Bitdefender®

ANTIVIRUS FOR MAC

HANDLEIDING

Bitdefender Antivirus for Mac
Handleiding

Publication date 2018.04.11

GEBRUIKSVOORWAARDEN

Bitdefender

Inhoudsopgave

Gebruik van deze handleiding v
1. Voor wie is deze handleiding bedoeld? v
2. Hoe kunt u deze handleiding gebruiken? v
3. Conventies in deze handleiding v
3.1. Typografische conventies v
3.2. Waarschuw. vi
4. Verzoek om commentaar vii

1. Installeren en verwijderen 1
1.1. Systeemvereisten 1
1.2. Bitdefender Antivirus for Mac installeren 1
1.2.1. Installatieprocedure 2
1.3. Bitdefender Antivirus for Mac verwijderen 6

2. Aan de slag 7
2.1. Over Bitdefender Antivirus for Mac 7
2.2. Bitdefender Antivirus for Mac openen 7
2.3. Hoofdvenster van het programma 8
2.4. Dock-symbool van het programma 9

3. Bescherming tegen schadelijke software 11
3.1. Beste praktische toepassingen 11
3.2. Uw Mac scannen 12
3.3. Autopilot in- of uitschakelen 13
3.4. Bescherming Time Machine 13
3.5. Scan Wizard 15
3.6. Problemen herstellen 15
3.7. Webbeveiliging 17
3.8. Updates 18
3.8.1. Een update aanvragen 19
3.8.2. Updates downloaden via een proxyserver 19
3.8.3. Productupdates 19

4. Voorkeuren instellen 21
4.1. Voorkeuren weergeven 21
4.2. Accountinfo 21
4.3. Beschermingsvoorkeuren 21
4.3.1. Uitsluitingen scannen 23
4.4. Veilige bestanden 24
4.4.1. Toepassingen beheren 27
4.5. Geschiedenis 27
4.6. Quarantaine 28

5. VPN 30
5.1. Over VPN 30
5.2. VPN Installeren 30
5.3. VPN Openen 31
5.4. Interface 31
5.5. Abonnementen 33

6. Bitdefender Central 34
6.1. Over Bitdefender Central 34
6.2. Naar Bitdefender Central gaan 34
6.3. Mijn Abonnementen 35
6.3.1. Abonnement activeren 35
6.3.2. Abonnement kopen 35
6.4. Mijn Apparaten 36
6.4.1. Uw apparaten aanpassen 36
6.4.2. Beheer op afstand 37
7. Veelgestelde vragen 39
8. Hulp vragen 44
8.1. Ondersteuning 44
8.1.1. Online bronnen 44
8.1.2. Hulp inroepen 46
8.2. Contactinformatie 46
8.2.1. Webadressen 46
8.2.2. Lokale verdelers 47
8.2.3. Bitdefender-kantoren 47
Soorten malware (schadelijke software) 50

Gebruik van deze handleiding

1. Voor wie is deze handleiding bedoeld?

Deze handleiding is bedoeld voor alle Macintosh-gebruikers die **Bitdefender Antivirus for Mac** gebruiken als beveiligingsoplossing voor hun computers. De informatie in deze handleiding is niet alleen geschikt voor gevorderde computergebruikers, maar voor iedereen die met een Macintosh overweg kan.

U leest in deze handleiding hoe u Bitdefender Antivirus for Mac kunt configureren en gebruiken om uzelf te beschermen tegen virussen en andere schadelijke software, zodat u maximaal profijt hebt van Bitdefender.

Wij wensen u veel aangenaam en nuttig leesplezier.

2. Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Aan de slag (p. 7)
Kennismaking met Bitdefender Antivirus for Mac en de gebruikersinterface.

Bescherming tegen schadelijke software (p. 11)
Bescherm uzelf met Bitdefender Antivirus for Mac tegen schadelijke software en phishing-scams.

Voorkeuren instellen (p. 21)
De voorkeursinstellingen van Bitdefender Antivirus for Mac.

Hulp vragen (p. 44)
Informatie over waar u om hulp kunt vragen indien er zich onverwachte problemen voordoen.

3. Conventies in deze handleiding

3.1. Typografische conventies

In deze gids worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel weergegeven.

Weergave	Beschrijving
voorbeeld syntaxis	Syntaxisvoorbeelden zijn gedrukt in enkelspatietekens.
https://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Gebruik van deze handleiding (p. v)	Dit is een interne koppeling naar een locatie in het document.
filename	Bestandsnamen en mappen worden afgedrukt met een enkelspatielettertype.
optie	Alle productopties worden afgedrukt met **vet** tekens.
sleutelwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

3.2. Waarschuw.

De waarschuwingen zijn opmerkingen in de tekst die grafisch zijn gemarkeerd en uw aandacht wordt getrokken naar extra informatie met betrekking tot de huidige paragraaf.

Opmerking

De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

Belangrijk

Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritische, maar belangrijke informatie.

Waarschuwing

Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

4. Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com. Wij verzoeken u al uw e-mails met betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

1. INSTALLEREN EN VERWIJDEREN

Dit hoofdstuk bevat de volgende onderwerpen:

- *Systeemvereisten* (p. 1)
- *Bitdefender Antivirus for Mac installeren* (p. 1)
- *Bitdefender Antivirus for Mac verwijderen* (p. 6)

1.1. Systeemvereisten

U kunt Bitdefender Antivirus for Mac alleen installeren op een op Intel gebaseerde Macintosh-computer met OS X Mavericks (10.9.5), OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra(10.12.5 of later), macOS High Sierra 10.13.

Uw Mac moet bovendien aan deze vereisten voldoen:

- Minimaal 1 GB RAM-geheugen
- Minimum 600 MB beschikbare harde schijfruimte

Om Bitdefender Antivirus for Mac te registreren en bij te werken, hebt u een internetverbinding nodig.

Zo vindt u uw macOS-versie en hardware-informatie over uw Mac

Klik linksboven in het scherm op het Apple-symbool en kies **Over deze Mac**. Er wordt nu een venster geopend met informatie over de versie van uw besturingssysteem. Klik op **Meer info** voor uitgebreide informatie over de hardware.

1.2. Bitdefender Antivirus for Mac installeren

De Bitdefender Antivirus for Mac-app kan als volgt geïnstalleerd worden vanaf uw Bitdefender-account:

1. Log in als beheerder.
2. Ga naar: https://central.bitdefender.com.
3. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
4. Selecteer het paneel **Apparaten** en klik dan op **LOKALE BESCHERMING INSTALLEREN**.

5. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

     Klik op de knop en sla het installatiebestand op.
   - **Op een ander apparaat**

     Selecteer **macOS** om uw Bitdefender-product te downloaden en klik vervolgens op **Doorgaan**. Typ een e-mailadres in het e-mailveld en klik op **Verzenden**.
6. Start het gedownloade Bitdefender-programma.
7. Voer de installatiestappen uit.

1.2.1. Installatieprocedure

Zo installeert u Bitdefender Antivirus for Mac:

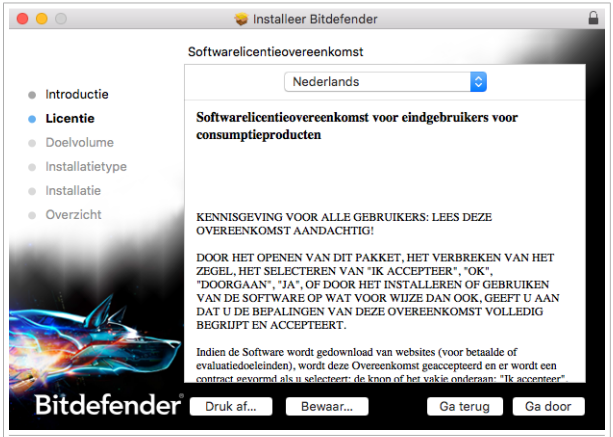
1. Klik op het gedownloade bestand. Hiermee start u het installatieprogramma, dat u begeleidt bij de installatie.
2. Volg de stappen van de installatiewizard.

Stap 1 – Welkomstvenster

Welkomstvenster

Klik op **Doorgaan**.

Stap 2 - Abonnementsovereenkomst lezen



Lees de Abonnementsovereenkomst

De Abonnementsovereenkomst is een wettelijk bindende overeenkomst tussen u en Bitdefender over het gebruik van Bitdefender Antivirus for Mac. U kunt de Abonnementsovereenkomst afdrukken of opslaan om het later nog eens na te lezen.

Lees de Abonnementsovereenkomst aandachtig. U kunt de installatie van de software alleen voortzetten als u akkoord gaat met de bepalingen van de Abonnementsovereenkomst. Klik op **Doorgaan** en vervolgens op **Akkoord**.

Belangrijk

Als u niet instemt met de voorwaarden in de Licentieovereenkomst, klikt u op **Doorgaan** en vervolgens op **Niet akkoord** om de installatie te annuleren en het installatieprogramma af te sluiten.

Stap 3 - Installatie starten

Installatie starten

Bitdefender Antivirus for Mac wordt geïnstalleerd in de map Macintosh HD/Bibliotheek/Bitdefender. **Dit installatiepad kan niet worden gewijzigd.**

Klik op **Installeren** om de installatie te starten.

