ja verkon valvontatoimenpiteitä. Seuraavia ohjeita noudattamalla voit suorittaa nopean turvallisuustarkistuksen verkossasi.

12.6.1. Tee Rootkit tarkistus

Ennen kuin alat etsiä tietotuvariskejä verkon tietokoneista varmista, että kone jossa LinuxDefenderiä käytetään ei ole saastunut. Voit suorittaa virustarkistuksen tietokoneen kiintolevyille, ohjeen **Tarkista viruksia vastaan** mukaisesti tai voit tehdä Unix rootkit tarkistuksen.

Ensimmäiseksi, ota käyttöön kiintolevyosiot kaksoisklikkaamalla niiden työpöytäkuvakkeita tai käyttämällä **mount** -komentoa konsolissa. Kaksoisklikkaa tämän jälkeen **ChkRootKit** -kuvaketta tarkistaaksesi CD:n sisällön tai suorita **chkrootkit** -komento konsolissa käyttämällä `-r NEWROOT` parametriä uuden / (root) hakemiston määrittelemiseksi tietokoneessa.

```
# chkrootkit -r /dev/hda3
```

Jos rootkit löydetään, chkrootkit näyttää löydöksen **LIHAVOITUNA**, käyttäen isoja kirjaimia.

12.6.2. Nessus - verkkoskanneri

> Nessus on maailman suosituin vapaan ohjelmistokoodin verkon haavoittuvuusskanneri, jota käytetään yli 75000:ssa organisaatiossa kautta maailman. Monet maailman suurimmista organisaatioista saavuttavat merkittäviä kustannussäästöjä käyttämällä Nessusta liiketoiminnan kannalta kriittisten laitteiden ja sovellusten valvontaan.
>
> *—www.nessus.org*

Nessusta voidaan etäkäyttää verkon tietokoneiden tarkistamiseksi erilaisia haavoittuvuuksia vastaan. Se ehdottaa myös joitakin mittauksia suoritettavaksi tietoturvariskien vähentämiseksi ja estämiseksi.

Kaksoisklikkaa **Nessus Security Scanner** -kuvaketta työpöydällä tai suorita **startnessus** -komento terminaalissa. Odota kunnes seuraava ikkuna tulee näkyviin. Tietokoneesi resursseista riippuen, Nessuksen lataaminen voi kestää jopa 10 minuuttia johtuen sen yli 5000 lisäosasta ja haavoittuvuus tietokannoista. Käytä `knoppix` käyttäjänimeä ja `knoppix` salasanaa sisäänkirjautumiseksi.

Valitse **Target selection** -välilehti ja kiroita tietokoneiden IP-osoite tai -nimet, jotka halua tarkistaa haavoittuvuuksia vastaan. Varmista, että määrittelet kaikki skannausvalinnat verkon tai järjestelmän kokoonpanon mukaisesti, ennen kuin aloitat skannauksen. Tämä voi säästää merkittävästi verkon kapasiteettia ja resursseja sekä tuottaa tarkemman skannaustuloksen. Valitse sen jälkeen **Start the scan**.

Kun tarkistusprosessi on valmis, Nessus näyttää löydökset ja niiden pohjalta tehdyt suositukset. Voit tallentaa raportin eri muodoissa, mukaanlukien HTML ja graafiset kuvaajat. Tallennettua raporttia voidaan tarkastella käyttämälläsi selaimella.

12.7. Tarkista järjestelmäsi keskusmuistin (RAM) kunto

Jos järjestelmäsi käyttäytyy odottamattomasti (jää jumiin tai käynnistyy jatkuvasti uudelleen omia aikojaan), useimmiten kyseessä voi olla muistiongelma. Voit testata RAM-muistikortit seuraavaksi kuvatulla tavalla, käyttäen ohjelmaa **memtest**

Käynnistä tietokone käyttäen LinuxDefender CD:tä. Kirjoita **memtest** käynnistyksen aikana ja paina Enter.

Memtest käynnistyy välittömästi ja suorittaa muutamia testejä tarkistaakseen RAM-muistin tilan. Voit määritellä, mitä testejä suoritetaan ja muita Memtest-valintoja, painamalla `c` näppäintä.

