Bitdefender ANTIVIRUS PLUS

ANVÄNDARMANUAL

Bitdefender Antivirus Plus
Användarmanual

Publication date 05-10-2018

Juridisk notering

Bitdefender

Innehållsförteckning

INSTALLATION

1. FÖRBEREDER FÖR INSTALLATION

Innan du installerar Bitdefender Antivirus Plus, fullför dessa förberedelser för att försäkra att installationen ska gå smidigt:

- Försäkra dig om att datorn som du har tänkt installera Bitdefender på, uppfyller de lägsta systemkraven. Om datorn inte uppfyller alla minsta systemkrav kommer inte Bitdefender att installeras, eller om den installeras kommer den inte att fungera som den ska och orsaka avmattning samt instabilitet på systemet. För en komplett lista över systemkrav, se "*Systemkrav*" (p. 3).
- Logga in på datorn genom att använda ett administratörskonto.
- Ta bort alla andra liknande program från datorn. Om något upptäcks under Bitdefender-installationsprocessen blir du meddelad om att avinstallera det. Att köra två säkerhetsprogram samtidigt kan påverka deras aktivitet samt orsaka stora problem med systemet. Windows Defender inaktiveras under installationen.
- Vi rekommenderar att din dator är ansluten till Internet under installationen, även vid installation från en CD/DVD. Om nyare versioner av de app-filer som ingår i installationspaketet är tillgängliga kan Bitdefender hämta och installera dem.

2. SYSTEMKRAV

Du kan endast installera Bitdefender Antivirus Plus på datorer som använder följande operativsystem:

- Windows 7 med Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Innan installation, försäkra dig om att din dator möter minimisystemkraven.

Notera

Du hittar det Windows-operativsystem din dator kör och maskinvaruinformation:

- I **Windows 7** högerklickar du på **Min dator** på skrivbordet och väljer sedan **Egenskaper** från menyn.
- I **Windows 8**, från Windows Start-skärm, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt i startskärmen) och högerklicka sedan på dess ikon. I **Windows 8.1** letar du upp **Den här datorn**.

  Välj**Egenskaper** i menyn längst ned. Titta i **System**-området för att hitta information om din systemtyp.
- I **Windows 10**, skriver du **System** i sökrutan från aktivitetsfältet och klickar på ikonen. Titta i **System**-området för att hitta information om din systemtyp.

2.1. Minsta systemkrav

- 2 GB ledigt hårddiskutrymme tillgängligt
- Dual Core 1.6 GHz processor
- 1 GB minne (RAM)

2.2. Rekommenderade systemkrav

- 2,5 GB tillgängligt hårddiskutrymme (minst 800 MB på systemenheten)
- Intel CORE Duo (2 GHz) eller motsvarande processor
- 2 GB minne (RAM)

2.3. Programvarukrav

För att kunna använda Bitdefender och alla dess funktioner måste din dator uppfylla följande programvarukrav:

- Microsoft Edge 40 och senare
- Internet Explorer 10 och senare
- Mozilla Firefox 51 och senare
- Google Chrome 34 och senare

3. INSTALLERA DIN BITDEFENDER-PRODUKT

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet hämtat till din dator från Bitdefender Central.

Om ditt köp omfattar mer än en dator (du har till exempel köpt Bitdefender Antivirus Plus för 3 datorer), upprepar du installationsprocessen och aktiverar din produkt med samma konto på varje dator. Det konto du måste använda är det som innehåller din Bitdefender aktiva prenumeration.

3.1. Installera från Bitdefender Central

Från Bitdefender Central kan du hämta installationspaketet som motsvarar den köpta prenumerationen. När installationsprocessen är klar är Bitdefender Antivirus Plus aktiverad.

Hämta Bitdefender Antivirus Plus från Bitdefender Central:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:
   - **Skydda den här enheten**

     Välj det här alternativet och spara installationsfilen.
   - **Skydda andra enheter**

     Välj det här alternativet och klicka därefter på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

     Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.
4. Vänta tills nedladdningen är slutfört och kör sedan installationsprogrammet.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om systemet inte uppfyller de minsta kraven för att installera Bitdefender informeras du om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender hittas, uppmanas du att ta bort den från systemet. Följ anvisningarna för att ta bort programvaran från systemet och därmed undvika problem som inträffar senare. Du kanske måste starta om datorn för att slutföra borttagningen av de hittade säkerhetslösningarna.

Bitdefender Antivirus Plus-installationspaketet uppdateras fortlöpande.

Notera
Hämtning av installationsfilerna kan ta lång tid, särskilt över långsamma Internet-anslutningar.

När installationen är validerad visas konfigurationsguiden. Följ stegen för att installera Bitdefender Antivirus Plus.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Antivirus Plus.

Om du inte accepterar dessa villkor stänger du fönstret. Installationsprocessenn kommer att överges och du kommer att lämna installationen.

Två ytterligare uppgifter kan utföras vid det här steget:

- Behåll alternativet **Skicka produktrapporter** aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information om hur du använder produkten till Bitdefender-servrarna. Den här informationen är viktig för att förbättra produkten och kan hjälpa oss att tillhandahålla en bättre upplevelse i framtiden. Observera att dessa rapporter inte innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.
- Välj det språk du vill installera produkten på.

Klicka på **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills det är slutfört. Detaljerad information om förloppet visas.

Viktiga områden i systemet skannas för hot, de senaste versionerna av app-filerna hämtas och installeras och Bitdefender-tjänsterna startas. Det här steget kan ta några minuter. Klicka **HOPPA ÖVER SKANNING** om du vill skanna systemet senare. Mer information om hur du kör en systemskanning finns i *"Kör en systemskanning"* (p. 77).

Steg 3 - Installation slutförd

Din Bitdefender har installerats.

En sammanfattning av install processen kommer att visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av datorn behövas. Klicka på **BÖRJA ANVÄNDA Bitdefender** för att fortsätta.

Steg 4 - Kom igång

I fönstret **Kom igång** kan du se information om din aktiva prenumeration.

Klicka på **AVSLUTA** för att komma till Bitdefender Antivirus Plus-gränssnittet.

3.2. Installera från installationsskiva

Sätt i skivan i den optiska enheten för att installera Bitdefender från installationsskivan.

En installationsskärm visas inom några ögonblick. Följ instruktionerna för att starta installationen.

Om installationsskärmen inte visas använder du Utforskaren för att bläddra till skivans rotkatalog och dubbelklickar på filen autorun.exe.

Om din Internet-hastighet är långsam eller om systemet inte är anslutet till Internet klickar du på knappen **Installera från CD/DVD**. I det här fallet installeras den Bitdefender-produkt som är tillgänglig på skivan och en nyare version hämtas från Bitdefender-servrarna via produktuppdatering.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om systemet inte uppfyller de minsta kraven för att installera Bitdefender informeras du om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender hittas, uppmanas du att ta bort den från systemet. Följ anvisningarna för att ta bort programvaran från systemet och därmed undvika problem som inträffar senare. Du kanske måste starta om datorn för att slutföra borttagningen av de hittade säkerhetslösningarna.

Notera
Hämtning av installationsfilerna kan ta lång tid, särskilt över långsamma Internet-anslutningar.

När installationen är validerad visas konfigurationsguiden. Följ stegen för att installera Bitdefender Antivirus Plus.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Antivirus Plus.

Om du inte accepterar dessa villkor stänger du fönstret. Installationsprocessenn kommer att överges och du kommer att lämna installationen.

Två ytterligare uppgifter kan utföras vid det här steget:

- Behåll alternativet **Skicka produktrapporter** aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information om hur du använder produkten till Bitdefender-servrarna. Den här informationen är viktig för att förbättra produkten och kan hjälpa oss att tillhandahålla en bättre upplevelse i framtiden. Observera att dessa rapporter inte innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.
- Välj det språk du vill installera produkten på.

Klicka på **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills det är slutfört. Detaljerad information om förloppet visas.

Viktiga områden på systemet skannas för hot och Bitdefender-servrarna startas. Det här steget kan ta några minuter. Klicka **HOPPA ÖVER SKANNING** om du vill skanna systemet senare. Mer information om hur du kör en systemskanning finns i *"Kör en systemskanning"* (p. 77).

Steg 3 - Installation slutförd

En sammanfattning av install processen kommer att visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av datorn behövas. Klicka på **BÖRJA ANVÄNDA Bitdefender** för att fortsätta.

Steg 4 - Bitdefender-konto

När du slutför den initiala konfigurationen visas Bitdefender-kontofönstret. Ett Bitdefender-konto krävs för att aktivera produkten och använda dess onlinefunktioner. Mer information finns på *"Bitdefender Central"* (p. 30).

Fortsätt beroende på din situation.

- **Jag vill skapa ett Bitdefender-konto**

  1. Skriv in den önskade informationen i de motsvarande fälten. De uppgifter du lämnar här kommer att hållas konfidentiella. Lösenordet måste vara minst 8 tecken långt och innehålla en siffra.
  2. Innan du går vidare måste du godkänna användningsvillkoren. Öppna användningsvillkoren och läs dem noggrant eftersom de innehåller de villkor under vilka du får använda Bitdefender.

     Dessutom kan du öppna och läsa sekretesspolicyn.
  3. Klicka på **SKAPA KONTO**.

  > **Notera**
  > När kontot har skapats kan du använda den medföljande e-postadressen och lösenordet för att logga in på ditt konto på https://central.bitdefender.com eller i Bitdefender Central-appen förutsatt att den är installerad på en av dina Android- eller iOS-enheter. För att installera Bitdefender Central-appen på Android måste du öppna Google Play, söka efter Bitdefender Central och sedan trycka på motsvarande installationsalternativ. För att installera Bitdefender Central-appen på iOS måste du öppna App Store, söka efter Bitdefender Central och sedan trycka på motsvarande installationsalternativ.

- **Jag har redan ett Bitdefender konto**

1. Klicka på **Logga in** och skriv sedan e-postadressen och lösenordet till ditt Bitdefender-konto.

   Klicka **LOGGA IN** för att fortsätta.

2. Om du glömt lösenordet till ditt konto eller bara vill återställa det du redan ställt in klickar du på **Glömt mitt lösenord**. Skriv din e-postadress och klicka sedan på **GLÖMT LÖSENORD**. Kontrollera ditt e-postkonto och följ de angivna instruktionerna för att ställa in ett nytt lösenord för ditt Bitdefender-konto.

   Notera
   Om du redan har ett MyBitdefender-konto kan du använda det för att logga in på ditt Bitdefender-konto. Om du glömt lösenordet måste du först gå till https://my.bitdefender.com för att återställa det. Använd sedan de uppdaterade inloggningsuppgifterna för att logga in på ditt Bitdefender-konto.

- **Jag vill använda mitt Microsoft-, Facebook- eller Google-konto för att logga in**

  Logga in med ditt Microsoft-, Facebook- eller Google-konto:

  1. Välj den tjänst du vill använda. Du kommer att omdirigeras till inloggningssidan för den tjänsten.
  2. Följ instruktionerna från den valda tjänsten för att koppla ditt konto till Bitdefender.

  Notera
  Bitdefender får inte åtkomst till någon konfidentiell information som lösenordet till kontot du använder för att logga in eller personlig information om vänner och kontakter.

Steg 5 - Aktivera din produkt

Notera
Det här steget visas om du har valt att skapa ett nytt Bitdefender-konto under föregående steg eller om du har loggat in med ett konto med en prenumeration som gått ut.

En aktiv Internet-uppkoppling krävs för att slutföra aktiveringen av din produkt.

Fortsätt beroende på din situation:

- Jag har en aktiveringskod

  I det här fallet aktiverar du produkten genom att följa de här stegen:

  1. Skriv aktiveringskoden i fältet **Jag har en aktiveringskod** och klicka därefter på **FORTSÄTT**.

     Notera
     Du hittar din aktiveringskod:
     - på CD/DVD-etiketten.
     - på kortet för produktregistering.
     - i onlineköpsmeddelandet.

  2. **Jag vill utvärdera Bitdefender**

     I det här fallet kan du använda produkten i 30 dagar. Starta utvärderingsperioden genom att välja **Jag har ingen prenumeration, jag vill prova produkten gratis** och klicka sedan på **FORTSÄTT**.

Steg 6 - Kom igång

I fönstret **Kom igång** kan du se information om din aktiva prenumeration.

Klicka på **AVSLUTA** för att komma till Bitdefender Antivirus Plus-gränssnittet.

KOMMA IGÅNG

4. GRUNDERNA

När du har installerat Bitdefender Antivirus Plus är din dator skyddad mot alla typer av hot (som skadlig kod, spionprogramvara, ransomware, exploateringar, botnets och trojaner).

Appen använder Photon-teknik för att förbättra hastigheten och prestanda för hotskanningsprocessen. Det fungerar genom att lära sig användningsmönstren för dina systemappar för att veta vad och när det ska skanna och minimerar därmed påverkan på din systemprestanda.

Att ansluta till offentliga nätverk som tillhör flygplatser, köpcenter, kaféer eller hotell utan skydd kan vara farligt för din enhet och dina data. Huvudsakligen för att bedragare kan se din aktivitet och hitta det rätta ögonblicket för att stjäla personlig information, men också för att alla kan se din IP-adress och därmed göra din maskin till ett offer för framtida cyberattacker. För att undvika sådana olyckliga situationer ska du installera och använda appen *"VPN"* (p. 116).

Du kan hålla reda på dina lösenord och onlinekonton genom att lagra dem med *"Lösenordshanteringsskydd för dina inloggningsuppgifter"* (p. 109) i en plånbok. Med ett enda huvudlösenord kan du skydda din integritet från inkräktare som kan försöka komma åt dina pengar.

För att skydda dig från eventuella snokar och spioner när din enhet är ansluten till ett osäkert trådlöst nätverk, analyserar Bitdefender dess säkerhetsnivå och när det behövs, ger rekommendationer för att öka säkerheten för dina onlineaktiviteter. Se *"Wi-Fi Security Advisor"* (p. 99) för anvisningar om hur du håller dina personuppgifter säkra.

Dina personliga filer lagrade lokalt som dokument, foton eller filmer och även de som är lagrade i molnet kan hållas långt bort från dagens farligaste hot, nämligen ransomware. Se *"Safe Files"* (p. 103) för information om hur du placerar personliga filer i ett skydd.

Filer som krypterats av ransomware kan nu återställas utan att behöva betala pengar för en begärd lösensumma. Se *"Avhjälpning av ransomware"* (p. 106) för information om hur du återställer krypterade filer.

När du arbetar, spelar spel eller tittar på film kan Bitdefender ge dig en kontinuerlig användarupplevelse genom att fördröja uppgifter, eliminera avbrott och justera systemets visuella effekter. Du kan utnyttja allt detta genom att aktivera och konfigurera *"Profiler"* (p. 127).

Bitdefender fattar de mest säkerhetsrelaterade besluten åt dig och visar sällan popup-meddelanden. Detaljer om åtgärder som vidtas och information om programdrift finns i fönstret Meddelanden. Mer information finns på *"Aviseringar"* (p. 15).

Då och då bör du öppna Bitdefender och lösa eventuella existerande problem. Du kan behöva konfigurera särskilda Bitdefenderkomponenter eller ta till förebyggande åtgärder för att skydda din dator och din information.

För att använda onlinefunktionerna i Bitdefender Antivirus Plus och hantera dina prenumerationer och enheter öppnar du ditt Bitdefender-konto. Mer information finns på *"Bitdefender Central"* (p. 30).

I avsnitt "Hur" (p. 40) hittar du alla steg för steg-anvisningar om hur du utför vanliga uppgifter. Om du upplever problem med Bitdefender kan du läsa avsnittet *"Lösa vanliga problem"* (p. 135) för möjliga lösningar till de vanligaste problemen.

4.1. Öppna Bitdefender-fönstret

Följ stegen nedan för att komma till huvudgränssnittet i Bitdefender Antivirus Plus:

- I **Windows 7**:
  1. Klicka på **Start** och gå till **Alla program**.
  2. Klicka på **Bitdefender**.
  3. Klicka på **Bitdefender Antivirus Plus** eller, snabbare, dubbelklicka på Bitdefender -ikonen i systemfältet.
- I **Windows 8 och Windows 8.1**:

  Leta upp Bitdefender från Windows Start-skärm (du kan till exempel börja skriva "Bitdefender" direkt på Start-skärmen) och därefter klicka på ikonen. Alternativy kan du öppna skrivbordsappen och sedan dubbelklicka på Bitdefender -ikonen i systemfältet.
- I **Windows 10**:

  Skriv "Bitdefender" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon. Alternativt dubbelklickar du på Bitdefender -ikonen i systemfältet.

Mer information om Bitdefender-fönstret och ikonen i systemfältet finns i *"Bitdefender-gränssnitt"* (p. 19).

4.2. Aviseringar

Bitdefender för endetaljerad logg över händelser som rör dess aktivitet på din dator. Varje gång något som är relevant för säkerheten för system eller data inträffar, läggs ett nytt meddelande till i området Bitdefender-meddelanden, på ett liknande sätt som när ett nytt e-postmeddelande visas i inkorgen.

Meddelanden är ett viktigt verktyg för att övervaka och hantera ditt Bitdefender-skydd. Exempelvis kan du enkelt kontrollera om uppdateringen utfördes med framgång, om hot eller säkerhetsrisker hittades på din dator osv. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som vidtagits av Bitdefender.

Öppna meddelandeloggen genom att klicka på **Meddelanden** på navigeringsmenyn på Bitdefender-gränssnittet. Varje gång en kritisk händelse inträffar kan du se en räknare på -ikonen.

Beroende på typ och allvarlighetsgrad grupperas meddelanden i:

- **Kritiska** händelser indikerar kritiska problem. Du bör kontrollera dem omedelbart.
- **Varnings**-händelser anger problem som inte är kritiska. Du bör kontrollera dem och åtgärda dem när du har tid.
- **Informations**-händelser indikerar lyckade åtgärder.

Klicka på varje flik för att hitta mer information om de genererade händelserna. Kort information visas med ett klicka på varje händelserubrik, nämligen: en kort beskrivning, åtgärden Bitdefender vidtog för den när den inträffade samt datum och tid när den inträffade. Alternativ kan finnas för att vidta ytterligare åtgärder om det behövs.

För att det ska vara enklare att hantera loggade händelser har meddelandefönstret alternativ för att ta bort alla händelser i det avsnittet eller markera dem som lästa.

4.3. Profiler

Vissa datoraktiviteter, som onlinespel eller videopresentationer, kräver ökad systemresponsivitet, hög prestanda och inga avbrott. När din bärbara dator körs på batterikraft är det bäst att onödiga åtgärder, som kräver ytterligare kraft, skjuts upp tills datorn återigen är ansluten till elnätet.

Bitdefender-profiler tilldelar mer systemresurser till de appar som körs genom att tillfälligt ändra skyddsinställningar och justera systemkonfiguration. Följdriktligen minimeras systeminverkan på din aktivitet.

För att anpassa sig till olika aktiviteter levereras Bitdefender med följande profiler:

Arbetsprofil
: Optimerar din arbetseffektivitet genom att identifiera och justera produkt- och systeminställningarna.

Filmprofil
: Förbättrar visuella effekter och eliminerar avbrott när du tittar på film.

Spelprofil
: Förbättrar visuella effekter och eliminerar avbrott när du spelar spel.

Publik Wi-Fi-profil
: Tillämpar produktinställningar för att dra nytta av fullständigt skydd vid anslutning till ett osäkert trådlöst nätverk.

Batterilägesprofil
: Tillämpar produktinställningar och håller ned bakgrundsaktivitet för att spara batteritid.

4.3.1. Konfigurera automatisk aktivering av profiler

För en lättanvänd upplevelse kan du konfigurera Bitdefender att hantera din arbetsprofil. I det här fallet upptäcker Bitdefender automatiskt den aktivitet du utför och tillämpar optimeringsinställningar för system och produkt.

För att tillåta Bitdefender att aktivera profiler:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Använd motsvarande omkopplare för att slå på **Aktivera profiler automatiskt**.

Om du inte vill att profilerna ska aktiveras automatiskt slår du av omkopplaren.

Slå på motsvarande omkopplare för att aktivera en profil manuellt. Endast en profil i taget kan aktiveras manuellt.

Mer information om profiler finns i"*Profiler*" (p. 127)

4.4. Lösenordskyddade Bitdefender-inställningar

Om du inte är den enda personen med administrativa rättigheter som använder den här datorn, rekommenderas det att du skyddar dina Bitdefenderinställningar med ett lösenord.

Konfigurera lösenordsskydd för Bitdefender-inställningarna:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** aktiverar du **Lösenordsskydd**.
3. Skriv lösenordet i de två fälten och klicka därefter på **OK**. Lösenordet måste innehålla minst 8 tecken

När du har ställt in ett lösenord måste den som försöker ändra Bitdefender-inställningarna först ange lösenordet.

Viktigt

Kom ihåg ditt lösenord eller förvara det på en säker plats. Om du glömmer bort lösenordet måste du ominstallera programmet eller kontakta Bitdefender för support.

För att ta bort lösenordsskydd:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** inaktiverar du **Lösenordsskydd**.
3. Skriv lösenordet och klicka sedan på **OK**.

Notera

Ändra lösenordet för din produkt genom att klicka på **Ändra lösenord**. Skriv ditt aktuella lösenord och klicka sedan på **OK**. I det nya fönster som visas skriver du det nya lösenord du vill använda från och med nu för att begränsa åtkomsten till dina Bitdefender-inställningar.

4.5. Produktrapporter

Produktrapporter innehåller information om hur du använder den Bitdefender-produkt du har installerat. Den här informationen är viktig för att förbättra produkten och kan hjälpa oss att ge dig en bättre upplevelse i framtiden.

Observera att dessa rapporter inte innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.

Om du under installationsprocessen har valt att skicka sådana rapporter till Bitdefender-servrarna och nu vill stoppa processen:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till **Avancerat** fliken.
3. Stäng av **Produktrapporter**.

4.6. Meddelanden om särskilda erbjudanden

När kampanjerbjudanden är tillgängliga ställs Bitdefender-produkten in på att meddela dig via ett popup-fönster. Det här ger dig möjlighet att dra nytta ab fördelaktiga priser och hålla dina enheter skyddade under en längre tidsperiod.

För att slå av eller på meddelanden om specialerbjudanden:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Slå av eller på motsvarande omkopplare i fönstret **Allmänt**.

Alternativet för specialerbjudanden och produktmeddelanden är aktiverad som standard.

4.7. Skanningstjänst mot skadlig kod

Bitdefender integreras med Microsoft Antimalware Scan Interface (AMSI), ett sätt att hjälpa dig fortsätta vara skyddad från dynamisk skriptbaserad skadlig kod och icke-traditionella cyberattacker. AMSI är en generisk gränssnittsstandard som låter program och tjänster integreras med Bitdefender-produkter.

Stänga av eller slå på integration med Antimalware Scan Interface:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Slå av eller på motsvarande omkopplare i fönstret **Allmänt**.

Alternativet för integrering med Antimalware Scan Interface är aktiverat som standard och är endast tillgängligt i Windows 10.

5. BITDEFENDER-GRÄNSSNITT

Bitdefender Antivirus Plus uppfyller behoven lika mycket för nybörjare på datorer som för väldigt tekniska människor. Dess grafiska användargränssnitt är utformat för att passa alla sorters människor.

För att gå igenom Bitdefender-gränssnittet finns en introduktionsguide som innehåller information om hur du interagerar med produkten och hur du konfigurerar den på den övre vänstra sidan. Välj rätt höger vinkelparentes för att fortsätta guidas eller **Hoppa över rundtur** för att stänga guiden.

Bitdefenders systemfältsikon är tillgänglig när som helst, oavsett om du vill öppna huvudfönstret, köra en produktuppdatering eller visa information om den installerade versionen.

I huvudfönstret finns information om din säkerhetsstatus. Baserat på din enhetsanvändning och behov visar Autopilot här olika typer av rekommendationer som hjälper dig att förbättra din enhetssäkerhet och prestanda. Dessutom kan du lägga till snabbåtgärder som du använder ofta, så att du har dem till hands när du behöver dem.

Från navigeringsmenyn till vänster kan du öppna ditt Bitdefender-konto, inställningarna, meddelanden och Bitdefender-avsnitten för detaljerad konfiguration och avancerade administrativa uppgifter. Du kan även kontakta oss för support om du har frågor eller något oväntat inträffar.

Om du vill hålla ett konstant öga på viktig säkerhetsinformation och ha snabb åtkomst till viktiga inställningar lägger du till säkerhetswidgeten på skrivbordet.

5.1. Systemfältsikon

För att snabbare hantera hela produkten kan du använda Bitdefender-ikonen i systemfältet.

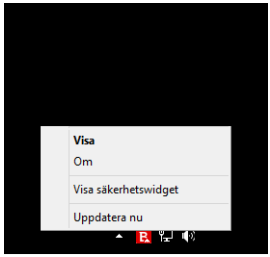
Notera
Bitdefender-ikonen kanske inte är synlig hela tiden. För att ikonen ska visas permanent:

- I **Windows 7, Windows 8 och Windows 8.1**:
  1. Klicka på pilen i det nedre högra hörnet på skärmen.
  2. Klicka på **Anpassa...** för att öppna fönstret Meddelandeområdesikoner.

3. Välj alternativet **Visa ikoner och meddelanden** för **Bitdefender-agent**-ikonen.

- I **Windows 10**:
  1. Högerklicka aktivitetsfältet och välj **Egenskaper**.
  2. Klicka på **Anpassa** i fönstret Aktivitetsfält.
  3. Klicka på länken **Välj vilka ikoner som ska visas i aktivitetsfältet** i fönstret **Meddelanden och åtgärder**.
  4. Aktivera omkopplaren bredvid **Bitdefender-agenten**.

Om du dubbelklickar den här ikonen kommer Bitdefender att öppnas. Genom att högerklicka ikonen kommer en kontextmeny att snabbt låta dig hantera Bitdefenderprodukten.



Systemikon

- **Visa** - öppnar huvudfönstret i Bitdefender.
- **Om** - öppnar ett fönster där du kan se information om Bitdefender, var du kan få hjälp om något oväntat inträffar, var du hittar och visar prenumerationsavtalet, tredjepartskomponenter och sekretesspolicy.
- **Dölj/Visa säkerhetswidget** - aktiverar/inaktiverar Säkerhetswidget.
- **Uppdatera nu** - startar en omedelbar uppdatering. Du kan följa upp uppdateringsstatusen i uppdateringspanelen i Bitdefenders huvudfönster.

Bitdefender systemfältsikon informerar dig när problem påverkar din dator eller om hur produkten fungerar, genom att visa en speciell symbol, enligt följande:

Det finns inga problem som påverkar ditt systems säkerhet.
Kritiska problem påverkar ditt systems säkerhet. De kräver din omedelbara uppmärksamhet och måste lösas så snart som möjligt.

Om Bitdefender inte fungerar visas systemfältsikonen mot en grå bakgrund: . Det här händer oftast när prenumerationen går ut. Det kan även hända när Bitdefender tjänsterna inte svarar eller när andra fel påverkar Bitdefender normala aktivitet.

5.2. Navigeringsmeny

På den vänstra sidan i Bitdefender-gränssnittet finns navigeringsmenyn, som gör det möjligt för dig att snabbt komma till Bitdefender-funktionerna och verktygen du behöver för att hantera din produkt. Flikarna som finns i det området är:

- **Kontrollpanel**. Härifrån kan du snabbt åtgärda säkerhetsproblem, visa rekommendationer enligt dina systembehov och användningsmönster och utföra snabbåtgärder.
- **Skydd**. Härifrån kan du starta och konfigurera antivirusskanningar, öppna brandväggsinställningar, skydda filer och appar från ransomwareattacker, återställa data ifall de krypteras av ransomware och konfigurera skydd medan du surfar på Internet.
- **Sekretess**. Härifrån kan du skapa lösenordshanterare för dina onlinekonton, skydda åtkomsten till din webbkamera från oönskade ögon, göra onlinebetalningar i en säker miljö och öppna VPN-appen.
- **Meddelanden**. Härifrån har du åtkomst till de genererade meddelandena.
- **Mitt konto**. Härifrån kan du komma åt ditt Bitdefender-konto för att verifiera dina prenumerationer och utföra säkerhetsåtgärder på de enheter du hanterar. Information om Bitdefender-konto och pågående prenumeration finns också.
- **Inställningar**. Härifrån har du åtkomst till allmänna inställningar.
- **Support**. Härifrån kan du, när du behöver hjälp med att lösa ett problem med Bitdefender Antivirus Plus, kontakta Bitdefenders tekniska supportavdelning.