Stap 4 - Bitdefender Antivirus for Mac installeren

Bitdefender Antivirus for Mac installeren

Wacht tot de installatie uitgevoerd is en klik vervolgens op **Doorgaan**.

Stap 5 - Voltooien

Voltooien

Klik op **Sluiten** om het installatie venster te sluiten.

De installatieprocedure is nu voltooid.

Belangrijk
Als u Bitdefender Antivirus for Mac op macOS High Sierra 10.13 of een recentere versie installeert, verschijnt het bericht **Systeem Extensie geblokkeerd**. Dit bericht informeert u dat de extensies van Bitdefender geblokkeerd zijn en handmatig moeten worden geactiveerd. Klik op **OK** om door te gaan. In het Bitdefender Antivirus for Mac venster dat verschijnt, klik op de**Veiligheid & Privacy** link. Vink het vakje van Bitdefender in de lijst aan en klik daarna op **OK**.

Wanneer u Bitdefender Antivirus for Mac voor het eerst installeert, verschijnen de wizards Veilige bestanden en Time Machine Protection. Zie *Veilige bestanden* (p. 24) eb *Bescherming Time Machine* (p. 13) voor meer informatie.

U krijgt een inleiding in de VPN-functie. Klik op **Next** om verder te gaan. Voor meer informatie, raadpleeg *VPN* (p. 30).

1.3. Bitdefender Antivirus for Mac verwijderen

Omdat Bitdefender Antivirus for Mac een geavanceerd programma is, kunt u het niet op de gewone manier verwijderen door het programmasymbool van de map Programma's naar de Prullenmand te slepen.

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster ga naar de map Programma's en kies Hulpprogramma's.
2. Dubbelklik op het programma Bitdefender for Mac-verwijdertool om dit programma te starten.
3. Klik op de knop **Verwijderen** en wacht tot de verwijdering is uitgevoerd.
4. Klik op **Sluiten**.

Belangrijk
Als er problemen optreden, kunt u contact opnemen met Bitdefender Klantenondersteuning volgens de aanwijzingen in *Ondersteuning* (p. 44).

2. AAN DE SLAG

Dit hoofdstuk bevat de volgende onderwerpen:

- *Over Bitdefender Antivirus for Mac* (p. 7)
- *Bitdefender Antivirus for Mac openen* (p. 7)
- *Hoofdvenster van het programma* (p. 8)
- *Dock-symbool van het programma* (p. 9)

2.1. Over Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac is een krachtige antivirusscanner die alle soorten schadelijke software ("malware") kan detecteren en verwijderen, waaronder:

- ransomware
- Adware
- virussen gevonden
- spyware
- Trojaanse paarden
- keyloggers
- wormen.

Dit programma detecteert en verwijdert niet alleen malware voor de Mac, maar ook malware voor Windows. Hierdoor weet u zeker dat u nooit ongemerkt een besmet bestand doorstuurt naar familie, vrienden of kennissen die een Windows-pc gebruiken.

2.2. Bitdefender Antivirus for Mac openen

U kunt Bitdefender Antivirus for Mac op verschillende manieren starten:

- Klik in Launchpad op het symbool van Bitdefender Antivirus for Mac.
- Klik in de menubalk op  en kies **Hoofdvenster openen**.
- Open een Finder-venster, ga naar Programma's en dubbelklik op het symbool van Bitdefender Antivirus for Mac.

2.3. Hoofdvenster van het programma

In het hoofdvenster van het programma kunt u de beveiligingsstatus van uw computer bekijken, systeemscans uitvoeren, uw webbrowser beveiligen of inloggen op uw Bitdefender-account.

Hoofdvenster van het programma

De functie **Autopilot**, rechtsboven in het hoofdvenster, bewaakt automatisch alle programma's die op de computer actief zijn, detecteert gebeurtenissen die op malware kunnen wijzen en verhindert dat nieuwe malwaredreigingen tot uw systeem doordringen.

Om veiligheidsredenen adviseren we u om Autopilot altijd ingeschakeld te laten. Als u Autopilot uitschakelt, bent u niet langer automatisch beschermd tegen malware.

De statusbalk boven in het venster geeft informatie over de beveiligingsstatus van het systeem in de vorm van tekstberichten met een kleurcodering. Als er geen waarschuwingen van Bitdefender Antivirus for Mac zijn, is de statusbalk groen. Als er een beveiligingsprobleem is gedetecteerd, krijgt de statusbalk de kleur geel. Klik op de knop **Problemen weergeven** om te zien welke problemen de beveiliging van uw systeem in gevaar brengen. Zie *Problemen herstellen* (p. 15) voor meer informatie over mogelijke problemen en hun oplossingen.

Onder de statusbalk bevinden zich drie knoppen waarmee u scans kunt uitvoeren:

- **Snelle scan** - controleert op de aanwezigheid van malware op de meest kwetsbare locaties van uw systeem (bijvoorbeeld de mappen met documenten, downloads, Mail-downloads en tijdelijke bestanden van alle gebruikers).
- **Volledige scan** - voert een uitgebreide malwarescan uit op het volledige systeem. Ook alle geactiveerde volumes worden gescand.
- **Aangepaste scan** - hiermee kunt u specifieke bestanden, mappen of volumes scannen op malware.

Zie *Uw Mac scannen* (p. 12) voor meer informatie.

Onder de scanknoppen zijn de volgende opties beschikbaar:

- **Webbeveiliging** - filtert al het webverkeer en blokkeert schadelijke content, zodat u veilig op het web kunt surfen. Zie *Webbeveiliging* (p. 17) voor meer informatie.
- **Ga naar Bitdefender-account** - klik rechtsonder in het hoofdvenster op de koppeling **Ga naar uw account** om uw Bitdefender-account te openen. Zie *Bitdefender Central* (p. 34) voor meer informatie.
- **Aantal resterende dagen** - hier ziet u hoe lang het nog duurt voordat uw abonnement verloopt. Als de einddatum niet meer veraf is, kunt u op de koppeling klikken om een webpagina te openen voor het verlengen van uw abonnement.
- **Kopen** - hiermee gaat u naar de Bitdefender-website, waar u aanbiedingen kunt bekijken of een abonnement kunt nemen.
- **Feedback** - opent een nieuw berichtvenster in uw standaard e-mailclient, zodat u ons een e-mail kunt sturen.

2.4. Dock-symbool van het programma

Het symbool van Bitdefender Antivirus for Mac verschijnt in het Dock zodra u het programma opent. Met het Dock-symbool kunt u heel gemakkelijk bepaalde mappen en bestanden scannen op malware. Als u een bestand of een map naar het Dock-symbool sleept, wordt het bestand of de map onmiddellijk gescand.

Dock-symbool

3. BESCHERMING TEGEN SCHADELIJKE SOFTWARE

Dit hoofdstuk bevat de volgende onderwerpen:

- *Beste praktische toepassingen* (p. 11)
- *Uw Mac scannen* (p. 12)
- *Autopilot in- of uitschakelen* (p. 13)
- *Bescherming Time Machine* (p. 13)
- *Scan Wizard* (p. 15)
- *Problemen herstellen* (p. 15)
- *Webbeveiliging* (p. 17)
- *Updates* (p. 18)

3.1. Beste praktische toepassingen

Om uw systeem vrij van malware te houden en te voorkomen dat andere systemen onbedoeld vanaf uw computer geïnfecteerd worden, gelden de volgende aanbevelingen:

- Zorg dat **Autopilot** altijd ingeschakeld is, zodat de systeembestanden automatisch door Bitdefender Antivirus for Mac worden gescand.
- Zorg dat Bitdefender Antivirus for Mac altijd over de nieuwste productupdates en malwarehandtekeningen beschikt, door **Autopilot** ingeschakeld te laten.
- Controleer regelmatig of er problemen worden gemeld door Bitdefender Antivirus for Mac, en los deze problemen op. Zie *Problemen herstellen* (p. 15) voor meer informatie.
- Bekijk ook de gedetailleerde Bitdefender Geschiedenis over de activiteiten van Bitdefender Antivirus for Mac op uw computer. Zodra er iets gebeurt dat van belang is voor de veiligheid van uw systeem of uw gegevens, wordt een melding toegevoegd aan dit logbestand. Zie *Geschiedenis* (p. 27) voor meer informatie.
- Volg ook de volgende adviezen op:

- Maak er een gewoonte van om alle bestanden te scannen die u laadt vanaf een extern opslagmedium, zoals een usb-stick of cd. Dit is extra belangrijk als u niet zeker bent van de herkomst van het bestand.
- Als u een DMG-bestand hebt, moet u dit eerst activeren en vervolgens scant u de inhoud (de bestanden in het geactiveerde volume of de geactiveerde schijfkopie).

De handigste manier om een bestand, een map of een volume te scannen, is door het object naar het venster of het Dock-symbool van Bitdefender Antivirus for Mac te slepen.

Verder hoeft u niets te doen of in te stellen. Als u dit wilt, kunt u de instellingen en voorkeuren van het programma aan uw wensen aanpassen. Zie *Voorkeuren instellen* (p. 21) voor meer informatie.

3.2. Uw Mac scannen

De functie **Autopilot** bewaakt automatisch alle programma's die op uw computer worden uitgevoerd, detecteert gebeurtenissen die op malware wijzen en verhindert dat nieuwe malwaredreigingen uw systeem binnendringen, maar u kunt daarnaast ook op elk gewenst moment handmatig uw Mac of specifieke bestanden of mappen scannen.