Täyellinen Memtest -testi voi kestää jopa 8 tuntia, riippuen järjestelmäsi RAM-muitin kapasiteetista ja nopeudesta. On suositeltavaa antaa Memtestin suorittaa kaikki testit kaikkien mahdollisten RAM-virheiden varalta. Voit lopettaa testin milloin tahansa painamalla `ESC` näppäintä.

Jos olet uusimassa järjestelmääsi (koko järjestelmän tai vain joitakin komponentteja), on hyvä käyttää LinuxDefenderiä ja memtest-ohjelmaa virheiden tai yhteensopivuusongelmien selvittämiseksi.

Avun saaminen

Luku 13. Tuki

13.1. Tukiosasto

Korkeatasoisen palvelun tarjoajana, BitDefender panostaa vertaansa vailla olevan, nopean ja luotettavan tuen tarjoamiseen asiakkailleen. Tukikeskus (johon voit ottaa yhteyttä alla olevia yhteystietoja käyttäen) on jatkuvasti viimeisimpien uhkien tasalla. Tukikeskuksesta saat nopeasti vastauksen kaikkiin kysymyksiisi.

BitDefenderille on aina ollut tärkein asia toimittaa huippuluokan tuotteet kohtuulliseen hintaan, tavoitteenaan säästää asiakkaan aikaa ja rahaa. Lisäksi uskomme, että menestyksellinen liiketoiminta perustuu hyvään vuorovaikutukseen ja laadukkaaseen asiakastukeen sitoutumiseen.

Olet tervetullut pyytämään tukea sähköpostitse osoitteessa <support@bitdefender.com> milloin tahansa. Saadaksesi nopean vastauksen, sisällytä viestiisi niin paljon yksityiskohtia kuin voit BitDefender-tuotteestasi sekä järjestemästäsi ja kuvaile kohtaamasi ongelma niin tarkasti kuin mahdollista.

13.2. On-line tuki

13.2.1. BitDefender tukitietokanta

BitDefenderin tukitietokanta (Knowledge Base) on verkossa sijaitseva tietovarasto BitDefender tuotteista. Se sisältää helposti käytettävässä muodossa raportteja teknisen tuen käynnissä olevista tapauksista ja tuotevirheiden korjaamistoimista, joita pitää yllä BitDefenderin tuki- ja kehitystiimit. Se sisältää myös yleistä tietoa virusten ennaltaehkäisystä, yksityiskohtaisia tietoja BitDefender tuotteiden hallinnasta, ja monia muita artikkeleita.

BitDefender tukitietokanta on avoin kaikille ja sisältää vapaan hakutoiminnon. Sen sisältämä laaja informaatio auttaa BitDefender -asiakkaita löytämään tarvitsemaansa yksityiskohtaisempaa teknistä tietoa. Kaikki oleelliset kyselyt ja virheraportit, jotka tulevat BitDefender -asiakkailta, löytävät tiensä lopulta BitDefender tukitietokantaan, kuten virheiden korjaukset, toimintaohjeet ja informatiiviset artikkelit, jotka täydentävät tuotteiden ohjetiedostoja.

BitDefender tukitietokanta on käytettävissä milloin tahansa osoitteessa http://kb.bitdefender.com.

13.3. Yhteystiedot

Tehokas kommunikaatio on avain menestykselliseen liiketoimintaan. Menneiden 10 vuoden aikana, SOFTWIN on saavuttanut kiistattoman maineen jatkuvasti paremmaksi kehittyvään kommunikaatioon panostamisessa, täyttäen asiakkaidemme ja kumppaneidemme odotukset. Jos sinulla on mitä tahansa kysyttävää, älä epäröi ottaa yhteyttä meihin.

13.3.1. Internet-osoitteet

Myynti: <sales@bitdefender.com>
Tekninen tuki: <support@bitdefender.com>
Dokumentaatio: <documentation@bitdefender.com>.
Kumppaniohjelma: <partners@bitdefender.com>
Markkinointi: <marketing@bitdefender.com>
Mediayhteydet: <pr@bitdefender.com>
Työpaikat: <jobs@bitdefender.com>
Virusten toimitus: <virus_submission@bitdefender.com>
Roskapostin toimitus: <spam_submission@bitdefender.com>
Ilmoitus ohjelman väärinkäytöstä: <abuse@bitdefender.com>
Tuotteen kotisivut: http://www.bitdefender.com
Tuotteen ftp-arkisto: ftp://ftp.bitdefender.com/pub
Paikalliset jakelijat: http://www.bitdefender.com/partner_list
BitDefender tukitietokanta: http://kb.bitdefender.com

13.3.2. Toimipaikat

BitDefenderin toimistot ovat valmiita vastaamaan mihin tahansa kyselyihin toimintojensa mukaisesti, sekä kaupallisissa, että yleisissä asioissa. Toimistojen osoitteet ja yhteystiedot on lueteltu alla.

