Bitdefender®
ANTIVIRUS FOR MAC

HANDLEIDING

Mac

Bitdefender Antivirus for Mac
Handleiding

Publication date 2020.07.19

Kennisgevingen

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. Opmerkingen 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 starten 7
2.3. Hoofdvenster Toepassing 8
2.4. Dock-symbool toepassing 9
2.5. Navigatiemenu 10
2.6. Donkere modus 10

3. Bescherming tegen schadelijke software 12
3.1. Aanbevelingen 12
3.2. Uw Mac scannen 13
3.3. Scanwizard 14
3.4. Quarantaine 15
3.5. Bitdefender Shield (realtime bescherming) 16
3.6. Uitzonderingen scannen 16
3.7. Webbescherming 17
3.8. Anti-tracker 19
3.8.1. Interface van Anti-tracker 20
3.8.2. Uitschakelen van de Bitdefender Anti-tracker 21
3.8.3. Toestaan dat een website aan tracking doet 21
3.9. Veilige Bestanden 21
3.9.1. Toegang toepassingen 22
3.10. Bescherming Time Machine 23
3.11. Problemen oplossen 24
3.12. Notificaties 25
3.13. Updates 26
3.13.1. Zelf een update uitvoeren 26
3.13.2. Updates downloaden via een proxyserver 27
3.13.3. Productupdates 27
3.13.4. Informatie over Bitdefender Antivirus for Mac vinden 27

4. VPN 28
4.1. Over VPN 28
4.2. VPN Openen 28

4.3. Interface ... 29
4.4. Abonnementen ... 31
5. Voorkeuren instellen ... 32
5.1. Voorkeuren weergeven ... 32
5.2. Beschermingsvoorkeuren ... 32
5.3. Geavanceerde voorkeuren ... 33
5.4. Speciale aanbieding ... 33
6. Bitdefender Central ... 34
6.1. Over Bitdefender Central ... 34
6.2. Naar Bitdefender Central gaan ... 35
6.3. Twee-factorenauthenticatie ... 35
6.4. Betrouwbare apparaten toevoegen ... 36
6.5. Activiteit ... 37
6.6. Mijn abonnementen ... 38
6.6.1. Abonnement activeren ... 38
6.7. Mijn apparaten ... 38
6.7.1. Uw apparaten aanpassen ... 39
6.7.2. Beheer op afstand ... 39
7. Veelgestelde vragen ... 41
8. Hulp vragen ... 46
8.1. Ondersteuning ... 46
8.1.1. Online bronnen ... 46
8.1.2. Hulp inroepen ... 48
8.2. Contactinformatie ... 48
8.2.1. Webadressen ... 48
8.2.2. Lokale distributeurs ... 49
8.2.3. Bitdefender-vestigingen ... 49
Soorten malware (schadelijke software) ... 52

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 bedreigingen en andere schadelijke software. zodat u maximaal profijt hebt van Bitdefender.

We wensen u veel leesplezier met deze handleiding.

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. 12)
Bescherm uzelf met Bitdefender Antivirus for Mac tegen schadelijke software en phishing-scams.

Voorkeuren instellen (p. 32)
De voorkeursinstellingen van Bitdefender Antivirus for Mac.

Hulp vragen (p. 46)
Informatie opzoeken en hulp vragen bij onverwachte problemen.

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	Voorbeelden van syntaxis worden weergegeven in een niet-proportioneel lettertype.
https://www.bitdefender.be	URL-koppelingen verwijzen naar een externe locatie (bijvoorbeeld een website of FTP-server).
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Gebruik van deze handleiding (p. v)	Dit is een interne verwijzing naar een paragraaf binnen het document.
filename	Namen van bestanden en mappen worden weergegeven in een niet-proportioneel lettertype.
optie	Alle productopties worden **vet** weergegeven.
sleutelwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

3.2. Opmerkingen

De tekst bevat verschillende soorten opmerkingen, die met een speciaal symbool worden aangegeven om uw aandacht te vestigen op extra informatie.

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 installeren op Macintosh-computers met OS X Yosemite (10.10) of nieuwere versies.

Uw Mac moet ook minstens 1 GB beschikbare ruimte hebben op de harde schijf.

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

Opmerking

Bitdefender Anti-tracker en Bitdefender VPN kunnen enkel op systemen met macOS 10.12 of nieuwere versies geïnstalleerd worden.

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 **Systeemrapport** 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 **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.

5. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Sla het installatiebestand op.
   - **Bescherm andere apparaten**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Klik op **DOWNLOADLINK VERSTUREN**.
     c. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**.

        De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.
     d. Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.
6. Start het gedownloade Bitdefender-programma.
7. Voer de installatiestappen uit.

1.2.1. Installatieprocedure

Zo installeert u Bitdefender Antivirus for Mac:

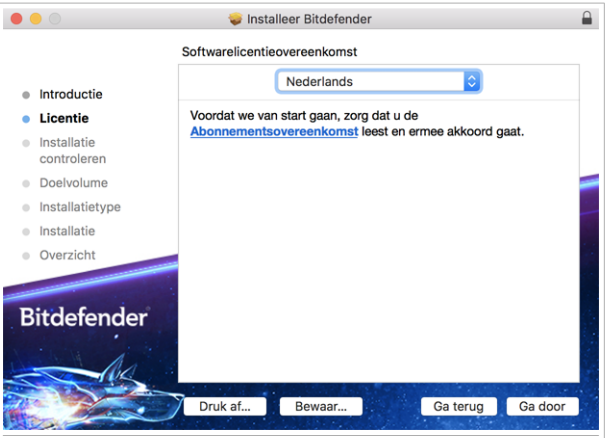
1. Klik op het gedownloade bestand. Hierdoor wordt het installatieprogramma gestart.
2. Volg de stappen van de installatiewizard.

