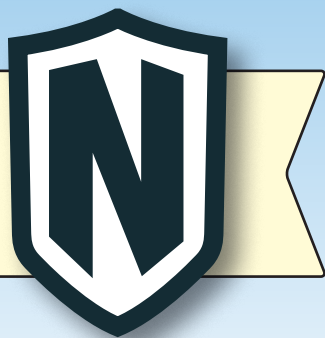




OVELA RATKAISU:

Viritä ansa hakkereille

Jos tietokoneeseen iskee kiristysohjelma, se lukitsee tiedotosi ja tekee niistä käyttökeltottomia. Kätevällä Data Sentinel -työkalulla päihität hakkerit ja turvaat tiedotosi.



Toimittaja
Niklas Ernst

Yleensä on vaarana langeta itse ansaan, kun tietoverkkorikolliset ja hakkerit tekevät häilyjä suunnitelmiaan ja saavat sinut asentamaan tietokoneellesi haittaohjelmia, viruksia tai kiristysohjelmia. NeuShield Data Sentinel -ohjelmalla sinä sen sijaan asetat itse ansan hakkereille.

Periaatteessa se suojaa sinua ransomware-ohjelmilta eli haittaohjelmilta, jotka voivat lukita tiedostosi. Sitten niiden tekijät voivat vaatia lunnaita tiedostojen lukituksen avaamisesta, jotta voisit käyttää niitä uudel-

leen. Kun Data Sentinel on tietokoneellasi, sinun ei kuitenkaan tarvitse maksaa konnille penniäkään, sillä se auttaa sinua pelastamaan tiedostosi hakkerien tehokkaalta salaukselta. Tai se ei oikeastaan pelasta tiedostojasi vaan piilottaa ne, jolloin hakkerit luulevat saaneensa tiedostosi käsiinsä – mutta todellisuudessa on tapahtunut jotain aivan muuta.

Ohjelman toimintaperiaate

Näin se toimii: Kuvittele suuri valkotalu, jossa on tekstiä. Teksti on tiedostosi. Kuvittele nyt, että taulun päälle asetetaan näkymätön, suuri lasilevy. Kun joku yrittää muuttaa tekstiäsi, näyttää siltä kuin hän olisi kir-

joittanut jotain sen päälle. Hän on kuitenkin kirjoittanut vain lasilevylle, joka on helppo pyyhkiä puhtaaksi – ja levyn alla teksti on edelleen täsmälleen samanlainen kuin ennenkin.

Data Sentinel luo tiedostoistasi joukon väärennettyjä versioita, joita hakkerit luulevat oikeiksi tiedostoiksi, jotka he sitten salaavat kiristysohjelmalla. Oikeat tiedostosi pysyvät turvassa, ja voit helposti noukkia ne näkyville kiristysohjelmahyökkäyksen jälkeen, sillä hakkerit ovat saaneet haltuunsa vain väärennetyt syötittiedostot. Roistot saavat pitkän nenän – ja sinä saat pitää tiedostosi turvassa – sillä ulkopuoliset eivät pääse käsiksi mihinkään tärkeään.

Salaus

Kun tiedot tai viestintä salataan, sisältö muutetaan lukukeltvottomaksi matemaattisella menetelmällä, jolloin aineiston lukeminen uudelleen vaatii avaimen (joka on tyypillisesti salasana).

Kiristysohjelmat

Ransomware eli kiristysohjelma on haittaohjelma, joka salaa ja lukitsee tiedostosi. Sitten sen tekijät vaativat lunnaita purkaakseen salauksen, jotta saisit taas pääsyn niihin.



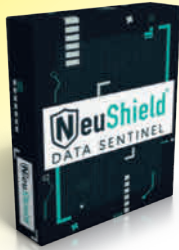
**NeuShield Data
Sentinel**

Pidä hyvää huolta tiedostoistasi ja varmista, että hakkerit tai tietoverkkorikolliset eivät onnistu salaamaan niitä.