Saksa

Softwin GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Saksa
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>

Myynti: <sales@bitdefender.com>
Internet: http://www.bitdefender.com
Tekninen tuki: <support@bitdefender.com>

Iso-Britannia ja Irlanti

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Myynti: <sales@bitdefender.com>
Internet: http://www.bitdefender.co.uk
Tekninen tuki: <support@bitdefender.com>

Espanja

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Tekninen tuki: <support@bitdefender.com>
Customer Service: 954-776-6262
Internet: http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>

Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Sanasto

ActiveX

ActiveX on tapa kirjoittaa ohjelmia niin, että muut ohjelmat tai käyttöjärjestelmä voi kutsua niitä käyttööntä. ActiveX teknologiaa käytetään Microsoft Internet Explorerin kanssa interaktiivisten Internet-sivustojen tekemiseen, jotka näyttävät ja toimivat kuin tietokoneohjelmat. ActiveX:ää käyttäen, käyttäjät voivat kysyä tai vastata kysymyksiin, käyttää painikkeita ja olla muilla tavoin vuorovaikutuksessa Internet-sivustojen kanssa. ActiveX kontrollit kirjoitetaan usein Visual Basicilla.

ActiveX voidaan luokitella täydellisen tietoturvan puutteen aiheuttajaksi; tietoturva-asiantuntijat varoittavat sen käytöstä Internetissä.

Mainosohjelmat

Mainosohjelmat on usein yhdistetty sovellukseen, joka on ilmainen niin kauan kuin käyttäjä hyväksyy mainosohjelman suorittamisen tietokoneessa. Koska mainosohjelmat asentuvat useimmiten sen jälkeen, kun käyttäjä on hyväskynyt ohjelmiston käyttöehdot, mitään laitonta ei ole tapahtunut.

Tästä huolimatta, ponnahdusikkunoihin avautuvat mainokset voivat alkaa tulla häiritseviksi ja joissakin tapauksissa kuluttaa tietokoneen resursseja. Lisäksi jotkin mainosohjelmat voivat kerätä tietoa, joka liittyy käyttäjien yksityisyyteen, eikä käyttäjä ehkä ole ollut täysin tietoinen käyttöehtojen yksityiskohdista.

Arkisto

Levyke, nauha tai hakemisto, joka sisältää tietoja jotka on varmuuskopioitu.

Tiedosto, joka sisältää yhden tai useamman tiedoston pakatussa muodossa.

Takaportti (Backdoor)

Aukko järjestelmän tietoturvassa, joka on jätetty tarkoituksella auki järjestelmän suunnittelijoiden tai ylläpitäjien toimesta. Tällaisten aukkojen tarkoitus ei aina ole arvelluttava, esimerkiksi niitä voidaan jättää, jotta teknikot tai ylläpitäjät voivat päästä ohjelmaan käsiksi etäyhteyden kautta.

Käynnistyssektori

Sektori joka sijaitsee jokaisen kiintolevyn alussa ja joka yksilöi levyn kokoonpanon (sektorin koko, klusterin koko, jne). Käynnistävillä levyillä, käynnistyssektori sisältää myös ohjelman, joka lataa käyttöjärjestelmän.

Käynnistyssektori-virus

Virus, joka saastuttaa käynnistyslevykkeen käynnistyssektorin. Jos järjestelmä käynnistetään levykkeellä, jonka käynnistyssektorissa on virus, virus aktivoituu

tietokoneen muistiin. Tämän jälkeen virus aktivoituu muistiin joka kerta kun järjestelmä käynnistetään.

Selain

Lyhennys Internet-selaimesta, ohjelmistosovellus jota käytetään Internet-sivustojen etsimiseen ja näyttämiseen. Kaksi suosituinta selainta ovat Netscape Navigator ja Microsoft Internet Explorer. Molemmat näistä omaavat graafisen käyttöliittymän, mikä tarkoittaa, että ne voivat näyttää sekä tekstiä että grafiikkaa. Lisäksi useimmat nykyaikaiset selaimet pystyvät näyttämään myös multimediaa, mukaanlukien ääntä ja videota, erilaisten selaimen lisäosien avulla.

