F-Secure Anti-Virus 2013

Innehåll

Kapitel 1: Installation.....5

Innan du installerar för första gången.....6
Installera produkten för första gången.....6
Installera och uppgradera program.....6
Hjälp och support.....7

Kapitel 2: Komma igång.....9

Så här använder du automatiska uppdateringar.....10
Kontrollera status på uppdateringar.....10
Ändra inställningarna för Internetanslutningen.....10
Kontrollera status på realtidsskyddsnätverket.....11
Så här ser du vad produkten har gjort.....11
Visa aviseringshistorik.....11
Ändra aviseringsinställningarna.....11
Realtidsskyddsnätverk.....12
Vad är realtidsskyddsnätverket?.....12
Fördelar med realtidsskyddsnätverket.....12
Data du bidrar med.....13
Så här skyddar vi din integritet.....14
Bli bidragsgivare till realtidsskyddsnätverket.....14
Frågor om realtidsskyddsnätverket.....14
Hur kan jag veta att prenumerationen är giltig.....15
Åtgärdscenter.....15
Aktivera en prenumeration.....15

Kapitel 3: Introduktion.....17

Visa övergripande status på mitt skydd.....18
Visa produktstatistik.....18
Hantera produktuppdateringarna.....19
Visa databasversioner.....19
Ändra inställningarna för mobilt bredband.....19
Vad är virus och andra skadeprogram.....20
Virus.....20
Spionprogram.....20
Rootkit.....21
Riskprogram.....21

Kapitel 4: Skydda datorn mot skadeprogram.....23
Så här genomsöker du datorn.....24
Söka igenom filer automatiskt.....24
Söka igenom filer manuellt.....26
Söka igenom e-postmeddelanden.....29
Visa genomsökningsresultat.....30
Utesluta filer från genomsökningen.....30
Undanta filtyper.....30
Undanta filer efter plats.....31
Visa undantagna program.....31
Så här använder du karantänen.....32
Visa objekt i karantän.....32
Återställ objekt i karantän.....33
Vad är DeepGuard.....33
Akitvera eller inaktivera DeepGuard.....33
Tillåta program som DeepGuard har blockerat.....34
Använda DeepGuard i kompatibilitetsläget.....34
Vad vill du göra vid varningar om misstänkt beteende?.....34

Kapitel

1

Installation

Ämnen:

- *Innan du installerar för första gången*
- *Installera produkten för första gången*
- *Installera och uppgradera program*
- *Hjälp och support*

Innan du installerar för första gången

Tack för att du väljer F-Secure.

Om du vill installera produkten behöver du följande:

- Installations-cd eller installationspaket. Om du använder en minidator utan cd-enhet kan du hämta installationspaketet på *www.f-secure.com/netbook*.
- Din prenumerationsnyckel.
- En Internetanslutning.

Om du har en säkerhetsprodukt från en annan leverantör kommer installationsprogrammet försöka ta bort den automatiskt. Ta bort den manuellt om detta inte sker.

Obs!: Om du har mer än ett konto på datorn loggar du med administratörsrättigheter när du installerar.

Installera produkten för första gången

Instruktioner för att installera produkten.

Följ de här anvisningarna om du vill installera produkten:

1. Infoga cd-skivan eller dubbelklicka på installationsprogrammet som du hämtade.

   Om cd-skivan inte startas automatiskt går du till Windows Explorer, dubbelklickar på CD-ROM-ikonen och dubbelklickar på installationsfilen för att starta installationen.

2. Följ instruktionerna på skärmen.

   - Om du köpte produkten på en CD-skiva i en butik hittar du prenumerationsnyckeln på fodralet till snabbinstallationsguiden.
   - Om du hämtade produkten från F-Secure eStore finns prenumerationsnyckeln i den orderbekräftelse du fått via e-post.

   Datorn kan behöva startas om innan du bekräftar prenumerationen och hämtar de senaste uppdateringarna från Internet. Kom ihåg att ta bort installations-cd:n innan du startar om datorn om du installerar från cd-skivan.

Installera och uppgradera program

Instruktioner för att aktivera din nya prenumeration.

Följ dessa instruktioner om du vill aktivera din nya prenumeration eller installera ett nytt program via startfönstret.

Obs!: Du hittar ikonen för startfönstret i Windows-systemfältet.

1. Högerklicka på ikonen längst till höger i startvyn.
   En snabbmeny öppnas.
2. Välj **Visa mina prenumerationer**
3. Under **Mina prenumerationer** går du till sidan **Prenumerationsstatus** och klickar på **Aktivera prenumeration**.
   Fönstret **Aktivera prenumeration** öppnas.

4. Ange din prenumerationsnyckel för programmet och klicka på **OK**.
5. När din prenumeration är verifierad och aktiverad klickar du på **Stäng**.
6. Under **Mina prenumerationer** går du till sidan **Installationsstatus**. Om installationen inte startar automatiskt följer du dessa instruktioner:
   a) Klicka på **Installera**.
   Installationsfönstret öppnas.
   b) Klicka på **Nästa**.
   Programmet hämtas och installationen påbörjas.
   c) När installationen är klar klickar du på **Stäng**.

Den nya prenumerationen har aktiverats.

Hjälp och support

Du får åtkomst till onlinehjälp för produkten genom att klicka på Hjälp-ikonen eller trycka på F1 på någon av produktens skärmar.

När du har registrerat licensen är du berättigad till ytterligare tjänster, som kostnadsfria produktuppdateringar och produktsupport. Du kan registrera dig på *www.f-secure.com/register*.

Kapitel

2

Komma igång

Ämnen:

- *Så här använder du automatiska uppdateringar*
- *Så här ser du vad produkten har gjort*
- *Realtidsskyddsnätverk*
- *Hur kan jag veta att prenumerationen är giltig*

Information om hur du kommer igång med produkten.

I det här avsnittet beskrivs det hur du ändrar gemensamma inställningar och hanterar prenumerationerna via startfönstret.

De gemensamma inställningarna i startfönstret är inställningar som gäller för alla program som är installerade i startfönstret. I stället för att ändra inställningarna separat i varje program kan du enkelt redigera de gemensamma inställningarna som sedan används för alla installerade program.

De gemensamma inställningarna i startfönstret omfattar:

- Hämtningar, där du kan visa information om vilka uppdateringar som har hämtats och manuellt kontrollera om några nya uppdateringar är tillgängliga.
- Anslutningsinställningar, där du kan ändra hur datorn ansluter till Internet.
- Aviseringar, där du kan visa tidigare aviseringar och ange vilken slags aviseringar du vill visa.
- Sekretessinställningar, där du kan välja om datorn ska kunna ansluta till realtidsskyddsnätverket.

Du kan även hantera dina prenumerationer för installerade program via startfönstret.

Så här använder du automatiska uppdateringar

Automatiska uppdateringar gör att skyddet på datorn hålls uppdaterat.

Produkten hämtar de senaste uppdateringarna till din dator när du är ansluten till Internet. Den identifierar nätverkstrafik och hindrar inte annan Internetanvändning, inte ens med en långsam nätverksanslutning.

Kontrollera status på uppdateringar

Visa datum och tid för den senaste uppdateringen.

När automatiska uppdateringar är aktiverat får produkten automatiskt de senaste uppdateringarna när du är ansluten till Internet.

Så här ser du till att du har de senaste uppdateringarna:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Öppna vanliga inställningar**.
3. Välj **Automatiska uppdateringar** > **Hämtningar**.
4. Klicka på **Kontrollera nu**.
   Produkten ansluts till Internet och de senaste uppdateringarna hittas. Om skyddet inte är uppdaterat hämtas de senaste uppdateringarna.