5.3. Kontrollpanel

I kontrollpanelsfönstret kan du utföra vanliga åtgärder, snabbt lösa säkerhetsproblem, visa information om produktfunktion och öppna panelerna varifrån du kan konfigurera produktinställningarna.

Allt är bara några klick borta.

Fönstret är indelat i tre huvudområden:

Säkerhetsstatusområde
: Härifrån kan du kontrollera datorns säkerhetsstatus.

Auto Pilot
: Härifrån kan du kontrollera Autopilot-rekommendationerna för att säkerställa korrekt funktionalitet i systemet.

Snabbåtgärder
: Härifrån kan du köra olika uppgifter för att hålla ditt system skyddat.

5.3.1. Säkerhetsstatusområde

Bitdefender använder system för spårning av problem för att upptäcka och informera dig om problem som kan påverka din dators säkerhet och information. Upptäckta problem omfattar viktiga skyddsinställningar som är avstängda och andra förhållanden som kan innebära en säkerhetsrisk.

Varje gång problem påverkar säkerheten för din dator ändras statusen som visas på den övre sidan av Bitdefender-gränssnittet till röd. Den visade statusen anger hur problemen påverkar ditt system. Dessutom ändras systemfältsikonen till och om du för muspekaren över ikonen kommer en popup att bekräfta att det finns olösta problem.

Eftersom de upptäckta problemen kan förhindra Bitdefender från att skydda dig mot hot eller utgöra en stor säkerhetsrisk, rekommenderar vi att du är uppmärksam och löser dem så snabbt som möjligt. Klicka på knappen bredvid det upptäckta problemet för att lösa det.

5.3.2. Auto Pilot

För att ge dig en effektiv drift och ökat skydd när du utför olika aktiviteter, fungerar Bitdefender Autopilot som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, om du antingen arbetar, utför onlinebetalningar, ser på film eller spelar spel, kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov. De föreslagna rekommendationerna kan också handla om åtgärder du behöver utföra för att din produkt ska fungera fullt ut.

För att börja använda en föreslagen funktion eller göra förbättringar av din produkt, klickar du på motsvarande knapp.

Stänga av Autopilot-meddelanden

För att du ska uppmärksamma Autopilot-rekommendationerna är Bitdefender-produkten inställd på att meddela dig via ett popupfönster.

Stänga av Autopilot-meddelanden:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** stänger du av **Rekommendationsmeddelanden**.

5.3.3. Snabbåtgärder

Med snabbåtgärder kan du snabbt starta uppgifter som anser vara viktiga för att hålla ditt system skyddat och förbättra ditt sätt att arbeta.

Som standard kommer Bitdefender med några snabbåtgärder som kan ersättas med dem du använder mest. Byta ut en snabbåtgärd:

1. Klicka på + -ikonen i det övre högra hörnet på det kort du vill ta bort.
2. Peka på den uppgift du vill lägga till i huvudgränssnittet och klicka sedan på **LÄGG TILL**.

De uppgifter du kan lägga till i huvudgränssnittet är:

- **Snabbsökning**. Kör en snabbskanning för att direkt upptäcka möjliga hot som kan finns på din dator.
- **Systemskanning**. Kör en systemskanning för att se till att din dator är ren från hot.
- **Vulnerability Scan**. Skanna din dator för säkerhetsrisker för att se till att alla installerade appar, tillsammans med operativsystemet, är uppdaterade och fungerar som de ska.
- **Kontrollera Wi-Fi-säkerhet**. Öppna Wi-Fi Security Advisor för att kontrollera om det trådlösa hemnätverk du är ansluten till är säkert eller inte och om det har säkerhetsrisker.
- **Plånböcker**. Visa och hantera dina plånböcker.
- **Öppna SafePay**. Öppna Bitdefender Safepay™ för att skydda dina känsliga data medan du utför onlinetransaktioner.
- **Öppna VPN**. Öppna Bitdefender VPN för att lägga till ett extra lager skydd när du är ansluten till Internet.
- **Filförstöraren**. Starta verktyget File Shredder för att ta bort spår efter känsliga data från din dator.
-

Börja skydda ytterligare enheter med Bitdefender:

1. Klicka på **Installera på en annan enhet**.

   Du omdirigeras till Bitdefender-kontosidan. Se till att du är inloggad med dina inloggningsuppgifter.

2. Klicka på **SKICKA HÄMTNINGSLÄNK** i det fönster som visas.

3. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

   Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och tryck på motsvarande hämtningsknapp.

Beroende på ditt val installeras följande Bitdefender-produkter:

- Bitdefender Antivirus Plus på Windows-baserade enheter.
- Bitdefender Antivirus for Mac på macOS-baserade enheter.
- Bitdefender Mobile Security på Android-baserade enheter.
- Bitdefender Mobile Security på iOS-baserade enheter.

5.4. Bitdefender-avsnitten

Bitdefender-produkten kommer med två avsnitt indelade i användbara funktioner som hjälper dig att hålla dig skyddad medan du arbetar, surfar på nätet, spelar spel eller vill göra onlinebetalningar.

När du vill komma åt funktionerna för ett specifikt avsnitt eller börja konfigurera din produkt använder du följande ikoner som finns på navigeringsmenyn på Bitdefender-gränssnittet:

- Skydd
- Sekretess

5.4.1. **Skydd**

In avsnittet Skydd kan du konfigurera dina avancerade säkerhetsinställningar, ställa in funktionerna Safe Files och Online Threat Prevention, kontrollera och åtgärda eventuella systemsårbarheter och komma åt säkerheten för de trådlösa nätverk du ansluter till.

De funktioner du kan hantera i avsnittet Skydd är:

VIRUSSKYDD

Antivirusskydd är grunden i din säkerhet. Bitdefender skyddar dig i realtid och på begäran mot alla typer av hot, som skadlig kod, trojaner, spionprogramvara, adware, mm.

Från antivirusfunktionen kan du enkelt komma åt följande skanningsåtgärder:

- Snabbsökning
- Systemskanning
- Hantera skanningar
- Räddningsläge (räddningsmiljö i Windows 10)

Mer information om skanningsjobb och hur du konfigurerar antivirusskydd finns i *"Antivirusskydd"* (p. 71).

FÖREBYGGANDE AV ONLINEHOT

Med förebyggande av onlinehot kan du skydda dig mot nätfiskeattacker, bedrägeriförsök och läckage av privat information, när du surfar på nätet.

Mr information om hur du konfigurerar Bitdefender för att skydda din nätaktivitet finns i *"Förebygga onlinehot"* (p. 93).

ADVANCED THREAT DEFENSE

Avancerat hotförsvar skyddar aktivt ditt system mot hot som ransomware, spyware och trojaner genom att analysera beteende hos alla installerade appar. Misstänkta processer identifieras och blockeras, om det behövs.

;er information om hur du skyddar systemet mot hot finns i *"Avancerat hotskydd"* (p. 91).

SÄKERHETSRISK

Funktionen Säkerhetsrisk hjälper dig att hålla det operativsystem och de appar du använder regelbundet uppdaterade och att identifiera de trådlösa nätverk du ansluter till.

Klicka på **Säkerhetsriskskanning** i funktionen Säkerhetsrisk för att börja identifiera viktiga Windows-uppdateringar, appuppdateringar, svaga lösenord som hör till Windows-konton och trådlösa nätverk som int är säkra.

Klicka på **Wi-Fi security** för att visa listan över de trådlösa nätverk du ansluter till, tillsammans med vår ryktesutvärdering för var och ett av

dem och de åtgärder du kan vidta för att skydda dig mot eventuella spioner.

Mer information om hur du konfigurerar säkerhetsriskskydd finns i *"Säkerhetsrisk"* (p. 96).

SÄKRA FILER

Funktionen Säkra filer ser till att dina personliga filer är skyddade från ransomwareattacker.

Mer information om hur du konfigurerar Säkra filer för att skydda dina personliga filer från ransomware attacker finns i *"Safe Files"* (p. 103).

AVHJÄLPNING AV RANSOMWARE

Funktionen Avhjälpning av ransomware hjälper dig att återställa filer ifall de krypteras av ransomware.

Mer information om hur du återställer krypterade filer finns i *"Avhjälpning av ransomware"* (p. 106).

5.4.2. Sekretess

I avsnittet Sekretess kan du öppna Bitdefender VPN-appen, skydda dina onlinetransaktioner och se till att din surfupplevelse är säker.

De funktioner du kan hantera i avsnittet Sekretess är:

VPN

VPN säkrar din onlineaktivitet och döljer din IP-adress varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, köpcenter, kaféer eller hotell. Dessutom kan du komma åt innehåll som i normala fall är begränsat i vissa områden.

Mer information om den här funktionen finns i *"VPN"* (p. 116).

PLÅNBOK

Bitdefender lösenordshanterare hjälper dig att hålla reda på dina lösenord, skyddar din integritet och ger en säker surfupplevelse.

Mer information om hur du konfigurerar lösenordshanteraren finns i *"Lösenordshanteringsskydd för dina inloggningsuppgifter"* (p. 109).

SAFEPAY

Webbläsaren Bitdefender Safepay™ hjälper dig att se till att dina bankärenden online, e-shopping och andra typer av onlinetransaktioner är privata och säkra.

Mer information om Bitdefender Safepay™ finns i *"Safepay-säkerhet för onlinetranslationer"* (p. 119).

DATASKYDD

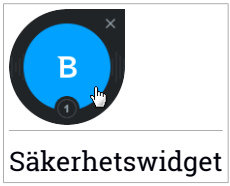
Med funktionen Dataskydd kan du ta bort filer permanent.
Klicka på **Filförstöraren** i panelen Dataskydd för att starta en guide där du kan helt eliminera filer från ditt system.

Mer information om hur du konfigurerar dataskydd finns i *"Dataskydd"* (p. 124).

5.5. Säkerhetswidget

Säkerhetswidget är det snabba och säkra sättet att övervaka och styra Bitdefender Antivirus Plus. Om du lägger till den här lilla och ej störande widgeten på skrivbordet kan du se kritisk information och utföra viktiga åtgärder hela tiden.

- öppna huvudfönstret i Bitdefender.
- övervaka skanningsaktivitet i realtid.
- övervaka säkerhetsstatus för ditt system och fixa befintliga problem.
- visa när en uppdatering pågår.
- via meddelanden och få åtkomst till de senaste händelserna som rapporterats av Bitdefender.
- skanna filer eller mappar genom att dra och släppa ett eller flera objekt över widgeten.



Säkerhetswidget

Den allmänna säkerhetsstatusen för din dator visas **i mitten** av widgeten. Statusen anges av färgen och formen för ikonen som visas i det här området.


Kritiska problem påverkar säkerheten i ditt system.

De kräver din omedelbara uppmärksamhet och måste lösas så snart som möjligt. Klicka på statusikonen för att börja åtgärda de rapporterade problemen.

 Icke-kritiska problem påverkar säkerheten i ditt system. Du bör kontrollera dem och åtgärda dem när du har tid. Klicka på statusikonen för att börja åtgärda de rapporterade problemen.

 Ditt system är skyddat.

 När en på begäran-åtgärd utförs visas den här animerade ikonen.

När problem rapporteras klickar du på statusikonen för att starta guiden Åtgärda problem.

Den lägre sidan av widgeten visar räknaren för olästa händelser (antalet utestående händelser som rapporterats av Bitdefender, om det finns några). Klicka på händelseräknaren, till exempel 1 för en oläst händelse, för att öppna meddelandefönstret. Mer information finns på *"Aviseringar"* (p. 15).

5.5.1. Skanna filer och mappar

Du kan använda säkerhetswidgeten för att snabbt skanna filer och mappar. Dra en fil eller mapp som du vill ska skannas och släpp den över **säkerhetswidgeten**.

Guiden för antivirusskanning kommer att visas och leda dig genom skanningsprocessen. Skanningsalternativen är förkonfigurerade för bästa upptäcktsresultat och kan inte ändras. Om smittade filer hittas försöker Bitdefender desinfektera dem (ta bort den skadliga koden). Om desinfektering misslyckas, kommer guiden för Antivirus-skanning att låta dig välja andra åtgärder att ta till mot infekterade filer.

5.5.2. Dölj/visa säkerhetswidget

När du inte längre vill se widgeten klickar du på ⊗.

Använd en av följande metoder för att återställa säkerhetswidgeten:

- Från systemfältet:
  1. Högerklicka på Bitdefender-ikonen i systemfältsikonen.
  2. Klicka på **Visa säkerhetswidget** i kontextmenyn som visas.

- Från Bitdefenders gränssnitt:
  1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I fönstret **Allmänt** slår du på **Säkerhetswidget**.

Bitdefenders säkerhetswidget är inaktiverad som standard.

6. BITDEFENDER CENTRAL

Bitdefender Central är en plattform vart du har tillgång till produktens alla onlinefunktioner och tjänster och kan fjärransluta viktiga uppgifter på enheterna Bitdefender är installerat på. Du kan logga in på ditt Bitdefender-konto från vilken dator som helst som är ansluten till Internet genom att gå till https://central.bitdefender.com, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

Så här installerar du Bitdefender Central-appen på dina enheter:

- **På Android** - sök Bitdefender Central på Google Play och hämta och installera appen. Följ stegen för att slutföra installationen.
- **På Android** - sök Bitdefender Central på App Store och hämta och installera appen. Följ stegen för att slutföra installationen.

När du är inloggad kan du börja göra följande:

- Hämta och installera Bitdefender på Windows, macOS, iOS och Android. De produkter som är tillgängliga för hämtning är:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus för Mac
  - Bitdefender Mobile Security för Android
  - Bitdefender Mobile Security för iOS
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter till nätverket och hantera dem var du än är.

6.1. Öppna Bitdefender Central

Det finns flera sätt att öppna Bitdefender Central:

- Från Bitdefenders huvudgränssnitt:
  1. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. Klicka på **Gå till Bitdefender Central**.
  3. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.
- Från din webbläsare:
  1. Öppna en webbläsare på en enhet med Internet-åtkomst.

2. Gå till: https://central.bitdefender.com.
3. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.

- Från din Android- eller iOS-enhet:

  Öppna Bitdefender Central-appen som du har installerat.

> **Notera**
> I det här materialet har du alternativ och instruktioner tillgängliga på webbplattformen.

6.2. Mina prenumerationer

Bitdefender Central-plattformen ger dig möjlighet att enkelt hantera de prenumerationer du har för alla dina enheter.

6.2.1. Kontrollera tillgängliga prenumerationer

Kontrollera dina tillgängliga prenumerationer:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina prenumerationer**.

Här har du information om de prenumerationer du äger och antal enheter som använder var och en av dem.

Du kan lägga till en ny enhet till en prenumeration eller förnya den genom att välja ett prenumerationskort.

> **Notera**
> Du kan ha en eller flera prenumerationer på ditt konto förutsatt att de är för olika plattformar (Windows, macOS, iOS eller Android).

6.2.2. Lägg till ny enhet

Om din prenumeration omfattar mer än en enhet kan du lägga till en ny enhet och installera din Bitdefender Antivirus Plus på den, enligt följande:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:

   - **Skydda den här enheten**

Välj det här alternativet och spara installationsfilen.

- **Skydda andra enheter**

  Välj det här alternativet och klicka därefter på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

  Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.

4. Vänta tills nedladdningen är slutfört och kör sedan installationsprogrammet.

6.2.3. Förnya prenumeration

Om du inte valde bort att automatiskt förnya din Bitdefender-prenumeration, kan du manuellt förnya den genom att följa de här stegen:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina prenumerationer**.
3. Välj önskat prenumerationskort.
4. Klicka på **FÖRNYA** för att fortsätta.

En webbsida öppnas i din webbläsare där du kan förnya din Bitdefender-prenumeration.

6.2.4. Aktivera prenumeration

En prenumeration kan aktiveras under installationsprocessen genom att använda ditt Bitdefender-konto. Tillsammans med aktiveringsprocessen börjar giltigheten räknas ned.

Om du har köpt en aktiveringskod från någon av våra återförsäljare eller om du fått den som present, kan du lägga till dess tillgänglighet till en befintlig Bitdefender-prenumeration som är tillgänglig på kontot, förutsatt att de är för samma produkt.

Aktivera en prenumeration med en aktiveringskod:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina prenumerationer**.

3. Klicka på knappen **AKTIVERINGSKOD** och skriv sedan in koden i motsvarande fält.
4. Klicka på **AKTIVERA** för att fortsätta.

Prenumerationen är nu aktiv. Gå till panelen **Mina enheter** och välj **INSTALLERA SKYDD** för att installera produkten på en av dina enheter.

6.3. Mina enheter

I området **Mina enheter** i Bitdefender Central har du möjlighet att installera, hantera och vidta fjärråtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till Internet. Enhetskorten visar enhetsnamn, skyddsstatus och om det finns säkerhetsrisker som påverkar enheternas skydd.

Visa en lista över dina enheter sorterad efter deras status eller användare genom att klicka på rullgardinspilen i det övre högra hörnet på skärmen.

För att enkelt identifiera dina enheter kan du anpassa enhetsnamnet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.
4. Välj **Inställningar**.
5. Skriv in ett nytt namn i fältet **Enhetsnamn**, klicka därefter på **SPARA**.

Du kan skapa och tilldela en ägare för varje enhet för bättre hantering:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.
4. Välj **Profil**.
5. Klicka på **Lägg till ägare** och fyll i motsvarande fält. Anpassa profilen genom att lägga till ett foto och välj ett födelsedatum.
6. Klicka på **LÄGG TILL** för att spara profilen.
7. Välj önskad ägare från listan **Enhetsägare** och klicka på **TILLDELA**.

Fjärruppdatera Bitdefender på en Windows-enhet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

Klicka på önskat enhetskort för fler fjärråtgärder och information angående din Bitdefender-produkt på en specifik enhet.

När du klickar på ett enhetskort är följande flikar tillgängliga:

- **Kontrollpanel**. I det här fönstret kan du visa information om den valda enheten, kontrollera dess skyddsstatus, status för Bitdefender VPN och hur många hot som har blockerats de senaste sju dagarna. Skyddsstatus kan vara grönt när det inte finns några problem som påverkar enheten, gult när enheten behöver åtgärdas från din sida eller rött när enheten är utsatt för risk. När det finns problem som påverkar enheten klickar du på rullgardinsmenyn i det övre statusområdet för att se mer information. Härifrån kan du manuellt åtgärda problem som påverkar dina enheters säkerhet.
- **Skydd**. Från det här fönstret kan du fjärrstyra en snabb- eller systemskanning på dina enheter. Klicka på knappen **SKANNA** för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och det finns en rapport från den senaste skanningen med den viktigaste informationen.Mer information om de här två skanningsprocesserna finns i *"Kör en systemskanning"* (p. 77) och *"Köra en snabbskanning"* (p. 77).
- **Säkerhetsrisk**. Klicka på knappen **SKANNA** på fliken Säkerhetsrisk för att kontrollera en enhet för eventuella säkerhetsrisker som saknade Windows-uppdateringar, utdaterade appar eller svaga lösenord. Säkerhetsrisker kan inte åtgärdas via fjärrstyrning. Om en säkerhetsrisk hittas måste du köra en ny skanning på enheten och sedan vidta rekommenderade åtgärder. Klicka på **Mer information** för att komma åt en detaljerad rapport om de problem som hittas. Mer information om den här funktionen finns i *"Säkerhetsrisk"* (p. 96).

6.4. Mitt konto

I området **Mitt konto** kan du anpassa din profil, byta det lösenord som är associerat med ditt konto, hantera inloggningssessionerna och Bitdefender Central-hjälpmeddelanden.

När du klickar på -ikonen på den övre högra sidan av skärmen och väljer **Mitt konto**, har du följande flikar:

- **Profil** - här kan du lägga till och redigera kontoinformation.
- **Ändra lösenord** - härifrån kan ändra lösenordet som är kopplat till ditt konto.
- **Sessionshantering** - här kan du visa och hantera de senaste inaktiva och aktiva inloggningssessionerna som körs på enheter som är kopplade till ditt konto.
- **Inställningar** - här kan du stänga av och slå på Bitdefender Central-hjälpmeddelanden och bestämma om du vill bli meddelad eller inte när stillbilder tas på dina Android-enheter.

6.5. Aviseringar

För att du ska vara informerad om vad som händer på de enheter som är kopplade till ditt konto finns -ikonen till hands. När du klickar på den har du en översiktsbild som består av information om aktiviteten för de Bitdefender-produkter som är installerade på dina enheter.

7. SE TILL ATT BITDEFENDER ÄR UPPDATERAD

Nya hot hittas och identifieras varje dag. Det här är orsaken till varför det är mycket viktig att se till att Bitdefender är uppdaterad med den senaste hotinformationsdatabasen.

Om du är ansluten till Internet via bredband eller DSL, tar Bitdefender hand om detta själv. Som standard söker det efter updateringar när du slår på din dator samt varje **timme** efter det. Om en uppdatering upptäcks kommer den automatiskt att hämtas och installeras på din dator.

Uppdateringsprocessen utförs i farten, vilket betyder att filerna som ska uppdateras ersätts efter hand. På så sätt kommer inte uppdateringsprocessen att påverka produktaktiviteten och samtidigt kommer alla säkerhetsrisker att exkluderas.

Viktigt
För att vara skyddad mot de senaste hoten ska du se till att Automatisk uppdatering är aktiverat.

I vissa särskilda situationer krävs ingripande från dig för att hålla ditt Bitdefender-skydd uppdaterat:

- Om din dator ansluts till Internet via en proxyserver måste du konfigurera proxyinställningarna såsom beskrivs i *"Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?"* (p. 64).
- Om du är ansluten till Internet via en uppringningsanslutning rekommenderas du att regelbundet uppdatera Bitdefender på användarbegäran. Mer information finns på *"Utför en uppdatering"* (p. 37).

7.1. Kontrollerar om Bitdefender är uppdaterad

Kontrollera tidpunkten för den senaste uppdateringen av din Bitdefender:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste uppdateringen.

Du kan ta reda på när uppdateringar startades och information om dem (om de lyckades eller inte, om det krävs en omstart för att slutföra installationen). Om så krävs startar du om systemet så snabbt som möjligt.

7.2. Utför en uppdatering

För att göra uppdateringar krävs en Internet-anslutning.

Starta en uppdatering genom att högerklicka på Bitdefender -ikonen i systemfälet och sedan välja **Uppdatera nu**.

Uppdateringsfunktionen ansluter till Bitdefender-uppdateringsserver och kontrollerar om det finns uppdateringar. Om en uppdatering upptäcks kommer du antingen att ombes att bekräfta uppdateringen, eller så utförs uppdateringen automatiskt, beroende påuppdateringsinställningarna.

Viktigt
Det kan vara nödvändigt att starta om datorn när du har slutfört uppdateringen. Vi rekommenderar att göra det så snart som möjligt.

Du kan också fjärrstyra uppdateringar på dina enheter, förutsatt att de är påslagna och anslutna till Internet.

Fjärruppdatera Bitdefender på en Windows-enhet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

7.3. Slå på eller av automatisk uppdatering

Slå på eller av automatisk uppdatering:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Uppdatera**.
3. Slå av eller på motsvarande omkopplare.
4. Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att automatiskt uppdatering ska vara inaktiv. Du kan inaktivera den automatiska uppdateringen i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart.

Varning
Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar automatisk uppdatering under så kort tid som möjligt. Om Bitdefender inte uppdateras regelbundet kan det inte skydda dig mot de senaste hoten.

7.4. Automatiska uppdateringsinställningar

Uppdateringarna kan utföras från det lokala nätverket, över Internet, direkt eller via en proxyserver. Som standard kommer Bitdefender att söka efter uppdateringar över Internet varje timme, och installera tillgängliga uppdateringar utan att meddela dig.

Standardinställningarna för uppdatering är anpassade efter de flesta användare och i normala fall behöver du inte ändra dem.

Justera uppdateringsinställningarna:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Uppdatera** och justera inställningarna enligt dina önskemål.

Uppdateringsfrekvens

Bitdefender är konfigurerad att kontrollera efter uppdateringar varje timme. Ändra uppdateringsfrekvensen genom att dra reglaget längs skalan för att ange önskad tidsperiod när uppdateringen ska ske.

Uppdatera bearbetningsregler

Varje gång en uppdatering är tillgänglig hämtar Bitdefender uppdateringen automatiskt och implementerar den utan att visa meddelanden. Stäng av alternativet **Tyst uppdatering** om du vill bli meddelad varje gång en ny uppdatering är tillgänglig.

Vissa uppdateringar kräver en omstart för att slutföra installationen.

Som standard fortsätter Bitdefender arbeta med de gamla filerna tills användaren frivilligt startar om datorn, om en uppdatering kräver en omstart. Det är för att förhindra Bitdefender-uppdateringsprocessen från att störa användarens arbete.

Om du vill ha ett meddelande när en uppdatering kräver en omstart slår du på **Omstartsmeddelande**.

7.5. Kontinuerliga uppdateringar

För att se till att du använder den senaste versionen kontrollerar Bitdefender automatiskt för produktuppdateringar. Dessa uppdateringar kan medföra nya funktioner och förbättringar, lösa produktproblem eller automatiskt uppgradera dig till en ny version. När den nya Bitdefender-versionen kommer via en uppdatering sparas anpassade inställningar och avinstallations- och ominstallationsproceduren hoppas över.

Dessa uppdateringar kräver en systemomstart för att installationen av nya filer ska starta. När en produktuppdatering är slutförd talar ett popup-fönster om att du ska starta om systemet. Om du missar det här meddelandet kan du antingen klicka på **STARTA OM NU** i fönstret Meddelanden där den senaste uppdateringen nämns eller starta om systemet manuellt.

Notera
Uppdateringarna omfattar nya funktioner och förbättringar som endast levereras till användare som har Bitdefender 2018 installerat.

HUR

8. INSTALLATION

8.1. Hur installerar jag Bitdefender på en andra dator?

Om den prenumeration du har köpt omfattar mer än en dator kan du använda ditt Bitdefender-konto för att aktivera en andra PC.

Installera Bitdefender på en andra dator:

1. Klicka på **Installera på annan enhet** i det nedre vänstra hörnet av Bitdefender-gränssnittet.

   Du omdirigeras till Bitdefender-kontosidan. Se till att du är inloggad med dina inloggningsuppgifter.

2. Klicka på **SKICKA HÄMTNINGSLÄNK** i det fönster som visas.

3. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

   Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och tryck på motsvarande hämtningsknapp.

4. Kör den Bitdefender-produkt du har hämtat.

Den nya enhet på vilken du har installerat Bitdefender-produkten visas i Bitdefender Central-kontrollpanelen.

8.2. Hur installerar jag om Bitdefender?

Typiska situationer när du skulle behöva installera om Bitdefender kan vara följande:

- du har installerat om operativsystemet.
- du vill lösa problem som kan ha orsakat nedgångar eller krascher.
- din Bitdefender-produkt startar inte eller fungerar inte korrekt.

Om något av de nämnda situationerna är ditt fall följer du de här stegen:

- I **Windows 7**:
  1. Klicka på **Start** och gå till **Alla program**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

3. Klicka på **INSTALLERA OM** i det fönster som visas.
4. Du måste starta om datorn för att slutföra processen.

- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **INSTALLERA OM** i det fönster som visas.
  5. Du måste starta om datorn för att slutföra processen.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Appar och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
  5. Klicka på **INSTALLERA OM**.
  6. Du måste starta om datorn för att slutföra processen.