Komentorivi

Komentorivi -käyttöliittymässä käyttäjä kirjoittaa komennot suoraan näytöllä olevalle komentoriville, käyttäen komentokieltä.

Eväste

Internetteollisuudessa evästeet kuvaillaan pieniksi tiedostoiksi, jotka sisältävät yksittäisistä tietokoneista kerättyä tietoa, jota voidaan analysoida ja käyttää kiinnostuksen kohteiden ja mieltymysten seuraamiseen mainostajien toimesta. Tällä alueella evästeteknologia kehittyy koko ajan ja tarkoituksena on suunnata mainokset suoraan vastaamaan kiinnostuksen kohteitasi. Tämä on "kaksiteräinen miekka" monille ihmisille, koska toisaalta saat nähtäväksesi vain mainoksia, jotka liittyvät kiinnostuksen kohteisiisi. Toisaalta siihen liittyy jatkuvaa "seurantaa" ja "valvontaa" siitä millä sivustoilla käyt ja mitä valintoja teet eri sivustoilla. Tämä luonnollisesti kyseenalaistaa yksityisyyden ja monia ihmisiä loukkaa tieto siitä, että he ovat ikään kuin "viivakoodilla" merkittyjä (samaan tapaan kuin kaupan kassalla rekisteröidään tuote viivakoodin avulla kaupan järjestelmiin). Tämä vertaus on ehkä äärimmäinen, mutta joissakin tapauksissa paikkansapitävä.

Levyasema

Laite, joka lukee ja kirjoittaa tietoa levylle.

Kiintolevyasema lukee ja kirjoittaa kiintolevylle.

Levykeasema käyttää levykkeitä.

Levyasemat voivat olla joko sisäisiä (tietokoneeseen kiinteästi asennettuja) tai ulkoisia (erillisiä laitteita, jotka liitetään tietokoneeseen).

Lataaminen

Tietostojen kopiointia päälähteestä etälaitteeseen. Tätä termiä käytetään usein kuvaamaan prosessia, jossa online palvelusta kopioidaan tiedosto omalle tietokoneelle. Lataus voi myös viitata tiedoston kopiointiin tietoverkon tiedostopalvelimelta toiselle verkon tietokoneelle.

Sähköposti

Sähköpostijärjestelmä on palvelu, joka välittää viestejä tietokoneille paikallisissa- tai maailmanlaajuisissa verkoissa.

Tapahtumat

Toiminto tai tapahtuma, jonka jokin ohjelma on havainnut. Tapahtumat voivat olla käyttäjän aiheuttamia, kuten hiiren klikkaus tai näppäimen painallus, tai järjestelmän tapahtumia, kuten muistin loppuminen.

Virheellinen tunnistus

Tapahtuma joka syntyy, kun tarkistuksessa havaitaan tiedosto saastuneeksi, vaikka se ei oikeasti olekaan saastunut.

Tiedostopääte

Tiedoston nime osa, joka on tiedoston nimessä pisteen jälkeen ja joka osoittaa minkälaista tietoa tiedosto sisältää.

Monet käyttöjärjestelmät käyttävät tiedostopäätteitä, esim. Unix, VMS ja MS-DOS. Tiedostopääte on useimmiten yhdestä kolmeen merkkiä (jotkin vanhat käyttöjärjestelmät tukevat vain kolmea merkkiä). Esimerkkejä tällaisista ovat "c" joka merkitsee C -lähdekoodia, "ps" PostScriptiä, "txt" teksitiedostoa.

Heuristinen suodatin

Sääntöihin perustuva menetelmä uusien virusten tunnistamiseksi. Tämä tarkistusmenetelmä ei perustu yksilöityihin virustunnisteisiin. Heuristisen tarkistuksen etuna on se, että olemassa olevien virusten uudet muunnelmat eivät pysty huijaamaan sitä. Se voi kuitenkin ajoittain ilmoittaa epäilyttävästä koodista normaalien ohjelmien kohdalla, aiheuttaen niin sanotun "väärän tunnistuksen"

IP

Internet-protokolla - reitittävä protokolla, joka on osa TCP/IP -protokollaa ja joka huolehtii IP-osoituksesta, reitittämisestä ja IP-pakettien pirstomisesta ja uudelleen kokoamisesta.

