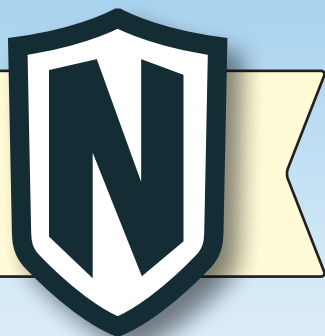




EN UTSPEKULERT LØSNING:

Lag en felle for hackerne

Får du løsepengevirus på maskinen, krypteres filene på den og blir ubrukelige. Med verktøyet Data Sentinel er det angriperne som går i baret.



Journalist
Niklas Ernst

Normalt er det vi vanlige databrukere som går fem på når hackere og andre legger skumle planer og får oss til å installere skadevare i form av for eksempel løsepengevirus. Med programmet NeuShield Data Sentinel er det derimot du som setter opp en felle for hackerne.

I utgangspunktet beskytter programmet mot løsepengevirus eller "ransomware", altså den typen skadelige programmer som kan kryptere filene dine, før folkene bak angrepet krever løsepenger for å låse opp de

samme filene, slik at du igjen får tilgang til dem. Installerer du Data Sentinel, slipper du å betale noe som helst. Programmet hjelper deg nemlig med å redde filene fra hackerens kraftfulle kryptering. Det vil si – programmet redder egentlig ikke filene, men skjuler dem, slik at hackerne tror at de har fått tak i filene – når virkeligheten er en annen.

Slik virker programmet

Det fungerer på følgende måte: Tenk deg en stor tavle der det er skrevet tekst. Teksten er filene dine. Forestill deg at det legges en stor glassplate over tavlen. Glassplaten er usynlig, men skaper likevel en barriere. Når

noen prøver å endre teksten, ser det ut som de har overskrevet den. Men i virkeligheten har de bare skrevet på glassplaten, som lett kan viskes ren – og under platen er teksten fortsatt i god behold.

På samme måte lager Data Sentinel et sett med falske versjoner av filene, som angriperne tror er ekte, og som de derfor krypterer ved hjelp av virus. De ekte filene er imidlertid i sikkerhet og kan lett hentes frem etter et løsepengeangrep, ettersom hackerne og programvaren deres ikke har fått tak i annet enn de falske filene programmet brukte som agn. Dermed har du lurt angriperne trill rundt – og får ha filene dine i fred.

Kryptering

Når man krypterer data, gjøres innholdet uleselig ved hjelp av en matematisk metode som krever en nøkkel (for eksempel et passord) for å gjøre informasjonen leselig igjen.

Ransomware

Ransomware kalles gjerne løsepengevirus på norsk og krypterer filer på maskinen til offeret. Deretter krever hackeren løsepenger for å dekryptere og gi tilgang til filene igjen.



NeuShield Data Sentinel

Ta vare på filene dine og sørg for at verken hackere eller andre banditter klarer å kryptere dem.

