Bitdefender ANTIVIRUS PLUS

ANVÄNDARMANUAL

Bitdefender Antivirus Plus

Användarmanual

Publiceringsdatum 2023-12-04

Rättsligt meddelande

Bitdefender®

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla Windows-användare som har valt Bitdefender Antivirus Plus som en säkerhetslösning för sina datorer. Informationen som presenteras i den här boken är inte bara lämplig för datorvana, den är tillgänglig för alla som kan arbeta med en Windows-dator.

Du kommer att få reda på hur du konfigurerar och använder Bitdefender Antivirus Plus för att skydda dig mot hot och annan skadlig programvara. Du kommer att lära dig hur du får ut det bästa av din Bitdefender.

Vi önskar dig en trevlig och användbar föreläsning.

Hur man använder den här guiden

Den här guiden är organiserad kring flera viktiga ämnen:

Komma igång (sida 13)

Kom igång med Bitdefender Antivirus Plus och dess användargränssnitt.

Hantera din säkerhet (sida 44)

Lär dig hur du använder Bitdefender Antivirus Plus för att skydda dig mot skadlig programvara.

Hur (sida 96)

Läs mer om Bitdefender Antivirus Plus.

Få hjälp (sida 140)

Var man ska leta och var man kan be om hjälp om något oväntat dyker upp.

Konventioner som används i denna guide

Typografiska konventioner

Flera textstilar används i den här guiden för att förbättra läsbarheten. Deras aspekt och betydelse presenteras i tabellen nedan.

Utseende	Beskrivning
`sample syntax`	Syntaxexempel skrivs ut med `monospaced` tecken.
https://www.bitdefender.com	URL-länken pekar på någon extern plats, på http- eller ftp-servrar.
documentation@bitdefender.com	E-postadresser infogas i texten för kontaktinformation.
Om den här guiden (sida 1)	Detta är en intern länk till någon plats i dokumentet.
`filename`	Filer och kataloger skrivs ut med `monospaced` font.
alternativ	Alla produktalternativ skrivs ut med hjälp av **djärv** tecken.
nyckelord	Viktiga sökord eller fraser markeras med hjälp av **djärv** tecken.

Förmaningar

Förmaningarna är anteckningar i texten, grafiskt markerade, som uppmärksammar dig på ytterligare information relaterad till det aktuella stycket.

Notera

Anteckningen är bara en kort observation. Även om du kan utelämna det, kan anteckningarna ge värdefull information, som specifik funktion eller en länk till något relaterat ämne.

Viktig

Detta kräver din uppmärksamhet och rekommenderas inte att hoppa över det. Vanligtvis ger den icke-kritisk men betydande information.

Varning

Detta är viktig information som du bör behandla med ökad försiktighet. Inget dåligt kommer att hända om du följer anvisningarna. Du bör läsa och förstå den, för den beskriver något extremt riskabelt.

Begäran om kommentarer

Vi inbjuder dig att hjälpa oss att förbättra boken. Vi har testat och verifierat all information efter bästa förmåga. Skriv för att berätta för oss om eventuella brister du hittar i den här boken eller hur du tror att den kan förbättras, för att hjälpa oss att förse dig med bästa möjliga dokumentation.

Meddela oss genom att skicka ett mejl till documentation@bitdefender.com. Skriv alla dina dokumentationsrelaterade e-postmeddelanden på engelska så att vi kan behandla dem effektivt.

1. INSTALLATION

1.1. Förbereder för installation

Innan du installerar Bitdefender Antivirus Plus, slutför dessa förberedelser för att säkerställa att installationen går smidigt:

- Se till att enheten där du planerar att installera Bitdefender uppfyller systemkraven. Om enheten inte uppfyller alla systemkrav kommer Bitdefender inte att installeras eller, om den är installerad, kommer den inte att fungera korrekt och det kommer att orsaka systemavbrott och instabilitet. För en fullständig lista över systemkrav, se Systemkrav (sida 3).
- Logga in på enheten med ett administratörskonto.
- Ta bort annan liknande programvara från enheten. Om någon upptäcks under Bitdefender-installationsprocessen kommer du att meddelas om att avinstallera den. Att köra två säkerhetsprogram samtidigt kan påverka deras funktion och orsaka stora problem med systemet. Windows Defender kommer att inaktiveras under installationen.
- Inaktivera eller ta bort eventuella brandväggsprogram som kan köras på enheten. Att köra två brandväggsprogram samtidigt kan påverka deras funktion och orsaka stora problem med systemet. Windows-brandväggen kommer att inaktiveras under installationen.
- Det rekommenderas att din enhet är ansluten till internet under installationen, även från en CD/DVD. Om nyare versioner av appfilerna som ingår i installationspaketet är tillgängliga kan Bitdefender ladda ner och installera dem.

1.2. Systemkrav

Du kan installera Bitdefender Antivirus Plus endast på enheter som kör följande operativsystem:

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

- 2,5 GB ledigt ledigt hårddiskutrymme (minst 800 MB på systemenheten)
- 2 GB minne (RAM)

Viktig
Systemprestandan kan påverkas på enheter som har gamla generationens processorer.

Notera
För att ta reda på vilket Windows-operativsystem din enhet körs och hårdvaruinformation:

- I **Windows 7**, Högerklicka **Min dator** på skrivbordet och välj sedan **Egenskaper** från menyn.
- I **Windows 8**, från startskärmen i Windows, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt på startskärmen) och sedan högerklicka på dess ikon. I **Windows 8.1**, lokalisera **Denna PC**.
  Välj **Egenskaper** i bottenmenyn. Titta i **Systemet** område för att hitta information om din systemtyp.
- I **Windows 10**, typ **Systemet** i sökrutan från aktivitetsfältet och klicka på dess ikon. Titta i **Systemet** område för att hitta information om din systemtyp.

1.3. Programvarukrav

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

- Microsoft Edge 40 och högre
- Internet Explorer 10 och senare
- Mozilla Firefox 51 och senare
- Google Chrome 34 och senare
- Microsoft Outlook 2007/2010/2013/2016
- Mozilla Thunderbird 14 och högre

1.4. Installera din Bitdefender-produkt

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet som laddats ner på din enhet från Bitdefender Central.

Om ditt köp omfattar mer än en enhet, upprepa installationsprocessen och aktivera din produkt med samma konto på varje enhet. Kontot du behöver använda är det som innehåller din aktiva Bitdefender-prenumeration.

1.4.1. Installera från Bitdefender Central

Från Bitdefender Central kan du ladda ner installationssatsen som motsvarar den köpta prenumerationen. När installationsprocessen är klar, Bitdefender Antivirus Plus är aktiverad.

Att ladda ned Bitdefender Antivirus Plus från Bitdefender Central:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
3. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Spara installationsfilen.
   - **Skydda andra enheter**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Klick **SKICKA NEDLADDNINGSLÄNK**.
     c. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**.
     Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
     d. På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.
4. Vänta tills nedladdningen är klar och kör sedan installationsprogrammet.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om ditt system inte uppfyller systemkraven för att installera Bitdefender kommer du att informeras om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender upptäcks kommer du att uppmanas att ta bort den från ditt system. Följ anvisningarna för att ta bort programvaran från ditt system, så att du undviker problem som uppstår senare. Du kan behöva starta om enheten för att slutföra borttagningen av upptäckta säkerhetslösningar.

Installationspaketet för Bitdefender Total Security uppdateras ständigt.

> **Notera**
> Att ladda ner installationsfilerna kan ta lång tid, särskilt över långsammare internetanslutningar.

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

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren som du får använda Bitdefender Antivirus Plus.

Om du inte godkänner dessa villkor, stäng fönstret. Installationsprocessen kommer att överges och du kommer att avsluta installationen.

Två ytterligare uppgifter kan utföras i detta steg:

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

Klick **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills installationen är klar. Detaljerad information om framstegen visas.

Steg 3 - Installationen slutförd

Din Bitdefender-produkt har installerats.

En sammanfattning av installationen visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av systemet krävas.

Steg 4 - Enhetsanalys

Du kommer nu att bli tillfrågad om du vill utföra en analys av din enhet för att säkerställa att den är säker. Under detta steg kommer Bitdefender att skanna kritiska systemområden. Klick **Starta enhetsanalys** att initiera det.

Du kan dölja skanningsgränssnittet genom att klicka på **Kör Scan i bakgrunden**. Därefter väljer du om du vill bli informerad när skanningen är klar eller inte.

Klicka på när skanningen är klar **Öppna Bitdefender-gränssnittet**.

> **Notera**
> Alternativt, om du inte vill utföra skanningen kan du helt enkelt klicka på **Hoppa**.

Steg 5 - Kom igång

I den **Komma igång** fönster kan du se detaljer om din aktiva prenumeration.

Klick **AVSLUTA** för att komma åt Bitdefender Antivirus Plus gränssnitt.

1.4.2. Installera från installationsskivan

För att installera Bitdefender från installationsskivan, sätt in skivan i den optiska enheten.

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

Om installationsskärmen inte visas, använd Windows Explorer för att bläddra till skivans rotkatalog och dubbelklicka på filen *autorun.exe*.

Om din internethastighet är långsam, eller om ditt system inte är anslutet till internet, klicka på **Installera från CD/DVD** knapp. I det här fallet kommer Bitdefender-produkten som är tillgänglig på skivan att installeras och en nyare version kommer att laddas ner från Bitdefender-servrarna via produktuppdatering.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om ditt system inte uppfyller systemkraven för att installera Bitdefender kommer du att informeras om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender upptäcks kommer du att uppmanas att ta bort den från ditt system. Följ anvisningarna för att ta bort programvaran från ditt system, så att du undviker problem som uppstår senare. Du kan behöva starta om enheten för att slutföra borttagningen av upptäckta säkerhetslösningar.

Installationspaketet för Bitdefender Total Security uppdateras ständigt.

Notera

Att ladda ner installationsfilerna kan ta lång tid, särskilt över långsammare internetanslutningar.

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

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren som du får använda Bitdefender Antivirus Plus.

Om du inte godkänner dessa villkor, stäng fönstret. Installationsprocessen kommer att överges och du kommer att avsluta installationen.

Två ytterligare uppgifter kan utföras i detta steg:

- Behåll **Skicka produktrapporter** alternativet aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information om hur du använder produkten till Bitdefender-servrarna. Denna information är viktig för att förbättra produkten och kan hjälpa oss att ge en bättre upplevelse i framtiden. Observera att dessa rapporter inte innehåller några konfidentiella uppgifter, såsom ditt namn eller

IP-adress, och att de inte kommer att användas för kommersiella ändamål.

- Välj det språk du vill installera produkten på.

Klick **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills installationen är klar. Detaljerad information om framstegen visas.

Steg 3 - Installationen slutförd

En sammanfattning av installationen visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av systemet krävas.

Steg 4 - Enhetsanalys

Du kommer nu att bli tillfrågad om du vill utföra en analys av din enhet för att säkerställa att den är säker. Under detta steg kommer Bitdefender att skanna kritiska systemområden. Klick **Starta enhetsanalys** att initiera det.

Du kan dölja skanningsgränssnittet genom att klicka på **Kör Scan i bakgrunden**. Därefter väljer du om du vill bli informerad när skanningen är klar eller inte.

Klicka på när skanningen är klar **Fortsätt med Skapa konto**.

Notera

Alternativt, om du inte vill utföra skanningen kan du helt enkelt klicka på **Hoppa**.

Steg 5 - Bitdefender-konto

När du har slutfört den första installationen, visas Bitdefender-kontofönstret. Ett Bitdefender-konto krävs för att aktivera produkten och använda dess onlinefunktioner. För mer information, se Bitdefender Central (sida 28).

Fortsätt enligt din situation.

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

  1. Skriv in den information som krävs i motsvarande fält. De uppgifter du lämnar här kommer att förbli konfidentiella. Lösenordet måste

vara minst 8 tecken långt, innehålla minst en siffra eller symbol och innehålla gemener och versaler.

2. Innan du går vidare måste du godkänna användarvillkoren. Gå till användarvillkoren och läs dem noggrant eftersom de innehåller villkoren under vilka du får använda Bitdefender.
   Dessutom kan du komma åt och läsa sekretesspolicyn.
3. Klick **SKAPA KONTO**.

> **Notera**
> När kontot har skapats kan du använda den angivna 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 komma åt Google Play, söka i Bitdefender Central och sedan trycka på motsvarande installationsalternativ. För att installera Bitdefender Central-appen på iOS måste du gå till App Store, söka i Bitdefender Central och sedan trycka på motsvarande installationsalternativ.

○ **Jag har redan ett Bitdefender-konto**

1. Klick **Logga in**.
2. Skriv in e-postadressen i motsvarande fält och klicka sedan **NÄSTA**.
3. Skriv ditt lösenord och klicka sedan **LOGGA IN**.
   Om du har glömt lösenordet för ditt konto eller bara vill återställa det du redan har ställt in:
   a. Klick **Glömt ditt lösenord?**.
   b. Skriv din e-postadress och klicka sedan **NÄSTA**.
   c. Kontrollera ditt e-postkonto, skriv in säkerhetskoden du har fått och klicka sedan **NÄSTA**.
      Alternativt kan du klicka **ändra lösenord** i e-postmeddelandet som vi skickade till dig.
   d. Skriv det nya lösenordet du vill ställa in och skriv det sedan igen. Klick **SPARA**.

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

- **Jag vill logga in med mitt Microsoft-, Facebook- eller Google-konto**
  Så här loggar du 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 länka ditt konto till Bitdefender.

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

Steg 6 - Aktivera din produkt

Notera
Det här steget visas om du har valt att skapa ett nytt Bitdefender-konto under föregående steg, eller om du loggade in med ett konto med en utgången prenumeration.

En aktiv internetanslutning krävs för att slutföra aktiveringen av din produkt.

Fortsätt enligt din situation:

- Jag har en aktiveringskod
  I så fall aktiverar du produkten genom att följa dessa steg:
  1. Skriv in aktiveringskoden i fältet Jag har en aktiveringskod och klicka sedan **FORTSÄTTA**.

Notera

Du kan hitta din aktiveringskod:

- på CD/DVD-etiketten.
- på produktregistreringskortet.
- i e-postmeddelandet om köp online.

2. **Jag vill utvärdera Bitdefender**
   I det här fallet kan du använda produkten under en 30-dagarsperiod. För att börja provperioden, välj **Jag har ingen prenumeration, jag vill prova produkten gratis**, och klicka sedan **FORTSÄTTA**.

Steg 7 - Kom igång

I den **Komma igång** fönster kan du se detaljer om din aktiva prenumeration.

Klick **AVSLUTA** för att komma åt Bitdefender Antivirus Plus gränssnitt.

2. KOMMA IGÅNG

2.1. Det grundläggande

När du har installerat Bitdefender Antivirus Plus, din enhet är skyddad mot alla typer av hot (som skadlig programvara, spionprogram, ransomware, utnyttjande, botnät och trojaner) och internethot (som hackare, nätfiske och spam).

Appen använder Photon-tekniken för att förbättra hastigheten och prestandan för hotskanningsprocessen. Det fungerar genom att lära sig användningsmönstren för dina systemappar för att veta vad och när du ska skanna, vilket minimerar inverkan på systemets prestanda.

Att ansluta till offentliga trådlösa nätverk som tillhör flygplatser, gallerior, kaféer eller hotell utan skydd kan vara farligt för din enhet och data. Detta beror främst på att bedragare kan titta på din aktivitet och hitta det bästa tillfället att stjäla personlig data, men också för att alla kan se din IP-adress, vilket gör din maskin till ett offer för framtida cyberattacker. För att undvika sådana olyckliga situationer, installera och använd VPN (sida 79) app.

Webbkamera skydd håller borta de opålitliga apparna från att komma åt din videokamera och undviker på så sätt alla försök att bli hackad. Baserat på Bitdefender-användarnas val kommer åtkomsten av populära appar till din webbkamera att tillåtas eller blockeras.

För att skydda dig från potentiella snoops och spioner när din enhet är ansluten till ett osäkrat trådlöst nätverk, analyserar Bitdefender dess säkerhetsnivå och kommer vid behov med rekommendationer för att öka säkerheten för dina onlineaktiviteter. För instruktioner om hur du skyddar dina personuppgifter, se Wi-Fi säkerhetsrådgivare (sida 71).

Filer krypterade med ransomware kan nu återställas utan att behöva spendera pengar för någon begärd lösen. För information om hur du återställer krypterade filer, se Ransomware-sanering (sida 75).

Medan du arbetar, spelar spel eller tittar på filmer kan Bitdefender erbjuda dig en kontinuerlig användarupplevelse genom att skjuta upp underhållsuppgifter, eliminera avbrott och justera systemets visuella effekter. Du kan dra nytta av alla dessa genom att aktivera och konfigurera Profiler (sida 88).

Bitdefender kommer att fatta de flesta säkerhetsrelaterade beslut åt dig och kommer sällan att visa popup-varningar. Detaljer om vidtagna åtgärder och information om programdrift finns i meddelandefönstret. För mer information, se Aviseringar (sida 14).

Då och då bör du öppna Bitdefender och åtgärda eventuella befintliga problem. Du kan behöva konfigurera specifika Bitdefender-komponenter eller vidta förebyggande åtgärder för att skydda din enhet och dina data.

För att använda onlinefunktionerna i Bitdefender Antivirus Plus och hantera dina prenumerationer och enheter, få tillgång till ditt Bitdefender-konto. För mer information, se Bitdefender Central (sida 28).

Sektionen Hur (sida 96) är där du hittar steg-för-steg-instruktioner om hur du utför vanliga uppgifter. Om du upplever problem när du använder Bitdefender, kontrollera Löser vanliga problem (sida 122) avsnitt för möjliga lösningar på de vanligaste problemen.

2.1.1. Aviseringar

Bitdefender håller en detaljerad logg över händelser som rör dess aktivitet på din enhet. Närhelst något som är relevant för säkerheten för ditt system eller data inträffar läggs ett nytt meddelande till i Bitdefender-meddelandeområdet, på liknande sätt som ett nytt e-postmeddelande som visas i din inkorg.

Meddelanden är ett viktigt verktyg för att övervaka och hantera ditt Bitdefender-skydd. Du kan till exempel enkelt kontrollera om uppdateringen genomfördes framgångsrikt, om hot eller sårbarheter hittades på din enhet, etc. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som Bitdefender vidtar.

För att komma åt **Aviseringar** logga, klicka på Aviseringar på navigeringsmenyn på Bitdefender-gränssnitt. Varje gång en kritisk händelse inträffar kan en räknare märkas på 2 ikon.

Beroende på typ och svårighetsgrad grupperas meddelanden i:

- **Kritisk** händelser indikerar kritiska problem. Du bör kontrollera dem omedelbart.
- **Varning** händelser indikerar icke-kritiska frågor. Du bör kontrollera och fixa dem när du har tid.
- **Information** händelser indikerar framgångsrika operationer.

Klicka på varje flik för att hitta mer information om de genererade händelserna. Korta detaljer visas med ett enda klick på varje händelsetitel, nämligen: en kort beskrivning, åtgärden Bitdefender vidtog när den hände och datum och tid när den inträffade. Alternativ kan tillhandahållas för att vidta ytterligare åtgärder vid behov.

För att hjälpa dig att enkelt hantera loggade händelser, ger meddelandefönstret alternativ för att ta bort eller markera som lästa alla händelser i det avsnittet.

2.1.2. Profiler

Vissa datoraktiviteter, som onlinespel eller videopresentationer, kräver ökad systemrespons, hög prestanda och inga avbrott. När din bärbara dator körs på batteri är det bäst att onödiga operationer, som förbrukar ytterligare ström, skjuts upp tills den bärbara datorn är ansluten till A/C-ström.

Bitdefender-profiler tilldelar fler systemresurser till de appar som körs genom att tillfälligt ändra skyddsinställningar och justera systemkonfigurationen. Följaktligen minimeras systemets påverkan på din aktivitet.

För att anpassa sig till olika aktiviteter kommer 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.

Offentlig Wi-Fi-profil

Tillämpar produktinställningar för att dra nytta av fullt skydd medan den är ansluten till ett osäkert trådlöst nätverk.

Batterilägesprofil

Tillämpar produktinställningar och håller ner bakgrundsaktivitet för att spara batteritid.

Konfigurera automatisk aktivering av profiler

För en lättanvänd upplevelse kan du konfigurera Bitdefender för att hantera din arbetsprofil. I det här fallet upptäcker Bitdefender automatiskt aktiviteten du utför och tillämpar system- och produktoptimeringsinställningar.

Första gången du kommer åt **Profiler** du kommer att bli ombedd att aktivera automatiska profiler. För att göra det kan du helt enkelt klicka på **SÄTTA PÅ** i det visade fönstret.

Du kan klicka på **INTE NU** om du vill aktivera funktionen vid ett senare tillfälle.

För att tillåta Bitdefender att aktivera profiler automatiskt:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Använd motsvarande strömbrytare för att slå på **Aktivera profiler automatiskt**.

Om du inte vill att profilerna ska aktiveras automatiskt, stäng av strömbrytaren.

Aktivera en profil manuellt genom att slå på motsvarande strömbrytare. Av de tre första profilerna kan endast en aktiveras manuellt på en gång.

För mer information om profiler, se Profiler (sida 88).

2.1.3. Lösenordsskyddande Bitdefender-inställningar

Om du inte är den enda personen med administrativa rättigheter som använder den här enheten, rekommenderas det att du skyddar dina Bitdefender-inställningar med ett lösenord.

Så här konfigurerar du lösenordsskydd för Bitdefender-inställningarna:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allmän** fönster, slå på **Lösenordsskydd**.
3. Skriv lösenordet i de två fälten och klicka sedan på OK. Lösenordet måste vara minst 8 tecken långt.

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

Viktig
Se till att komma ihåg ditt lösenord eller spara det på ett säkert ställe. Om du glömmer lösenordet måste du installera om programmet eller kontakta Bitdefender för support.

Så här tar du bort lösenordsskyddet:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allmän** fönster, stäng av **Lösenordsskydd**.
3. Skriv lösenordet och klicka sedan **OK**.

Notera
För att ändra lösenordet för din produkt, klicka på **Lösenordsändring**. Skriv ditt nuvarande lösenord och klicka sedan **OK**. I det nya fönstret som visas skriver du det nya lösenordet du vill använda från och med nu för att begränsa åtkomsten till dina Bitdefender-inställningar.

2.1.4. Produktrapporter

Produktrapporter innehåller information om hur du använder Bitdefender-produkten du har installerat. Denna information är viktig för att förbättra produkten och kan hjälpa oss att erbjuda dig en bättre upplevelse i framtiden.

Observera att dessa rapporter inte innehåller några konfidentiella uppgifter, såsom ditt namn eller IP-adress, och att de inte används för kommersiella ändamål.

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

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Avancerad** flik.
3. Stäng av **Produktrapporter**.

2.1.5. Aviseringar om specialerbjudanden

När kampanjerbjudanden är tillgängliga är Bitdefender-produkten inställd för att meddela dig via ett popup-fönster. Detta ger dig möjlighet att dra nytta av förmånliga priser och hålla dina enheter skyddade under en längre tid.

Så här aktiverar eller inaktiverar du aviseringar om specialerbjudanden:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allmän** fönster, slå på eller av motsvarande strömbrytare.

Alternativet för specialerbjudanden och produktaviseringar är aktiverat som standard.

2.2. Bitdefender-gränssnitt

Bitdefender Antivirus Plus tillgodoser behoven hos både datornybörjare och mycket tekniska personer. Dess grafiska användargränssnitt är utformat för att passa varje kategori av användare.

För att gå igenom Bitdefender-gränssnittet visas en introduktionsguide som innehåller information om hur man interagerar med produkten och hur man konfigurerar den på den övre vänstra sidan. Välj den räta vinkeln för att fortsätta guidas, eller **Skippa rundtur** för att stänga guiden.

Bitdefendern ikonen i systemfältet är tillgänglig när som helst, oavsett om du vill öppna huvudfönstret, köra en produktuppdatering eller visa information om den installerade versionen.

Huvudfönstret ger dig information om din säkerhetsstatus. Baserat på din enhetsanvändning och behov, Autopilot visar här olika typer av rekommendationer som hjälper dig att förbättra din enhets säkerhet och prestanda. Dessutom kan du lägga till snabba åtgärder som du använder mest, så att du kan ha dem till hands när du behöver.

Från navigeringsmenyn på vänster sida kan du komma åt inställningsområdet, aviseringar och Bitdefender-sektioner för detaljerad konfiguration och avancerade administrativa uppgifter.

Från den övre delen av huvudgränssnittet kan du komma åt din Bitdefender-konto. Du kan också kontakta oss för support om du har frågor eller något oväntat dyker upp.

2.2.1. Ikonen i systemfältet

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

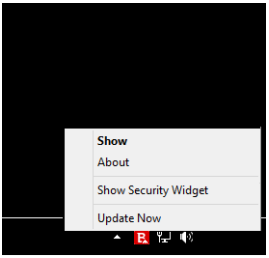
Notera

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

- I **Windows 7, Windows 8 och Windows 8.1**
  1. Klicka på pilen i det nedre högra hörnet av skärmen.
  2. Klick **Anpassa...** för att öppna fönstret Meddelandefältsikoner.
  3. Välj alternativet **Visa ikoner och aviseringar** för **Bitdefender-agent** ikon.
- I **Windows 10**
  1. Högerklicka på aktivitetsfältet och välj **Aktivitetsfältets inställningar**.
  2. Scrolla ner och klicka på **Välj vilka ikoner som ska visas i aktivitetsfältet** länk under **Meddelandefältet**.
  3. Aktivera omkopplaren bredvid **Bitdefender-agent**.

Om du dubbelklickar på den här ikonen öppnas Bitdefender. Genom att högerklicka på ikonen kan du också snabbt hantera Bitdefender-produkten i en kontextmeny.

- **Show** - öppnar huvudfönstret i Bitdefender.
- **Handla om** - öppnar ett fönster där du kan se information om Bitdefender, var du kan söka hjälp om något oväntat dyker upp, var du kan komma åt och se prenumerationsavtalet, komponenter från tredje part och sekretesspolicy.
- **Uppdatera nu** - startar en omedelbar uppdatering. Du kan följa uppdateringsstatusen i uppdateringspanelen på huvudet Bitdefender-fönster.