Notera
Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

8.3. Varifrån kan jag hämta min Bitdefender-produkt?

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet du kan hämta till din dator från Bitdefender Central-plattformen.

Notera
Innan du kör satsen rekommenderar vi att du tar bort alla säkerhetslösningar som är installerade på ditt system. När du använder fler än en säkerhetslösning på samma dator blir systemet instabilt.

Installera Bitdefender från Bitdefender Central:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:
   - **Skydda den här enheten**

     Välj det här alternativet och spara installationsfilen.
   - **Skydda andra enheter**

     Välj det här alternativet och klicka därefter på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

     Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.
4. Kör den Bitdefender-produkt du har hämtat.

8.4. Hur ändrar jag språk på min Bitdefender-produkt?

Om du vill använda Bitdefender på ett annat språk måste du ominstallera produkten med rätt språk.

Använda Bitdefender på ett annat språk:

1. Ta bort Bitdefender genom att följa dessa steg:
   - I **Windows 7**:
     a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
     b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
     c. Klicka på **TA BORT** i det fönster som visas.
     d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
   - I **Windows 8 och Windows 8.1**:
     a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.

c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

d. Klicka på **TA BORT** i det fönster som visas.

e. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 10**:

a. Klicka på **Start**, därefter på Inställningar.

b. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.

c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

d. Klicka på **Avinstallera** igen för att bekräfta ditt val.

e. Klicka på **TA BORT** i det fönster som visas.

f. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

2. Ändra språk för Bitdefender Central:

a. Öppna Bitdefender Central.

b. Klicka på ikonen uppe till höger på skärmen.

c. Klicka på **Mitt konto** i reglagemenyn.

d. Gå till fliken **Profil**.

e. Välj ett språk från rullgardinsmenyn **Språk** och klicka sedan på **SPARA**.

3. Hämta installationsfilen:

a. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.

b. Välj ett av två möjliga alternativ:

- **Skydda den här enheten**

  Välj det här alternativet och spara installationsfilen.

- **Skydda andra enheter**

  Välj det här alternativet och klicka därefter på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och klicka på motsvarande hämtningsknapp.

4. Kör den Bitdefender-produkt du har hämtat.

Notera
Den här ominstallationsproceduren tar bort de anpassade inställningarna permanent.

8.5. Hur använder jag min Bitdefender-prenumeration efter en Windows-uppgradering?

Den här situationen uppstår när du uppgraderar operativsystemet och du vill fortsätta använda din Bitdefender-prenumeration.

Om du använder en tidigare Bitdefender-version kan du uppgradera utan kostnad till den senaste Bitdefender, enligt följande:

- Från en tidigare Bitdefender Antivirus-version till den senaste Bitdefender Antivirus som finns tillgänglig.
- Från en tidigare Bitdefender Internet Security-version till den senaste Bitdefender Internet Security som finns tillgänglig.
- Från en tidigare Bitdefender Total Security-version till den senaste Bitdefender Total Security som finns tillgänglig.

Det är två fall som kan dyka upp:

- Du har uppgraderat operativsystemet med Windows Update och märker att Bitdefender inte längre fungerar.

  I det här fallet måste du installera om produkten genom att följa de här stegen:

  - I **Windows 7**:

    1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
    2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
    3. Klicka på **INSTALLERA OM** i det fönster som visas.
    4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

       Öppna gränssnittet i din nyinstallerade Bitdefender-produkt för att komma åt funktionerna.

- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **INSTALLERA OM** i det fönster som visas.
  5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

     Öppna gränssnittet i din nyinstallerade Bitdefender-produkt för att komma åt funktionerna.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
  5. Klicka på **INSTALLERA OM** i det fönster som visas.
  6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

     Öppna gränssnittet i din nyinstallerade Bitdefender-produkt för att komma åt funktionerna.

> **Notera**
> Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

- Du ändrade systemet och vill fortsätta använda Bitdefender-skyddet. Därför måste du installera om produkten med den senaste versionen.

  Åtgärda den här situationen:

  1. Hämta installationsfilen:
     a. Öppna Bitdefender Central.
     b. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.

c. Välj ett av två möjliga alternativ:

- **Skydda den här enheten**

  Välj det här alternativet och spara installationsfilen.

- **Skydda andra enheter**

  Välj det här alternativet och klicka därefter på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

  Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.

2. Kör den Bitdefender-produkt du har hämtat.

Mer information om Bitdefender-installationsprocessen finns i *"Installera din Bitdefender-produkt"* (p. 5).

8.6. Hur uppgraderar jag till den senaste Bitdefender-versionen?

Från och med nu går det att uppgradera till den nyaste versionen utan att följa proceduren med manuell avinstallation och ominstallation. Mer exakt så levereras den nya produkten inklusive nya funktioner och stora produktförbättringar via produktuppdatering och om du redan har en aktiv Bitdefender-prenumeration aktiveras produkten automatiskt.

Om du använde 2018-versionen kan du uppgradera till den senaste versionen genom att följa de här stegen:

1. Klicka på **STARTA OM NU** i det meddelande du får med uppgraderingsinformationen. Om du missade det öppnar du fönstret Meddelanden, pekar på den senaste uppdateringen och klickar därefter på knappen **STARTA OM NU**. Vänta tills datorn startar om.

   Fönstret **Nyheter** med information om de förbättrade och nya funktionerna visas.

2. Klicka på länkarna **Läs mer** för att dirigeras om till vår särskilda sida med mer information och användbara artiklar.

3. Stäng fönstret **Nyheter** för att gå till gränssnittet för den installerade versionen.

Användare som vill uppgradera kostnadsfritt från Bitdefender 2016 eller en tidigare version till den senaste versionen av Bitdefender måste ta bort den aktuella versionen från Kontrollpanelen och därefter hämta den senaste installationsfilen från Bitdefenders webbplats på följande adress: https://www.bitdefender.com/Downloads/. Aktiveringen är endast möjlig med en giltig prenumeration.

9. PRENUMERATIONER

9.1. Hur aktiverar jag Bitdefender-prenumeration med en licensnyckel?

Om du har en giltig licensnyckel och vill använda den för att aktivera en prenumeration för Bitdefender Antivirus Plus finns det två möjliga fall:

- Du har uppgraderat från en tidigare version av Bitdefender till den nya:
  1. När uppgraderingen till Bitdefender Antivirus Plus är klar ombes du logga in till ditt Bitdefender-konto.
  2. Klicka på **Logga in** och skriv sedan e-postadressen och lösenordet till ditt Bitdefender-konto.
  3. Klicka **LOGGA IN** för att fortsätta.
  4. Ett meddelande som informerar dig om att en prenumeration har skapats visas på din kontoskärm. Den skapade prenumerationen är giltig för de återstående dagarna av din licensnyckel och för samma antal användare.

     Enheter som använder tidigare Bitdefender-versioner och som är registrerade med den licensnyckel du har konverterat till en prenumeration måste aktivera produkten med samma Bitdefender-konto.
- Bitdefender fanns inte installerad sedan tidigare på systemet:
  1. Så fort installationsprocessen är klar ombes du logga in på ditt Bitdefender-konto.
  2. Klicka på **Logga in** och skriv sedan e-postadressen och lösenordet till ditt Bitdefender-konto.
  3. Klicka på **LOGGA IN** för att fortsätta och sedan på knappen **SLUTFÖR** för att öppna gränssnittet för Bitdefender Antivirus Plus.
  4. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
  5. Klicka på **Aktivera nu**.

     Ett nytt fönster visas.
  6. Klicka på länken **Få din KOSTNADSFRIA uppgradering nu!**.

7. Skriv in din licensnyckel i motsvarande fält och klicka på **UPPGRADERA MIN PRODUKT**. En prenumeration med samma tillgänglighet och antal användare för din licensnyckel som är kopplad till ditt konto.

10. BITDEFENDER CENTRAL

10.1. Hur loggar jag in på Bitdefender Central med ett annat onlinekonto?

Du har nu skapat ett nytt Bitdefender-konto och du vill använda det från och med nu.

Använda ett annat konto:

1. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **Växla konto** i det övre högra hörnet av skärmen för att ändra kontot som är länkat till datorn.
3. Skriv in e-postadressen och lösenord till ditt konto i motsvarande fält och klicka sedan på **LOGGA IN**.

Notera
Bitdefender-produkten från din enhet ändras automatiskt enligt prenumerationen som är kopplad till det nya Bitdefender-konto.
Om det inte finns någon tillgänglig prenumeration kopplad till det nya Bitdefender-kontot eller om du vill överföra den från det tidigare kontot, kontaktar du Bitdefender för support sosom beskrivs i avsnitt *"Be om hjälp"* (p. 157).

10.2. Hur stänger jag av Bitdefender Central-hjälpmeddelanden?

För att hjälpa dig förstå vad varje alternativ i Bitdefender Central används för visas hjälpmeddelanden på kontrollpanelen.

Om du inte längre vill se den här typen av meddelanden:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.
3. Klicka på **Mitt konto** i reglagemenyn.
4. Välj fliken **Inställningar**.
5. Inaktivera alternativet **Slå på/av hjälpmeddelanden**.

10.3. Jag har glömt det lösenord jag ställde in för mitt Bitdefender-konto. Hur återställer jag det?

Det finns två möjligheter att ange ett nytt lösenord för ditt Bitdefender-konto:

- Från Bitdefender-gränssnittet:
  1. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. Klicka på **Byt konto** i det övre högra hörnet av skärmen.

     Ett nytt fönster visas.
  3. Klicka på **Glömt mitt lösenord**.
  4. Skriv e-postadressen du använde för att skapa Bitdefender-kontot och klicka sedan på **GLÖMT LÖSENORD**.
  5. Kolla din e-post och klicka på den tillhandahållna knappen.

     Fönstret Bitdefender ÅTERSTÄLL LÖSENORD visas.
  6. Skriv in din e-postadressen och det nya lösenordet i det motsvarande fältet. Lösenordet måste vara minst 8 tecken långt och innehålla siffror.
  7. Klicka på **ÅTERSTÄLL LÖSENORD**.
- Från din webbläsare:
  1. Gå till: https://central.bitdefender.com.
  2. Klicka på **Glömt mitt lösenord**.
  3. Skriv din e-postadress och klicka sedan på **GLÖMT LÖSENORD**.
  4. Kontrollera ditt e-postkonto och följ de angivna instruktionerna för att ställa in ett nytt lösenord för ditt Bitdefender-konto.

För att öppna ditt Bitdefender-konto från och med nu skriver du din e-postadress och det nya lösenordet du precis har ställt in.

10.4. Hur hanterar jag inloggningssessionerna kopplade till mitt Bitdefender-konto?

I ditt Bitdefender-konto har du möjlighet att visa de senaste inaktiva och aktiva inloggningssessionerna som körs på enheter som är kopplade till ditt konto. Dessutom kan du logga ut via fjärrstyrning genom att följa de här stegen:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.
3. Klicka på **Mitt konto** i reglagemenyn.
4. Välj fliken **Sessionshantering**.
5. I området **Aktiva sessioner** väljer du alternativet **LOGGA UT** bredvid den enhet du vill ska slutföra inloggningssessionen.

11. SKANNA MED BITDEFENDER

11.1. Hur skannar jag en fil eller en mapp?

Det enklaste sättet att skanna en fil eller en mapp är att högerklicka på det objekt du vill skanna, peka på Bitdefender och välja **Skanna med Bitdefender** från menyn.

Följ Antivirus-guiden för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer.

Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

Typiska situationer när du skulle använda denna skanningsmetod innefattar följande:

- Du misstänker att en specifik fil eller mapp är infekterad.
- När du hämtar filer från Internet som du tror kan vara skadliga.
- Skanna nätverksresurser innan du kopierar filer till din dator.

11.2. Hur skannar jag mitt system?

Utföra en fullständig skanning av systemet:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
3. Följ guiden för Systemskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer.

   Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem. Mer information finns på *"Guiden för Antivirusskanning" (p. 81)*.

11.3. Hur schemalägger jag en skanning?

Du kan ställa in Bitdefender-produkten att börja skanna viktiga systemplatser när du inte sitter vid datorn.

Schemalägga en skanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.

2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
3. Välj den skanningstyp du vill schemalägga, Fullständig systemskanning eller Snabbskanning, klicka sedan på **SKANNINGSALTERNATIV**.

   Alternativt kan du skapa en skanningstyp som passar dina behov genom att klicka på **NYTT ANPASSAT JOBB**.
4. Aktivera **Schema**-alternativet.

   Välj ett av motsvarande alternativ för att ställa in ett schema:

   - Vid systemstart
   - En gång
   - Ibland

I fönstret **Skanningsmål** kan du välja de platser du vill ska skannas. Det här alternativet är endast tillgängligt om du väljer att skapa en ny anpassad skanning.

11.4. Hur skapar jag ett anpassat skanningsjobb?

Om du vill skanna specifika platser på din dator eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb.

Gör enligt följande för att skapa ett anpassat skanningsjobb:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
3. Klicka på **NYTT ANPASSAT JOBB**. I fönstret **Bas** anger du ett namn för skanningen och väljer vilka platser som ska skannas.
4. Om du vill konfigurera skanningsalternativen i detalj väljer du fliken **Avancerat**.

   Du kan enkelt konfigurera skanningsalternativen genom att justera skanningsnivån. Dra skjutreglaget längs skalan för att ställa in önskad skanningsnivå.

   Du kan också välja att stänga ned datorn när skanningen är klar om inga hot hittas. Kom ihåg att detta blir standardbeteende varje gång du kör det här jobbet.
5. Klicka **OK** för att spara ändringarna och stänga fönstret.

6. Använd motsvarande omkopplare om du vill ange ett schema för skanningsjobbet.
7. Klicka på **STARTA SKANNING** och följ skanningsguiden för att slutföra skanningen. I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.
8. Om du vill kan du snabbt köra om en föregående anpassad skanning genom att klicka på motsvarande post i den tillgängliga listan.

11.5. Hur undantar jag en mapp från att skannas?

Bitdefender tillåter undantag av specifika filer, mappar eller filändelsen från skanning.

Undantag ska användas av användare som har avancerad datorkunskap och endast i följande situationer:

- Du har en stor mapp på ditt system där du förvarar filmer och musik.
- Du har ett stort arkiv på ditt system där du förvarar olika data.
- Du har en mapp där du installerar olika typer av programvara och appar i testsyften. Skanning av mappen kan innebära att du förlorar vissa data.

Lägg till en mapp i undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Klicka på fliken **Undantag**.
4. Klicka på menyn **Lista över filer och mappar undantagna från skanning** och sedan på **Lägg till**.
5. Klicka på **BLÄDDRA**, välj den mapp du vill ska undantas från skanning och välj sedan den typ av skanning den ska undantas ifrån.
6. Klicka på **Lägg till** för att spara ändringarna och stänga fönstret.

11.6. Vad ska man göra när Bitdefender visar att en ren fil är infekterad?

Det finns tillfällen då Bitdefender av misstag flaggar en legitim fil som ett hot (en falsk positiv). För att rätta till det här felet lägger du till filen till området för Bitdefender-undantag:

1. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.

      Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktivt. Du kan inaktivera realtidsskyddet i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart.
2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?" (p. 66)* hur du gör det.
3. Återskapa filen från karantänområdet:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Karantän**.
   c. Välj filen och klicka sedan på **ÅTERSTÄLL**.
4. Lägg till filen till undantagslistan. Se i *"Hur undantar jag en mapp från att skannas?" (p. 56)* hur du gör det.
5. Slå på Bitdefender realtids-antivirusskydd.
6. Kontakta våra supportmedarbetare så att vi kan ta bort upptäckten av hotinformationsuppdateringen. Se i *"Be om hjälp" (p. 157)* hur du gör det.

11.7. Hur kontrollerar jag vilka hot Bitdefender upptäckte?

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen.

Skanningsloggen innehåller detaljerad information om de loggade skanningsprocesserna, som skanningsalternativ, skanningsmål, vilka hot som hittats samt vilka åtgärder som vidtagits på dessa hot.

Du kan öppna skanningsloggen direkt från guiden för skanning när skanningen slutförts, genom att klicka **VISA LOGG**.

Kontrollera en skanningslogg eller en upptäckt infektion vid ett senare tillfälle:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.

2. På fliken **Alla** väljer du meddelandet som avser den senaste skanningen.

   Här hittar du alla hotskanningshändelser, inklusive hot upptäckta av pågående skanning, användarinitierade skanningar och statusändringar för automatiska skanningar.

3. I meddelandelistan kan du kontrollera vilka skanningar som har utförts på senaste tiden. Klicka på ett meddelande för att visa information om det.

4. Öppna en skanningslogg genom att klicka på **Visa logg**.

12. KONTROLL AV SEKRETESS

12.1. Hur vet jag att min onlinetransaktion är säker?

För att vara säker på att det du gör online förblir privat kan du använda webbläsaren som finns i Bitdefender för att skydda dina transaktioner och bankappar.

Bitdefender Safepay™ är en säker webbläsare designad för att skydda din kreditkortsinformation, kontonummer eller annan känslig information du kan ange på olika platser online.

För att se till att din onlineaktivitet är säker och privat:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **Safepay**-panelen klickar du på **Öppna Safepay**.
3. Klicka på knappen för att öppna det **virtuella tangentbordet**.

   Använd det **virtuella tangentbordet** när du skriver känslig information som lösenord.

12.2. Hur tar jag bort en fil permanent med Bitdefender?

Om du vill ta bort en fil permanent från ditt system måste du ta bort data fysiskt från din hårddisk.

Bitdefender File Shredder hjälper dig att snabbt strimla filer eller mappar från datorn med kontextmenyn i Windows genom att följa de här stegen:

1. Högerklicka på filen eller mappen som du vill ta bot permanent, peka på Bitdefender och välj **File Shredder**.
2. Klicka på **TA BORT PERMANENT** och bekräfta sedan att du vill fortsätta med processen.

   Vänta medan Bitdefender slutför filborttagning.
3. Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.

12.3. Hur kan jag manuellt återställa krypterade filer när återställningsprocessen misslyckas?

ifall krypterade filer inte kan återställas automatiskt kan du manuellt återställa dem genom att följa de här stegen:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** markerar du information avseende det senast upptäckta ransomwarebeteendet som upptäckts och klickar sedan på **Krypterade filer**.
3. Listan med krypterade filer visas.

   Klicka på **ÅTERSTÄLL FILER** för att fortsätta.
4. Ifall hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de avkrypterade filerna ska sparas. Klicka på **ÅTERSTÄLL PLATS** och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.

   Klicka på **SLUTFÖR** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas ifall de blir krypterade:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

13. ANVÄNDBAR INFORMATION

13.1. Hur testar jag min säkerhetslösning?

För att vara säker på att din Bitdefender-produkt körs som den ska rekommenderar vi att du använder Eicar-testet.

Med Eicar-testet kan du kontrollera din säkerhetslösning med en säker fil utvecklad för detta ändamål.

Testa din säkerhetslösning:

1. Hämta testet från den officiella hemsidan för EICAR-organisationen http://www.eicar.org/.
2. Klicka på fliken **Antimalware-testfil**.
3. Klicka på **Hämta** i menyn på vänster sida.
4. Från **Hämtningsområde som använder standardprotokollet http** klickar du på testfilen **eicar.com**.
5. Du informeras om att den sida du försöker öppna innehåller EICAR-Test-File (inte ett hot).

   Om du klickar på **Jag förstår riskerna, ta mig dit iallafall**, startar hämtningen testet och en Bitdefender-popup informerar dig om att ett hot upptäcktes.

   Klicka på **Mer information** för att hitta mer information om den här åtgärden.

Om du inte får någon Bitdefender-avisering rekommenderar vi att du kontaktar Bitdefender för support såsom beskrivs i avsnitt *"Be om hjälp"* (p. 157).

13.2. Hur tar jag bort Bitdefender?

Om du vill ta bort Bitdefender Antivirus Plus:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klicka på **TA BORT** i det fönster som visas.

4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 8 och Windows 8.1**:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **TA BORT** i det fönster som visas.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 10**:

1. Klicka på **Start**, därefter på Inställningar.
2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **TA BORT** i det fönster som visas.
6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

Notera
Den här ominstallationsproceduren tar bort de anpassade inställningarna permanent.

13.3. Hur tar jag bort Bitdefender VPN?

Proceduren för att ta bort Bitdefender VPN liknar den du använder för att ta bort andra program från datorn:

- I **Windows 7**:

1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Hitta **Bitdefender VPN** och välj **Avinstall**.

   Vänta tills avinstallationsprocessen är slutförd.

- I **Windows 8 och Windows 8.1**:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender VPN** och välj **Avinstall**.

   Vänta tills avinstallationsprocessen är slutförd.

- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender VPN** och välj **Avinstall**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.

     Vänta tills avinstallationsprocessen är slutförd.

13.4. Hur stänger jag automatiskt ned datorn när skanningen är klar?

Bitdefender erbjuder flera skanningsjobb som du kan använda för att vara säker på att systemet inte är infekterat av hot. Att skanna hela datorn kan ta längre tid att slutföra beroende på systemet hårdvaru- och programvarukonfiguration.

Av det skälet tillåter Bitdefender att du konfigurerar din produkt så att den stänger systemet så fort skanningen är klar.

Fundera på det här exemplet: du har avslutat dit arbete vid datorn och vill gå och lägga dig. Du vill att Bitdefender ska kontrollera hela ditt system.

Så här konfigurerar du Bitdefender för att stänga ned systemet när skanningen är klar:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
3. I fönstret **Hantera skanningsjobb** klickar du på **NYTT ANPASSAT JOBB** för att ange ett namn för skanningen och välja vilka platser som ska skannas.

4. Om du vill konfigurera skanningsalternativen i detalj väljer du fliken **Avancerat**.
5. Du kan välja att stänga ned datorn när skanningen är klar om inga hot hittas.
6. Klicka **OK** för att spara ändringarna och stänga fönstret.
7. Klicka på **STARTA SKANNINGEN** för att skanna ditt system.

Om inga hot hittas stängs datorn ned.

Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem. Mer information finns på *"Guiden för Antivirusskanning"* (p. 81).

13.5. Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?

Om din dator ansluts till Internet via en proxyserver måste du konfigurera Bitdefender med proxyinställningarna. Normalt upptäcker och importerar Bitdefender automatiskt proxyinställningarna från ditt system.

> **Viktigt**
> Internet-anslutningar från hemmet använder vanligtvis inte en proxyserver. Som en tumregel ska du kontrollera och konfigurera proxyinställningarna för Bitdefender-programmet när uppdateringarna inte fungerar. Om Bitdefender kan uppdatera är den korrekt konfigurerad för att ansluta till Internet.

Hantera proxyinställningar:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till **Avancerat** fliken.
3. Aktivera **Proxy-server**.
4. Klicka på **Proxy-ändring**.
5. Det finns två alternativ för att ange proxyinställningarna:
   - **Importera proxyinställningar från standardwebbläsare** - proxyinställningar för aktuell användare, extraherade från standardwebbläsaren. Om proxyservern kräver ett användarnamn och lösenord måste du skriva in dem i motsvarande fält.

> **Notera**
> Bitdefender kan importera proxy-inställningar från de mest populära webbläsarna, däribland de senaste versionerna av Microsoft Edge, Internet Explorer, Mozilla Firefox och Google Chrome.

- **Anpassade proxy-inställningar** - proxy-inställningar som du kan konfigurera själv. Följande inställningar måste specificeras:
  - **Adress** - skriv in proxyserverns IP.
  - **Port** - skriv in vilken port som Bitdefender använder för att ansluta till proxyservern.
  - **Användarnamn** - skriv in ett användarnamn som känns igen av proxy.
  - **Lösenord** - skriv in det giltiga lösenordet för den tidigare valde användaren.

6. Klicka **OK** för att spara ändringarna och stänga fönstret.

Bitdefender använder tillgängliga proxy-inställningar tills den kan ansluta till Internet.

13.6. Använder jag en 32-bitars eller en 64-bitars version av Windows?

Ta reda på om du har ett 32-bitars eller ett 64-bitars operativsystem:

- I **Windows 7**:
  1. Klicka **Starta**.
  2. Lokalisera **Dator** i **Start** menyn.
  3. Högerklicka **Dator** och välj **Egenskaper**.
  4. Se under **System** för att kontrollera informationen om ditt system.
- I **Windows 8**:
  1. Från Windows Start-skärm, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt i startskärmen) och högerklicka sedan på dess ikon.

     I **Windows 8.1** letar du upp **Den här datorn**.
  2. Välj**Egenskaper** i menyn längst ned.
  3. Titta i området System för att se din systemtyp.
- I **Windows 10**:

1. Skriv "System" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon.
2. Titta i System-området för att hitta information om din systemtyp.

13.7. Hur visar jag dolda objekt i Windows?

Dessa steg är användbara i de fall där du arbetar med en situation med hot och behöver hitta och radera den infekterade filen, som kan vara dold.

Följ dessa steg för att visa dolda objekt i Windows:

1. Klicka på **Start** och gå sedan till **Kontrollpanelen**.

   I **Windows 8 och Windows 8.1**: Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Välj **Mappalternativ**.
3. Gå till fliken **Visa**
4. Välj **Visa dolda filer och mappar**.
5. Avmarkera **Dölj tillägg för kända filtyper**.
6. Rensa **Dölj skyddade operativsystemfiler**.
7. Klicka på **Verkställ** och sedan på **OK**.

I **Windows 10**:

1. Skriv "Visa dolda filer och mappar" i sökrutan från aktivitetsfältet och klicka på ikonen.
2. Välj **Visa dolda filer, mappar och enheter**.
3. Avmarkera **Dölj tillägg för kända filtyper**.
4. Rensa **Dölj skyddade operativsystemfiler**.
5. Klicka på **Verkställ** och sedan på **OK**.

13.8. Hur tar jag bort andra säkerhetslösningar?

Den huvudsakliga orsaken för att använda en säkerhetslösning är för att tillhandahålla skydd och säkerhet för dina data. Men vad händer om man har fler än en säkerhetsprodukt på samma system?

När du använder fler än en säkerhetslösning på samma dator blir systemet instabilt. Bitdefender Antivirus Plus installeraren upptäcker automatiskt andra säkerhetsprogram och ger dig möjlighet att avinstallera dessa.

Om du inte tog bort de andra säkerhetslösningarna under installationen:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Vänta ett ögonblick tills dess listan med installerade program visas.
  3. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
  4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Vänta ett ögonblick tills dess listan med installerade program visas.
  4. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
  5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
  5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

Om du misslyckas med att ta bort den andra säkerhetslösningen från ditt system, hämta avinstalleringsverktyget från försäljarens webbsida eller kontakta dem direkt för att få riktlinjer för avinstallering.

13.9. Hur startar jag om i Felsäkert läge?

Felsäkert läge ät ett diagnosticerande driftläge som vanligtvis används för att söka efter problem som påverkar den vanliga driften av Windows. Den typen av problem sträcker sig från konflikter mellan enheter, till hot som förhindrar att Windows startas normalt. I felsäkert läge fungerar endast ett fåtal appar och Windows laddar bara de grundläggande drivrutinerna samt ett minimum av operativsystemets komponenter. Det är därför de flesta hot är inaktiva och enkelt kan tas bort när du kör Windows i felsäkert läge.