Kieli
Englanti

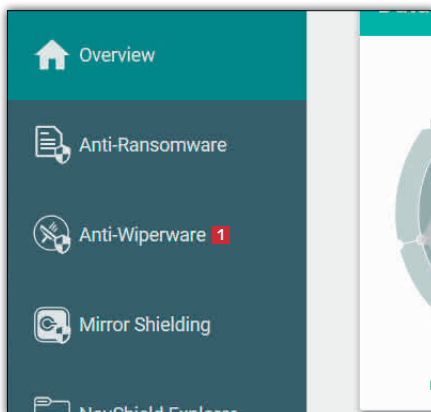
Järjestelmä
Windows 10 ja 11

**Lataa
ohjelma
verkkosivuiltamme:**
kotimikro.fi/2419

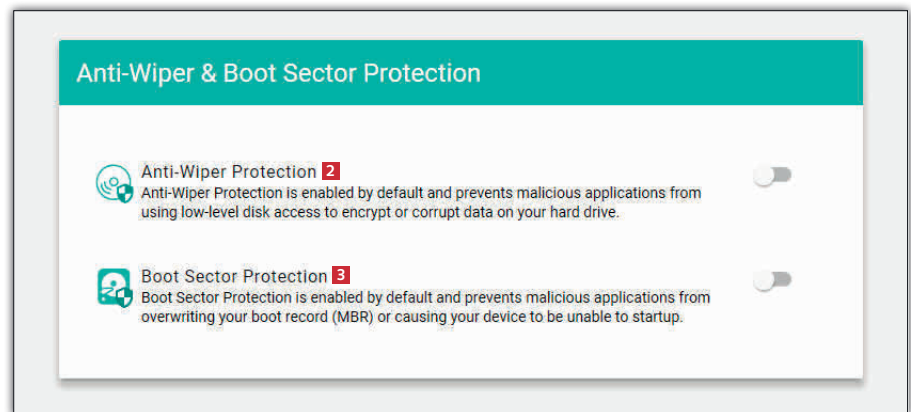


Valitse parhaat asetukset

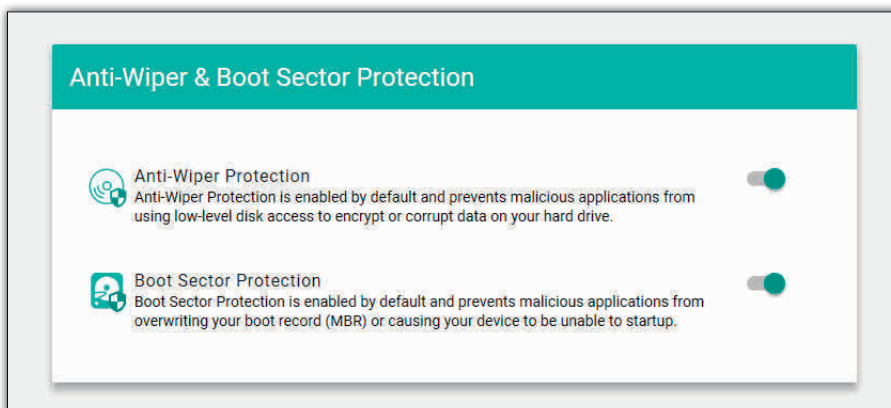
Jotta NeuShield Data Sentinel toimisi optimaalisesti, ja tiedostosi pysyisivät turvassa, sinun on otettava käyttöön tiettyjä asetuksia. Käymme ne läpi tässä.



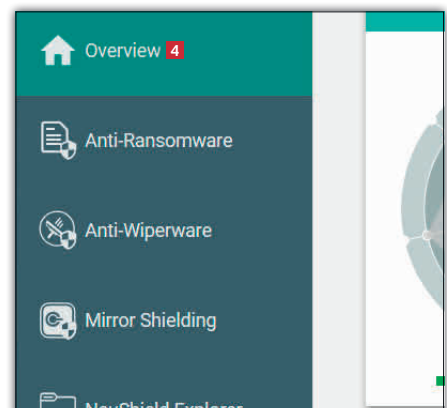
1 Avaa ohjelma ja siirry sen ikkunan vasemmalle puolelle. Siellä sinun on napsautettava kohtaa **Anti-Wiperware 1**.



2 Näet heti kaksi tehokasta työkalua: **Anti-Wiper Protection 2** ja **Boot Sector Protection 3**. Nämä kaksi työkalua vaikeuttavat hakkerien pääsyä tietokoneellesi erityisen tehokkaasti, joten ne kannattaa ottaa käyttöön, jos niitä ei ole vielä aktivoitu.