Bitdefender-ikonen i systemfältet informerar dig när problem påverkar din enhet eller hur produkten fungerar, genom att visa en speciell symbol, enligt följande:

Inga problem påverkar säkerheten för ditt system.

Kritiska problem påverkar säkerheten för ditt system. De kräver din omedelbara uppmärksamhet och måste åtgärdas så snart som möjligt.

Om Bitdefender inte fungerar visas ikonen i systemfältet på en grå bakgrund: . Detta händer vanligtvis när prenumerationen går ut. Det kan också inträffa när Bitdefender-tjänsterna inte svarar eller när andra fel påverkar den normala driften av Bitdefender.

2.2.2. Navigeringsmeny

På vänster sida av Bitdefender-gränssnittet finns navigeringsmenyn, som gör att du snabbt kan komma åt Bitdefender-funktionerna och verktygen du behöver för att hantera din produkt. Flikarna som är tillgängliga i det här området är:

- **instrumentbräda**. Härifrån kan du snabbt fixa säkerhetsproblem, visa rekommendationer enligt dina systembehov och användningsmönster, utföra snabba åtgärder och installera Bitdefender på andra enheter.
- **Skydd**. Härifrån kan du starta och konfigurera antivirusgenomsökningar, komma åt brandväggsinställningar, återställa data om de krypteras av en ransowmware och konfigurera skydd när du surfar på internet.
- **Integritet**. Härifrån kan du skapa lösenordshanterare för dina onlinekonton, skydda åtkomsten till din webbkamera från oönskade ögon, göra onlinebetalningar i en säker miljö, öppna VPN-appen och skydda dina barn genom att se och begränsa deras onlineaktivitet.
- **Verktyg**. Härifrån kan du förbättra systemets hastighet och konfigurera stöldskyddsfunktionen för dina enheter.
- **Aviseringar**. Härifrån har du tillgång till de genererade aviseringarna.
- **inställningar**. Härifrån har du tillgång till allmänna inställningar.
- **Stöd**. Härifrån, närhelst du behöver hjälp med att lösa en situation med din Bitdefender Antivirus Plus, kan du kontakta Bitdefender Technical Support-avdelningen.

- **Mitt konto**. Härifrån kan du komma åt ditt Bitdefender-konto för att verifiera dina prenumerationer och utföra säkerhetsuppgifter på de enheter du hanterar. Detaljer om Bitdefender-kontot och prenumerationen i bruk finns också tillgängliga.

2.2.3. instrumentbräda

Dashboard-fönstret låter dig utföra vanliga uppgifter, snabbt åtgärda säkerhetsproblem, visa information om produktdrift och komma åt panelerna där du konfigurerar produktinställningarna.

Allt är bara några klick bort.

Fönstret är organiserat i tre huvudområden:

Säkerhetsstatusområde

Det är här du kan kontrollera din enhets säkerhetsstatus.

Autopilot

Det är här du kan kontrollera autopilotens rekommendationer för att säkerställa korrekt funktionalitet hos systemet.

Snabba åtgärder

Det är här du kan köra olika uppgifter för att hålla ditt system skyddat och köra med optimal hastighet. Du kan också installera Bitdefender på andra enheter förutsatt att ditt abonnemang har tillräckligt med tillgängliga platser.

Säkerhetsstatusområde

Bitdefender använder ett problemspårningssystem för att upptäcka och informera dig om de problem som kan påverka säkerheten för din enhet och data. Upptäckta problem inkluderar viktiga skyddsinställningar som är avstängda och andra förhållanden som kan utgöra en säkerhetsrisk.

Närhelst problem påverkar säkerheten för din enhet visas statusen som visas på ovansidan av Bitdefender-gränssnitt ändras till rött. Statusen som visas indikerar typen av problem som påverkar ditt system. Även systemfältet ikonen ändras till och om du flyttar muspekaren över ikonen kommer ett popup-fönster att bekräfta förekomsten av väntande problem.

Eftersom de upptäckta problemen kan hindra Bitdefender från att skydda dig mot hot eller utgöra en stor säkerhetsrisk, rekommenderar vi att du

är uppmärksam och fixar dem så snart som möjligt. För att åtgärda ett problem, klicka på knappen bredvid det upptäckta problemet.

Autopilot

För att erbjuda dig en effektiv operation och ökat skydd medan du utför olika aktiviteter, kommer Bitdefender Autopilot att fungera som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, antingen du arbetar, gör onlinebetalningar, tittar på film eller spelar spel kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov.

De föreslagna rekommendationerna kan också vara relaterade till åtgärder som du behöver utföra för att din produkt ska fungera med sin fulla kapacitet.

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

Stänger av autopilotaviseringar

För att uppmärksamma autopilotens rekommendationer är Bitdefender-produkten inställd för att meddela dig via ett popup-fönster.

Så här stänger du av autopilotaviseringarna:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allmän** fönster, stäng av **Rekommendationsmeddelanden**.

Snabba åtgärder

Med hjälp av snabba åtgärder kan du snabbt starta uppgifter som du anser vara viktiga för att hålla ditt system skyddat och köra med optimal hastighet.

Som standard kommer Bitdefender med några snabba åtgärder som kan ersättas med de du vet att du oftast använder. Så här ersätter du en snabb åtgärd:

1. Klicka på ikonen i det övre högra hörnet av kortet du vill ta bort.
2. Peka på uppgiften du vill lägga till i huvudgränssnittet och klicka sedan **LÄGG TILL**.

De uppgifter du kan lägga till i huvudgränssnittet är:

- **Snabbskanning**. Kör en snabbskanning för att snabbt upptäcka möjliga hot som kan finnas på din enhet.
- **Genomsökning av systemet**. Kör en systemsökning för att se till att din enhet är fri från hot.
- **Sårbarhetsskanning**. Skanna din enhet efter sårbarheter för att se till att alla installerade appar, tillsammans med operativsystemet, är uppdaterade och fungerar korrekt.
- **Wi-Fi säkerhetsrådgivare**. Öppna fönstret Wi-Fi Security Advisor i sårbarhetsmodulen.
- **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 av skydd när du är ansluten till internet.
- **Pappers strimlare**. Starta verktyget File Shredder för att ta bort spår av känslig data från din enhet.
- **Öppna OneClick Optimizer**. Frigör diskutrymme, fixa registerfel och skydda din integritet genom att radera filer som kanske inte längre är användbara med ett enda klick på en knapp.

Så här börjar du skydda ytterligare enheter med Bitdefender:

1. Klick **Installera på en annan enhet**.
   Ett nytt fönster visas på skärmen.
2. Klick **DELA NEDLADDNINGSLÄNK**.
3. Följ stegen på skärmen för att installera Bitdefender.

Beroende på ditt val kommer följande Bitdefender-produkter att installeras:

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

2.2.4. Bitdefender-sektionerna

Bitdefender-produkten kommer med tre sektioner indelade i användbara funktioner för att hjälpa dig att hålla dig skyddad medan du arbetar,

surfar på webben eller utför onlinebetalningar, förbättrar hastigheten på ditt system och många fler.

Närhelst du vill komma åt funktionerna för en specifik sektion eller börja konfigurera din produkt, gå till följande ikoner som finns på navigeringsmenyn på Bitdefender-gränssnitt:

- Skydd
- Integritet
- Verktyg

Skydd

I avsnittet Skydd kan du konfigurera dina avancerade säkerhetsinställningar, hantera vänner och spammare, visa och redigera nätverksanslutningsinställningarna, ställa in funktionerna för förebyggande av onlinehot, kontrollera och åtgärda potentiella systemsårbarheter och bedöma säkerheten för de trådlösa nätverk du ansluter till .

Funktionerna du kan hantera i avsnittet Skydd är:

ANTIVIRUS

Antivirusskydd är grunden för din säkerhet. Bitdefender skyddar dig i realtid och på begäran mot alla typer av hot, som skadlig programvara, trojaner, spionprogram, adware, etc.

Från antivirusfunktionen kan du enkelt komma åt följande skanningsuppgifter:

- Snabbskanning
- Genomsökning av systemet
- Hantera skanningar
- Räddningsmiljö

För mer information om skanningsuppgifter och hur du konfigurerar antivirusskydd, se Antivirusskydd (sida 44).

ONLINE FÖREBYGGANDE AV HOT

Online Threat Prevention hjälper dig att hålla dig skyddad mot nätfiskeattacker, bedrägeriförsök och privata dataläckor medan du surfar på internet.

För mer information om hur du konfigurerar Bitdefender för att skydda din webbaktivitet, se Hotförebyggande online (sida 65).

BRANDVÄGGEN

Brandväggen skyddar dig medan du är ansluten till nätverk och internet genom att filtrera alla anslutningsförsök.

För mer information om brandväggskonfiguration, se Brandvägg.

AVANCERAD HOT FÖRSVAR

Advanced Threat Defense skyddar ditt system aktivt mot hot som ransomware, spionprogram och trojaner genom att analysera beteendet hos alla installerade appar. Misstänkta processer identifieras och blockeras vid behov.

För mer information om hur du håller ditt system skyddat från hot, se Avancerat hotförsvar (sida 63).

ANTI SPAM

Bitdefender antispam-funktionen säkerställer att din inkorg förblir fri från oönskade e-postmeddelanden genom att filtrera POP3-e-posttrafik.

För mer information om antispam-skyddet, se Anti Spam.

SÅRBARHET

Sårbarhetsmodulen hjälper dig att hålla operativsystemet och de appar du regelbundet använder uppdaterade och att identifiera de osäkra trådlösa nätverk du ansluter till. Klick **Öppen** i sårbarhetsmodulen för att komma åt dess funktioner.

De **Sårbarhetsskanning** funktionen låter dig identifiera viktiga Windows-uppdateringar, appuppdateringar, svaga lösenord som tillhör Windows-konton och trådlösa nätverk som inte är säkra. Klick **Starta skanning** för att utföra en skanning på din enhet.

Klicka på **Wi-Fi säkerhetsrådgivare** för att se listan över de trådlösa nätverk du ansluter till, tillsammans med vår anseendebedömning för vart och ett av dem och de åtgärder du kan vidta för att skydda dig från potentiella snoopar.

För mer information om att konfigurera sårbarhetsskydd, se Sårbarhet (sida 67).

RANSOMWARE ÅTGÄRD

Funktionen Ransomware Remediation hjälper dig att återställa filer i fall de krypteras av ransomware.

För mer information om hur du återställer krypterade filer, se Ransomware-sanering (sida 75).

Integritet

I avsnittet Sekretess kan du öppna Bitdefender VPN-appen, kryptera dina privata data, skydda dina onlinetransaktioner, hålla din webbkamera och surfupplevelse säker och skydda dina barn genom att se och begränsa deras onlineaktivitet.

Funktionerna 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 på flygplatser, gallerior, kaféer eller hotell. Dessutom kan du komma åt innehåll som normalt är begränsat i vissa områden.

För mer information om den här funktionen, se VPN (sida 79).

VIDEO & LJUDSKYDD

Video- och ljudskydd håller din webbkamera utom fara genom att blockera åtkomsten till opålitliga appar och meddelar dig när appar försöker få åtkomst till din mikrofon.

För mer information om hur du håller din webbkamera skyddad från oönskad åtkomst och hur du ställer in Bitdefender för att meddela dig om din mikrofonaktivitet, se Video- och ljudskydd.

SAFEPAY

Bitdefender Safepay™-webbläsaren hjälper dig att hålla din onlinebank, e-shopping och alla andra typer av onlinetransaktioner privata och säkra.

För mer information om Bitdefender Safepay™, se Safepay-säkerhet för onlinetransaktioner (sida 82).

FÖRÄLDRAKONTROLL

Bitdefender Parental Control låter dig övervaka vad dina barn gör på sin enhet. I händelse av olämpligt innehåll kan du bestämma dig för att begränsa hans tillgång till internet eller till specifika appar.

Klick **Konfigurera** i rutan Föräldrakontroll för att börja konfigurera dina barns enheter och övervaka deras aktivitet var du än är.

För mer information om att konfigurera föräldrakontroll, se Föräldrakontroll.

ANTI-TRACKER

Anti-tracker-funktionen hjälper dig att undvika spårning, så att din data förblir privat medan du surfar online, samtidigt som den minskar tiden det tar för webbplatser att ladda.

För mer information om Anti-tracker-funktionen, se Antispårare (sida 77).

Verktyg

I avsnittet Verktyg kan du förbättra systemets hastighet och hantera dina enheter.

OneClick Optimizer

Bitdefender Total Security erbjuder inte bara säkerhet, det hjälper dig också att hålla enhetens prestanda i form.

Vår OneClick Optimizer hjälper dig att hitta och ta bort onödiga filer från din enhet i ett enkelt steg.

För mer information om det, se OneClick Optimizer.

Anti-stöld

Bitdefender Anti-Theft skyddar din enhet och data mot stöld eller förlust. I händelse av en sådan händelse gör detta att du kan fjärrlokalisera eller låsa din enhet. Du kan också radera all data som finns i ditt system.

Bitdefender Anti-Theft erbjuder följande funktioner:

- Fjärrlokalisera
- Fjärrlås
- Fjärrtorka
- Fjärrvarning

För mer information om hur du kan hålla ditt system borta från fel händer, se Stöldskydd.

Dataskydd

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

För mer information om det, se Dataskydd (sida 94).

Profiler

Dagliga jobbaktiviteter, titta på film eller spela spel kan göra att systemet blir långsammare, särskilt om de körs samtidigt med Windows uppdateringsprocesser och underhållsuppgifter.

Med Bitdefender kan du nu välja och använda din föredragna profil, vilket gör systemjusteringar lämpade för att öka prestandan för specifika installerade appar.

För mer information om den här funktionen, se Profiler (sida 88).

2.2.5. Ändra produktspråk

Bitdefender-gränssnittet är tillgängligt på flera språk och kan ändras genom att följa dessa steg:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allmän** fönster, klicka **Ändra språk**.
3. Välj önskat språk i listan och klicka sedan **SPARA**.
4. Vänta ett par ögonblick tills inställningarna tillämpas.

2.3. Bitdefender Central

2.3.1. Om Bitdefender Central

Bitdefender Central är plattformen där du har tillgång till produktens onlinefunktioner och tjänster och kan utföra viktiga uppgifter på distans på enheter som Bitdefender är installerat på. Du kan logga in på ditt Bitdefender-konto från vilken dator eller mobil enhet 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 ladda sedan ner och installera appen. Följ de nödvändiga stegen för att slutföra installationen.

- **På iOS** - sök Bitdefender Central på App Store och ladda sedan ner och installera appen. Följ de nödvändiga stegen för att slutföra installationen.

När du har loggat in kan du börja göra följande:

- Ladda ner och installera Bitdefender på Windows, macOS, iOS och Android operativsystem. Produkterna som är tillgängliga för nedladdning är:
  - Bitdefender Windows produktlinje
  - Bitdefender Antivirus för Mac
  - Bitdefender Mobile Security för Android
  - Bitdefender Mobile Security för iOS
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter i ditt nätverk och hantera dem var du än är.
- Skydda nätverksenheterna och deras data mot stöld eller förlust med Anti-stöld.
- Konfigurera Föräldrakontroll inställningar för dina barns enheter och övervaka deras aktivitet var du än är.

2.3.2. Åtkomst till Bitdefender Central

Det finns flera sätt att komma åt Bitdefender Central. Beroende på vilken uppgift du vill utföra kan du använda någon av följande möjligheter:

- Från Bitdefender huvudgränssnitt:
  1. Klick **Mitt konto** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. Klick **Gå till Bitdefender Central**.
  3. Logga in på ditt Bitdefender-konto med din e-postadress och ditt lösenord.
- Från din webbläsare:
  1. Öppna en webbläsare på valfri enhet med internetåtkomst.
  2. Gå till: https://central.bitdefender.com.
  3. Logga in på ditt konto med din e-postadress och ditt lösenord.

- Från din Android- eller iOS-enhet:
  1. Öppna Bitdefender Central-appen som du har installerat.

Notera
I detta material har vi tagit med alternativen som du kan hitta på webbgränssnittet.

2.3.3. 2-faktorsautentisering

Metoden för 2-faktorautentisering lägger till ett extra säkerhetslager till ditt Bitdefender-konto genom att kräva en autentiseringskod utöver dina inloggningsuppgifter. På så sätt kommer du att förhindra kontoövertagande och hålla borta typer av cyberattacker, såsom keyloggers, brute-force eller ordbokattacker.

Aktiverar 2-faktorsautentisering

Genom att aktivera 2-faktorsautentisering kommer du att göra ditt Bitdefender-konto mycket säkrare. Din identitet kommer att verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera statusen för din prenumeration eller köra uppgifter på distans på dina enheter.

Så här aktiverar du tvåfaktorsautentisering:

1. Tillgång Bitdefender Central.
2. Klicka på ikonen i den övre högra sidan av skärmen.
3. Klick **Bitdefender-konto** i bildmenyn.
4. Välj **Lösenord och säkerhet** flik.
5. Klick **2-faktorsautentisering**.
6. Klick **KOMMA IGÅNG**.
   Välj en av följande metoder:
   - **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in på ditt Bitdefender-konto.
     Om du vill använda en autentiseringsapp, men du är osäker på vad du ska välja, finns en lista med de autentiseringsappar som vi rekommenderar.
     a. Klick **ANVÄND AUTENTICATOR-APPEN** att börja.

b. Om du vill logga in på en Android- eller iOS-baserad enhet använder du din enhet för att skanna QR-koden.
   För att logga in på en bärbar dator eller dator kan du lägga till den visade koden manuellt.
   Klick **FORTSÄTTA**.

c. Infoga koden från appen, eller den som visades i föregående steg, och klicka sedan **AKTIVERA**.

- **E-post** - varje gång du loggar in på ditt Bitdefender-konto kommer en verifieringskod att skickas till din e-postinkorg. Kontrollera mejlet och använd sedan koden du fick.

  a. Klick **ANVÄND E-POST** att börja.

  b. Kontrollera din e-post och skriv in den medföljande koden.

  c. Klick **AKTIVERA**.

  d. Du får tio aktiveringskoder. Du kan antingen kopiera, ladda ner eller skriva ut listan och använda den om du tappar din e-postadress eller inte kommer att kunna logga in. Varje kod kan bara användas en gång.

  e. Klick **GJORT**.

Om du vill sluta använda tvåfaktorsautentisering:

1. Klick **STÄNG AV 2-FAKTORS AUTENTISERING**.
2. Kontrollera din app eller e-postkonto och skriv in koden du har fått.
   Om du har valt att ta emot autentiseringskoden via e-post har du fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.
3. Bekräfta ditt val.

2.3.4. Lägger till betrodda enheter

För att vara säker på att bara du kan komma åt ditt Bitdefender-konto kan vi behöva en säkerhetskod först. Om du vill hoppa över det här steget varje gång du ansluter från samma enhet rekommenderar vi att du nominerar den som en betrodd enhet.

Så här lägger du till enheter som betrodda enheter:

1. Tillgång Bitdefender Central.
2. Klicka på ikonen i den övre högra sidan av skärmen.
3. Klick **Bitdefender-konto** i bildmenyn.
4. Välj **Lösenord och säkerhet** flik.
5. Klick **Betrodda enheter**.
6. Listan med enheterna som Bitdefender är installerade på visas. Klicka på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och ditt abonnemang är giltigt.

2.3.5. Aktivitet

I aktivitetsområdet har du tillgång till information om enheterna som har Bitdefender installerat.

När du väl kommer åt **Aktivitet** fönster finns följande kort tillgängliga:

- **Mina enheter**. Här kan du se antalet anslutna enheter tillsammans med deras skyddsstatus. För att åtgärda problem på distans på de upptäckta enheterna, tryck på **Fixa problem**och tryck sedan på **SKANNA OCH ÅTGÄRDA PROBLEM**.

  För att se detaljer om de upptäckta problemen, tryck på **Visa problem**.

  Information om upptäckta hot kan inte hämtas från iOS-baserade enheter.
- **Hot blockerade**. Här kan du se en graf som visar en övergripande statistik inklusive information om de hot som blockerats under de senaste 24 timmarna och sju dagarna. Den visade informationen hämtas beroende på det skadliga beteende som upptäcks på åtkomst till filer, appar och webbadresser.
- **Toppanvändare med hot blockerade**. Här kan du se en topp med användarna där de flesta hoten har hittats.
- **Toppenheter med hot blockerade**. Här kan du se en topp med enheterna där de flesta hoten har hittats.

2.3.6. mina prenumerationer

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

Kontrollera tillgängliga abonnemang

Så här kontrollerar du dina tillgängliga prenumerationer:

1. Tillgång Bitdefender Central.
2. Välj **mina prenumerationer** panel.

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

Du kan lägga till en ny enhet i ett abonnemang eller förnya den genom att välja ett abonnemangskort.

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

Aktivera prenumeration

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

Om du har köpt en aktiveringskod från en av våra återförsäljare eller fått den i present, kan du lägga till dess tillgänglighet till ditt Bitdefender-abonnemang.

För att aktivera ett abonnemang med en aktiveringskod, följ dessa steg:

1. Tillgång Bitdefender Central.
2. Välj **mina prenumerationer** panel.
3. Tryck på **AKTIVERINGSKOD** knappen och skriv sedan koden i motsvarande fält.
4. Knacka **AKTIVERA** att fortsätta.

Abonnemanget är nu aktiverat.

Förnya prenumeration

Om du inaktiverade den automatiska förnyelsen av din Bitdefender-prenumeration kan du förnya den manuellt genom att följa dessa steg:

1. Tillgång Bitdefender Central.
2. Välj **mina prenumerationer** panel.

3. Välj önskat abonnemangskort.
4. Knacka **FÖRNYA** att fortsätta.

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

2.3.7. Mina enheter

De **Mina enheter** område i ditt Bitdefender-konto ger dig 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 enhetens namn, skyddsstatus och om det finns säkerhetsrisker som påverkar skyddet av dina enheter.

Lägger till en ny enhet

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

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panelen och tryck sedan på **INSTALLATIONSSKYDD**.
3. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
   - **Skydda andra enheter**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
     Knacka **SKICKA NEDLADDNINGSLÄNK**. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
     På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och tryck sedan på motsvarande nedladdningsknapp.
4. Vänta tills nedladdningen är klar och kör sedan installationsprogrammet.

Anpassa din enhet

För att enkelt identifiera dina enheter kan du anpassa enhetens namn:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **inställningar**.
5. Skriv in ett nytt namn i **Enhetsnamn** fältet och tryck sedan på **SPARA**.

Du kan skapa och tilldela en ägare till var och en av dina enheter för bättre hantering:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **Profil**.
5. Knacka **Lägg till ägare**, fyll sedan i motsvarande fält. Anpassa profilen genom att lägga till ett foto, välja ett födelsedatum och lägga till en e-postadress och ett telefonnummer.
6. Knacka **LÄGG TILL** för att spara profilen.
7. Välj önskad ägare från **Enhetsägare** lista och tryck sedan på **TILLDELA**.

Fjärråtgärder

För att fjärruppdatera Bitdefender på en enhet:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **Uppdatering**.

För fler fjärråtgärder och information om din Bitdefender-produkt på en specifik enhet, tryck på önskat enhetskort.

När du trycker på ett enhetskort är följande flikar tillgängliga:

- **Instrumentbräda.** I det här fönstret kan du se detaljer om den valda enheten, kontrollera dess skyddsstatus, status för Bitdefender VPN och hur många hot som har blockerats under de senaste sju dagarna. Skyddsstatusen kan vara grön, när det inte finns några problem som påverkar din enhet, gul när enheten behöver din uppmärksamhet eller röd när enheten är i fara. När det finns problem som påverkar din enhet, tryck på rullgardinspilen i det övre statusområdet för att få mer information.
- **Skydd.** Från det här fönstret kan du fjärrköra en snabb- eller systemsökning på dina enheter. Tryck på **SKANNA** knappen för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och en rapport över den senaste skanningen med den viktigaste informationen finns tillgänglig.
- **Optimizer.** Här kan du förbättra en enhets prestanda på distans genom att snabbt skanna, upptäcka och rensa värdelösa filer. Tryck på **START** och välj sedan de områden du vill optimera. Tryck igen på **START** för att starta optimeringsprocessen. Knacka **Fler detaljer** för att få tillgång till en detaljerad rapport om de åtgärdade problemen.
- **Anti-stöld.** I händelse av felplacering, stöld eller förlust, med stöldskyddsfunktionen kan du lokalisera din enhet och vidta fjärråtgärder. Knacka **LOKALISERA** för att ta reda på enhetens position. Den senast kända positionen kommer att visas tillsammans med tid och datum.
- **Sårbarhet.** För att kontrollera en enhet för eventuella sårbarheter som saknade Windows-uppdateringar, föråldrade appar eller svaga lösenord tryck på **SKANNA** på fliken Sårbarhet. Sårbarheter kan inte fixas på distans. Om någon sårbarhet hittas måste du köra en ny skanning på enheten och sedan vidta de rekommenderade åtgärderna. Knacka **Fler detaljer** för att få tillgång till en detaljerad rapport om de hittade problemen.

2.3.8. Aviseringar

För att hjälpa dig att hålla dig informerad om vad som händer på enheterna som är kopplade till ditt konto 🔔 ikonen är till hands. När du väl trycker på den har du en övergripande bild som består av information om aktiviteten hos Bitdefender-produkterna installerade på dina enheter.

2.4. Håller Bitdefender uppdaterad

Nya hot hittas och identifieras varje dag. Det är därför det är mycket viktigt att hålla Bitdefender uppdaterad med den senaste hotinformationsdatabasen.

Om du är ansluten till internet via bredband eller DSL sköter Bitdefender detta själv. Som standard söker den efter uppdateringar när du slår på din enhet och varje **timme** efter det. Om en uppdatering upptäcks, laddas den ned automatiskt och installeras på din enhet.

Uppdateringsprocessen utförs i farten, vilket innebär att filerna som ska uppdateras ersätts successivt. På så sätt kommer uppdateringsprocessen inte att påverka produktens funktion och samtidigt kommer alla sårbarheter att undantas.

> **Viktig**
> Håll Automatisk uppdatering påslagen för att vara skyddad mot de senaste hoten.