   Obs!: Om du använder ett modem eller har en ISDN-anslutning till Internet måste anslutningen vara aktiv för att produkten ska kunna leta efter uppdateringar.

Ändra inställningarna för Internetanslutningen

Du behöver vanligtvis inte ändra standardinställningarna, men du kan konfigurera hur servern är ansluten till Internet så att du kan ta emot uppdateringar automatiskt.

Här ser du hur du ändrar inställningarna för Internetanslutning:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Öppna vanliga inställningar**.
3. Välj **Automatiska uppdateringar** > **Anslutning**.
4. I listan **Internetanslutning** väljer du hur datorn är ansluten till Internet.
   - Välj **Antag permanent anslutning** om du har en permanent nätverksanslutning.

     Obs!: Om din dator i själva verket inte har en permanent nätverksanslutning och är inställd på uppringning vid behov, kan alternativet **Antag permanent anslutning** förorsaka flera uppringningar.
   - Välj **Kontrollera anslutning** för att endast hämta uppdateringar när produkten identifierar en aktiv nätverksanslutning.
   - Välj **Identifiera trafik** om du vill hämta uppdateringar endast när produkten identifierar annan nätverkstrafik.

     Tips: Om du har en ovanlig maskinvarukonfiguration som gör att inställningen **Kontrollera anslutning** upptäcker en aktiv nätverksanslutning även när det inte finns någon sådan, ska du välja **Kontrollera trafik** istället.

5. På **HTTP-proxyn**-listan markerar du huruvida din dator använder en *proxyserver* för att ansluta till Internet eller inte.
   - Markera **Ingen HTTP-proxy** om din dator ansluter direkt till Internet.
   - Välj **Konfigurera HTTP-proxy manuellt** för att konfigurera *HTTP-proxy*-inställningarna.
   - Välj **Använd min webbläsares HTTP-proxy** om du vill använda samma *HTTP-proxy*-inställningar som du har konfigurerat i din webbläsare.

Kontrollera status på realtidsskyddsnätverket

Många produktfunktioner fungerar inte som de ska om produkten inte är ansluten till realtidsskyddsnätverket.

Om det finns problem med nätverket eller om brandväggen blockerar trafik från realtidsskyddsnätverket är din status "Frånkopplad". Om du inte har installerat några produktfunktioner som kräver tillgång till realtidsskyddsnätverket är din status "Används inte".

Så här kontrollerar du din status:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Öppna vanliga inställningar**.
3. Välj **Automatiska uppdateringar** > **Anslutning**.

Under **Realtidsskyddsnätverk** visas aktuell status för realtidsskyddsnätverket.

Så här ser du vad produkten har gjort

Du kan se vilka åtgärder som vidtagits av produkten för att skydda datorn på sidan **Aviseringar**.

Produkten visar en avisering när en åtgärd vidtas, till exempel när ett virus som blockeras påträffas. Vissa aviseringar kan även skickas via tjänsteleverantören, till exempel information om nya tjänster som är tillgängliga.

Visa aviseringshistorik

Du kan se vilka aviseringar som har visats i aviseringshistoriken

Så här visar du aviseringshistoriken:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Öppna vanliga inställningar**.
3. Välj **Övrigt** > **Aviseringar**.
4. Klicka på **Visa aviseringshistorik**.
   Listan över aviseringshistoriken öppnas.

Ändra aviseringsinställningarna

Du kan välja vilken slags aviseringar du vill att produkten ska visa.

Så här ändrar du aviseringsinställningarna:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Öppna vanliga inställningar**.
3. Välj **Övrigt** > **Aviseringar**.

4. Markera eller avmarkera **Tillåt programmeddelanden** om du vill aktivera eller inaktivera programmeddelanden.

   När den här inställningen är aktiverad visar produkten aviseringar från de installerade programmen.
5. Markera eller avmarkera **Tillåt reklammeddelanden** om du vill aktivera eller inaktivera reklammeddelanden.
6. Klicka på **OK**.

Realtidsskyddsnätverk

I det här dokumentet beskrivs realtidsskyddsnätverket, en onlinetjänst från F-Secure Corporation som identifierar säkra program och webbplatser, och samtidigt ger skydd mot skadlig programvara och webbplatsangrepp.

Vad är realtidsskyddsnätverket?

Realtidsskyddsnätverket är en onlinetjänst som tillhandahåller snabb respons gentemot de senaste Internetbaserade hoten.

Som bidragsgivare till realtidsskyddsnätverket kan du hjälpa oss att stärka skyddet mot nya och framväxande hot. Realtidsskyddsnätverket samlar in statistik om vissa okända, skadliga program och vad de gör på enheten. Den här informationen är anonym och skickas till F-Secure Corporation för kombinerad dataanalys. Vi använder den analyserade informationen till att förbättra säkerheten på din enhet mot de senaste hoten och skadliga filer.

Så här fungerar realtidsskyddsnätverket

Som bidragsgivare till realtidsskyddsnätverket kan du lämna information om okända program och webbplatser och om skadliga program och webbplatser som är känsliga för angrepp. Realtidsskyddsnätverket spårar inte din webbaktivitet eller samlar in information om webbplatser som har analyserats redan, och samlar inte in information om osmittade program som är installerade på datorn.

Om du inte vill bidra med dessa data samlar inte realtidsskyddsnätverket in information om installerade program eller besökta webbplatser. Produkten behöver däremot ställa en fråga till F-Secures servrar om ryktet för program, webbplatser, meddelanden och andra objekt. Frågan ställs med hjälp av en kryptografisk kontrollsumma där själva objektet som frågan ställdes om inte skickas till F-Secure. Vi spårar inte data per användare. Endast besöksräknaren för filen eller webbplatsen ökar.

Det är inte möjligt att helt stoppa all nätverkstrafik till realtidsskyddsnätverket, eftersom det utgör en bärande del av produktens skydd.

Fördelar med realtidsskyddsnätverket

Med realtidsskyddsnätverket får du snabbare och bättre skydd mot de senaste hoten och du slipper onödiga aviseringar om misstänkta program som inte är skadliga.

Som bidragsgivare till realtidsskyddsnätverket kan du hjälpa oss att hitta ny och oupptäckt skadlig programvara och ta bort felaktiga poster i vår virusdefinitionsdatabas.

Alla deltagare i realtidsskyddsnätverket hjälper varandra. Om realtidsskyddsnätverket hittar ett misstänkt program på din enhet kan du dra nytta av analysresultatet om samma program redan har påträffats på andra enheter. Realtidsskyddsnätverket förbättrar enhetens övergripande prestanda, eftersom de installerade säkerhetsprodukterna inte behöver genomsöka de program igen som realtidsskyddsnätverket har analyserat och identifierat som säkra. På samma sätt delas information om skadliga webbplatser och oönskade massutskick via realtidsskyddsnätverket, och vi kan erbjuda dig ett bättre skydd mot webbplatsangrepp och skräppost.

Ju fler personer som bidrar till realtidsskyddsnätverket, desto bättre skydd får enskilda deltagare.

Data du bidrar med

Som bidragsgivare till realtidsskyddsnätverket bidrar du med information om program som finns lagrade på din enhet och på webbplatser du besöker så att realtidsskyddsnätverket kan ge skydd mot de senaste skadliga programmen och misstänkta webbplatserna.

Analysera filens anseende

Realtidsskyddsnätverket samlar endast in information om program som inte har ett känt anseende och om filer som är misstänka eller kända för att vara skadlig programvara.

Realtidsskyddsnätverk samlar in anonym information om säkra och misstänkta program på enheten. Realtidsskyddsnätverk samlar endast in information om körbara filer (till exempel portabla körbara filer på Windows-plattformen, som har filtillägget .cpl, .exe, .dll, .ocx, .sys, .scr och .drv).

