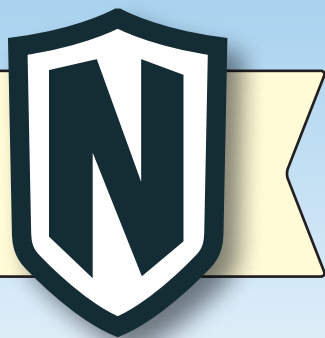




EN LISTIG LÖSNING

Gillra en fälla för hackarna

Om datorn drabbas av ransomware kommer dina filer att låsas och bli helt oanvändbara. Det fiffiga verktyget Data Sentinel kan lura hackarna och skydda dina filer.



Journalist
Niklas Ernst

Vanligtvis är det du som går i fällan när cyberbrottslingar och hackare smider lömska planer och får dig att installera skadlig kod som virus eller ransomware på din dator. Med hjälp av NeuShield Data Sentinel är det tvärtom du som ser till att gillra en fälla för hackarna.

I grunden är det här ett program som hjälper till att skydda dig mot ransomware, vilket är den typ av skadlig program som krypterar och därmed låser dina filer, för att sedan kräva en lösensumma för att låsa upp

filerna så att du kan använda dem igen. Med Data Sentinel på datorn behöver du dock inte betala ett öre eftersom programmet hjälper dig att rädda dina filer från hackarnas kraftfulla kryptering. Det räddar faktiskt inte dina filer, det döljer dem däremot så att hackarna tror att de har fått tag på dina filer – men i verkligheten är historien en helt annan.

Så fungerar programmet

Så här fungerar det: Tänk dig en stor whiteboard med lite text på. Texten på tavlan är dina filer. Föreställ dig nu att en glasskiva placeras framför whiteboardtavlan. Den är osynlig men skapar en skyddande barriär. När

någon försöker ändra din text ser det ut som att de har skrivit ovanpå din text, men i själva verket har de bara skrivit på glasskivan som kan torkas ren – och under den är din text helt intakt och exakt som tidigare.

På i princip samma sätt skapar Data Sentinel en uppsättning falska versioner av dina filer. Hackarna tror att det är riktiga filer som krypteras med ransomware. Dina riktiga filer är emellertid oskadda och kan enkelt fiskas upp efter en ransomware-attack, eftersom hackarna och deras ransomware bara har fått tag på de falska lockbetesfilerna. Hackarna får en lång näsa – och du har kvar dina oskadda filer.

Kryptering

Vid kryptering av data eller kommunikation görs innehållet oläsligt genom en matematisk metod som kräver en nyckel (vanligtvis ett lösenord) för att göra materialet läsbart igen.

Ransomware

Ransomware är en form av malware som kan kryptera och därmed låser dina filer. Därefter krävs offret på en lösensumma för att få sina filer dekrypterade och användbara igen.



NeuShield Data Sentinel

Håll dina filer säkra och se till att varken hackare eller cyberbrottslingar kan komma åt att kryptera dem.

