Bitdefender®
ANTIVIRUS FOR MAC

ANVÄNDARMAN
UAL

Bitdefender Antivirus för Mac

Användarmanual

Publiceringsdatum 2022-11-24

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla Macintosh-användare som har valt Bitdefender Antivirus for Mac 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 under Macintosh.

Du kommer att få reda på hur du konfigurerar och använder Bitdefender Antivirus for Mac 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 10)

Kom igång med Bitdefender Antivirus för Mac och dess användargränssnitt.

Skydda mot skadlig programvara (sida 14)

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

Konfigurera inställningar (sida 33)

Läs mer om inställningarna för Bitdefender Antivirus för Mac.

Få hjälp (sida 49)

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. VAD ÄR BITDEFENDER ANTIVIRUS FOR MAC

Bitdefender Antivirus for Mac är en kraftfull antivirusskanner som kan upptäcka och ta bort alla typer av skadlig programvara ("hot"), inklusive:

- ransomware
- adware
- virus
- spionprogram
- Trojaner
- keyloggers
- maskar

Den här appen upptäcker och tar bort inte bara Mac-hot, utan även Windows-hot, vilket förhindrar dig från att av misstag skicka infekterade filer till din familj, vänner och kollegor med hjälp av datorer.

2. INSTALLATION OCH BORTTAGNING

Det här kapitlet innehåller följande ämnen:

2.1. Systemkrav

Du kan installera Bitdefender Antivirus for Mac på Macintosh-datorer som kör OS X Yosemite (10.10) eller nyare versioner.

Din Mac måste också ha minst 1 GB tillgängligt hårddiskutrymme.

En internetanslutning krävs för att registrera och uppdatera Bitdefender Antivirus for Mac.

> **Notera**
> Bitdefender Anti-tracker och Bitdefender VPN kan endast installeras på system som kör macOS 10.12 eller nyare versioner.

> **Så här tar du reda på din macOS-version och hårdvaruinformation om din Mac**
> Klicka på Apple-ikonen i det övre vänstra hörnet av skärmen och välj Om **Denna Mac**. I fönstret som visas kan du se versionen av ditt operativsystem och annan användbar information. Klick **Systemrapport** för detaljerad hårdvaruinformation.

2.2. Installerar Bitdefender Antivirus for Mac

De Bitdefender Antivirus for Mac appen kan installeras från ditt Bitdefender-konto enligt följande:

1. Logga in som administratör.
2. Gå till: https://central.bitdefender.com.
3. Logga in på ditt Bitdefender-konto med din e-postadress och ditt lösenord.
4. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.

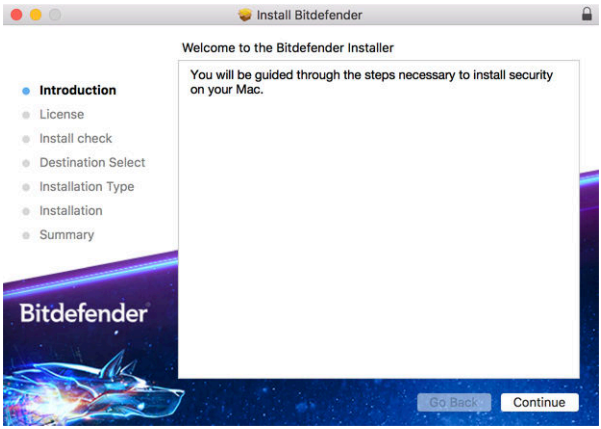
5. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Spara installationsfilen.
   - **Skydda andra enheter**
     a. Välj det här alternativet 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.
6. Kör Bitdefender-produkten du har laddat ner.
7. Slutför installationsstegen.

2.2.1. Installationsprocess

Att installera Bitdefender Antivirus for Mac:

1. Klicka på den nedladdade filen. Detta kommer att starta installationsprogrammet, som guidar dig genom installationsprocessen.
2. Följ installationsguiden.

Steg 1 - Välkomstfönster



Klick **Fortsätta**.

Steg 2 - Läs prenumerationsavtalet

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren under vilka du får använda Bitdefender Antivirus för Mac.

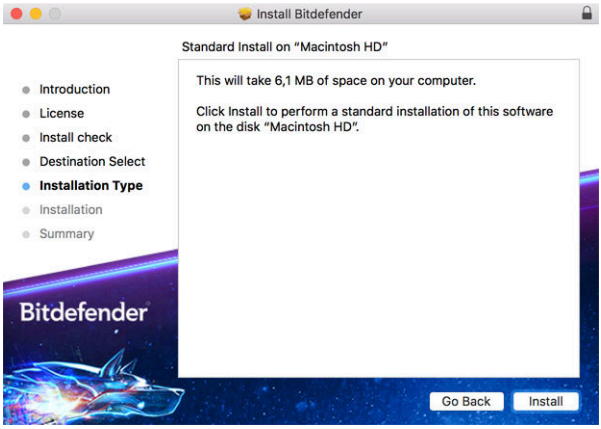
Från det här fönstret kan du också välja vilket språk du vill installera produkten på.

Klick **Fortsätta**, och klicka sedan **Hålla med**.

Viktig

Om du inte godkänner dessa villkor, klicka **Fortsätta**, och klicka sedan **Instämmer inte alls** för att avbryta installationen och avsluta installationsprogrammet.

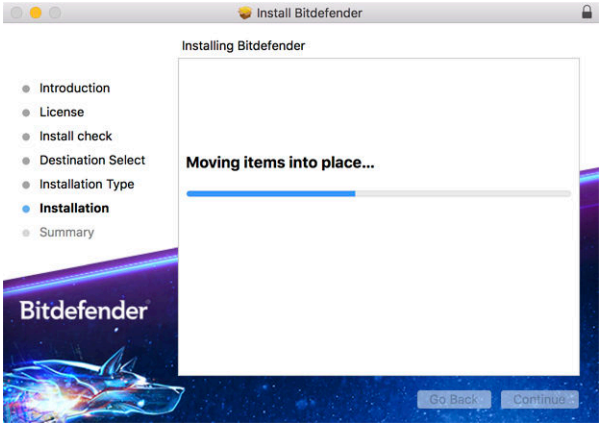
Steg 3 - Starta installationen



Bitdefender Antivirus för Mac kommer att installeras i `Macintosh HD/Library/Bitdefender`. Installationssökvägen kan inte ändras.