Insamlad information omfattar:

- filsökvägen där programmet är på enheten,
- storleken på filen och när den skapades eller ändrades,
- filattribut och privilegier,
- filsignaturinformation,
- den aktuella versionen av filen och företaget som skapade den,
- filens ursprung eller dess hämtnings-URL, samt
- F-Secure DeepGuard- och antivirusanalys av genomsökta filer, samt
- annan liknade information.

Realtidsskyddsnätverket samlar aldrig in någon information om dina personliga dokument, såvida det inte upptäcks att de är angripna. För alla slags skadliga filer samlar realtidsskyddsnätverket in namnet på smittan och rensningsstatus för filen.

Med realtidsskyddsnätverket kan du även skicka misstänkta program för analys. Program som du skickar innehåller endast portabla körbara filer. Realtidsskyddsnätverket samlar aldrig in någon information om dina personliga dokument och de överförs aldrig automatiskt för analys.

Skicka filer för analys

Med realtidsskyddsnätverket kan du också skicka in misstänkta program för analys.

Du kan skicka in enskilda misstänkta program manuellt när produkten uppmanar dig att göra det. Du kan bara skicka in portabelt körbara filer. Realtidsskyddsnätverket överför aldrig dina personliga dokument.

Analysera webbplatsens anseende

Realtidsskyddsnätverket spårar inte din webbaktivitet eller samlar in information om webbplatser som redan har analyserats. Det säkerställer att besökta webbplatser är säkra när du surfar på nätet. När du besöker en webbplats kontrollerar realtidsskyddsnätverket dess säkerhet och meddelar dig om webbplatsen är klassificerad som misstänkt eller skadlig.

Om webbplatsen du besöker innehåller farligt eller skadligt innehåll eller är känd för att vara känslig för angrepp, samlar realtidsskyddsnätverket in hela URL-adressen för webbplatsen, så att webbsidans innehåll kan analyseras.

Om du besöker en webbplats som inte har klassificerats än samlar realtidsskyddsnätverket in domän- och underdomännamn och i vissa fall sökvägen till den besökta sidan, så att webbplatsen kan analyseras och klassificeras. Alla URL-parametrar som kan innehålla information som kan länkas till dig i ett personligt identifierbart format tas bort för att skydda din integritet.

Obs!: Realtidsskyddsnätverket klassificerar eller analyserar inte webbsidor i privata nätverk, så det samlas aldrig in någon information om privata IP-nätverkadresser (till exempel företagsintranät).

Analysera systeminformationen

Realtidsskyddsnätverket samlar in information om namn och version av operativsystemet, information om Internetanslutningen och användningsstatistiken för realtidsskyddsnätverket (till exempel antalet gånger webbplatsens anseende har efterfrågats och den genomsnittliga tiden det tar att returnera ett resultat för frågan) så att vi kan övervaka och förbättra tjänsten.

Så här skyddar vi din integritet

Vi överför informationen på ett säkert sätt och tar automatiskt bort eventuell personlig information som informationen kan innehålla.

Realtidsskyddsnätverket tar bort identifierande data innan informationen skickas till F-Secure och krypterar all insamlad information under överföringen för att skydda den från obehörig åtkomst. Den insamlade informationen behandlas inte individuellt. Den grupperas med information från andra bidragsgivare till realtidsskyddsnätverket. Alla data analyseras statistiskt och anonymt, vilket innebär att inga data på något sätt kopplas samman med dig.

All information som skulle kunna användas för att identifiera dig personligen utesluts från informationen som samlas in. Realtidsskyddsnätverket samlar inte in privata IP-adresser eller personlig information, till exempel e-postadresser, användarnamn eller lösenord. Trots att vi gör vårt yttersta för att ta bort alla personligt identifierbara data kan det hända att vissa identifierande data finns kvar i informationen som samlas in. I dessa fall eftersträvar vi inte att använda sådana oavsiktligt insamlade data för att identifiera dig.

Vi tillämpar strikta säkerhetsåtgärder och använder fysiska, administrativa och tekniska skydd för att skydda informationen som samlas in när den överförs, lagras och bearbetas. Information lagras på säkra platser och på servrar som kontrolleras av oss. Servrarna finns antingen på våra kontor eller på kontor som tillhör våra underleverantörer. Endast behörig personal har åtkomst till informationen som samlas in.

F-Secure kan dela information som samlas in med sina dotterbolag, underleverantörer, distributörer och partner, men det sker alltid i ett format som är anonymt och icke-identifierbart.

Bli bidragsgivare till realtidsskyddsnätverket

Du hjälper oss att förbättra skyddet för realtidsskyddsnätverket genom att bidra med information om skadliga program och webbplatser.

Du kan välja att delta i realtidsskyddsnätverket under installationen. Med standardinstallationsinställningarna kan du bidra med data till realtidsskyddsnätverket. Du kan ändra den här inställningen senare i produkten.

Följ dessa instruktioner om du vill ändra inställningarna för realtidsskyddsnätverket:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Öppna vanliga inställningar**.
3. Välj **Övrigt** > **Sekretess**.
4. Markera kryssrutan för att bli bidragsgivare till realtidsskyddsnätverket.

Frågor om realtidsskyddsnätverket

Kontaktinformation för frågor om realtidsskyddsnätverket.

Om du har ytterligare frågor om realtidsskyddsnätverket kan du kontakta:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

Den senaste versionen av den här policyn finns alltid tillgänglig på vår webbsida.

Hur kan jag veta att prenumerationen är giltig

Din prenumerationstyp och-status visas på sidan **Prenumerationsstatus**.

När prenumerationen håller på att förfalla eller om prenumerationen har förfallit ändras den övergripande skyddsstatusen för programmet för motsvarande ikon i startfönstret.

Så här kontrollerar du prenumerationens giltighet:

1. Högerklicka på ikonen längst till höger i startvyn.
   En popup-meny visas.
2. Välj **Visa mina prenumerationer**.
3. Välj **Prenumerationsstatus** om du vill visa information om dina prenumerationer för installerade program.
4. Välj **Installationsstatus** om du vill visa vilka program som är tillgängliga att installeras.

Prenumerationsstatus och förfallodatum visas också på programmets **Statistik**-sida. Om prenumerationen har förfallit måste du förnya prenumerationen för att fortsätta få uppdateringar och använda produkten.

Obs!: När prenumerationen har löpt ut blinkar produktens statusikon i meddelandefältet.

Åtgärdscenter

I åtgärdscentret visas viktiga meddelanden som kräver din uppmärksamhet.

Om din prenumeration har upphört eller är på väg att upphöra meddelas du om detta i åtgärdscentret. Bakgrundsfärgen och innehållet i meddelandena från åtgärdscentret beror på prenumerationens typ och status:

- Om din prenumeration är på väg att upphöra och det finns kostnadsfria prenumerationer tillgängliga har meddelandet vit bakgrund och en **Aktivera**-knapp.
- Om din prenumeration är på väg att gå ut och det inte finns några tillgängliga prenumerationer har meddelandet gul bakgrund och **Köp**- och **Ange nyckel**-knappar. Om du redan har köpt en ny prenumeration kan du klicka på **Ange nyckel** för att ange prenumerationsnyckeln och aktivera din nya prenumeration.
- Om din prenumeration har gått ut och det inte finns några kostnadsfria prenumerationer tillgängliga har meddelandet röd bakgrund och en **Aktivera**-knapp.
- Om din prenumeration har gått ut och det inte finns några kostnadsfria prenumerationer tillgängliga har meddelandet röd bakgrund och **Köp**- och **Ange nyckel**-knappar. Om du redan har köpt en ny prenumeration kan du klicka på **Ange nyckel** för att lämna prenumerationsnyckeln och aktivera din nya prenumeration.