De handigste manier om een bestand, een map of een volume te scannen, is door het object naar het venster of het Dock-symbool van Bitdefender Antivirus for Mac te slepen. De scanwizard wordt gestart en begeleidt u tijdens het scanproces.

U kunt een scan ook op deze manier starten:

1. Bitdefender Antivirus for Mac openen.
2. Klik op een van de drie scanknoppen om de gewenste scan uit te voeren.
   - **Snelle scan** - controleert op de aanwezigheid van malware op de meest kwetsbare locaties van uw systeem (bijvoorbeeld de mappen met documenten, downloads, Mail-downloads en tijdelijke bestanden van alle gebruikers).
   - **Volledige scan** - voert een uitgebreide malwarescan uit op het volledige systeem. Ook alle geactiveerde volumes worden gescand.

Opmerking

Afhankelijk van de grootte van uw harde schijf kan een scan van het volledige systeem veel tijd in beslag nemen (soms wel een uur, of nog langer). Om de systeemprestaties niet te beïnvloeden, is het aan te raden geen volledige scans te starten terwijl u complexe taken (zoals videobewerking) uitvoert.
Als u wilt, kunt u instellen dat bepaalde geactiveerde volumes niet gescand worden, door deze volumes toe te voegen aan de lijst Uitsluitingen in het voorkeurenvenster.

- **Aangepaste scan** - hiermee kunt u specifieke bestanden, mappen of volumes scannen op malware.

3.3. Autopilot in- of uitschakelen

U kunt Autopilot op de volgende manieren in- of uitschakelen:

- Open Bitdefender Antivirus for Mac en klik op de schakelaar om Autopilot in of uit te schakelen.
- Klik in de menubalk op en kies **Zet Autopilot UIT**.

Waarschuwing

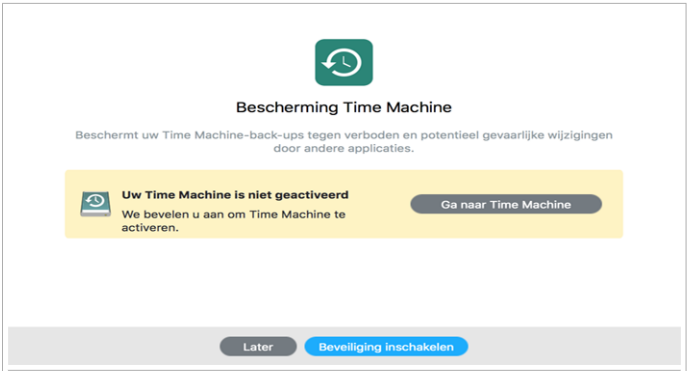
We adviseren u om Autopilot zo min mogelijk uit te schakelen. Als u Autopilot uitschakelt, bent u niet langer automatisch beschermd tegen malware.

3.4. Bescherming Time Machine

Bitdefender Time Machine Protection biedt een extra beveiligingslaag voor de bestanden die op uw Time Machine-schijf zijn opgeslagen, doordat externe toegang tot deze backupschijf wordt geblokkeerd. Mochten deze bestanden ooit worden gegijzeld door ransomware, kunt u ze vanaf uw Time Machine-schijf herstellen zonder losgeld te betalen.

De wizard Time Machine Protection

De wizard Bitdefender Time Machine Protection wordt gestart wanneer u Bitdefender Antivirus for Mac voor het eerst op uw Macintosh installeert.



De wizard Time Machine Protection

U moet het backupprogramma Time Machine configureren vóórdat u de Bitdefender-beveiliging inschakelt.

Als de functie Time Machine nog niet is ingeschakeld op uw computer:

1. Klik op de optie **Ga naar Time Machine**.

   Het venster **Time Machine** van Systeemvoorkeuren wordt geopend.

2. Activeer deze functie en selecteer waar de reservekopieën moeten worden opgeslagen.

Voor meer informatie over het activeren van Time Machine op uw systeem klikt u vanuit de wizard op de koppeling **Bekijk hier hoe u Time Machine kunt configureren**.

Zo activeert u Bitdefender Time Machine Protection voor uw backups:

1. Klik op de optie **Bescherming inschakelen**.

   Er wordt een bevestigingsvenster weergegeven.

2. Klik op **Sluiten**.

Time Machine Protection in- of uitschakelen

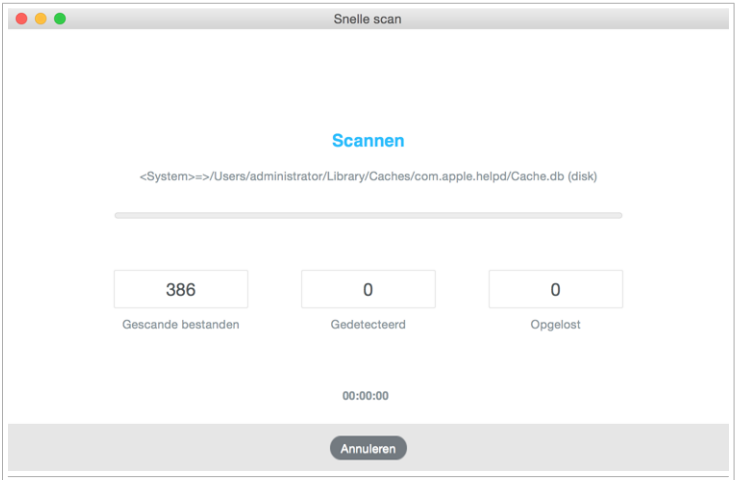
Zo schakelt u Time Machine Protection in of uit:

1. Bitdefender Antivirus for Mac openen.
2. Klik in de menubalk op Bitdefender Antivirus for Mac en kies **Voorkeuren**.
3. Selecteer het tabblad **Bescherming**.

4. Selecteer of wis het selectievakje **Bescherming Time Machine**.

3.5. Scan Wizard

Zodra u een scan start, verschijnt de scanwizard van Bitdefender Antivirus for Mac.



Scan wordt uitgevoerd

Tijdens elke scan wordt realtime informatie weergegeven over gedetecteerde en verwijderde dreigingen.

Wacht tot Bitdefender Antivirus for Mac het scannen beëindigt.

Opmerking
Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

3.6. Problemen herstellen

Bitdefender Antivirus for Mac detecteert en signaleert automatisch verschillende soorten problemen die van belang zijn voor de veiligheid van uw systeem en uw gegevens. Hierdoor kunt u eventuele veiligheidsrisico's tijdig verhelpen.

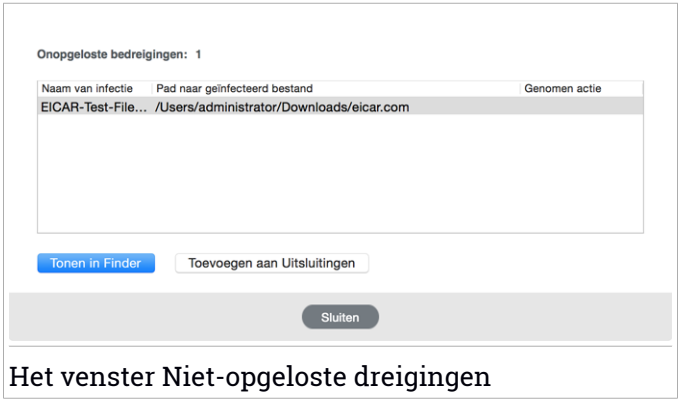
Als u de problemen oplost die door Bitdefender Antivirus for Mac worden gemeld, weet u zeker dat uw systeem en uw gegevens altijd veilig zijn.

Onder andere deze problemen kunnen worden gemeld:

- De nieuwe malwarehandtekeningen en productupdates worden niet van onze servers gedownload, omdat **Autopilot** is uitgeschakeld.
- Er zijn niet-opgeloste dreigingen op uw systeem aangetroffen.
- **Autopilot** is uitgeschakeld.

Zo kunt u controleren of er problemen zijn en deze verhelpen:

1. Bitdefender Antivirus for Mac openen.
2. Als er geen waarschuwingen van Bitdefender zijn, is de statusbalk groen. Als er een veiligheidsprobleem is gedetecteerd, wordt de statusbalk in de kleur geel weergegeven.
3. Lees de beschrijving voor meer informatie.
4. Als er een probleem is aangetroffen, klikt u op de knop **Problemen weergeven** om informatie te bekijken over het probleem voor de beveiliging van uw systeem. In het venster dat nu wordt weergegeven, kunt u maatregelen nemen om de problemen te verhelpen.



Het venster Niet-opgeloste dreigingen

Na elke systeemscan wordt de lijst met niet-opgeloste dreigingen bijgewerkt.

U kunt op de knoppen in het venster klikken om de volgende maatregelen te nemen voor deze dreigingen:

- Tonen in Finder. Kies deze actie als u besmettingen handmatig wilt verwijderen.

- Toevoegen aan Uitsluitingen. Deze actie is niet beschikbaar voor malware die is aangetroffen in een archief.

3.7. Webbeveiliging

Bitdefender Antivirus for Mac gebruikt de TrafficLight-extensies om uw webbrowser te beveiligen. De TrafficLight-extensies filteren, onderscheppen en verwerken al het webverkeer, waarbij schadelijke content automatisch wordt geblokkeerd.