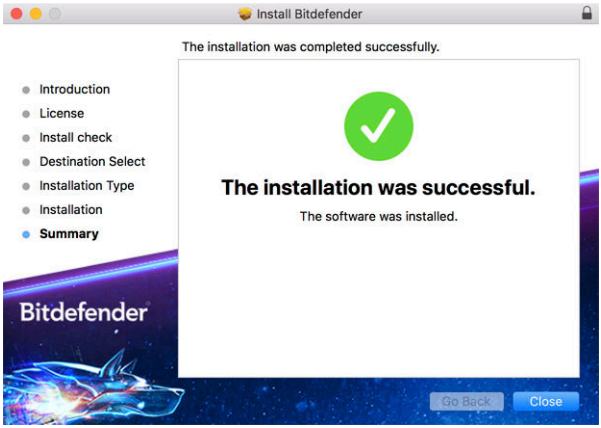
Klick **Installera** för att starta installationen.

Steg 4 - Installera Bitdefender Antivirus för Mac



Vänta tills installationen är klar och klicka sedan **Fortsätta**.

Steg 5 - Avsluta



Klick **Stänga** för att stänga installationsfönstret.

Installationsprocessen är nu klar.

Viktig

- Om du installerar Bitdefender Antivirus för Mac på macOS High Sierra 10.13.0 eller en nyare version, **Systemtillägg blockerat** meddelande visas. Det här meddelandet informerar dig om att tilläggen signerade av Bitdefender har blockerats och måste aktiveras manuellt. Klicka på OK för att fortsätta. I Bitdefender Antivirus för Mac-fönstret som visas klickar du på **Säkerhet och integritet** länk. Klick **Tillåta** i den nedre delen av fönstret, eller välj Bitdefender SRL från listan och klicka sedan **OK**.
- Om du installerar Bitdefender Antivirus för Mac på macOS Mojave 10.14 eller en nyare version kommer ett nytt fönster att visas som informerar dig om att du måste **Ge Bitdefender full diskåtkomst** och **Tillåt Bitdefender att ladda**. Följ instruktionerna på skärmen för att konfigurera produkten korrekt.

2.3. Ta bort Bitdefender Antivirus för Mac

Eftersom det är en komplex app kan Bitdefender Antivirus för Mac inte tas bort på vanligt sätt genom att dra appikonen från *Ansökningar* mappen till papperskorgen.

För att ta bort Bitdefender Antivirus för Mac, följ dessa steg:

1. Öppna a **Upphittare** fönstret och gå sedan till *Ansökningar* mapp.
2. Öppna Bitdefender-mappen i `Applications`, och dubbelklicka sedan **BitdefenderUninstaller**.
3. Välj önskat avinstallationsalternativ.

   Notera
   Om du försöker ta bort bara Bitdefender VPN-appen väljer du **Avinstallera VPN** endast.

4. Klick **Avinstallera** och vänta på att processen ska slutföras.
5. Klick **Stänga** att avsluta.

   Viktig
   Om det finns ett fel kan du kontakta Bitdefender kundtjänst enligt beskrivningen i Ber om hjälp (sida 49).

3. KOMMA IGÅNG

Det här kapitlet innehåller följande ämnen:

3.1. Öppna Bitdefender Antivirus för Mac

Du har flera sätt att öppna Bitdefender Antivirus för Mac.

- Klicka på Bitdefender Antivirus för Mac-ikonen i startfältet.
- Klicka på  ikonen i menyraden och välj **Öppna Antivirus-gränssnittet**.
- Öppna ett Finder-fönster, gå till Applications och dubbelklicka på ikonen **Bitdefender Antivirus för Mac**.

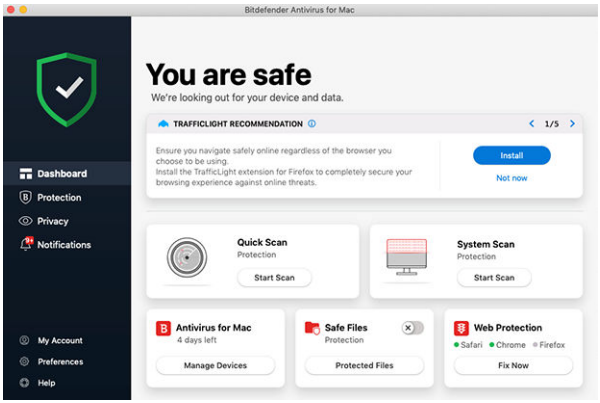
Viktig

Första gången du öppnar Bitdefender Antivirus för Mac på macOS Mojave 10.14 eller en nyare version visas en skyddsrekommendation. Den här rekommendationen visas eftersom vi behöver behörighet för att skanna hela ditt system efter hot. För att ge oss behörigheter måste du vara inloggad som administratör och följa dessa steg:

1. Klicka på **Systeminställningar** länk.
2. Klicka på  ikonen och skriv sedan in dina administratörsuppgifter.
3. Ett nytt fönster öppnas. Dra **BDLDaemon** filen till listan över tillåtna appar.

3.2. Appens huvudfönster

Bitdefender Antivirus för Mac möter 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.

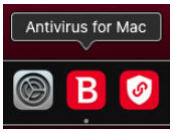
Statusfältet överst i fönstret informerar dig om systemets säkerhetsstatus med hjälp av explicita meddelanden och suggestiva färger. Om Bitdefender Antivirus för Mac inte har några varningar är statusfältet grönt. När ett säkerhetsproblem har upptäckts ändrar statusfältet sin färg till rött. För detaljerad information om problem och hur du åtgärdar dem, se Åtgärda problem (sida 24).

För att erbjuda dig en effektiv operation och ökat skydd samtidigt som du utför olika aktiviteter, **Bitdefender autopilot** kommer att fungera som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, antingen arbetar du eller gör onlinebetalningar Bitdefender Autopilot kommer med kontextuella rekommendationer baserat på din enhetsanvändning och behov. Detta hjälper dig att upptäcka och dra nytta av fördelarna med funktionerna som ingår i Bitdefender Antivirus för Mac-appen.