För att starta Windows i felsäkert läge:

- I **Windows 7**:
  1. Starta om datorn.
  2. Tryck tangenten **F8** flera gånger innan Windows startar för att nå boot-menyn.
  3. Välj **Felsäkert läge** i boot-menyn eller **Felsäkert läge med nätverk** om du vill ha Internet-åtkomst.
  4. Tryck **Enter** och vänta tills Windows laddas i Felsäkert läge.
  5. Den här processen avslutas med ett bekräftelsemeddelande. Klicka på **OK** för att bekräfta.
  6. För att starta Windows normalt, bara starta om systemet.
- I **Windows 8, Windows 8.1 och Windows 10**:
  1. Starta **Systemkonfiguration** i Windows genom att samtidigt trycka på knapparna **Windows + R** på tangentbordet.
  2. Skriv **msconfig** i dialogrutan **Öppna**, klicka därefter **OK**.
  3. Välj fliken **Boot**.
  4. I området **Startalternativ** markerar du kryssrutan **Säker start**.
  5. Klicka på **Nätverk** och därefter **OK**.
  6. Klicka **OK** i fönstret **Systemkonfiguration** som informerar dig om att systemet måste startas om för att kunna göra de ändringar du har ställt in.

     Ditt system startar om i felsäkert läge med nätverksanslutning.

För att starta om i normalläge ställer du tillbaka inställningarna genom att starta **Systemdrift** igen och avmarkera kryssrutan **Säker start**. Klicka på **OK** och sedan på **Starta om**. Vänta tills de nya inställningarna tillämpas.

HANTERA DIN SÄKERHET

14. ANTIVIRUSSKYDD

Bitdefender skyddar din dator från alla typer av hot (skadlig kod, trojaner, spionprogram, spökprogram osv). Skyddet som Bitdefender erbjuder delas in i två kategorier:

- Skanning vid åtkomst - förhindrar nya hot från att komma in i systemet. Bitdefender kan till exempel skanna ett Word-dokument efter kända hot när du öppnar det och ett e-postmeddelande när du får det.

  Skanning vid åtkomst säkerställer realtidsskydd mot hot och är en viktig komponent i alla datorsäkerhetsprogram.

  Viktigt
  Förhindra hot från att infektera din dator genom att ha **skanning vid åtkomst** aktiverat.

- På begäran-skanning - tillåter upptäckt och borttagning av hot som redan finns i systemet. Detta är en klassisk skanning som startats av användaren - du bestämmer vilken enhet, mapp eller fil som Bitdefender ska skanna, och Bitdefender skannar den på begäran.

Bitdefender skannar automatiskt alla borttagbara medier som är anslutna till datorn för att se till att den går att använda säkert. Mer information finns på *"Automatisk skanning av borttagbara medier"* (p. 85).

Avancerade användare kan konfigurera undantag från skanning om de inte vill att särskilda filer eller filtyper ska skannas. Mer information finns på *"Konfigurera skanningsundantag"* (p. 87).

När det upptäcker ett hot kommer Bitdefender automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering. Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Mer information finns på *"Hantera filer i karantän"* (p. 89).

Om din dator har infekterats med virus finns mer information i *"Ta bort hot från ditt system"* (p. 147). För att hjälpa dig rensa datorn från hot som inte kan tas bort inifrån Windows-operativsystemet, tillhandahåller Bitdefender *"Bitdefender Räddningsläge (räddningsmiljö i Windows 10)"* (p. 147). Det här en betrodd miljö, särskilt utvecklad för att ta bort hot, silket gör det möjligt för dig att starta din dator oberoende av Windows. När datorn körs i

räddningsläger (räddningsmiljö i Windows 10) är Windows-hot inaktiva, vilket gör det enkelt att ta bort dem.

14.1. Skanning vid åtkomst (realtidsskydd)

Bitdefender ger realtidsskydd mot flera olika hot genom att skanna alla öppnade filer och e-postmeddelanden.

14.1.1. Stänga av eller slå på realtidsskydd

Stänga av eller slå på realtidsskydd mot hot:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** stänger du av eller slår på **Bitdefender Shield**.
4. Om du vill inaktivera realtidsskydd visas ett varningsfönster. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktivt. Du kan inaktivera realtidsskyddet i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart. Realtidsskyddet slås automatiskt på när den valda tiden löper ut.

Varning
Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat är du inte skyddad mot hot.

14.1.2. Konfigurerar avancerade inställningar för realtidsskydd

Avancerade användare kan vilja dra fördel av de skanningsinställningar som Bitdefender erbjuder. Du kan konfigurera inställningarna för realtidsskyddet detaljerat genom att skapa en anpassad skyddsnivå.

Konfigurera avancerade inställningar för realtidsskydd:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** klickar du på rullgardinsmenyn **Visa avancerade inställningar**.

Ett panelfönster visas.

4. Bläddra upp och ned i fönstret för att konfigurera de skanningsinställningarna efter behov.

Information om skanningsalternativ

Du kan finna denna information användbar:

- **Skanna endast program.** Du kan konfigurera Bitdefender till att skanna endast öppnade appar.
- **Skanna potentiellt oönskade program.** Välj det här alternativet för att skanna efter oönskade program. En eventuellt oönskad applikation (PUA) eller eventuellt oönskat program (PUP) är en programvara som oftast ingår i freewareprogram och som visar popup-rutor eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem ändrar hemsidan eller sökmotorn, andra kär flera processer i bakgrunden som gör datorn långsammare eller visar många annonser. De här programmen kan installeras utan ditt samtycke (kallas även adware) eller ingår som standard i expressinstallationspaketet (annonsstöd).
- **Skanna nätverksresurser.** För att säkert komma åt ett fjärrnätverk från datorn rekommenderar vi att du har alternativet Skanna nätverksdelningar aktiverat.
- **Skanna inuti komprimerade filer.** Att skanna inne i arkiv är en långsam och resursintensiv process och rekommenderas därför inte för realtidsskydd. Arkiv som innehåller infekterade filer är inte ett direkt hot mot ditt systems säkerhet. Hotet kan endast påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att realtidsskyddet är aktiverat.

  Om du bestämmer dig för att använda det här alternativet aktiverar du det och drar sedan reglaget ängs skalan för att ange en maximalt accepterad storleksgräns (i MB) av arkiv som som ska skannas vid åtkomst.
- **Skanna e-postmeddelanden.** För att förhindra att hot hämtas till din dator, skannar Bitdefender automatiskt inkommande och utgående e-postmeddelanden.

  Även om det inte rekommenderas kan du inaktivera hotskanning för att öka systemprestandan. Om du inaktiverar de motsvarande skanningsalternativen kommer de e-postmeddelanden och filer som tas emot inte att skannas och tillåter därmed att infekterade filer sparas på

din dator. Det här är inte ett stort hot eftersom realtidsskyddet kommer att blockera hotet när de infekterade filerna används (Öppnas, flyttas,kopieras eller körs).

- **Skanna bootsektorer.** Du kan konfigurera Bitdefender att skanna startsektorerna på hårddisken. Den här sektorn på hårddisken innehåller den datorkod som behövs för att starta bootprocessen. När ett hot infekterar startsektorn kan enheten bli oåtkomlig och du kanske inte kan starta systemet och komma åt dina data.
- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och ändrade filer, kan du kraftigt förbättra systemets responsivitet med en minimal förlust av säkerhet.
- **Skanna efter tangentloggning.** Välj det här alternativet för att skanna systemet efter keyloggerappar. Keyloggers spelar in det du skriver på tangetbordet och skickar rapporter över Internet till en person med ont uppsåt (hackare). Hackaren kan utvinna känslig information, såsom bankkontonummer och lösenord ur den stulna uppgifterna, och använda detta för att skaffa sig personliga fördelar.
- **Skanna vid systemstart.** Välj alternativet **Tidig startskanning** för att skanna systemet vid start så fort alla kritiska tjänster har laddats. Syftet med den här funktionen är att förbättra hotupptäckt vid systemstart och starttid för systemet.

Åtgärder som vidtas vid upptäckta hot

Du kan konfigurera de åtgärder som vidtas av realtidsskyddet genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** klickar du på rullgardinsmenyn **Visa avancerade inställningar**.

   Ett panelfönster visas.
4. Bläddra nedåt i fönstret till du ser alternativet **Hotåtgärder**.
5. Konfigurera skanningsinställningarna efter behov.

Följande åtgärder kan vidtas av realtidsskyddet i Bitdefender:

Vidta rätt åtgärder

Bitdefender vidtar rekommenderade åtgärder beroende på typ av upptäckt fil:

- **Smittade filer.** Filer som upptäcks som infekterade matchar en del av den hotinformation som hittas i Bitdefenders hotinformationsdatabas. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering.

  Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på *"Hantera filer i karantän"* (p. 89).

  > **Viktigt**
  > För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

- **Misstänkta filer.** Filer har upptäckts som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen desinfektionsrutin finns tillgänglig. De flyttas till karantän för att förhindra en eventuell infektion.

  Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en hotinformationsuppdatering för att tillåta borttagning av hotet.

- **Arkiv som innehåller infekterade filer.**
  - Arkiv som endast innehåller infekterade filer tas bort automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer försöker Bitdefender att ta bort de infekterade filerna förutsatt att det går att rekonstruera arkivet med rena filer. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Flytta filer till karantän

Flyttar upptäckta filer till karantän. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på *"Hantera filer i karantän"* (p. 89).

Neka åtkomst
Om en infekterad fil hittas nekas åtkomst till den.

14.1.3. Återställa standardinställningarna

Standardinställningarna för realtidsskyddet försäkrar ett bra skydd mot hot, med liten påverkan på systemets prestanda.

För att återställa standardinställningarna för realtidsskyddet:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** klickar du på rullgardinsmenyn **Visa avancerade inställningar**.

   Ett panelfönster visas.
4. Bläddra nedåt i fönstret till du ser alternativet **Återställ inställningar**. Välj det här alternativet för att återställa antivirusinställningarna till standard.

14.2. Skanning på begäran

Huvudmålet för Bitdefender är att hålla din dator ren från hot. Detta görs genom att hålla nya hot borta från din dator och genom att skanna dina e-postmeddelanden och alla nya filer som hämtas eller kopieras till ditt system.

Det finns en risk för att ett hot redan finns i systemet innan du ens installerar Bitdefender. Därför är det en god idé att skanna din dator för befintliga hot efter att du installerat Bitdefender. Och det är definitivt en bra idé att regelbundet skanna datorn för hot.

På begäran-skanning baseras på skanningsuppgifter. Skanningsuppgifter specificerar skanningsalternativen och de objekt som ska skannas. Du kan när du vill skanna datorn genom att köra standarduppgifterna för dina egna skanningsuppgifter (användardefinierade uppgifter). Om du vill skanna specifika platser på din dator eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb.

14.2.1. Skanna en fil eller mapp för hot

Du borde alltid skanna filer och mappar när du misstänker att de kan vara infekterade. Högerklicka på de filer eller mappar du vill skanna, peka på

Bitdefender och välj **Skanna med Bitdefender**. Guiden för antivirusskanning kommer att visas och leda dig genom skanningsprocessen. I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.

14.2.2. Köra en snabbskanning

Snabbskanning använder skanning i "molnet" för att upptäcka hot som körs på ditt system. Att köra en snabbskanning tar vanligtvis under en minut och använder en bråkdel av de systemresurser som krävs vid en vanlig antivirusskanning.

Köra en snabbskanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Snabbskanning**.
3. Följ guiden för Antivirusskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

14.2.3. Kör en systemskanning

Systemskanningen skannar hela datorn efter alla typer av hot som är riskabla för säkerheten, som skadlig kod, spionprogramvara, adware, rootkits och annat.

> **Notera**
> Eftersom **Systemskanning** utför en noggrann skanning av hela systemet kan skanningen ta en stund. Därför rekommenderas du att köra det här jobbet när du inte använder din dator.

Innan du kör en skanning rekommenderas följande:

- Se till att Bitdefender är uppdaterad med sin hotinformationsdatabas. Om du skannar datorn med en utdaterad hotinformationsdatabas kan Bitdefender förhindras från att upptäcka nya hot som hittats sedan den senaste uppdateringen. Mer information finns på *"Se till att Bitdefender är uppdaterad"* (p. 36).
- Stäng ned alla öppna program.

Om du vill skanna specifika platser på din dator eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb. Mer information finns på *"Konfigurera en anpassad skanning"* (p. 78).

Köra en systemskanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
3. Första gången du kör en systemskanning presenteras du för funktionen. Klicka **JAG FATTAR** för att fortsätta.
4. Följ guiden för Antivirusskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

14.2.4. Konfigurera en anpassad skanning

Konfigurera en anpassad skanning i detalj och sedan köra den:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
3. Klicka på **NYTT ANPASSAT JOBB**. I fönstret **Bas** anger du ett namn för skanningen och väljer vilka platser som ska skannas.
4. Om du vill konfigurera skanningsalternativen i detalj väljer du fliken **Avancerat**. Ett nytt fönster visas. Följ dessa steg:
   a. Du kan enkelt konfigurera skanningsalternativen genom att justera skanningsnivån. Dra skjutreglaget längs skalan för att ställa in önskad skanningsnivå. Använd beskrivningen på höger sida av skalan för att välja den skanningsnivå som bättre passar dina behov.

      Avancerade användare kan vilja dra fördel av de skanningsinställningar som Bitdefender erbjuder. För att detaljerat konfigurera alternativen för skanning klickar du på **Anpassa**. Du hittar information om dem i slutet av det här avsnittet.

   b. Du kan även konfigurera de här allmänna alternativen:

      - **Kör uppgiften med låg prioritet .** Sänker prioriteten för skanningsprocessen. Du kommer att tillåta andra program att köras snabbare och minska tiden som behövs för att skanningsprocessen ska slutföras.

- **Minimera guiden för skanning till systemfältet .** Minimerar skanningsfönstret till systemfältet. Dubbelklicka på Bitdefender-ikonen för att öppna den.
- Välj vilken åtgärd som ska utföras om inga hot upptäcks.

c. Klicka **OK** för att spara ändringarna och stänga fönstret.

5. Om du vill ange ett schema för ditt skanningsjobb använder du **Schema**-omkopplaren i fönstret **Grundläggande**. Välj ett av motsvarande alternativ för att ställa in ett schema:
   - Vid systemstart
   - En gång
   - Ibland
6. Klicka på **STARTA SKANNING** och följ Antivirusskanningsguiden för att slutföra skanningen. Beroende på de platser som ska skannas kan skanningen ta en stund. I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.
7. Om du vill kan du snabbt köra om en föregående anpassad skanning genom att klicka på motsvarande post i den tillgängliga listan.

Information om skanningsalternativ

Du kan finna denna information användbar:

- Om du inte är bekant med några av dessa termer, kontrollera dem i ordlistan. Du kan också hitta användbar information genom att söka på Internet.
- **Skanna filer.** Du kan konfigurera Bitdefender att endast skanna alla typer av filer eller appar (programfiler). Att skanna alla filer tillhandahåller det bästa skyddet, medan skanning av appar endast kan användas för att utföra en snabbare skanning.

  Appar (eller programfiler) är mycket mer sårbara för attacker från hot än andra typer av filer. Denna kategori inkluderar följande filändelser: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq;

mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Skanningsalternativ för arkiv.** Arkiv som innehåller infekterade filer är inte ett direkt hot mot ditt systems säkerhet. Hotet kan endast påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att realtidsskyddet är aktiverat. Det rekommenderas dock att använda det här alternativet för att upptäcka och ta bort alla potentiella hot, även om det inte är ett direkt hot.

  Notera
  Skanning av arkiverade filer ökar den totala skanningstiden och kräver högre systemresurser.

- **Skanna bootsektorer.** Du kan konfigurera Bitdefender att skanna startsektorerna på hårddisken. Den här sektorn på hårddisken innehåller den datorkod som behövs för att starta bootprocessen. När ett hot infekterar startsektorn kan enheten bli oåtkomlig och du kanske inte kan starta systemet och komma åt dina data.
- **Skanna minne.** Välj det här alternativet för att skanna program som körs i systemets minne.
- **Skanna register.** Välj det här alternativet för att skanna registernycklar. Windows Registry är en databas som lagrar konfigurationsinställningar och alternativ för systemkomponenter i Windows operativsystem, samt för installerade appar.
- **Skanna cookies.** Välj det här alternativet för att skanna de cookies som din webbläsare har lagrat på datorn.
- **Skanna endast nya och/eller ändrade filer.** Genom att endast skanna nya och ändrade filer, kan du kraftigt förbättra systemets responsivitet med en minimal förlust av säkerhet.
- **Ignorera kommersiella tangentloggare.** Välj det här alternativet om du har installerat och använder kommersiella keyloggerprogramvara på datorn.

Kommersiella keyloggers är legitima datorövervakningsprogram vars mest grundläggande funktion är att registrera allt som skrivs på tangentbordet.

- **Skanna efter spökprogram.** Välj det här alternativet för att skanna efter rootkits och objekt dolda i sådan programvara.
- **Skanna potentiellt oönskade program.** Välj det här alternativet för att skanna efter oönskade program. En eventuellt oönskad applikation (PUA) eller eventuellt oönskat program (PUP) är en programvara som oftast ingår i freewareprogram och som visar popup-rutor eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem ändrar hemsidan eller sökmotorn, andra kär flera processer i bakgrunden som gör datorn långsammare eller visar många annonser. De här programmen kan installeras utan ditt samtycke (kallas även adware) eller ingår som standard i expressinstallationspaketet (annonsstöd).

14.2.5. Guiden för Antivirusskanning

När du än inleder en på begäranskanning (till exempel högerklickar på en mapp, pekar på Bitdefender och väljer **Skanna med Bitdefender**), kommer Bitdefenders guide för antivirusskanning att visas. Följ guiden för att slutföra skanningsprocessen.

Notera

Om guiden för skanning inte visas kan skanningen vara konfigurerad att köras tyst i bakgrunden. Sök efter ikonen för skanningsframgång i systemfältet. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsframgången.

Steg 1 - Utför skanning

Bitdefender kommer att börja skanna de valda objekten. Du kan se realtidsinformation om skanningsstatus och statistik (däribland förfluten tid, en uppskattning av återstående tid och antalet upptäckta hot).

Vänta medan Bitdefender slutför skanningen. Skanningsprocessen kan ta en stund beroende på hur komplicerad den är.

Stoppar eller pausar skanningen. Du kan stoppa skanningen när du vill genom att klicka på **STOPP**. Du kommer att gå direkt till att se guidens sista steg. För att tillfälligt stoppa skanningsprocessen klickar du bara på **Pause**. Du måste klicka på **FORTSÄTT** för att återuppta skanningen.

Lösenordsskyddade arkiv. När ett lösenordsskyddat arkiv upptäcks, beroende på skanningsinställningarna, kan du bli ombedd att skriva in lösenordet. Lösenordsskyddade arkiv kan inte skannas om du inte skriver in lösenordet. Följande alternativ är tillgängliga:

- **Lösenord.** Om du vill att Bitdefender ska skanna arkivet, välj detta alternativ och skriv in lösenordet. Om du inte kan lösenordet, välj ett av de andra alternativen.
- **Fråga inte efter lösenordet och hoppa över denna post för skanning.** Välj det här alternativet för att hoppa över skanning av det här arkivet.
- **Hoppa över alla lösenordsskyddade poster utan att skanna dem.** Välj detta alternativ om du ej vill störas om lösenordsskyddade arkiv. Bitdefender kommer inte att kunna skanna dem, men ett register kommer att finnas i skanningsloggen.

Välj önskat alternativ och klicka på **OK** för att fortsätta skanningen.

Steg 2 - Välj åtgärder

I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.

Notera

När du kör en snabbskanning eller en systemskanning vidtar Bitdefender automatiskt rekommenderade åtgärder på upptäckta filer under skanningen. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

De infekterade objekten visas i grupper baserade på vilken typ av hot de är infekterade med. Klicka länken som motsvarar ett hot för att få mer information om de infekterade objekten.

Du kan välja en omfattande åtgärd som ska tas på alla problem, eller så kan du välja separata åtgärder för varje problemgrupp. Ett eller flera av följande alternativ kan visas i menyn:

Vidta rätt åtgärder

Bitdefender vidtar rekommenderade åtgärder beroende på typ av upptäckt fil:

- **Smittade filer.** Filer som upptäcks som infekterade matchar en del av den hotinformation som hittas i Bitdefenders hotinformationsdatabas.

Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering.

Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på *"Hantera filer i karantän"* (p. 89).

Viktigt
För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

- **Misstänkta filer.** Filer har upptäckts som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen desinfektionsrutin finns tillgänglig. De flyttas till karantän för att förhindra en eventuell infektion.

  Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en informationsuppdatering för att tillåta borttagning av hotet.

- **Arkiv som innehåller infekterade filer.**
  - Arkiv som endast innehåller infekterade filer tas bort automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer försöker Bitdefender att ta bort de infekterade filerna förutsatt att det går att rekonstruera arkivet med rena filer. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Radera

Tar bort upptäckta filer från enheten.

Om infekterade filer lagras i ett arkiv tillsammans med rena filer försöker Bitdefender ta bort de infekterade filerna och bygga om arkivet med de rena filerna. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Vidta ingen åtgärd.

Ingen åtgärd kommer att tas på de upptäckta filerna. När skanningen är slutförd kan du öppna skanningsloggen för att se information om dessa filer.

Klicka **Fortsätt** för att tillämpa den valda åtgärden.

Steg 3 - Sammanfattning

När Bitdefender är färdig med att lösa problemen kommer skanningsresultaten att visas i ett nytt fönster. Om du vill få omfattande information om skanningsprocessen, klicka **VISA LOGG** för att visa skanningsloggen. Loggen tillhandahålls i .xml-format och kan sparas lokalt genom att du klickar på knappen **Spara logg** och därefter väljer en plats.

Viktigt

I de flesta fall lyckas Bitdefender desinficera de infekterade filer den upptäcker, annars isolerar den infektionen. Dock finns det problem som inte kan lösas automatiskt. Om det krävs startar du om systemet för att slutföra rensningsprocessen. Mer information och instruktioner om hur du tar bort ett hot manuellt finns i *"Ta bort hot från ditt system"* (p. 147).

14.2.6. Kontrollera skanningsloggar

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen i fönstret Antivirus. Skanningsloggen innehåller detaljerad information om de loggade skanningsprocesserna, som skanningsalternativ, skanningsmål, vilka hot som hittats samt vilka åtgärder som vidtagits på dessa hot.

Du kan öppna skanningsloggen direkt från guiden för skanning när skanningen slutförts, genom att klicka **VISA LOGG**.

Kontrollera en skanningslogg eller en upptäckt infektion vid ett senare tillfälle:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste skanningen.

   Här hittar du alla hotskanningshändelser, inklusive hot upptäckta av pågående skanning, användarinitierade skanningar och statusändringar för automatiska skanningar.

3. I meddelandelistan kan du kontrollera vilka skanningar som har utförts på senaste tiden. Klicka på ett meddelande för att visa information om det.
4. Öppna skanningsloggen genom att klicka på **Visa logg**.

14.3. Automatisk skanning av borttagbara medier

Bitdefender upptäcker automatiskt när du ansluter en flyttbar lagringsenhet till din dator och skannar den i bakgrunden när alternativet Autoskanning är aktiverad. Detta rekommenderas för att förhindra hot från att infektera datorn.

Upptäckta enheter placeras i en av dessa kategorier:

- CDs/DVDs
- Flash-enheter, som flash-stickor och externa hårddiskar
- kartlagda (fjärr) nätverksenheter

Du kan konfigurera automatisk skanning separat för varje kategori lagringsenheter. Automatisk skanning av mappade nätverksenheter är inaktiverat som standard.

14.3.1. Hur fungerar det?

När Bitdefender upptäcker en borttagbar lagringsenhet börjar den skanna efter hot (förutsatt att automatisk skanning är aktiverat för den typen av enhet). Du meddelas via ett popup-fönster att en ny enhet har upptäckts och att den skannas.

En Bitdefender-skanningsikon visas i systemfältet. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsframgången.

När skanningen är klar visas skanningsresultatfönstret för att informera dig om du säkert kan öppna filer på det borttagbara mediet.

I de flesta fall tar Bitdefender automatiskt bort upptäckta hot eller isolerar infekterade filer i karantän. Om olösta hot återstår efter skanningen uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

Notera
Tänk på att inga åtgärder kan vidtas för infekterade eller misstänkta filer som hittas på CD-/DVD-skivor. På samma sätt kan inga åtgärder vidtas för infekterade eller misstänkta filer som upptäcks på mappade nätverksenheter om du inte har rätt behörigheter.

Den här informationen kan vara användbar för dig:

- Var försiktig när du använder en hotinfekterad CD/DVD, eftersom hotet inte kan tas bort från disken (mediet är skrivskyddat). Se till att realtidsskydd är aktiverat för att förhindra hot från att spridas till ditt system. Det är bästa praxis att kopiera alla värdefulla data från skivan till ditt system och sedan kasta bort skivan.
- I vissa fall kan inte Bitdefender ta bort hot från specifika filer på grund av juridiska eller tekniska begränsningar. Ett sådant exempel är filer som arkiverats med en egen teknik (det är för att arkivet inte kan rekonstrueras korrekt).

  Information om hur du hanterar hot finns i "*Ta bort hot från ditt system*" (p. 147).

14.3.2. Hantera skanning av borttagbara medier

Hantera automatisk skanning av borttagbara medier:

För bästa skydd rekommenderar vi att alternativet **Autoskanning** är markerat för alla typer av borttagbara lagringsenheter.

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Diskar och enheter**.

Skanningsalternativen är förkonfigurerade för bästa upptäcktsresultat. Om smittade filer hittas försöker Bitdefender desinfektera dem (ta bort den skadliga koden) eller flytta dem till karantän. Om båda åtgärderna misslyckas, kommer guiden för Antivirus-skanning att låta dig välja andra åtgärder att ta till mot infekterade filer. Skanningsalternativen är standard och du kan inte ändra dem.

14.4. Skanna värdens fil

Värdens filer kommer som standard med installationen av operativsystemet och används för att mappa värdnamn till IP-adresser varje gång du öppnar en ny webbsida, ansluter till en FTP eller till andra Internet-servrar. Det är vanlig textfil och skadliga program kan ändra den. Avancerade användare vet hur de ska använda den för att blockera irriterande annonser, banners, tredjepartscookies eller kapare.

Konfigurera skanning av värdfil:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till **Avancerat** fliken.
3. Aktivera eller inaktivera **Skanna värdfil**.

14.5. Konfigurera skanningsundantag

Bitdefender tillåter undantag av specifika filer, mappar eller filändelsen från skanning. Den här funktionen är avsedd för att undvika att du störs i ditt arbete och den kan också bidra till att förbättra systemprestanda. Undantag ska användas av användare som har avancerad datorkunskap eller som annars följer rekommendationerna från en Bitdefender-medarbetare.

Du kan konfigurera undantag att gälla endast för vid åtkomst- eller på begäran-skanning, eller för båda. De objekt som exkluderas från en på begäran-skanning kommer inte att skannas även om de öppnas av dig eller ett program.

Notera

Undantag kommer INTE att tillämpas på system- och kontextskanning. Systemskanning är en på begäran-skanning som ger dig möjlighet att analysera hela systemet för skadliga hot som kan riskera säkerheten för dina data. Innehållsskanning är en typ av på begäran-skanning: du högerklickar filen eller mappen du vill söka igenom och väljer **Skanna med Bitdefender**.

14.5.1. Undanta filer och mappar från skanning

Undanta specifika filer och mappar från skanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Undantag**.
4. Klicka på rullgardinsmenyn **Lista över filer och mappar undantagna från skanning**. I det fönster som visas kan du hantera de filer och mappar som är undantagna från skanning.
5. Lägg till undantag genom att följa dessa steg:

   a. Klicka **Lägg till**.

b. Klicka **BLÄDDRA**, välj den fil eller mapp som du vill ska undantas från skanningen och klicka sen på **LÄGG TILL**. Alternativt kan du skriva (eller kopiera och klistra in) sökvägen till filen eller mappen i redigeringsfältet.

c. Som standard undantas den valda filen eller mappen från både vid åtkomst- och på begäran-skanning. För att ändra när undantaget ska tillämpas väljer du ett av de andra alternativen.

d. Klicka **Lägg till**.