Obs!: Länken **Visa meddelandehistorik** i åtgärdscentret visar en lista med meddelanden om produkter, inte tidigare meddelanden från åtgärdscentret.

Aktivera en prenumeration

Om du har en ny prenumerationsnyckel eller kampanjkod för en produkt måste du aktivera den.

Så här aktiverar du en prenumeration:

1. Högerklicka på ikonen längst till höger i startvyn.

En popup-meny visas.

2. Välj **Visa mina prenumerationer**.
3. Välj ett av följande alternativ:
   - Klicka på **Aktivera prenumeration**.
   - Klicka på **Aktivera kampanjkod**.
4. I dialogrutan som öppnas anger du den nya prenumerationsnyckeln eller kampanjkoden och klickar på **OK**.

   Tips: Om du har fått din prenumeration via e-post kan du kopiera nyckeln från e-postmeddelandet och klistra in den i fältet.

Efter att du har angett prenumerationsnyckeln visas den nya prenumerationsnyckeln på sidan **Prenumerationsstatus**.

Kapitel

3

Introduktion

Ämnen:

- *Visa övergripande status på mitt skydd*
- *Visa produktstatistik*
- *Hantera produktuppdateringarna*
- *Vad är virus och andra skadeprogram*

Den här produkten skyddar datorn från virus och andra skadliga program.

Produkten söker igenom filer, analyserar program och uppdateringar automatiskt. Ingen åtgärd krävs av dig.

Visa övergripande status på mitt skydd

På sidan **Status** visas en snabböversikt över installerade produktfunktioner och deras aktuella status.

Så här öppnar du sidan **Status**:

På huvudsidan klickar du på **Status**.

Sidan **Status** öppnas.

Med hjälp av ikonerna kan du se status på programmet och dess säkerhetsfunktioner.

Statusikon	Statusnamn	Beskrivning
	OK	Datorn är skyddad. Funktionen är aktiverad och fungerar som den ska.
	Information	Du får information om att en funktion har en speciell status. Funktionen uppdateras, till exempel.
	Varning	Datorn är inte fullständigt skyddad. Produkten har till exempel inte uppdaterats på länge, eller statusen för en funktion kräver uppmärksamhet.
	Fel	Datorn är inte skyddad Prenumerationen har till exempel löpt ut eller en viktig funktion är avstängd.
	Av	En icke-kritisk funktion har inaktiverats.

Visa produktstatistik

Du kan se vad produkten har gjort sedan den installerades på sidan **Statistik**.

Så här öppnar du sidan **Statistik**:

Gå till huvudsidan och klicka på **Statistik**.

Sidan **Statistik** öppnas.

- **Senast utförda uppdateringskontroll** visar när den senaste uppdateringen utfördes.
- **Virus- och spionprogramgenomsökning** visar hur många filer som produkten har genomsökt och rensat sedan den installerades.
- **Program** visar hur många program DeepGuard har tillåtit eller blockerat sedan installationen.

- **Brandväggsanslutningar** visar antalet tillåtna och blockerade anslutningar sedan installationen.
- Med **Skräppost- och phishingfiltrering** visas hur många e-postmeddelanden produkten har identifierats som giltiga e-postmeddelanden och som skräppostmeddelanden.

Hantera produktuppdateringarna

Produkten håller skyddet uppdaterat automatiskt.

Visa databasversioner

Du kan se de senaste uppdateringstiderna och versionsnummer på sidan **Databasuppdateringar**.

Så här öppnar du sidan **Databasuppdateringar**:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Andra inställningar** > **Databasversioner**.

På sidan **Databasversioner** visas det senaste datumet då virus- och spionprogramsdefinitioner, DeepGuard samt skräppost- och phishingfiltrering uppdaterades samt deras versionsnummer.

Ändra inställningarna för mobilt bredband

Välj om du vill hämta säkerhetsuppdateringar när du använder mobilt bredband.

Obs!: Den här funktionen finns endast i Microsoft Windows 7.

Som standard hämtas alltid säkerhetsuppdateringar när du använder hemoperatörens nätverk. Uppdateringarna skjuts upp när du besöker en annan operatörs nätverk. Detta beror på att anslutningspriserna kan variera mellan olika operatörer, till exempel i olika länder. Det kan vara bäst att inte ändra den här inställningen, om du vill spara bandbredd och även hålla kostnaderna nere under ditt besök.

Obs!: Den här inställningen gäller endast för mobila bredbandsanslutningar. Om datorn är ansluten till ett fast eller trådlöst nätverk uppdateras produkten automatiskt.

Så här ändrar du inställningen:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Andra inställningar** > **Mobilt bredband** > **Hämta säkerhetsuppdateringar**.
3. Välj önskat uppdateringsalternativ för mobila anslutningar:
   - **Endast i min hemoperatörs nätverk**

     Uppdateringarna hämtas alltid när du använder din hemoperatörs nätverk. Om du besöker en annan operatörs nätverk skjuts uppdateringarna upp. Vi rekommenderar att du väljer det här alternativet för att enklast hålla produkten uppdaterad samtidigt som du håller kostnaderna nere.
   - **Aldrig**

     Uppdateringar hämtas inte när du använder mobilt bredband.
   - **Alltid**

     Uppdateringar hämtas alltid, oavsett vilket nätverk du använder. Välj det här alternativet om du vill vara säker på att datorns säkerhet alltid är uppdaterad, oavsett vad det kostar.

4. Om du vill godkänna varje enskild gång du lämnar din hemoperatörs nätverk väljer du **Fråga mig varje gång jag lämnar min hemoperatörs nätverk**.

Uppskjutna säkerhetsuppdateringar

Säkerhetsuppdateringarna kanske skjuts upp när du använder mobilt bredband utanför din hemoperatörs nätverk.

I det här fallet kan du se meddelandet **Inaktiverad** i det nedre högra hörnet av skärmen. Uppdateringarna är inaktiverade eftersom priserna på anslutningar kan variera beroende på exempelvis operatörer i olika länder. Du kan överväga att behålla den här inställningen om du vill spara bandbredd, och eventuellt kostnader, under ditt besök. Om du däremot vill ändra inställningar klickar du på länken **Ändra**.

Obs!:

Den här funktionen finns endast i Microsoft Windows 7.

Vad är virus och andra skadeprogram

Skadeprogram är specifikt utformade för att skada din dator, använda den i olagliga syften utan din vetskap eller stjäla information från den.

Skadeprogram kan:

- ta kontroll över din webbläsare,
- dirigera om dina sökningar,
- visa oönskade annonser,
- hålla reda på vilka webbplatser du besöker,
- stjäla personliga uppgifter om dig som t.ex. bankuppgifter,
- använda din dator för att skicka skräppost, och
- använda din dator för att attackera andra datorer.

Skadeprogram kan även göra datorn långsam och instabil. Du kan misstänka att du har *skadeprogram* på datorn om den plötsligt blir väldigt långsam och ofta kraschar.

Virus

Ett virus är vanligtvis ett program som kan bifoga sig själv till filer och mångfaldiga sig själv upprepade gånger. Det kan ändra sig och ersätta innehållet i filer på ett sätt som kan skada din dator.

Ett *virus* är ett program som normalt installeras på din dator utan att du vet om det. När viruset har gjort det försöker det mångfaldiga sig själv. Viruset:

- använder några av datorns systemresurser
- kan ändra eller skada filer på datorn
- försöker förmodligen använda datorn för att infektera andra datorer
- kan tillåta att din dator används i olagliga syften.

Spionprogram

Spionprogram är program som samlar in personlig information om dig.

Spionprogram kan samla in personliga uppgifter som:

- webbplatser som du har besökt,
- e-postadresser från din dator,
- lösenord eller

- kreditkortsnummer.