I vissa speciella situationer krävs ditt ingripande för att hålla ditt Bitdefender-skydd uppdaterat:

- Om din enhet ansluter till internet via en proxyserver måste du konfigurera proxyinställningarna enligt beskrivningen i .
- Om du är ansluten till internet via en uppringd anslutning, rekommenderas det att regelbundet uppdatera Bitdefender på begäran av användaren. För mer information, se.

2.4.1. Kontrollerar om Bitdefender är uppdaterad

Så här kontrollerar du tiden för den senaste uppdateringen av din Bitdefender:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken väljer du meddelandet om den senaste uppdateringen.

Du kan ta reda på när uppdateringar initierades och information om dem (om de lyckades eller inte, om de kräver en omstart för att slutföra installationen). Om det behövs, starta om systemet så snart som möjligt.

2.4.2. Utför en uppdatering

För att utföra uppdateringar krävs en internetanslutning.

För att starta en uppdatering, högerklicka på Bitdefender ikonen i systemfältet, och välj sedan **Uppdatera nu**.

Uppdateringsfunktionen kommer att ansluta till Bitdefender-uppdateringsservern och den kommer att söka efter uppdateringar. Om en uppdatering upptäcks kommer du att bli ombedd att bekräfta den eller så kommer uppdateringen att utföras automatiskt, beroende på uppdatera inställningarna.

> **Viktig**
> Det kan bli nödvändigt att starta om enheten när du har slutfört uppdateringen. Vi rekommenderar att du gör det så snart som möjligt.

Du kan också utföra uppdateringar på distans på dina enheter, förutsatt att de är påslagna och anslutna till internet.

För att fjärruppdatera Bitdefender på en Windows-enhet:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Klicka på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **Uppdatering**.

2.4.3. Slår på eller av automatisk uppdatering

Så här aktiverar eller inaktiverar du automatisk uppdatering:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Uppdatering** flik.
3. Slå på eller av motsvarande strömbrytare.
4. Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att den automatiska uppdateringen ska vara inaktiverad.

Du kan inaktivera den automatiska uppdateringen i 5, 15 eller 30 minuter, i en timme eller tills ett system startar om.

Varning

Detta är en kritisk säkerhetsfråga. Vi rekommenderar att du inaktiverar automatisk uppdatering så kort tid som möjligt. Om Bitdefender inte uppdateras regelbundet kommer det inte att kunna skydda dig mot de senaste hoten.

2.4.4. Justera uppdateringsinställningar

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

Standardinställningarna för uppdateringar är lämpliga för de flesta användare och du behöver normalt inte ändra dem.

Så här justerar du uppdateringsinställningarna:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Uppdatering** och justera inställningarna enligt dina önskemål.

Uppdateringsfrekvens

Bitdefender är konfigurerad att söka efter uppdateringar varje timme. För att ändra uppdateringsfrekvensen, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när uppdateringen ska ske.

Uppdatera bearbetningsregler

Varje gång en uppdatering är tillgänglig kommer Bitdefender automatiskt att ladda ner och implementera uppdateringen utan att visa aviseringar. Stäng av **Tyst uppdatering** alternativet om du vill bli meddelad varje gång en ny uppdatering är tillgänglig.

Vissa uppdateringar kräver en omstart för att slutföra installationen.

Som standard, om en uppdatering kräver omstart, fortsätter Bitdefender att arbeta med de gamla filerna tills användaren frivilligt startar om enheten. Detta för att förhindra att Bitdefender-uppdateringsprocessen stör användarens arbete.

Om du vill bli tillfrågad när en uppdatering kräver omstart, slå på **Starta om avisering**.

2.4.5. Kontinuerliga uppdateringar

För att vara säker på att du använder den senaste versionen söker din Bitdefender automatiskt efter produktuppdateringar. Dessa uppdateringar kan ge nya funktioner och förbättringar, åtgärda produktproblem eller automatiskt uppgradera dig till en ny version. När den nya Bitdefender-versionen kommer via uppdatering, sparas anpassade inställningar och proceduren för avinstallation och ominstallation hoppas över.

Dessa uppdateringar kräver en omstart av systemet för att initiera installationen av nya filer. När en produktuppdatering är klar kommer ett popup-fönster att informera dig om att starta om systemet. Om du missar det här meddelandet kan du antingen klicka **STARTA OM NU** i Aviseringar fönster där den senaste uppdateringen nämns, eller starta om systemet manuellt.

Notera
Uppdateringarna inklusive nya funktioner och förbättringar kommer endast att levereras till användare som har Bitdefender 2020 installerat.

2.5. Smart rösthjälp

Om du använder Amazon Alexa-smarthögtalaren eller Google Assistant-appen kan du initiera röstkommandon för att köra en uppsättning uppgifter eller kontrollera information om enheterna som har Bitdefender installerat. Således kan du utföra skannings- och optimeringsuppgifter, pausa internet på de anslutna enheterna, kontrollera statusen för ditt nuvarande abonnemang eller kontrollera dina barns platser eller onlineaktiviteter. För att se hela listan över röstkommandon som du kan initiera, se Röstkommandon för att interagera med Bitdefender (sida 42).

2.5.1. Ställa in röstkommandon

Bitdefender röstkommandon kan konfigureras för:

- **Google Home-appen på**
  - Android 5.0 och senare
  - iOS 10.0 och senare

- Chromebooks

- **Amazon Alexa-appen på**
  - Eko
  - Echo Dot
  - Echo Show
  - Echo Spot
  - Fire TV Cube

Ställa in Amazon Alexa-röstkommandon för Bitdefender

För att ställa in Bitdefender röstkommandon på Amazon Alexa:

1. Öppna Amazon Alexa-appen.
2. Tryck på **Meny** ikonen och gå sedan till **Kompetens**.
3. Sök efter Bitdefender.
4. Knacka **Bitdefender** och tryck sedan på **GÖR DET MÖJLIGT**.
5. Du uppmanas att logga in på ditt Bitdefender-konto.
   Skriv ditt användarnamn och lösenord och tryck sedan på **LOGGA IN**.

Så snart synkroniseringen av Bitdefender med din Amazon Alexa är klar introduceras du i röstkommandon som du kan använda för att initiera uppgifter eller kontrollera information om enheterna som har Bitdefender installerat.

Närhelst du behöver assistenten för att ge dig listan över alla tillgängliga röstkommandon eller färdigheter, säg **HJÄLP MIG**.

Ställa in Google Home-röstkommandon för Bitdefender

Så här ställer du in röstkommandon på Google Home:

1. Öppna Google Home-appen.
2. Tryck på Meny i det övre vänstra hörnet på hemskärmen och tryck sedan på **Utforska**.
3. Sök efter Bitdefender.
4. Knacka **Bitdefender**och tryck sedan på **Länk**.

5. Du uppmanas att logga in på ditt Bitdefender-konto.
   Skriv ditt användarnamn och lösenord och tryck sedan på **LOGGA IN**.

Så snart synkroniseringen av Bitdefender med Google Home är klar introduceras du i röstkommandon som du kan använda för att initiera uppgifter eller kontrollera information om enheterna som har Bitdefender installerat.

Närhelst du behöver assistenten för att ge dig listan över alla tillgängliga röstkommandon eller färdigheter, säg **HJÄLP MIG**.

2.5.2. Röstkommandon för att interagera med Bitdefender

För att öppna Bitdefender röstkommandon:

- På Amazon Alexa: **Alexa, öppna Bitdefender**
- På Google Home: **OK, Google, prata med Bitdefender**

För att starta Bitdefender röstkommandon:

- På Amazon Alexa: **Alexa, fråga Bitdefender**
- På Google Home: **OK, Google, fråga Bitdefender**

Frågorna och uppgifterna du kan initiera när Bitdefender-assistenten är öppen är:

- Hur är min aktivitet idag?
- Vad är min prenumerationsstatus?
- Optimera mina enheter. (Detta kommando kommer att starta OneClick Optimizer på de anslutna Windows-baserade enheterna).
- Kör en snabbskanning på min [enhetstyp]. (Som enhetstyp kan man säga laptop, dator, telefon eller surfplatta).

Om du har föräldrakontroll konfigurerad på dina barns enheter, är frågorna och uppgifterna du kan initiera när Bitdefender-assistenten är öppen:

- Pausa internetanslutningen för [profilnamn].
- Återuppta internetanslutningen för [profilnamn].
- Hitta mitt barn.
- Var är mitt barn?
- Hur mycket tid spenderade mitt barn på sina enheter?

- Hur mycket tid spenderade mitt barn på Facebook idag?
- Hur mycket tid spenderade mitt barn på Instagram idag?

Om du har fler föräldrakontrollprofiler kan du säga ditt barns namn i kommandot. Till exempel, **Hitta Jennifer**.

3. HANTERA DIN SÄKERHET

3.1. Antivirusskydd

Bitdefender skyddar din enhet från alla typer av hot (skadlig programvara, trojaner, spionprogram, rootkits och så vidare). Skyddet Bitdefender erbjuder är indelat i två kategorier:

- Skanning vid åtkomst - förhindrar att nya hot kommer in i ditt system. Bitdefender kommer till exempel att skanna ett word-dokument efter kända hot när du öppnar det och ett e-postmeddelande när du får ett.

  Genomsökning vid åtkomst säkerställer realtidsskydd mot hot, vilket är en viktig komponent i alla datorsäkerhetsprogram.

  Viktig
  För att förhindra hot från att infektera din enhet, behåll **skanning vid åtkomst** aktiverad.

- Skanning på begäran - gör det möjligt att upptäcka och ta bort hotet som redan finns i systemet. Detta är den klassiska skanningen som initieras av användaren - du väljer vilken enhet, mapp eller fil Bitdefender ska skanna, och Bitdefender skannar den - på begäran.

Bitdefender skannar automatiskt alla flyttbara media som är anslutna till enheten för att se till att de kan nås på ett säkert sätt. För mer information, se Automatisk skanning av flyttbara media (sida 57).

Avancerade användare kan konfigurera skanningsundantag om de inte vill att specifika filer eller filtyper ska skannas. För mer information, se Konfigurerar skanningsundantag (sida 59).

När den upptäcker ett hot kommer Bitdefender automatiskt att försöka ta bort den skadliga koden från den infekterade filen och rekonstruera den ursprungliga filen. Denna operation kallas desinfektion. Filer som inte kan desinficeras flyttas till karantän för att innehålla infektionen. För mer information, se Hantera filer i karantän (sida 62).

Om din enhet har infekterats med hot, se Ta bort hot från ditt system (sida 133). För att hjälpa dig att rensa din enhet från hot som inte kan tas bort från Windows-operativsystemet, ger Bitdefender dig Räddningsmiljö (sida 133). Detta är en pålitlig miljö, speciellt utformad för att ta bort hot, som gör att du kan starta upp din enhet oberoende av Windows. När enheten

körs i Rescue Environment är Windows-hoten inaktiva, vilket gör det enkelt att ta bort dem.

3.1.1. Skanning vid åtkomst (realtidsskydd)

Bitdefender tillhandahåller realtidsskydd mot ett brett utbud av hot genom att skanna alla tillgängliga filer och e-postmeddelanden.

Slå på eller av realtidsskydd

Så här slår du på eller av realtidsskydd mot hot:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönster, slå på eller av **Bitdefender Shield**.
4. Om du vill inaktivera realtidsskyddet visas ett varningsfönster. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktiverat. Du kan inaktivera realtidsskydd i 5, 15 eller 30 minuter, i en timme, permanent eller tills ett system startar om. Realtidsskyddet aktiveras automatiskt när den valda tiden går ut.

Varning
Detta är en kritisk säkerhetsfråga. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat kommer du inte att skyddas mot hot.

Konfigurera avancerade inställningar för realtidsskydd

Avancerade användare kanske vill dra fördel av skanningsinställningarna som Bitdefender erbjuder. Du kan konfigurera realtidsskyddsinställningarna i detalj genom att skapa en anpassad skyddsnivå.

Så här konfigurerar du realtidsskyddets avancerade inställningar:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönstret kan du konfigurera skanningsinställningarna efter behov.

Information om skanningsalternativen

Du kan hitta den här informationen användbar:

- **Skanna endast applikationer.** Du kan ställa in Bitdefender för att endast skanna appar som är tillgängliga.
- **Skanna potentiellt oönskade applikationer.** Välj det här alternativet för att söka efter oönskade program. Ett potentiellt oönskat program (PUA) eller ett potentiellt oönskat program (PUP) är en programvara som vanligtvis levereras med gratisprogram och som visar popup-fönster eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem kommer att ändra hemsidan eller sökmotorn, andra kommer att köra flera processer i bakgrunden som saktar ner datorn eller kommer att visa många annonser. Dessa program kan installeras utan ditt samtycke (även kallat adware) eller kommer att ingå som standard i expressinstallationspaketet (reklamstöds).
- **Skanna skript.** Funktionen Skanna skript gör att Bitdefender kan skanna powershell-skript och kontorsdokument som kan innehålla skriptbaserad skadlig programvara.
- **Skanna nätverksresurser.** För att säkert få åtkomst till ett fjärrnätverk från din enhet rekommenderar vi att du håller alternativet Skanna nätverksresurser aktiverat.
- **Skanna processminne.** Söker efter skadlig aktivitet i minnet av pågående processer.
- **Skanna kommandoraden.** Genomsöker kommandoraden för nystartade program för att förhindra fillösa attacker.
- **Skanna arkiv.** Att skanna inuti arkiv är en långsam och resurskrävande process, som därför inte rekommenderas för realtidsskydd. Arkiv som innehåller infekterade filer är inte ett omedelbart hot mot säkerheten för ditt system. Hotet kan bara påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att ha realtidsskydd aktiverat.

  Om du bestämmer dig för att använda det här alternativet, aktivera det och dra sedan skjutreglaget längs skalan för att utesluta arkiv som är större än ett givet värde i MB (megabyte) från skanning.
- **Skanna startsektorer.** Du kan ställa in Bitdefender att skanna startsektorerna på din hårddisk. Denna sektor av hårddisken innehåller den nödvändiga datorkoden för att starta uppstartsprocessen. När ett hot infekterar startsektorn kan enheten bli otillgänglig och du kanske inte kan starta ditt system och komma åt dina data.

- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och modifierade filer kan du avsevärt förbättra systemets övergripande reaktionsförmåga med en minimal kompromiss i säkerhet.
- **Skanna keyloggers.** Välj det här alternativet för att skanna ditt system efter keylogger-appar. Keyloggers registrerar vad du skriver på ditt tangentbord och skickar rapporter över internet till en illvillig person (hacker). Hackaren kan ta reda på känslig information från de stulna uppgifterna, såsom bankkontonummer och lösenord, och använda den för att få personliga fördelar.
- **Tidig startskanning.** Välj **Tidig startskanning** alternativet att skanna ditt system vid uppstart så snart alla dess kritiska tjänster är laddade. Uppdraget med den här funktionen är att förbättra upptäckten av hot vid systemstart och uppstartstiden för ditt system.

Åtgärder vidtagna för upptäckta hot

Du kan konfigurera de åtgärder som vidtas av realtidsskyddet genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönstret, scrolla ner i fönstret tills du ser **Hotåtgärder** alternativ.
4. Konfigurera skanningsinställningarna efter behov.

Följande åtgärder kan vidtas av realtidsskyddet i Bitdefender:

Vidta lämpliga åtgärder

Bitdefender kommer att vidta de rekommenderade åtgärderna beroende på typen av upptäckt fil:

- **Infekterade filer.** Filer som upptäckts som infekterade matchar en del av hotinformation som finns i Bitdefender Hot Information Database. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och rekonstruera den ursprungliga filen. Denna operation kallas desinfektion.

  Filer som inte kan desinficeras flyttas till karantän för att innehålla infektionen. Filer i karantän kan inte köras eller öppnas; därför försvinner risken att bli smittad. För mer information, se Hantera filer i karantän (sida 62).

Viktig
För särskilda typer av hot är desinficering inte möjlig eftersom den upptäckta filen är helt skadlig. I sådana fall tas den infekterade filen bort från disken.

- **Misstänkta filer.** Filer upptäcks som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen desinfektionsrutin finns tillgänglig. De kommer att flyttas till karantän för att förhindra en potentiell infektion.
  Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefender-hotforskarna. Om ett hot bekräftas, släpps en hotinformationsuppdatering för att ta bort hotet.
- **Arkiv som innehåller infekterade filer.**
  - Arkiv som bara innehåller infekterade filer raderas automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer kommer Bitdefender att försöka ta bort de infekterade filerna förutsatt att det kan rekonstruera arkivet med de rena filerna. Om arkivrekonstruktion inte är möjlig kommer du att informeras om att inga åtgärder kan vidtas för att undvika att förlora rena filer.

Flytta till karantän

Flyttar upptäckta filer till karantän. Filer i karantän kan inte köras eller öppnas; därför försvinner risken att bli smittad. För mer information, se Hantera filer i karantän (sida 62).

Neka åtkomst

Om en infekterad fil upptäcks kommer åtkomsten till denna att nekas.

Återställer standardinställningarna

Standardinställningarna för realtidsskydd säkerställer ett bra skydd mot hot, med mindre inverkan på systemets prestanda.

Så här återställer du standardinställningarna för realtidsskydd:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.

3. I den **Avancerad** fönstret, scrolla ner i fönstret tills du ser **Återställ avancerade inställningar** alternativ. Välj det här alternativet för att återställa antivirusinställningarna till standardinställningarna.

3.1.2. Skanning på begäran

Huvudsyftet för Bitdefender är att hålla din enhet ren från hot. Detta görs genom att hålla nya hot borta från din enhet och genom att skanna dina e-postmeddelanden och alla nya filer som laddats ner eller kopierats till ditt system.

Det finns en risk att ett hot redan finns i ditt system, innan du ens installerat Bitdefender. Det är därför det är en mycket bra idé att skanna din enhet efter invånande hot efter att du har installerat Bitdefender. Och det är definitivt en bra idé att ofta skanna din enhet efter hot.

Skanning på begäran baseras på skanningsuppgifter. Skanningsuppgifter anger skanningsalternativen och de objekt som ska skannas. Du kan skanna enheten när du vill genom att köra standarduppgifterna eller dina egna skanningsuppgifter (användardefinierade uppgifter). Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen, konfigurera och kör en anpassad skanning.

Skanna en fil eller mapp efter hot

Du bör skanna filer och mappar när du misstänker att de kan vara infekterade. Högerklicka på filen eller mappen du vill skannas, peka på **Bitdefender** och välj **Skanna med Bitdefender**. De Antivirus Scan guide visas och guidar dig genom skanningsprocessen. I slutet av skanningen kommer du att bli ombedd att välja vilka åtgärder som ska vidtas på de upptäckta filerna, om några.

Kör en snabbskanning

Snabbskanning använder genomsökning i molnet för att upptäcka hot som körs i ditt system. Att köra en snabbsökning tar vanligtvis mindre än en minut och använder en bråkdel av de systemresurser som behövs för en vanlig antivirusskanning.

Så här kör du en snabbskanning:

1. Klicka på Skydd på navigeringsmenyn i Bitdefender-gränssnittet.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.

3. I den **Skanningar** windows klickar du på **Kör Scan** knappen bredvid **Snabbskanning**.
4. Följ Antivirus Scan guide för att slutföra skanningen. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer. Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

Kör en systemsökning

System Scan-uppgiften skannar hela enheten efter alla typer av hot som äventyrar dess säkerhet, såsom skadlig programvara, spionprogram, adware, rootkits och andra.

> **Notera**
> Därför att **Genomsökning av systemet** utför en grundlig genomsökning av hela systemet, kan genomsökningen ta ett tag. Därför rekommenderas det att köra den här uppgiften när du inte använder din enhet.

Innan du kör en systemsökning rekommenderas följande:

- Se till att Bitdefender är uppdaterad med sin databas med hotinformation. Genom att skanna din enhet med en föråldrad hotinformationsdatabas kan det hindra Bitdefender från att upptäcka nya hot som hittats sedan den senaste uppdateringen. För mer information, se Håller Bitdefender uppdaterad (sida 37).
- Stäng av alla öppna program.

Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen, konfigurera och kör en anpassad skanning. För mer information, se Konfigurera en anpassad skanning (sida 51).

Så här kör du en systemsökning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** windows klickar du på **Kör Scan** knappen bredvid **Genomsökning av systemet**.
4. Första gången du kör en systemsökning introduceras du i funktionen. Klick **Okej, förstår** att fortsätta.
5. Följ Antivirus Scan guide för att slutföra skanningen. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på

upptäckta filer. Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

Konfigurera en anpassad skanning

I den **Hantera skanningar** fönster kan du ställa in Bitdefender för att köra skanningar närhelst du anser att din enhet behöver en kontroll för potentiella hot. Du kan välja att schemalägga en Genomsökning av systemet eller a Snabbskanning, eller så kan du skapa en anpassad skanning när det passar dig.

Så här konfigurerar du en ny anpassad skanning i detalj:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** windows, klicka **+Skapa skanning**.
4. I den **Arbetsnamn** fältet, skriv ett namn för skanningen, välj sedan de platser du vill ska skannas och klicka sedan **Nästa**.
5. Konfigurera dessa allmänna alternativ:
   - **Skanna endast applikationer.** Du kan ställa in Bitdefender för att endast skanna appar som är tillgängliga.
   - **Skanningsuppgiftsprioritet.** Du kan välja vilken inverkan en skanningsprocess ska ha på systemets prestanda.
     - Auto - Prioriteten för skanningsprocessen beror på systemaktiviteten. För att säkerställa att skanningsprocessen inte kommer att påverka systemaktiviteten kommer Bitdefender att bestämma om skanningsprocessen ska köras med hög eller låg prioritet.
     - Hög - Prioriteten för skanningsprocessen kommer att vara hög. Genom att välja det här alternativet låter du andra program köras långsammare och minskar tiden som krävs för att skanningsprocessen ska slutföras.
     - Låg - Prioriteten för skanningsprocessen kommer att vara låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka den tid som krävs för att skanningsprocessen ska slutföras.
   - **Åtgärder efter skanning.** Välj vilken åtgärd Bitdefender ska vidta om inga hot hittas:

- Visa sammanfattningsfönster
- Stäng av enheten
- Stäng skanningsfönstret

6. Om du vill konfigurera skanningsalternativen i detalj, klicka på **Visa avancerade alternativ**. Du kan hitta information om de listade skanningarna i slutet av det här avsnittet.
   Klick **Nästa**.
7. Du kan aktivera **Schemalägg skanningsuppgift** om du vill, och välj sedan när den anpassade skanningen du skapade ska starta.
   - Vid systemstart
   - Dagligen
   - En gång i månaden
   - Varje vecka

   Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.
8. Klick **Spara** för att spara inställningarna och stänga konfigurationsfönstret.
   Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot kommer att hittas under skanningsprocessen kommer du att uppmanas att välja vilka åtgärder som ska vidtas på de upptäckta filerna.

Information om skanningsalternativen

Du kan hitta den här informationen användbar:

- Om du inte är bekant med några av termerna, kontrollera dem i ordlista. Du kan också hitta användbar information genom att söka på internet.
- **Skanna potentiellt oönskade applikationer.** Välj det här alternativet för att söka efter oönskade program. Ett potentiellt oönskat program (PUA) eller ett potentiellt oönskat program (PUP) är en programvara som vanligtvis levereras med gratisprogram och som visar popup-fönster eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem kommer att ändra hemsidan eller sökmotorn, andra kommer att köra flera processer i bakgrunden som saktar ner datorn eller kommer

att visa många annonser. Dessa program kan installeras utan ditt samtycke (även kallat adware) eller kommer att ingå som standard i expressinstallationspaketet (reklamstöds).

- **Skanna arkiv.** Arkiv som innehåller infekterade filer är inte ett omedelbart hot mot säkerheten för ditt system. Hotet kan bara påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att ha realtidsskydd aktiverat. Det rekommenderas dock att använda det här alternativet för att upptäcka och ta bort alla potentiella hot, även om det inte är ett omedelbart hot.
  Dra skjutreglaget längs skalan för att utesluta arkiv som är större än ett givet värde i MB (megabyte) från skanning.

  Notera
  Genom att skanna arkiverade filer ökar den totala skanningstiden och kräver mer systemresurser.

- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och modifierade filer kan du avsevärt förbättra systemets övergripande reaktionsförmåga med en minimal kompromiss i säkerhet.
- **Skanna startsektorer.** Du kan ställa in Bitdefender att skanna startsektorerna på din hårddisk. Denna sektor av hårddisken innehåller den nödvändiga datorkoden för att starta uppstartsprocessen. När ett hot infekterar startsektorn kan enheten bli otillgänglig och du kanske inte kan starta ditt system och komma åt dina data.
- **Skanna minne.** Välj det här alternativet för att skanna program som körs i systemets minne.
- **Skanna registret.** Välj det här alternativet för att skanna registernycklar. Windows-registret är en databas som lagrar konfigurationsinställningar och alternativ för Windows-operativsystemets komponenter, såväl som för installerade appar.
- **Skanna cookies.** Välj det här alternativet för att skanna cookies som lagras av webbläsare på din enhet.
- **Skanna keyloggers.** Välj det här alternativet för att skanna ditt system efter keylogger-appar. Keyloggers registrerar vad du skriver på ditt tangentbord och skickar rapporter över internet till en illvillig person (hacker). Hackaren kan ta reda på känslig information från den stulna

informationen, såsom bankkontonummer och lösenord, och använda den för att få personliga fördelar.

Antivirus Scan Wizard

När du initierar en genomsökning på begäran (till exempel högerklicka på en mapp, peka på Bitdefender och välj **Skanna med Bitdefender**), kommer Bitdefender Antivirus Scan-guiden att visas. Följ guiden för att slutföra skanningsprocessen.

Notera

Om skanningsguiden inte visas kan skanningen vara konfigurerad att köras tyst i bakgrunden. Leta efter skanningsförloppsikonen i systemfältet. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsförloppet.

Steg 1 - Utför skanning

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

Vänta på att Bitdefender ska slutföra skanningen. Skanningsprocessen kan ta ett tag, beroende på hur komplex skanningen är.

Stoppa eller pausa skanningen. Du kan sluta skanna när du vill genom att klicka **SLUTA**. Du kommer direkt till det sista steget i guiden. För att tillfälligt stoppa skanningsprocessen klickar du bara **PAUS**. Du måste klicka **ÅTERUPPTA** för att återuppta skanningen.

