

Norman Internet Control v5.8

Täydellinen Internet- ja virussuoja

Norman Internet Control (NIC) tarjoaa täydellisen suojan hakkereita sekä muita haitallisia toimintoja vastaan yhdellä helppokäyttöisellä ratkaisulla. Tämä tuote sisältää palkintoja voittaneen Norman Virus Controlin sekä Norman Personal Firewallin yhtenä tuotteena, jolloin käyttäjä voi rauhassa selata internet-sivuilla.

Norman Internet Controllin avainominaisuudet

- Tarkistaa sähköpostit viruksilta, madoilta ja troijalaisilta
- Tiedostojen reaaliaikainen virustarkistus
- Ainutlaatuinen Norman SandBox-teknologia tuntemattomien virusten reaaliaikaiseen havaitsemiseen ja eliminoimiseen
- Lapsenvahti, jolla voidaan rajoittaa lasten surffaamista epäasiallisilla Internet-sivustoilla
- Kiusallinen aineisto
- Hakkereiden esto
- Automaattinen päivitys Internetistä

Ominaisuudet

Sähköpostin ja uutisryhmien skannaus

Reaaliaikainen virustarkistus

Norman SandBox

Turvallinen yhteys

«Lapsenvahti»

Ajastin, jolla voidaan määrittää yhteyksien sallittu käyttöaika

Kiusallinen aineisto

Tarkistussumma

Evästeiden hallinta

Luotetut sivustot

MAC-osoitteen luvallisuuden tarkistus

Porttiskannausten tarkkailu ja kirjaus

JavaScriptillä toteutettujen mainosten esto

Luotetut IP-osoitteet

Automaattiset päivitykset

Sähköpostin ja uutisryhmien skannaus

NVC skannaa kaikki sisään tulevat ja ulos lähtevät sähköpostiviestit sekä uutisryhmiin jätetyt ja niistä ladatut viestit tarkastaen, etteivät ne sisällä minkäänlaisia haitallisia ohjelmia. Lisäksi tietyt nimiset tai tietyllä tiedostotunnisteella varustetut liitteet voidaan torjua. Sähköpostiviestien skannaus toimii useimmilla nykyisin saatavissa olevilla sähköpostiohjelmilla.

NIP ottaa tarkkailuun kaikki Winsockia käyttävät sovellukset. Kaikkien porttien liikenteestä skannataan POP3, SMTP ja NNTP. Norman Internet Protection (NIP) minimoi uusien ja nykyisten sähköpostimatojen aiheuttaman vaaran parhaalla virusskannauksella ja suoraviivaisella liitteiden torjunnalla. Suosittelemme, että käytössä on myös Normanin SandBox. Se parantaa suojausta tuntemattoman ja tunnetun haitallisen ohjelman aiheuttamaa vaaraa vastaan.

Reaaliaikainen virustarkistus

On-access-skannaus tarkoittaa sitä, että työasemien tiedostojärjestelmiä tarkkaillaan jatkuvasti. On olennaista, että virustorjuntaohjelma havaitsee ja torjuu haitallisen ohjelman ennen sen aktivoitumista. Aina kun tiedostoa luetaan tai siihen kirjoitetaan tai kun ohjelma suoritetaan, on-access-skanneri saa ilmoituksen ja tarkastaa tiedoston automaattisesti. Jos haitallinen ohjelma löytyy, käytettävissä ovat seuraavat vaihtoehdot:

- puhdistus
- poisto
- pelkkä varoitus
- huomiotta jättäminen

Norman SandBox

Norman SandBox -teknologia perustaa tietokoneen muistiin virtuaalisen tietokoneen ja -verkon, jossa virus voi monistua suljetulla alueella tiukan tarkkailun alaisena. Kun virus on aktivoitunut, «hiekkalaatikko» tutkitaan ja virukselle kehitetään torjuntatapa samanaikaisesti. Tämä ainutlaatuinen tekniikka pysäyttää ja eristää tietokonetta uhkaavat vahingolliset ohjelmat niiden käyttäytymisen perusteella jopa ennen kuin kyseisiä vahingollisia ohjelmia vastaan on julkaistu mitään virusmääritetietokantojen päivityksiä.

Turvallinen yhteys

Norman Personal Firewall valvoo tietoliikennettä molempiin suuntiin.

NPF:lla voidaan kontrolloida sitä, kuka voi katsella ja kenellä on pääsy jaettuihin kansioihin. Sillä voidaan jopa estää muita näkemästä, että koneesi on kytketty verkkoon. Näin ulkopuoliset eivät pääse tunkeutumaan tietokoneellesi luvatta.