Spionprogram installerar nästan alltid sig själva utan ditt uttryckliga tillstånd. Spionprogram kan installeras tillsammans med användbara program eller genom att lura dig att klicka på ett alternativ i ett missvisande popup-fönster.

Rootkit

Rootkit är program som gör det svårt att hitta andra *skadeprogram*.

Rootkit döljer filer och processer. Syftet är i allmänhet att dölja skadlig aktivitet på datorn. När ett rootkit döljer *skadeprogram* är det svårt att upptäcka att det finns skadeprogram på datorn.

Denna produkt har en rootkitsökmotor som söker specifikt efter rootkit, så *skadeprogram*men har svårt att gömma sig.

Riskprogram

Riskprogram har inte skapats i syfte att skada datorn, men kan göra det om de används på fel sätt.

Riskprogram är inte egentliga skadeprogram. Riskprogram utför vissa användbara, men potentiellt farliga funktioner.

Exempel på riskprogram är:

- program för chatt, som IRC (Internet Relay Chat),
- program för att överföra filer över Internet från en dator till en annan,
- Program för Internettelefoni, som t.ex. VoIP (*Voice Over Internet Protocol*),
- Programvara för fjärranslutning, till exempel VNC,
- skrämselprogram, som kan försöka skrämma eller lura personer att köpa falsk säkerhetsprogramvara, eller
- programvara som har utformats för att kringgå CD-kontroller eller kopieringsskydd.

Om du medvetet har installerat programmet och ställt in det korrekt, är det mindre troligt att det är skadligt.

Om riskprogrammet har installerats utan din vetskap har det troligtvis installerats i skadligt syfte och bör tas bort.

Kapitel

4

Skydda datorn mot skadeprogram

Ämnen:

- *Så här genomsöker du datorn*
- *Utesluta filer från genomsökningen*
- *Så här använder du karantänen*
- *Vad är DeepGuard*

Genomsökning efter virus och spionprogram skyddar datorn mot program som kan stjäla personliga uppgifter, skada datorn eller använda datorn i olagliga syften.

Som standard hanteras all slags skadlig programvara direkt när den påträffas, så att den inte orsakar någon skada.

Vid skanning efter virus och spionprogram genomsöks som standard de lokala hårddiskarna, eventuella flyttbara media (till exempel bärbara enheter eller CD-skivor) och hämtat material automatiskt. Du kan ange att även din e-post ska skannas automatiskt.

Vid skanning efter virus och spionprogram bevakas även datorn efter eventuella ändringar som kan tyda på förekomst av *skadlig programvara*. Om farliga systemändringar, till exempel gällande systeminställningar, eller försök att ändra viktiga systemprocesser påträffas, stoppar DeepGuard programmet från att köras eftersom det kan röra sig om *skadlig programvara*.

Så här genomsöker du datorn

När Genomsökning efter virus och spionprogram är aktiverat genomsöks datorn automatiskt efter skadliga filer. Du kan även söka igenom filer manuellt och konfigurera schemalagda genomsökningar.

Vi rekommenderar att du alltid låter Genomsökning efter virus och spionprogram vara aktiverat. Sök igenom filerna manuellt när du vill kontrollera att det inte finns några skadliga filer på datorn eller om du vill söka igenom filer som du uteslöt från realtidsgenomsökningen.

Genom att konfigurera en schemalagd genomsökning tas skadliga filer bort från datorn vid angivna tidpunkter.

Söka igenom filer automatiskt

Realtidsgenomsökning skyddar din dator genom att söka igenom alla filer när de används och blockera åtkomst till de filer som innehåller *skadeprogram*.

När datorn försöker öppna en fil söks den igenom med Realtidsgenomsökning efter skadeprogram innan datorn får åtkomst till filen. Om realtidsgenomsökningen hittar något skadligt innehåll sätts filen i karantän innan den kan orsaka någon skada.

Påverkar realtidsgenomsökning datorns prestanda?

Du märker vanligtvis inte genomsökningsprocessen eftersom den går snabbt och endast upptar en liten del av systemets resurser. Den tid och och de systemresurser som realtidsgenomsökningen tar i anspråk beror t.ex. på filens innehåll, plats och typ.

Filer som tar längre tid att söka igenom:

- Filer på flyttbara enheter, till exempel CD-skivor, DVD-skivor och bärbara USB-enheter.
- Komprimerade filer, som t.ex. *.zip*- filer.

  Obs!: Komprimerade filer genomsöks inte som standard.

Realtidsgenomsökning kan göra datorn långsammare om:

- du har en dator som inte uppfyller systemkraven, eller
- du öppnar många filer samtidigt. När du till exempel öppnar en katalog som innehåller många filer som måste sökas igenom.

Aktivera eller inaktivera realtidsgenomsökning

Låt realtidsgenomsökning vara aktiverat så förhindrar du att *skadeprogram* skadar datorn.

Så här startar och stoppar du realtidsgenomsökning:

1. På huvudsidan klickar du på **Status**.
2. Klicka på **Ändra inställningar på den här sidan.**.

   Obs!: Du måste ha administratörsbehörighet för att inaktivera säkerhetsfunktioner.

3. Aktivera eller inaktivera **Genomsökning efter virus och spionprogram**.
4. Klicka på **Stäng**.

Hantera skadliga filer automatiskt

Realtidsgenomsökning kan hantera skadliga filer automatiskt utan att fråga dig om något.

Gör så här om du vill att realtidsgenomsökning ska hantera skadliga filer automatiskt:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram**.
3. Välj **Hantera skadliga filer automatiskt**.

Om du väljer att inte hantera skadliga filer automatiskt blir du tillfrågad under realtidsgenomsökningen vad du vill göra med en skadlig fil när den hittas.

Hantera spionprogram

Med genomsökning efter virus och spionprogram blockeras spionprogram omedelbart när det försöker starta.

Innan ett spionprogram kan starta blockeras det av produkten och du får bestämma vad du vill göra med det.

Välj någon av följande åtgärder när ett spionprogram hittas:

Åtgärd som ska utföras	Detta händer med spionprogrammet
Hantera automatiskt	Låt produkten avgöra vilken åtgärd som är bäst beroende på vilket spionprogram som hittas.
Sätt spionprogrammet i karantän	Flytta spionprogrammet till karantänen där det inte kan skada datorn.
Ta bort spionprogrammet	Ta bort alla filer som är relaterade till spionprogrammet från datorn.
Blockera endast spionprogrammet	Blockera åtkomst till spionprogrammet men lämna det på datorn.
Uteslut spionprogrammet från genomsökning	Tillåt att spionprogram körs och uteslut det från framtida genomsökningar.

Hantera riskprogram

Med genomsökning efter virus och spionprogram blockeras riskprogram omedelbart när det försöker starta.

Innan ett riskprogram kan starta blockeras det av produkten och du får bestämma vad du vill göra med det.

Välj någon av följande åtgärder när ett riskprogram hittas:

Åtgärd som ska utföras	Vad händer med riskprogrammet?
Blockera endast riskprogrammet	Blockera åtkomst till riskprogrammet men lämna det på datorn.
Sätt riskprogrammet i karantän	Flytta riskprogrammet till karantänen där det inte kan skada datorn.
Ta bort riskprogrammet	Ta bort alla filer som är relaterade till riskprogrammet från datorn.
Uteslut riskprogrammet från genomsökning	Tillåt att riskprogrammet körs och uteslut det från framtida genomsökningar.

Ta bort spårningscookies automatiskt

Genom att ta bort spårningscookies förhindrar du att webbplatser kan spåra vilka platser du besöker på Internet.

Spårningscookies är små filer som gör att webbplatser kan registrera vilka webbplatser du besöker. Följ de här instruktioner om du vill förhindra att spårningscookies lagras på datorn.