Java -pienoissovellus

Java-ohjelma, joka on suunniteltu suoritettavaksi vain Internet-sivulla. Käyttääksesi pienoissovellusta Internet-sivulla, sen nimi ja koko, jonka pienoissovellus voi ottaa käyttöön, pitää määritellä (pituus ja leveys pikseleinä). Kun Internet-sivulle siirrytään, selain lataa pienoissovelluksen palvelimelta ja suorittaa sen käyttäjän tietokoneella. Pienoissovellukset eroavat sovelluksista siten, että tiukat tietoturvaprotokollat eivät ohjaa niitä.

Esimerkiksi, vaikka pienoissovellukset suoritetaan asiakkaan tietokoneessa, ne eivät voi lukea tai kirjoittaa tietoja asiakkaan tietokoneeseen. Lisäksi pienoissovellukset ovat rajoitettuja toiminnaltaan, niin että ne voivat vain lukea ja kirjoittaa tietoja toimialueensa sisällä.

Makrovirus

Tietokonevirus, joka on koodattu makroksi dokumentin sisälle. Monet sovellukset, kuten Microsoft Word ja Excel, tukevat makroja.

Nämä sovellukset sallivat makrojen sisällyttämisen dokumentteihin ja makrojen suorittamisen aina, kun dokumentti avataan.

Sähköpostisovellus

Sähköpostisovellus on ohjelma, jolla voi lähettää ja vastaanottaa sähköpostia.

Muisti

Tietokoneen sisäinen tietovarasto. Termi "muisti" tarkoittaa tietovarastoa, joka on mikropiirin muodossa ja sanaa tietovarasto käytetään muistista, joka sijaitsee nauhalla tai levyillä. Jokainen tietokone toimitetaan tietyllä määrällä fyysistä muistia, useimmiten tästä käytetään nimitystä keskusmuisti tai RAM-muisti.

Ei-heuristinen

Tämä tarkistustapa perustuu määrättyihin virustunnisteisiin. Ei-heuristisen tarkistuksen etuna on se, että sitä ei voi huijata jokin ohjelma, joka näyttäisi olevan virus, eikä näin ollen aiheuta vääriä hälytyksiä.

Pakatut ohjelmat

Tiedosto pakatussa muodossa. Monet käyttöjärjestelmät ja sovellukset sisältävät komentoja, jotka sallivat sinun pakata tiedostoja, jotta ne veisivät vähemmän tilaa. Esimerkiksi voitaisiin olettaa, että sinulla on tekstitiedosto, joka sisältää kymmenen peräkkäistä välilyöntiä. Normaalisti tämä vaatisi kymmenen tavua tilaa.

Ohjelma, joka pakkaa tiedostoja, korvaa välilyöntimerkit erityisellä välilyönti-sarja merkillä ja numerolla, joka kertoo kuinka monta välilyöntiä sillä korvataan. Tässä tapauksessa kymmentä välilyöntiä varten tarvitaan vain kaksi tavua tilaa. Tämä on vain yksi pakkaustapa - niitä on olemassa monia muitakin.

Polku

Tarkka viittaus tiedostoon tietokoneella. Nämä viittaukset ovat usein kuvattu hierarkkisena arkistoinitijärjestelmänä, lueteltuna ylhäältä alaspäin.

Reitti minkä tahansa kahden pisteen välillä, kuten viestintäkanavana kahden tietokoneen välillä.

Tietokalastelu (Phising)

Käyttäjälle lähetetään sähköposti, jossa väitetään valheellisesti sen olevan luotettavasta lähteestä, ja jossa huijataan käyttäjää antamaan yksityisiä tietoja, joita käytetään laittomiin tarkoituksiin. Sähköpostiviesti ohjaa käyttäjiä käymään Internet-sivustolla, joissa heitä pyydetään päivittämään henilökohtaisia tietojaan, kuten salasanoja ja luottokorttitietoja, henkilötunnusta ja pankkitilitietoja - tietoja jotka laillisella taholla olisi tiedossaan jo muutenkin. Tällainen Internet-sivusto on kuitenkin hämäystä ja tehty vain käyttäjän tietojen varastamiseksi.