Peace of Mind

Norman is one of the world's leading companies within the field of data security. With products for virus control, spam control, email control, download control, personal firewall, encryption, data recovery, certified data erasure and computer forensics, the company plays an important role in the data industry.

NORMAN®

www.norman.com



- Toisaalta NPF tarkkailee jokaista sovellusta, joka pyrkii luomaan yhteyden ulospäin Internetiin tai lähiverkkoon. Jokaiselle sovellukselle osoitetaan oma «vartija» tarkkailua varten. Sovelluksia, jotka eivät käytä Internetiä tai verkkoa, ei valvota ollenkaan. Näin tietokoneen tehoa ei kuluteta turhaan.

- Enää sinun ei tarvitse kytkeytyä Internetiin tai verkkoon huolehtien siitä, että koneeseesi asennetut sovellukset lähettävät tietojasi ulkopuolelle sinun tietämättäsi. Troijalaiset, jotka pyrkivät kontrolloimaan järjestelmäsi sisään tulevien yhteyksien kautta, havaitaan heti samoin kuin scriptit, jotka pyrkivät lähettämään sähköpostia sinun nimissäsi.

Lapsilukko Web-selailuun

- Tämä ominaisuus mahdollistaa sen, että vanhemmat määrittävät erilaisia käyttäjätilejä erilaisilla käyttöoikeuksilla eri Web-sivustoille.

Skenaario:

- *4-vuotias Mari saa selailla ainoastaan joitakin Web-sivustoja (www.disney.com jne.) Jari puolestaan voi selailla mitä tahansa sivustoja paitsi niitä, joilla on pornograafista materiaalia. Kielletyt sivut estetään URL-osoitteen, osoitteessa esiintyvien sanojen tai sivustolla esiintyvien sanojen perusteella.*
- *Vanhemmat voivat editoida kiellettyjen sanojen listaa ja lisätä esim. sanoja, joita he eivät halua Jarin näkevän.*

Ajastin

- Vanhemmat voivat määrittää yhdelle tai useammalle käyttäjätilille salasanan.

- Jokaiselle käyttäjätilille voidaan määrittää erillinen käyttöaika per päivä/vko/kk ja/tai vuorokauden kellonaika.

Skenaario:

- *Jonilla on pääsy Internetiin illalla klo 16-21.00 välisenä aikana korkeintaan 5 tuntia vkossa. Mari saa myös käyttää Internetiä 5 tuntia vkossa, mutta sen pitää tapahtua klo 13- 18.00*

Kiusallinen aineisto

- Active-X:t, Java/VB Scriptit ja Java Appletit on tarkoitettu rikastuttamaan käyttäjien kokemuksia ja elämyksiä Internetissä. Kuitenkin, niiden vahingolliset versiot voivat aiheuttaa vakavia tietoturvaohkia.
- NPF antaa sinulle kattavan kontrollin siitä, mitkä sivustot voivat aktivoida tälläisen koodin koneessasi ja mitkä estetään. Kun tietokoneeseesi on asennettu NPF, tällaiset tietoturvaohjat ovat historiaa.

Tarkistussumma

- Tarkistussumma on tarkoitettu kaikille suoritettaville ohjelmille (sovelluksille), jotka on tallennettu sääntötietokantaan (pois lukien itse järjestelmä). Näin NPF tunnistaa mahdollisen troijalaisen, joka yrittää teeskennellä olevansa tunnettu Internet-sovellus.

Skenaario:

- *Joku asentaa koneeseesi takaoven, jonka nimi on IEXPLORER.EXE. Se sattuu olemaan sama nimi kuin Microsoftin Internet Explorerilla. NPF:n pitäisi sisälittää säännöt, jotka sallivat tämän ohjelman yhteydenotot http, https ja ftp –protokollia käyttäville sivustoille. Koska NPF ei tunnista tiedostojen eroa sisällön perusteella, se sallisi yhteyden Internetiin. Käyttäjällä pitää olla mahdollisuus ylläpitää ja päivittää tarkistussumma jos NPF havaitsee virheen. Tarkistussumman päivittäminen sallitaan ainoastaan silloin kun käyttäjä tiedostaa, että järjestelmä on päivitetty service pack:illa tai uudella ohjelmaversiolla..*

Evästeiden hallinta

- Internetissä surffatessasi web-sivustot yrittävät kerätä käyttäytymismalleja. Pieniä informaatiopalasia lähetetään selaimesi ja tarkastelemasi web-sivuston välillä. Näiden informaatiopalasten nimi on englanniksi «cookie», suomeksi niitä sanotaan esim. pipareiksi tai evästeiksi. Niiden avulla sivustot erottavat kävijät toisistaan, mutta niitä voidaan myös kerätä ja käyttää tiedon hankkimiseen sinun surfaustavoitiasi. Norman Internet Controlin avulla voit määrätä, mitkä sivustot saavat kerätä sinusta tätä informaatiota, mitkä eivät.