1. Gå till huvudsidan och klicka på **Inställningar**.

Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram**.
3. Välj **Ta bort spårningscookies**.
4. Klicka på **OK**.

Söka igenom filer manuellt

Du kan söka igenom filerna manuellt, när du till exempel ansluter en extern enhet till datorn och vill kontrollera att den inte innehåller något skadeprogram.

Starta den manuella genomsökningen

Du kan välja att söka igenom hela datorn eller söka efter en specifik typ av *skadeprogram* eller en specifik plats.

Om du är misstänksam när det gäller en viss typ av *skadeprogram* kan du söka efter enbart den typen. Om du är misstänksam när det gäller en viss plats på datorn kan du välja att endast söka igenom den delen. Dessa genomsökningar går mycket snabbare än att söka igenom hela datorn.

Så här börjar du söka igenom datorn manuellt:

1. Klicka på pilen under **Genomsök** på huvudsidan.

   Sökalternativen visas.
2. Välj typ av genomsökning.

   Välj **Ändra inställningar för genomsökning** om du vill optimera den manuella genomsökningen efter virus och andra skadliga program.
3. Om har valt **Välj vad du vill genomsöka** öppnas ett fönster där du kan välja vilken plats som ska genomsökas.
   Scan Wizard öppnas.

Typ av genomsökning

Du kan välja att söka igenom hela datorn eller söka efter en specifik typ av skadeprogram eller en specifik plats.

Nedan står de olika typerna av genomsökning:

Typ av genomsökning	Vad genomsöks	När ska den här typen användas
Genomsökning efter virus	Delar av datorn söks igenom efter virus, spionprogram och riskprogram	Den här typen av genomsökning är mycket snabbare än en fullständig genomsökning. Den söker endast igenom de delar av datorn som innehåller installerade programfiler. Den här typen av genomsökning rekommenderas om du snabbt vill kontrollera att datorn är ren eftersom den effektivt hittar och tar bort alla aktiva skadeprogram på datorn.
Fullständig datorgenomsökning	Hela datorn (interna och externa hårddiskar) söks igenom efter virus, spionprogram och riskprogram	När du vill vara helt säker på att det inte finns några skadeprogram eller riskprogram på datorn. Den här typen av genomsökning tar längst tid att utföra. Den kombinerar snabbgenomsökningen efter skadeprogram med genomsökningen av hårddisken. Den letar även efter objekt som möjligen döljs av ett rootkit.

Typ av genomsökning	Vad genomsöks	När ska den här typen användas
Välj vad som ska genomsökas	En särskild fil, mapp eller enhet söks igenom efter virus, spionprogram eller riskprogram	När du misstänker att det kan finnas ett skadeprogram på en specifik plats på datorn. Det kan till exempel vara så att platsen innehåller filer som hämtats från källor som kan vara farliga, exempelvis nätverk för peer to peer-fildelning. Hur länge genomsökningen pågår beror på hur stort det valda målet är. Genomsökningen avslutas snabbt om du t.ex. genomsöker en mapp som bara innehåller ett fåtal mindre filer.
Rootkitsökning	Viktiga platser i systemet, där ett misstänkt objekt kan innebära ett säkerhetsproblem. Söker efter dolda filer, mappar, enheter eller processer	När du misstänker att ett rootkit kan ha installerats på datorn. Om ett skadeprogram till exempel nyligen upptäcktes på datorn och du vill kontrollera att skadeprogrammet inte har installerat ett rootkit.

Genomsök i Utforskaren

Du kan söka igenom enheter, mappar och filer efter *virus*, *spionprogram* och *riskprogram* i Windows Explorer.

Så här söker du igenom en enhet, mapp eller fil:

1. Placera muspekaren på den enhet, mapp eller fil som du vill söka igenom och högerklicka.
2. Högerklicka och välj **Genomsök mappar efter virus** på menyn. (Namnet på alternativet beror på huruvida du söker igenom en enhet, mapp eller fil.)
   Fönstret **Scan Wizard** öppnas och genomsökningen startar.

Om ett *virus* eller *spionprogram* hittas vägleder **Scan Wizard** dig genom rensningsprocessen.

Välja filer att söka igenom

I manuella och schemalagda genomsökningar kan du välja de filtyper som du vill söka igenom efter *virus* och *spionprogram*.

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Andra inställningar** > **Manuell genomsökning**.
3. Under **Sökalternativ** väljer du bland de följande inställningarna:

Sök endast igenom kända filtyper	Om du bara vill skanna de filtyper som mest sannolikt har infektioner, till exempel körbara filer. Om du väljer det här alternativet blir skanningen även snabbare. Filer med följande filnamnstillägg skannas: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` och `.hqx`.
Sök inuti komprimerade filer	Om du vill söka i arkivfiler och arkivmappar.

Använd avancerad heuristik	Om du vill använda all tillgänglig heuristik under genomsökningen så att du bättre kan hitta nya eller okända skadeprogram. **Obs!:** Om du väljer det här alternativet tar genomsökningen längre tid och kan resultera i fler falska positiver (ofarliga filer som rapporteras som misstänkta).

4. Klicka på **OK**.

Obs!: Uteslutna filer på listan med uteslutna objekt söks inte igenom även om du markerar dem för genomsökning här.

Vad vill du göra när skadliga filer hittas?

Välj hur du vill hantera skadliga filer när de hittas.

Så här väljer du åtgärd när skadligt innehåll hittas vid den manuella genomsökningen:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Andra inställningar** > **Manuell genomsökning**.
3. I **När virus eller spionprogram hittas** väljer du ett av följande alternativ:

Alternativ	Beskrivning
Fråga mig (standard)	Du kan välja vilken åtgärd som ska utföras när ett objekt hittas vid manuell genomsökning.
Rensa filerna	Produkten försöker automatiskt rensa infekterade filer som hittas vid manuell genomsökning. **Obs!:** Om produkten inte kan rensa den infekterade filen sätts den i karantän (utom om den hittas på nätverksenheter eller flyttbara enheter) så att den inte kan skada datorn.
Placera filerna i karantän	Produkten flyttar eventuella skadliga filer som hittas vid manuell genomsökning till karantän där de inte kan skada datorn.
Ta bort automatiskt	Produkten tar bort eventuella skadliga filer som hittas under manuell genomsökning.
Rapportera bara	Produkten lämnar eventuella skadliga filer som hittas vid manuell genomsökning som de är och registerar identifieringen i genomsökningsrapporten. **Obs!:** Om realtidsskanningen är inaktiverad kan skadlig programvara fortfarande skada datorn om du väljer det här alternativet.

Obs!: När skadliga filer hittas under en schemalagd genomsökning rensas de automatiskt.

Schemalägg en genomsökning

Konfigurera datorn så att den söker efter och tar bort virus och andra skadliga program automatiskt när du inte använder den, eller konfigurera genomsökningen så att den körs regelbundet så att du håller datorn ren.

Så här schemalägger du en genomsökning:

1. Gå till huvudsidan och klicka på **Inställningar**.

Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Andra inställningar** > **Schemalagd genomsökning**.
3. Aktivera **Schemalagd genomsökning**.
4. Välj när du vill starta genomsökningen.

Alternativ	Beskrivning
Varje dag	Sök igenom datorn varje dag.
Varje vecka	Sök igenom daton vissa dagar varje vecka. Välj dagar på listan.
Varje månad	Sök igenom datorn vissa dagar varje månad. Så här väljer du dagar: 1. Välj bland alternativen för **Dag**. 2. Välj datumet i månaden från listan bredvid den valda dagen.

5. Välj när du vill starta genomsökningen de valda dagarna.

Alternativ	Beskrivning
Starttid	Starta genomsökning vid angiven tidpunkt.
När datorn har varit oanvänd i	Starta genomsökningen när du inte har använt datorn under angiven tid.