De extensies zijn geschikt voor de webbrowsers Mozilla Firefox, Google Chrome en Safari.

TrafficLight-extensies inschakelen

Zo schakelt u de TrafficLight-extensies in:

1. Bitdefender Antivirus for Mac openen.
2. Klik op **Nu herstellen** om de webbeveiliging te activeren.
3. Bitdefender Antivirus for Mac detecteert automatisch de webbrowser die op uw systeem is geïnstalleerd. Om de TrafficLight-extensie in uw browser te installeren, klikt u op **Extensie downloaden**.
4. U wordt doorgestuurd naar deze webpagina:

   https://bitdefender.nl/solutions/trafficlight.html
5. Selecteer **Gratis download**.
6. Volg de aanwijzingen om de juiste TrafficLight-extensie voor uw webbrowser te installeren.

Extensie-instellingen beheren

Een waaier aan functies is beschikbaar om u te beschermen tegen de verschillende soorten bedreigingen die u tijdens het browsen kunt tegenkomen. Om deze functies te gebruiken: klik op de icoon TrafficLight naast de instellingen van uw browser en dan op **Instellingen**:

- **Instellingen Bitdefender TrafficLight**
  - Geavanceerd dreigingsfilter: beschermt u tegen bezoeken aan websites die worden gebruikt voor malware-, phishing- en fraudeaanvallen.

- Tracker detector - spoort trackers op de bezochte webpagina's op en houdt u op de hoogte over hun aanwezigheid.
- Analyse van zoekresultaten: waarschuwt u van tevoren over riskante websites die worden genoemd in zoekresultaten.

  Indien alle instellingen uitgeschakeld zijn, wordt geen enkele website gescand.

- **Witte lijst**

  Websites kunnen uitgesloten worden van scannen door Bitdefender engines. Geef in het overeenstemmende veld de naam van de website in die u wilt toevoegen aan de witte lijst en klik dan op **TOEVOEGEN**.

  Er wordt geen waarschuwing weergegeven wanneer er bedreigingen zijn op de uitgesloten pagina's. Daarom dient u enkel websites die u volledig vertrouwt toe te voegen aan de lijst.

Paginabeoordelingen en waarschuwingen

Afhankelijk van de beoordeling door TrafficLight van de webpagina die u momenteel bekijkt, worden de volgende pictogrammen weergegeven, in de kleuren van een verkeerslicht:

Dit is een pagina die u veilig kunt bezoeken. U kunt gewoon doorgaan.
Deze webpagina bevat mogelijke gevaarlijke onderdelen. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.
U dient de webpagina onmiddellijk te verlaten: de pagina bevat malware en andere bedreigingen.

In Safari is de achtergrond van de iconen van TrafficLight zwart.

3.8. Updates

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u Bitdefender Antivirus for Mac up-to-date houdt met de meest recente malware handtekeningen.

Zorg dat **Autopilot** altijd ingeschakeld is, zodat de malwarehandtekeningen en productupdates automatisch naar uw systeem worden gedownload. Als er een update is gedetecteerd, wordt deze automatisch gedownload en geïnstalleerd op uw computer.

Het malwarehandtekeningen-update wordt “on the fly” uitgevoerd. Dit betekent dat de bestanden die moeten worden bijgewerkt, progressief worden

vervangen. Hierdoor zal het update de productwerking niet beïnvloeden wordt tegelijkertijd elk zwak punt uitgeschakeld.

- Als Bitdefender Antivirus for Mac up-to-date is, kunnen ook de nieuwste dreigingen worden gedetecteerd en uit geïnfecteerde bestanden worden verwijderd.
- Maar als Bitdefender Antivirus for Mac niet goed is bijgewerkt, bent u niet beveiligd tegen de nieuwste soorten malware die zijn ontdekt door Bitdefender Labs.

3.8.1. Een update aanvragen

U kunt altijd handmatig een update uitvoeren.

Om te kijken of er nieuwe updates zijn en deze te downloaden, hebt u een actieve internetverbinding nodig.

Zo voert u handmatig een update uit:

1. Bitdefender Antivirus for Mac openen.
2. Klik in de menubalk op de knop **Acties**.
3. Kies **Virusdatabase bijwerken**.

U kunt een handmatige update ook uitvoeren door op Command+U te drukken.

Er wordt informatie weergegeven over de voortgang van de update en de gedownloade bestanden.

3.8.2. Updates downloaden via een proxyserver

Bitdefender Antivirus for Mac kan alleen updates downloaden via een proxyserver die géén authenticatie vereist. U hoeft hiervoor verder geen programma-instellingen te wijzigen.

Als u normaal gesproken verbinding met het internet maakt via een proxyserver die wél authenticatie vereist, moet u regelmatig overschakelen naar een rechtstreekse internetverbinding om te zorgen dat u updates van malwarehandtekeningen kunt ontvangen.

3.8.3. Productupdates

Van tijd tot tijd voeren we een productupdate uit om nieuwe functies en verbeteringen aan het product toe te voegen of om problemen te verhelpen.

Bij een dergelijke update moet soms het systeem opnieuw worden opgestart, zodat nieuwe bestanden kunnen worden geïnstalleerd. Als het voor een productupdate noodzakelijk is het systeem opnieuw op te starten, blijft Bitdefender Antivirus for Mac de oude bestanden gebruiken zolang u de computer nog niet opnieuw hebt opgestart. U kunt dan gewoon doorwerken tijdens het updateproces.

Nadat de productupdate voltooid is, verschijnt een popup-venster met de melding dat het systeem opnieuw moet worden opgestart. Als u deze melding over het hoofd hebt gezien, kunt u in de menubalk op **Opnieuw opstarten voor upgrade** klikken of het systeem handmatig opnieuw opstarten.

4. VOORKEUREN INSTELLEN

Dit hoofdstuk bevat de volgende onderwerpen:

- *Voorkeuren weergeven* (p. 21)
- *Accountinfo* (p. 21)
- *Beschermingsvoorkeuren* (p. 21)
- *Uitsluitingen scannen* (p. 23)
- *Veilige bestanden* (p. 24)
- *Geschiedenis* (p. 27)
- *Quarantaine* (p. 28)

4.1. Voorkeuren weergeven

Zo opent u het voorkeurenvenster van Bitdefender Antivirus for Mac:

1. Bitdefender Antivirus for Mac openen.
2. Voer een van de volgende bewerkingen uit:
   - Klik in de menubalk op Bitdefender Antivirus for Mac en kies **Voorkeuren**.
   - Klik in de menubalk op en kies **Voorkeuren**.
   - Druk op Command+komma (,).

4.2. Accountinfo

Het venster Accountinfo toont informatie over uw abonnement en uw Bitdefender-account.

Wanneer u wilt inloggen op een andere Bitdefender-account, klikt u op de knop **Andere account**, typt u het nieuwe e-mailadres en wachtwoord in het programmavenster van Bitdefender-account en klikt u op **Aanmelden**.

4.3. Beschermingsvoorkeuren

In het venster Beschermingsvoorkeuren kunt u de instellingen voor de malwarescans aanpassen. Naast enkele algemene instellingen kunt u ook instellen wat er moet gebeuren met geïnfecteerde of verdachte bestanden.

Beschermingsvoorkeuren

- **Actie voor geïnfecteerde bestanden.** Wanneer een virus of andere malware wordt gedetecteerd, zal Bitdefender Antivirus for Mac automatisch proberen de malwarecode te verwijderen uit het geïnfecteerde bestand en het originele bestand reconstrueren. Deze bewerking wordt een desinfectie genoemd. Bestanden die niet kunnen worden gedesinfecteerd, worden in quarantaine geplaatst om verdere besmetting te voorkomen.

  U kunt ook instellen dat er geen actie moet worden ondernomen op geïnfecteerde bestanden, maar deze instelling wordt niet aanbevolen. Als u toch voor deze instelling kiest, worden gedetecteerde bestanden alleen vermeld in het logbestand.

  De functie Autopilot zorgt voor een gedegen bescherming tegen malware, zonder dat de systeemprestaties merkbaar worden beïnvloed. Als er niet-opgeloste dreigingen zijn, kunt u deze bekijken en besluiten wat u ermee wilt doen.

- **Actie voor verdachte objecten.** De bestanden worden gedetecteerd als verdacht door de heuristische analyse. Verdachte bestanden kunnen niet worden gedesinfecteerd omdat er geen desinfectieroutine beschikbaar is.

  De standaardinstelling is dat verdachte bestanden in quarantaine worden geplaatst. Wanneer het virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

  U kunt er desgewenst ook voor kiezen verdachte bestanden te negeren. Als u toch voor deze instelling kiest, worden gedetecteerde bestanden alleen vermeld in het logbestand.

- **Alleen nieuwe en gewijzigde bestanden scannen.** Selecteer dit aankruisvak als u wilt dat Bitdefender Antivirus for Mac alleen bestanden scant die nog niet eerder zijn gescand of die sinds de laatste scan zijn gewijzigd.

  Als u wilt, kunt u deze instelling negeren voor scans die worden gestart door middel van slepen en neerzetten. Selecteer hiervoor het desbetreffende aankruisvak.