- Sellainen surfausinformaatio kuin «referrer» (se sivu, jolta tulit kyseiselle sivulle) voidaan myös estää.

Luotetut sivustot

- Tämä ominaisuus parantaa käyttäjystävällisyyttä, koska se antaa käyttäjän hyväksyä tietyn sivuston kaiken aktiivisen sisällön (siis luottaa siihen) yhdellä säännöllä. Se vähentää niiden «varoitusten» määrää, joiden vuoksi käyttäjän on tehtävä joitain toimenpiteitä tuolla sivustolla käydessään.

Järjestelmävaatimukset

MAC-osoitteen luvallisuuden tarkistus

- Tämä ominaisuus on hyödyllinen tilanteissa, jossa kaksi tietokonetta tai useampi on kytketty sellaiseen DSL-reitittimeen, joka antaa oman julkisen IP-osoitteen jokaiselle siihen kytketylle tietokoneelle.
- Ilmoittamalla Norman Internet Controlille, mihin MAC-osoitteeseen tulee luottaa, samaan keskittimeen kytketyt, julkiset IP-osoitteet omaavat tietokoneet voivat kommunikoida vapaasti toistensa kanssa.

Porttiskannausten tarkkailu ja kirjaus

- Järjestelmäsi eri portteihin voi joskus saapua lukuisia paketteja samasta lähteestä. Kun tämä tapahtuu tietyn ajan puiteissa, Norman Internet Control katsoo tapahtuman porttiskannaukseksi ja merkitsee sen lokiin. Porttiskannausten tarkoitus on saada selville, mitä palveluja järjestelmäsi tarjoaa, ja sitä voidaan käyttää esitutkimuksena ennen kuin järjestelmäsi yritetään tunkeutua.

JavaScriptillä toteutettujen pop-up-ikkunoiden esto

- Norman Internet Controlilla voit torjua tai hyväksyä JavaScript-tekniikalla lähetetyt pop-up-ikkunat.
- Vaikka tämä toiminto pysäyttää useimmat automaattisesti lähetetyt pop-upit, se voi päästää läpi muilla tekniikoilla lähetettyjä pop-upeja. Ota myös huomioon, että jos joku sivusto lähettää tällä tekniikalla asiallisen ikkunan, sekin torjutaan.

Luotetut IP-osoitteet

- Tällä toiminnolla voit lisätä yksittäisiä IP-osoitteita tai osoitesarjoja, joihin luotat ja joiden kanssa haluat jakaa palveluja.

Automaattiset päivitykset

- Norman Internet Update (NIU) on NVC:n kiinteä osa, ja se voidaan asettaa hakemaan säännöllisin väliajoin uusia ja päivitettyjä tiedostoja Normanin tuotepalvelimista. NIU päivittää sovellusohjelman ja virusten määrittelytiedoston varmistuen, että asennettuna on aina ohjelman uusin versio.

- NIU käyttää määrittelytiedostojen inkrementaalipäivitystä, jolloin päivitykset ovat mahdollisimman pieniä, mikä lyhentää latausaikaa.

- Pentium tasoinen PC, jossa Windows 95/98/Me tai Windows NT/2000/XP.
- Windows 95 Internet Explorer versio 4.0 tai uudempi vaaditaan.
- Windows NT Service Pack 4 tai uudempi vaaditaan.



22 x "100%" awards



Norman solutions for clients/workstations: Norman Virus Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (On-Demand scanning) | Norman Internet Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP | Norman Personal Firewall | Norman Privacy

Norman solutions for servers: Norman Virus Control for Microsoft Windows NT4.0, 2000, 2003, XP | Norman Virus Control Firebreak for Novell Netware 4.11 and later | Norman Virus Control for Linux

Norman solutions for web, gateways and mailservers: Norman Spam Control | Norman Email Control | Norman Download Control | Norman Virus Control Net | Norman Virus Control for Lotus Domino (Win32, OS/2) | Norman Virus Control for Firewall-1 NG | Norman Virus Control for Microsoft Internet Information Server | Norman Virus Control for Microsoft Exchange | Norman Virus Control for MIMESweeper

NORMAN[®]

www.norman.com