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

- **Lösenord.** Om du vill att Bitdefender ska skanna arkivet, välj det här alternativet och skriv lösenordet. Om du inte känner till lösenordet, välj ett av de andra alternativen.
- **Be inte om ett lösenord och hoppa över det här objektet från genomsökningen.** Välj det här alternativet för att hoppa över att skanna det här arkivet.
- **Hoppa över alla lösenordsskyddade objekt utan att skanna dem.** Välj det här alternativet om du inte vill bry dig om lösenordsskyddade arkiv.

Bitdefender kommer inte att kunna skanna dem, men en post kommer att sparas i skanningsloggen.

Välj önskat alternativ och klicka **OK** för att fortsätta skanna.

Steg 2 - Välj åtgärder

I slutet av skanningen kommer du att bli ombedd att välja vilka åtgärder som ska vidtas på de upptäckta filerna, om några.

Notera

När du kör en snabbsökning eller en systemgenomsökning, kommer Bitdefender automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer under skanningen. Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

De infekterade objekten visas i grupper, baserat på de hot de är infekterade med. Klicka på länken som motsvarar ett hot för att ta reda på mer information om de infekterade objekten.

Du kan välja en övergripande åtgärd som ska vidtas för alla frågor eller så kan du välja separata åtgärder för varje grupp av frågor. Ett eller flera av följande alternativ kan visas på menyn:

Vidta lämpliga åtgärder

Bitdefender kommer att vidta de rekommenderade åtgärderna beroende på typen av upptäckt fil:

- **Infekterade filer.** Filer som upptäckts som infekterade matchar en del av hotinformation som finns i Bitdefender Hot Information Database. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och rekonstruera den ursprungliga filen. Denna operation kallas desinfektion.

  Filer som inte kan desinficeras flyttas till karantän för att innehålla infektionen. Filer i karantän kan inte köras eller öppnas; därför försvinner risken att bli smittad. För mer information, se Hantera filer i karantän (sida 62).

Viktig

För särskilda typer av hot är desinficering inte möjlig eftersom den upptäckta filen är helt skadlig. I sådana fall tas den infekterade filen bort från disken.

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

  Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefender-hotforskarna. Om ett hot bekräftas släpps en informationsuppdatering för att ta bort hotet.

- **Arkiv som innehåller infekterade filer.**
  - Arkiv som bara innehåller infekterade filer raderas automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer kommer Bitdefender att försöka ta bort de infekterade filerna förutsatt att det kan rekonstruera arkivet med de rena filerna. Om arkivrekonstruktion inte är möjlig kommer du att informeras om att inga åtgärder kan vidtas för att undvika att förlora rena filer.

Radera

Tar bort upptäckta filer från disken.

Om infekterade filer lagras i ett arkiv tillsammans med rena filer, kommer Bitdefender att försöka ta bort de infekterade filerna och rekonstruera arkivet med de rena filerna. Om arkivrekonstruktion inte är möjlig kommer du att informeras om att inga åtgärder kan vidtas för att undvika att förlora rena filer.

Gör inga åtgärder

Inga åtgärder kommer att vidtas på de upptäckta filerna. När skanningen är klar kan du öppna skanningsloggen för att visa information om dessa filer.

Klick **Fortsätta** för att tillämpa de angivna åtgärderna.

Steg 3 - Sammanfattning

När Bitdefender har åtgärdat problemen, visas skanningsresultaten i ett nytt fönster. Om du vill ha omfattande information om skanningsprocessen, klicka **VISA LOGG** för att se skanningsloggen.

Viktig

I de flesta fall desinficerar Bitdefender framgångsrikt de infekterade filerna som den upptäcker eller isolerar infektionen. Det finns dock problem som inte kan lösas automatiskt. Om det behövs, starta om systemet för att slutföra rengöringsprocessen. För mer information och instruktioner om hur man tar bort ett hot manuellt, se Ta bort hot från ditt system (sida 133).

3.1.3. Kontrollerar skanningsloggar

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen i antivirusfönstret. Skanningsloggen innehåller detaljerad information om den loggade skanningsprocessen, såsom skanningsalternativ, skanningsmålet, hoten som hittats och de åtgärder som vidtagits mot dessa hot.

Du kan öppna skanningsloggen direkt från skanningsguiden, när skanningen är klar, genom att klicka **VISA LOGG**.

Så här kontrollerar du en skanningslogg eller någon upptäckt infektion vid ett senare tillfälle:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken väljer du meddelandet om den senaste skanningen.
   Det är här du kan hitta alla hotskanningshändelser, inklusive hot som upptäcks av skanning vid åtkomst, användarinitierade genomsökningar och statusändringar för automatiska genomsökningar.
3. I aviseringslistan kan du kontrollera vilka skanningar som har utförts nyligen. Klicka på ett meddelande för att se detaljer om det.
4. Klicka på för att öppna skanningsloggen **Visa logg**.

3.1.4. Automatisk skanning av flyttbara media

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

Upptäckta enheter faller inom en av dessa kategorier:

- CD/DVD

- Flash-enheter, såsom flash-pennor och externa hårddiskar
- mappade (fjärr) nätverksenheter

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

Hur fungerar det?

När den upptäcker en flyttbar lagringsenhet börjar Bitdefender skanna den efter hot (förutsatt att automatisk genomsökning är aktiverad för den typen av enhet). Du kommer att få ett meddelande via ett popup-fönster om att en ny enhet har upptäckts och att den skannas.

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

När skanningen är klar visas fönstret för skanningsresultat för att informera dig om du säkert kan komma åt filer på det flyttbara mediet.

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

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

Denna information kan vara användbar för dig:

- Var försiktig när du använder en hotinfekterad CD/DVD, eftersom hotet inte kan tas bort från skivan (mediet är skrivskyddat). Se till att realtidsskydd är aktiverat för att förhindra att hot sprids till ditt system. Det är bäst att kopiera all värdefull data från skivan till ditt system och sedan kassera skivan.
- I vissa fall kanske Bitdefender inte kan ta bort hot från specifika filer på grund av juridiska eller tekniska begränsningar. Ett sådant exempel är filer som arkiveras med en proprietär teknologi (detta beror på att arkivet inte kan återskapas korrekt).
  För att ta reda på hur man hanterar hot, se Ta bort hot från ditt system (sida 133).

Hantera skanning av flyttbara media

Så här hanterar du automatisk genomsökning av flyttbara media:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Välj **inställningar** fönster.

Skanningsalternativen är förkonfigurerade för bästa detekteringsresultat. Om infekterade filer upptäcks kommer Bitdefender att försöka desinficera dem (ta bort den skadliga koden) eller flytta dem till karantän. Om båda åtgärderna misslyckas låter guiden Antivirussökning dig ange andra åtgärder som ska vidtas på infekterade filer. Skanningsalternativen är standard och du kan inte ändra dem.

För bästa skydd rekommenderas det att låta valt den **Automatisk skanning** alternativ för alla typer av flyttbara lagringsenheter.

3.1.5. Skanna värdfil

Hosts-filen kommer som standard med din operativsysteminstallation och används för att mappa värdnamn till IP-adresser varje gång du går in på en ny webbsida, ansluter till en FTP eller till andra internetservrar. Det är en vanlig textfil och skadliga program kan ändra den. Avancerade användare vet hur man använder det för att blockera irriterande annonser, banners, cookies från tredje part eller kapare.

Så här konfigurerar du fil för skanningsvärd:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Avancerad** flik.
3. Slå på eller av **Skanna värdfil**.

3.1.6. Konfigurerar skanningsundantag

Bitdefender tillåter att man undantar specifika filer, mappar eller filtillägg från genomsökning. Den här funktionen är avsedd att undvika störningar i ditt arbete och den kan också bidra till att förbättra systemets prestanda. Undantag ska användas av användare som har avancerad datorkunskap eller på annat sätt följer rekommendationerna från en Bitdefender-representant.

Du kan konfigurera undantag så att de endast gäller för skanning vid åtkomst eller på begäran, eller för båda. Objekten undantagna från

skanning vid åtkomst kommer inte att skannas, oavsett om de nås av dig eller en app.

> **Notera**
> Undantag kommer INTE att gälla för kontextuell skanning. Kontextgenomsökning är en typ av skanning på begäran: du högerklickar på filen eller mappen du vill skanna och väljer **Skanna med Bitdefender**.

Undantag filer och mappar från skanning

För att undanta specifika filer och mappar från skanning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Ange sökvägen till den mapp som du vill utom genom att skanna i motsvarande fält.
   Alternativt kan du navigera till mappen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.
6. Slå på strömbrytaren bredvid skyddsfunktionen som inte ska skanna mappen. Det finns tre alternativ:
   - Antivirus
   - Hotförebyggande online
   - Avancerat hotförsvar
7. Klick **Spara** för att spara ändringarna och stänga fönstret.

Undantag filtillägg från skanning

När du undantar ett filtillägg från genomsökning, kommer Bitdefender inte längre att skanna filer med det tillägget, oavsett var de befinner sig på din enhet. Undantaget gäller även filer på flyttbara media, såsom CD-skivor, DVD-skivor, USB-lagringsenheter eller nätverksenheter.

Viktig
Var försiktig när du undantar tillägg från genomsökning eftersom sådana undantag kan göra din enhet sårbar för hot.

För att undanta filtillägg från skanning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Skriv de tillägg som du vill ska undantas från att skanna med en punkt före dem, separera dem med semikolon (;).
   `txt;avi;jpg`
6. Slå på strömbrytaren bredvid skyddsfunktionen som inte ska skanna tillägget.
7. Klick **Spara**.

Hantera skanningsundantag

Om de konfigurerade skanningsundantagen inte längre behövs, rekommenderas att du tar bort dem eller inaktiverar skanningsundantag.

Så här hanterar du skanningsundantag:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**. En lista med alla dina undantag kommer att visas.
4. För att ta bort eller redigera skanningsundantag, klicka på en av de tillgängliga knapparna. Fortsätt enligt följande:
   - För att ta bort en post från listan, klicka på 🗑 knappen bredvid.
   - För att redigera en post från tabellen, klicka på **Redigera** knappen bredvid. Ett nytt fönster visas där du kan ändra tillägget eller sökvägen som ska undantas och säkerhetsfunktionen du vill att de ska undantas från, efter behov. Gör nödvändiga ändringar och klicka sedan **ÄNDRA**.

3.1.7. Hantera filer i karantän

Bitdefender isolerar de hotinfekterade filerna som den inte kan desinficera och de misstänkta filerna i ett säkert område som heter karantän. När ett hot är i karantän kan det inte göra någon skada eftersom det inte kan verkställas eller läsas.

Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefender-hotforskarna. Om ett hot bekräftas släpps en informationsuppdatering för att ta bort hotet.

Dessutom skannar Bitdefender filerna i karantän varje gång hotinformationsdatabasen uppdateras. Rensade filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Så här kontrollerar och hanterar du filer i karantän:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Gå till **inställningar** fönster.
   Här kan du se namnet på filerna i karantän, deras ursprungliga plats och namnet på de upptäckta hoten.
4. Filer i karantän hanteras automatiskt av Bitdefender enligt standardkarantäninställningarna.
   Även om det inte rekommenderas, kan du justera karantäninställningarna enligt dina preferenser genom att klicka **Visa inställningar**.
   Klicka på omkopplarna för att slå på eller av:
   Skanna om karantänen efter uppdatering av hotinformation
   Behåll det här alternativet aktiverat för att automatiskt skanna filer i karantän efter att varje databas med hotinformation har uppdaterats. Rensade filer flyttas automatiskt tillbaka till sin ursprungliga plats.
   Ta bort innehåll som är äldre än 30 dagar
   Filer i karantän som är äldre än 30 dagar raderas automatiskt.
   Skapa undantag för återställda filer
   Filerna du återställer från karantän flyttas tillbaka till sin ursprungliga plats utan att repareras och undantas automatiskt från framtida skanningar.

5. Om du vill ta bort en fil i karantän markerar du den och klickar på **Radera** knapp. Om du vill återställa en fil i karantän till sin ursprungliga plats, välj den och klicka **Återställ**.

3.2. Avancerat hotförsvar

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

Advanced Threat Defense övervakar kontinuerligt apparna som körs på enheten och letar efter hotliknande åtgärder. Var och en av dessa åtgärder poängsätts och en totalpoäng beräknas för varje process.

Som en säkerhetsåtgärd kommer du att meddelas varje gång hot och potentiellt skadliga processer upptäcks och blockeras.

3.2.1. Slå på eller av Advanced Threat Defense

Så här aktiverar eller inaktiverar du Advanced Threat Defense:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. Gå till **inställningar** fönstret och klicka på knappen bredvid **Bitdefender Advanced Threat Defense**.

> **Notera**
> För att hålla ditt system skyddat från ransomware och andra hot rekommenderar vi att du inaktiverar Advanced Threat Defense under så kort tid som möjligt.

3.2.2. Kontrollerar upptäckta skadliga attacker

Närhelst hot eller potentiellt skadliga processer upptäcks kommer Bitdefender att blockera dem för att förhindra att din enhet infekteras av ransomware eller annan skadlig programvara. Du kan när som helst kontrollera listan över upptäckta skadliga attacker genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. Gå till **Hotförsvar** fönster.

De attacker som upptäckts under de senaste 90 dagarna visas. För att hitta information om typen av en upptäckt ransomware, sökvägen till den skadliga processen, eller om desinfektionen har lyckats, klicka helt enkelt på den.

3.2.3. Lägga till processer till undantag

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

Så här börjar du lägga till processer till undantagslistan för avancerade hotförsvar:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Ange sökvägen till den mapp som du vill utom genom att skanna i motsvarande fält.
   Alternativt kan du navigera till den körbara filen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.
6. Slå på strömbrytaren bredvid **Avancerat hotförsvar**.
7. Klick **Spara**.

3.2.4. Utnyttjar upptäckt

Ett sätt som hackare använder för att bryta mot system är att dra fördel av särskilda buggar eller sårbarheter som finns i datorprogram (appar eller plugins) och hårdvara. För att se till att din enhet håller sig borta från sådana attacker, som normalt sprids väldigt snabbt, använder Bitdefender den senaste anti-exploateringstekniken.

3.2.5. Aktivera eller inaktivera exploateringsdetektering

Så här aktiverar eller inaktiverar du upptäckt av utnyttjande:

- Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
- I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.

- Gå till **inställningar** fönstret och klicka på knappen bredvid **Exploateringsdetektering** för att slå på eller av funktionen.

> **Notera**
> Alternativet Detektering av utnyttjande är aktiverat som standard.

3.3. Hotförebyggande online

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

Bitdefender tillhandahåller hotförebyggande online i realtid för:

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

Så här konfigurerar du inställningar för onlinehotprevention:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ONLINE FÖREBYGGANDE AV HOT** rutan, klicka **inställningar**.

I den **Nätskydd** sektioner, klicka på reglagen för att slå på eller av:

- Förebyggande av webbattacker blockerar hot som kommer från internet, inklusive drive-by-nedladdningar.
- Search Advisor, en komponent som betygsätter resultaten av dina sökmotorfrågor och länkarna som publiceras på sociala nätverkswebbplatser genom att placera en ikon bredvid varje resultat:
  Du bör inte besöka denna webbsida.
  Den här webbsidan kan innehålla farligt innehåll. Var försiktig om du bestämmer dig för att besöka den.
  Detta är en säker sida att besöka.
  Search Advisor betygsätter sökresultaten från följande webbsökmotorer:

- Google
- Yahoo!
- Bing
- Baidu

Search Advisor betygsätter länkarna som publiceras på följande sociala nätverkstjänster online:

- Facebook
- Twitter

- Krypterad webbskanning.
  Mer sofistikerade attacker kan använda säker webbtrafik för att vilseleda sina offer. Därför rekommenderar vi att du håller alternativet Krypterad webbskanning aktiverat.
- Bedrägeriskydd.
- Nätfiskeskydd.

Scrolla ner så kommer du till **Förebyggande av nätverkshot** sektion. Här har du **Förebyggande av nätverkshot** alternativ. För att hålla din enhet borta från attacker från komplexa skadliga program (som ransomware) genom utnyttjande av sårbarheter, låt det här alternativet vara aktiverat.

Du kan skapa en lista över webbplatser, domäner och IP-adresser som inte kommer att skannas av Bitdefender-motorerna för anti-hot, antinätfiske och antibedrägeri. Listan bör endast innehålla webbplatser, domäner och IP-adresser som du helt litar på.

För att konfigurera och hantera webbplatser, domäner och IP-adresser med hjälp av funktionen Online Threat Prevention som tillhandahålls av Bitdefender:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ONLINE FÖREBYGGANDE AV HOT** rutan, klicka **inställningar**.
3. Klick **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Skriv i motsvarande fält namnet på webbplatsen, namnet på domänen eller IP-adressen du vill lägga till i undantag.
6. Klicka på knappen bredvid **Hotförebyggande online**.

7. För att ta bort en post från listan, klicka på 🗑 knappen bredvid.
   Klick **Spara** för att spara ändringarna och stänga fönstret.

3.3.1. Bitdefender-varningar i webbläsaren

När du försöker besöka en webbplats som klassificeras som osäker, blockeras webbplatsen och en varningssida visas i din webbläsare.

Sidan innehåller information som webbadressen och det upptäckta hotet.

Du måste bestämma dig för vad du ska göra härnäst. Följande alternativ är tillgängliga:

- Navigera bort från webbplatsen genom att klicka **TA MIG TILLBAKA TILL SÄKERHET**.
- Fortsätt till webbplatsen, trots varningen, genom att klicka **Jag förstår riskerna, ta mig dit ändå**.
- Om du är säker på att den upptäckta webbplatsen är säker klickar du på **SKICKA IN** för att lägga till det till undantag. Vi rekommenderar att du bara lägger till webbplatser som du litar på till fullo.

3.4. Sårbarhet

Ett viktigt steg för att skydda din enhet mot skadliga åtgärder och appar är att hålla operativsystemet och de appar du regelbundet använder uppdaterade. Dessutom, för att förhindra obehörig fysisk åtkomst till din enhet, måste starka lösenord (lösenord som inte är lätta att gissa) konfigureras för varje Windows-användarkonto och även för de Wi-Fi-nätverk du ansluter till.

Bitdefender tillhandahåller två enkla sätt att fixa sårbarheterna i ditt system:

- Du kan skanna ditt system efter sårbarheter och åtgärda dem steg för steg med hjälp av **Sårbarhetsskanning** alternativ.
- Med hjälp av automatisk sårbarhetsövervakning kan du kontrollera och åtgärda upptäckta sårbarheter i Aviseringar fönster.

Du bör kontrollera och fixa systemsårbarheter varannan eller varannan vecka.

3.4.1. Skanna ditt system efter sårbarheter

För att upptäcka systemsårbarheter kräver Bitdefender en aktiv internetanslutning.

För att skanna ditt system efter sårbarheter:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. I den **Sårbarhetsskanning** flikklicka **Starta skanning**, vänta sedan på att Bitdefender ska kontrollera ditt system för sårbarheter. De upptäckta sårbarheterna är grupperade i tre kategorier:
   - **OPERATIV SYSTEM**
     - **Säkerhet för operativsystem**
       Ändrade systeminställningar som kan äventyra din enhet och data, som att inte visa varningar när körda filer utför ändringar på ditt system utan din tillåtelse eller när MTP-enheter som telefoner eller kameror ansluter och utför olika operationer utan din vetskap.
     - **Kritiska Windows-uppdateringar**
       En lista över viktiga Windows-uppdateringar som inte är installerade på din dator visas. En omstart av systemet kan krävas för att tillåta Bitdefender att slutföra installationen. Observera att det kan ta ett tag att installera uppdateringarna.
     - **Svaga Windows-konton**
       Du kan se listan över Windows-användarkonton som konfigurerats på din enhet och skyddsnivån deras lösenord ger. Du kan välja mellan att be användaren att byta lösenord vid nästa inloggning eller att byta lösenord själv direkt. För att ställa in ett nytt lösenord för ditt system, välj **Ändra lösenordet nu**.
       För att skapa ett starkt lösenord rekommenderar vi att du använder en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).
   - **ANSÖKNINGAR**
     - **Webbläsarsäkerhet**

Ändra enhetens inställningar som tillåter körning av filer och program som laddas ner via Internet Explorer utan integritetsvalidering, vilket kan leda till att din enhet äventyras.

- **Appuppdateringar**
  För att se information om appen som behöver uppdateras, klicka på dess namn i listan.
  Om en app inte är uppdaterad klickar du **Ladda ner ny version** för att ladda ner den senaste versionen.

- **NÄTVERK**
  - **Nätverk och referenser**
    Ändrade systeminställningar som att automatiskt ansluta till öppna hotspot-nätverk utan din vetskap eller att inte upprätthålla kryptering på den utgående säkra kanaltrafiken.
  - **Wi-Fi-nätverk och routrar**
    För att ta reda på mer om det trådlösa nätverket och routern du är ansluten till, klicka på dess namn i listan. Om det rekommenderas att ställa in ett starkare lösenord för ditt hemnätverk, se till att du följer våra instruktioner, så att du kan hålla dig uppkopplad utan att oroa dig för din integritet.
    När andra rekommendationer finns tillgängliga, följ instruktionerna för att se till att ditt hemnätverk skyddas från hackarnas nyfikna ögon.

3.4.2. Använder automatisk sårbarhetsövervakning

Bitdefender skannar ditt system efter sårbarheter regelbundet, i bakgrunden, och håller register över upptäckta problem i Aviseringar fönster.

Så här kontrollerar och åtgärdar du de upptäckta problemen:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken väljer du meddelandet om sårbarhetsgenomsökningen.
3. Du kan se detaljerad information om de upptäckta systemets sårbarheter. Beroende på problemet, fortsätt enligt följande för att åtgärda en specifik sårbarhet:
   - Om Windows-uppdateringar är tillgängliga klickar du på **Installera**.

- Om automatisk Windows-uppdatering är inaktiverad klickar du på **Gör det möjligt**.
- Om en app är föråldrad klickar du på **Uppdatera nu** för att hitta en länk till leverantörens webbsida där du kan installera den senaste versionen av den appen.
- Om ett Windows-användarkonto har ett svagt lösenord, klicka **ändra lösenord** för att tvinga användaren att ändra lösenordet vid nästa inloggning eller ändra lösenordet själv. För ett starkt lösenord, använd en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).
- Om Windows Autorun-funktionen är aktiverad klickar du på **Fixera** för att inaktivera den.
- Om routern du har konfigurerat har angett ett svagt lösenord, klicka på **ändra lösenord** för att komma åt dess gränssnitt där du kan ställa in ett starkt.
- Om nätverket du är ansluten till har sårbarheter som kan utsätta ditt system för risk, klicka **Ändra Wi-Fi-inställningar**.

Så här konfigurerar du inställningarna för sårbarhetsövervakning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.

   Viktig
   För att automatiskt bli meddelad om system- eller appsårbarheter, behåll **Sårbarhet** alternativet aktiverat.

3. Gå till **inställningar** flik.
4. Välj de systemsårbarheter som du vill ska kontrolleras regelbundet genom att använda motsvarande växlar.

   Windows-uppdateringar
   Kontrollera om ditt Windows-operativsystem har de senaste kritiska säkerhetsuppdateringarna från Microsoft.

   Appuppdateringar
   Kontrollera om appar som är installerade på ditt system är uppdaterade. Föråldrade appar kan utnyttjas av skadlig programvara, vilket gör din dator sårbar för attacker utifrån.

   Användarlösenord

Kontrollera om lösenorden för Windows-konton och routrar som är konfigurerade på systemet är lätta att gissa eller inte. Att ställa in lösenord som är svåra att gissa (starka lösenord) gör det mycket svårt för hackare att bryta sig in i ditt system. Ett starkt lösenord inkluderar stora och små bokstäver, siffror och specialtecken (som #, $ eller @).

Autospela

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

Vissa typer av hot använder Autorun för att spridas automatiskt från flyttbara media till datorn. Det är därför det rekommenderas att inaktivera denna Windows-funktion.

Wi-Fi säkerhetsrådgivare

Kontrollera om det trådlösa hemnätverket du är ansluten till är säkert eller inte, och om det har sårbarheter. Kontrollera också om lösenordet för din hemrouter är tillräckligt starkt och hur du kan göra det säkrare.

De flesta oskyddade trådlösa nätverk är inte säkra, vilket gör att hackarnas nyfikna ögon har tillgång till dina privata aktiviteter.

Notera

Om du stänger av övervakning av en specifik sårbarhet kommer relaterade problem inte längre att registreras i meddelandefönstret.

3.4.3. Wi-Fi säkerhetsrådgivare

När du är på språng, arbetar på ett kafé eller väntar på flygplatsen kan det vara den snabbaste lösningen att ansluta till ett allmänt trådlöst nätverk för att göra betalningar, kolla e-post eller konton i sociala nätverk. Men nyfikna ögon som försöker kapa din personliga data kan vara där och se hur informationen läcker genom nätverket.

Personuppgifter avser lösenorden och användarnamnen du använder för att få tillgång till dina onlinekonton, såsom e-post, bankkonton, konton i sociala medier, men även de meddelanden du skickar.

Vanligtvis är det mer sannolikt att offentliga trådlösa nätverk är osäkra eftersom de inte kräver lösenord vid inloggning, och om de gör det kan lösenordet göras tillgängligt för alla som vill ansluta. Dessutom kan de vara skadliga nätverk eller nätverk som representerar ett mål för cyberbrottslingar.

För att skydda dig mot farorna med osäkra eller okrypterade offentliga trådlösa hotspots analyserar Bitdefender Wi-Fi Security Advisor hur säkert ett trådlöst nätverk är, och vid behov rekommenderar den att du använder Bitdefender VPN.

Bitdefender Wi-Fi Security Advisor ger information om:

- Hemma Wi-Fi-nätverk
- Office Wi-Fi-nätverk
- Offentliga Wi-Fi-nätverk

Slå på eller av aviseringar från Wi-Fi Security Advisor

Så här slår du på eller av Wi-Fi Security Advisor-meddelanden:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **inställningar** fönstret och slå på eller av **Wi-Fi säkerhetsrådgivare** alternativ.