Från navigeringsmenyn på vänster sida kan du komma åt Bitdefender-sektionerna för detaljerad konfiguration och avancerade administrativa uppgifter (**Skydd** och **Integritet** flikar), aviseringar, din Bitdefender-konto och den Inställningar område. Du kan också kontakta oss (**Hjälp** fliken) för support om du har frågor eller något oväntat dyker upp.

3.3. App Dock-ikon

Bitdefender Antivirus för Mac-ikonen kan ses i Dock så snart du öppnar appen. Ikonen i Dock ger dig ett enkelt sätt att skanna filer och mappar efter hot. Dra och släpp filen eller mappen över Dock-ikonen så startar skanningen omedelbart.



3.4. Navigeringsmeny

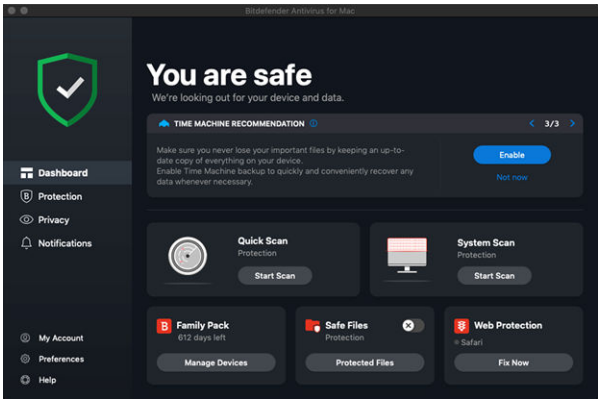
På vänster sida på Bitdefender-gränssnittet finns navigeringsmenyn, som gör att du snabbt kan komma åt Bitdefender-funktionerna du behöver för att hantera din produkt. Flikarna som är tillgängliga i det här området är:

- **instrumentbräda**. Härifrån kan du snabbt fixa säkerhetsproblem, visa rekommendationer enligt dina systembehov och användningsmönster, utföra snabba åtgärder och gå till ditt Bitdefender-konto för att hantera de enheter du har lagt till i ditt Bitdefender-abonnemang.
- **Skydd**. Härifrån kan du starta antivirusgenomsökningar, lägga till filer i undantagslistan, skydda filer och appar från ransomware-attacker, säkra dina Time Machine-säkerhetskopior och konfigurera skydd när du surfar på internet.
- **Integritet**. Härifrån kan du öppna Bitdefender VPN-appen och installera Anti-tracker-tillägget i din webbläsare.
- **Aviseringar**. Härifrån kan du se detaljer om de åtgärder som vidtagits på skannade filer.
- **Mitt konto**. Härifrån kan du se Bitdefender-kontot och prenumerationen som din enhet skyddas av, samt byta konto om det behövs.
- **Inställningar**. Härifrån kan du konfigurera Bitdefender-inställningarna.
- **Hjälp**. Härifrån, närhelst du behöver hjälp med att lösa en situation med din Bitdefender-produkt, kan du kontakta avdelningen för teknisk

support. Du kan också skicka oss din feedback för att hjälpa oss att förbättra produkten.

3.5. Mörkt läge

För att ge dina ögon skydd mot bländning och ljus när du arbetar på natten eller i ett ljusfritt tillstånd, stöder Bitdefender Antivirus för Mac Dark Mode för Mojave 10.14 och senare. Färgerna på gränssnittet har optimerats så att du kan använda din Mac utan att anstränga ögonen. Bitdefender Antivirus för Mac-gränssnittet justerar sig själv beroende på enhetens utseendeinställningar.



4. SKYDDA MOT SKADLIG PROGRAMVARA

Det här kapitlet innehåller följande ämnen:

4.1. Bästa metoder

För att hålla ditt system skyddat mot hot och för att förhindra oavsiktlig infektion av andra system, följ dessa bästa metoder:

- Ha kvar **Bitdefender Shield** aktiverat för att tillåta att systemfiler automatiskt skannas av Bitdefender Antivirus för Mac.
- Håll din Bitdefender Antivirus för Mac-produkt uppdaterad med den senaste hotinformationen och produktuppdateringarna.
- Kontrollera och åtgärda problemen som rapporterats av Bitdefender Antivirus för Mac regelbundet. För detaljerad information, se Åtgärda problem (sida 24).
- Kontrollera den detaljerade loggen över händelser som rör Bitdefender Antivirus för Mac-aktiviteten på din dator. Närhelst något som är relevant för säkerheten för ditt system eller data inträffar läggs ett nytt

meddelande till i Bitdefender-meddelandeområdet. För mer information, gå till Aviseringar (sida 26).

- Du bör också följa dessa bästa metoder:
  - Ta för vana att skanna filer som du laddar ner från ett externt lagringsminne (som ett USB-minne eller en CD), särskilt när du inte känner till källan.
  - Om du har en DMG-fil, montera den och skanna sedan dess innehåll (filerna i den monterade volymen/bilden).

  Det enklaste sättet att skanna en fil, en mapp eller en volym är att dra och släppa den över Bitdefender Antivirus för Mac-fönstret eller Dock-ikonen.

Ingen annan konfiguration eller åtgärd krävs. Men om du vill kan du justera appinställningarna och inställningarna för att bättre passa dina behov. För mer information, se Konfigurera inställningar (sida 33).

4.2. Skanna din Mac

Förutom **Bitdefender Shield** funktion, som övervakar de installerade apparna regelbundet, letar efter hotliknande åtgärder och förhindrar nya hot från att komma in i ditt system. Du kan skanna din Mac eller specifika filer när du vill.

Det enklaste sättet att skanna en fil, en mapp eller en volym är att dra och släppa den över Bitdefender Antivirus för Mac-fönstret eller Dock-ikonen. Skanningsguiden visas och guidar dig genom skanningsprocessen.

Du kan också starta en skanning enligt följande:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Antivirus** flik.
3. Klicka på en av de tre skanningsknapparna för att starta den önskade skanningen.
   - **Snabbskanning** - söker efter hot på de mest sårbara platserna på ditt system (till exempel mapparna som innehåller dokument, nedladdningar, e-postnedladdningar och temporära filer för varje användare).
   - **Genomsökning av systemet** - utför en omfattande kontroll av hot från hela systemet. Alla anslutna fästen skannas också.