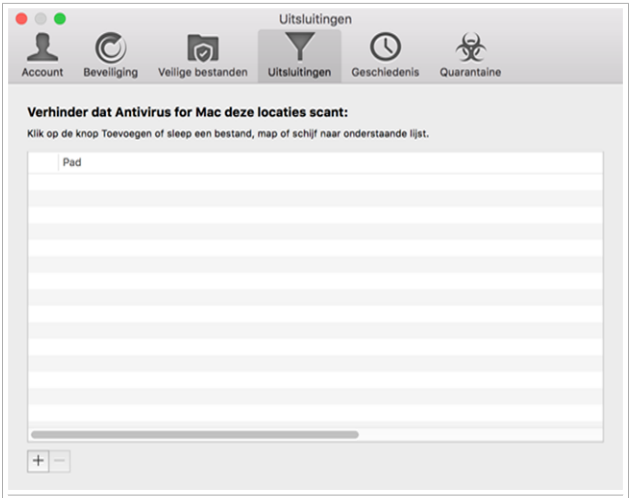
- **Inhoud in back-ups niet scannen.** Selecteer dit aankruisvak als u niet wilt dat backup-bestanden worden gescand. Als een geïnfecteerd backup-bestand later wordt teruggezet, wordt dit automatisch door Bitdefender Antivirus for Mac gedetecteerd en zal de juiste actie worden ondernomen.

- **Bescherming Time Machine.** Selecteer dit selectievakje om de bestanden in Time Machine te beveiligen. Mochten deze bestanden ooit worden gegijzeld door ransomware, kunt u ze vanaf uw Time Machine-schijf herstellen zonder losgeld te betalen.

4.3.1. Uitsluitingen scannen

Als u wilt, kunt u instellen dat Bitdefender Antivirus for Mac bepaalde bestanden, mappen of zelfs complete volumes overslaat bij het scannen. U kunt bijvoorbeeld de volgende objecten uitsluiten van het scannen:

- Bestanden die tijdens een scan ten onrechte als 'geïnfecteerd' worden aangemerkt (zogeheten fout-positieven)
- Bestanden die fouten veroorzaken tijdens het scannen
- Backup-volumes



Uitsluitingen scannen

De lijst Uitsluitingen bevat de paden die zijn uitgesloten van het scanproces.

U kunt een uitsluiting op twee manieren instellen:

- Sleep een bestand, map of volume naar de lijst Uitsluitingen.
- Klik onder de lijst Uitsluitingen op de knop met het plusteken (+). Selecteer vervolgens het bestand, de map of het volume dat u van het scannen wilt uitsluiten.

Als u een uitsluiting uit de lijst wilt verwijderen, klikt u onder de lijst Uitsluitingen op de knop met het minteken (-).

4.4. Veilige bestanden

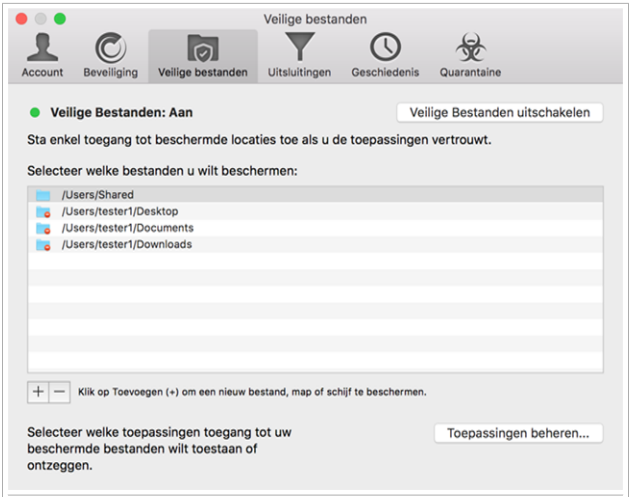
Ransomoware is een schadelijke software die kwestbare systemen aanvalt door ze te vergrendelen en later om geld te vragen zodat de gebruiker terug de controle over zijn systeem te krijgen. Deze schadelijke software handelt op een intelligente manier door valse berichten weer te geven zodat de gebruiker panikeert, om hem aan te sporen om de gevraagde betaling uit te voeren.

Gebruik makend van de recentste technologie garandeert Bitdefender systeemintegriteit door kritieke systeemgebieden te beschermen tegen ransomwareaanvallen zonder het systeem te belasten. Mogelijks wilt u echter

ook uw persoonlijke bestanden beschermen, zoals documenten, foto's of films tegen ongeoorloofde toegang door onbetrouwbare apps. Met Bitdefender Veilige bestanden kunt u persoonlijke bestanden op een veilige plek bewaren en zelf configureren welke apps toestemming mogen krijgen om wijzigingen aan te brengen in de beschermde bestanden en welke niet.

Wizard Veilige bestanden

De wizard Veilige bestanden van Bitdefender verschijnt zodra u Bitdefender Antivirus for Mac op uw Macintosh installeert. Selecteer of voeg nieuwe locaties toe die u wilt beschermen en klik daarna op **Veilige bestanden activeren**.



Veilige bestanden

Er zijn twee manieren om achteraf bestanden toe te voegen aan de beschermde omgeving:

- Sleep een bestand, map of volume naar het venster Veilige bestanden.
- Klik op de knop met het +-teken (+) onder de lijst beschermde bestanden. Kies vervolgens het bestand, de map of het volume dat beschermd moet worden indien tijdens ransomware-aanvallen wordt getracht ze te openen.

Om vertragingen in het systeem te voorkomen, bevelen we u aan om maximaal 30 mappen toe te voegen of om meerdere bestanden in een map op te slaan.

Standaard worden de mappen Afbeeldingen, Documenten, Bureaublad en Downloads beschermd tegen bedreigingsaanvallen.

Opmerking

Aangepaste mappen kunnen enkel beschermd worden voor huidige gebruikers. Externe schijven, systemen en toepassingsbestanden kunnen niet worden toegevoegd aan de beschermingsomgeving.

Telkens wanneer een ongekend app met een verdacht gedrag probeert om de bestanden die u hebt toegevoegd, te wijzigen, zult u een melding

ontvangen. Klik op **Toestaan** of **Blokkeren** en voeg toe aan de lijst Toepassingen beheren.

4.4.1. Toepassingen beheren

De toepassingen die proberen om beschermde bestanden te wijzigen of te verwijderen kunnen als potentieel onveilig worden aangemerkt en worden toegevoegd aan de lijst met Geblokkeerde toepassingen. Indien een dergelijke toepassing wordt geblokkeerd en u zeker bent dat het gedrag normaal is, kunt u het toestemming geven door te klikken op de knop **Toepassingen beheren** en vervolgens de status te wijzigen naar Toestaan.

Apps die als Toestaan ingesteld zijn, kunnen ook Geblokkeerd worden.

Gebruik de versleepmethode of klik op het +-teken (+) om meer apps aan de lijst toe te voegen.

4.5. Geschiedenis

Bitdefender houdt een uitgebreid logbestand bij over de activiteiten op uw computer. Zodra er iets gebeurt dat van belang is voor de beveiliging van uw systeem en uw gegevens, wordt een nieuw bericht toegevoegd aan de Geschiedenis van Bitdefender Antivirus for Mac, op een manier die te vergelijken is met een nieuwe e-mail die aan uw inkomende postbus wordt toegevoegd.

Gebeurtenissen zijn een zeer belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging. U kunt bijvoorbeeld heel gemakkelijk zien of de laatste update is geslaagd, of er malware op uw computer is aangetroffen en of een onbevoegde applicatie heeft geprobeerd uw Time Machine-schijf te openen.

Er worden gegevens over de activiteiten van het product weergegeven.

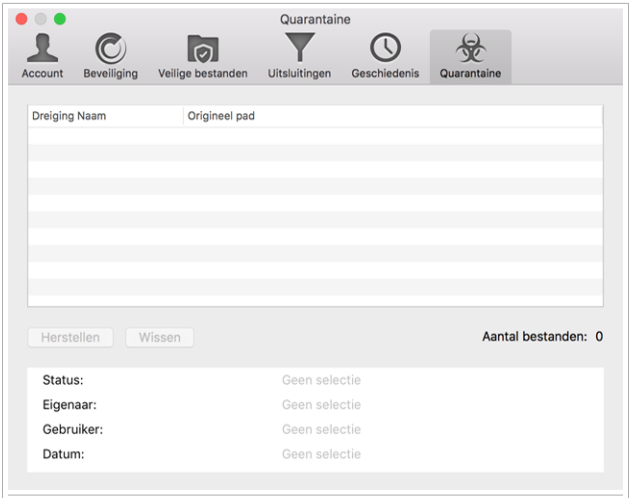
Geschiedenis

Als u het logbestand wilt wissen, klikt u op de knop **Geschiedenis wissen**.

Met de knop **Kopiëren** kunt u de weergegeven informatie naar het klembord kopiëren.

4.6. Quarantaine

Bitdefender Antivirus for Mac biedt u de mogelijkheid geïnfecteerde of verdachte bestanden te isoleren in een beveiligd gebied, de quarantaine. Wanneer het virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.



Bestanden in quarantaine

In de quarantainesectie ziet u alle bestanden die op dit moment zijn geïsoleerd in de quarantainemap.

Als u een bestand uit de quarantaine wilt verwijderen, selecteert u het bestand en klikt u op **Verwijderen**. Als u een bestand uit quarantaine wilt terugzetten op zijn oorspronkelijke locatie, selecteert u het en klikt u op **Herstellen**.