Konfigurera Wi-Fi-hemnätverk

Så här börjar du konfigurera ditt hemnätverk:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **Wi-Fi säkerhetsrådgivare** fönstret och klicka **Hemma Wi-Fi**.
4. I den **Hemma Wi-Fi** fliken, klicka **VÄLJ HEM WI-FI**.
   En lista med de trådlösa nätverk som du anslutit till hittills visas.
5. Peka på ditt hemnätverk och klicka sedan **VÄLJ**.

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

För att ta bort det trådlösa nätverket du har ställt in som ett hemnätverk, klicka på **AVLÄGSNA** knapp.

För att lägga till ett nytt trådlöst nätverk som hem, klicka **Välj nytt hem wi-fi**.

Konfigurera Office Wi-Fi-nätverk

Så här börjar du konfigurera ditt kontorsnätverk:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **Wi-Fi säkerhetsrådgivare** fönster, klicka **Office Wi-Fi**.
4. I den **Office Wi-Fi** fliken, klicka **VÄLJ KONTOR WI-FI**.
   En lista med de trådlösa nätverk som du anslutit till hittills visas.
5. Peka på ditt kontorsnätverk och klicka sedan **VÄLJ**.

Om ett kontorsnätverk anses osäkert eller osäkert visas konfigurationsrekommendationer för att förbättra dess säkerhet.

För att ta bort det trådlösa nätverket du har ställt in som kontorsnätverk, klicka på **AVLÄGSNA**.

För att lägga till ett nytt trådlöst nätverk som kontor, klicka **Välj nytt kontorswi-fi**.

Offentligt Wi-Fi

När den är ansluten till ett osäkert eller osäkert trådlöst nätverk är den offentliga Wi-Fi-profilen aktiverad. När du kör i den här profilen, Bitdefender Antivirus Plus är inställd på att automatiskt utföra följande programinställningar:

- Advanced Threat Defense är aktiverat
- Bitdefender-brandväggen är påslagen och följande inställningar tillämpas på din trådlösa adapter:
  - Stealth-läge - PÅ
  - Nätverkstyp - Offentlig
- Följande inställningar från Online Threat Prevention är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägerier
  - Skydd mot nätfiske
- En knapp som öppnar Bitdefender Safepay™ är tillgänglig. I det här fallet är hotspot-skyddet för osäkra nätverk aktiverat som standard.

Kontrollera information om Wi-Fi-nätverk

Så här kontrollerar du information om de trådlösa nätverk du vanligtvis ansluter till:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **Wi-Fi säkerhetsrådgivare** fönster.
4. Beroende på vilken information du behöver, välj en av de tre flikarna, **Hemma Wi-Fi**, **Office Wi-Fi** eller **Offentligt Wi-Fi**.
5. Klick **Visa detaljer** bredvid nätverket du vill hitta mer information om.

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

Wi-Fi är osäkert - indikerar att säkerhetsnivån för nätverket är låg. Detta innebär att det finns en hög risk att använda den, och det rekommenderas inte att göra betalningar eller kontrollera bankkonton utan ett extra skydd. I sådana situationer rekommenderar vi att du använder Bitdefender Safepay™ med Hotspot-skydd för osäkra nätverk aktiverat.

Wi-Fi är osäkert - indikerar att säkerhetsnivån för nätverket är måttlig. Detta innebär att den kan ha sårbarheter och det rekommenderas inte att göra betalningar eller kontrollera bankkonton utan ett extra skydd. I sådana situationer rekommenderar vi att du använder Bitdefender Safepay™ med Hotspot-skydd för osäkra nätverk aktiverat.

Wi-Fi är säkert - indikerar att nätverket du använder är säkert. I det här fallet kan du använda känsliga uppgifter för att göra onlineoperationer.

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

- **Säkrad** - här kan du se om det valda nätverket är skyddat eller inte. Okrypterade nätverk kan lämna data du använder exponerad.
- **Krypteringstyp** - här kan du se vilken krypteringstyp som används av det valda nätverket. Vissa krypteringstyper kanske inte är säkra. Därför rekommenderar vi starkt att du kontrollerar information om den visade krypteringstypen för att vara säker på att du är skyddad när du surfar på webben.

- **Kanal/frekvens** - här kan du se kanalfrekvensen som används av det valda nätverket.
- **Lösenordsstyrka** - här kan du se hur starkt lösenordet är. Observera att de nätverk som har angett svaga lösenord är ett mål för cyberbrottslingar.
- **Typ av inloggning** - här kan du se om det valda nätverket är skyddat med ett lösenord eller inte. Det rekommenderas starkt att endast ansluta till nätverk som har ställt in starka lösenord.
- **Autentiseringstyp** - här kan du se vilken autentiseringstyp som används av det valda nätverket.

3.5. Ransomware-sanering

Bitdefender Ransomware Remediation säkerhetskopierar dina filer såsom dokument, bilder, videor eller musik för att se till att de är skyddade från att skadas eller förloras i händelse av ransomware-kryptering. Varje gång en ransomware-attack upptäcks kommer Bitdefender att blockera alla processer som är involverade i attacken och starta åtgärdsprocessen. På så sätt kommer du att kunna återställa innehållet i hela dina filer utan att betala för någon begärd lösen.

3.5.1. Slå på eller av Ransomware Remediation

Så här slår du på eller av Ransomware Remediation:

1. 1. Klicka **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **RANSOMWARE ÅTGÄRD** rutan, slå på eller av strömbrytaren.

> **Notera**
> För att säkerställa att dina filer är skyddade mot ransomware rekommenderar vi att du håller Ransomware Remediation aktiverat.

3.5.2. Slå på eller av automatisk återställning

Automatisk återställning ser till att dina filer automatiskt återställs i händelse av ransomware-kryptering.

Så här aktiverar eller inaktiverar du automatisk återställning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.

2. I den **RANSOMWARE ÅTGÄRD** rutan, klicka **Hantera**.
3. Slå på eller av i fönstret Inställningar **Automatisk återställning** växla.

3.5.3. Visa filer som har återställts automatiskt

När **Automatisk återställning** alternativet är aktiverat, kommer Bitdefender automatiskt att återställa filer som krypterades av ett ransomware. Härigenom kan du njuta av en bekymmersfri upplevelse och veta att dina filer är säkra.

Så här visar du filer som har återställts automatiskt:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken, välj aviseringen om det senast åtgärdade ransomware-beteendet och klicka sedan **Återställda filer**.
   Listan med de återställda filerna visas. Här kan du också se platsen där dina filer har återställts.

3.5.4. Återställa krypterade filer manuellt

Om du måste återställa filer som krypterades av ett ransomware manuellt, följ dessa steg:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken, välj meddelandet om det senaste ransomware-beteendet som upptäckts och klicka sedan **Krypterade filer**.
3. Listan med de krypterade filerna visas.
   Klick **Återställ filer** att fortsätta.
4. Om hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de dekrypterade filerna ska sparas. Klick **Återställ plats**, och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.
   Klick **Avsluta** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas om 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;

3.5.5. Lägga till applikationer till undantag

Du kan konfigurera undantagsregler för betrodda appar så att Ransowmare Remediation-funktionen inte blockerar dem om de utför ransomware-liknande åtgärder.

Så här lägger du till appar till undantagslistan för Ransomware Remediation:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **RANSOMWARE ÅTGÄRD** rutan, klicka **Hantera**.
3. Gå till **Undantag** fönstret och klicka **+Lägg till ett undantag**.

3.6. Antispårare

Många webbplatser du besöker använder spårare för att samla in information om ditt beteende, antingen för att dela den med tredjepartsföretag eller för att visa annonser som är mer relevanta för dig. Härmed tjänar webbplatsägare pengar för att kunna ge dig innehåll gratis eller fortsätta att fungera. Förutom att samla in information kan spårare sakta ner din surfupplevelse eller slösa bort din bandbredd.

Med Bitdefender Anti-tracker-tillägget aktiverat i din webbläsare undviker du att bli spårad så att dina data förblir privata medan du surfar online och du påskyndar den tid som webbplatser behöver laddas.

Bitdefender-tillägget är kompatibelt med följande webbläsare:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

De spårare vi upptäcker är grupperade i följande kategorier:

- **Reklam** - används för att analysera webbplatstrafik, användarbeteende eller besökarnas trafikmönster.

- **Kundinteraktion** - används för att mäta användarinteraktion med olika inmatningsformer som chatt eller support.
- **Grundläggande** - används för att övervaka viktiga webbsidors funktioner.
- **Webbplatsanalys** - används för att samla in data om webbsidaanvändning.
- **Sociala media** - används för att övervaka social publik, aktivitet och användarengagemang med olika sociala medieplattformar.

3.6.1. Anti-tracker gränssnitt

När Bitdefender Anti-tracker-tillägget är aktiverat, visas bredvid sökfältet i din webbläsare. Varje gång du besöker en webbplats kan en räknare märkas på ikonen som hänvisar till de upptäckta och blockerade spårarna. För att se mer information om de blockerade spårarna, klicka på ikonen för att öppna gränssnittet. Förutom antalet blockerade spårare kan du se hur lång tid det tar för sidan att ladda och kategorierna som de upptäckta spårarna tillhör. För att se listan över webbplatser som spårar, klicka på önskad kategori.

För att inaktivera Bitdefender från att blockera spårare på webbplatsen du för närvarande besöker, klicka **Pausa skyddet på denna webbplats**. Den här inställningen gäller bara så länge du har webbplatsen öppen och kommer att återställas till det ursprungliga tillståndet när du stänger webbplatsen.

För att tillåta spårare från en specifik kategori att övervaka din aktivitet, klicka på önskad aktivitet och klicka sedan på motsvarande knapp. Om du ändrar dig, klicka på samma knapp en gång till.

3.6.2. Stänger av Bitdefender Anti-tracker

Så här stänger du av Bitdefender Anti-tracker:

- Från din webbläsare:
  1. Öppna din webbläsare.
  2. Klicka på ikonen bredvid adressfältet i din webbläsare.
  3. Klicka på ikonen i det övre högra hörnet.
  4. Använd motsvarande strömbrytare för att stänga av. Bitdefender-ikonen blir grå.

- Från Bitdefender-gränssnittet:
  1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **ANTI-TRACKER** rutan, klicka **inställningar**.
  3. Bredvid webbläsaren som du vill inaktivera tillägget för, stäng av motsvarande strömbrytare.

3.6.3. Tillåter att en webbplats spåras

Om du vill bli spårad när du besöker en viss webbplats kan du lägga till dess adress till undantag enligt följande:

1. Öppna din webbläsare.
2. Klicka på ikonen bredvid sökfältet.
3. Klicka på ikonen i det övre högra hörnet.
4. Om du är på webbplatsen du vill lägga till undantag klickar du på **Lägg till aktuell webbplats till listan**.
   Om du vill lägga till en annan webbplats anger du dess adress i motsvarande fält och klickar sedan .

3.7. VPN

VPN-appen kan installeras från din Bitdefender-produkt och användas varje gång du vill lägga till ett extra skyddslager till din anslutning. VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter för att säkra din anslutning, kryptera data med bankklassad kryptering och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet nästan omöjlig att identifieras genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via Bitdefender VPN, kan du komma åt innehåll som normalt är begränsat i specifika områden.

Notera

Vissa länder utövar internetcensur och därför har användningen av VPN på deras territorium förbjudits enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen för första gången. Genom att fortsätta använda appen bekräftar du att du är medveten om tillämpliga landsbestämmelser och de risker som du kan utsättas för.

3.7.1. Installerar VPN

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

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VPN** rutan, klicka **Installera VPN**.
3. I fönstret med beskrivningen av VPN-appen, läs **Prenumerationsavtal**, och klicka sedan **INSTALLERA BITDEFENDER VPN**.
   Vänta några ögonblick tills filerna har laddats ner och installerats.
   Om en annan VPN-app upptäcks rekommenderar vi att du avinstallerar den. Efter att ha installerat flera VPN-lösningar kan du stöta på systemavbrott eller andra funktionsproblem.
4. Klick **ÖPPNA BITDEFENDER VPN** för att avsluta installationsprocessen.

Notera
Bitdefender VPN kräver att .Net Framework 4.5.2 eller högre installeras. Om du inte har det här paketet installerat visas ett meddelandefönster. Klick **installera .Net Framework** att omdirigeras till en sida där du kan ladda ner den senaste versionen av denna programvara.

3.7.2. Öppnar VPN

För att komma åt huvudgränssnittet för Bitdefender VPN, använd en av följande metoder:

- Från systemfältet
  1. Högerklicka på ikonen i systemfältet och klicka sedan på **Show**.
- Från Bitdefender-gränssnittet
  1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **VPN** rutan, klicka **Öppna VPN**.

3.7.3. VPN-gränssnitt

VPN-gränssnittet visar status för appen, ansluten eller frånkopplad. Serverplatsen för användare med gratisversionen ställs automatiskt in av Bitdefender till den mest lämpliga servern, medan premiumanvändare har möjlighet att ändra serverplatsen de vill ansluta till. För mer information om VPN-prenumerationer, se Prenumerationer (sida 82).

För att ansluta eller koppla från, klicka helt enkelt på statusen som visas högst upp på skärmen, eller högerklicka på ikonen i systemfältet. Ikonen i systemfältet visar en grön bock när VPN är ansluten och en röd bock när VPN är frånkopplat.

När du är ansluten visas den förflutna tiden och bandbreddsanvändningen på den nedre delen av gränssnittet.

För att se **Meny** område helt, klicka på ≡ ikonen uppe till vänster. Här har du följande alternativ:

- **Mitt konto** - detaljer om ditt Bitdefender-konto och VPN-prenumeration visas. Klick **Byt konto** om du vill logga in med ett annat konto.
  Klick **Lägg till det här** för att lägga till en aktiveringskod för Bitdefender Premium VPN.
- **inställningar** – beroende på dina behov kan du anpassa beteendet hos din produkt. Inställningarna är grupperade i två kategorier:
  - **Allmän**
    - Aviseringar
    - Start - välj om du vill köra Bitdefender VPN vid start eller inte
    - Produktrapporter – skicka in anonyma produktrapporter för att hjälpa oss att förbättra din upplevelse
    - Mörkt läge
    - Språk
  - **Avancerad**
    - Internet Kill-Switch - den här funktionen stänger tillfälligt av all internettrafik om VPN-anslutningen av misstag bryts. Så snart du är online igen kommer VPN-anslutningen att återupprättas.
    - Autoanslut - Anslut Bitdefender VPN automatiskt när du ansluter till ett offentligt/osäkert Wi-Fi-nätverk eller när en peer-to-peer fildelningsapp startas
- **Stöd** - du kan komma åt supportcenterplattformen där du kan läsa en användbar artikel om hur du använder Bitdefender VPN eller skicka feedback till oss.
- **Handla om** - information om den installerade versionen visas.

3.7.4. Prenumerationer

Bitdefender VPN erbjuder gratis en daglig trafikkvot på 200 MB per enhet för att säkra din anslutning varje gång du behöver, och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad tillgång till innehåll över hela världen genom att välja en serverplats efter din vilja, uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst genom att klicka på **Uppgradera** knappen tillgänglig i produktgränssnittet.

Bitdefender Premium VPN-prenumeration är oberoende av Bitdefender Antivirus Plus prenumeration, vilket innebär att du kommer att kunna använda den under hela dess tillgänglighet, oavsett status för säkerhetslösningsprenumerationen. Om Bitdefender Premium VPN-prenumeration går ut, men den för Bitdefender Antivirus Plus fortfarande är aktiv kommer du att återgå till gratisplanen.

Bitdefender VPN är en plattformsoberoende produkt, tillgänglig i Bitdefender-produkter som är kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kommer du att kunna använda ditt abonnemang på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

3.8. Safepay-säkerhet för onlinetransaktioner

Datorn blir snabbt det främsta verktyget för shopping och bank. Att betala räkningar, överföra pengar, köpa i stort sett allt du kan tänka dig har aldrig varit snabbare eller enklare.

Det handlar om att skicka personlig information, konto- och kreditkortsdata, lösenord och andra typer av privat information över internet, med andra ord exakt den typ av informationsflöde som cyberbrottslingar är mycket intresserade av att utnyttja. Hackare är obevekliga i sina ansträngningar att stjäla denna information, så du kan aldrig vara för försiktig med att säkra onlinetransaktioner.

Bitdefender Safepay™ är först och främst en skyddad webbläsare, en förseglad miljö som är utformad för att hålla din onlinebank, e-shopping och alla andra typer av onlinetransaktioner privata och säkra.

För bästa integritetsskydd har Bitdefender Password Manager integrerats i Bitdefender Safepay™ för att säkra dina referenser när du vill komma åt privata onlineplatser.

Bitdefender Safepay™ erbjuder följande funktioner:

- Det blockerar åtkomst till ditt skrivbord och alla försök att ta ögonblicksbilder av din skärm.
- Det skyddar dina hemliga lösenord när du surfar online med Password Manager.
- Den levereras med ett virtuellt tangentbord som, när det används, gör det omöjligt för hackare att läsa dina tangenttryckningar.
- Det är helt oberoende av dina andra webbläsare.
- Den kommer med inbyggt hotspot-skydd som kan användas när din enhet är ansluten till osäkra Wi-fi-nätverk.
- Den stöder bokmärken och låter dig navigera mellan dina favoritbanker/shoppingsajter.
- Det är inte begränsat till bank och e-shopping. Alla webbplatser kan öppnas i Bitdefender Safepay™.

3.8.1. Använder Bitdefender Safepay™

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

För att komma åt huvudgränssnittet för Bitdefender Safepay™, använd en av följande metoder:

- Från Bitdefender-gränssnitt:
  1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **SAFEPAY** rutan, klicka **inställningar**.
  3. I den **Safepay** fönster, klicka **Starta Safepay**.
- Från Windows:
  - I **Windows 7**:
    1. Klick **Start** och gå till **Alla program**.

2. Klick **Bitdefender**.
3. Klick **Bitdefender Safepay™**.

- I **Windows 8** och **Windows 8.1**:
  Leta upp Bitdefender Safepay™ från startskärmen i Windows (du kan till exempel börja skriva "Bitdefender Safepay™" direkt på startskärmen) och klicka sedan på ikonen.
- I **Windows 10** och **Windows 11**:
  Skriv "Bitdefender Safepay™" i sökrutan från aktivitetsfältet och klicka på dess ikon.

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

- ange webbadresser du vill gå till i adressfältet.
- lägg till flikar för att besöka flera webbplatser i Bitdefender Safepay™-fönstret genom att klicka ⊞ .
- navigera fram och tillbaka och uppdatera sidor med hjälp av ← → ↻ respektive.
- komma åt Bitdefender Safepay™ inställningar genom att klicka och välja **inställningar**.
- skydda dina lösenord med Lösenordshanteraren genom att klicka .
- hantera din bokmärken genom att klicka ☆ bredvid adressfältet.
- öppna det virtuella tangentbordet genom att klicka .
- öka eller minska webbläsarens storlek genom att trycka samtidigt **Ctrl** och den **+/-** knapparna på det numeriska tangentbordet.
- visa information om din Bitdefender-produkt genom att klicka ⋯ och välja **Handla om**.
- skriv ut viktig information genom att klicka ⋯ och välja **Skriva ut**.

Notera
För att växla mellan Bitdefender Safepay™ och Windows skrivbord, tryck på **Alt+Tab** eller klicka på **Växla till skrivbordet** alternativet på den övre vänstra sidan av fönstret.

3.8.2. Konfigurera inställningar

Klick ··· och välj **inställningar** för att konfigurera Bitdefender Safepay™:

Tillämpa Bitdefender Safepay-regler för tillgängliga domäner

Webbplatserna du har lagt till Bokmärken med **Öppna automatiskt i Safepay** alternativet aktiverat visas här. Om du vill sluta automatiskt öppna en webbplats från listan med Bitdefender Safepay™, klicka på × bredvid den önskade posten från **Avlägsna** kolumn.

Blockera popup-fönster

Du kan välja att blockera popup-fönster genom att klicka på motsvarande knapp.

Du kan också skapa en lista över webbplatser att tillåta popup-fönster från. Listan bör endast innehålla webbplatser som du litar på till fullo.

För att lägga till en webbplats i listan, ange dess adress i motsvarande fält och klicka **LÄGG TILL DOMÄN**.

För att ta bort en webbplats från listan, välj X som motsvarar önskad post.

Hantera plugins

Du kan välja om du vill aktivera eller inaktivera specifika plugins i Bitdefender Safepay™.

Hantera certifikat

Du kan importera certifikat från ditt system till ett certifikatlager.

Klick **IMPORTERA** och följ guiden för att använda certifikaten i Bitdefender Safepay™.

Använd virtuellt tangentbord

Det virtuella tangentbordet visas automatiskt när ett lösenordsfält väljs.

Använd motsvarande omkopplare för att aktivera eller inaktivera funktionen.

Utskriftsbekräftelse

Aktivera det här alternativet om du vill ge din bekräftelse innan utskriftsprocessen startar.

3.8.3. Hantera bokmärken

Om du inaktiverade den automatiska upptäckten av vissa eller alla webbplatser, eller Bitdefender helt enkelt inte upptäcker vissa webbplatser,

kan du lägga till bokmärken till Bitdefender Safepay™ så att du enkelt kan starta favoritwebbplatser i framtiden.

Följ dessa steg för att lägga till en URL till Bitdefender Safepay™-bokmärken:

1. Klick ··· och välj **Bokmärken** för att öppna sidan Bokmärken.

   Notera
   Bokmärkessidan öppnas som standard när du startar Bitdefender Safepay™.

2. Klicka på **+** för att lägga till ett nytt bokmärke.
3. Skriv in webbadressen och titeln på bokmärket och klicka sedan **SKAPA**. Kolla **Öppna automatiskt i Safepay** alternativet om du vill att den bokmärkta sidan ska öppnas med Bitdefender Safepay™ varje gång du kommer åt den. URL:en läggs också till i listan Domäner på inställningssidan.

3.8.4. Stänger av Safepay-aviseringar

När en banksajt upptäcks ställs Bitdefender-produkten in för att meddela dig via ett popup-fönster.

Så här stänger du av Safepay-aviseringarna:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SAFEPAY** rutan, klicka **inställningar**.
3. I den **inställningar** fönster, stäng av strömbrytaren bredvid **Safepay-aviseringar**.

3.8.5. Använder VPN med Safepay

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

Så här börjar du använda VPN-appen tillsammans med Safepay:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SAFEPAY** rutan, klicka **inställningar**.

3. I den **inställningar** fönster, slå på knappen bredvid **Använd VPN med Safepay**.

3.9. USB-immuniserare

Autorun-funktionen inbyggd i Windows operativsystem är ett mycket användbart verktyg som gör att enheter automatiskt kan köra en fil från media som är anslutna till den. Programvaruinstallationer kan till exempel starta automatiskt när en CD-skiva sätts in i den optiska enheten.

Tyvärr kan den här funktionen också användas av hot för att automatiskt starta och infiltrera din enhet från omskrivbara media som USB-minnen och minneskort anslutna via kortläsare. Många Autorun-baserade attacker har skapats under de senaste åren.

Med USB Immunizer kan du förhindra att någon NTFS-, FAT32- eller FAT-formaterad flash-enhet automatiskt utför hot någonsin igen. När en USB-enhet har immuniserats kan hot inte längre konfigurera den att köra en viss app när enheten är ansluten till en enhet som kör Windows.

Så här immuniserar du en USB-enhet:

1. Anslut flashenheten till din enhet.
2. Bläddra i din enhet för att hitta den flyttbara lagringsenheten och högerklicka på dess ikon.
3. Peka på i den sammanhangsberoende menyn **Bitdefender** och välj **Immunisera denna enhet**.

Notera

Om enheten redan har immuniserats visas meddelandet **USB-enheten är skyddad mot autorun-baserat hot** visas istället för alternativet Immunisera.

För att förhindra din enhet från att starta hot från oimmuniserade USB-enheter, inaktivera media-autorun-funktionen. För mer information, se Använder automatisk sårbarhetsövervakning (sida 69).

4. VERKTYG

4.1. Profiler

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

Bitdefender tillhandahåller följande profiler:

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

Om du bestämmer dig för att inte använda **Profiler**, en standardprofil som kallas **Standard** är aktiverat och det ger ingen optimering till ditt system.

Beroende på din aktivitet tillämpas följande produktinställningar när jobb-, film- eller spelprofiler är aktiverade:

- Alla Bitdefender-varningar och popup-fönster är inaktiverade.
- Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Antispam-funktionen är aktiverad.
- Sökrådgivare är ur funktion.
- Aviseringar om specialerbjudanden är inaktiverade.

Beroende på din aktivitet tillämpas följande systeminställningar när jobb-, film- eller spelprofiler är aktiverade:

- Windows Automatiska uppdateringar skjuts upp.
- Windows-varningar och popup-fönster är inaktiverade.
- Onödiga bakgrundsprogram stängs av.
- Visuella effekter justeras för bästa prestanda.

- Underhållsuppgifter skjuts upp.
- Inställningarna för energischemat justeras.

När du kör i den offentliga Wi-Fi-profilen, Bitdefender Antivirus Plus är inställd på att automatiskt utföra följande programinställningar:

- Advanced Threat Defense är aktiverat
- Bitdefender-brandväggen är påslagen och följande inställningar tillämpas på din trådlösa adapter:
  - Stealth-läge - PÅ
  - Nätverkstyp - Offentlig
- Följande inställningar från Online Threat Prevention är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägerier
  - Skydd mot nätfiske

4.1.1. Arbetsprofil

Att köra flera uppgifter på jobbet, som att skicka e-post, ha en videokommunikation med dina avlägsna kollegor eller arbeta med designappar kan påverka din systemprestanda. Arbetsprofilen har utformats för att hjälpa dig att förbättra din arbetseffektivitet genom att stänga av några av dina bakgrundstjänster och underhållsuppgifter.

Konfigurerar arbetsprofil

Så här konfigurerar du de åtgärder som ska vidtas i arbetsprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** knappen från området Arbetsprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på jobbappar
   - Optimera produktinställningar för arbetsprofilen
   - Skjut upp bakgrundsprogram och underhållsuppgifter

- Skjut upp Windows automatiska uppdateringar

5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till appar manuellt i listan med arbetsprofiler

Om Bitdefender inte automatiskt går in i arbetsprofilen när du startar en viss jobbapp, kan du lägga till appen manuellt i **Lista över arbetsansökningar**.