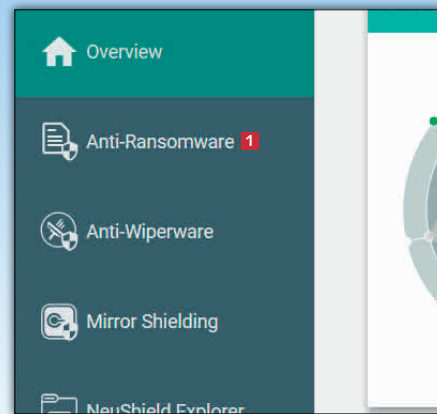
3 Ikkuna näyttää tältä, kun nämä kaksi työkalua on aktivoitu ohjelmassa. Nyt olet valmis tutustumaan työkalun muihin ominaisuuksiin.



4 Palaa lopuksi takaisin ohjelman päävalikkoon napsauttamalla vielä kohtaa **Overview 4**.

Valitse suojattavat kansiot

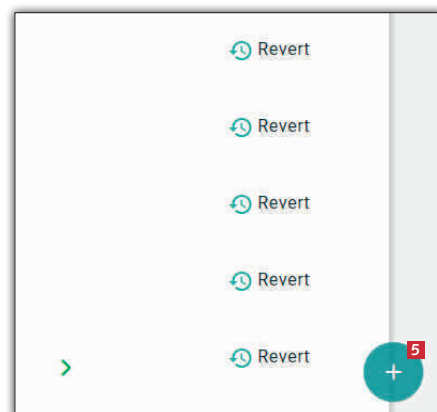
Valitse ne kansiot, jotka haluat suojata kiristysohjelmahyökkäyksiltä. Sovellus valitsee oletusarvoisesti useita kansioita, mutta voit helposti lisätä niitä lisää.



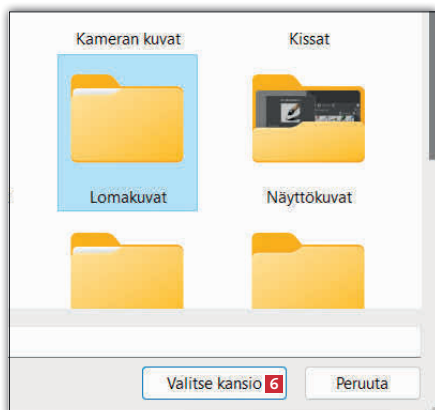
1 Napsauta ohjelmaikkunan vasemmalla puolella kohtaa **Anti-Ransomware** **1**.



2 Nyt saat luettelon kaikista kansioista, jotka ohjelma on tällä hetkellä suojannut. Tässä niitä ovat esimerkiksi **Tiedostot** **2**, **Työpöytä** **3**, **Kuvat** **4** ja niin edelleen.



3 Voit lisätä jonkin kansion nap-sauttamalla ohjelman alareunassa olevaa plusmerkkiä **5**.



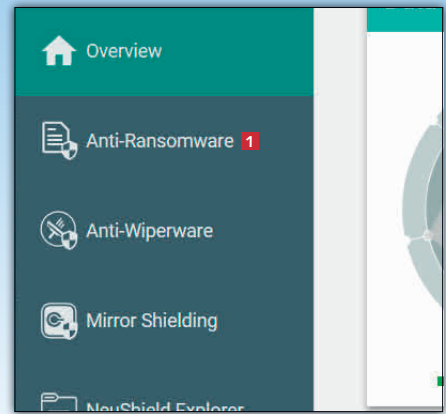
4 Valitse sovellukseen lisättävä ja siten suojattava kansio. Napsauta sitten kohtaa **Valitse kansio** **6**.



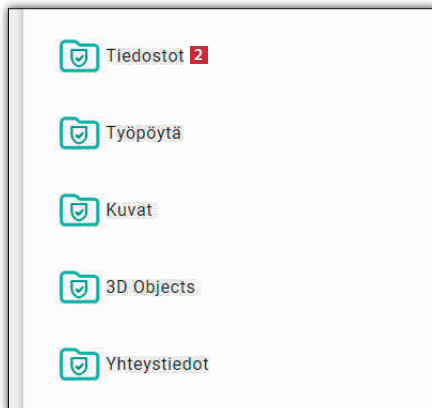
5 Kansio **7** on nyt lisätty ohjelmaan ja pysyy suojassa hyökkäyksen sattuessa. Toista prosessi, jos haluat lisätä muita kansioita.