Språk
Engelska

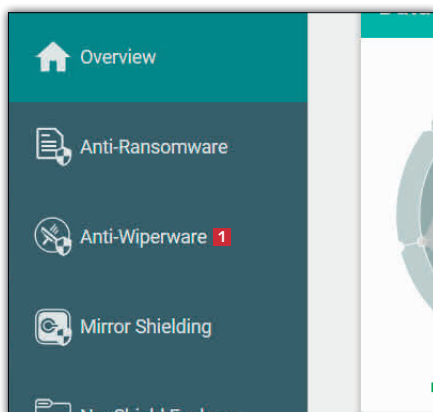
Fungerar med
Windows 10 och 11

Hämta programmet
på vår hemsida:
pctidningen.se/2419

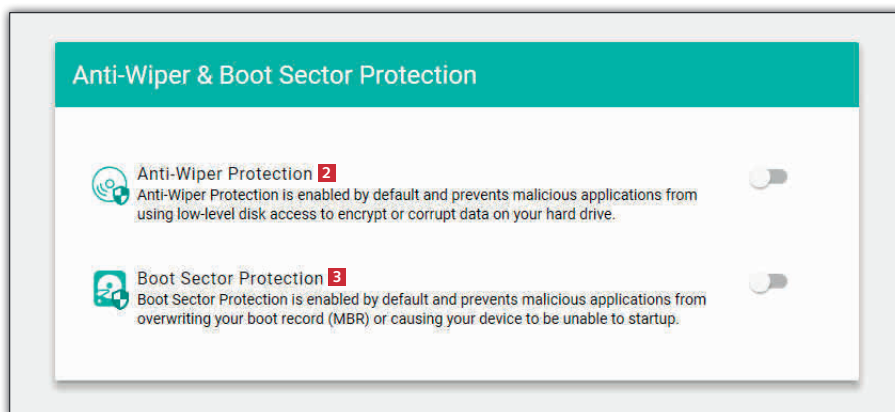


Välj de bästa inställningarna

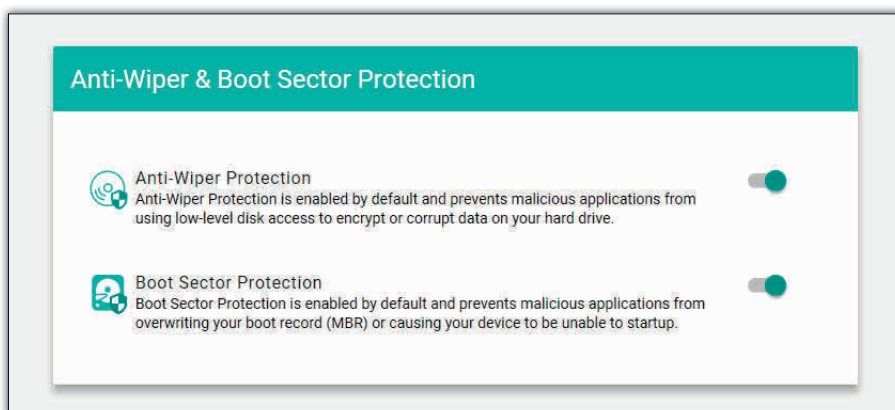
För att NeuShield Data Sentinel ska fungera optimalt och hålla dina filer säkra finns det några inställningar som du måste aktivera. Vi går igenom dem här.



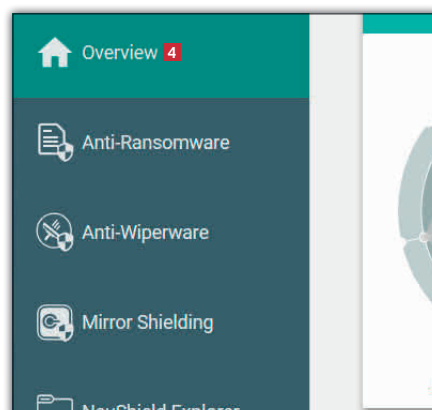
1 Öppna programmet och titta på vänster sida. Här ska du klicka på **Anti-Wiperware** **1**.



2 Du kommer att introduceras till två begrepp: **Anti-Wiper Protection** **2** och **Boot Sector Protection** **3**. Dessa två verktyg gör det extra svårt för hackare att få tillgång till din dator, så du bör aktivera dem om de inte redan är det.



3 Så här ser det ut när de två verktygen har aktiverats i programmet. Nu är du redo att lära dig mer om de andra funktionerna i verktyget.