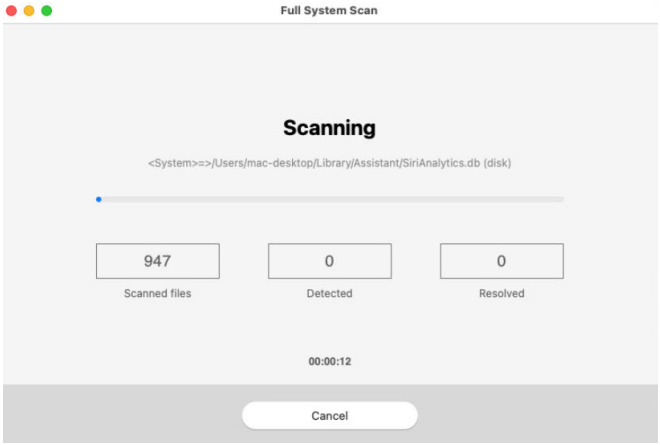
> **Notera**
> Beroende på storleken på din hårddisk kan det ta en stund att skanna hela systemet (upp till en timme eller till och med mer). För förbättrad prestanda rekommenderas att du inte kör den här uppgiften medan du utför andra resurskrävande uppgifter (som videoredigering).
>
> Om du föredrar det kan du välja att inte skanna specifika monterade volymer genom att lägga till dem i Undantag lista från skyddsfönstret.

- **Anpassad skanning** - hjälper dig att kontrollera specifika filer, mappar eller volymer för hot.

Du kan också starta ett system eller en snabbsökning från Dashboard.

4.3. Scan Wizard

När du initierar en skanning visas skanningsguiden för Bitdefender Antivirus för Mac.



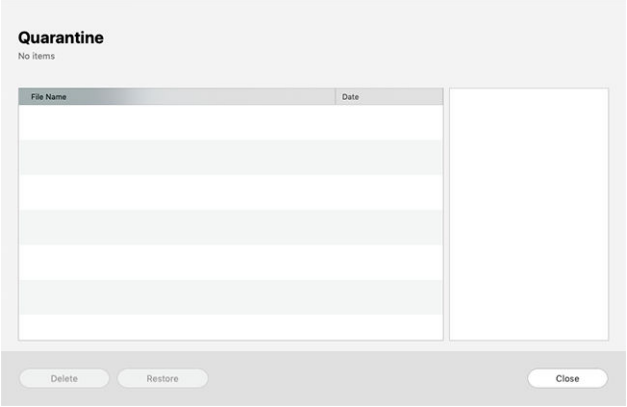
Realtidsinformation om upptäckta och lösta hot visas under varje skanning.

Vänta tills Bitdefender Antivirus för Mac ska avslutas.

> **Notera**
> Skanningsprocessen kan ta ett tag, beroende på hur komplex skanningen är.

4.4. Karantän

Bitdefender Antivirus för Mac gör det möjligt att isolera de infekterade eller misstänkta filerna i ett säkert område, kallat karantän. När ett hot är i karantän kan det inte göra någon skada eftersom det inte kan verkställas eller läsas.



Avsnittet Karantän visar alla filer som för närvarande är isolerade i karantänmappen.

För att ta bort en fil från karantänen, välj den och klicka **Radera**. Om du vill återställa en fil i karantän till sin ursprungliga plats, välj den och klicka **Återställ**.

Så här visar du en lista med alla objekt som lagts till i karantänen:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Klick **Öppen** i **Karantän** rutan.

4.5. Bitdefender Shield (realtidsskydd)

Bitdefender ger realtidsskydd mot ett brett utbud av hot genom att skanna alla installerade appar, deras uppdaterade versioner och nya och modifierade filer.

Så här inaktiverar du realtidsskyddet:

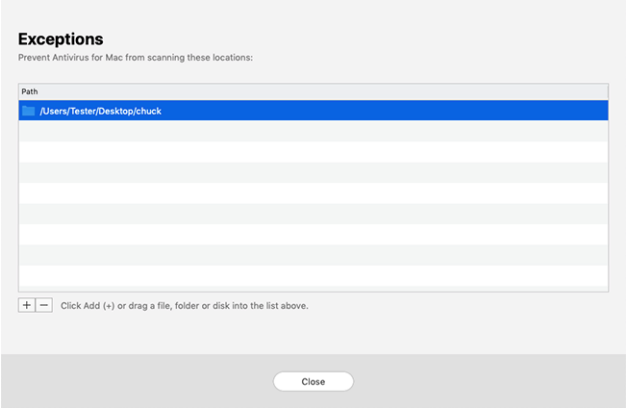
1. Klick **Inställningar** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Stäng av **Bitdefender Shield** i **Skydd** fönster.

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.

4.6. Scan Undantag

Om du vill kan du ställa in Bitdefender Antivirus för Mac att inte skanna specifika filer, mappar eller ens en hel volym. Du kanske till exempel vill utesluta från skanning:

- Filer som av misstag identifieras som infekterade (kända som falska positiva)
- Filer som orsakar skanningsfel
- Säkerhetskopieringsvolymer



Undantagslistan innehåller de sökvägar som har undantagits från skanning.

För att komma åt undantagslistan:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Klick **Öppen** i **Undantag** rutan.

Det finns två sätt att ställa in ett skanningsundantag:

- Dra och släpp en fil, mapp eller volym över undantagslistan.

- Klicka på knappen märkt med plustecknet (+), som finns under undantagslistan. Välj sedan den fil, mapp eller volym som ska undantas från skanning.

För att ta bort ett skanningsundantag, välj det från listan och klicka på knappen märkt med minustecknet (-), som finns under undantagslistan.

4.7. Nätskydd

Bitdefender Antivirus för Mac använder TrafficLight-tilläggen för att helt säkra din webbupplevelse. TrafficLight-tilläggen fångar upp, bearbetar och filtrerar all webbtrafik och blockerar skadligt innehåll.

Tilläggen fungerar och integreras med följande webbläsare: Mozilla Firefox, Google Chrome och Safari.

4.7.1. Aktiverar TrafficLight-tillägg

Så här aktiverar du TrafficLight-tilläggen:

1. Klick **Fixa nu** i **Nätskydd** kort på instrumentpanelen.
2. De **Nätskydd** fönstret öppnas.
   Den upptäckta webbläsaren som du har installerat på ditt system visas. Klicka på för att installera TrafficLight-tillägget i din webbläsare **Skaffa förlängning**.
3. Du omdirigeras till:
   https://bitdefender.com/solutions/trafficlight.html
4. Välj **Gratis nedladdning**.
5. Följ stegen för att installera TrafficLight-tillägget som motsvarar din webbläsare.