Palauta vaurioitunut tiedosto

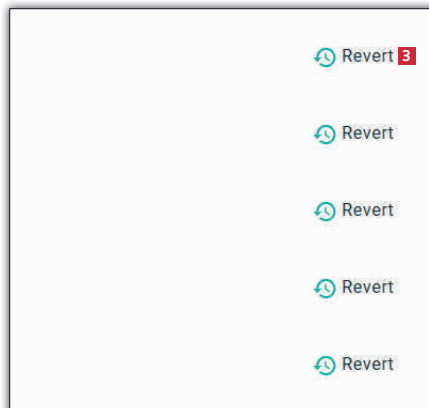
Valitut kansiot ja tiedostot on nyt suojattu. Jos huomaat, että jokin tiedosto on lukittu kiristysohjelmalla, voit palauttaa sen NeuShield Data Sentinel -ohjelmalla siitä riippumatta, onko tiedosto lukittu, muokattu vai kokonaan kadonnut.



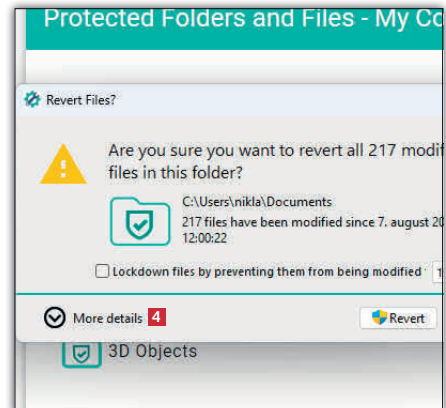
1 Avaa NeuShield Data Sentinel ja valitse **Anti-Ransomware** **1** ohjelman vasemmalla puolella.



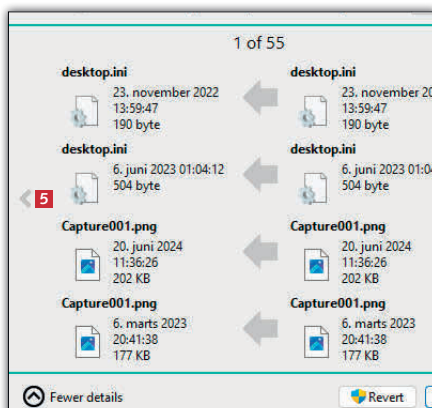
2 Etsi sitten kansio, johon tiedosto on alkujaan tallennettu. Tässä tapauksessa se oli **Tiedostot** **2** -kansiossa oleva tiedosto.



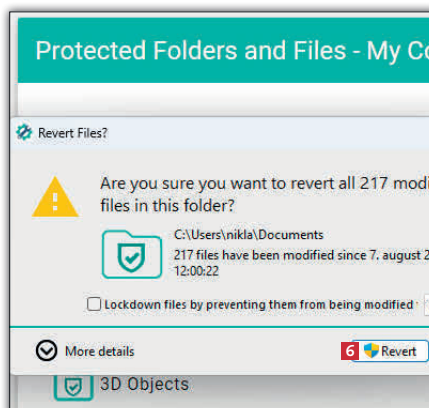
3 Käynnistä seuraavaksi tiedoston tai tiedostojen palautusprosessi painamalla kansion nimen vieressä painiketta **Revert** **3**.



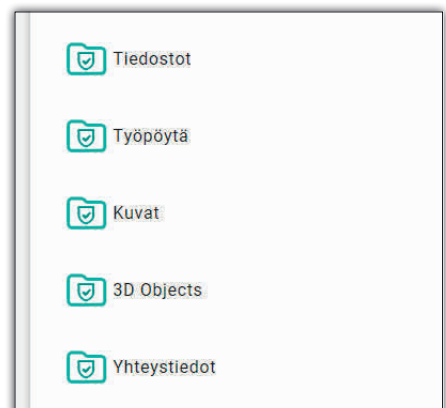
4 Napsauta avautuvassa ikkunassa kohtaa **More details** **4**, niin saat kerralla yleiskuvan palauttamiskelpoisista tiedostoista.



5 Voit nyt nähdä tiedostot, joissa on rekisteröityjä muutoksia. Siirry niiden välillä napsauttamalla sivujen nuolipainikkeita **5**.



6 Napsauta kohtaa **Revert** **6** palauttaaksesi tiedostot hyökkäystä edeltäneeseen tilaansa. Napsauta avautuvassa ikkunassa kohtaa **Kyllä**.



7 Tiedostot on nyt palautettu käyttöön, ja löydät ne niiden alkuperäisistä sijainneista.