Språk
Engelsk

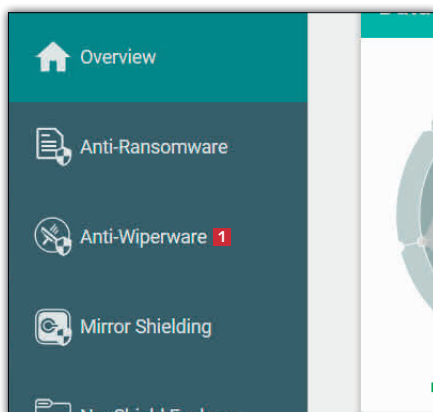
Virker med
Windows 10 og 11

Programmet
laster du
ned fra:
komputer.no/2419

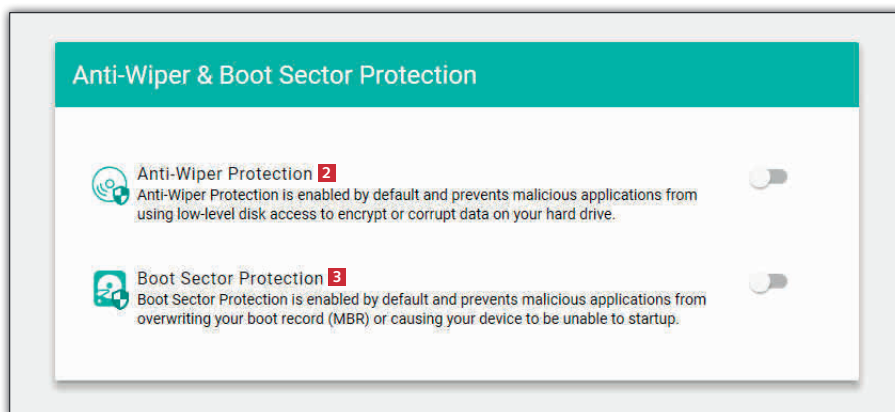


Velg de optimale innstillingene

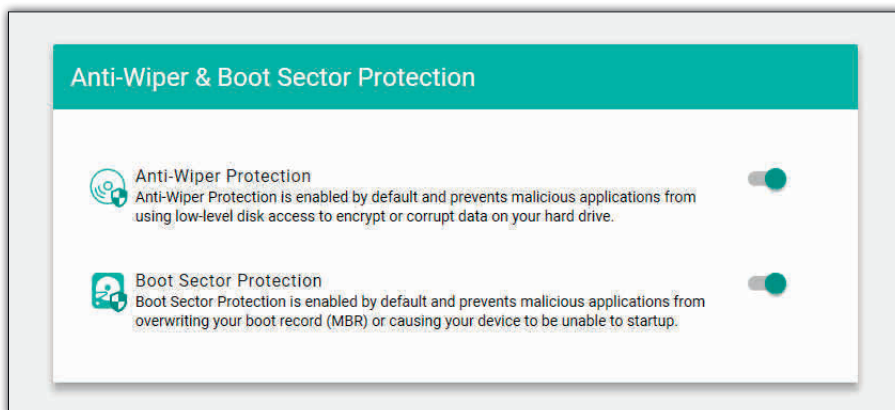
For å få NeuShield Data Sentinel til å fungere etter hensikten, slik at filene forblir sikre, er det et par innstillinger du må aktivere. Det forklarer vi her.



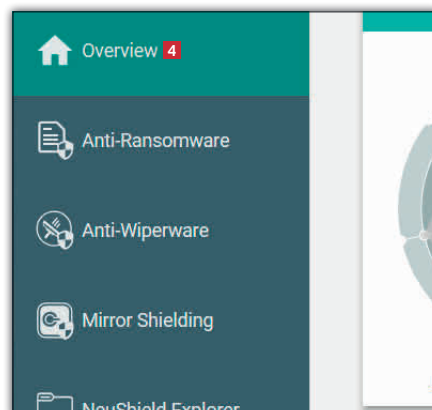
1 Åpne programmet og se på venstre side. Der klikker du på **Anti-Wiperware** **1**.



2 Nå blir du presentert for to begreper, nemlig **Anti-Wiper Protection** **2** og **Boot Sector Protection** **3**. De to verktøyene gjør det ekstra vrient for hackere å få tilgang til maskinen, så dem skal du aktivere, hvis det ikke allerede er gjort.



3 Slik ser det ut når de to verktøyene i programmet er aktivert. Deretter er du klar til å lære mer om de andre funksjonene i verktøyet.