4.7.2. Hantera tilläggsinställningar

En rad funktioner finns tillgängliga för att skydda dig från alla typer av hot du kan stöta på när du surfar på webben. För att komma åt dem, klicka på TrafficLight-ikonen bredvid din webbläsares inställningar och klicka sedan på ⚙ **inställningar** knapp:

- **Bitdefender TrafficLight-inställningar**
  - Webbskydd – hindrar dig från att komma åt webbplatser som används för skadlig programvara, nätfiske och bedrägerisattacker.

- Search Advisor - ger förvarning för riskfyllda webbplatser i dina sökresultat.

- **Undantag**
  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 .
  Ingen varning kommer att visas om hot förekommer på de undantagna sidorna. Det är därför endast webbplatser du litar på bör läggas till i den här listan.

4.7.3. Sidbetyg och varningar

Beroende på hur TrafficLight klassificerar webbsidan du för närvarande visar, visas en av följande ikoner i dess område:

Det här är en säker sida att besöka. Du kan fortsätta ditt arbete.

Den här webbsidan kan innehålla farligt innehåll. Var försiktig om du bestämmer dig för att besöka den.

Du bör lämna webbsidan omedelbart eftersom den innehåller skadlig programvara eller andra hot.

I Safari är bakgrunden för TrafficLight-ikonerna svart.

4.8. 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:

- Google Chrome

- Mozilla Firefox
- Safari

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.

4.8.1. Aktiverar Bitdefender Anti-tracker

Så här aktiverar du Bitdefender Anti-tracker-tillägget i din webbläsare:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Antispårare** flik.
3. Klick **Aktivera tillägg** bredvid webbläsaren som du vill aktivera tillägget för.

4.8.2. 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.

4.8.3. 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.

4.8.4. 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 .

4.9. Säkra filer

Ransomware är en skadlig programvara som attackerar sårbara system genom att låsa dem, och ber om pengar för att låta användaren ta tillbaka kontrollen över sitt system. Denna skadliga programvara agerar intelligent genom att visa falska meddelanden för att få användaren i panik, och uppmanar honom att fortsätta med den begärda betalningen.

Genom att använda den senaste tekniken säkerställer Bitdefender systemets integritet genom att skydda kritiska systemområden mot ransomware-attacker utan att påverka systemet. Men du kanske också vill skydda dina personliga filer som dokument, foton eller filmer från att nås av opålitliga appar. Med Bitdefender Safe Files kan du placera personliga

filer till ett skydd och konfigurera på egen hand vilka appar som ska tillåtas göra ändringar i de skyddade filerna och vilka som inte ska göra det.

Så här lägger du till filer i den skyddade miljön:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Anti-Ransomware** flik.
3. Klick **Skyddade filer** i området Säkra filer.
4. Klicka på knappen märkt med plustecknet (+), som finns under listan med skyddade filer. Välj sedan filen, mappen eller volymen som ska skyddas ifall ransomware-attacker försöker komma åt dem.

För att undvika att systemet går långsammare rekommenderar vi att du lägger till maximalt 30 mappar eller sparar flera filer i en enda mapp.

Som standard är mapparna Bilder, Dokument, Skrivbord och Nedladdningar skyddade mot hotattacker.

> **Notera**
> Anpassade mappar kan endast skyddas för nuvarande användare. Externa enheter, system- och appfiler kan inte läggas till i skyddsmiljön.

Du kommer att informeras varje gång en okänd app med ett ovanligt beteende försöker ändra filerna du lagt till. Klick **Tillåta** eller **Blockera** för att lägga till den i Hantera applikationer lista.

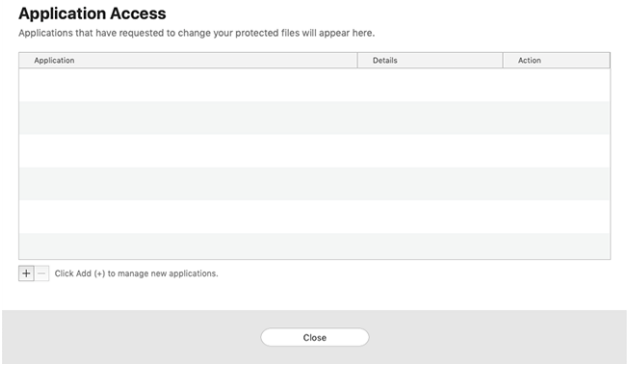
4.9.1. Tillgång till applikationer

De appar som försöker ändra eller ta bort skyddade filer kan flaggas som potentiellt osäkra och läggas till i listan med blockerade appar. Om en sådan app är blockerad och du är säker på att dess beteende är normalt kan du tillåta det genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Anti-Ransomware** flik.
3. Klick **Applikationsåtkomst** i området Säkra filer.
4. Ändra statusen till Tillåt bredvid den blockerade appen.

Appar som är inställda på Tillåt kan också ställas in på Blockerade.

Använd dra och släpp-metoden eller klicka på plustecknet (+) för att lägga till fler appar i listan.



4.10. Time Machine-skydd

Bitdefender Time Machine Protection fungerar som ett extra lager av säkerhet för din säkerhetskopieringsenhet, inklusive alla filer du har bestämt dig för att lagra i den, genom att blockera åtkomsten för någon extern källa. Om filer från din Time Machine-enhet kommer att krypteras med ransomware, kommer du att kunna återställa dem utan att betala för den begärda lösen.

Om du behöver återställa objekt från en Time Machine-säkerhetskopia, kolla Apples supportsida för instruktioner.

4.10.1. Slå på eller av Time Machine Protection

Så här slår du på eller av inaktiverar Time Machine Protection:

1. Klick **Skydd** på navigeringsmenyn på **Bitdefender-gränssnitt**.
2. Välj **Anti-Ransomware** flik.
3. Aktivera eller inaktivera **Time Machine-skydd** växla.

4.11. Åtgärda problem

Bitdefender Antivirus för Mac upptäcker och informerar dig automatiskt om en rad problem som kan påverka säkerheten för ditt system och dina data. På så sätt kan du åtgärda säkerhetsrisker enkelt och i rätt tid.