Vid schemalagd genomsökning används inställningarna för manuell genomsökning, förutom att arkiv söks igenom varje gång och skadliga filer rensas automatiskt.

Söka igenom e-postmeddelanden

Genomsökning av e-post skyddar dig från skadliga filer i e-postmeddelanden som skickas till dig.

Genomsökning efter virus och spionprogram måste vara aktiverat om du vill söka igenom e-postmeddelanden efter virus.

Så här aktiverar du e-postskanning:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram**.
3. Välj **Ta bort skadliga bilagor i e-postmeddelanden**.
4. Klicka på **OK**.

När genomsöks e-postmeddelanden och bilagor

Vid virus- och spionprogramsgenomsökningen kan skadligt innehåll från e-postmeddelanden som du tar emot tas bort.

Virus- och spionprogramsgenomsökning tar bort skadliga e-postmeddelanden som tas emot av e-postprogram, t.ex. Microsoft Outlook och Outlook Express, Microsoft Mail eller Mozilla Thunderbird. Då genomsöks okrypterade e-postmeddelanden och bilagor varje gång ditt e-postprogram tar emot dem från e-postservern med hjälp av POP3-protokoll.

Genomsökning efter virus och spionprogram kan inte söka igenom e-postmeddelanden i webbmail, vilket omfattar e-postprogram som körs i webbläsaren, till exempel Hotmail, Yahoo! mail och Gmail. Du skyddas ändå från *virus* även om du inte tar bort skadliga bilagor eller använder webbmail. När du öppnar bifogade filer i e-postmeddelanden tas skadliga filer bort av realtidsgenomsökningen innan de hinner göra någon skada.

Obs!: Realtidsgenomsökning skyddar bara din dator, men inte dina vänner. Realtidsgenomsökning söker inte igenom bifogade filer om du inte öppnar den bifogade filen. Om du använder webbmail och vidarebefordrar ett meddelande innan du öppnar den bifogade filen kan det alltså hända att du vidarebefordrar ett infekterat e-postmeddelande till dina vänner.

Visa genomsökningsresultat

I historiken för virus och spionprogram visas alla skadliga filer som produkten har hittat.

Ibland kan produkten inte utföra den åtgärd du har valt när något skadligt hittas. Om du till exempel väljer att rensa filer, och en fil inte kan rensas, flyttar produkten filen till karantän. Du kan visa den här informationen i historiken för virus och spionprogram.

Så här visar du historiken:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram**.
3. Klicka på **Visa borttagningshistorik**.

I historiken för virus och spionprogram visas följande information:

- datum och tid när den skadliga filen hittades,
- namnet på skadeprogrammet och dess plats på datorn, samt
- utförd åtgärd.

Utesluta filer från genomsökningen

Ibland kanske du vill utesluta vissa filer eller program från genomsökningen. Utelutna objekt söks inte igenom om du inte tar bort dem från listan med uteslutna objekt.

Obs!: Uteslutningslistor är separata för realtidsgenomsökning och för manuell genomsökning. Om du till exempel utesluter en fil från realtidsgenomsökningen söks den ändå igenom vid den manuella genomsökningen om du inte utesluter den där också.

Undanta filtyper

När du utesluter filer efter filtypen genomsöks inte filer med angivna filnamnstillägg efter skadligt innehåll.

Så här lägger du till och tar bort filtyper som du vill utesluta:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj om du vill utesluta filtypen från realtidsgenomsökning eller manuell genomsökning:
   - Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram** för att utesluta filtypen från realtidsgenomsökningen.
   - Välj **Andra inställningar** > **Manuell genomsökning** för att utesluta filtypen från den manuella genomsökningen.
3. Klicka på **Uteslut filer från genomsökningen**.
4. Så här undantar du en filtyp:
   a) Välj fliken **Filtyper**.

b) Välj **Undanta filer med följande filtillägg**.
c) I fältet bredvid knappen **Lägg till** skriver du in ett filtillägg som identifierar vilken filtyp du vill exkludera.

   Om du vill ange filer som inte har något filnamnstillägg skriver du ".". Du kan använda jokertecknet "?" som vilket tecken som helst eller "*" som vilket antal tecken som helst.

   Om du till exempel vill undanta körbara filer, skriver du `exe` i fältet.
d) Klicka på **Lägg till**.

5. Upprepa föregående steg för alla filtillägg som du vill exkludera från virusgenomsökning.
6. Klicka på **OK** för att stänga dialogrutan **Undanta från genomsökning**.
7. Klicka på **OK** för att aktivera de nya inställningarna.

De valda fityperna utesluts från framtida genomsökningar.

Undanta filer efter plats

När du utesluter filer efter plats genomsöks inte filer på angivna enheter eller i angivna mappar efter skadligt innehåll.

Så här lägger du till och tar bort filsökvägar som du vill utesluta:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj om du vill utesluta platsen från realtidsgenomsökning eller manuell genomsökning:
   - Välj **Dator** > **Genomsökning efter virus och spionprogram** om du vill utesluta platsen från realtidsgenomsökning.
   - Välj **Dator** > **Manuell genomsökning** om du vill utesluta platsen från manuell genomsökning.
3. Klicka på **Uteslut filer från genomsökningen**.
4. Så här undantar du en fil, enhet eller mapp:
   a) Välj fliken **Objekt**.
   b) Välj **Undanta objekt (filer, mappar m.m.)**.
   c) Klicka på **Lägg till**.
   d) Välj den fil, enhet eller mapp som du vill ska exkluderas från virusgenomsökning.

      Obs!: Vissa enheter kan representera borttagbara enheter som cd- eller dvd-enheter eller nätverksenheter. Nätverksenheter och tomma borttagbara enheter kan inte exkluderas

   e) Klicka på **OK**.
5. Upprepa föregående steg för att exkludera andra filer, enheter, eller mappar från att genomsökas efter virus.
6. Klicka på **OK** för att stänga dialogrutan **Undanta från genomsökning**.
7. Klicka **OK** för att använda de nya inställningarna.

De valda filerna, enheterna eller mapparna utesluts från framtida genomsökningar.

Visa undantagna program

Du kan visa de program du har uteslutit från genomsökning och ta bort dem från listan med uteslutna objekt om du vill söka igenom dem i framtiden.

Om ett program påträffas i realtidsgenomsökningen eller den manuella genomsökningen som beter sig som ett spionprogram eller riskprogram, men som du vet är säkert, kan du utesluta det från genomsökningen så att produkten inte varnar dig om det.

Obs!: Om programmet beter sig som ett virus eller annan skadlig programvara kan det inte uteslutas.

Du kan inte utesluta program direkt. Nya program visas på uteslutningslistan endast om du utesluter dem under genomsökningen.

Så här visar du de program som är undantagna från genomsökning:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj om du vill visa program som har uteslutits från realtidsgenomsökning eller manuell genomsökning:
   - Välj **Dator** > **Genomsökning efter virus och spionprogram** om du vill visa vilka program som har uteslutits från realtidsgenomsökning.
   - Välj **Dator** > **Manuell genomsökning** om du vill visa program som har uteslutits från manuell genomsökning.
3. Klicka på **Uteslut filer från genomsökningen**.
4. Välj fliken **Program**.

   Obs!: Endast spionprogram och riskprogram kan undantas, inte virus.

5. Gör så här om du vill söka igenom det uteslutna programmet igen:
   a) Välj vilket program du vill ta med i genomsökningen.
   b) Klicka på **Ta bort**.
6. Klicka på **OK** för att stänga dialogrutan **Undanta från genomsökning**.
7. Klicka på **OK** när du vill avsluta.