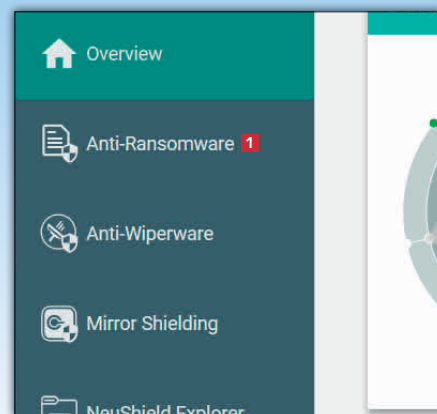


4 Til slutt klikker du på **Overview** **4** for å gå tilbake til hovedmenyen i programmet.

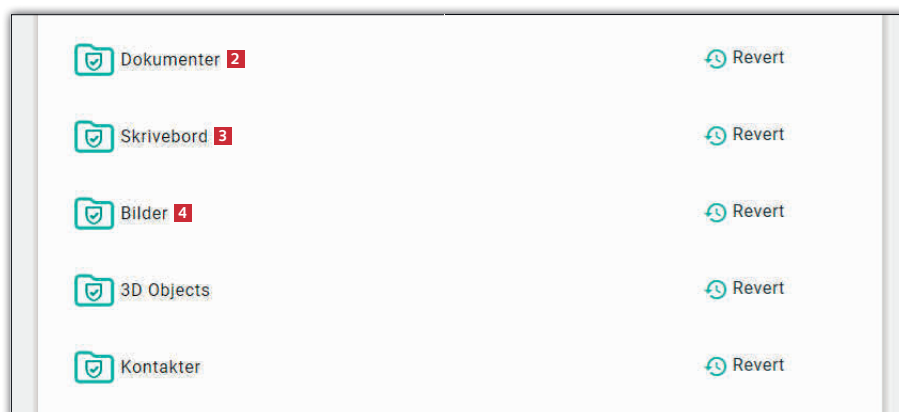


Velg mappene som skal beskyttes

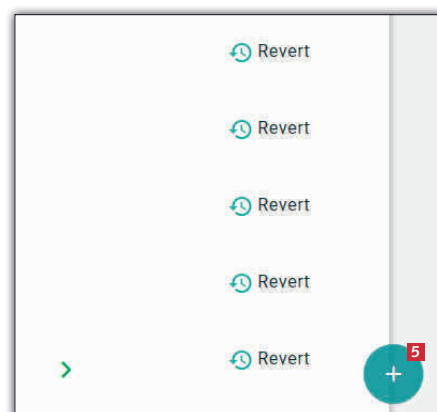
Nå er du klar til å velge ut mappene som skal sikres mot løsepengeangrep. Programmet velger en rekke mapper som standard, men det er lett å legge til flere.



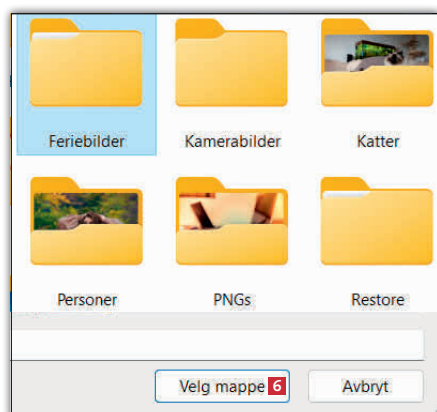
1 Klikk på **Anti-Ransomware** **1** til venstre i programvinduet.



2 Nå får du en liste over alle mapper som for øyeblikket er beskyttet av programmet. Her ser du eksempelvis **Dokumenter** **2**, **Skrivebord** **3**, **Bilder** **4** og så videre.



3 For å legge til en mappe, klikker du på krysset **5** nederst i programmet.



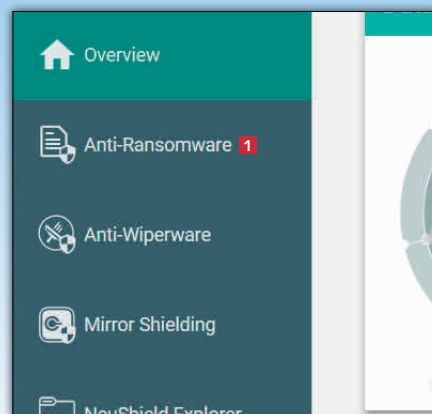
4 Velg mappen som skal legges til og beskyttes. Klikk på **Velg mappe** **6**.



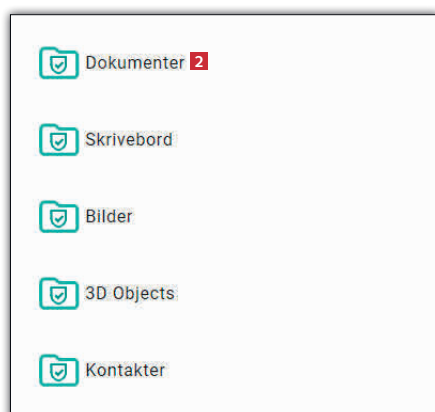
5 Nå er mappen **7** lagt til i programmet og dermed beskyttet mot et eventuelt angrep. Vil du legge til flere mapper, er det bare å gjenta prosessen.