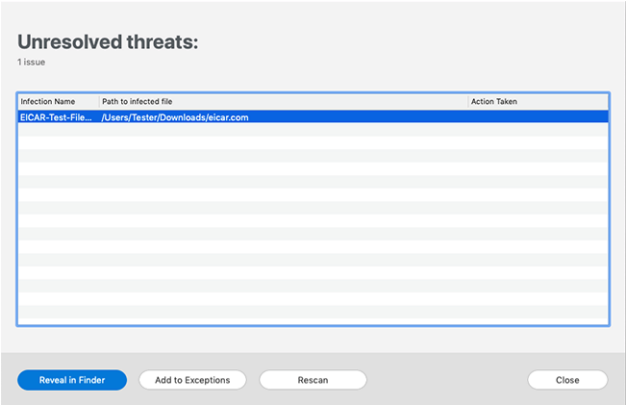
Att åtgärda problemen som indikeras av Bitdefender Antivirus för Mac är ett snabbt och enkelt sätt att säkerställa optimalt skydd av ditt system och dina data.

Upptäckta problem inkluderar:

- Den nya hotinformationsuppdateringen laddades inte ner från våra servrar.
- Hot har upptäckts på ditt system och produkten kan inte desinficera dem automatiskt.
- Realtidsskyddet är inaktiverat.

Så här kontrollerar och åtgärdar du upptäckta problem:

1. Om Bitdefender inte har några varningar är statusfältet grönt. När ett säkerhetsproblem har upptäckts ändrar statusfältet sin färg till rött.
2. Se beskrivningen för mer information.
3. När ett problem upptäcks klickar du på motsvarande knapp för att vidta åtgärder.



Listan över olösta hot uppdateras efter varje systemgenomsökning oavsett om genomsökningen görs automatiskt i bakgrunden eller initieras av dig.

Du kan välja att vidta följande åtgärder för olösta hot:

- Radera manuellt. Vidta den här åtgärden för att ta bort infektionerna manuellt.
- Lägg till i undantag. Den här åtgärden är inte tillgänglig för hot som finns i arkiv.

4.12. Aviseringar

Bitdefender håller en detaljerad logg över händelser som rör dess aktivitet på din dator. 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 dator, etc. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som Bitdefender vidtar.

Klicka på för att komma åt meddelandeloggen **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnittet. Varje gång en kritisk händelse inträffar kan en räknare märkas på 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.

4.13. Uppdateringar

Nya hot hittas och identifieras varje dag. Det är därför det är mycket viktigt att hålla Bitdefender Antivirus för Mac uppdaterad med de senaste hotinformationsuppdateringarna.

Hotinformationsuppdateringarna utförs i farten, vilket innebär att filerna som ska uppdateras ersätts successivt. På detta sätt kommer

uppdateringen inte att påverka produktens funktion och samtidigt kommer alla sårbarheter att undantas.

- Om Bitdefender Antivirus för Mac är uppdaterad kan det upptäcka de senaste hoten som upptäckts och rensa de infekterade filerna.
- Om Bitdefender Antivirus för Mac inte är uppdaterad kommer det inte att kunna upptäcka och ta bort de senaste hoten som upptäckts av Bitdefender Labs.

4.13.1. Begär en uppdatering

Du kan begära en uppdatering manuellt när du vill.

En aktiv internetanslutning krävs för att söka efter tillgängliga uppdateringar och ladda ner dem.

Så här begär du en uppdatering manuellt:

1. Klicka på **Handlingar** knappen i menyraden.
2. Välja **Uppdatera databas för hotinformation**.

Alternativt kan du begära en uppdatering manuellt genom att trycka på CMD + U.

Du kan se uppdateringsförloppet och nedladdade filer.

4.13.2. Få uppdateringar via en proxyserver

Bitdefender Antivirus för Mac kan endast uppdateras via proxyservrar som inte kräver autentisering. Du behöver inte konfigurera några programinställningar.

Om du ansluter till internet via en proxyserver som kräver autentisering måste du byta till en direkt internetanslutning regelbundet för att få uppdateringar av hotinformation.

4.13.3. Uppgradera till en ny version

Ibland lanserar vi produktuppdateringar för att lägga till nya funktioner och förbättringar eller åtgärda produktproblem. Dessa uppdateringar kan kräva en omstart av systemet för att initiera installationen av nya filer. Som standard, om en uppdatering kräver omstart av datorn, fortsätter Bitdefender Antivirus för Mac att arbeta med de tidigare filerna tills du startar om systemet. I det här fallet kommer uppdateringsprocessen inte att störa användarens arbete.

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 för att uppgradera** från menyraden eller starta om systemet manuellt.

4.13.4. Hitta information om Bitdefender Antivirus för Mac

För att hitta information om Bitdefender Antivirus för Mac-versionen som du har installerat, gå till **Handla om** fönster. I samma fönster kan du komma åt och se prenumerationsavtalet, sekretesspolicyn och licenser för öppen källkod.

För att komma åt Om-fönstret:

1. Öppna Bitdefender Antivirus för Mac.
2. Klicka på Bitdefender Antivirus för Mac i menyraden och välj **Om Antivirus för Mac**.

5. VPN

Det här kapitlet innehåller följande ämnen:

5.1. Om VPN

Med Bitdefender VPN kan du hålla din data privat varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personlig data eller försök att göra din enhets IP-adress tillgänglig för hackare undvikas.

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 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.

5.2. Öppnar VPN

Det finns tre sätt att öppna Bitdefender VPN-appen:

- Klick **Integritet** på navigeringsmenyn på **Bitdefender-gränssnitt**. Klick **Öppen** i Bitdefender VPN-kortet.

- Klicka på ikonen från menyraden.
- Gå till mappen Applications, öppna Bitdefender-mappen och dubbelklicka sedan på Bitdefender VPN-ikonen.

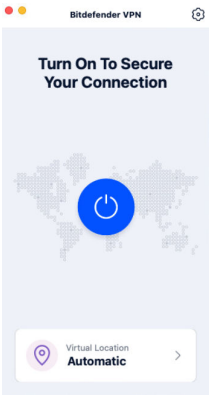
Första gången du öppnar appen uppmanas du att tillåta Bitdefender att lägga till konfigurationer. Genom att tillåta Bitdefender att lägga till konfigurationer samtycker du till att all nätverksaktivitet på din enhet kan filtreras eller övervakas när du använder VPN-appen.