Monimuotoinen virus

Virus, joka vaihtaa muotoaan jokaisen saastuttamansa tiedoston kohdalla. Koska tällaisilla viruksilla ei ole johdonmukaista binäärimallia, niitä on vaikea tunnistaa.

Portti

Tietokoneen liittymä, johon voidaan kytkeä laitteita. Tietokoneissa on eri tyyppisiä portteja. Tietokoneen on erinäisiä portteja, joihin voidaan liittää levyasemia, näyttöjä, näppäimistöjä, modeemeja, tulostimia, hiiriä ja muita oheislaitteita.

TCP/IP ja UDP -verkoissa, portti on loogisen yhteyden päätepiste. Portin numero yksilöi, minkä tyyppinen portti on. Esimerkiksi porttia 80 käytetään HTTP liikenteeseen.

Raportti tiedosto

Tiedosto, joka luetteloi tapahtumia. BitDefender ylläpitää raporttitiedostoa, joka luetteloi tarkistupolut, kansiot, tarkistettujen tiedostojen ja arkistojen lukumäärän ja kuinka monta saastunutta ja epäilyttävää tiedostoa löydettiin.

Rootkit

Rootkit on joukko ohjelmistotyökaluja, jotka mahdollistavat pääkäyttäjätason pääsyn järjestelmään. Termiä käytettiin ensiksi UNIX-käyttöjärjestelmissä ja se viittasi uudelleen käännettyihin työkaluihin, jotka antoivat tunkeutujille pääkäyttäjän oikeudet ja mahdollistivat niiden piiloutumisen niin, ettei verkon pääkäyttäjät voineet havaita niitä.

Rootkittien päärooli on piilottaa prosesseja, tiedostoja, kirjautumisia ja lokeja. Ne voivat myös siepata tietoja päätteistä, verkkoyhteyksistä tai oheislaitteista, jos ne ovat yhteydessä kyseessä olevaan ohjelmistoon.

Rootkitit eivät ole haitallisia luonnostaan. Esimerkiksi, järjestelmät ja jopa jotkin sovellukset piilottavat kriittisiä tiedostoja käyttäen rootkittejä. Niitä käytetään kuitenkin useimmiten kätkemään haittaohjelmia tai piilottamaan tunkeutujan järjestelmässä. Kun rootkit on yhdistetty haittaohjelmaan, se on suuri uhka järjestelmän eheydelle ja turvallisuudelle. Ne voivat tarkkailla liikennettä, tehdä takaportteja järjestelmään, muuttaa tiedostoja ja lokeja ja välttää tunnistautumisen.

Script

Toinen nimitys makro- tai komentojonotiedostolle, script on luettelo komennoista, jotka voidaan suorittaa ilman käyttäjän toimia.

Roskaposti

Sähköistä roskapostia tai -uutisryhmäviestejä. Yleisesti mikä tahansa roskapostiksi tunnistettava sähköpostiviesti.

Vakoiluohjelma

Mikä tahansa ohjelmisto, joka kerää salaa käyttäjätietoja tämän Internet-liittymän kautta niin, ettei käyttäjä tiedä siitä, useimmiten mainostamistarkoituksessa.

Vakoiluohjelmat on tyypillisesti paketoitu piilotetuksi komponentiksi ilmaiseen tai vapaasti jaettavaan ohjelmistoon, joka voidaan ladata Internetistä; on kuitenkin huomattava, että suurin osa ilmais- ja vapaasti jaeltavista ohjelmista eivät sisällä vakoiluohjelmia. Kun vakoiluohjelman sisältävä ohjelmisto on kerran asennettu, vakoiluohjelma tarkkailee käyttäjän toimia Internetissä ja välittää tiedot jollekin muulle taholle. Vakoiluohjelma voi myös kerätä tietoja sähköpostiosoitteista ja jopa salasanoja sekä luottokorttinumeroita.

Vakoiluohjelman samankaltaisuus Troijan hevosten kanssa on siinä, että käyttäjä tietämättään asentaa tällaisen ohjelmiston asentaessaan jotain muuta ohjelmistoa. Yleinen tapa joutua vakoiluohjelman uhriksi on ladata jokin tiedosto vertaisverkoista (peer-to-peer), joissa vaihdetaan ja jaellaan tiedostoja.