14.5.2. Undanta filtillägg från skanning

När du undantar ett filtillägg från skanning, skannar Bitdefender inte längre filer med det tillägget, oavsett var de finns på din dator. Undantaget gäller även filer på borttagbara medier, som CD-skivor, DVD-skivor, USB-lagringsenheter eller nätverksenheter.

Viktigt
Var försiktig när du undantar filtillägg från skanning eftersom sådana undantag kan göra datorn mer sårbar för hot.

Undanta filtillägg från skanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Undantag**.
4. Klicka på rullgardinsmenyn **Lista med tillägg undantagna från skanning**. I det fönster som visas kan du hantera filtillägg som är undantagna från skanning.
5. Lägg till undantag genom att följa dessa steg:
   a. Klicka **Lägg till**.
   b. Skriv in de filtillägg som du vill ska undantas från skanning, separerade med semikolon (;). Här är ett exempel:

      txt;avi;jpg

   c. Som standard är alla filer med de specificerade tilläggen undantagna från både vid åtkomst- och på begäran-skanning. För att ändra när undantaget ska tillämpas väljer du ett av de andra alternativen.
   d. Klicka på **LÄGG TILL**.

14.5.3. Hantera skanningsundantag

Om de inställda undantagen från skanning inte längre behövs rekommenderar vi att du raderar dem eller inaktiverar skanningsundantag.

Hantera skanningsundantag:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Undantag**.
4. Använd alternativen i rullgardinsmenyn **Lista över filer och mappar undantagna från skanning** för att hantera skanningsundantag.
5. Ta bort eller redigera skanningsundantag genom att klicka på en a de tillgängliga länkarna. Fortsätt enligt följande:
   - Ta bort en post från listan genom att markera den och klicka på **Ta bort**.
   - Redigera en post från tabellen genom att dubbelklicka på den (eller markera den och klicka på **Redigera**). Ett nytt fönster visas där du kan ändra det tillägg eller den sökväg som ska undantas och den typ av skanning du vill att de ska undantas från, efter behov. Gör de nödvändiga ändringarna och klicka sedan på **ÄNDRA**.

14.6. Hantera filer i karantän

Bitdefender isolerar de hotinfekterade filerna den inte kan desinfektera och de misstänkta filerna i ett säkert område som kallas karantän. När ett hot är satt i karantän kan det inte göra någon skada eftersom det inte kan köras eller läsas.

Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en informationsuppdatering för att tillåta borttagning av hotet.

Dessutom skannar Bitdefender filerna som är satta i karantän varje gång hotinformationsdatabasen uppdateras. Rengjorda filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Kontrollera och hantera filer i karantän:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Karantän**.

Här kan du visa namnet på filerna i karantän, deras ursprungliga plats och namnet på de upptäckta hoten.

3. Filer satta i karantän hanteras automatiskt av Bitdefender enligt standardinställningarna för karantän.

   Även om det inte rekommenderas kan du justera karantäninställningarna enligt dina önskemål genom att klicka på **Visa inställningar**.

   Klicka på reglagen för att aktivera eller inaktivera:

   Skanna om karantän efter uppdatering av information
   Behåll detta alternativ aktiverat för att automatiskt skanna filer i karantän varje gång hotinformationsdatabas uppdateras. Rengjorda filer flyttas automatiskt tillbaka till sin ursprungliga plats.

   Ta bort innehåll äldre än 30 dagar
   Filer i karantän äldre än 30 dagar raderas automatiskt.

   Skapa undantag för återställda filer
   De filer du återställer från karantän flyttas tillbaka till sin ursprungliga plats utan att repareras och undantas automatiskt från kommande skanningar.

4. Ta bort en fil i karantän genom att markera den och klicka på knappen **TA BORT**. Om du vill återställa en fil från karantän till sin ursprungliga plats, välj den och klicka **ÅTERSTÄLL**.

15. AVANCERAT HOTSKYDD

Bitdefender Advanced Threat Defense är en innovativ proaktiv detekteringsteknologi som använder avancerade heuristiska metoder för att upptäcka ransomware och andra nya eventuella hot i realtid.

Advanced Threat Defense övervakar kontinuerligt de appar som körs på datorn på jakt efter hotlika aktiviteter. Alla dessa åtgärder poängsätts och en total poäng räknas ut för varje process.

Som en säkerhetsåtgärd meddelas du varje gång hot och eventuellt skadliga processer upptäcks och blockeras.

15.1. Aktivera eller inaktivera Advanced Threat Defense

Aktivera eller inaktivera Advanced Threat Defense:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** aktiverar eller inaktiverar du omkopplaren.

> **Notera**
> För att systemet ska vara skyddat mot ransomware och andra hot rekommenderar vi att du inaktiverar Advanced Threat Defense under så kort tid som möjligt.

15.2. Kontrollera upptäckta skadliga attacker

Varje gång hot eller potentiellt skadliga processer upptäcks blockerar Bitdefender dem för att förhindra att datorn infekteras av ransomware eller annan skadlig kod. Du kan när som helst kontrollera listan med upptäckta skadliga attacker genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Hotförsvar**.
3. Första gången du öppnar ransomwareskyddet presenteras du för funktionen. Klicka **JAG FATTAR** för att fortsätta.

   De attacker som upptäckts under de senaste 90 dagarna visas. För att visa information om typen av upptäckt ransomware, sökvägen till den

skadliga processen eller om desinfektionen har lyckats, klickar du bara på det.

15.3. Lägga till processer till undantag

Du kan konfigurera uteslutningsregler för betrodda program så att Advanced Threat Defense inte blockerar dem om de utför hotliknande åtgärder.

Börja lägga till processer till undantagslistan för Advanced Threat Defense:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Inställningar**.
3. I fönstret **Undantag** klickar du på **Lägg till program till undantag**.
4. Hitta och välj den app du vill ska undantas och klicka sedan på **OK**.

   Om du vill ta bort en post från listan klickar du på alternativet **Ta bort** bredvid den.

16. FÖREBYGGA ONLINEHOT

Bitdefender Online Threat Prevention säkerställer en säker surfupplevelse genom att varna dig om möjliga skadliga webbsidor.

Bitdefender tillhandahåller förebyggande av onlinehot för:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Konfigurera inställningar för förebyggande av onlinehot:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Inställningar**.

I fönstret **Webbskydd** klickar du på reglagen för att aktivera eller inaktivera:

- Förebyggande av webbattack blockerar hot som kommer från Internet, däribland drive-by-nedladdningar.
- Search Advisor, en komponent som rankar resultat från dina sökmotorfrågor och de länkar som publicerats på sociala nätverk genom att placera en ikon bredvid varje resultat:

  Du bör inte besöka den här webbsidan.

  Den här webbsidan kan innehålla farligt innehåll. Iaktta försiktighet om du besöker den.

  Det här är en säker sida att besöka.

  Search Advisor rankar resultaten från följande sökmotorer:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor rankar länkar som publicerats på följande sociala nätverkstjänster:
  - Facebook

- Twitter
- Krypterad webbskanning.

  Mer sofistikerade attacker kan använda säker webbtrafik för att missleda sina offer. Därför rekommenderar vi att du har alternativet Krypterad webbskanning aktiverat.
- Skydd mot bedrägeri.
- Skydd mot nätfiske.

I fönstret **Förebyggande av nätverkshot** finns alternativet **Förebyggande av näthot**. För att hålla datorn borta från attacker från komplexa skadeprogram (som ransomware) via exploatering av säkerhetsbrister ska du ha det här alternativet aktiverat.

Du kan skapa en lista över webbplatser som inte skannas av antihot-, antinätfiske- och antibedrägerimotorerna i Bitdefender. Listan bör endast innehålla webbsidor du litar fullständigt på. Lägg till exempel till de webbplatser där du shoppar online.

Konfigurera och hantera webbplatser via funktionen Online Threat Prevention från Bitdefender:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Undantag**.
3. Skriv namnet på den webbplats du vill lägga till i vitlistan i motsvarande fält och klicka sedan på **LÄGG TILL**.

   Om du vill ta bort en webbsida från listan väljer du den i listan och klickar på motsvarande länk **Ta bort**.

   Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

16.1. Bitdefender-varningar i webbläsaren

Varje gång du försöker besöka en webbplats som är klassad som osäker blockeras webbplatsen och en varningssida visas i webbläsaren.

Den här sidan innehåller information som webbplats-URL och upptäckta hot.

Du måste bestämma vad som ska göras härnäst. Följande alternativ är tillgängliga:

- Navigera bort från sidan genom att klicka på **TA MIG TILLBAKA TILL SÄKERHETEN**.

- Fortsätt till sidan, trots varningen, genom att klicka på **Jag förstår risken, ta mig dit ändå**.
- Om du är säker på att den hittade sidan är säker klickar du på **SKICKA** för att lägga till den i vitlistan. Vi rekommenderar att du bara lägger till webbsidor du verkligen litar på.

17. SÄKERHETSRISK

Ett viktig steg för att skydda din dator mot skadliga aktiviteter och program är att se till att operativsystemet och de appar du regelbundet använder är uppdaterade. Dessutom måste starka lösenord (lösenord som inte enkelt kan gissas) konfigureras för varje Windows-användarkonto och för de Wi-Fi-nätverk du ansluter till, för att förhindra obehörig fysisk åtkomst till din dator.

Bitdefender kontrollerar automatiskt ditt system efter sårbarheter och varnar dig om dem. Den skannar efter följande:

- utdaterade appar på datorn.
- saknade Windowsuppdateringar
- svaga lösenord till Windows användarkonton.
- osäkra trådlösa nätverk och routrar.

Bitdefender har två enkla sätt att åtgärda säkerhetsbristerna i ditt system:

- Du kan skanna systemet efter säkerhetsbrister och åtgärda dem steg för steg genom att använda alternativet **Sårbarhetsskanning**.
- Med automatisk sårbarhetsövervakning kan du kontrollera och åtgärda upptäckta säkerhetsbrister i fönstret Meddelanden.

Du bör kontrollera och åtgärda systemsäkerhetsbrister varje eller varannan vecka.

17.1. Skanna systemet för säkerhetsrisker

Åtgärda systemsäkerhetsbrister med hjälp av alternativet Sårbarhetsskanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSRISK** klickar du på **Sårbarhetsskanning**.
3. Vänta medan Bitdefender kontrollerar ditt system för säkerhetsbrister. Stoppa skanningsprocessen genom att klicka på knappen **Hoppa över** längst upp i fönstret.

   - **Kritiska Windows-uppdateringar**

     Klicka på **Visa information** för att se listan med kritiska Windows-uppdateringar som inte är installerade på datorn.

Initiera installationen av valda uppdateringar genom att klicka på **Installera uppdateringar**. Observera att det kan ta en stund att installera uppdateringarna och vissa av dem kan kräva en omstart av systemet för att installationen ska slutföras. Om så krävs startar du om systemet så snabbt som möjligt.

- **Programuppdateringar**

  Om en app inte är uppdaterad klickar du på länken **Hämta ny version** för att hämta den senaste versionen.

  Klicka på **Visa information** för att se information om den app som måste uppdateras.

- **Svaga Windows-kontolösenord**

  Du kan se den ändrade listan över Windows-användarkonton på din dator, och skyddsnivån deras lösenord håller.

  Klicka på **Ändra lösenord vid inloggning** för att ställa in ett nytt lösenord för systemet.

  Klicka på **Visa information** för att ändra de svaga lösenorden. Du kan välja mellan att be användaren ändra lösenordet vid nästa inloggning eller ändra lösenordet själv direkt. För ett starkt lösenord, använd en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).

- **Wi-Fi-nätverk**

  Klicka på **Visa information** för att ta reda på mer om det trådlösa nätverk du är ansluten till. Om du blir rekommenderad att ange ett starkare lösenord för ditt hemnätverk klickar du på motsvarande länk.

  När andra rekommendationer är tillgängliga följer du angivna instruktioner för att se till att hemnätverket förblir säkert för hackares nyfikna ögon.

I det övre högra hörnet på fönstret kan du filtrera resultaten enligt dina preferenser.

17.2. Använda automatisk sårbarhetsövervakning

Bitdefender skannar regelbundet systemet efter sårbarheter, i bakgrunden, och håller reda på upptäckta problem i fönstret Meddelanden.

Kontrollera och åtgärda upptäckta problem:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste sårbarhetsskanningen.
3. Du kan se detaljerad information avseende de upptäckta säkerhetsbristerna i systemet. Beroende på händelse, för att åtgärda ett specifikt säkerhetsproblem fortsätt enligt följande:
   - Om det finns tillgängliga Windows-uppdateringar klickar du på **Installera**.
   - Om automatisk Windows-uppdatering är inaktiverat klickar du på **Aktivera**.
   - Om en app är utdaterad klickar du på **Uppdatera nu** för att hitta en länk till leverantörens hemsida varifrån du kan installera den senaste versionen av appen.
   - Om ett Windows-användarkonto har ett svagt lösenord klickar du på **Byt lösenord** för att tvinga användaren att byta lösenord vid nästa inloggning eller så kan du ändra lösenordet själv. För ett starkt lösenord, använd en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).
   - Om Windows-funktionen Autorun är aktiverad klickar du **Åtgärda** för att inaktivera den.
   - Om den router du har konfigurerat har angett ett svagt lösenord klickar du på **Ändra lösenord** för att komma till dess gränssnitt varifrån du kan ange ett starkt.
   - Om det nätverk du är ansluten till har säkerhetsbrister som kan försätta systemet i risk klickar du på **Ändra Wi-Fi-lösenord**.

Konfigurera inställningar för säkerhetsbristövervakning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Inställningar**.

   Viktigt
   För att regelbundet meddelas om system- eller appsäkerhetsbrister ska du har alternativet **Säkerhetsbrist** aktiverat.

3. Välj de systemsäkerhetsbrister du regelbundet vill ska kontrolleras genom att använda motsvarande omkopplare.

Windowsuppdateringar
Kontrollera om operativsystemet Windows har de senaste kritiska säkerhetsuppdateringarna från Microsoft.

Programuppdateringar
Kontrollera om appar installerade på ditt system är uppdaterade. Utdaterade appar kan exploateras av skadlig programvara, vilket gör din PC sårbar för utomstående attacker.

Användarlösenord
Kontrollera om lösenorden för de Windows-konton och routrar som är konfigurerade på systemet är enkla att gissa eller inte. Att konfigurera lösenord som svåra att gissa (starka lösenord) gär det mycket svårt för hackare att bryta sig in i systemet. Ett starkt lösenord innehåller en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).

Spela automatiskt
Kontrollera statusen för Windows-funktionen Autorun. Den här funktionen gör att appar automatiskt startas från CD-skivor, DVD-skivor, USB-enheter eller andra externa enheter.

Vissa typer av hot använder Autorun för att spridas automatiskt från borttagbara medier till datorn. Därför rekommenderar vi att du inaktiverar den här Windows-funktionen.

Wi-Fi-säkerhet
Kontrollera om det trådlösa hemnätverk du är ansluten till är säkert eller inte, eller om det har säkerhetsbrister. Kontrollera också om lösenordet för din hemrouter är tillräckligt starkt och hur du kan göra det säkrare.

De flesta oskyddade nätverk är inte säkra och tillåter därmed att en hackare får tillgång till dina privata aktiviteter.

Notera
Om du stänger av övervakning av en specifik säkerhetsbrist kommer tillhörande problem inte längre att registreras i meddelandefönstret.

17.3. Wi-Fi Security Advisor

När du är på språng, arbetar på kafé eller väntar på flygplatsen, kan den snabbaste lösningen vara att ansluta till ett publikt trådlöst nätverk för att

göra betalningar, kolla e-post eller sociala nätverkskonton. Men det kan finnas någon som försöker kapa dina personuppgifter där och som ser hur informationen läcker genom nätverket.

Personuppgifter innebär lösenord och användarnamn du använder för att få åtkomst till dina onlinekonton, som e-post, bankkonton, sociala mediekonton, men även de meddelanden du skickar.

Oftast är det mer troligt att publika trådlösa nätverk är osäkra, eftersom de inte kräver lösenord vid inloggning, och om de gör det, kan det lösenordet göras tillgängligt för alla som vill ansluta. Dessutom kan de vara skadliga nätverk, som utgör en måltavla för kriminella.

För att skydda dig mot farorna med osäkra eller okrypterade publika trådlösa surfzoner, analyserar Bitdefender Wi-Fi Security Advisor hur säkert ett trådlöst nätverk är, och om det behövs, rekommenderar dig att använda Bitdefender VPN.

Bitdefender Wi-Fi Security Advisor ger dig följande information om:

- Trådlösa hemnätverk
- Trådlösa publika nätverk

17.3.1. Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor

Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Inställningar**.
3. I fönstret **Inställningar** kan du aktivera eller inaktivera alternativet **Wi-Fi-säkerhet**.

17.3.2. Konfigurera trådlöst hemnätverk

För att börja konfigurera ditt hemnätverk:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Wi-Fi-säkerhet**.
3. På fliken **HEM-Wi-Fi** klickar du på knappen **VÄLJ HEM-WI-FI**.

   En lista med de trådlösa nätverk du anslutit till hittills visas.

4. Peka på ditt hemnätverk och klicka därefter på **VÄLJ**.

Om ett hemnätverk anses vara osäkert, visas konfigurationsrekommendationer för att förbättra dess säkerhet.

Ta bort det trådlösa nätverk du har angett som hemnätverk genom att klicka på knappen **TA BORT**.

17.3.3. Offentlig Wi-Fi

Medan du är ansluten till ett osäkert trådlöst nätverk är profilen Publikt Wi-Fi aktiverad. När den körs i den här profilen är Bitdefender Antivirus Plus inställd på att automatiskt uppnå följande programinställningar:

- Advanced Threat Defense är aktiverat
- Följande inställningar från Förebyggande av onlinehot är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägeri
  - Skydd mot nätfiske
- En knapp som öppnar Bitdefender Safepay™ är tillgänglig. I det här fallet är hotspot-skydd för osäkra nätverk aktiverat som standard.

17.3.4. Kontrollera information om Wi-Fi-nätverk

Kontrollera information om de trådlösa nätverk du oftast ansluter till:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Wi-Fi-säkerhet**.
3. beroende på vilken information du behöver väljer du en av de två flikarna, **HEM-Wi-Fi** eller **PUBLIKT Wi-Fi**.
4. Klicka på **Visa information** bredvid det nätverk du vill hitta mer information om.

Det finns tre typer av trådlösa nätverk som filtreras efter deras betydelse, varje typ anges av en specifik ikon:

Wi-Fi är osäkert - anger att säkerhetsnivån för nätverket är låg. Det innebär att det är en stor risk att använda det och vi rekommenderar inte att göra betalningar eller kontrollera bankkonton utan extra skydd. I sådana

situationer rekommenderar vi att du har Bitdefender Safepay™ med hotspotskydd för osäkra nätverk aktiverat.

Wi-Fi är osäkert - anger att säkerhetsnivån för nätverket är måttlig. Det innebär att det kan finnas säkerhetsbrister och vi rekommenderar inte att göra betalningar eller kontrollera bankkonton utan extra skydd. I sådana situationer rekommenderar vi att du har Bitdefender Safepay™ med hotspotskydd för osäkra nätverk aktiverat.

Wi-Fi är säkert - anger att det nätverk du använder är säkert. I det här fallet kan du använda känslig information för onlineåtgärder.

Genom att klicka på **Visa information** i området för varje nätverk, visas följande information:

- **Säkert** - här kan du se om det valda nätverket är säkert eller inte. Okrypterade nätverk kan exponera den information du använder.
- **Krypteringstyp** - här kan du visa den krypteringstyp som används av valt nätverk. Vissa krypteringstyper kanske inte är säkra. Därför rekommenderar vi att du kontrollerar informationen om den visade krypteringstypen för att vara säker på att du är skyddad när du surfar på nätet.
- **Kanal/Frekvens** - här kan du visa den kanalfrekvens som används av det valda nätverket.
- **Lösenordsstyrka** - här kan du visa hur starkt lösenordet är. Observera att de nätverk som har svaga lösenord utgör en måltavla för cyberbrottslingar.
- **Typ av inloggning** - här kan du visa om valt nätverk är skyddat av ett lösenord eller inte. Vi rekommenderar att du endast ansluter till nätverk som har konfigurerat starka lösenord.
- **Autentiseringstyp** - här kan du visa den autentiseringstyp som används av valt nätverk.

Håll alternativet **Meddela** aktiverat för att ta emot meddelanden varje gång systemet ansluter till det här nätverket.

18. SAFE FILES

Ransomware är skadlig programvara som attackerar sårbara system genom att låsa dem och be om pengar för att låta användaren få tillbaka kontroll över sitt system. Sådan här skadlig programvara agerar smart genom att visa falska meddelanden för att skrämma användaren och tvinga denne att gå vidare med betalningen.

Infektionen kan spridas via spam e-post, genom att ladda ned bilagor eller genom att besöka smittade webbplatser och installera skadliga program utan att låta användaren veta vad som händer på systemet.

Ransomware kan ha ett av följande beteenden för att förhindra användaren att komma åt sitt system:

- Krypterar känsliga och personliga filer utan möjligheten att dekryptera tills en lösen betalas av offret.
- Låser datorns skärm och visar ett meddelande som ber om pengar. I det här fallet är ingen fil krypterad, men användaren är tvungen att fortsätta med betalningen.
- Blockerar appar från att köras.

Med Bitdefender Safe Files kan du hålla personliga filer, som dokument, foton eller filmer skyddade från ransomwareattacker.

Notera
Advanced Threat Defense och Safe Files är två lager skydd som skyddar mot ransomware. Advanced Threat Defense är funktionen som stoppar ransomwareattacker när de spårar systemets kritiska områden, medan Safe Files ser till att ingen viktig fil på datorn krypteras.

18.1. Aktivera och inaktivera Safe Files

Aktivera och inaktivera funktionen Safe Files:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SAFE FILES** aktiverar eller inaktiverar du omkopplaren.

Varje gång en app försöker öppna en av de skyddade filerna visas en Bitdefender-popupruta. Du kan tillåta eller blockera åtkomst.

Notera
Funktionen Safe Files är som standard inte aktiverad.

18.2. Skydda personliga filer från ransomwareattacker

Om du vill placera personliga filer i ett skydd:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SAFE FILES** klickar du på **Skyddade mappar**.
3. Första gången du öppnar Skyddade mappar presenteras du för funktionen. Klicka på **SKYDDA FLER MAPPAR** för att fortsätta.
4. Välj den mapp du vill skydda och klicka sedan på **OK**.

   Klicka på länken **Skydda fler mappar** för att lägga till ytterligare mappar. Alternativt så drar du mappar till det här fönstret.

Som standard skyddas mapparna Bilder, Videor, Dokument och Musik mot hotattacker. Personlig information som lagras i onlinefiltjänster som Box, Dropbox, Google Drive och OneDrive omfattas också av skyddsmiljö, förutsatt att deras appar är installerade på systemet.

För att undvika att systemet blir långsammare rekommenderar vi att du lägger till som mest 30 mappar eller sparar flera filer i en mapp.

Notera
Anpassade mappar kan endast skyddas för aktuella användare. System- och appfiler kan inte läggas till som undantag.

18.3. Konfigurera appåtkomst

De appar som försöker ändra eller ta bort skyddade filer kan flaggas som potentiellt osäkra och läggas till i listan Blockerade appar. Om en sådan app blockeras och du är säker på att dess beteende är normalt, kan du tillåta den genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SAFE FILES** klickar du på **Programåtkomst**.
3. Apparna som har begärt att ändra filer i dina skyddade mappar listades. Aktivera omkopplaren bredvid den app du vet är säker.

I samma fönster kan du inaktivera ransomwareskydd för specifika appar genom att inaktivera motsvarande omkopplare.

Om du vill lägga till nya appar i listan klickar du på länken **Lägg till nytt program i listan**.

18.4. Skydd vid start

Det är känt att många skadliga appar är konfigurerade att köras vid systemstart, något som allvarligt kan skada en maskin. Bitdefenders starttidsskydd skannar alla viktiga systemområden innan alla filer laddas, utan att systemet påverkas.

Inaktivera skydd vid start:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **SAFE FILES**-panelen klickar du på **Inställningar**.
3. Inaktivera **Skydd vid start**.

Notera
Appar som läggs till i undantag skannas och behandlas utifrån det.

19. AVHJÄLPNING AV RANSOMWARE

Bitdefender Ransomware Remediation säkerhetskopierar filer som dokument, bilder, videor eller musik för att se till att de skyddas från att skadas eller förloras i händelse av ransomwarekryptering. Varje gång en ransomwareattack upptäcks blockerar Bitdefender alla processer som är inblandade i attacken och startar avhjälpningsprocessen. På så sätt kan du återställa innehållet för alla dina filer utan att betala den begärda lösensumman.

19.1. Aktivera eller inaktivera ransomwareavhjälpning

Aktivera eller inaktivera ransomwareavhjälpning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** aktiverar eller inaktiverar du omkopplaren.

> **Notera**
> För att säkerställa att dina filer är skyddade mot ransomware rekommenderar vi att du har Avhjälpning av ransomware aktiverat.

19.2. Aktivera eller inaktivera automatisk återställning

Med Automatisk återställning kan du se till att dina filer återställs automatiskt i händelse av ransomwarekryptering.

Aktivera eller inaktivera automatisk återställning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** klickar du på **Inställningar**.
3. Aktivera eller inaktivera omkopplaren **Automatisk återställning**.

19.3. Visa filer som har återställts automatiskt

När alternativet **Automatisk återställning** är aktiverat återställer Bitdefender automatiskt filer som krypterats av ransomware. På så sätt kan du ha en bekymmersfri datorupplevelse och veta att dina filer är säkra.

Visa filer som har återställts automatiskt:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.

2. På fliken **Alla** markerar du meddelandet avseende det senast upptäckta ransomwarebeteendet som avhjälpts och klickar sedan på **Återställda filer**.

   Listan med återställda filer visas. Här kan du även visa platsen dit dina filer har återställts.

19.4. Återställa krypterade filer manuellt

Ifall du manuellt måste återställa filer som krypterats av ransomware följer du de här stegen:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** markerar du information avseende det senast upptäckta ransomwarebeteendet som upptäckts och klickar sedan på **Krypterade filer**.
3. Listan med krypterade filer visas.

   Klicka på **ÅTERSTÄLL FILER** för att fortsätta.
4. Ifall hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de avkrypterade filerna ska sparas. Klicka på **ÅTERSTÄLL PLATS** och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.

   Klicka på **SLUTFÖR** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas ifall de blir krypterade:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

19.5. Lägga till program till undantag

Du kan konfigurera undantagsregler för betrodda appar så att funktion Avhjälpning av ransomware inte blockerar dem om de utför ransomwareliknande åtgärder.

Lägga till appar till undantagslistan för avhjälpning av ransomware:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** klickar du på **Undantag**.
3. Om du vill lägga till appar i listan klickar du på **Lägg till ett nytt program i listan**.

20. LÖSENORDSHANTERINGSSKYDD FÖR DINA INLOGGNINGSUPPGIFTER

Vi använder våra datorer för att shoppa online eller betala räkningar, för att ansluta till sociala media-plattformar eller logga in med snabbmeddelandeappar.

Men som alla vet är det inte alltid så lätt att komma ihåg lösenordet!

Och om vi inte är försiktiga när vi surfar online kan vår privata information, som e-postadress, snabbmeddelande-ID eller kreditkortsinformation komprometteras.

Att ha sina lösenord eller personuppgifter på ett papper eller i datorn kan vara farligt, eftersom de kan hittas och användas av andra personer som vill stjäla och använda den informationen. Och det är inte så lätt att komma ihåg alla lösenord du ställt in för dina onlinekonton eller för dina favoritwebbsidor.

Finns det därför något sätt för att vi ska vara säkra på att vi hittar våra lösenord när vi behöver dem? Och kan vi lita på att våra hemliga lösenord alltid är säkra?

lösenordshanterare hjälper dig att hålla reda på dina lösenord, skyddar din integritet och ger en säker surfupplevelse.