> **Notera**
> Bitdefender VPN-appen kan endast installeras på macOS Sierra (10.12.6), macOS High Sierra (10.13.6) eller macOS Mojave (10.14) eller senare versioner av operativsystemet.

5.3. 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 genom att välja den från listan med virtuella platser. Mer information om VPN-prenumerationer finns i Prenumerationer (sida 32).

För att ansluta eller koppla från, klicka bara på statusen som visas högst upp på skärmen. Menyradens ikon visar svart när VPN är anslutet och vitt när VPN är frånkopplat.



När den är ansluten visas den förflutna tiden på den nedre delen av gränssnittet. För att få tillgång till fler alternativ, klicka på ⚙ ikonen i det övre högra hörnet:

- **Mitt konto** - detaljer om ditt Bitdefender-konto och VPN-prenumeration visas. Klick **Byt konto** om du vill logga in med ett annat konto.
- **inställningar** - beroende på dina behov kan du anpassa beteendet hos din produkt:
  - **Allmän**
    - Aviseringar - Visa produktaviseringar.
    - Kör vid start - Starta Bitdefender VPN automatiskt vid inloggning.
    - Produktrapporter – Skicka in anonyma produktrapporter för att hjälpa oss att förbättra din upplevelse och dina skyddsmöjligheter.
  - **Avancerad**
    - Internet Kill-Switch - Avbryter tillfälligt all internettrafik om VPN-anslutningen av misstag bryts.
    - Annonsblockerare och antispårare - Blockera annonser och spårare för att få en renare och snabbare webb.
    - Split tunneling - Utvalda webbplatser kommer att kringgå VPN och komma åt Internet direkt.

      Notera
      Klick **Hantera** och då **Lägg till webbplats** för att lägga till webbsidor till denna lista.
    - Autoanslut - Anslut VPN automatiskt när:
      - Ansluter till ett osäkert eller offentligt Wi-Fi.
      - En peer-to-peer fildelningsapp startas.

- **Stöd** - du omdirigeras till vår supportcenterplattform där du kan läsa en användbar artikel om hur du använder Bitdefender VPN.
- **Handla om** - information om den installerade versionen visas.
- **Sluta** - avsluta appen.

5.4. Prenumerationer

Bitdefender VPN erbjuder gratis en daglig trafikkvot på 200 MB per enhet för att säkra anslutningen 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-prenumerationen är oberoende av Bitdefender Antivirus för Mac-prenumerationen, vilket innebär att du kommer att kunna använda den under hela dess tillgänglighet, oavsett status för säkerhetsprenumerationen. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Antivirus för Mac fortfarande är aktiv, kommer du att återgå till den kostnadsfria planen.

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.

6. KONFIGURERA INSTÄLLNINGAR

Det här kapitlet innehåller följande ämnen:

6.1. Åtkomst till inställningar

Så här öppnar du fönstret Bitdefender Antivirus för Mac-inställningar:

- Gör något av följande:
  - Klick **Inställningar** på navigeringsmenyn på Bitdefender-gränssnittet.
  - Klicka på Bitdefender Antivirus för Mac i menyraden och välj **Inställningar**.

6.2. Skyddsinställningar

Fönstret med skyddsinställningar låter dig konfigurera den övergripande skanningsmetoden. Du kan konfigurera de åtgärder som vidtas på de upptäckta infekterade och misstänkta filerna och andra allmänna inställningar.

- **Bitdefender Shield.** Bitdefender Shield ger realtidsskydd mot ett brett utbud av hot genom att skanna alla installerade appar, deras uppdaterade versioner och nya och modifierade filer. Vi rekommenderar inte att du inaktiverar Bitdefender Shield, men om du måste, gör det så kort tid som möjligt. Om Bitdefender Shield är inaktiverat kommer du inte att skyddas mot hot.
- **Skanna endast nya och ändrade filer.** Markera den här kryssrutan för att ställa in Bitdefender Antivirus för Mac att endast skanna filer som inte har skannats tidigare eller som har ändrats sedan den senaste genomsökningen.
  Du kan välja att inte använda den här inställningen för anpassad och dra och släpp skanning genom att avmarkera motsvarande kryssruta.

- **Skanna inte innehåll i säkerhetskopior.** Markera den här kryssrutan för att utesluta säkerhetskopior från genomsökning. Om de infekterade filerna återställs vid ett senare tillfälle kommer Bitdefender Antivirus för Mac automatiskt att upptäcka dem och vidta lämpliga åtgärder.

6.3. Avancerade inställningar

Du kan välja en övergripande åtgärd som ska vidtas för alla problem och misstänkta föremål som hittas under en skanningsprocess.

Åtgärd för infekterade föremål

- **Försök att desinficera eller flytta till karantän** - Om infekterade filer upptäcks kommer Bitdefender att försöka desinficera dem (ta bort den skadliga koden) eller flytta dem till karantän.
- **Gör inga åtgärder** - Inga åtgärder kommer att vidtas på de upptäckta filerna.

Åtgärd för misstänkta föremål

- **Flytta filer till karantän** - Om misstänkta filer upptäcks kommer Bitdefender att flytta dem till karantän.
- **Gör inga åtgärder** - Inga åtgärder kommer att vidtas på de upptäckta filerna.

6.4. 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-gränssnittet.
2. Välj **Övrig** flik.
3. Slå på eller av **Mina erbjudanden** växla.

> **Notera**
> De **Mina erbjudanden** alternativet är aktiverat som standard.

7. 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 Antivirus för Mac
  - Bitdefender Windows produktlinje
  - 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.

7.1. 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 Antivirus för Mac huvudgränssnitt:
  1. Klicka på **Gå till ditt konto** länk längst ned till höger på skärmen.

- 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.

7.2. 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.

7.2.1. 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 **KOMMA IGÅNG**.
   Välj en av följande metoder:
   - **Authenticator App** - 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**.

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.

7.3. 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.

7.4. 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.

7.4.1. 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 for Mac 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.

7.4.2. 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**.

7.4.3. 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.

7.5. 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.

7.6. mina prenumerationer

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

7.6.1. 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).

7.6.2. 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.

7.6.3. 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.