Så här lägger du till appar manuellt till listan över appar för arbete i arbetsprofil:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** knappen från området Arbetsprofil.
4. I den **Arbetsprofilinställningar** fönster, klicka **Applikationslista**.
5. Klick **LÄGG TILL**.
   Ett nytt fönster visas. Bläddra till appens körbara fil, välj den och klicka **OK** för att lägga till den i listan.

4.1.2. Filmprofil

Att visa videoinnehåll av hög kvalitet, t.ex. högupplösta filmer, kräver betydande systemresurser. Movie Profile justerar system- och produktinställningar så att du kan njuta av en oavbruten och sömlös filmupplevelse.

Konfigurera filmprofil

Så här konfigurerar du de åtgärder som ska vidtas i filmprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** från filmprofilområdet.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestandan på videospelare
   - Optimera produktinställningar för filmprofil

- Skjut upp bakgrundsprogram och underhållsuppgifter
- Skjut upp Windows automatiska uppdateringar
- Justera energischemainställningar för filmer

5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till videospelare manuellt till filmprofillistan

Om Bitdefender inte automatiskt går in i filmprofilen när du startar en viss videospelarapp, kan du lägga till appen manuellt i **Filmapplikationslista**.

Så här lägger du till videospelare manuellt i filmprogramlistan i filmprofil:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** från filmprofilområdet.
4. I den **Filmprofilinställningar** fönster, klicka **Spelarlista**.
5. Klick **LÄGG TILL**.
   Ett nytt fönster visas. Bläddra till appens körbara fil, välj den och klicka **OK** för att lägga till den i listan.

4.1.3. Spelprofil

Att njuta av en oavbruten spelupplevelse handlar om att minska systembelastningen och minska nedgångarna. Genom att använda beteendeheuristik tillsammans med en lista över kända spel kan Bitdefender automatiskt upptäcka pågående spel och optimera dina systemresurser så att du kan njuta av din spelpaus.

Konfigurera spelprofil

Så här konfigurerar du de åtgärder som ska vidtas i spelprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **Konfigurera** från spelprofilområdet.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på spel

- Optimera produktinställningar för spelprofilen
- Skjut upp bakgrundsprogram och underhållsuppgifter
- Skjut upp Windows automatiska uppdateringar
- Justera energischemainställningar för spel

5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Lägger till spel manuellt i spellistan

Om Bitdefender inte automatiskt går in i spelprofilen när du startar ett visst spel eller en viss app, kan du lägga till appen manuellt i **Lista över spelapplikationer**.

Så här lägger du till spel manuellt i spelapplikationslistan i spelprofil:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **Konfigurera** från spelprofilområdet.
4. I den **Spelprofilinställningar** fönster, klicka **Spellista**.
5. Klick **LÄGG TILL**.
   Ett nytt fönster visas. Bläddra till spelets körbara fil, välj den och klicka **OK** för att lägga till den i listan.

4.1.4. Offentlig Wi-Fi-profil

Att skicka e-postmeddelanden, skriva känsliga uppgifter eller handla online medan du är ansluten till osäkra trådlösa nätverk kan utsätta dina personuppgifter för risker. Public Wi-Fi Profile justerar produktinställningar för att ge dig möjlighet att göra betalningar online och använda känslig information i en skyddad miljö.

Konfigurerar offentlig Wi-Fi-profil

Så här konfigurerar du Bitdefender att tillämpa produktinställningar när du är ansluten till ett osäkert trådlöst nätverk:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** knappen från området Public Wi-Fi Profile.

4. Låt **Justerar produktinställningar för att öka skyddet när du är ansluten till ett osäkert offentligt Wi-Fi-nätverk** kryssrutan aktiverad.
5. Klick **Spara**.

4.1.5. Batterilägesprofil

Batterilägesprofilen är speciellt utformad för användare av bärbara datorer och surfplattor. Syftet är att minimera både systemets och Bitdefender-effekten på strömförbrukningen när batteriladdningsnivån är lägre än standarden eller den du väljer.

Konfigurera batterilägesprofil

Så här konfigurerar du batterilägesprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **Konfigurera** knappen 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 energischemainställningar för batteriläge.
   - Inaktivera externa enheter och nätverksportar.
5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Skriv ett giltigt värde i rutan eller välj ett med upp- och nedpiltangenterna för att ange när systemet ska börja arbeta i batteriläge. Som standard aktiveras läget när batteriladdningsnivån sjunker under 30 %.

Följande produktinställningar tillämpas när Bitdefender arbetar i batterilägesprofilen:

- Bitdefender Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.

Bitdefender upptäcker när din bärbara dator har bytt till batteridrift och baserat på batteriladdningsnivån går den automatiskt in i batteriläge. På

samma sätt lämnar Bitdefender automatiskt batteriläget när den upptäcker att den bärbara datorn inte längre körs på batteri.

4.1.6. Realtidsoptimering

Bitdefender Realtidsoptimering är ett plugin som förbättrar din systemprestanda tyst, i bakgrunden, och ser till att du inte blir avbruten medan du är i ett profilläge. Beroende på CPU-belastningen övervakar plugin alla processer, med fokus på de som tar upp en högre belastning, för att anpassa dem efter dina behov.

Så här aktiverar eller inaktiverar du realtidsoptimering:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Rulla nedåt tills du ser alternativet Realtidsoptimering och använd sedan motsvarande knapp för att slå på eller av det.

4.2. Dataskydd

4.2.1. Raderar filer permanent

När du tar bort en fil kan den inte längre nås på vanliga sätt. Filen fortsätter dock att lagras på hårddisken tills den skrivs över när nya filer kopieras.

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

Du kan snabbt strimla filer eller mappar från din enhet med Windows sammanhangsberoende meny genom att följa dessa steg:

1. Högerklicka på filen eller mappen som du vill ta bort permanent.
2. Välj **Bitdefender > Filförstörare** i snabbmenyn som visas.
3. Klick **Ta bort permanent**och bekräfta sedan att du vill fortsätta med processen.
   Vänta tills Bitdefender har avslutat fragmenteringen av filerna.
4. Resultaten visas. Klick **Avsluta** för att avsluta guiden.

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

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Dataskydd** rutan, klicka **Pappers strimlare**.

3. Följ guiden File Shredder:
   a. Klicka på **Lägg till mappar** för att lägga till de filer eller mappar som du vill ska tas bort permanent.
      Alternativt kan du dra dessa filer eller mappar till det här fönstret.
   b. Klick **ta bort permanent**och bekräfta sedan att du vill fortsätta med processen.
      Vänta tills Bitdefender har avslutat fragmenteringen av filerna.
   c. **Resultatsammanfattning**
      Resultaten visas. Klick **Avsluta** för att avsluta guiden.

5. HUR

5.1. Installation

5.1.1. Hur installerar jag Bitdefender på en andra enhet?

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

Så här installerar du Bitdefender på en andra enhet:

1. Klick **Installera på en annan enhet** i det nedre vänstra hörnet av Bitdefender-gränssnitt.
   Ett nytt fönster visas på skärmen.
2. Klick **DELA NEDLADDNINGSLÄNK**.
3. Följ instruktionerna på skärmen för att installera Bitdefender.

Den nya enheten som du har installerat Bitdefender-produkten på kommer att visas i Bitdefender Central-instrumentpanelen.

5.1.2. Hur kan jag installera om Bitdefender?

Typiska situationer när du skulle behöva installera om Bitdefender inkluderar följande:

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

I händelse av att en av de nämnda situationerna är ditt fall, följ dessa steg:

- I **Windows 7**:
  1. Klick **Start** och gå till **Alla program**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klick **INSTALLERA OM** i fönstret som visas.
  4. Du måste starta om enheten för att slutföra processen.
- I **Windows 8** och **Windows 8.1**:

1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
2. Klick **Avinstallera** ett program eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klick **INSTALLERA OM** i fönstret som visas.
5. Du måste starta om enheten för att slutföra processen.

- I **Windows 10** och **Windows 11**:

1. Klick **Start**, Klicka sedan **inställningar**.
2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klick **Avinstallera** igen för att bekräfta ditt val.
5. Klick **INSTALLERA OM**.
6. Du måste starta om enheten för att slutföra processen.

Notera
Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

5.1.3. Var kan jag ladda ner min Bitdefender-produkt från?

Du kan installera Bitdefender från installationsskivan, eller använda webbinstallationsprogrammet som du kan ladda ner på din enhet från Bitdefender Central-plattformen.

Notera
Innan du kör satsen, rekommenderas det att ta bort alla säkerhetslösningar som är installerade på ditt system. När du använder mer än en säkerhetslösning på samma enhet blir systemet instabilt.

För att installera Bitdefender från Bitdefender Central:

1. Tillgång Bitdefender Central.

2. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
3. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
   - **Skydda andra enheter**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     Klick **SKICKA NEDLADDNINGSLÄNK**. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
     På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.
4. Kör Bitdefender-produkten du har laddat ner.

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

Denna situation uppstår när du uppgraderar ditt operativsystem och du vill fortsätta använda ditt Bitdefender-abonnemang.

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

- Från en tidigare version av Bitdefender Antivirus till den senaste tillgängliga Bitdefender Antivirus.
- Från en tidigare version av Bitdefender Internet Security till den senaste tillgängliga Bitdefender Internet Security.
- Från en tidigare version av Bitdefender Total Security till den senaste tillgängliga Bitdefender Total Security.

Det finns två fall som kan dyka upp:

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

I det här fallet måste du installera om produkten genom att följa dessa steg:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klick **INSTALLERA OM** i fönstret som visas.
  4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
     Öppna gränssnittet för din nya installerade Bitdefender-produkt för att få tillgång till dess funktioner.

- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **INSTALLERA OM** i fönstret som visas.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
     Öppna gränssnittet för din nya installerade Bitdefender-produkt för att få tillgång till dess funktioner.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, Klicka sedan **inställningar**.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **INSTALLERA OM** i fönstret som visas.
  6. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

Öppna gränssnittet för din nya installerade Bitdefender-produkt för att få tillgång till dess funktioner.

Notera
Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

- Du ändrade ditt system och du vill fortsätta använda Bitdefender-skyddet. Därför måste du installera om produkten med den senaste versionen.
  För att lösa denna situation:

  1. Ladda ner installationsfilen:

     a. Tillgång Bitdefender Central.

     b. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.

     c. Välj ett av de två tillgängliga alternativen:

     - **Skydda den här enheten**
       Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.

     - **Skydda en annan enhet**
       Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
       Klick **SKICKA NEDLADDNINGSLÄNK**. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
       På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.

  2. Kör Bitdefender-produkten du har laddat ner.

  För mer information om Bitdefender installationsprocessen, se Installera din Bitdefender-produkt (sida 4).

5.1.5. Hur kan jag uppgradera till den senaste Bitdefender-versionen?

Från och med nu är uppgraderingen till den senaste versionen möjlig utan att följa den manuella proceduren för avinstallation och ominstallation. Mer exakt, den nya produkten inklusive nya funktioner och större produktförbättringar levereras via produktuppdatering och om du redan har ett aktivt Bitdefender-abonnemang aktiveras produkten automatiskt.

Om du använder 2020-versionen kan du uppgradera till den senaste versionen genom att följa dessa steg:

1. Klick **STARTA OM NU** i meddelandet du får med uppgraderingsinformationen. Om du missar det, gå till Aviseringar peka på den senaste uppdateringen och klicka sedan på **STARTA OM NU** knapp. Vänta tills enheten startar om.

   De **Vad är nytt** fönster med information om de förbättrade och nya funktionerna visas.

2. Klicka på **Läs mer** länkar som ska omdirigeras till vår dedikerade sida med mer information och användbara artiklar.

3. Stäng **Vad är nytt** fönster för att komma åt gränssnittet för den nya installerade versionen.

Användare som vill uppgradera gratis från Bitdefender 2016 eller en lägre version till den senaste Bitdefender-versionen måste ta bort sin nuvarande version från kontrollpanelen och sedan ladda ner den senaste installationsfilen från Bitdefender-webbplatsen på följande adress: https://www.bitdefender.com/Downloads/. Aktiveringen är endast möjlig med ett giltigt abonnemang

5.2. Bitdefender Central

5.2.1. Hur loggar jag in på Bitdefender-kontot med ett annat konto?

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

För att lyckas logga in med ett annat Bitdefender-konto:

1. Klicka på ditt kontonamn i den övre delen av Bitdefender-gränssnitt.

2. Klick **Byt konto** i det övre högra hörnet av skärmen för att ändra kontot som är kopplat till enheten.
3. Skriv in e-postadressen i motsvarande fält och klicka sedan **NÄSTA**.
4. Skriv ditt lösenord och klicka sedan **LOGGA IN**.

> **Notera**
> Bitdefender-produkten från din enhet ändras automatiskt enligt prenumerationen som är kopplad till det nya Bitdefender-kontot. Om det inte finns något tillgängligt abonnemang kopplat till det nya Bitdefender-kontot, eller om du vill överföra det från det tidigare kontot, kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

5.2.2. Hur stänger jag av Bitdefender Central hjälpmeddelanden?

För att hjälpa dig förstå vad varje alternativ i Bitdefender Central är användbart för, visas hjälpmeddelanden i instrumentpanelen.

Om du vill sluta se den här typen av meddelanden:

1. Tillgång Bitdefender Central.
2. Klicka på ikonen i den övre högra sidan av skärmen.
3. Klick **Mitt konto** i bildmenyn.
4. Klick **inställningar** i bildmenyn.
5. Inaktivera Turn **på/av hjälpmeddelanden** alternativ.

5.2.3. Jag har glömt lösenordet som jag angav för mitt Bitdefender-konto. Hur återställer jag den?

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

- Från Bitdefender-gränssnitt:
  1. Klick **Mitt konto** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. Klick **Byt konto** i det övre högra hörnet av skärmen.
     Ett nytt fönster visas.
  3. Skriv din e-postadress och klicka **NÄSTA**.

Ett nytt fönster visas.

4. Klick **Glömt ditt lösenord?**.
5. Klick **NÄSTA**.
6. Kontrollera ditt e-postkonto, skriv in säkerhetskoden du har fått och klicka sedan **NÄSTA**.
   Alternativt kan du klicka **ändra lösenord** i e-postmeddelandet som vi skickade till dig.
7. Skriv det nya lösenordet du vill ställa in och skriv det sedan igen. Klick **SPARA**.

- Från din webbläsare:
  1. Gå till: https://central.bitdefender.com.
  2. Klick **LOGGA IN**.
  3. Skriv din e-postadress och klicka sedan **NÄSTA**.
  4. Klick **Glömt ditt lösenord?**.
  5. Klick **NÄSTA**.
  6. Kontrollera ditt e-postkonto och följ instruktionerna för att ställa in ett nytt lösenord för ditt Bitdefender-konto.

För att komma åt ditt Bitdefender-konto från och med nu, skriv in din e-postadress och det nya lösenordet du just har angett.

5.2.4. Hur kan jag hantera inloggningssessionerna som är kopplade till mitt Bitdefender-konto?

I ditt Bitdefender-konto har du möjlighet att se de senaste inaktiva och aktiva inloggningssessionerna som körs på enheter som är kopplade till ditt konto. Dessutom kan du logga ut på distans genom att följa dessa steg:

1. Tillgång Bitdefender Central.
2. Klicka på ikonen i den övre högra sidan av skärmen.
3. Klick **Sessioner** i bildmenyn.
4. I den **Aktiva Sessioner** område, välj **LOGGA UT** alternativet bredvid den enhet du vill avsluta inloggningssessionen.

5.3. Skanna med Bitdefender

5.3.1. Hur skannar jag en fil eller en mapp?

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

För att slutföra skanningen, följ guiden Antivirus Scan. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer.

Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

Typiska situationer när du använder den här skanningsmetoden inkluderar följande:

- Du misstänker att en specifik fil eller mapp är infekterad.
- När du laddar ner filer från internet som du tror kan vara farliga.
- Skanna en nätverksresurs innan du kopierar filer till din enhet.

5.3.2. Hur skannar jag mitt system

För att utföra en fullständig genomsökning av systemet:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klicka på **Kör Scan** knappen bredvid **Genomsökning av systemet**.
4. Följ systemsökningsguiden för att slutföra skanningen. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer.
   Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem. För mer information, se.

5.3.3. Hur schemalägger jag en skanning?

Du kan ställa in din Bitdefender-produkt så att den börjar skanna viktiga systemplatser när du inte är på framsidan av enheten.

Så här schemalägger du en skanning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.

2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klick ··· bredvid skanningstypen som du vill schemalägga, System Scan eller Quick Scan, i den nedre delen av gränssnittet, välj sedan **Redigera**. Alternativt kan du skapa en skanningstyp som passar dina behov genom att klicka **+Skapa Scan** bredvid **Hantera skanningar**.
4. Anpassa skanningen efter dina behov och klicka sedan **Nästa**.
5. Markera rutan bredvid **Välj när du vill schemalägga denna uppgift**. Välj ett av motsvarande alternativ för att ställa in ett schema:
   - Vid systemstart
   - Dagligen
   - Varje vecka
   - En gång i månaden

   Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.

Om du väljer att skapa en ny anpassad skanning, **Skanningsuppgift** fönstret visas. Härifrån kan du välja de platser du vill ska skannas.

5.3.4. Hur skapar jag en anpassad skanningsuppgift?

Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen, konfigurera och kör en anpassad skanningsuppgift.

Gör så här för att skapa en anpassad skanningsuppgift:

1. I den **ANTIVIRUS** rutan, klicka **Öppen**.
2. Klick **+Skapa Scan** bredvid **Hantera skanningar**.
3. I uppgiftsnamnsfältet anger du ett namn för skanningen, väljer de platser du vill ska skannas och klickar sedan på **NÄSTA**.
4. Konfigurera dessa allmänna alternativ:
   - **Skanna endast applikationer**. Du kan ställa in Bitdefender för att endast skanna appar som är tillgängliga.
   - **Skanningsuppgiftsprioritet**. Du kan välja vilken inverkan en skanningsprocess ska ha på systemets prestanda.
     - Auto - Prioriteten för skanningsprocessen beror på systemaktiviteten. För att säkerställa att skanningsprocessen

inte kommer att påverka systemaktiviteten kommer Bitdefender att bestämma om skanningsprocessen ska köras med hög eller låg prioritet.

- Hög - Prioriteten för skanningsprocessen kommer att vara hög. Genom att välja det här alternativet låter du andra program köras långsammare och minskar tiden som krävs för att skanningsprocessen ska slutföras.
- Låg - Prioriteten för skanningsprocessen kommer att vara låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka den tid som krävs för att skanningsprocessen ska slutföras.

- **Åtgärder efter skanning**. Välj vilken åtgärd Bitdefender ska vidta om inga hot hittas:
  - Visa sammanfattningsfönster
  - Stäng av enheten
  - Stäng skanningsfönstret

5. Om du vill konfigurera skanningsalternativen i detalj, klicka på **Visa avancerade alternativ**.
   Klick **Nästa**.
6. Du kan aktivera **Schemalägg skanningsuppgift** alternativet, om du vill, välj sedan när den anpassade skanningen du skapade ska starta.
   - Vid systemstart
   - Dagligen
   - En gång i månaden
   - Varje vecka

   Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.
7. Klick **Spara** för att spara inställningarna och stänga konfigurationsfönstret.
   Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot kommer att hittas under skanningsprocessen kommer du att

uppmanas att välja vilka åtgärder som ska vidtas på de upptäckta filerna.

Om du vill kan du snabbt köra en tidigare anpassad skanning igen genom att klicka på motsvarande post i den tillgängliga listan.

5.3.5. Hur undantar jag en mapp från att skannas?

Bitdefender tillåter att man undantar specifika filer, mappar eller filtillägg från genomsökning.

Undantag ska användas av användare med 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 mjukvara och appar för teständamål. Genom att skanna mappen kan du förlora en del av data.

Så här lägger du till en mapp i listan med undantag:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klicka på **inställningar** flik.
4. Klicka på **Hantera undantag**.
5. Klick **+Lägg till ett undantag**.
6. Ange sökvägen till den mapp som du vill utom genom att skanna i motsvarande fält.
   Alternativt kan du navigera till mappen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.
7. Slå på strömbrytaren bredvid skyddsfunktionen som inte ska skanna mappen. Det finns tre alternativ:
   - Antivirus
   - Hotförebyggande online
   - Avancerat hotförsvar
8. Klick **Spara** för att spara ändringarna och stänga fönstret.

5.3.6. Vad ska man göra när Bitdefender upptäckte en ren fil som infekterad?

Det kan finnas fall då Bitdefender av misstag flaggar en legitim fil som ett hot (en falsk positiv). För att rätta till detta fel, lägg till filen i området Bitdefender Exceptions:

1. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
   Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktiverat. Du kan inaktivera realtidsskydd i 5, 15 eller 30 minuter, i en timme, permanent eller tills ett system startar om.
2. Visa dolda objekt i Windows. För att ta reda på hur du gör detta, se Hur visar jag dolda objekt i Windows? (sida 118).
3. Återställ filen från karantänområdet:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. Gå till **inställningar** windows och klicka **Hantera karantän**.
   d. Välj filen och klicka sedan **Återställ**.
4. Lägg till filen i listan med undantag. För att ta reda på hur du gör detta, se Hur undantar jag en mapp från att skannas? (sida 107).
5. Slå på Bitdefender antivirusskydd i realtid.
6. Kontakta våra supportrepresentanter så att vi kan ta bort upptäckten av hotinformationsuppdateringen. För att ta reda på hur du gör detta, se Ber om hjälp (sida 140).

5.3.7. 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 den loggade skanningsprocessen, såsom skanningsalternativ, skanningsmålet, hoten som hittats och de åtgärder som vidtagits mot dessa hot.

Du kan öppna skanningsloggen direkt från skanningsguiden, när skanningen är klar, genom att klicka **VISA LOGG**.

Så här kontrollerar du en skanningslogg eller någon upptäckt infektion vid ett senare tillfälle:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken väljer du meddelandet om den senaste skanningen.
   Det är här du kan hitta alla hotskanningshändelser, inklusive hot som upptäcks av skanning vid åtkomst, användarinitierade genomsökningar och statusändringar för automatiska genomsökningar.
3. I aviseringslistan kan du kontrollera vilka skanningar som har utförts nyligen. Klicka på ett meddelande för att se detaljer om det.
4. För att öppna en skanningslogg, klicka **Visa logg**.

5.4. Privat skydd

5.4.1. Hur ser jag till att min onlinetransaktion är säker?

För att se till att din onlineverksamhet förblir privat kan du använda webbläsaren som tillhandahålls av Bitdefender för att skydda dina transaktioner och appar för hembanker.

Bitdefender Safepay™ är en säker webbläsare utformad för att skydda din kreditkortsinformation, kontonummer eller andra känsliga uppgifter du kan ange när du kommer åt olika onlineplatser.

Så här håller du din onlineaktivitet säker och privat:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SAFEPAY** rutan, klicka **inställningar**.
3. I den **Safepay** fönster, klicka **Starta Safepay**.
4. Klicka på knappen för att komma åt **Virtuellt tangentbord**.
   Använd **Virtuellt tangentbord** när du skriver känslig information som dina lösenord.

5.4.2. Vad kan jag göra om min enhet har blivit stulen?

Stöld av mobila enheter, oavsett om det är en smartphone, en surfplatta eller en bärbar dator, är en av huvudproblemen idag som påverkar individer och organisationer över hela världen.

Bitdefender Anti-Theft låter dig inte bara lokalisera och låsa den stulna enheten, utan också torka all data för att säkerställa att den inte kommer att användas av tjuven.

Så här kommer du åt stöldskyddsfunktionerna från ditt konto:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Klicka på önskat enhetskort och välj sedan **Anti-stöld**.
4. Välj den funktion du vill använda:
   - **LOKALISERA** - visa enhetens plats på Google Maps.
     Visa IP - visar den senaste IP-adressen för den valda enheten.
   - **Varna** - skicka en varning på enheten.
   - **Låsa** - lås din enhet och ställ in en numerisk PIN-kod för att låsa upp den. Alternativt, aktivera motsvarande alternativ för att låta Bitdefender ta ögonblicksbilder av personen som försöker komma åt din enhet.
   - **Torka** - radera all data från din enhet.

> **Viktig**
> När du har torkat en enhet upphör alla stöldskyddsfunktioner att fungera.

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

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

Bitdefender File Shredder hjälper dig att snabbt strimla filer eller mappar från din enhet med hjälp av Windows sammanhangsberoende meny genom att följa dessa steg:

1. Högerklicka på filen eller mappen du vill ta bort permanent, peka på Bitdefender och välj **Pappers strimlare**.
2. Klick **ta bort permanent**och bekräfta sedan att du vill fortsätta med processen.
   Vänta tills Bitdefender har avslutat fragmenteringen av filerna.
3. Resultaten visas. Klick **AVSLUTA** för att avsluta guiden.

5.4.4. Hur skyddar jag min webbkamera från att bli hackad?

Du kan ställa in din Bitdefender-produkt för att tillåta eller neka åtkomst av installerade appar till din webbkamera genom att följa dessa steg:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå till **Webbkamera skydd** fönstret och du kommer att se listan med appar som har begärt åtkomst till din kamera.
4. Peka på appen du vill tillåta eller förbjuda åtkomst och klicka sedan på knappen som representeras av en videokamera, som ligger bredvid den.
   För att se vad de andra Bitdefender-användarna har valt att göra med den valda appen, klicka på ikon. Du kommer att meddelas varje gång en av de listade apparna blockeras av Bitdefender-användarna.

För att manuellt lägga till appar till den här listan, klicka på **Lägg till applikation** och välj ett av de två alternativen.

- Från Windows Store
- Från dina appar

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

Om krypterade filer inte kan återställas automatiskt kan du återställa dem manuellt genom att följa dessa steg:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken, välj meddelandet om det senaste ransomware-beteendet som upptäckts och klicka sedan **Krypterade filer**.