Genom att använda ett enda huvudlösenord för att komma åt dina inloggningsuppgifter gör Password Manager det enkelt för dig att ha dina lösenord säkra i en plånbok.

Password Manager är integrerat med Bitdefender Safepay™ för att erbjuda det bästa skyddet för dina onlineaktiviteter och ger en enhetlig lösning för de olika sätt på vilka din privata information kan komprometteras.

Password Manager skyddar följande privata information:

- Personlig information, som e-postadress eller telefonnummer
- Inloggningsuppgifter för webbplatserna
- Bankkontoinformation eller kreditkortsnummer
- Komma åt data till e-postkonton
- Lösenord till apparna
- Lösenord för Wi-Fi-nätverken

20.1. Skapa en ny plånboksdatabas

Bitdefender Wallet är platsen där du kan lagra din personliga information. För en enklare surfupplevelse måste du skapa en plånboksdatas så här:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **PASSWORD MANAGER** fliken, klicka på **Skapanyplånbok**.
3. Klicka på **Skapa ny**.
4. Skriv in den önskade informationen i de motsvarande fälten.
   - Plånboksetikett - skriv ett unikt namn för din plånboksdatabas.
   - Huvudlösenord - skriv ett lösenord för din plånbok.
   - Skriv lösenordet igen - skriv in det lösenord du angav igen.
   - Ledtråd - skriv en ledtråd för att komma ihåg lösenordet.
5. Klicka på **FORTSÄTT**.
6. I det här steget kan du välja att lagra din information i molnet. Om du väljer Ja lagras bankinformation lokalt på din enhet. Välj önskat alternativ och klicka på **FORTSÄTT**.
7. Välj den webbläsare du vill importera inloggningsuppgifter från.
8. Klicka på **SLUTFÖR**.

20.2. Importera en befintlig databas

Importera en plånbok lagrad lokalt:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **PASSWORD MANAGER** fliken, klicka på **Skapanyplånbok**.
3. Klicka på **FRÅN MÅL**.
4. Gå till den plats på enheten där du vill spara plånboksdatabasen och välj sedan ett namn för den.
5. Klicka **Öppna**.
6. Ge ett namn åt din plånbok och skriv in det lösenord du tilldelade när den skapades första gången.
7. Klicka på **IMPORTERA**.

8. Välj de program du vill att plånboken ska importera inloggningsuppgifter från och sedan knappen **SLUTFÖR**.

20.3. Exportera plånboksdatabasen

Exportera plånboksdatabasen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Mina plånböcker**.
3. Klicka på ⋮ -ikonen i önskad plånbok och välj sedan **Exportera**.
4. Sök på platsen för din plånboksdatabas och välj den (.dtb-filen).
5. Klicka **Spara**.

Notera
Plånböckerna måste vara öppna för att **Exportera**-funktionen ska vara tillgänglig.
Om den plånbok du behöver exportera är låst klickar du på **AKTIVERA PLÅNBOK** och skriver därefter i det lösenord som tilldelades när den skapades första gången.

20.4. Synkronisera plånböckerna i molnet

Aktivera eller inaktivera plånbokssynkronisering i molnet:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Mina plånböcker**.
3. Klicka på ⋮ -ikonen i önskad plånbok och välj sedan **Inställningar**.
4. Välj det önskade alternativet i det fönster som visas och klicka sedan på **Spara**.

Notera
Plånböckerna måste vara öppna för att **Exportera**-funktionen ska vara tillgänglig.
Om den plånbok du behöver synkronisera är låst klickar du på **AKTIVERA PLÅNBOK** och skriver därefter i det lösenord som tilldelades när den skapades första gången.

20.5. Hantera dina plånboksinloggningsuppgifter

Hantera dina lösenord:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Mina plånböcker**.
3. Välj den önskade plånboksdatabasen och klicka sedan på **AKTIVERA PLÅNBOK**.
4. Skriv huvudlösenordet och klicka sedan på **OK**.

Ett nytt fönster visas. Välj önskad kategori från den övre delen i fönstret:

- Identitet
- Webbsidor
- Internetbank
- E-postmeddelanden
- Appar
- Wi-Fi-nätverk

Lägga till/redigera inloggningsuppgifter

- Lägg till ett nytt lösenord genom att välja önskad kategori överst, klicka på **+ Lägg till objekt**, infoga informationen i motsvarande fält och klicka på Spara.
- För att redigera en post i tabellen, välj den och klicka på **Redigera** knappen.
- Ta bort en post genom att markera den och klicka på **Ta bort** .

20.6. Aktivera eller inaktivera Password Manager-skyddet

Aktivera eller inaktivera Password Manager-skyddet:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** aktiverar eller inaktiverar du omkopplaren.

20.7. Hantera inställningarna för Password Manager

Konfigurera huvudlösenordet i detalj:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fliken **Säkerhetsinställningar**.

Följande alternativ är tillgängliga:

- **Fråga om mitt huvudlösenord när jag loggar in till min enhet** - du ombes att infoga ditt huvudlösenord när du öppnar enheten.
- **Fråga om mitt huvudlösenord när jag öppnar mina webbläsare och appar** - du ombes att infoga ditt huvudlösenord när du öppnar en webbläsare eller en app.
- **Fråga inte efter mitt huvudlösenord** - du kommer inte att tillfrågas om ditt huvudlösenord när du öppnar datorn, en webbläsare eller en app.
- **Lås automatiskt plånbok när jag lämnar min enhet utan uppsikt** - du uppmanas att infoga ditt huvudlösenord när du återgår till enheten efter 15 minuter.

Viktigt
Kom ihåg ditt huvudlösenord eller förvara det på en säker plats. Om du glömmer bort lösenordet måste du ominstallera programmet eller kontakta Bitdefender för support.

Förbättra din upplevelse

Välj de mappar eller appar där du vill integrera Password Manager:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fliken **Insticksprogram**.

   Markera en app för att använda Password Manager och förbättra din upplevelse:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome

- Säker betalning

Konfigurera Automatisk ifyllnad

Funktionen Automatisk ifyllnad gör det enkelt att ansluta till dina favoritwebbsidor eller logga in med dina onlinekonton. Första gången du anger dina inloggningsuppgifter och personliga information i webbläsaren är de automatiskt säkrade i plånboken.

Konfigurera inställningarna för **Automatisk ifyllnad**:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fliken **Inställningar för Automatisk ifyllnad**.
4. Konfigurera följande alternativ:
   - **Konfigurera hur plånboken håller dina inloggningsuppgifter säkra**:
     - **Spara inloggningsuppgifter automatiskt i plånboken** - inloggningsuppgifter och annan identifierbar information som person- och kreditkortsuppgifter sparas automatiskt och uppdateras i plånboken.
     - **Fråga mig varje gång** - du tillfrågas varje gång du om du vill lägga till dina uppgifter i plånboken.
     - **Spara inte, jag uppdaterar informationen manuellt** - inloggningsuppgifterna kan endast läggas till manuellt i plånboken.
   - **Fyll i inloggningsuppgifter automatiskt**:
     - **Fyll i inloggningsuppgifter automatiskt varje gång** - inloggningsuppgifterna infogas automatiskt i webbläsaren.
   - **Fyll i formulär automatiskt**:
     - **Fråga efter mina ifyllningsalternativ när jag besöker en sida med formulär** - en popupruta med ifyllningsalternativen visas varje gång Bitdefender upptäcker att du vill utföra en onlinebetalning eller registrera dig.

Hantera Password Manager-information från webbläsaren

Du kan enkelt hantera Password Manager-information direkt från webbläsaren för att ha all viktig information till hands. Tillägget Bitdefender-plånbok stöds

av följande webbläsare: Google Chrome, Internet Explorer och Mozilla Firefox, och är även integrerat med Safepay.

För att komma till Bitdefender-plånboken öppnar du webbläsaren, tillåter att tillägget installeras och klickar på  -ikonen i verktygsfältet.

Tillägget Bitdefender-plånbok innehåller följande alternativ:

- Öppna plånbok - öppnar plånboken.
- Lås plånbok - låser plånboken.
- Webbsidor - öppnar en undermeny med alla webbplatsinloggningar sparade i plånboken. Klicka på **Lägg till webbsida** för att lägga till nya webbplatser i listan.
- Fyll i formulär - öppnar en undermeny som innehåller den information du lagt till för en särskild kategori. Härifrån kan du lägga till nya uppgifter i plånboken.
- Lösenordsgenerator - gör att du kan generera slumpmässiga lösenord du kan använda för befintliga konton. Klicka på **Visa avancerade inställningar** för att anpassa komplexiteten för lösenordet.
- Inställningar - öppnar inställlningsfönstret för lösenordshanteraren.
- Rapportera problem - rapportera alla problem du stöter på med Bitdefenders lösenordshanterare.

21. VPN

VPN-appen kan installeras från din Bitdefender-produkt och användas varje gång du vill lägga till en extra skyddslag till din anslutning. VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter till för att säkra din anslutning, kryptera data med kryptering i bankklass och dölja din IP-adress oavsett var du är. Din trafik omdirigeras via en separat server och gör det därmed näst intill omöjligt att identifiera din enhet bland de myriader av andra enheter som använder våra tjänster. När du är ansluten till Internet via Bitdefender VPN, kan du dessutom ha åtkomst till innehåll som i normala fall är begränsat i vissa områden.

Notera
Vissa länder censurerar Internet och därför kan användning av VPN på deras territorier vara förbjudet enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om regelverken i det land du befinner dig i och de risker du kan utsättas för.

21.1. Installera VPN

VPN-appen kan installeras från ditt Bitdefender gränssnitt enligt följande:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VPN** klickar du på **Installera VPN**.
3. I fönstret med beskrivningen av VPN-appen, läs **Prenumerationsavtalet** och klicka sedan på **INSTALLERA BITDEFENDER VPN**.

   Vänta flera ögonblick tills filerna hämtas och installeras.
4. Klicka på **ÖPPNA BITDEFENDER VPN** för att avsluta installationsprocessen.

Notera
Bitdefender VPN kräver att .Net Framework 4.5.2 eller högre är installerat. Om du inte har det här paketet installerat visas ett meddelandefönster. Klicka på **Installera .Net Framework** för omdirigering till en sida där du kan hämta den senaste versionen av den här programvaran.

21.2. Öppna VPN

För att komma åt huvudgränssnittet för Bitdefender VPN använder du en av följande metoder:

- Från systemfältet
  1. Högerklicka på -ikonen i systemfältet och klicka sedan på **Visa**.
- Från Bitdefenders gränssnitt:
  1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **VPN**-panelen klickar du på **Öppna VPN**.

21.3. VPN-gränssnitt

VPN-gränssnittet visar status för appen, ansluten eller frånkopplad. Serverplatsen för användare med den fria versionen ställs automatiskt av Bitdefender till den lämpligaste servern, medan premium användare har möjlighet att ändra serverplatsen de vill ansluta till. Mer information om VPN-prenumerationer finns i "*Prenumerationer*" (p. 118).

Klicka bara på den status som visas längst upp på skärmen för att ansluta eller koppla ifrån, eller högerklicka på systemfältsikonen. Systemfält ikonen visar ett grönt kontrollmärke när VPN är ansluten och en röd markering när VPN är frånkopplad.

När du är ansluten visas i nedre delen av gränssnittet den förflutna tiden och den IP-adress som automatiskt tilldelas till din enhet.

För att få tillgång till fler alternativ går du till **Meny**-området genom att högerklicka på -ikonen på den övre vänstra sidan. Här har du följande alternativ:

- **Mitt Konto** - information om ditt Bitdefender-konto och VPN-prenumeration visas. Klicka på **Växla konto** om du vill logga in med ett annat konto.
- **Inställningar** – beroende på dina behov kan du anpassa produktens beteende:
  - ta emot meddelanden när VPN automatiskt ansluter eller kopplar ifrån
  - kör automatiskt VPN-appen när Windows startas
  - starta automatiskt VPN-appen när enheten ansluter till osäkra trådlösa nätverk

- **Uppgradera till Premium** - om du använder den fria versionen kan du uppgradera till premiumplanen härifrån.
- **Support** - du omdirigeras till vår supportcenterplattform varifrån du kan läsa en användbar artikel om hur du använder Bitdefender VPN.
- **Om** - information om den installerade versionen visas.

21.4. Prenumerationer

Bitdefender VPN erbjuder utan kostnad 200 MB trafiksaldo per enhet för att säkra din anslutning varje gång du behöver det och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en server när du vill, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst genom att klicka på knappen **FÅ OBEGRÄNSAD TRAFIK** som finns i produktgränssnittet.

Bitdefender Premium VPN-prenumerationen är oberoende av Bitdefender Antivirus Plus-prenumerationen, vilket betyder att du kommer att kunna använda den under hela tillgänglighetsperioden, oavsett säkerhetslösningens prenumetationsstatus. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Antivirus Plus fortfarande är aktiv återgår du till gratisversionen.

Bitdefender VPN är en produkt över flera plattformar, tillgänglig i Bitdefender-produkter kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kan du använda din prenumeration på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

22. SAFEPAY-SÄKERHET FÖR ONLINETRANSLATIONER

Datorn blir snabbt huvudverktyg för att shoppa och utföra bankärenden. Betala räkningar, överföra pengar, köpa i princip allt du kan föreställa dig har aldrig varit snabbare eller enklare.

Det innebär att skicka personlig information, konto- och kreditkortsuppgifter, lösenord och andra typer av privat information över Internet, med andra ord exakt den typ av informationsflöde som cyberbrottslingar är mycket intresserade av att komma över. Hackare är outtröttliga i sina ansträngningar att stjäla den här informationen, så du kan aldrig vara nog försiktig när det gäller säkra onlinetransaktioner.

Bitdefender Safepay™ är först och främst en skydda webbläsare, en förseglad miljö som är utvecklad för att hålla dina bankärende, e-handel och andra typer av onlinetransaktioner privata och säkra.

För bästa integritetsskydd har Bitdefender Password Manager integrerats i Bitdefender Safepay™ för att säkra dina inloggningsuppgifter varje gång du vill öppna privata onlineplatser. Mer information finns på *"Lösenordshanteringsskydd för dina inloggningsuppgifter"* (p. 109).

Bitdefender Safepay™ erbjuder följande funktioner:

- Det blockerar åtkomst till ditt skrivbord och alla försök att ta bilder av din skärm.
- Det skyddar dina hemliga lösenord när du surfar online med Password Manager.
- Den har ett virtuellt tangentbord som när det används, gör det omöjligt för hackare att avläsa tangenttryckningar.
- Den är helt oberoende av dina andra webbläsare.
- Den har inbyggt hotspotskydd som ska användas när datorn är ansluten till osäkra Wi-Fi-nätverk.
- Den har stöd för bokmärken och tillåter att du navigerar mellan dina favoritwebbplatser för bankärenden/shopping.
- Den är inte begränsad till bankärenden och e-handel. Alla webbplatser kan öppnas i Bitdefender Safepay™.

22.1. Använda Bitdefender Safepay™

Som standard upptäcker Bitdefender när du navigerar till en bankwebbplats online eller onlinebutik i en webbläsare på datorn och uppmanar dig att starta den i Bitdefender Safepay™.

För att komma åt huvudgränssnittet för Bitdefender Safepay™ använder du en av följande metoder:

- Från Bitdefender-gränssnittet:
  1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **Safepay**-panelen klickar du på **Öppna Safepay**.
- Från Windows:
  - I **Windows 7**:
    1. Klicka på **Start** och gå till **Alla program**.
    2. Klicka på **Bitdefender**.
    3. Klicka på **Bitdefender Safepay™**.
  - I **Windows 8 och Windows 8.1**:

    Leta upp Bitdefender Safepay™ från Windows Start-skärm (du kan till exempel börja skriva "Bitdefender Safepay™" direkt på Start-skärmen) och därefter klicka på ikonen.
  - I **Windows 10**:

    Skriv "Bitdefender Safepay™" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon.

> **Notera**
> Om insticksprogrammet Adobe Flash Player inte är installerat eller utdaterat visas ett Bitdefender-meddelande. Klicka på motsvarande knapp för att fortsätta.
> När installationsprocessen är slutförd, måste du manuellt öppna Bitdefender Safepay™-webbläsaren igen för att fortsätta ditt arbete.

Om du är van vid webbläsare har du inga problem med att använda Bitdefender Safepay™ - den ser ut och fungerar som en vanlig webbläsare:

- ange de webbadresser du vill gå till i adressfältet.

- lägg till flikar för att besöka flera webbplatser i Bitdefender Safepay™-fönstret genom att klicka på .
- navigera tillbaka och framåt och uppdatera sidor med respektive.
- öppna Bitdefender Safepay™-inställningar genom att klicka på och välja **Inställningar**.
- skydda dina lösenord med Password Manager genom att klicka på .
- hantera dina bokmärken genom att klicka på bredvid adressfältet.
- öppna det virtuella tangentbordet genom att klicka på .
- öka eller minska webbläsarens storlek genom att trycka samtidigt på **Ctrl**- och **+/-**-tangenterna på den numeriska knappsatsen.
- visa information om din Bitdefender-produkt genom att klicka på och välja **Om**.
- skriv ut information genom att klicka på .

Notera
För att växla mellan Bitdefender Safepay™ och Windows-skrivbordet trycker du på **Alt+Tab**-tangenterna eller klickar på alternativet **Växla till skrivbord** på den övre vänstra sidan av fönstret.

22.2. Konfigurera inställningar

Klicka på och välj **Inställningar** för att konfigurera Bitdefender Safepay™:

Domänlista

Välj hur Bitdefender Safepay™ ska bete sig när du besöker webbplatser från specifika domäner i din vanliga webbläsare genom att lägga till dem till domänlistan och välj hur var och en ska bete sig:

- Öppna automatiskt i Bitdefender Safepay™.
- Låt Bitdefender uppmana dig att göra något varje gång.
- Använd aldrig Bitdefender Safepay™ när du besöker en sida från domänen i en vanlig webbläsare.

Blockera popup-rutor

Du kan välja att blockera popup-rutor genom att klicka på motsvarande omkopplare.

Du kan också skapa en lista över webbplatser att tillåta popup-rutor från. Listan bör endast innehålla webbsidor du litar fullständigt på.

Lägg till en webbplats till listan, ange dess adress i motsvarande fält och klicka på **Lägg till domän**.

Ta bort en webbplats från listan genom att välja X för önskad post.

Hantera plugin-program
Du kan välja om du vill aktivera eller inaktivera specifika insticksprogram i Bitdefender Safepay™.

Hantera certifikat
Du kan importera certifikat från systemet till ett certifikatlager.

Välj **Importera certifikat** och följ guiden för att använda certifikaten i Bitdefender Safepay™.

Automatiskt starta virtuellt tangentbord vid lösenordsfält
Det virtuella tangentbordet visas automatiskt när ett lösenordsfält väljs.

Använd motsvarande omkopplare för att aktivera eller inaktivera funktionen.

Be om bekräftelse innan utskrift
Aktivera det här alternativet om du vill bekräfta innan utskriftsprocessen startar.

22.3. Hantera bokmärken

Om du har inaktiverat den automatiska upptäckten av vissa eller alla webbplatser eller om Bitdefender helt enkelt inte hittar vissa webbplatser kan du lägga till bokmärken till Bitdefender Safepay™ så att du enkelt kan gå till favoritwebbplatser i framtiden.

Följ de här stegen för att lägga till en webbadress till Bitdefender Safepay™-bokmärken:

1. Klicka på -ikonen bredvid adressfältet för att öppna bokmärkessidan.

   Notera
   Sidan Bokmärken öppnas som standard när du startar Bitdefender Safepay™.

2. Klicka på **+**-knappen för att lägga till ett nytt bokmärke.
3. Skriv in webbadressen och titel på bokmärket och klicka på **Skapa**. Markera alternativet **Öppna automatiskt i Safepay** om du vill att den bokmärkta

sidan ska öppnas med Bitdefender Safepay™ varje gång du öppnar den. Webbadressen läggs också till i domänlistan på sidan Inställningar.

22.4. Inaktivera Safepay-meddelanden

När en bankwebbplats hittas är Bitdefender-produkten inställd på att meddela dig via en popup-ruta.

Inaktivera Safepay-meddelandena:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **Safepay**-panelen klickar du på **Inställningar**.
3. Inaktivera **Safepay-meddelanden**.

22.5. Använda VPN med Safepay

För att göra onlinebetalningar i en säker miljö när du är ansluten till osäkra nätverk kan Bitdefender-produkten ställas in för att automatiskt starta VPN-appen samtidigt med Safepay.

Börja använda VPN-appen tillsammans med Safepay:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **Safepay**-panelen klickar du på **Inställningar**.
3. Aktivera **Använd VPN med Safepay**.

23. DATASKYDD

23.1. Radera filer permanent

När du raderar en fil kan den inte längre nås på normalt sätt. Filen är dock fortfarande lagrad på hårddisken tills den skrivs över, då du kopierar nya filer.

Bitdefender File Shredder hjälper dig att radera data och fysiskt ta bort dem från din hårddisk permanent.

Du kan snabbt strimla filer eller mappar från datorn med Windows-kontextmenyn genom att följa de här stegen:

1. Högerklicka på den fil eller mapp du vill ta bort permanent.
2. Välj **Bitdefender** > **File Shredder** i kontextmenyn som visas.
3. Klicka på **TA BORT PERMANENT** och bekräfta sedan att du vill fortsätta med processen.

   Vänta medan Bitdefender slutför filborttagning.
4. Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.

Alternativt kan du strimla filer från Bitdefender-gränssnittet enligt följande:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **DATASKYDD** klickar du på **File Shredder**.
3. Följ File Shredder-guiden:
   a. Klicka på knappen **LÄGG TILL MAPPAR** för att lägga till filer och mappar du vill ta bort permanent.

      Alternativt drar du dessa filer eller mappar till det här fönstret.
   b. Klicka på **TA BORT PERMANENT** och bekräfta sedan att du vill fortsätta med processen.

      Vänta medan Bitdefender slutför filborttagning.
   c. **Sammanfattning resultat**

      Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.

24. USB IMMUNIZER

Den inbyggda funktionen Autorun i Windows-operativsystem är ett mycket användbart verktyg som gör att datorer automatiskt kör en fil från de medier som är anslutna till den. Till exempel kan programvaruinstallationer startas automatiskt när en CD sätts in i den optiska enheten.

Tyvärr kan den här funktionen även användas av hot för att automatiskt starta och infiltrera din dator från skrivbara medier, som USB-flashenheter och minneskort anslutna via kortläsare. Flera Autorun-baserade attacker har skapats de senaste åren.

Med USB Immunizer kan du förhindra att NTFS-, FAT32- eller FAT.formaterade flashenheter från att automatiskt exekvera hot. När en USB-enhet är immuniserad kan inte hot längre konfigurera den för att köra vissa appar när enheten är ansluten till en dator som kör Windows.

Immunisera en USB-enhet:

1. Anslut flashenheten till datorn.
2. Sök på datorn för att hitta den borttagbara lagringsenheten och högerklicka på dess ikon.
3. I kontextmenyn pekar du på **Bitdefender** och väljer **Immunisera den här enheten**.

> **Notera**
> Om enheten redan är immuniserad visas meddelandet **USB-enheten är skyddad mot autorun-baserade hot** istället för alternativet Immunisera.

För att förhindra datorn från att köra hot från ej immuniserade USB-enheter inaktiverar du funktionen för autokörning av medier. Mer information finns på *"Använda automatisk sårbarhetsövervakning"* (p. 97).

SYSTEMOPTIMERING

25. PROFILER

Dagliga jobbaktiviteter, titta på film eller spela spel kan orsaka att systemet blir långsammare, särskilt om de körs samtidigt med Windows-uppdateringsprocesser och underhållsåtgärder. Med Bitdefender kan du nu välja och tillämpa din föredragna profil, vilket gör att systemjusteringar anpassas för att öka prestandan för specifika installerade appar.

Bitdefender tillhandahåller följande profiler:

- Arbetsprofil
- Filmprofil
- Spelprofil
- Publik Wi-Fi-profil
- Batterilägesprofil

Om du bestämmer dig för att inte använda **Profiler**, aktiveras en standardprofil som heter **Standard** och den skapar ingen optimering för ditt system.

Enligt din aktivitet tillämpas följande produktinställningar när profilerna Arbete, Film eller Spel aktiveras:

- Alla Bitdefendervarningar och popups är inaktiverade.
- Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Säkhjälp inaktiveras.
- Meddelanden om specialerbjudanden inaktiveras.

Enligt din aktivitet tillämpas följande systeminställningar när profilerna Arbete, Film eller Spel aktiveras:

- Automatiska uppdateringar för Windows skjuts upp.
- Windows-varningar och popups är inaktiverade.
- Onödiga bakgrundsprogram stängs av.
- Visuella effekter justeras för bästa prestanda.
- Underhållsåtgärder skjuts upp.

- Energiplansinställningar justeras.

När den körs i profilen publik Wi-Fi är Bitdefender Antivirus Plus inställd på att automatiskt uppnå följande programinställningar:

- Advanced Threat Defense är aktiverat
- Följande inställningar från Förebyggande av onlinehot är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägeri
  - Skydd mot nätfiske

25.1. Arbetsprofil

Att köra flera uppgifter på jobbet, som att skicka e-post, ha en videokommunikation med avlägsna kollegor eller arbeta med att designa appar kan påverka systemprestanda. Arbetsprofilen har designats för att hjälpa dig förbättra din arbetseffektivitet, genom att stänga av vissa av dina bakgrundstjänster och underhållsuppgifter.

Konfigurera Arbetsprofil

Konfigurera de åtgärder som ska vidtas när Arbetsprofil används:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Arbetsprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Ökar prestanda på arbetsappar
   - Optimera produktinställningar för arbetsprofil
   - Skjut upp bakgrundsprogram och underhållsuppgifter
   - Skjut upp Windows automatiska uppdateringar
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till appar manuellt till arbetsprofillistan

Om Bitdefender inte automatiskt laddar Jobbprofil när du startar en viss jobbapp, kan du manuellt lägga till appen till **listan Jobbappar**.

Lägga till appar i listan Jobbprogram i Jobbprofil manuellt:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Arbetsprofil.
4. I fönstret **Inställningar av jobbprofil** klickar du på **Programlista**.
5. Klicka på **LÄGG TILL**.

   Ett nytt fönster visas. Bläddra till appens exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

25.2. Filmprofil

Att visa högkvalitativt videoinnehåll, som HD-filmer, kräver mycket systemresurser. Filmprofil justerar system- och produktinställningar så att du kan njuta av en oavbruten och smidig filmupplevelse.

Konfigurera filmprofil

Konfigurera de åtgärder som ska vidtas när filmprofil används:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området filmprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på videospelare
   - Optimera produktinställningar för filmprofil
   - Skjut upp bakgrundsprogram och underhållsuppgifter
   - Skjut upp Windows automatiska uppdateringar
   - Justera energiplansinställningar för filmer
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till videospelare till listan Filmprofil manuellt

Om Bitdefender inte automatiskt laddar Filmprofil när du startar en viss videospelarapp, kan du manuellt lägga till appen till **listan Filmappar**.

Lägga till videospelare till listan Filmappar i Filmprofil manuellt:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området filmprofil.
4. I fönstret **Inställningar av filmprofil** klickar du på **Spelarlista**.
5. Klicka på **LÄGG TILL**.

   Ett nytt fönster visas. Bläddra till appens exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

25.3. Spelprofil

Att njuta av en oavbruten spelupplevelse handlar om att minska spelbelastningen och minska nedgångar. Genom att använda beteendemässig heuristik tillsammans med en lista med kända spel kan Bitdefender automatiskt upptäcka spel som körs och optimera dina systemresurser så att du kan njuta av din spelstund.