7.7. 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.

8. VANLIGA FRÅGOR

Hur kan jag prova Bitdefender Antivirus för Mac innan jag ansöker om en prenumeration?

Du är en ny kund hos Bitdefender och skulle vilja prova vår produkt innan du köper den. Provperioden är 30 dagar och du kan fortsätta använda den installerade produkten endast om du köper ett Bitdefender-abonnemang. För att prova Bitdefender Antivirus för Mac måste du:

1. Skapa ett Bitdefender-konto genom att följa dessa steg:
   a. Gå till: https://central.bitdefender.com.
   b. Skriv in den information som krävs i motsvarande fält. De uppgifter du lämnar här kommer att förbli konfidentiella.
   c. 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.
   d. Klick **SKAPA KONTO**.

2. Ladda ner Bitdefender Antivirus för Mac enligt följande:
   a. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
   b. Välj ett av de två tillgängliga alternativen:
      - **Skydda den här enheten**
        i. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
        ii. Spara installationsfilen.
      - **Skydda andra enheter**
        i. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
        ii. Klick **SKICKA NEDLADDNINGSLÄNK**.
        iii. 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.

iv. På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.

c. Kör Bitdefender-produkten du har laddat ner.

Jag har en aktiveringskod. Hur lägger jag till dess giltighet till mitt abonnemang?

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

Tillägget är nu synligt i ditt Bitdefender-konto och i din Bitdefender Antivirus för Mac-installerade produkt, i den nedre högra delen av skärmen.

Skanningsloggen indikerar att det fortfarande finns olösta objekt. Hur tar jag bort dem?

De olösta objekten i skanningsloggen kan vara:

- arkiv med begränsad åtkomst (xar, rar, etc.)
  Lösning: Använd **Avslöja i Finder** alternativet för att hitta filen och radera den manuellt. Se till att tömma papperskorgen.
- postlådor med begränsad åtkomst (Thunderbird, etc.)
  Lösning: Använd appen för att ta bort posten som innehåller den infekterade filen.
- Innehåll i säkerhetskopior
  Lösning: Aktivera **Skanna inte innehåll i säkerhetskopior** alternativ i Skyddsinställningar eller **Lägg till i undantag** de upptäckta filerna.

Om de infekterade filerna återställs vid ett senare tillfälle kommer Bitdefender Antivirus för Mac automatiskt att upptäcka dem och vidta lämpliga åtgärder.

> **Notera**
> Filer med begränsad åtkomst betyder att filer som Bitdefender Antivirus för Mac bara kan öppna, men inte ändra dem.

Var kan jag se information om produktaktiviteten?

Bitdefender håller en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden relaterade till dess aktivitet. För att komma åt denna information, klicka **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnittet.

Kan jag uppdatera Bitdefender Antivirus för Mac via en proxyserver?

Bitdefender Antivirus för Mac kan endast uppdateras via proxyservrar som inte kräver autentisering. Du behöver inte konfigurera några programinställningar.

Om du ansluter till internet via en proxyserver som kräver autentisering måste du byta till en direkt internetanslutning regelbundet för att få uppdateringar av hotinformation.

Hur tar jag bort Bitdefender Antivirus för Mac?

Följ dessa steg för att ta bort Bitdefender Antivirus för Mac:

1. Öppna a **Upphittare** fönstret och gå sedan till mappen Applications.
2. Öppna mappen Bitdefender och dubbelklicka sedan på BitdefenderUninstaller.
3. Klick **Avinstallera** och vänta på att processen ska slutföras.
4. Klick **Stänga** att avsluta.

> **Viktig**
> Om det finns ett fel kan du kontakta Bitdefender kundtjänst enligt beskrivningen i Ber om hjälp (sida 49).

Hur tar jag bort TrafficLight-tilläggen från min webbläsare?

- Följ dessa steg för att ta bort TrafficLight-tilläggen från Mozilla Firefox:
  1. Gå till **Verktyg** och välj **Tillägg**.

2. Välj **Tillägg** i den vänstra kolumnen.
3. Välj tillägget och klicka **Avlägsna**.
4. Starta om webbläsaren för att borttagningsprocessen ska slutföras.

- Följ dessa steg för att ta bort TrafficLight-tilläggen från Google Chrome:
  1. Klicka på uppe till höger **Mer** ⋮ .
  2. Gå till **Fler verktyg** och välj **Tillägg**.
  3. Klicka på **Avlägsna** ikonen bredvid tillägget du vill ta bort.
  4. Klick **Avlägsna** för att bekräfta borttagningsprocessen.
- För att ta bort Bitdefender TrafficLight från Safari, följ dessa steg:
  1. Gå till **Inställningar** eller tryck **Kommando-Komma(,)**.
  2. Välj **Tillägg**.
     En lista med installerade tillägg visas.
  3. Välj Bitdefender TrafficLight-tillägget och klicka sedan **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta borttagningsprocessen.

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du använder, laddar ner eller laddar upp innehåll på internet. För att se till att du är säker när du surfar på webben rekommenderar vi att du använder Bitdefender VPN när du:

- vill ansluta till offentliga trådlösa nätverk
- vill komma åt innehåll som normalt är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, kreditkortsinformation, etc.)
- vill dölja din IP-adress

Kommer Bitdefender VPN att ha en negativ inverkan på batteritiden för min enhet?

Bitdefender VPN är utformad för att skydda dina personliga data, dölja din IP-adress när du är ansluten till osäkra trådlösa nätverk och komma åt begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning av din enhet rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort när du är offline.

Varför stöter jag på internetnedgångar när jag är ansluten till Bitdefender VPN?

Bitdefender VPN är designad för att erbjuda dig en lätt upplevelse när du surfar på webben; din internetanslutning eller serveravståndet du ansluter till kan dock orsaka nedgången. I det här fallet, om det inte är ett måste att ansluta från din plats till en fjärransluten server (t.ex. från USA till Kina), rekommenderar vi att du tillåter Bitdefender VPN att automatiskt ansluta dig till närmaste server, eller hitta en server närmare din nuvarande plats.

9. FÅ HJÄLP

9.1. 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.

9.2. 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.

9.2.1. 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/.

9.2.2. 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/

9.2.3. 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/.

9.3. 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 49).

https://www.bitdefender.se/consumer/support/

9.3.1. 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.