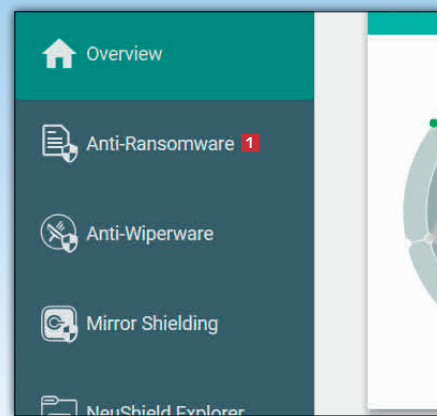


4 Klicka på **Overview** **4** för att komma tillbaka till programmets huvudmeny.



Bestäm vilka mappar som ska skyddas

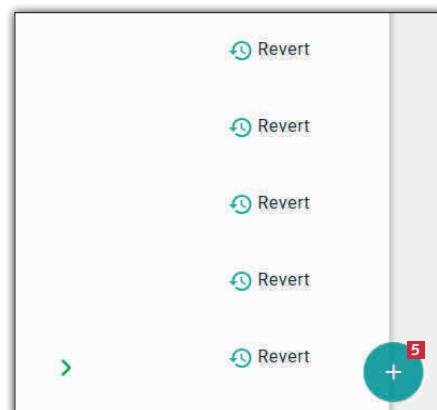
Nu är du redo att välja vilka mappar som ska skyddas mot ransomwareattacker. Programmet väljer ett antal mappar som standard, men du kan enkelt lägga till fler.



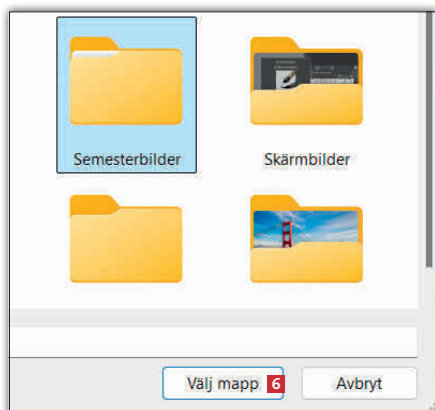
1 Klicka på **Anti-Ransomware** **1** till vänster i programmet.



2 Du kommer nu att få en lista över alla mappar som för närvarande skyddas av programmet. Här är det till exempel **Dokument** **2**, **Skrivbord** **3**, **Bilder** **4** och så vidare



3 För att lägga till en mapp klickar du på kryssset **5** längst ner i programmet.



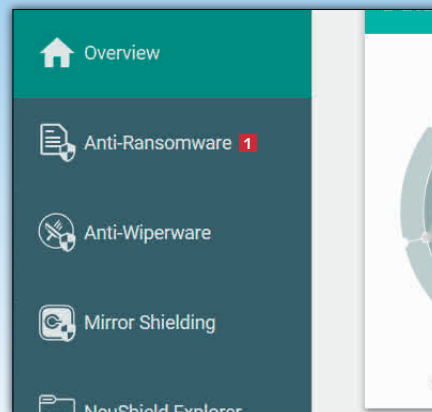
4 Välj den mapp som ska läggas till i programmet och skyddas. Klicka på knappen **Välj mapp** **6**.



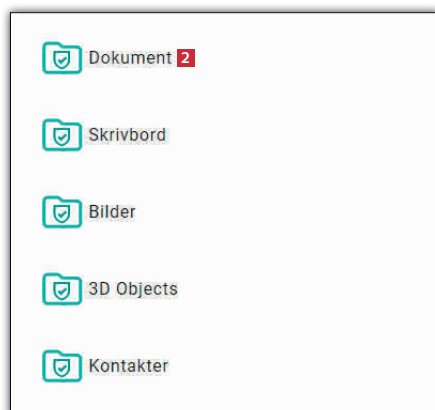
5 Nu har mappen **7** lagts till i programmet och är skyddad vid en eventuell attack. Om du vill lägga till fler mappar är det bara att upprepa processen.