Yksityisyys- ja eettisyyskysymysten lisäksi, vakoiluohjelma varastaa tietokoneen muistiresursseja ja hidastaa käyttäjän Internet-yhteyttä lähettäessään tietoja vakoiluohjelman lähteelle. Koska vakoiluohjelma käyttää musti- ja järjestelmäresursseja, taustalla käynnissä olevat ohjelmat voivat aiheuttaa järjestelmän kaatumisia tai yleistä epävakautta.

Käynnistyksen kohteet

Mikä tahansa tiedosto, joka on sijoitettu tähän kansioon, käynnistyy tietokoneen käynnistymisen yhteydessä. Esimerkiksi aloitusikkuna, ääni joka soitetaan tietokoneen käynnistyessä, kalenteri tai jokin sovellus voi olla käynnistyksen kohde. Normaalisti tällaisen ohjelman pikakuvake on sijoitettu tähän kansioon, ei itse tiedosto.

Ilmaisinalue

Windows 95:stä lähtien, ilmaisinalue on sijoitettu tehtäväpalkkiin (useimmiten alhaalla kellon vieressä) ja sisältää pienoiskuvakkeet järjestelmän toimintoihin, kuten fax, tulostin, äänenvoimakkuus ja muut toiminnot. Kaksoisklikkaa tai klikkaa hiiren oikella painikkeella kuvaketta tarkastellaksesi kohteen tietoja tai hallitaksesi kohdetta.

TCP/IP

Transmission Control Protocol/Internet Protocol - joukko verkkoprotokollia, joita käytetään laajasti Internetissä ja jotka mahdollistavat tietokoneiden viestinnän yhteiskäyttöverkkojen yli erilaisten järjestelmäkokoonpanojen ja käyttöjärjestelmien välillä. TCP/IP sisältää standardeja, millä tavoin tietokoneet viestivät, kuinka ne yhdistyvät verkkoihin ja reitittävät liikenteen.

Troijalainen

Tuhoisa ohjelma, joka naamioituu turvalliseksi ohjelmaksi. Toisin kuin virukset, Troijalaiset eivät monista itseään, mutta voivat olla aivan yhtä tuhoisia. Yksi kaikkein petollisimmista Troijalais-tyypeistä on ohjelma, joka väittää puhdistavansa tietokoneesi viruksista, mutta sen sijaan asentaakin viruksia tietokoneeseesi.

Termi on peräisin historiasta, Homeroksen Iliaan tarinasta, jossa Kreikkalaiset antavat valtavatn puisen hevosen vihollisilleen Troijalaisille, näennäisesti rauhantarjouksena. Mutta kun Troijalaiset ovat siirtäneet hevosen kaupungin muurien sisäpuolelle, Kreikkalaiset sotilaan hiipivät ulos hevosen sisältä ja avaavat kaupungin portit, jolloin heidän maanmiehensä syöksyvät sisään ja valloittavat kaupungin.

Päivitys

Uusi versio ohjelmasta tai laitteesta, joka on tarkoitettu korvaamaan vanhempi versio samasta tuotteesta. Päivitysten asennusrutiinit tarkistavat useimmiten, onko tuotteesta olemassa vanhempi versio tietokoneessa; jos sitä ei löydy, päivitystä ei voi asentaa.

BitDefenderissä on oma päivitysosa, joka sallii käyttäjän tarkistaa päivitysten saatavuus, tai antaa sen automaattisesti päivittää tuotteen.

Virus

Ohjelmisto tai osa koodia, joka ladataan tietokoneeseesi tietämättäsi ja suoritetaan tahtomattasi. Useimmat virukset voivat myös monistaa itsensä. Kaikki tietokonevirukset ovat jonkun tekemiä. Ykisinkertainen virus, joka osaa kopioida itsensä uudestaan ja uudestaan, on suhteellisen helppo tehdä. Jopa tällainen yksinkertainen virus on vaarallinen, koska se ottaa käyttöönsä nopeasti kaiken vapaana olevan muistin ja lamauttaa järjestelmän. Vielä vaarallisempi virustyyppi on sellainen, joka pystyy välittämään itsensä verkkojen yli ja ohittamaan tietoturvajärjestelmät.

Virustunniste

Viruksen binäärimalli, jota käytetään virustorjuntatuotteissa virusten havaitsemiseksi ja poistamiseksi.

Mato

Ohjelma, joka levittää itseään verkon yli, monistaen itseään jatkuvasti. Se ei voi liittää itseään muihin ohjelmiin.