5. VPN

Dit hoofdstuk bevat de volgende onderwerpen:

- *Over VPN* (p. 30)
- *VPN Installeren* (p. 30)
- *VPN Openen* (p. 31)
- *Interface* (p. 31)
- *Abonnementen* (p. 33)

5.1. Over VPN

Met Bitdefender VPN houdt u uw data privé telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. Zo vermijdt u onfortuinlijke situaties, bijvoorbeeld diefstal van persoonlijke gegevens of pogingen om het IP-adres van uw apparaat toegankelijk te maken voor hackers.

De VPN werkt zoals een tunnel tussen uw apparaat en het netwerk waarmee u verbindt: de VPN beveiligt die verbinding, door aan de hand van versleuteling volgens bankrichtlijnen de gegevens te versleutelen en door uw IP-adres te verbergen, waar u ook bent. Uw dataverkeer wordt omgeleid via een andere server, waardoor het praktisch onmogelijk wordt om uw apparaat te identificeren tussen de talloze andere toestellen die gebruikmaken van onze diensten. Wanneer u via Bitdefender VPN verbonden bent met het internet kunt u bovendien inhoud bekijken die normaal afgeschermd wordt in bepaalde gebieden.

Opmerking

Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de app Bitdefender VPN voor het eerst probeert te gebruiken. Door het gebruik van de app verder te zetten, bevestigt u dat u op de hoogte bent van de toepasselijke reguleringen van het land en van de risico's die u mogelijk loopt.

5.2. VPN Installeren

De VNP-app kan vanuit het hoofdvenster van Bitdefender als volgt worden geïnstalleerd:

1. Bitdefender Antivirus for Mac openen.
2. Klik in de linkerbenedenhoek op **Nu installeren**.
3. In het venster met de beschrijving van de VPN-app kunt u de **Licentieovereenkomst** lezen. Klik vervolgens op **VPN Installeren**. Als u niet akkoord gaat met deze voorwaarden, klik dan op **Later** om de installatie te annuleren.
4. Klik op **Begrepen** om de installatieprocedure af te ronden.

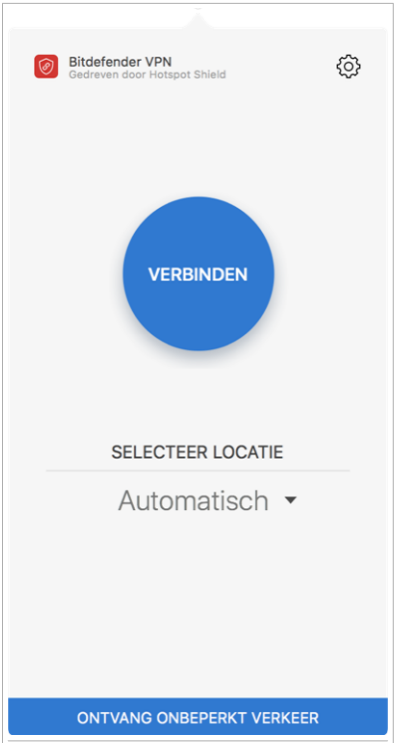
5.3. VPN Openen

Om de app Bitdefender VPN te openen, klikt u op de icoon in de menubalk. Of u kunt naar de map Toepassingen gaan, de map Bitdefender openen en vervolgens dubbelklikken op de icoon Bitdefender VPN.

5.4. Interface

De VPN-interface geeft de status van de app weer: verbonden of niet verbonden. Voor gebruikers met een gratis versie kiest Bitdefender automatisch de meest geschikte server. Premium-gebruikers kunnen zelf de locatie van de server wijzigen door de juiste server te kiezen uit de lijst **KIES LOCATIE**. Voor details over VPN-abonnementen, raadpleeg *Abonnementen* (p. 33).

Om te verbinden of om de verbinding te verbreken, klik op de status bovenaan op het scherm. De icoon in de menubalk is zwart wanneer de VPN verbonden is, en wit wanneer deze niet verbonden is.



VPN-interface

Tijdens de verbinding wordt de verstreken tijd weergegeven op onderste gedeelte van de interface. Voor meer opties, klik op de icoon ⚙ aan de rechterbovenkant:

- **Mijn Account** - gegevens over uw Bitdefender-account en VPN-abonnement worden weergegeven. Klik op **Account Wisselen** indien u met een andere account wenst in te loggen.
- **Instellingen** - u kunt het gedrag van uw product aanpassen naargelang uw noden:
  - stel de VPN in om op te starten wanneer het systeem opgestart wordt
  - ontvang notificaties wanneer de VPN automatisch verbindt of de verbinding verbreekt

- **Upgrade naar Premium** - indien u een gratis versie van het product gebruikt, kunt u hier upgraden naar premium. Klik op **NU UPGRADEN** om naar een webpagina te gaan waar u een abonnement kunt aankopen.
- **Ondersteuning** - u wordt doorgestuurd naar ons platform Ondersteuningscentrum, waar u een nuttig artikel kunt lezen over hoe u Bitdefender VPN gebruikt.
- **Over deze versie** - informatie over de geïnstalleerde versie.
- **Afsluiten** - verlaat de toepassing.

5.5. Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om uw verbinding te beveiligen telkens u dit nodig hebt, en verbindt bovendien automatisch met de beste serverlocatie.

Upgrade naar de premium-versie voor onbeperkt dataverkeer en toegang tot afgeschermde inhoud overal ter wereld, doordat u de serverlocatie naar wens kunt selecteren.

U kunt op elk ogenblik upgraden naar de Bitdefender Premium VPN-versie door te klikken op de knop **ONTVANG ONBEPERKT DATAVERKEER** in de productinterface.

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het abonnement voor Bitdefender Antivirus for Mac: u kunt het dus gedurende de hele geldigheid ervan gebruiken, onafhankelijk van de status van het antivirusabonnement. Indien het BitdefenderPremium VPN-abonnement vervalt, maar als het abonnement voor Bitdefender Antivirus for Mac nog actief is, gaat u terug naar de gratis versie.

6. BITDEFENDER CENTRAL

Dit hoofdstuk bevat de volgende onderwerpen:

- *Over Bitdefender Central* (p. 34)
- *Mijn Abonnementen* (p. 35)
- *Mijn Apparaten* (p. 36)

6.1. Over Bitdefender Central

Bitdefender Central is het webplatform waar u toegang hebt tot de online functies en diensten van het product en waar u van op afstand belantrijke taken kunt uitvoeren op toestellen waar Bitdefender op geïnstalleerd is. U kunt zich aanmelden bij uw Bitdefender-account vanaf elke computer en elk mobiel toestel dat met het internet verbinden is als u naar https://central.bitdefender.com gaat. Zodra u toegang hebt, kunt u beginnen met het volgende:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:
  - Bitdefender Antivirus for Mac
  - De Bitdefender-productlijn voor Windows
  - Bitdefender Mobile Security voor Android
  - Bitdefender Mobile Security voor iOS
  - Bitdefender Parental Advisor
- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Nieuwe toestellen aan uw netwerk toevoegen en ze beheren, waar u ook bent.

6.2. Naar Bitdefender Central gaan

Er bestaan verschillende manieren om naar Bitdefender Central te gaan. Afhankelijk van de taak die u wilt uitvoeren, kunt een van de volgende mogelijkheden gebruiken:

- Vanuit de Bitdefender Antivirus for Mac-hoofdinterface:

1. Klik rechtsonder in het scherm op de koppeling **Ga naar uw account**.

- Vanuit uw internetbrowser:

  1. Open een internetbrowser op een willekeurig toestel met toegang tot het internet.
  2. Ga naar: https://central.bitdefender.com.
  3. Log in op uw account met uw e-mailadres en wachtwoord.

6.3. Mijn Abonnementen

Via Bitdefender Central beheert u heel eenvoudig de abonnementen die u voor uw apparaten hebt aangeschaft.

6.3.1. Abonnement activeren

U kunt een abonnement tijdens het installatieproces activeren via uw Bitdefender-account. De geldigheidsduur van het abonnement begint te lopen vanaf het moment van activering.

Als u een activeringscode hebt ontvangen van een van onze leveranciers, of als u een activeringscode cadeau hebt gekregen, kunt u deze toevoegen aan uw Bitdefender-abonnement.

Om een abonnement te activeren via een activeringscode, volgt u de volgende stappen:

1. Ga naar Bitdefender Central.
2. Klik linksboven in het venster op het symbool ☰ en selecteer vervolgens het paneel **Mijn abonnementen**.
3. Klik op de **ACTIVERINGSCODE**-knop en tik vervolgens de code in het overeenkomstige veld in.
4. Klik op **ACTIVERINGSCODE** om door te gaan.

Het abonnement is nu geactiveerd.

Zie *Bitdefender Antivirus for Mac installeren* (p. 1) voor informatie over het installeren van het product op uw apparaten.

6.3.2. Abonnement kopen

U kunt rechtstreeks vanuit uw Bitdefender-account een abonnement aanschaffen door deze stappen te volgen:

1. Ga naar Bitdefender Central.
2. Klik linksboven in het venster op het symbool ☰ en selecteer vervolgens het paneel **Mijn abonnementen**.
3. Klik op de koppeling **Nu kopen**. U wordt doorgestuurd naar een webpagina, waar u de aanschaf kunt afronden.