Återställ en korrupt fil

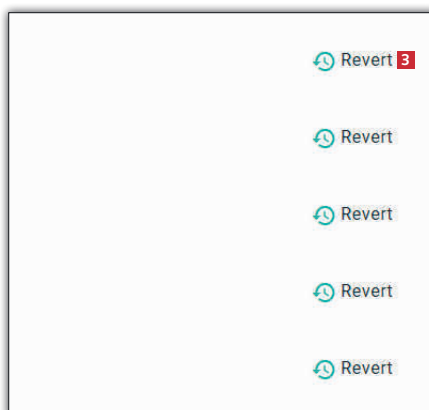
Nu är dina valda mappar och filer skyddade. Om du någonsin upptäcker att en fil är låst av ransomware kan du använda NeuShield Data Sentinel för att få tillbaka den, oavsett om filen är låst, modifierad eller helt borta.



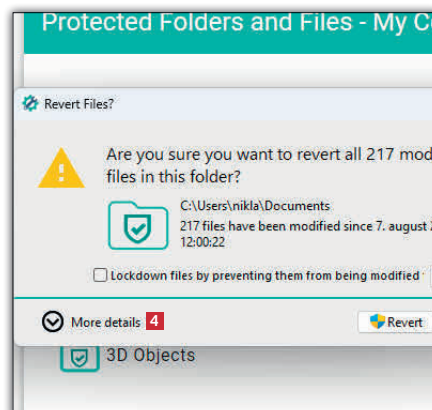
1 Öppna NeuShield Data Sentinel. Till vänster i programmet klickar du på **Anti-Ransomware** **1**.



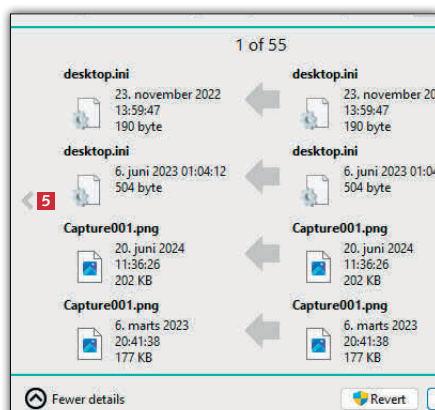
2 Identifiera den mapp som filen lagrades i. I det här fallet var det en fil i mappen **Dokument** **2**.



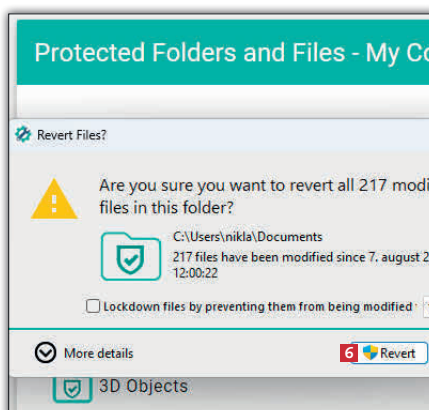
3 Klicka på **Revert** **3** vid mappens namn för att inleda processen att få tillbaka den drabbade filen eller filerna i oskadat tillstånd.



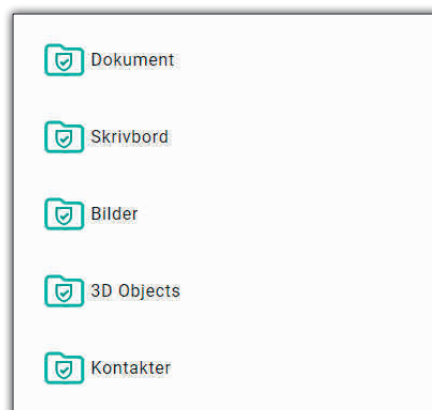
4 I fönstret som öppnas klickar du på **More details** **4** för att få en överblick över de filer som kan återställas.



5 Nu kan du se de filer där det har registrerats ändringar. Klicka på pilarna **5** för att navigera mellan dem.



6 Klicka på **Revert** **6** för att få tillbaka filerna som de var före ransomwareattacken. Klicka på **Revert** i rutan som öppnas.



7 Filerna återställs och du kan hitta dem igen på de platser där de ursprungligen befann sig.