Så här använder du karantänen

Karantänen är en säker databas för filer som skulle kunna vara skadliga.

Filer som är i karantän kan inte spridas eller orsaka skada på din dator.

Du kan placera *skadeprogram*, *spionprogram* och *riskprogram* i karantän för att oskadliggöra dem. Du kan återställa program eller filer från karantänen senare om du behöver dem.

Om du inte behöver ett visst objekt i karantän kan du radera det. När ett objekt i karantän raderas tas det bort permanent från datorn.

- Du kan i allmänhet radera *skadeprogram* i karantän.
- Du kan i de flesta fall radera *spionprogram* i karantän. Det är möjligt att *spionprogram*met är en del av ett legitimt program som slutar fungera korrekt om spionprogrammet tas bort. Om du vill behålla programmet på datorn kan du återställa *spionprogram*met som är i karantän.
- Eventuellt kan *riskprogram* i karantän vara legitima program. Om du installerade och ställde in programmet själv kan du återställa det från karantänen. Om *riskprogram*met installerades utan din vetskap installerades det troligtvis i skadligt syfte och bör tas bort.

Visa objekt i karantän

Du kan visa mer information om objekt i karantän.

Så här visar du detaljerad information om objekt i karantän:

1. Gå till huvudsidan och klicka på **Inställningar**.

Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram**.
3. Klicka på **Visa karantän**.
   På sidan **Karantän** visas det totala antalet objekt som finns lagrade i karantän.
4. Om du vill visa detaljerad information om objekt i karantän klickar du på **Detaljer**.
   Du kan sortera innehållet på antingen skadligt namn eller sökvägen.
   En lista över de hundra första objekten visas med typen för objekten i karantän, deras namn och sökvägen där filerna installerades.
5. Om du vill visa mer information om ett objekt i karantän klickar du på ikonen bredvid objektet i kolumnen **Tillstånd**.

Återställ objekt i karantän

Du kan återställa objekt i karantän som du behöver.

Du kan återställa program eller filer från karantänen om du behöver dem. Återställ endast objekt från karantänen om du är säker på att dessa objekt inte utgör något hot. Återställda objekt flyttas tillbaka till sin ursprungliga plats på datorn.

Återställ objekt i karantän

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **Genomsökning efter virus och spionprogram**.
3. Klicka på **Visa karantän**.
4. Markera de objekt i karantän som du vill återställa.
5. Klicka på **Återställ**.

Vad är DeepGuard

DeepGuard analyserar innehållet i filer och programbeteenden och övervakar program som inte är betrodda.

DeepGuard blockerar nya och oupptäckta *virus*, *maskar* och andra skadliga program som försöker göra ändringar i din dator och hindrar misstänkta program från att få tillgång till Internet.

När DeepGuard identifierar ett nytt program som försöker göra potentiellt skadliga ändringar i systemet tillåts programmet köra i en säker zon. I den säkra zonen kan programmet inte skada datorn. DeepGuard analyserar vilka ändringar programmet försöker göra och utifrån denna analys avgörs det hur troligt det är att programmet är ett *skadeprogram*. Om det är troligt att programmet är ett *skadeprogram* blockeras det av DeepGuard.

Potentiellt skadliga systemändringar som DeepGuard identifierar omfattar:

- ändringar i systeminställningarna (Windows-registret),
- försök att stänga av viktiga systemprogram, till exempel säkerhetsprogram som den här produkten, och
- försök att redigera viktiga systemfiler.

Akitvera eller inaktivera DeepGuard

Låt DeepGuard vara aktiverat så förhindrar du att misstänkta program kan göra potentiellt skadliga ändringar i datorns system.

Om du har Windows XP ska du se till att Service Pack 2 är installerat innan du aktiverar DeepGuard.

Så här aktiverar och inaktiverar du DeepGuard:

1. På huvudsidan klickar du på **Status**.
2. Klicka på **Ändra inställningar på den här sidan.**.

   Obs!: Du måste ha administratörsbehörighet för att inaktivera säkerhetsfunktioner.

3. Aktivera eller inaktivera **DeepGuard**.
4. Klicka på **Stäng**.

Tillåta program som DeepGuard har blockerat

Du kan kontrollera vilka program DeepGuard tillåter och blockerar.

Ibland kan DeepGuard blockera ett säkert program från att köras, även om du vill använda programmet och vet att det är säkert. Det händer eftersom programmet försöker göra systemändringar som kan vara potentiellt skadliga. Du kan även ha råkat blockera programmet när ett popup-fönster från DeepGuard har visats.

Så här tillåter du ett program som har blockerats av DeepGuard:

1. Klicka på **Verktyg** på huvudsidan.
2. Klicka på **Program**.
   Listan **Övervakade program** visas.
3. Hitta det program du vill tillåta.

   Obs!: Du kan sortera listan genom att klicka på kolumnrubriker. Klicka till exempel på kolumnen **Tillstånd** om du vill sortera listan i grupper om tillåtna och blockerade program.

4. Välj **Tillåt** i kolumnen **Tillstånd**.
5. Klicka på **Stäng**.

DeepGuard tillåter att programmet gör ändringar i systemet igen.

Använda DeepGuard i kompatibilitetsläget

För bästa skydd ändrar DeepGuard tillfälligt program som körs. Vissa program kontrollerar att de inte har skadats eller ändrats och kanske inte är kompatibla med den här funktionen. Onlinespel med antifuskverktyg kontrollerar till exempel att de inte har ändrats på något sätt när de körs. I så fall kan du aktivera kompatibilitetsläget.

Så här aktiverar du kompatibilitetsläget:

1. Gå till huvudsidan och klicka på **Inställningar**.

   Obs!: Du måste ha administrativa behörigheter för att ändra inställningarna.

2. Välj **Datorsäkerhet** > **DeepGuard**.
3. Välj **Använd kompatibilitetsläget**.
4. Klicka på **OK**.

Vad vill du göra vid varningar om misstänkt beteende?

DeepGuard övervakar program som inte är betrodda. Om ett övervakat program försöker få tillgång till Internet, försöker göra ändringar i systemet eller uppträder misstänkt blockeras det av DeepGuard.

När du har valt **Varna mig om misstänkt beteende** i inställningarna för DeepGuard meddelas du när DeepGuard identifierar ett potentiellt skadligt program eller när du startar ett program som är okänt.

Så här bestämmer du vad du vill göra med programmet som har blockerats av DeepGuard:

1. Klicka på **Information** om du vill visa mer information om programmet.
   I informationsavsnittet visas:
   - programmets plats,
   - programmets rykte i nätverket för realtidsskydd, samt
   - hur vanligt programmet är.
2. Bestäm om du litar på det program som DeepGuard har blockerat:
   - Välj **Jag litar på programmet. Låt det fortsätta.** om du inte vill blockera programmet.

     Det är mer troligt att programmet är säkert om:
     - DeepGuard blockerade programmet som ett resultat av något du gjorde,
     - du känner igen programmet, eller
     - du har fått programmet från en betrodd källa.
   - Välj **Jag litar inte på programmet. Blockera det.** om du vill att programmet ska vara blockerat.

     Det är mer troligt att programmet är osäkert om:
     - programmet är ovanligt,
     - programmet är okänt, eller
     - du inte känner till programmet.
3. Gör så här om du vill skicka in ett misstänkt program för analys:
   a) Klicka på **Rapportera programmet till F-Secure**.
   Produkten visar villkoren för att skicka in ett program.
   b) Klicka på **Godkänn** om du godkänner villkoren och vill skicka in provet.

   Vi rekommenderar att du skickar ett prov i följande fall:
   - DeepGuard blockerar ett program som du vet är säkert, eller
   - du misstänker att programmet är ett *skadeprogram*.