3. Listan med de krypterade filerna visas.
   Klick **Återställ filer** att fortsätta.
4. Om hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de dekrypterade filerna ska sparas. Klick **Återställ plats**, och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.
   Klick **Avsluta** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas om de blir krypterade:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .fladdermus; .bin; .bmp; .c; .cda; .cgi; .klass; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .burk; .java; .jpeg; .jpg;.js; .jsp; .nyckel; .m4v; .mdb; .mitten; .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; .snabb; .swf; .tjära; .tex; .tif; .tiff; .Text; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .blixtlås;

5.5. Användbar information

5.5.1. Hur testar jag min säkerhetslösning?

För att säkerställa att din Bitdefender-produkt fungerar korrekt rekommenderar vi att du använder Eicar-testet.

Eicar-testet låter dig kontrollera din säkerhetslösning med hjälp av en säker fil utvecklad för detta ändamål.

Så här testar du din säkerhetslösning:

1. Ladda ner testet från den officiella webbsidan för EICAR-organisationen http://www.eicar.org/.
2. Klicka på **Anti-Malware testfil** flik.
3. Klick **Ladda ner** i menyn till vänster.
4. Från **Nedladdningsområde med standardprotokollet http** Klicka på **eicar.com** testfil.
5. Du kommer att informeras om att sidan du försöker komma åt innehåller EICAR-testfilen (inte ett hot).

Om du klickar **Jag förstår riskerna, ta mig dit ändå**, kommer nedladdningen av testet att börja och en Bitdefender-popup kommer att informera dig om att ett hot upptäcktes.

Klick **Fler detaljer** för att få mer information om denna åtgärd.

Om du inte får någon Bitdefender-varning rekommenderar vi att du kontaktar Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

5.5.2. Hur tar jag bort Bitdefender?

Om du vill ta bort din Bitdefender Antivirus Plus:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klick **AVLÄGSNA** i fönstret som visas.
  4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **AVLÄGSNA** i fönstret som visas.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.

4. Klick **Avinstallera** igen för att bekräfta ditt val.
5. Klick **AVLÄGSNA** i fönstret som visas.
6. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

Notera
Denna ominstallation kommer att ta bort de anpassade inställningarna permanent.

5.5.3. Hur tar jag bort Bitdefender VPN?

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

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender VPN** och välj **Avinstallera**.
     Vänta tills avinstallationsprocessen är klar.
- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera** ett program eller **Program och funktioner**.
  3. Hitta **Bitdefender VPN** och välj **Avinstallera**.
     Vänta tills avinstallationsprocessen är klar.
- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender VPN** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
     Vänta tills avinstallationsprocessen är klar.

5.5.4. Hur tar jag bort Bitdefender Anti-tracker-tillägget?

Beroende på vilken webbläsare du använder, följ dessa steg för att avinstallera Bitdefender Anti-tracker-tillägget:

- Internet Explorer
  1. Klick bredvid sökfältet och välj sedan Hantera tillägg. En lista med installerade tillägg visas.
  2. Klicka på Bitdefender Anti-tracker.
  3. Klick **Inaktivera** längst ner till höger.
- Google Chrome
  1. Klick ⋮ bredvid sökfältet.
  2. Välj **Fler verktyg**, och då **Tillägg**.
     En lista med installerade tillägg visas.
  3. Klick **Avlägsna** i Bitdefender Anti-tracker-kortet.
  4. Klick **Avlägsna** i popup-fönstret som visas.
- Mozilla Firefox
  1. Klick bredvid sökfältet.
  2. Välj **Tillägg**, och då **Tillägg**.
     En lista med installerade tillägg visas.
  3. Klick ··· och välj sedan **Avlägsna**.

5.5.5. Hur stänger jag av enheten automatiskt efter att skanningen är över?

Bitdefender erbjuder flera skanningsuppgifter som du kan använda för att se till att ditt system inte är infekterat med hot. Att skanna hela enheten kan ta längre tid att slutföra beroende på systemets hård- och mjukvarukonfiguration.

Av denna anledning låter Bitdefender dig konfigurera din produkt för att stänga av ditt system så snart genomsökningen är över.

Tänk på det här exemplet: du har avslutat ditt arbete och du vill gå och lägga dig. Du skulle vilja ha hela ditt system kontrollerat för hot av Bitdefender.

Så här stänger du av enheten när Quick Scan eller System Scan är över:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** fönster, klicka ··· bredvid Quick Scan eller System Scan och välj **Redigera**.
4. Anpassa skanningen efter dina behov och klicka **Nästa**.
5. Markera rutan bredvid **Välj när du vill schemalägga denna uppgift**, och välj sedan när uppgiften ska starta.
   Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.
6. Klick **Spara**.

Så här stänger du av enheten när en anpassad skanning är över:

1. Klick ··· bredvid den anpassade skanningen du skapade.
2. Klick **Nästa** och klicka sedan **Nästa** igen.
3. fan rutan bredvid **Välj när du vill schemalägga denna uppgift**, och välj sedan när uppgiften ska starta.
4. Klick **Spara**.

Om inga hot hittas kommer enheten att stängas av.

Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem. För mer information, se Antivirus Scan Wizard (sida 54).

5.5.6. Hur konfigurerar jag Bitdefender för att använda en proxy-internetanslutning?

Om din enhet ansluter till internet via en proxyserver måste du konfigurera Bitdefender med proxyinställningarna. Normalt upptäcker och importerar Bitdefender automatiskt proxyinställningarna från ditt system.

Viktig

Internetanslutningar i hemmet använder normalt inte en proxyserver. Som en tumregel, kontrollera och konfigurera proxyanslutningsinställningarna för ditt Bitdefender-program när uppdateringar inte fungerar. Om Bitdefender kan uppdatera är den korrekt konfigurerad för att ansluta till internet.

Så här hanterar du proxyinställningarna:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Avancerad** flik.
3. Sätta på **Proxyserver**.
4. Klick **Byte av proxy**.
5. Det finns två alternativ för att ställa in proxyinställningarna:
   - **Importera proxyinställningar från standardwebbläsaren** - proxyinställningar för den aktuella användaren, extraherad från standardwebbläsaren. Om proxyservern kräver ett användarnamn och ett lösenord måste du ange dem i motsvarande fält.

     Notera
     Bitdefender kan importera proxyinställningar från de mest populära webbläsarna, inklusive de senaste versionerna av Microsoft Edge, Internet Explorer, Mozilla Firefox och Google Chrome.

   - **Anpassade proxyinställningar** - proxyinställningar som du kan konfigurera själv.
     Följande inställningar måste anges:
     - **Adress** - skriv in proxyserverns IP.
     - **Hamn** - skriv in porten som Bitdefender använder för att ansluta till proxyservern.
     - **Användarnamn** - skriv in ett användarnamn som känns igen av proxyn.
     - **Lösenord** - skriv in det giltiga lösenordet för den tidigare angivna användaren.
6. Klick **OK** för att spara ändringarna och stänga fönstret.

Bitdefender kommer att använda de tillgängliga proxyinställningarna tills den lyckas ansluta till internet.

5.5.7. Använder jag en 32-bitars eller en 64-bitarsversion av Windows?

Så här tar du reda på om du har ett 32-bitars eller ett 64-bitars operativsystem:

- I **Windows 7**:
  1. Klick **Start**.
  2. Lokalisera **Dator** på **Start** meny.
  3. Högerklicka **Dator** och välj **Egenskaper**.
  4. Titta under **Systemet** för att kontrollera informationen om ditt system.
- I **Windows 8**:
  1. Från startskärmen i Windows, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt på startskärmen) och sedan högerklicka på dess ikon.
     I **Windows 8.1**, lokalisera **Denna PC**.
  2. Välj **Egenskaper** i bottenmenyn.
  3. Titta i systemområdet för att se din systemtyp.
- I **Windows 10** och **Windows 11**:
  1. Skriv "System" i sökrutan från aktivitetsfältet och klicka på dess ikon.
  2. Titta i området System för att hitta information om din systemtyp.

5.5.8. Hur visar jag dolda objekt i Windows?

Dessa steg är användbara i de fall där du har att göra med en hotsituation och du behöver hitta och ta bort de infekterade filerna, som kan vara dolda.

Följ dessa steg för att visa dolda objekt i Windows:

1. Klick **Start**, gå till **Kontrollpanel**.
   I **Windows 8** och **Windows 8.1**: Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.

2. Välj **Mappalternativ**.
3. Gå till **Se** flik.
4. Välj **Visa dolda filer och mappar**.
5. Klar **Dölj filnamnstillägg för kända filtyper**.
6. Klar **Dölj skyddade operativsystemfiler**.
7. Klick **Tillämpa**, Klicka sedan **OK**.

I **Windows 10** och **Windows 11**:

1. Skriv "Visa dolda filer och mappar" i sökrutan från aktivitetsfältet och klicka på dess ikon.
2. Välj **Visa dolda filer, mappar och enheter**.
3. Klar **Dölj filnamnstillägg för kända filtyper**.
4. Klar **Dölj skyddade operativsystemfiler**.
5. Klick **Tillämpa**, Klicka sedan **OK**.

5.5.9. Hur tar jag bort andra säkerhetslösningar?

Det främsta skälet till att använda en säkerhetslösning är att ge skydd och säkerhet för dina data. Men vad händer när du har mer än en säkerhetsprodukt på samma system?

När du använder mer än en säkerhetslösning på samma enhet blir systemet instabilt. De Bitdefender Antivirus Plus installationsprogrammet upptäcker automatiskt andra säkerhetsprogram och erbjuder dig möjligheten att avinstallera dem.

Om du inte tog bort de andra säkerhetslösningarna under den första installationen:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Vänta några ögonblick tills listan med installerad programvara visas.
  3. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.

4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera ett program** eller **Program och funktioner**.
  3. Vänta några ögonblick tills listan med installerad programvara visas.
  4. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar**.
  3. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

Om du misslyckas med att ta bort den andra säkerhetslösningen från ditt system, skaffa avinstallationsverktyget från leverantörens webbplats eller kontakta dem direkt för att ge dig riktlinjerna för avinstallation.

5.5.10. Hur startar jag om i felsäkert läge?

Säkert läge är ett diagnostiskt driftläge, som främst används för att felsöka problem som påverkar normal drift av Windows. Sådana problem sträcker sig från motstridiga drivrutiner till hot som hindrar Windows från att starta normalt. I felsäkert läge fungerar bara ett fåtal appar och Windows laddar bara de grundläggande drivrutinerna och ett minimum av operativsystemkomponenter. Det är därför de flesta hot är inaktiva när du använder Windows i felsäkert läge och de kan enkelt tas bort.

Så här startar du Windows i felsäkert läge:

- I **Windows 7**:
  1. Starta om enheten.
  2. tryck på **F8** flera gånger innan Windows börjar komma åt startmenyn.
  3. Välj **Säkert läge** i startmenyn eller **Säkert läge med nätverk** om du vill ha tillgång till internet.
  4. Tryck **Stiga på** och vänta medan Windows laddas i felsäkert läge.
  5. Denna process avslutas med ett bekräftelsemeddelande. Klick **OK** att erkänna.
  6. Starta Windows normalt genom att helt enkelt starta om systemet.
- I **Windows 8**, **Windows 8.1**, **Windows 10** och **Windows 11**:
  1. Lansera **Systemkonfiguration** i Windows genom att samtidigt trycka på **Windows + R** tangenterna på ditt tangentbord.
  2. Skriva **msconfig** i **Öppen** dialogrutan och klicka sedan på **OK**.
  3. Välj **Känga** flik.
  4. I den **Startalternativ** område, välj **Säker stövel** kryssruta.
  5. Klick **Nätverk**, och då **OK**.
  6. Klick **OK** i **Systemkonfiguration** fönster som informerar dig om att systemet måste startas om för att kunna göra de ändringar du ställt in.
     Ditt system startar om i felsäkert läge med nätverk.

För att starta om i normalt läge, byt tillbaka inställningarna genom att starta igen **System operation** och rensa **Säker stövel** kryssruta. Klick **OK**, och då **Omstart**. Vänta tills de nya inställningarna tillämpas.

6. FELSÖKNING

6.1. Löser vanliga problem

Det här kapitlet presenterar några problem du kan stöta på när du använder Bitdefender och ger dig möjliga lösningar på dessa problem. De flesta av dessa problem kan lösas genom lämplig konfiguration av produktinställningarna.

Om du inte kan hitta ditt problem här, eller om de presenterade lösningarna inte löser det, kan du kontakta Bitdefender tekniska supportrepresentanter som presenteras i kapitel Ber om hjälp (sida 140).

6.1.1. Mitt system verkar vara långsamt

Vanligtvis, efter installation av en säkerhetsprogramvara, kan det förekomma en liten nedgång i systemet, vilket till en viss grad är normalt.

Om du märker en betydande avmattning kan det här problemet uppstå av följande anledningar:

- **Bitdefender är inte det enda säkerhetsprogrammet som är installerat på systemet**.
  Även om Bitdefender söker och tar bort säkerhetsprogrammen som hittas under installationen, rekommenderas det att ta bort alla andra säkerhetslösningar som du kan använda innan du

installerar Bitdefender. För mer information, se Hur tar jag bort andra säkerhetslösningar? (sida 119).

- **Systemkraven för att köra Bitdefender är inte uppfyllda.**
  Om din maskin inte uppfyller systemkraven kommer enheten att bli trög, särskilt när flera appar körs samtidigt. För mer information, se Systemkrav (sida 3).

- **Du har installerat appar som du inte använder.**
  Alla enheter har program eller appar som du inte använder. Och många oönskade program körs i bakgrunden och tar upp diskutrymme och minne. Om du inte använder ett program, avinstallera det. Detta gäller även för alla andra förinstallerade program eller testappar som du har glömt att ta bort.

  Viktig
  Om du misstänker att ett program eller en app är en viktig del av ditt operativsystem, ta inte bort det och kontakta Bitdefender kundtjänst för hjälp.

- **Ditt system kan vara infekterat.**
  Din systemhastighet och dess allmänna beteende kan också påverkas av hot. Spionprogram, skadlig programvara, trojaner och adware tar alla hårt på enhetens prestanda. Se till att skanna ditt system med jämna mellanrum, minst en gång i veckan. Det rekommenderas att använda Bitdefender System Scan eftersom den söker efter alla typer av hot som äventyrar säkerheten för ditt system.
  Så här startar du systemsökningen:

  1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
  3. I den **Skanningar** fönster, klicka **Kör Scan** bredvid **Genomsökning av systemet**.
  4. Följ stegen i guiden.

6.1.2. Skanningen startar inte

Den här typen av problem kan ha två huvudorsaker:

- **En tidigare Bitdefender-installation som inte togs bort helt eller en felaktig Bitdefender-installation.**

I det här fallet installerar du om Bitdefender:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klick **INSTALLERA OM** i fönstret som visas.
  4. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera** ett program eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **INSTALLERA OM** i fönstret som visas.
  5. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, Klicka sedan **inställningar**.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **INSTALLERA OM** i fönstret som visas.
  6. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.

Notera

Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

- **Bitdefender är inte den enda säkerhetslösningen som är installerad på ditt system.**
  I detta fall:

  1. Ta bort den andra säkerhetslösningen. För mer information, se Hur tar jag bort andra säkerhetslösningar? (sida 119).
  2. Installera om Bitdefender:
     - I **Windows 7**:
       a. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
       b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
       c. Klick **INSTALLERA OM** i fönstret som visas.
       d. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.
     - I **Windows 8** och **Windows 8.1**:
       a. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
       b. Klick **Avinstallera** ett program eller **Program och funktioner**.
       c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
       d. Klick **INSTALLERA OM** i fönstret som visas.
       e. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.
     - I **Windows 10** och **Windows 11**:
       a. Klick **Start**, Klicka sedan **inställningar**.
       b. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
       c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
       d. Klick **Avinstallera** igen för att bekräfta ditt val.
       e. Klick **INSTALLERA OM** i fönstret som visas

f. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.

Notera
Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.1.3. Jag kan inte längre använda en app

Det här problemet uppstår när du försöker använda ett program som fungerade normalt innan du installerade Bitdefender.

Efter installation av Bitdefender kan du stöta på en av dessa situationer:

- Du kan få ett meddelande från Bitdefender om att programmet försöker göra en modifiering av systemet.
- Du kan få ett felmeddelande från programmet du försöker använda.

Denna typ av situation uppstår när Advanced Threat Defense av misstag upptäcker vissa appar som skadliga.

Advanced Threat Defense är en Bitdefender-funktion som ständigt övervakar apparna som körs på ditt system och rapporterar dem med potentiellt skadligt beteende. Eftersom den här funktionen är baserad på ett heuristiskt system kan det finnas fall då legitima appar rapporteras av Advanced Threat Defense.

När denna situation inträffar kan du undanta respektive app från att övervakas av Advanced Threat Defense.

Så här lägger du till programmet i undantagslistan:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Ange sökvägen för den körbara filen du vill ha förutom skanning i motsvarande fält.

Alternativt kan du navigera till den körbara filen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.

6. Slå på strömbrytaren bredvid **Avancerat hotförsvar**.
7. Klick **Spara**.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.1.4. Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker

Bitdefender erbjuder en säker webbupplevelse genom att filtrera all webbtrafik och blockera allt skadligt innehåll. Det är dock möjligt att Bitdefender betraktar en webbplats, en domän, en IP-adress eller onlineapp som är säkra som osäkra, vilket gör att Bitdefender HTTP-trafikskanning blockerar dem felaktigt.

Skulle samma sida, domän, IP-adress eller onlineapp blockeras upprepade gånger, kan de läggas till i undantagen så att de inte skannas av Bitdefender-motorerna, vilket säkerställer en smidig webbupplevelse.

För att lägga till en webbplats **Undantag**:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ONLINE FÖREBYGGANDE AV HOT** rutan, klicka **inställningar**.
3. Klick **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Skriv i motsvarande fält namnet på webbplatsen, namnet på domänen eller IP-adressen du vill lägga till i undantag.
6. Klicka på knappen bredvid **Hotförebyggande online**.
7. Klick **Spara** för att spara ändringarna och stänga fönstret.

Endast webbplatser, domäner, IP-adresser och appar som du litar på bör läggas till i den här listan. Dessa kommer att undantas från genomsökning av följande motorer: hot, nätfiske och bedrägeri.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.1.5. Hur man uppdaterar Bitdefender på en långsam internetanslutning

Om du har en långsam internetanslutning (som uppringd), kan fel uppstå under uppdateringsprocessen.

För att hålla ditt system uppdaterat med den senaste Bitdefender hotinformationsdatabasen:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Uppdatering** flik.
3. Stäng av **Tyst uppdatering** växla.
4. Nästa gång när en uppdatering blir tillgänglig kommer du att bli ombedd att välja vilken uppdatering du vill ladda ner. Välj endast **Uppdatering av signaturer**.
5. Bitdefender kommer endast att ladda ner och installera hotinformationsdatabasen.

6.1.6. Bitdefender-tjänsterna svarar inte

Den här artikeln hjälper dig att felsöka **Bitdefender Services svarar inte** fel. Du kan stöta på detta fel enligt följande:

- Bitdefender-ikonen i systemfältet är nedtonad och du informeras om att Bitdefender-tjänsterna inte svarar.
- Bitdefender-fönstret indikerar att Bitdefender-tjänsterna inte svarar.

Felet kan orsakas av något av följande tillstånd:

- tillfälliga kommunikationsfel mellan Bitdefender-tjänsterna.
- några av Bitdefender-tjänsterna stoppas.
- andra säkerhetslösningar som körs på din enhet samtidigt med Bitdefender.

För att felsöka det här felet, prova dessa lösningar:

1. Vänta en stund och se om något förändras. Felet kan vara tillfälligt.
2. Starta om enheten och vänta några ögonblick tills Bitdefender laddas. Öppna Bitdefender för att se om felet kvarstår. Att starta om enheten löser vanligtvis problemet.

3. Kontrollera om du har någon annan säkerhetslösning installerad eftersom de kan störa den normala driften av Bitdefender. Om så är fallet rekommenderar vi att du tar bort alla andra säkerhetslösningar och sedan installerar om Bitdefender.

   För mer information, se Hur tar jag bort andra säkerhetslösningar? (sida 119).

Om felet kvarstår, kontakta våra supportrepresentanter för hjälp enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.1.7. Borttagning av Bitdefender misslyckades

Om du vill ta bort din Bitdefender-produkt och du märker att processen hänger ut eller systemet fryser, klicka på **Annullera** för att avbryta åtgärden. Om detta inte fungerar, starta om systemet.

När borttagningen misslyckas kan vissa Bitdefender-registernycklar och filer finnas kvar i ditt system. Sådana rester kan förhindra en ny installation av Bitdefender. De kan också påverka systemets prestanda och stabilitet.

För att helt ta bort Bitdefender från ditt system:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  3. Klick **AVLÄGSNA** i fönstret som visas.
  4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **AVLÄGSNA** i fönstret som visas.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **AVLÄGSNA** i fönstret som visas.
  6. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

6.1.8. Mitt system startar inte upp efter installation av Bitdefender

Om du precis har installerat Bitdefender och inte kan starta om ditt system i normalt läge längre kan det finnas olika orsaker till detta problem.

Antagligen orsakas detta av en tidigare Bitdefender-installation som inte togs bort ordentligt eller av en annan säkerhetslösning som fortfarande finns på systemet.

Så här kan du hantera varje situation:

- **Du hade Bitdefender tidigare och du tog inte bort den ordentligt.**
  För att lösa detta:
  1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 120).
  2. Ta bort Bitdefender från ditt system:
     - I **Windows 7**:
       a. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
       b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
       c. Klick **AVLÄGSNA** i fönstret som visas.
       d. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
       e. Starta om ditt system i normalt läge.

- I **Windows 8** och **Windows 8.1**:
  a. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  b. Klick **Avinstallera ett program** eller **Program och funktioner**.
  c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  d. Klick **AVLÄGSNA** i fönstret som visas.
  e. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
  f. Starta om ditt system i normalt läge.
- I **Windows 10** och **Windows 11**:
  a. Klick **Start**, klicka sedan på Inställningar.
  b. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
  d. Klick **Avinstallera** igen för att bekräfta ditt val.
  e. Klick **AVLÄGSNA** i fönstret som visas.
  f. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
  g. Starta om ditt system 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 detta:
  1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 120).
  2. Ta bort den andra säkerhetslösningen från ditt system:
     - I **Windows 7**:

a. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.

b. Hitta namnet på programmet du vill ta bort och välj **Avlägsna**.

c. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

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

  a. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.

  b. Klick **Avinstallera ett program** eller **Program och funktioner**.

  c. Hitta namnet på programmet du vill ta bort och välj **Avlägsna**.

  d. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 10** och **Windows 11**:

  a. Klick **Start**, klicka sedan på Inställningar.

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

  c. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.

  d. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

För att korrekt avinstallera den andra programvaran, gå till deras webbplats och kör deras avinstallationsverktyg eller kontakta dem direkt för att ge dig riktlinjerna för avinstallation.

3. Starta om ditt system i normalt läge och installera om Bitdefender.

Du har redan följt stegen ovan och situationen är inte löst.

För att lösa detta:

1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 120).

2. Använd alternativet Systemåterställning från Windows för att återställa enheten till ett tidigare datum innan du installerar Bitdefender-produkten.
3. Starta om systemet i normalt läge och kontakta våra supportrepresentanter för hjälp enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.2. Ta bort hot från ditt system

Hot kan påverka ditt system på många olika sätt och Bitdefender-metoden beror på typen av hotattack. Eftersom hot ändrar sitt beteende ofta är det svårt att skapa ett mönster för deras beteende och handlingar.

Det finns situationer när Bitdefender inte automatiskt kan ta bort hotinfektionen från ditt system. I sådana fall krävs ditt ingripande.

Om du inte kan hitta ditt problem här, eller om de presenterade lösningarna inte löser det, kan du kontakta Bitdefender tekniska supportrepresentanter som presenteras i kapitel Ber om hjälp (sida 140).

6.2.1. Räddningsmiljö

Räddningsmiljö är en Bitdefender-funktion som låter dig skanna och desinficera alla befintliga hårddiskpartitioner i och utanför ditt operativsystem.

Bitdefender Rescue Environment är integrerad med Windows RE.

Starta ditt system i Rescue Environment

Du kan endast gå in i Rescue Environment från din Bitdefender-produkt, enligt följande:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klick **Öppen** bredvid **Räddningsmiljö**.
4. Klick **STARTA OM** i fönstret som visas.
   Bitdefender Rescue Environment laddas på några ögonblick.

Skanna ditt system i Rescue Environment

För att skanna ditt system Rescue Environment:

1. Gå in i Rescue Environment, som beskrivs i Starta ditt system i Rescue Environment (sida 134).
2. Bitdefender-skanningsprocessen startar automatiskt så snart systemet laddas i Rescue Environment.
3. Vänta tills skanningen är klar. Om något hot upptäcks, följ instruktionerna för att ta bort det.
4. För att avsluta Rescue Environment, klicka på knappen Stäng i fönstret med skanningsresultaten.

6.2.2. Vad ska jag göra när Bitdefender hittar hot på din enhet?

Du kan få reda på att det finns ett hot på din enhet på något av följande sätt:

- Du skannade din enhet och Bitdefender hittade infekterade föremål på den.
- En hotvarning informerar dig om att Bitdefender blockerade ett eller flera hot på din enhet.

I sådana situationer, uppdatera Bitdefender för att se till att du har den senaste hotinformationsdatabasen och kör en systemsökning för att analysera systemet.

Så snart systemgenomsökningen är över, välj önskad åtgärd för de infekterade föremålen (Desinficera, Ta bort, Flytta till karantän).

Varning
Om du misstänker att filen är en del av Windows-operativsystemet eller att den inte är en infekterad fil, följ inte dessa steg och kontakta Bitdefender kundtjänst så snart som möjligt.

Om den valda åtgärden inte kunde vidtas och skanningsloggen avslöjar en infektion som inte kunde raderas, måste du ta bort filen/filerna manuellt:

Den första metoden kan användas i normalt läge:

1. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
2. Visa dolda objekt i Windows. För att ta reda på hur du gör detta, se Hur visar jag dolda objekt i Windows? (sida 118).
3. Bläddra till platsen för den infekterade filen (kontrollera skanningsloggen) och ta bort den.
4. Slå på Bitdefender antivirusskydd i realtid.