Zodra u de procedure hebt voltooid, wordt de aanwezigheid van het abonnement rechtsonder in het hoofdvenster van het programma weergegeven.

6.4. Mijn Apparaten

Vanaf **Mijn apparaten** in uw Bitdefender-account kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en die verbinding hebben met het internet. De apparaatkaarten geven de naam en de beveiligingsstatus van het apparaat weer en geven weer of er beveiligingsrisico's zijn die de bescherming van uw apparaten beïnvloeden.

6.4.1. Uw apparaten aanpassen

Om uw toestellen makkelijk te identificeren, kunt u de naam van het toestel aanpassen:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. Voer een nieuwe naam in het veld **Naam apparaat** in en klik op **OPSLAAN**.

U kunt een eigenaar aanmaken en toekennen aan elk van uw toestellen, om het beheer te vergemakkelijken:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.

4. Selecteer **Profiel**.
5. Klik op **Eigenaar toevoegen** en vul de bijbehorende velden in. Pas het profiel aan: voeg een foto toe, selecteer een geboortedatum en voeg een e-mailadres en geboortedatum toe.
6. Klik op **TOEVOEGEN** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de **Apparaateigenaar**-lijst en klik op **TOEKENNEN**.

6.4.2. Beheer op afstand

Bitdefender van op afstand op een apparaat updaten:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Update**.

Om de functie Autopiloot vanop afstand in te schakelen:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**. Klik vervolgens op de desbetreffende schakelaar om Autopilot in te schakelen.

Zodra u op een toestelkaart klikt, zijn de volgene tabbladen beschikbaar:

- **Dashboard**. In dit venster kunt u de gegevens van het geselecteerde apparaat bekijken, de beschermingsstatus en nakijken hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus is altijd groen (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Wanneer er problemen zijn met uw apparaat, klik dan op het uitklappijltje in het bovenste statusgebied voor meer details. Hier kunt u de problemen die de beveiliging van uw apparaat beïnvloeden handmatig herstellen.

- **Bescherming**. In dit tabblad kunt u op afstand een Snelle scan of een Volledige scan uitvoeren op uw apparaten. Klik op de knop **Scan** om de scan te starten. U kunt ook zien wanneer de laatste scan op het apparaat is uitgevoerd en er is een rapport beschikbaar met de belangrijkste gegevens van de laatste scan. Zie *Uw Mac scannen* (p. 12) voor meer informatie over deze twee scanprocessen.

7. VEELGESTELDE VRAGEN

Hoe kan ik Bitdefender Antivirus for Mac uitproberen voordat ik een abonnement neem?

Als nieuwe klant van Bitdefender kunt u ons product uitproberen voordat u tot aanschaf overgaat. De proefperiode duurt 30 dagen. Na die tijd kunt u het geïnstalleerde product alleen blijven gebruiken als u een Bitdefender-abonnement neemt. Om Bitdefender Antivirus for Mac vrijblijvend uit te proberen, doet u het volgende:

1. Volg de onderstaande stappen om een Bitdefender-account aan te maken:
   - Ga naar: https://central.bitdefender.com.
   - Voer de vereiste informatie in de overeenkomstige velden in en klik op de **ACCOUNT AANMAKEN**-knop.

     De gegevens die u hier opgeeft blijven vertrouwelijk.
2. Volg de onderstaande stappen om Bitdefender Antivirus for Mac te downloaden:
   - Selecteer het paneel **Apparaten** en klik dan op **LOKALE BESCHERMING INSTALLEREN**.
   - Kies een van de twee beschikbare opties:
     - **DOWNLOADEN**

       Klik op de knop en sla het installatiebestand op.
     - **Op een ander apparaat**

       Selecteer **macOS** om uw Bitdefender-product te downloaden en klik vervolgens op **Doorgaan**. Typ een e-mailadres in het e-mailveld en klik op **Verzenden**.
   - Start het gedownloade Bitdefender-programma.

Ik heb een activeringscode. Hoe kan ik deze aan mijn abonnement toevoegen?

Als u een activeringscode hebt ontvangen van een van onze leveranciers, of als u een activeringscode cadeau hebt gekregen, kunt u deze toevoegen aan uw Bitdefender-abonnement.

Om een abonnement te activeren via een activeringscode, volgt u de volgende stappen:

1. Ga naar Bitdefender Central.
2. Klik linksboven in het venster op het symbool ☰ en selecteer vervolgens het paneel **Mijn abonnementen**.
3. Klik op de **ACTIVERINGSCODE**-knop en tik vervolgens de code in het overeenkomstige veld in.
4. Klik opnieuw op de knop **ACTIVATIECODE**.

De nieuwe geldigheidsduur is nu zichtbaar in uw Bitdefender-account en rechtsonder in het scherm van Bitdefender Antivirus for Mac.

Volgens het scanlog zijn er nog niet-opgeloste problemen. Hoe kan ik deze problemen oplossen?

De niet-opgeloste problemen kunnen betrekking hebben op:

- Archieven met beperkte toegang (bijvoorbeeld xar of rar)

  Oplossing: gebruik de functie **Tonen in Finder** om naar het bestand te gaan en dit handmatig te verwijderen. Vergeet niet ook de Prullenmand leeg te maken.

- Postbussen met beperkte toegang (bijvoorbeeld Thunderbird)

  Oplossing: gebruik het desbetreffende mailprogramma om het item met het geïnfecteerde bestand te verwijderen.

- Inhoud in backups

  Oplossing: selecteer de optie **Inhoud in back-ups niet scannen** bij Beschermingsvoorkeuren of kies **Toevoegen aan uitsluitingen** om de gedetecteerde bestanden uit te sluiten van de scans.

  Als een geïnfecteerd backup-bestand later wordt teruggezet, wordt dit automatisch door Bitdefender Antivirus for Mac gedetecteerd en zal de juiste actie worden ondernomen.

> **Opmerking**
> Bestanden "met beperkte toegang": dit betekent dat Bitdefender Antivirus for Mac de bestanden wel kan openen, maar niet mag wijzigen.

Waar kan ik informatie opvragen over de activiteiten van het product?

Bitdefender houdt een logbestand bij van alle belangrijke acties, statuswijzigingen en berichten over de activiteiten van het product. Om deze informatie weer te geven, opent u het voorkeurenvenster van Bitdefender Antivirus for Mac:

1. Bitdefender Antivirus for Mac openen.
2. Voer een van de volgende bewerkingen uit:
   - Klik in de menubalk op Bitdefender Antivirus for Mac en kies **Voorkeuren**.
   - Klik in de menubalk op en kies **Voorkeuren**.
   - Druk op Command+komma (,).
3. Klik op het tabblad **Geschiedenis**.

   Er worden gegevens over de activiteiten van het product weergegeven.

Kan ik Bitdefender Antivirus for Mac bijwerken via een proxyserver?

Bitdefender Antivirus for Mac kan alleen updates downloaden via een proxyserver die géén authenticatie vereist. U hoeft hiervoor verder geen programma-instellingen te wijzigen.

Als u normaal gesproken verbinding met het internet maakt via een proxyserver die wél authenticatie vereist, moet u regelmatig overschakelen naar een rechtstreekse internetverbinding om te zorgen dat u updates van malwarehandtekeningen kunt ontvangen.

Hoe kan ik Bitdefender Antivirus for Mac verwijderen?

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster ga naar de map Programma's en kies Hulpprogramma's.
2. Dubbelklik op het programma Bitdefender verwijdertool om dit programma te starten.
3. Klik op **Verwijderen** om door te gaan.
4. Wacht tot de verwijderingsprocedure gereed is en klik ten slotte op **Sluiten**.

> **Belangrijk**
> Als er problemen optreden, kunt u contact opnemen met Bitdefender Klantenondersteuning volgens de aanwijzingen in *Ondersteuning* (p. 44).

Hoe kan ik de TrafficLight-extensies uit mijn webbrowser verwijderen?

- Zo verwijdert u de TrafficLight-extensies uit Mozilla Firefox:

  1. Open Mozilla Firefox.

2. Ga naar **Extra** en selecteer **Add-ons**.
3. Selecteer **Extensies** in de linkerkolom.
4. Selecteer de extensie en klik op **Verwijderen**.
5. Start de browser opnieuw om de verwijdering te voltooien.

- Zo verwijdert u de TrafficLight-extensies uit Google Chrome:
  1. Open Google Chrome.
  2. Klik rechtsboven op **Meer** .
  3. Ga naar **Extra** en selecteer **Extensies**.
  4. Klik naast de extensie die u wenst te verwijderen op de icoon **Verwijderen uit Chrome...** .
  5. Klik op **Verwijderen** om de verwijdering te bevestigen.
- Zo verwijdert u Bitdefender TrafficLight uit Safari:
  1. Open Safari.
  2. Klik in de werkbalk op en kies **Voorkeuren**.
  3. Selecteer het tabblad **Extensies** en ga in de lijst naar **Bitdefender TrafficLight on Safari**.
  4. Selecteer de extensie en klik op **Verwijderen**.
  5. Klik op **Verwijderen** om de verwijdering te bevestigen.

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om ervoor te zorgen dat u beveiligd bent wanneer u surft op het internet, raden we aan dat u Bitdefender VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht of u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

Zal Bitdefender VPN een negatief effect hebben op de batterij van mijn apparaat?