Konfigurera spelprofil

Konfigurera de åtgärder som ska vidtas när spelprofil används:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området spelprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på spel
   - Optimera produktinställningar för spelprofil
   - Skjut upp bakgrundsprogram och underhållsuppgifter
   - Skjut upp Windows automatiska uppdateringar
   - Justera energiplansinställningar för spel

5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till spel manuellt till spellistan

Om Bitdefender inte automatiskt laddar Spelprofil när du startar ett visst spel eller app, kan du manuellt lägga till appen till **listan Spelappar**.

Lägga till spel i listan Spelappar i Spelprofil manuellt:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området spelprofil.
4. I fönstret **Inställningar av spelprofil** klickar du på **Spellista**.
5. Klicka på **LÄGG TILL**.

   Ett nytt fönster visas. Bläddra till spelets exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

25.4. Publik Wi-Fi-profil

Att skicka e-post, skriv in känsliga personuppgifter eller shoppa online medan du är ansluten till osäkra trådlösa nätverk kan utsätta din personliga information för risk. Publik Wi-Fi-profil justerar produktinställningar för att ge dig möjlighet att göra betalningar online och använda känslig information i en skyddad miljö.

Konfigurera publik Wi-Fi-profil

För att konfigurera Bitdefender att använda produktinställningar när du är ansluten till ett osäkert trådlöst nätverk:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Publik Wi-Fi-profil.
4. Låt kryssrutan **Justerar produktinställningar för att öka skyddet när du är ansluten till ett osäkert publikt Wi-Fi-nätverk** vara markerad.
5. Klicka **Spara**.

25.5. Batterilägesprofil

Batterilägesprofil är specialdesignad för användare av bärbar dator och surfplatta. Dess syfte är att minimera både system- och Bitdefender-inverkan på strömförbrukning när batteriladdningsnivån är lägre än standard eller den du valt.

Konfigurera batterilägesprofil

Konfigurera batterilägesprofil:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Batterilägesprofil.
4. Välj de systemjusteringar som ska tillämpas genom att markera följande alternativ:
   - Optimera produktinställningar för batteriläge.
   - Skjut upp bakgrundsprogram och underhållsuppgifter.
   - Skjut upp Windows automatiska uppdateringar.
   - Justera energiplansinställningar för batteriläge.
   - Inaktivera externa enheter och nätverksportar.
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Skriv in ett giltigt läge i listrutan eller välj ett med upp- och nedpilarna för att ange när systemet ska gå över till batteriläge. Som standard aktiveras läget när batteriladdningsnivån faller lägre än 30 %.

Följande produktinställningar tillämpas när Bitdefender drivs av batterilägesprofilen:

- Bitdefender Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Säkerhetswidget är avstängd.

Bitdefender upptäcker när din bärbara dator har växlat till batterikraft och utifrån batteriladdningsnivån går den automatiskt över till batteriläge. På samma sätt går Bitdefender automatiskt ur Batteriläge när det upptäcker att den bärbara datorn inte längre körs på batteri.

25.6. Realtidsoptimering

Bitdefender Realtidsoptimering är ett insticksprogram som förbättrar systemprestanda tyst, i bakgrunden, och ser till att du inte blir avbruten när du är i ett profilläge. Beroende på CPU-belastningen övervakar insticksprogrammet alla processer, med fokus på dem som tar upp en högre belastning, för att justera dem efter dina behov.

Aktivera eller inaktivera realtidsoptimering:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Bläddra ned tills du ser alternativet Realtidsoptimering och använd sedan motsvarande omkopplare för att aktivera eller inaktivera.

FELSÖKNING

26. LÖSA VANLIGA PROBLEM

Det här kapitlet presenterar några problem du kan stöta på när du använder Bitdefender och tillhandahåller dig med möjliga lösningar till dessa problem. De flesta av dessa problem kan lösas genom passande konfigurering av produktinställningarna.

Om du ej kan finna ditt problem här eller om den valda lösningen inte fungerar kan du kontakta Bitdefender representanter för teknisk support som visat i kapitlet *"Be om hjälp"* (p. 157).

26.1. Mitt system verkar vara långsamt

Vanligtvis när man installerat ett säkerhetsprogram, kan det förekomma en liten sänkning av systemhastigheten, detta är i viss grad normalt.

Om du märker en betydande försämring av hastigheten kan bero på något av följande:

- **Bitdefender är inte det enda installerade säkerhetsprogrammet på systemet.**

  Även om Bitdefender söker och tar bort funna säkerhetsprogram under installationen, rekommenderas det att man tar bort alla andra

säkerhetslösningar du använder innan du installerar Bitdefender. Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 66).

- **Minsta systemkrav för att köra Bitdefender är inte uppfyllda.**

  Om din maskin inte uppfyller de minsta systemkraven, kommer datorn att bli trög, särskilt när flera olika appar körs samtidigt. Mer information finns på *"Minsta systemkrav"* (p. 3).

- **Du har installerat appar du inte använder**.

  Alla datorer har program eller appar som inte används. Och många oönskade program körs i bakgrunden vilket tar upp diskutrymme och minne. Om du inte använder ett program, avinstallera det. Det gäller även för annan förinstallerad programvara eller utvärderingsappar du glömt att ta bort.

  > **Viktigt**
  > Om du misstänker att ett program eller en app är en viktig del av ditt operativsystem tar du inte bort det och kontaktar Bitdefenders kundtjänst för att få hjälp.

- **Ditt system kan vara infekterat**.

  Systemets hastighet och allmänna beteende kan också påverkas av hot. Spionprogramvara, skadlig kod, trojaner och adware belastar alla datorns prestanda. Se till att du skannar systemet regelbundet, minst en gång i veckan. Vi rekommenderar att du använder Bitdefender Systemskanning eftersom den skannar efter alla typer av hot som riskerar säkerheten för ditt system.

  Starta systemskanningen:

  1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
  3. Följ guidestegen.

26.2. Skanningen startar inte

Denna typ av problem kan ha två huvudsakliga orsaker:

- **En tidigare Bitdefenderinstallation som inte var helt borttagen eller en felaktig Bitdefenderinstallation**.

I det här fallet installer du om Bitdefender:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klicka på **INSTALLERA OM** i det fönster som visas.
  4. Vänta tills ominstallationen slutförts och starta sedan om ditt system.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **INSTALLERA OM** i det fönster som visas.
  5. Vänta tills ominstallationen slutförts och starta sedan om ditt system.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
  5. Klicka på **INSTALLERA OM** i det fönster som visas.
  6. Vänta tills ominstallationen slutförts och starta sedan om ditt system.

> **Notera**
> Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

- **Bitdefender är inte den enda installerade säkerhetslösningen på ditt system**.

  I det här fallet:

1. Ta bort den andra säkerhetslösningen. Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 66).
2. Installera om Bitdefender:
   - I **Windows 7**:
     a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
     b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
     c. Klicka på **INSTALLERA OM** i det fönster som visas.
     d. Vänta tills ominstallationen slutförts och starta sedan om ditt system.
   - I **Windows 8 och Windows 8.1**:
     a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
     b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
     c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
     d. Klicka på **INSTALLERA OM** i det fönster som visas.
     e. Vänta tills ominstallationen slutförts och starta sedan om ditt system.
   - I **Windows 10**:
     a. Klicka på **Start**, därefter på Inställningar.
     b. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
     c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
     d. Klicka på **Avinstallera** igen för att bekräfta ditt val.
     e. Klicka på **INSTALLERA OM** i det fönster som visas.
     f. Vänta tills ominstallationen slutförts och starta sedan om ditt system.

> **Notera**
> Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

26.3. Jag kan inte längre använda en app

Detta problem inträffar när du försöker använda ett program som fungerade normalt innan du installerade Bitdefender.

När du har installerat Bitdefender kan du stöta på någon av följande situationer:

- Du kan få ett meddelande från Bitdefender om att programmet försöker göra en ändring av systemet.
- Det kan hända att du får ett felmeddelande från programmet du försöker använda.

Detta inträffar när Advanced Threat Defense av misstag anger vissa appar som skadliga.

Advanced Threat Defense är en Bitdefender-funktion som hela tiden övervakar de program som körs på ditt system och rapporterar de med potentiellt skadligt beteende. Eftersom den här funktion baseras på ett heuristiskt system kan det finnas fall då legitima appar rapporteras av Advanced Threat Defense.

När den här situationen kan du undanta respektive app från att övervakas av Advanced Threat Defense.

Lägga till en app i undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Inställningar**.
3. I fönstret **Undantag** klickar du på **Lägg till program till undantag**.
4. Hitta och välj den app du vill ska undantas och klicka sedan på **OK**.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

26.4. Gör så här när Bitdefender blockerar en säker webbplats eller onlineapp

Bitdefender erbjuder en säker surfupplevelse genom att filtrera all webbtrafik och blockera skadligt innehåll. Det är dock möjligt att Bitdefender ser en säker webbplats eller onlineapp som osäker, vilket gör att Bitdefender HTTP-trafikskanning blockerar dem felaktigt.

Om samma sida eller app blockeras flera gånger kan de läggas till i undantagen så att de inte skannas av Bitdefender-motorerna, och därmed säkerställa en smidig surfupplevelse.

Lägga till en webbplats till **Undantag**:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Undantag**.
3. Ange adressen till den blockerade webbplatsen eller onlineappen i motsvarande fält och klicka på **LÄGG TILL**.
4. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Endast webbplatser och appar som du litar fullständigt på ska läggas till i den här listan. Dessa undantas från skanning av följande motorer: hot, nätfiske och bedrägeri.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

26.5. Det här ska du göra om Bitdefender anger en säker app som ransomware

Ransomware är ett skadligt program som försöker tjäna pengar från användarna genom att låsa deras sårbara system. För att hålla systemet säkert för otursamma situationer ger Bitdefender ger dig möjlighet att trygga personliga filer.

När en app försöker ändra eller ta bort en av dina skyddade filer anses den vara osäker och Bitdefender blockerar dess funktionalitet.

Om en sådan app läggs till i listan över ej betrodda appar och du är säker på att den är säker att använda, gör du så här:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.

2. I panelen **SAFE FILES** klickar du på **Programåtkomst**.
3. Apparna som har begärt att ändra filer i dina skyddade mappar listades. Klicka på omkopplaren **Tillåt** bredvid den app du är säker på är säker.

26.6. Så här uppdaterar du Bitdefender på en långsam Internet-anslutning

Om du har en långsam Internet-anslutning (som uppringd) kan fel inträffa under uppdateringsprocessen.

För att se till att systemet är uppdaterat med den senaste Bitdefender-hotinformationsdatabasen:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Uppdatera**.
3. Inaktivera omkopplaren **Tyst uppdatering** switch.
4. Nästa gång en uppdatering är tillgänglig uppmanas du att välja vilken uppdatering du vill ladda ner. Välj endast **Uppdatering av signaturer**.
5. Bitdefender hämtar och installerar bara hotinformationsdatabasen.

26.7. Tjänsterna för Bitdefender svarar inte

Denna artikel hjälper dig att felsöka felet **Bitdefender Tjänster svarar inte**. Du kan få det här problemet på följande sätt:

- Bitdefender-ikonen i systemfältet är utgråad och du informeras om att Bitdefender-tjänsterna inte svarar.
- Bitdefenderfönstret visar att Bitdefenders tjänster inte svarar.

Felet kan vara orsakat av något av följande:

- temporära kommunikationsfel mellan Bitdefendertjänsterna.
- några av Bitdefender tjänster har stoppats
- andra säkerhetslösningar körs på din dator samtidigt som Bitdefender.

För att felsöka detta fel, testa dessa lösningar:

1. Vänta en stund och se om något förändras. Felet kan vara temporärt.

2. Starta om datorn och vänta ett tag tills Bitdefender har laddats. Öppna Bitdefender för att se om felet kvarstår. Omstart av datorn löser oftast problemet.
3. Kontrollera om du har en annan säkerhetslösning installerad då den i så fall kan störa Bitdefender normala aktivitet. Om så är fallet rekommenderar vi dig att ta bort alla andra säkerhetslösningar och sedan installera Bitdefender igen.

   Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 66).

Om felet kvarstår kontaktar du våra supportmedarbetare för hjälp, såsom beskrivs i avsnitt *"Be om hjälp"* (p. 157).

26.8. Funktionen Autofill i min plånbok fungerar inte

Du har sparat dina onlineuppgifter i din Bitdefender Password Manager och du märker att automatisk ifyllnad inte fungerar. Oftast dyker det här problemet upp när Bitdefender-plånbokstilläget inte är installerat i din webbläsare.

Följ de här stegen för att lösa den här situationen:

- I **Internet Explorer:**
  1. Öppna Internet Explorer.
  2. Klicka på Verktyg.
  3. Klicka på Hantera tillägg.
  4. Klicka på Verktygsfält och tillägg.
  5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.
- I **Mozilla Firefox:**
  1. Öppna Mozilla Firefox.
  2. Klicka på Verktyg.
  3. Klicka på Tilläggsprogram.
  4. Klicka på Tillägg.
  5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.
- I **Google Chrome:**
  1. Öppna Google Chrome.

2. Gå till Meny-ikonen.
3. Klicka på Fler verktyg.
4. Klicka på Tillägg.
5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.

Notera
Tillägget aktiveras när du startat om webbläsaren.

Kontrollera nu om funktionen för automatisk ifyllnad i plånboken fungerar för dina onlinekonton.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

26.9. Bitdefender-borttagning misslyckades

Om du vill ta bort din Bitdefender-produkt och märker att processen hänger sig eller systemet fryser, så klickar du på **Avbryt** för att avbryta åtgärden. Om det inte fungerar startar du om systemet.

När borttagning misslyckas kan vissa Bitdefender-registernycklar och filer vara kvar i systemet. Sådana rester kan förhindra en ny installation av Bitdefender. De kan även påverka systemets prestanda och stabilitet.

Gör så här för att helt ta bort Bitdefender från systemet:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klicka på **TA BORT** i det fönster som visas.
  4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

4. Klicka på **TA BORT** i det fönster som visas.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
  5. Klicka på **TA BORT** i det fönster som visas.
  6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

26.10. Mitt system startar inte efter att ha installerat Bitdefender

Om du precis har installerat Bitdefender och inte kan starta om systemet i normalt läge längre kan det finns flera olika orsaker till det här problemet.

Mest troligt är att det orsakas av en tidigare Bitdefender-installation, som inte togs bort korrekt eller av en annan säkerhetslösning som fortfarande finns kvar på systemet.

Så här kan du ta hand om varje situation:

- **Du hade Bitdefender tidigare och du tog inte bort det ordentligt.**

  För att lösa det:

  1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 68) hur du gör det.
  2. Ta bort Bitdefender från ditt system:
     - I **Windows 7**:
       a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
       b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
       c. Klicka på **TA BORT** i det fönster som visas.
       d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

e. Starta om systemet i normalt läge.

- I **Windows 8 och Windows 8.1**:

  a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

  b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.

  c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

  d. Klicka på **TA BORT** i det fönster som visas.

  e. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

  f. Starta om systemet i normalt läge.

- I **Windows 10**:

  a. Klicka på **Start**, därefter på Inställningar.

  b. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.

  c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

  d. Klicka på **Avinstallera** igen för att bekräfta ditt val.

  e. Klicka på **TA BORT** i det fönster som visas.

  f. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

  g. Starta om systemet i normalt läge.

3. Installera om din Bitdefender-produkt.

- **Du hade en annan säkerhetslösning tidigare och du tog inte bort den ordentligt.**

  För att lösa det:

  1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 68) hur du gör det.
  2. Ta bort den andra säkerhetslösningen från systemet:

     - I **Windows 7**:

a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.

b. Hitta namnet på det program du vill ta bort och välj **Ta bort**.

c. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 8 och Windows 8.1**:

  a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

  b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.

  c. Hitta namnet på det program du vill ta bort och välj **Ta bort**.

  d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 10**:

  a. Klicka på **Start**, därefter på Inställningar.

  b. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.

  c. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.

  d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

För att korrekt avinstallera den andra programvaran går du till deras webbplats och kör deras avinstallationsverktyg eller kontaktar dem direkt så att de kan ge dig riktlinjer för avinstallationen.

3. Starta om systemet i normalt läge och installera om Bitdefender.

Du har redan följt stegen ovan och situationen är inte löst.

För att lösa det:

1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 68) hur du gör det.
2. Använd alternativet Systemåterställning från Windows för att återställa datorn till ett tidigare datum innan du installerade Bitdefender-produkten.
3. Starta om systemet i normalt läge och kontakta vår support för hjälp såsom beskriv i avsnitt *"Be om hjälp"* (p. 157).

27. TA BORT HOT FRÅN DITT SYSTEM

Hot kan påverka ditt system på många olika sätt och Bitdefender tillvägagångssätt beror på typen av hotattack. Eftersom hota ofta ändrar sitt beteende är det svårt att bestämma ett mönster för deras beteenden och handlingar.

Det finns situationer när Bitdefender inte automatiskt kan ta bort hotinfektionen från ditt system. I sådana fall krävs en åtgärd av dig.

- *"Bitdefender Räddningsläge (räddningsmiljö i Windows 10)"* (p. 147)
- *"Vad ska du göra när Bitdefender hittar hot på din dator?"* (p. 151)
- *"Hur rensar jag bort ett hot i ett arkiv?"* (p. 152)
- *"Hur rensar jag ett e-postarkiv från hot?"* (p. 153)
- *"Vad gör jag om jag misstänker att en fil är farlig?"* (p. 154)
- *"Vad är de lösenordsskyddade filerna i skanningsloggen?"* (p. 154)
- *"Vad är de överhoppade posterna i skanningsloggen?"* (p. 155)
- *"Vad är de överkomprimerade filerna i skanningsloggen?"* (p. 155)
- *"Varför raderade Bitdefender en infekterad fil automatiskt?"* (p. 155)

Om du ej kan finna ditt problem här eller om den valda lösningen inte fungerar kan du kontakta Bitdefender representanter för teknisk support som visat i kapitlet *"Be om hjälp"* (p. 157).

27.1. Bitdefender Räddningsläge (räddningsmiljö i Windows 10)

Räddningsläge är en Bitdefender-funktion som gör att du kan skanna och desinfektera alla befintliga hårddiskpartitioner inuti och utanför operativsystemet.

När Bitdefender Antivirus Plus installeras på **Windows 7, Windows 8 och Windows 8.1** och Bitdefenders räddningslägesavbildning laddas ner, räddningsläget användas även om du inte längre kan starta i Windows.

I Windows 10 är Bitdefenders räddningsmiljö integrerad med Windows RE, vilket innebär att du inte behöver ladda ner någon räddningslägesavbildning på det här operativsystemet och funktionen kan inte användas för

uppstartsproblem. För att rensa systemet innan Windows-tjänster laddas, rekommenderar vi att använda Bitdefender Rescue CD.

Bitdefender Rescue CD är ett gratisverktyg som skannar och rensar din dator varje gång du misstänker att ett hot påverkar dess funktion. Användbara artiklar innehåller information om hur du skapar och använder den finns på Bitdefender Support Center-plattformen på https://www.bitdefender.com/support/consumer.html.

Hämtar Bitdefender Rescue Mode Image

För att kunna använda räddningsläget i **Windows 7, Windows 8 och Windows 8.1**, måste du först hämta dess avbildningsläget enligt följande:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Räddningsläge**.
3. Klicka på **Ja** i det bekräftelsefönster som visas för att starta om datorn.

   Vänta tills Bitdefender Rescue Mode Image-filen laddas ner från Bitdefender-servrarna. Så fort hämtningsprocessen är avslutad, startar datorn om.

   En meny visas som uppmanar dig att välja ett operativsystem. I det här steget kan du välja att starta ditt system i räddningsläge eller i normalt läge.

Notera
På grund av integrationen med Windows återställningsmiljö i **Windows 10**, finns det inget behov av att ladda ner någon räddningslägesavbildning på det här operativsystemet.

Starta ditt system i räddningsläget i Windows 7, Windows 8 och Windows 8.1

Du kan öppna räddningsläget på ett av två sätt:

Från Bitdefender-gränssnittet

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Räddningsläge**.
3. Klicka på **Ja** i det bekräftelsefönster som visas för att starta om datorn.

4. När datorn startat om visas en meny som uppmanar dig att välja ett operativsystem. Välj **Bitdefender Rescue Mode** för att starta i en Bitdefender-miljö varifrån du kan rensa din Windows-partition.
5. Vid uppmaning trycker du på **Enter** och väljer skärmupplösningen närmast den du normalt använder. Tryck sedan på **Enter** igen.

   Bitdefender Rescue Mode laddas på några minuter.

Starta din dator direkt i räddningsläge

Om Windows inte startar längre kan du starta datorn direkt i Bitdefenders räddningsläge genom att följa stegen nedan:

- I **Windows 7**:
  1. Tryck på **F8** tills skärmen **Avancerade startalternativ** visas.
  2. Använd piltangenterna för att välja Bitdefenders räddningsläge och tryck sedan på **Enter**.

     Bitdefenders räddningsläge laddas om några minuter.
- I **Windows 8 och Windows 8.1**:
  1. Tryck på **Shift**-tangenten tills skärmen **Avancerade startalternativ** visas.
  2. Välj alternativet **Använd ett annat operativsystem** och sedan Bitdefender Rescue Mode.

     Bitdefenders räddningsläge laddas om några minuter.

> **Notera**
> Det är möjligt att starta datorn i räddningsläge endast om räddningslägesavbildningen tidigare har har hämtats såsom beskrivs i "Hämtar Bitdefender Rescue Mode Image" (p. 148).

Starta systemet i räddningsmiljö i Windows 10

Du kan endast komma in i räddningsmiljön från din Bitdefender-produkt enligt följande:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Räddningsläge**.
3. Klicka på **Starta om** i det fönster som visas.

   Bitdefender Rescue Environment laddas på några minuter.

Skanna systemet i räddningsläge (räddningsmiljö i Windows 10)

Skanna systemet i räddningsläge (räddningsmiljö):

- I **Windows 7, Windows 8 och Windows 8.1**:
  1. Öppna räddningsläget såsom beskrivs i "Starta ditt system i räddningsläget i Windows 7, Windows 8 och Windows 8.1" (p. 148).
  2. Bitdefender-logotypen visas och säkerhetslösningsmotorerna börjar kopieras.
  3. Ett välkomstfönster visas. Klicka på **Fortsätt**.
  4. En uppdatering av hotinformationsdatabasen startas.
  5. När uppdateringen är klar visas fönstret Bitdefender On-demand Antivirus Scanner.
  6. Klicka på **Skanna nu**, välj skanningsmål i det fönster som visas och klicka därefter på **Öppna** för att börja skanna.

     Du rekommenderas att skanna hela Windows-partitionen.

     > **Notera**
     > När du arbetar i räddningsläget hanterar du partitionsnamn av Linux-typ. Diskpartitioner visas som sda1 motsvarar troligen (C:) som Windows-typpartition, sda2 motsvarar (D:) och så vidare.

  7. Vänta tills skanningen är klar. Om ett hot upptäcks följer du instruktionerna för att ta bort det.
  8. Avsluta räddningsläget genom att högerklicka på ett tomt område på skrivbordet, välj **Avsluta** i menyn som visas och välj sedan om du vill starta om eller stänga ned datorn.
- I **Windows 10**:
  1. Öppna räddningsmiljön såsom beskrivs i "Starta systemet i räddningsmiljö i Windows 10" (p. 149).
  2. Bitdefender-skanningsprocessen startar automatiskt så fort systemet laddas i räddningsmiljön.
  3. Vänta tills skanningen är klar. Om ett hot upptäcks följer du instruktionerna för att ta bort det.

4. Avsluta räddningsmiljön genom att klicka på knappen **STÄNG** i fönstret med skanningsresultaten.

27.2. Vad ska du göra när Bitdefender hittar hot på din dator?

Du kan få reda på att det finns hot på din dator på något av följande sätt:

- Du skannade din dator och Bitdefender fann infekterade objekt på den.
- En hotvarning meddelar dig om att Bitdefender blockerat ett eller flera hot på din dator.

I dessa situationer uppdaterar du Bitdefender för att försäkra dig om att du har den senaste hotinformationsdatabasen och kör en systemskanning för att analysera systemet.

Så fort systemskanningen är avslutad, väljer du önskad åtgärd för de infekterade objekten (desinficera, radera, flytta till karantän).

Varning
Om du misstänker att en fil är en del av Windows operativsystem eller att det inte är en infekterad fil, följ inte dessa steg utan kontakta Bitdefender kundtjänst så snart som möjligt.

Om vald handling inte kunde utföras och att loggen för skanning visar att en smitta inte kunde tas bort, måste filen (-erna) tas bort manuellt.

Den första metoden kan användas i normalt läge:

1. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.
2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?" (p. 66)* hur du gör det.
3. Bläddra till den infekterade filens plats (sök igenom skanningsloggen) och radera den.
4. Slå på Bitdefender realtids-antivirusskydd.

Om den första metoden misslyckas med att ta bort infektionen:

1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 68) hur du gör det.
2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?"* (p. 66) hur du gör det.
3. Bläddra till den infekterade filens plats (sök igenom skanningsloggen) och radera den.
4. Starta om ditt system och gå in i normalt läge.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

27.3. Hur rensar jag bort ett hot i ett arkiv?

En komprimerad fil innehåller en eller flera filer som packats ihop till ett speciellt format för att spara på diskutrymmet.

Vissa av dessa format är öppna format, och tillhandahåller såvida Bitdefender möjligheten att skanna dem på insidan för att sen vidta passande åtgärder för att ta bort dem.

Andra komprimerade format är delvis eller helt stängda och Bitdefender kan endast hitta hot inuti dem, men kan inte vidta andra åtgärder.

Om Bitdefender meddelar dig om att ett hot upptäckts inuti ett arkiv och att ingen åtgärd är tillgänglig, betyder detta att det inte är möjligt att ta bort hotet på grund av begränsningar av arkivets inställningar för behörigheter.

Så här kan du rensa bort ett hot som lagrats i ett arkiv:

1. Identifiera arkivet som innehåller hotet genom att utföra en Systemskanning av systemet.
2. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.
3. Gå till arkivets plats och dekomprimera det genom att använda en arkiveringsapp, som WinZip.
4. Identifiera den infekterade filen och radera den.

5. Radera det ursprungliga arkivet för att vara säker på att infektionen är fullständigt borttagen.
6. Komprimera filerna i ett nytt arkiv med hjälp av en arkiveringsapp, som WinZip.
7. Slå igång Bitdefenders realtidsskydd och kör en systemskanning för att försäkra dig om att det inte finns någon mer infektion på systemet.

> **Notera**
> Det är viktigt att notera, att ett hot som är lagrat i ett arkiv inte utgör ett omedelbart hot mot ditt system eftersom hotet måste expanderas och verkställas för att kunna infektera ditt system.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

27.4. Hur rensar jag ett e-postarkiv från hot?

Bitdefender kan också identifiera hot i e-postdatabaser och e-postarkiv lagrade på en disk.

Ibland är det nödvändigt att identifiera det infekterade meddelandet, genom att använda den information du fått i skanningsrapporten, och radera det manuellt.

Så här kan du rensa bort ett hot som lagrats i ett e-postarkiv:

1. Skanna e-postdatabasen med Bitdefender.
2. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.
3. Öppna skanningsrapporten och använd identifieringsinformationen (ämne, från, till) från de infekterade meddelandena för att hitta dem i din e-postklient.
4. Radera de infekterade meddelandena. De flesta e-postklienter flyttar även det raderade meddelandet till en återställningsmapp, från vilken meddelandet kan återställas. Du bör försäkra dig om att meddelandet även är raderat från denna återställningsmapp.

5. Komprimera mappen som innehåller det infekterade meddelandet.
   - I Microsoft Outlook 2007: I filmenyn, klicka datafilshantering. Välj de personliga mappar-filerna (.pst) du har tänkt komprimera och klicka sen på inställningar. Klicka på Packa nu.
   - I Microsoft Outlook 2010/2013/2016: På menyn Arkiv klickar du på Info och därefter på Kontoinställningar (Lägg till eller ta bort konton eller ändra befintliga anslutningsinställningar). Klicka sedan på Dataarkiv, välj de personliga mappfiler (.pst) du avser att komprimera och klicka på Inställningar. Klicka på Packa nu.
6. Slå på Bitdefender realtids-antivirusskydd.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 157).