Om den första metoden inte lyckades ta bort infektionen:

1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 120).
2. Visa dolda objekt i Windows. För att ta reda på hur du gör detta, se Hur visar jag dolda objekt i Windows? (sida 118).
3. Bläddra till platsen för den infekterade filen (kontrollera skanningsloggen) och ta bort den.
4. Starta om ditt system och gå in i normalt läge.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.2.3. Hur rensar jag ett hot i ett arkiv?

Ett arkiv är en fil eller en samling filer komprimerade under ett speciellt format för att minska det utrymme på disken som behövs för att lagra filerna.

Vissa av dessa format är öppna format, vilket ger Bitdefender möjlighet att skanna inuti dem och sedan vidta lämpliga åtgärder för att ta bort dem.

Andra arkivformat är delvis eller helt stängda, och Bitdefender kan bara upptäcka förekomsten av hot inuti dem, men kan inte vidta några andra åtgärder.

Om Bitdefender meddelar dig att ett hot har upptäckts i ett arkiv och ingen åtgärd är tillgänglig, betyder det att det inte är möjligt att ta bort hotet på grund av begränsningar i arkivets behörighetsinställningar.

Så här kan du rensa ett hot som lagras i ett arkiv:

1. Identifiera arkivet som innehåller hotet genom att utföra en systemsökning av systemet.
2. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
3. Gå till platsen för arkivet och dekomprimera det med en arkiveringsapp, som WinZip.
4. Identifiera den infekterade filen och ta bort den.
5. Ta bort det ursprungliga arkivet för att se till att infektionen är helt borttagen.
6. Komprimera om filerna i ett nytt arkiv med en arkiveringsapp, som WinZip.
7. Slå på Bitdefender-antivirusskyddet i realtid och kör en systemsökning för att säkerställa att det inte finns någon annan infektion på systemet.

Notera
Det är viktigt att notera att ett hot som lagras i ett arkiv inte är ett omedelbart hot mot ditt system, eftersom hotet måste dekomprimeras och exekveras för att infektera ditt system.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.2.4. Hur rensar jag ett hot i ett e-postarkiv?

Bitdefender kan också identifiera hot i e-postdatabaser och e-postarkiv lagrade på disk.

Ibland är det nödvändigt att identifiera det infekterade meddelandet med hjälp av informationen i skanningsrapporten och radera det manuellt.

Så här kan du rensa ett hot som lagras i ett e-postarkiv:

1. Skanna e-postdatabasen med Bitdefender.
2. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
3. Öppna skanningsrapporten och använd identifieringsinformationen (Ämne, Från, Till) för de infekterade meddelandena för att hitta dem i e-postklienten.
4. Ta bort de infekterade meddelandena. De flesta e-postklienter flyttar också det raderade meddelandet till en återställningsmapp, från vilken det kan återställas. Du bör se till att meddelandet också raderas från denna återställningsmapp.
5. Komprimera mappen som lagrar det infekterade meddelandet.
   - I Microsoft Outlook 2007: Klicka på Datafilhantering på Arkiv-menyn. Välj de personliga mappfiler (.pst) som du tänker komprimera och klicka på Inställningar. Klicka på Komprimera nu.
   - I Microsoft Outlook 2010/2013/2016: På Arkiv-menyn, klicka på Info och sedan Kontoinställningar (Lägg till och ta bort konton eller ändra befintliga anslutningsinställningar). Klicka sedan på Datafil, välj de personliga mappfilerna (.pst) som du tänker komprimera och klicka på Inställningar. Klicka på Komprimera nu.
6. Slå på Bitdefender antivirusskydd i realtid.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 140).

6.2.5. Vad ska jag göra 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 att se till att ditt system är skyddat:

1. Kör a **Genomsökning av systemet** med Bitdefender. För att ta reda på hur du gör detta, se Hur skannar jag mitt system (sida 104).
2. Om skanningsresultatet verkar vara rent, men du fortfarande har tvivel och vill vara säker på filen, kontakta våra supportrepresentanter så att vi kan hjälpa dig.
   För att ta reda på hur du gör detta, se Ber om hjälp (sida 140).

6.2.6. Vilka är de lösenordsskyddade filerna i skanningsloggen?

Detta är bara ett meddelande som indikerar att Bitdefender har upptäckt att dessa filer antingen är skyddade med ett lösenord eller av någon form av kryptering.

Vanligast är de lösenordsskyddade objekten:

- Filer som tillhör en annan säkerhetslösning.
- Filer som tillhör operativsystemet.

För att faktiskt skanna innehållet måste dessa filer antingen extraheras eller på annat sätt dekrypteras.

Skulle innehållet extraheras, skulle Bitdefenders realtidsskanner automatiskt skanna dem för att hålla din enhet skyddad. Om du vill skanna dessa filer med Bitdefender måste du kontakta produkttillverkaren för att ge dig mer information om dessa filer.

Vår rekommendation till dig är att ignorera dessa filer eftersom de inte är ett hot mot ditt system.

6.2.7. Vilka är de överhoppade objekten i skanningsloggen?

Alla filer som visas som överhoppade i skanningsrapporten är rena.

För ökad prestanda skannar inte Bitdefender filer som inte har ändrats sedan den senaste skanningen.

6.2.8. Vilka är de överkomprimerade filerna i skanningsloggen?

De överkomprimerade objekten är element som inte kunde extraheras av skanningsmotorn eller element för vilka dekrypteringstiden skulle ha tagit för lång tid och gjort systemet instabilt.

Överkomprimerad betyder att Bitdefender hoppade över skanningen i det arkivet eftersom uppackning av det visade sig ta för många systemresurser. Innehållet skannas vid realtidsåtkomst om det behövs.

6.2.9. Varför tog Bitdefender automatiskt bort en infekterad fil?

Om en infekterad fil upptäcks kommer Bitdefender automatiskt att försöka desinficera den. Om desinfektionen misslyckas flyttas filen till karantän för att innehålla infektionen.

För särskilda typer av hot är desinficering inte möjlig eftersom den upptäckta filen är helt skadlig. I sådana fall tas den infekterade filen bort från disken.

Detta är vanligtvis fallet med installationsfiler som laddas ner från opålitliga webbplatser. Om du hamnar i en sådan situation, ladda ner installationsfilen från tillverkarens webbplats eller annan pålitlig webbplats.

7. FÅ HJÄLP

7.1. Ber om hjälp

Bitdefender ger sina kunder en oöverträffad nivå av snabb och exakt support. Om du upplever några problem eller om du har några frågor om din Bitdefender-produkt, kan du använda flera onlineresurser för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefender Customer Care-teamet. Våra supportrepresentanter kommer att svara på dina frågor i tid och ge dig den hjälp du behöver.

7.2. Onlineresurser

Flera onlineresurser finns tillgängliga för att hjälpa dig att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefender Support Center:
  https://www.bitdefender.se/consumer/support/
- Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Du kan också använda din favoritsökmotor för att ta reda på mer information om datorsäkerhet, Bitdefender-produkterna och företaget.

7.2.1. Bitdefender Support Center

Bitdefender Support Center är ett onlineförråd med information om Bitdefender-produkterna. Den lagrar, i ett lättillgängligt format, rapporter om resultaten av den pågående tekniska supporten och buggfixningsaktiviteterna för Bitdefender-support- och utvecklingsteamen, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefender Support Center är öppet för allmänheten och fritt sökbart. Den omfattande informationen den innehåller är ytterligare ett sätt att förse Bitdefender-kunder med den tekniska kunskap och insikt de behöver. Alla giltiga förfrågningar om information eller buggrapporter

som kommer från Bitdefender-klienter hittar så småningom vägen till Bitdefender Support Center, som bugfixrapporter, fuskblad för lösningar eller informationsartiklar för att komplettera produkthjälpfiler.

Bitdefender Support Center är tillgängligt när som helst på följande adress: https://www.bitdefender.se/consumer/support/.

7.2.2. Bitdefender Expert Community

Expertgemenskapen är en miljö där Bitdefender-användare, entusiaster och fans kan engagera sig, utbyta idéer, stödja varandra och dela sina kunskaper och lösningar. Det är också en plats för idéer och ger värdefull feedback till våra utvecklingsteam. Community-medlemmarna är erfarna Bitdefender-användare som gärna hjälper andra kamrater på sin egen tid. Med deras enorma bidrag och genuina frivilliga insatser har vi skapat en kunskapsbas där användare kan hitta svar och vägledning, men med den mänskliga touchen.

Här hittar du meningsfulla konversationer med personer som använder Bitdefender på sina enheter. Gemenskapen erbjuder en sann kontakt med våra medlemmar och gör din röst hörd. Det är en plats där du uppmuntras att delta i vetskapen om att din åsikt och din input respekteras och omhuldas. Som en uppskattad leverantör strävar vi efter att erbjuda en oöverträffad nivå av snabb, exakt support och vi vill föra våra användare närmare oss. Vi har utformat vår community med detta syfte i åtanke.

Du hittar vår webbsida för expertgemenskapen här:

https://community.bitdefender.com/en/

7.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia har all information du behöver om de senaste cyberhoten. Det här är platsen där Bitdefender-experter delar med sig av tips och tricks om hur man kan hålla sig skyddad från hackare, dataintrång, identitetsstöld och sociala identitetsförsök.

Bitdefender Cyberpedias webbsida finns här:

https://www.bitdefender.com/cyberpedia/.

7.3. Kontaktinformation

Effektiv kommunikation är nyckeln till ett framgångsrikt företag. Sedan 2001 har BITDEFENDER etablerat ett obestridligt rykte genom att ständigt

sträva efter bättre kommunikation för att överträffa våra kunders och partners förväntningar. Om du har några frågor, tveka inte att kontakta oss direkt via vår Bitdefender Support Center (sida 140).

https://www.bitdefender.se/consumer/support/

7.3.1. Lokala distributörer

Bitdefender lokala distributörer är redo att svara på alla förfrågningar om deras verksamhetsområden, både i kommersiella och allmänna frågor.

Så här hittar du en Bitdefender-distributör i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din stad med hjälp av motsvarande alternativ.

ORDLISTA

Aktiveringskod

Är en unik nyckel som kan köpas från detaljhandeln och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av ett giltigt abonnemang under en viss tidsperiod och antal enheter och kan även användas för att förlänga ett abonnemang med villkoret att genereras för samma produkt eller tjänst.

ActiveX

ActiveX är en modell för att skriva program så att andra program och operativsystemet kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och beter sig som datorprogram, snarare än statiska sidor. Med ActiveX kan användare ställa eller svara på frågor, använda tryckknappar och interagera på andra sätt med webbsidan. ActiveX-kontroller skrivs ofta med Visual Basic. Active X är anmärkningsvärt för en fullständig brist på säkerhetskontroller; datorsäkerhetsexperter avråder från att använda det över internet.

Avancerat ihållande hot

Advanced persistent hot (APT) utnyttjar sårbarheter i system för att stjäla viktig information för att leverera den till källan. Stora grupper som organisationer, företag eller regeringar är föremål för detta hot. Målet med ett avancerat ihållande hot är att förbli oupptäckt under lång tid och kunna övervaka och samla in viktig information utan att skada de riktade maskinerna. Metoden som används för att injicera hotet i nätverket är genom en PDF-fil eller ett Office-dokument som ser ofarliga ut så att alla användare kan köra filerna.

Reklamprogram

Adware kombineras ofta med en värdapp som tillhandahålls utan kostnad så länge som användaren accepterar adware. Eftersom adware-appar vanligtvis installeras efter att användaren har godkänt ett licensavtal som anger syftet med appen, begås inget brott. Men popup-annonser kan bli irriterande och i vissa fall försämra systemets prestanda. Dessutom kan informationen som vissa av dessa appar samlar in orsaka integritetsproblem för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En disk, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera filer i ett komprimerat format.

Bakdörr

Ett hål i säkerheten i ett system som medvetet lämnats på plats av designers eller underhållare. Motivationen för sådana hål är inte alltid olycksbådande; vissa operativsystem, till exempel, kommer ur lådan med privilegierade konton avsedda att användas av fältservicetekniker eller säljarens underhållsprogrammerare.

Boot sektor

En sektor i början av varje disk som identifierar diskens arkitektur (sektorstorlek, klusterstorlek, och så vidare). För startdiskar innehåller bootsektorn även ett program som laddar operativsystemet.

Boot virus

Ett hot som infekterar startsektorn på en fast eller diskett. Ett försök att starta från en diskett som är infekterad med ett bootsektorvirus gör att hotet blir aktivt i minnet. Varje gång du startar ditt system från den tidpunkten kommer du att ha hotet aktivt i minnet.

Botnet

Termen "botnät" är sammansatt av orden "robot" och "nätverk". Botnät är internetanslutna enheter som är infekterade med hot och kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogram, ransomware och andra typer av hot. Deras mål är att infektera så många uppkopplade enheter som möjligt, såsom datorer, servrar, mobila eller IoT-enheter som tillhör stora företag eller industrier.

Webbläsare

Förkortning för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare inkluderar Microsoft Internet Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare, vilket innebär att de kan visa grafik såväl som text. Dessutom kan de flesta moderna webbläsare presentera multimediainformation, inklusive ljud och video, även om de kräver plugin-program för vissa format.

Brute Force Attack

Lösenordsgissningsattack används för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast med det enklast att gissa lösenordet.

Kommandorad

I ett kommandoradsgränssnitt skriver användaren kommandon i utrymmet som tillhandahålls direkt på skärmen med hjälp av kommandospråk.

Småkakor

Inom internetbranschen beskrivs cookies som små filer som innehåller information om enskilda datorer som kan analyseras och användas av annonsörer för att spåra dina intressen och smaker online. I det här området utvecklas fortfarande cookieteknologi och avsikten är att rikta annonser direkt till det du har sagt att dina intressen är. Det är ett tveeggat svärd för många människor eftersom det å ena sidan är effektivt och relevant eftersom du bara ser annonser om det du är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" vart du går och vad du klickar på. Det är förståeligt nog att det finns en debatt om integritet och många känner sig kränkta av uppfattningen att de ses som ett "SKU-nummer" (ni vet, streckkoden på baksidan av paketen som skannas vid utcheckningslinjen) . Även om denna synpunkt kan vara extrem, är den i vissa fall korrekt.

Cybermobbning

När kamrater eller främlingar begår kränkande handlingar mot barn med avsikt för att fysiskt skada dem. För att skada känslomässigt skickar angriparna elaka meddelanden eller föga smickrande bilder, vilket gör att deras offer isolerar sig från andra eller känner sig frustrerade.

Ordbok Attack

Lösenordsgissningsattacker används för att bryta sig in i ett datorsystem genom att ange en kombination av vanliga ord för att generera potentiella lösenord. Samma metod används för att gissa dekrypteringsnycklar för krypterade meddelanden eller dokument. Ordboksattacker lyckas eftersom många människor är benägna att välja korta och enstaka ordlösenord som är lätta att gissa.

Diskenhet

Det är en maskin som läser data från och skriver data till en disk. En hårddisk läser och skriver hårddiskar. En diskettenhet får åtkomst till

disketter. Diskenheter kan antingen vara interna (inrymd i en dator) eller externa (inrymd i en separat låda som ansluts till datorn).

Ladda ner

Att kopiera data (vanligtvis en hel fil) från en huvudkälla till en kringutrustning. Termen används ofta för att beskriva processen att kopiera en fil från en onlinetjänst till sin egen dator. Nedladdning kan också syfta på att kopiera en fil från en nätverksfilserver till en dator i nätverket.

E-post

E-post. En tjänst som skickar meddelanden på datorer via lokala eller globala nätverk.

evenemang

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 minnet blir slut.

Utnyttjar

Ett sätt att dra nytta av olika buggar eller sårbarheter som finns i en dator (mjukvara eller hårdvara). Således kan hackare få kontroll över datorer eller nätverk.

Falskt positivt

Uppstår när en skanner identifierar en fil som infekterad när den faktiskt inte är det.

Filnamnstillägg

Den del av ett filnamn, efter den sista punkten, som anger vilken typ av data som lagras i filen. Många operativsystem använder filnamnstillägg, t.ex. Unix, VMS och MS-DOS. De är vanligtvis från en till tre bokstäver (vissa tråkiga gamla operativsystem stöder inte mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Heuristisk

En regelbaserad metod för att identifiera nya hot. Denna metod för skanning är inte beroende av specifik databas med hotinformation. Fördelen med den heuristiska skanningen är att den inte luras av en ny variant av ett befintligt hot. Det kan dock ibland rapportera misstänkt kod i vanliga program, vilket genererar den så kallade "falska positiva".

Honungsburk

Ett lockdatorsystem som lockar hackare att studera hur de agerar och identifiera de kätterska metoder de använder för att samla in systeminformation. Företag och företag är mer intresserade av att implementera och använda honeypots för att förbättra sin övergripande säkerhet.

IP

Internet Protocol - Ett routbart protokoll i TCP/IP-protokollsviten som ansvarar för IP-adressering, routing och fragmentering och återmontering av IP-paket.

Java applet

Ett Java-program som är designat för att endast köras på en webbsida. För att använda en applet på en webbsida skulle du ange namnet på appleten och storleken (längd och bredd, i pixlar) som appleten kan använda. När webbsidan nås laddar webbläsaren ner appleten från en server och kör den på användarens dator (klienten). Applets skiljer sig från appar genom att de styrs av ett strikt säkerhetsprotokoll.

Till exempel, även om appletar körs på klienten, kan de inte läsa eller skriva data på klientens dator. Dessutom är appletar ytterligare begränsade så att de bara kan läsa och skriva data från samma domän som de betjänas från.

Keylogger

En keylogger är en app som loggar allt du skriver. Keyloggers är inte skadliga till sin natur. De kan användas för legitima ändamål, som att övervaka anställda eller barnaktivitet. De används dock i allt högre grad av cyberbrottslingar i skadliga syften (till exempel för att samla in privata uppgifter, såsom inloggningsuppgifter och personnummer).

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, stöder kraftfulla makrospråk. Dessa appar låter dig bädda in ett makro i ett dokument och få makrot att köras varje gång dokumentet öppnas.

E-postklient

En e-postklient är en app som gör att du kan skicka och ta emot e-post.

Minne

Interna lagringsutrymmen i datorn. Termen minne identifierar datalagring som kommer i form av chips, och ordet lagring används för minne som finns på band eller diskar. Varje dator kommer med en viss mängd fysiskt minne, vanligtvis kallat huvudminne eller RAM.

Icke-heuristisk

Denna metod för skanning bygger på specifik databas med hotinformation. Fördelen med den icke-heuristiska skanningen är att den inte luras av vad som kan tyckas vara ett hot och inte genererar falsklarm.

Rovdjur online

Individer som försöker locka minderåriga eller tonåringar till konversationer med avsikt att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den idealiska platsen där utsatta barn lätt kan jagas och förföras till att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Packade program

En fil i ett komprimeringsformat. Många operativsystem och appar innehåller kommandon som gör att du kan packa en fil så att den tar mindre minne. Anta till exempel att du har en textfil som innehåller tio på varandra följande mellanslagstecken. Normalt skulle detta kräva tio byte lagring.

Ett program som packar filer skulle dock ersätta mellanslagstecken med ett speciellt mellanslagsserietecken följt av antalet mellanslag som ersätts. I detta fall skulle de tio utrymmena endast kräva två byte. Detta är bara en packningsteknik - det finns många fler.

Väg

Den exakta vägbeskrivningen till en fil på en dator. Dessa riktningar beskrivs vanligtvis med hjälp av det hierarkiska arkiveringssystemet uppifrån och ner.

Rutten mellan två valfria punkter, till exempel kommunikationskanalen mellan två datorer.

Nätfiske

Handlingen att skicka ett e-postmeddelande till en användare som falskeligen påstår sig vara ett etablerat legitimt företag i ett försök att lura användaren till att överlämna privat information som kommer att användas för identitetsstöld. E-postmeddelandet uppmanar användaren att besöka

en webbplats där de ombeds att uppdatera personlig information, såsom lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och inrättad endast för att stjäla användarens information.

Foton

Photon är en innovativ, icke-påträngande Bitdefender-teknik, designad för att minimera prestandapåverkan från din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den användningsmönster som hjälper till att optimera uppstarts- och skanningsprocesser.

Polymorft virus

Ett hot som ändrar form för varje fil som den infekterar. Eftersom de inte har något konsekvent binärt mönster är sådana hot svåra att identifiera.

Hamn

Ett gränssnitt på en dator som du kan ansluta en enhet till. Persondatorer har olika typer av portar. Internt finns det flera portar för att ansluta diskenheter, bildskärmar och tangentbord. Externt har persondatorer portar för anslutning av modem, skrivare, möss och annan kringutrustning.

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 på användare genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall, är bara några varianter som jagar användarnas personliga system.

Infektionen kan spridas genom att komma åt skräppostmeddelanden, ladda ner e-postbilagor eller installera appar, utan att låta användaren veta vad som händer på hans system. Dagliga användare och företag riktas mot ransomware-hackare.

Rapportfil

En fil som listar åtgärder som har inträffat. Bitdefender har en rapportfil som visar sökvägen som skannats, mapparna, antalet skannade arkiv och filer, hur många infekterade och misstänkta filer som hittades.

Rootkit

Ett rootkit är en uppsättning mjukvaruverktyg som ger åtkomst till ett system på administratörsnivå. Termen användes först för UNIX-operativsystemen och den hänvisade till omkompilerade verktyg som gav inkräktare administrativa rättigheter, så att de kunde dölja sin närvaro så att de inte syns av systemadministratörerna.

Den huvudsakliga rollen för rootkits är att dölja processer, filer, inloggningar och loggar. De kan också fånga upp data från terminaler, nätverksanslutningar eller kringutrustning, om de innehåller lämplig programvara.

Rootkits är inte skadliga till sin natur. Till exempel döljer system och till och med vissa appar viktiga filer med rootkits. Men de används mest för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. I kombination med hot utgör rootkits ett stort hot mot integriteten och säkerheten i ett system. De kan övervaka trafik, skapa bakdörrar i systemet, ändra filer och loggar och undvika upptäckt.

Manus

En annan term för makro- eller batchfil, ett skript är en lista med kommandon som kan köras utan användarinteraktion.

Spam

Elektronisk skräppost eller skräpnyhetsgrupper. Allmänt känd som all oönskad e-post.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens internetanslutning utan hans eller hennes vetskap, vanligtvis i reklamsyfte. Spionprogram är vanligtvis paketerade som en dold komponent av gratisprogram eller shareware-program som kan laddas ner från internet; Det bör dock noteras att majoriteten av shareware och freeware-appar inte kommer med spionprogram. När det väl har installerats övervakar spionprogrammet användaraktivitet på internet och överför informationen i bakgrunden till någon annan. Spionprogram kan också samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med ett trojansk hästhot är det faktum att användare omedvetet installerar produkten när de installerar något annat. Ett vanligt sätt att bli offer för spionprogram är att ladda ner vissa peer-to-peer filbytesprodukter som är tillgängliga idag.

Bortsett från frågorna om etik och integritet stjäl spionprogram från användaren genom att använda datorns minnesresurser och även genom att äta bandbredd då det skickar information tillbaka till spionprogrammets hembas via användarens internetanslutning. Eftersom spionprogram använder minne och systemresurser kan apparna som körs i bakgrunden leda till systemkrascher eller allmän systeminstabilitet.

Startobjekt

Alla filer som placeras i den här mappen öppnas när datorn startar. Till exempel kan en startskärm, en ljudfil som ska spelas upp när datorn startar, en påminnelseskalender eller appar vara startobjekt. Normalt placeras ett alias för en fil i den här mappen istället för själva filen.

Prenumeration

Köpeavtal som ger användaren rätt att använda en viss produkt eller tjänst på ett visst antal enheter och under en viss tid. Ett utgånget abonnemang kan förnyas automatiskt med den information som användaren lämnade vid första köpet.

Systemfältet

Systemfältet, som introducerades med Windows 95, finns i aktivitetsfältet i Windows (vanligtvis längst ner bredvid klockan) och innehåller miniatyrikoner för enkel åtkomst till systemfunktioner som fax, skrivare, modem, volym med mera. Dubbelklicka eller högerklicka på en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Transmission Control Protocol/Internet Protocol - En uppsättning nätverksprotokoll som ofta används på internet som tillhandahåller kommunikation över sammankopplade nätverk av datorer med olika hårdvaruarkitekturer och olika operativsystem. TCP/IP innehåller standarder för hur datorer kommunicerar och konventioner för att ansluta nätverk och dirigera trafik.

Hot

Ett program eller kod som läses in på din dator utan din vetskap och som körs mot din vilja. De flesta hot kan också replikera sig själva. Alla datorhot är konstgjorda. Ett enkelt hot som kan kopiera sig själv om och om igen är relativt lätt att producera. Även ett så enkelt hot är farligt eftersom det snabbt kommer att använda allt tillgängligt minne och få systemet att

stanna. En ännu farligare typ av hot är en som kan överföra sig själv över nätverk och kringgå säkerhetssystem.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att upptäcka och eliminera hotet.

Trojan

Ett destruktivt program som maskerar sig som en godartad app. Till skillnad från skadliga program och maskar replikerar trojaner inte sig själva men de kan vara lika destruktiva. En av de mest lömska typerna av trojanska hästhot är ett program som påstår sig befria din dator från hot men istället introducerar hot på din dator.

Termen kommer från en berättelse i Homeros Iliaden, där grekerna ger en gigantisk trähäst till sina fiender, trojanerna, skenbart som ett fredsoffer. Men efter att trojanerna släpat hästen innanför sina stadsmurar, smyger grekiska soldater ut ur hästens ihåliga mage och öppnar stadsportarna, så att deras landsmän kan strömma in och fånga Troja.

Uppdatering

En ny version av en mjuk- eller hårdvaruprodukt utformad för att ersätta en äldre version av samma produkt. Dessutom kontrollerar installationsrutinerna för uppdateringar ofta att en äldre version redan är installerad på din dator; Om inte kan du inte installera uppdateringen.

Bitdefender har sin egen uppdateringsfunktion som låter dig söka manuellt efter uppdateringar, eller låta den uppdatera produkten automatiskt.

Virtual Private Network (VPN)

Är en teknik som möjliggör en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka och ta emot data, svårt att fångas av snokare. Ett bevis på säkerhet är autentiseringen, som endast kan göras med ett användarnamn och lösenord.

Mask

Ett program som sprider sig över ett nätverk och reproducerar sig själv allt eftersom. Den kan inte koppla sig till andra program.