Bitdefender VPN werd ontworpen om uw persoonlijke gegevens te beschermen, om uw IP-adres te verbergen wanneer u verbonden bent met onbeveiligde draadloze netwerken en om afgeschermde inhoud te bekijken in bepaalde landen. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

Waarom is het internet soms trager wanneer ik verbonden ben met Bitdefender VPN?

Bitdefender VPN is ontworpen om u een aangename ervaring te bieden tijdens het surfen. Uw internetconnectiviteit of de afstand met de server waarmee u verbonden bent, kan echter zorgen voor vertraging. In dat geval, indien het niet noodzakelijk is om te verbinden met een server die veraf gehost wordt (bijv. van China naar de VS), raden we aan Bitdefender VPN toe te staan om u automatisch te verbinden met de dichtstbijzijnde server, of een server te vinden die dichter bij uw huidige locatie gelegen is.

8. HULP VRAGEN

Dit hoofdstuk bevat de volgende onderwerpen:

- *Ondersteuning* (p. 44)
- *Contactinformatie* (p. 46)

8.1. Ondersteuning

Bitdefender streeft ernaar haar klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning te bieden. Als u problemen ondervindt met of vragen hebt over uw Bitdefender-product, kunt u meerdere online bronnen gebruiken om snel een oplossing of antwoord te vinden. Als u dat wenst, kunt u ook contact opnemen met de Bitdefender-klantenservice. Onze medewerkers van de ondersteuningsdienst zullen uw vragen snel beantwoorden en u alle hulp bieden die u nodig hebt.

8.1.1. Online bronnen

Er zijn meerdere online bronnen beschikbaar om u te helpen bij het oplossen van uw problemen en vragen met betrekking tot Bitdefender.

- Bitdefender-Ondersteuningscentrum:

  https://www.bitdefender.com/support/consumer.html

- Bitdefender Ondersteuningsforum:

  http://forum.bitdefender.com

- het HOTforSecurity-portaal voor computerbeveiliging:

  http://www.hotforsecurity.com

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

Bitdefender-Ondersteuningscentrum

Het Bitdefender-ondersteuningscentrum is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer

algemene artikels over viruspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

Het Bitdefender-ondersteuningscentrum is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog een middel om Bitdefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van Bitdefender-klanten komen, vinden uiteindelijk hun weg naar het Bitdefender-ondersteuningscentrum, als rapporten over het oplossen van problemen, "spiekbriefjes" om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Ondersteuningscentrum is 24 uur per dag toegankelijk via dit adres: https://www.bitdefender.com/support/consumer.html.

Bitdefender Ondersteuningsforum

Het Bitdefender-ondersteuningsforum biedt Bitdefender-gebruikers een eenvoudige manier om hulp te krijgen en anderen te helpen. U kunt uw problemen of vragen in verband met uw Bitdefender-producten op het forum posten.

Bitdefender-ondersteuningstechnici controleren het forum en plaatsen nieuwe informatie om u te helpen. U kunt ook een antwoord of oplossing krijgen van een meer ervaren Bitdefender-gebruiker.

Voordat u uw probleem of vraag verzendt, moet u op het forum zoeken of er geen soortgelijk of verwant onderwerp is.

Het Bitdefender-ondersteuningsforum is beschikbaar op http://forum.bitdefender.com in 5 verschillende talen: Engels, Duits, Frans, Spaans en Roemeens. Klik op de koppeling **Home & Home Office Protection** om toegang te krijgen tot het gebied voor verbruiksproducten.

HOTforSecurity-portaal

Het HOTforSecurity-portaal is een rijke bron aan informatie over de computerbeveiliging. Hier leert u meer over de verschillende bedreigingen waaraan uw computer wordt blootgesteld wanneer u verbinding met internet maakt (malware, phishing, spam, cybercriminelen). Een handige woordenlijst helpt u om de termen van computerbeveiliging die u niet goed kent te begrijpen.

Er worden regelmatig nieuwe artikels gepubliceerd om u op de hoogte te houden van de recentst opgespoorde bedreigingen, de huidige beveiligingstrends en andere informatie over de sector van computerbeveiliging.

De webpagina van HOTforSecurity is http://www.hotforsecurity.com.

8.1.2. Hulp inroepen

U kunt onze hulp inroepen via het online Ondersteuningscentrum:

1. Ga naar https://www.bitdefender.com/support/consumer.html.
2. Zoek eerst in het Ondersteuningscentrum naar artikelen die mogelijk een oplossing voor uw probleem bevatten.
3. Lees de relevante artikels of documenten en probeer de voorgestelde oplossingen.
4. Als u geen werkende oplossing hebt kunnen vinden, klikt u onder in het venster op **Neem contact op**.
5. Gebruik het contactformulier om een e-mailticket te openen of op een andere manier contact op te nemen.

8.2. Contactinformatie

Efficiënte communicatie is de sleutel tot succes. BITDEFENDER heeft sinds 2001 een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners steeds opnieuw te overtreffen. Aarzel daarom niet om contact op te nemen indien u vragen hebt.

8.2.1. Webadressen

Verkoopsafdeling: sales@bitdefender.com
Ondersteuningscentrum:https://www.bitdefender.com/support/consumer.html
Documentatie: documentation@bitdefender.com
Lokale verdelers:https://www.bitdefender.com/partners
Partnerprogramma: partners@bitdefender.com
Perscontact: pr@bitdefender.com
Jobs: jobs@bitdefender.com
Virusverzendingen: virus_submission@bitdefender.com
Spamverzendingen: spam_submission@bitdefender.com

Misbruikmeldingen: abuse@bitdefender.com
Website:https://www.bitdefender.com

8.2.2. Lokale verdelers

De lokale Bitdefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Een Bitdefender-verdeler in uw land zoeken:

1. Ga naar https://www.bitdefender.com/partners.
2. Ga naar **Partnerzoeker**.
3. De contactgegevens van de lokale Bitdefender-verdelers zouden automatisch moeten verschijnen. Als dat niet gebeurt, selecteert u het land waarin u zich bevindt om de informatie weer te geven.
4. Als u geen Bitdefender-distributeur in uw land kunt vinden, kunt u via e-mail rechtstreeks contact met ons opnemen via sales@bitdefender.com. Noteer uw e-mail in het Engels zodat wij u onmiddellijk kunnen helpen.

8.2.3. Bitdefender-kantoren

De Bitdefender-kantoren zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak. Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

V.S.

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefoon (kantoor&verkoop): 1-954-776-6262
Verkoop: sales@bitdefender.com
Technische ondersteuning: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Verenigde Arabische Emiraten

Dubai Internet City

Building 17, Office # 160
Dubai, UAE
Telefoon verkoop: 00971-4-4588935 / 00971-4-4589186
E-mail verkoop: mena-sales@bitdefender.com
Technische ondersteuning: https://www.bitdefender.com/support/consumer.html
Website: https://www.bitdefender.com

Duitsland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Kantoor: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Verkoop: vertrieb@bitdefender.de
Technische ondersteuning: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Spanje

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefoon: +34 902 19 07 65
Verkoop: comercial@bitdefender.es
Technische ondersteuning: https://www.bitdefender.es/support/consumer.html
Website: https://www.bitdefender.es

Roemenië

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefoon verkoop: +40 21 2063470
E-mail verkoop: sales@bitdefender.ro

Technische ondersteuning: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Soorten malware (schadelijke software)

Adware

Adware wordt vaak gecombineerd met een hostapplicatie die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adwareprogramma's doorgaans worden geïnstalleerd nadat de gebruiker een licentie- of abonnementsovereenkomst heeft geaccepteerd die het doel van het programma vermeldt, worden er geen wetten overtreden.

Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentie- of abonnementsovereenkomst.

Keylogger

Een keylogger is een toepassing die alles wat u typt registreert.

Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Polymorf virus

Een virus dat zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien zij geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

Ransomware

Ransomware is kwaadaardige software waarmee criminelen proberen geld af te persen van gebruikers, door hun systemen ontoegankelijk te maken totdat er losgeld is betaald. Enkele van de vele varianten van ransomware voor persoonlijke computersystemen zijn CryptoLocker, CryptoWall en TeslaWall.

De infectie kan verspreid worden door spam-email te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de

gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rootkit

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met malware, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is geïnstalleerd, worden de activiteiten van de gebruiker op het Internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Net als Trojaanse paarden worden spywareprogramma's meestal ongemerkt geïnstalleerd terwijl een gebruiker probeert een ander product te installeren. Besmettingen met spyware ontstaan vaak door het downloaden van P2P-programma's voor bestandsuitwisseling.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeembronnen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot virussen, maken ze geen kopie van zichzelf, maar ze kunnen wel even vernietigend zijn. Een van de meest verraderlijke types van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van virussen, maar dat in werkelijkheid virussen op uw computer installeert.

De term komt uit een verhaal uit de Illias van Homerus, dat vertelt over de Grieken die hun vijanden, de Trojanen een reusachtig houten paard schonken, zogenaamd als een vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten, die in de holle romp van het paard verborgen zaten te voorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Virus

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste virussen kunnen zichzelf ook dupliceren. Alle computervirussen zijn door de mens gemaakt. Een eenvoudig virus dat zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudig virus is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren; Een nog gevaarlijker type is een virus dat in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.