27.5. Vad gör jag om jag misstänker att en fil är farlig?

Du kan misstänka att en fil från ditt system är farlig, även om din Bitdefender-produkt inte upptäckte den.

För vara säker på att ditt system är skyddat:

1. Kör en **Systemskanning** med Bitdefender. Se i *"Hur skannar jag mitt system?"* (p. 54) hur du gör det.
2. Om skanningsresultatet visar sig vara rent, men du fortfarande är tveksam och vill vara säker på filen, kontaktar du vår support så att vi kan hjälpa dig.

   Se i *"Be om hjälp"* (p. 157) hur du gör det.

27.6. Vad är de lösenordsskyddade filerna i skanningsloggen?

Det här är bara ett meddelande som visar att Bitdefender har upptäckt att dessa filer antingen skyddas med ett lösenord eller någon form av kryptering.

De vanligaste lösenordsskyddade posterna är:

- Filer som tillhör en annan säkerhetslösning.
- Filer som hör till operativsystemet.

För att verkligen kunna skanna innehållet, skulle dessa filer behöva antingen extraheras eller på annat sätt avkrypteras.

Skulle dessa innehåll extraheras, skulle Bitdefenderns realtidsskanner automatiskt skanna dem för att hålla din dator skyddad. Om du vill skanna de filerna med Bitdefender måste du kontakta tillverkaren av produkten så att de kan ge dig fler detaljer om filerna.

Vår rekommendation till dig är att ignorera dessa filer då de ej utgör något hot mot ditt system.

27.7. Vad är de överhoppade posterna i skanningsloggen?

Alla filer som visas som överhoppade i skanningsrapporten är rena.

För bättre prestanda skannar inte Bitdefender filer som inte har ändrats sedan den senaste skanningen.

27.8. Vad är de överkomprimerade filerna i skanningsloggen?

De överkomprimerade posterna är delar som inte kunde extraheras av skanningsmotorn, eller delar som det skulle ta för lång tid att dekryptera vilket skulle göra systemet instabilt.

Överkomprimerad betyder att Bitdefender hoppade över skanning av det arkivet eftersom det skulle krävas för stora systemresurser för att packa upp det. Innehållet kommer att skannas i realtid vid behov.

27.9. Varför raderade Bitdefender en infekterad fil automatiskt?

Om en infekterad fil upptäcks, kommer Bitdefender automatiskt att försöka desinficera den. Om desinficering misslyckas flyttas filen till karantän för att innesluta infektionen.

För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

Detta är vanligtvis fallet med installationsfiler som hämtas från opålitliga webbsidor. Om du hamnar i en sådan situation, hämta installationsfilen från tillverkarens webbsida eller annan betrodd webbsida.

KONTAKTA OSS

28. BE OM HJÄLP

Bitdefender erbjuder sina kunder en oöverträffad nivå av snabb och korrekt support. Om du upplever några problem med, eller om du har några frågor om din Bitdefender-produkt kan du använda flera resurser på nätet för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefenders kundtjänst. Våra supportmedarbetare besvarar dina frågor snabbt och ger dig den hjälp du behöver.

Avsnitt *"Lösa vanliga problem"* (p. 135) innehåller den nödvändiga informationen avseende de vanligaste problemen du kan stöta på när du använder den här produkten.

Om du inte svaret på din fråga med de resurser du fått kan du kontakta oss direkt:

- "Kontakta oss direkt från Bitdefender Antivirus Plus" (p. 157)
- "Kontakta oss via vårt onlinesupportcenter" (p. 158)

Kontakta oss direkt från Bitdefender Antivirus Plus

Om du har en fungerande Internet-anslutning kan du kontakta Bitdefender för hjälp direkt från produktgränssnittet.

Följ dessa steg:

1. Klicka på **Support** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Du har följande alternativ:
   - **ANVÄNDARGUIDE**

     Gå till vår databas och sök efter nödvändig information.
   - **SUPPORTCENTER**

     Gå till våra onlineartiklar och videohandledningar.
   - **KONTAKTA SUPPORT**

     Klicka på **KONTAKTA SUPPORT** för att starta Bitdefender-supportverktyget och kontakta kundtjänsten.

     a. Fyll i formuläret med nödvändig information:

        i. Välj vilken typ av problem du upplever.

        ii. Skriv en beskrivning av det problem du stötte på.

iii. Klicka på **FÖRSÖK ATT ÅTERSKAPA DET HÄR PROBLEMET** ifall du stöter på ett produktproblem. Återskapa problemet och klicka därefter på **SLUTFÖR** i ramen ÅTERSKAPA PROBLEMET.

iv. Klicka på **BEKRÄFTA ÄRENDE**.

b. Fortsätt fylla i formuläret med nödvändig information.

i. Skriv ditt fullständiga namn.

ii. Ange din e-postadress.

iii. Markera avtalskryssrutan.

iv. Klicka **SKAPA FELSÖKNINGSPAKET**.

Vänta en stund medan Bitdefender samlar in produktrelaterad information. Denna information kommer att hjälpa våra tekniker att finna en lösning på ditt problem.

c. Klicka på **STÄNG** för att lämna guiden. Du kommer att bli kontaktad så fort som möjligt av en av våra medarbetare.

Kontakta oss via vårt onlinesupportcenter

Om du inte kommer åt nödvändig information via Bitdefender-produkten, gå till vårt onlinesupportcenter:

1. Gå till https://www.bitdefender.com/support/consumer.html.

   Bitdefender Support Center har flera artiklar som innehåller lösningar på Bitdefender-relaterade frågor.

2. Använd sökfältet längst upp i fönstret för att hitta artiklar som kan ge en lösning på ditt problem. För att söka skriver du bara in en term i sökfältet och klickar på **Sök**.

3. Läs de relevanta artiklarna och dokumenten, och prova de föreslagna lösningarna.

4. Om lösningen inte löser ditt problem går du till

   https://www.bitdefender.com/support/contact-us.htmloch kontaktar våra supportmedarbetare.

29. ONLINERESURSER

Flera på nätet-resurser finns tillgängliga för att hjälpa dig med att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefenders supportcenter:

  https://www.bitdefender.com/support/consumer.html

- Bitdefender Supportforum:

  https://forum.bitdefender.com

- Datorsäkerhetsportalen HOTforSecurity:

  https://www.hotforsecurity.com

Du kan även använda din favoritsökmotor för att hitta mer information om datorsäkerhet, Bitdefenderprodukter och företaget.

29.1. Bitdefenders supportcenter

Bitdefenders supportcenter är en databas med information om Bitdefenderprodukter på nätet. Den lagrar, i ett lättåtkomligt format, rapporter om resultaten för utgående teknisk support och felkorrigeringsåtgärder för Bitdefenders support- och utvecklingsteam, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefenders supportcenter är öppet för allmänheten och gratis att söka igenom. Den omfattande information den innehåller är ännu ett sätt att förse Bitdefenders kunder med den tekniska kunskap och insikt de behöver. Alla giltiga begäran om information eller buggrapporter som kommer från Bitdefender-klienter hittar till slut in i Bitdefenders supportcenter, som felkorrigeringsrapporter, workaroundbeskrivningar eller informationsartiklar som tillägg till produkthjälpfiler.

Bitdefendera supportcenter är alltid tillgängligt på

https://www.bitdefender.com/support/consumer.html.

29.2. Bitdefender Supportforum

Bitdefender Supportforum tillhandahåller Bitdefender användare med ett enkelt sätt att få hjälp samt att hjälpa andra.

Om din Bitdefender-produkt inte fungerar som den ska, om den inte kan ta bort specifika hot från din dator eller om du har frågor om hur den fungerar, postar du dina problem eller frågor i forumet.

Bitdefenders supporttekniker söker i forumet efter nya poster för att kunna hjälpa dig. Du kan även få svar eller en lösning från en mer van Bitdefenderanvändare.

Innan du skickar ditt problem eller din fråga, sök igenom forumet efter ett liknande eller relaterat ämne.

Bitdefenders supportforum är tillgängligt på https://forum.bitdefender.com, på 5 olika språk: Engelska, Tyska, Franska, Spanska och Rumänska. Klicka länken **Hemma & Hemma Kontor Skydd** för att öppna sektionen som är avsedd för konsumentprodukter.

29.3. HOTforSecurity Portal

HOTforSecurity är en rik källa till datorsäkerhetsinformation. Här kan du lära dig om olika hot din dator utsätts för när den är ansluten till Internet (skadlig kod, nätfiske, spam, cyberbrottslingar).

Nya artiklar postas regelbundet för att hålla dig uppdaterad med de senaste hot som upptäckts, de nuvarande säkerhetstrenderna och annan information om branschen för datorsäkerhet.

Webbsidan HOTforSecurity är https://www.hotforsecurity.com.

30. KONTAKTUPPGIFTER

Effektiv kommunikation är nyckeln till en framgångsrik affärsverksamhet. Sedan 2001 har BITDEFENDER etablerat ett obestridligt anseende genom att hela tiden sträva efter bättre kommunikation för att överträffa våra klienters och partners förväntningar. Om du har frågor, tveka inte att kontakta oss.

30.1. Webbadresser

Försäljningsavdelning: sales@bitdefender.com
Supportcenter:https://www.bitdefender.com/support/consumer.html
Dokumentation: documentation@bitdefender.com
Lokala återförsäljare:https://www.bitdefender.com/partners
Partnerprogram: partners@bitdefender.com
Mediarelationer: pr@bitdefender.com
Jobbmöjligheter: jobs@bitdefender.com
Virusinlagor: virus_submission@bitdefender.com
Skräppostinlagor: spam_submission@bitdefender.com
Rapportera missbruk: abuse@bitdefender.com
Webbplats:https://www.bitdefender.com

30.2. Lokala återförsäljare

Bitdefenders lokala återförsäljare är redo att svara på alla frågor rörande deras uppgiftsområde, både i kommersiella allmänna ärenden.

För att finna en återförsäljare av Bitdefender i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din ort genom att använda motsvarande alternativ.
3. Om du inte hittar någon Bitdefender-återförsäljare i ditt land får du gärna kontakta oss via e-post på sales@bitdefender.com. Skriv ditt e-postmeddelande på engelska så att vi kan hjälpa dig så snart som möjligt.

30.3. Bitdefender-kontor

Bitdefenders kontor är redo att svara på alla frågor rörande deras verksamhetsområde, både i kommersiella och allmänna ärenden. Deras respektive adresser och kontakter finns listade nedanför.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (office&sales): 1-954-776-6262
Försäljning: sales@bitdefender.com
Tekniskt stöd: https://www.bitdefender.com/support/consumer.html
Webb: https://www.bitdefender.com

UK och Irland

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-post: info@bitdefender.co.uk
Telefon: (+44) 2036 080 456
Försäljning: sales@bitdefender.co.uk
Tekniskt stöd: https://www.bitdefender.co.uk/support/
Webb: https://www.bitdefender.co.uk

Tyskland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Office: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Försäljning: vertrieb@bitdefender.de
Tekniskt stöd: https://www.bitdefender.de/support/consumer.html
Webb: https://www.bitdefender.de

Danmark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Office: +45 7020 2282
Tekniskt stöd: http://bitdefender-antivirus.dk/
Webb: http://bitdefender-antivirus.dk/

Spanien

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Försäljning: comercial@bitdefender.es
Tekniskt stöd: https://www.bitdefender.es/support/consumer.html
Webbplats: https://www.bitdefender.es

Rumänien

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax: +40 21 2641799
Försäljning Telefon: +40 21 2063470
Försäljnings-e-post: sales@bitdefender.ro
Tekniskt stöd: https://www.bitdefender.ro/support/consumer.html
Webbplats: https://www.bitdefender.ro

Förenade Arabemiraten

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Försäljning Telefon: 00971-4-4588935 / 00971-4-4589186
Försäljnings-e-post: mena-sales@bitdefender.com
Tekniskt stöd: https://www.bitdefender.com/support/consumer.html
Webbplats: https://www.bitdefender.com

Ordlista

Abonnemang

Köpeavtal som ger användaren behörighet att använda en viss produkt eller tjänst på ett visst antal enheter och för en viss tidsperiod. En utgången prenumeration kan automatiskt förnyas med den information som användaren uppger vid det första köpet.

ActiveX

ActiveX är ett sätt att skriva program på så att andra program kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och uppför sig som datorprogram mer än statiska sidor. med ActiveX kan användare ställa eller besvara frågor, använda knappar och interagera på andra sätt med webbsidan. ActiveX-kontroller är ofta skrivna i Visual Basic.

Active X är känt för total avsaknad av säkerhetskontroller; experter på datorsäkerhet avråder från att använda det på Internet.

Aktiveringskod

Det är en unik nyckel som kan köpas från återförsäljare och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av en giltig prenumeration för en viss tidsperiod och antal enheter och kan också användas för att förlänga en prenumeration med villkoret att genereras för samma produkt eller tjänst.

Annonsprogram

Annonsprogram kombineras ofta med ett värdprogram som är gratis så länge som användaren går med på att tillåta annonsprogrammet. Eftersom sådana program oftast installeras efter att användaren gått med på licensavtalet, har inget brott begåtts.

Popup-reklam kan dock bli ett irritationsmoment, och i vissa fall försämra systemets prestanda. Även den privata information som vissa av dessa program samlar in kan vara oroande för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En skiva, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera komprimerade filer.

Avancerat kvarstående hot

APT (Advanced persistent threat) exploaterar säkerhetsrisker i system för att stjäla viktig information att leverera till källan. Stora grupper som organisationer, företag eller myndigheter, är måltavlor för detta hot.

Målet med ett APT är att förbli oupptäckt under en lång tid för att kunna övervaka och samla in viktig information utan att skada målmaskinerna. Den metod som används är att injicera hotet i nätverket via en PDF-fil eller ett Office-dokument som ser ofarligt ut så att alla användare kan köra filerna.

Bakdörr

Ett hål i säkerhetssystemet som avsiktligen lämnats av de som utformat och underhåller systemet. Meningen med sådana hål är inte alltid ondskefull, till exempel, "come out of the box with privileged accounts" är menat för fälttekniker eller för försäljarens underhållsprogrammerare.

Boot virus

Ett hot som infekterar startsektorn på en fast eller flyttbar disk. Ett försök att starta från en diskett infekterad med ett startsektorvirus gör att viruset blir aktivt i minnet. Varje gång du startar ditt system från och med nu innebär att du har hotet aktivt i minnet.

Bootsektor:

En sektor i början av varje enhet som identifierar enhetens arkitektur (sektorstorlek, klusterstorlek osv). För startenheter innehåller boot-sektorn även ett program laddar operativsystemet.

Botnet

Termen “botnet” är sammansatt av orden “robot” och “nätverk”. Botnets är Internet-anslutna enheter infekterade med hot och som kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogramvara, ransomware och andra typer av hot. Deras mål är att infektera sp många anslutna enheter som möjligt, som datorer, servrar, mobil- eller IoT-enheter som tillhör stora företag eller industrier.

E-post

Elektronisk post. En tjänst som sänder datormeddelanden via lokala eller globala nätverk.

E-postklient
En e-postklient är en app som låter dig sända och ta emot e-postmeddelanden.

Falska positiva
Inträffar när en skanning identifierar en fil som ett hot när den i själva verket inte är det.

Filändelse
Den del av ett filnamn, som kommer efter sista punkten, som visar vilken typ av data som finns lagrad på filen.

Många operativsystem använder sig av filändelser,t.ex. Unix, VMS, och MS-DOS. De består oftast av en till tre bokstäver (vissa sorgliga gamla operativsystem har inte stöd för mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Hämta
För att kopiera data (vanligtvis en hel fil) från en huvudkälla till en fjärrenhet. Termen används ofta för att beskriva processen att kopiera en fil från en tjänst på nätet till sin egen dator. Hämta kan även hänvisa till att kopiera en fil från en nätverksfilserver till en dator på nätverket.

Händelser
En åtgärd eller händelse som upptäckts av ett program. Händelser kan vara användaråtgärder, som att klicka på en musknapp eller trycka på en tangent, eller systemhändelser, som att få slut minnesutrymme.

Hårddisk
Det är en maskin som läser data från, och skriver data till en skiva.

En hårddisk skriver och läser hårddiskar.

En diskettenhet har tillgång till disketter.

Diskar kan antingen vara interna (inuti ett datorchassi) eller externa (inuti en mindre extern låda som ansluts till en dator).

Heuristiskt
En regelbaserad metod för att identifiera nya hot. Den här skanningsmetoden förlitar sig inte på en specifik hotinformationsdatabas. Fördelen med den heuristiska skanningen är att den inte luras av en ny variant av ett befintligt hot. Det kan dock hända

att den ibland rapporterar misstänkta koder i vanliga program, genererar de så kallade "falsk positiv".

Honungsfälla

Ett lockbetessystem som konfigureras för att locka hackare för att studera hur de agerar och identifiera vilka metoder de använder för att samla in systeminformation. Företag och koncerner är mer intresserade av att implementera och använda honungsfällor för att förbättra sin allmänna säkerhetsstatus.

Hot

Ett program eller en kod som utan din vetskap laddas upp till din dator mot din vilja. De flesta virus kan även kopiera sig själva. Alla datorvirus är tillverkade av människor. Ett simpelt virus som kan kopiera sig själv om och om igen är relativt lätt att tillverka. Även ett sådant simpelt virus är farligt eftersom det snabbt kommmer att använda upp allt ledigt minnesutrymme och orsaka en systemkrasch. Ett ännu farligare typ av virus är ett virus som kan sända sig själv via nätverk och ta sig förbi säkerhetssystem.

Icke-heuristiskt

Den här skanningsmetoden förlitar sig på en specifik hotinformationsdatabas. Fördelen med icke-heuristisk skanning är att den inte låter sig luras av vad som kan se ut som ett hot och genererar inte falska alarm.

IP

Internetprotokoll - Ett routabelt protokoll i TCP/IP som ansvarar för IP-adressering, routing, och fragmenteringen och återmonteringen av IP-paket.

Java-applet

Ett Java-program som är konstruerat för att endast köras på en webbsida. För att använda en applet på en webbsida måste du ange namnet op appleten och storleken (längd och bredd, i pixlar) som appleten kan använda. När webbsidan öppnas laddar webbläsaren ner appleten från en server och kör den på användarens maskin (klienten). Appletar skiljer sig från appar eftersom de styrs av ett strikt säkerhetsprotokoll.

Till exempel, fastän applets körs på klienten kan de inte läsa eller skriva data till klientens maskin. Dessutom är applets mer begränsade till att endast kunna läsa och skriva data från samma domän de kommer ifrån.

Kaka

I Internet-branschen beskrivs cookies som små filer som innehåller information om individuella datorer, som kan analyseras och användas av annonsörer för att följa vad du gör och dina intressen på nätet. Inom detta område utvecklas cookie-teknologin fortfarande, och målet är att kunna rikta annonser direkt mot vad su sagt att du är intresserad av. För många är det ett tveeggat svärd då det å ena sidan är effektivt och relevant eftersom man bara ser annonser om sådant man är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" dina aktviteter. Förståeligt nog så finns det en debatt om privatliv, och många människor känner sig kränkta av känslan att de behandlas som en EAN-kod (du vet streckkoden på baksidan av förpackningar som skannas i matbutiken). Även om detta sätt att se på saken kan vara extremt, så är det i vissa fall sant.

Keylogger

En keylogger är en app som loggar allt du skriver.

Keyloggers är inte skadliga till sin natur. De kan användas i legitima syften, som att övervaka anställdas eller barns aktivitet. De används dock mer och mer av cyberbrottslingar för skadliga syften (till exempel för att samla in privat information, som inloggningsuppgifter och personnummer).

Kommandorad

I ett kommandorads-gränssnitt skriver användaren kommandon i utrymmet som finns direkt på skärmen genom att använda kommandospråk.

Komprimerade program

En fil i komprimerat format. Många operativsystem och appar innehåller kommandon som gör att du kan komprimera en fil så att den tar upp mindre minne. Till exempel, säg att du har en textfil som innehåller tio blanksteg på varandra. Detta skulle normalt kräva tio bytes lagringsutrymme.

Dock skulle ett program som komprimerar filer ersätta blankstegen med ett speciellt tecken för blanksteg följt av hur många blanksteg som ersätts. I detta fall kommer de tio stegen endast kräva två bytes utrymme. Detta är bara en komprimeringsmetod - det finns många fler.

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, har stöd för kraftfulla makrospråk.

Dessa appar tillåter dig att bädda in ett makro i ett dokument samt låter makrot köras varje gång dokumentet öppnas.

Mask

Ett program som sprider sig själv över ett nätverk och reproducerar sig självt efter hand. Det kan inte fästa sig till andra program.

Minne

Interna lagringsytor på datorn. Med termen minne menas lagring av information i kretsar, och ordet lagring används för minne som finns på band eller diskar. Till varje dator följer det en viss mängd fysiskt minne, vilket brukar kallas för internminne eller RAM-minne.

Phishing

Att skicka ett e-postmeddelanden till en användare och utge sig för att vara ett legitimt företag i ett försök att lura användaren att uppge privat information som kan användas för identitetsstöld. E-postmeddelandet skickar användaren till en webbsida där de ombes uppdatera personlig information, som lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och endast uppsatt för att stjäla användarens information.

Photon

Photon är en innovativ, ej störande Bitdefender-teknik, konstruerat för att minimera prestandainverkan för din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den ett användningsmönster som bidrar till att optimera start- och skanningsprocesser.

Polymorfa Virus

Ett virus som ändrar form med varje fil det smittar. Eftersom det inte har något konsekvent binärt mönster är sådana virus svåra att identifiera.

Port

En dators gränssnitt till vilket du kan ansluta en enhet. Hemdatorer har olika sorters portar. Internt finns flera portar för anslutning av diskenheter, skärmar och tangentbord. Externt finn portar för anslutning av modem, skrivare, möss och andra externa enheter.

I TCP/IP- och UDP-nätverk, en slutpunkt till en logisk anslutning. Portnumret identifierar vilken typ av port det är. Till exempel används port 80 för HTTP-trafik.

Ransomware

Ransomware är ett skadligt program som försöker tjäna pengar från användarna genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall är några varianter som jagar personliga användarsystem.

Infektionen kan spridas genom att öppna skräppostmeddelanden, hämta e-postbilagor eller installera appar, utan att låta användaren vet vad som händer på deras system. Varje dag utsätts användare och företag för ransomwarehackare.

Rapportera fil

En fil som listar inträffade åtgärder. Bitdefender underhåller en rapportfil som listar den skannade sökvägen, de mappar, antal filer och arkiv som skannats, hur många infekterade och misstänkta filer som hittats.

Script

En annan term för makro eller batch-fil, ett script är en lista med kommandon som kan utföras utan användarens medverkan.

Skräppost

Elektronisk skräppost eller skräp nyhetsgruppsinlägg. Generellt känt som oönskade e-postmeddelanden.

Sökväg

Exakt anvisning till en fil på en dator. Dessa anvisningar är vanligtvis beskrivna i ett hierarkiskt katalogsystem uppifrån och nedåt.

Vägen mellan två punkter, exempelvis vägen för kommunikation mellan två datorer.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens Internetuppkoppling utan hans eller hennes vetande, vanligen ur reklamsyfte. Spionprogram är vanligtvis paketerat som en dold komponent i gratisprogram eller delningsprogram som kan laddas ner från Internet; det bör dock noteras att majoriteten av gratisprogrammen och delningsprogrammen inte bär på spionprogram. När det väl installerats så övervakar spionprogrammet användarens aktiviteter på Internet och skickar i bakgrunden denna information till någon annan. Spionprogram kan även samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med Trojanska hästar är att användare ovetande installerar produkten när de installerar något annat. Ett vanligt sätt att falla offer för spionprogram är att hämta vissa pir till pir fildelningsprodukter som finns tillgängliga idag.

Förutom frågorna om etik och sekretess stjäl spionprogram från användaren genom att använda datorns minnesresurser och ta upp bandbredd när den sänder tillbaka information till sin hemmabas via användarens Internetanslutning. Eftersom spionprogram använder minnes- och systemresurser kan de program som körs i bakgrunden leda till systemkrasch eller generell systeminstabilitet.

Spökprogram

Ett rootkit är en uppsättning programvaruverktyg som erbjuder administratörsnivååtkomst till ett system. Termen användes från början av operativsystemet UNIX och refererade till ombyggnadsverktyg som gav inkräktare administrativa rättigheter och lät dem dölja sin närvaro för att inte upptäckas av systemadministratörerna.

Den huvudsakliga uppgiften för spökprogram är att gömma processer, filer, inloggningsuppgifter och loggar. De kan även snappa upp information från terminaler, nätverksanslutningar och externa enheter om de lyckas nästla sig in i "rätt" program.

Spökprogram är inte naturligt skadliga. Till exempel gömmer system och även vissa program kritiska filer genom att använda spökprogram. De används dock oftast för att dölja hot eller för att dölja närvaron av

en inkräktare i systemet. När de kombineras med hot utgör rootkits ett stort hot till systemets integritet och säkerhet. De kan övervaka trafik, skapa bakdörrar in i system, ändra filter och loggar för att undgå upptäckt.

Startposter

Alla filer som placeras i denna mapp kommer att öppnas när datorn startas. Till exempel, en startskärm, en ljudfil som ska spelas upp när datorn först startar, en påminnelsekalender eller appar kan vara uppstartsobjekt. Vanligen placeras ett alias för filen i mappen istället för den aktuella filen.

Systemfältet

Introducerat med Windows 95, finns systemfältet i Windows aktivitetsfält (vanligtvis längst ner vid klockan) och innehåller miniatyrikoner för enkel tillgång till systemfunktioner såsom fax, skrivare, modem, volym och mer. Dubbelklicka eller högerklicka en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Överföringskontroll/Internetprotokoll - En uppsättning nätverksprotokoll som ofta används på Internet och erbjuder kommunikation över sammankopplade datornätverk med diverse maskinvaruarkitekturer och operativsystem. TCP/IP omfattar standard för hur datorer kommunicerar och konvent för anslutna nätverk och routing-trafik.

Trojansk

Ett destruktivt program som maskerar sig som ett godartat. Till skillnad från skadliga program och maskar kan inte trojaner kopiera sig själva, men de kan vara minst lika destruktiva. Ett av de mest försåtliga typerna av trojaner är ett program som gör anspråk på att rensa datorn från hot, men istället inför hot på datorn.

Termen kommer från en berättelse i Homeros Illiaden där Grekerna ger en enorm trähäst till sina fiender Trojanerna, skenbart en fredsgåva. Men när Trojanerna dragit hästen innanför murarna så smyger Grekiska soldater ut ur hästens mage och öppnar porten till staden så deras kamrater kan välla in och ta över Troja.

Uppdatera

En ny version av programvara eller maskinvara utformad för att ersätta äldre versioner av samma produkt. Dessutom kontrollerar ofta installations-rutinerna för uppdatering, din dator för att vara säker på att en äldre version redan finns installerad på din dator; om inte, kan du installera uppdateringen.

Bitdefender har sin egen uppdateringsmodul som låter dig manuellt kontrollera efter uppdateringar, eller automatiskt låter den uppdatera produkten.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att hitta och ta bort hotet.

Utforskaren

Kort för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare omfattar Microsoft Internet Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare vilket betyder att de kan visa både grafik och text. Dessutom kan de flesta moderna webbläsare visa multimediainformation som inkluderar ljud och bild, även om det för vissa format krävs insticksprogram.

Virtual Private Network (VPN)

Är en teknik som aktiverar en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka data och svårt för snokare att få tag på dem. Ett bevis på säkerheten är autentiseringen, som endast kan göras med ett användarnamn och lösenord.