Gjenopprett en skadet fil

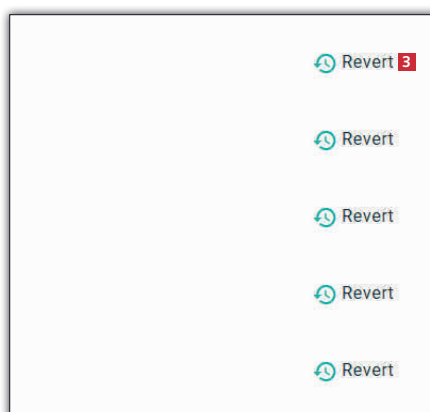
Nå er de utvalgte mappene og filene beskyttet. Hvis du på et tidspunkt kommer ut for at en fil blir låst av løsepengevirus, kan du bruke NeuShield Data Sentinel til å gjenopprette den, uansett om filen er låst, endret eller fjernet.



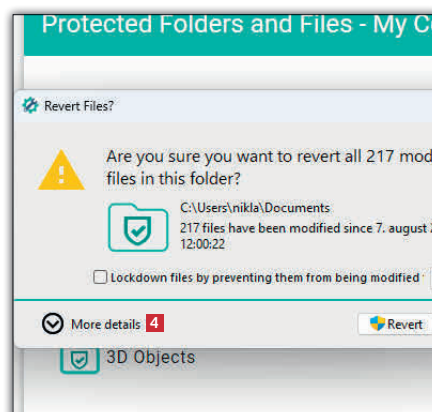
1 Åpne NeuShield Data Sentinel og klikk på **Anti-Ransomware** **1** til venstre i programvinduet.



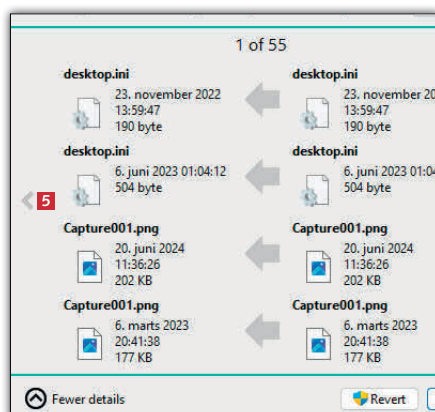
2 Finn mappen der den aktuelle filen var lagret. I dette tilfellet var det snakk om en fil i mappen **Dokumenter** **2**.



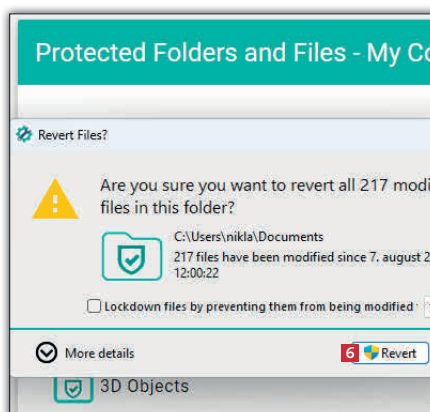
3 Klikk på **Revert** **3** ved mappenavnet for å starte prosessen med å få filen eller filene uskadet tilbake.



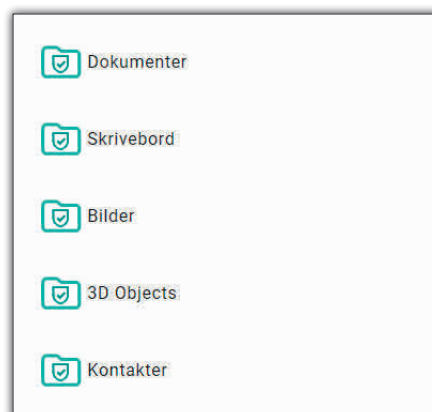
4 I vinduet som åpnes, klikker du på **More details** **4** for å få oversikt over filer som kan gjenopprettes.



5 Nå ser du filene der det er registrert endringer. Klikk på pilene **5** på sidene for å navigere mellom dem.



6 Klikk på **Revert** **6** for å få tilbake filene slik de var før angrepet. Klikk på **Ja** i vinduet som åpnes.



7 Dermed er filene gjenopprettet, og du kan igjen finne dem på den opprinnelige plasseringen.