Stap 1 - Welkomstvenster

Welkomstvenster

Klik op **Doorgaan**.

Stap 2 - Abonnementsovereenkomst lezen



Lees de Abonnementsovereenkomst

Voordat u verdergaan met de installatie, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig

door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Antivirus for Mac.

Vanuit dit venster kunt u ook de taal waarin u het product wilt installeren, selecteren.

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.

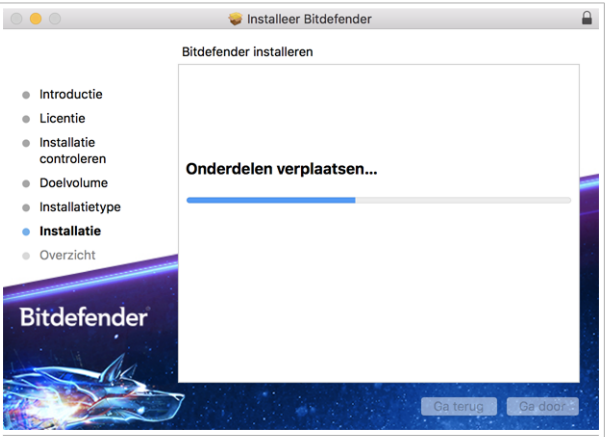
Stap 3 - Installatie starten

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 10.13.0 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. Klik in het onderste gedeelte van het venster op **Toestaan** of selecteer de Bitdefender SRL uit de lijst en klik op **OK**.
- Als u Bitdefender Antivirus for Mac installeert op macOS Mojave 10.14 of een nieuwere versie, verschijnt er een nieuw venster met de informatie het volgende te doen: **Bitdefender Volledige toegang tot de schijf verlenen** en **Toestaan dat Bitdefender laadt**. Volg de instructies op het scherm om het product correct te configureren.

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 en ga naar de map Programma's.
2. Open de Bitdefender-map en dubbelklik op Bitdefender Uninstaller.
3. Klik op **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. 46).

2. AAN DE SLAG

Dit hoofdstuk bevat de volgende onderwerpen:

- *Over Bitdefender Antivirus for Mac* (p. 7)
- *Bitdefender Antivirus for Mac starten* (p. 7)
- *Hoofdvenster Toepassing* (p. 8)
- *Dock-symbool toepassing* (p. 9)
- *Navigatiemenu* (p. 10)
- *Donkere modus* (p. 10)

2.1. Over Bitdefender Antivirus for Mac

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

- ransomware
- adware
- virussen
- spyware
- Trojaanse paarden
- keyloggers
- wormen.

Deze toepassing detecteert en verwijdert niet alleen Mac-bedreigingen, maar ook Windows-bedreigingen. Hierdoor weet u zeker dat u nooit ongemerkt een besmet bestand doorstuurt naar familieleden, vrienden of collega's die een Windows-pc gebruiken.

2.2. Bitdefender Antivirus for Mac starten

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.

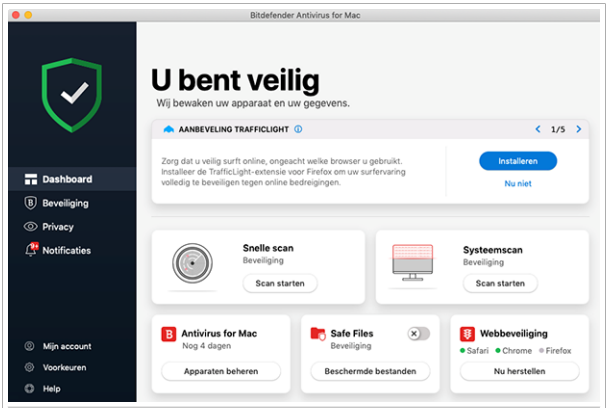
Belangrijk

Wanneer u Bitdefender Antivirus for Mac voor het eerst opent op macOS Mojave 10.14 of een nieuwere versie, verschijnt er een beschermingsaanbeveling. Deze aanbeveling verschijnt omdat we machtigingen nodig hebben om uw hele systeem te scannen op bedreigingen. Om ons deze machtigingen te verlenen, moet u ingelogd zijn als beheerder en de volgende stappen volgen:

1. Klik op de link **Systeemvoorkeuren**.
2. Klik op de icoon en voer vervolgens de beheerder-identificatiegegevens in.
3. Er verschijnt een nieuw venster. Versleep het bestand **BDLDaemon** naar de lijst met toegestane toepassingen.

2.3. Hoofdvenster Toepassing

Bitdefender Antivirus for Mac voldoet niet alleen aan de behoeften van beginnende computergebruikers, maar ook aan de eisen van bijzonder technische gebruikers. De grafische gebruikersinterface is ontworpen zodat elke categorie gebruikers deze probleemloos kunnen gebruiken.



Hoofdvenster Toepassing

Om door de Bitdefender-interface te gaan, wordt een inleidingswizard getoond met informatie over hoe u moet omgaan met het product en hoe u het moet configureren. Dit wordt in de linkerbovenhoek weergegeven. Selecteer het

juiste pijltje om de gids voort te zetten of **Rondleiding overslaan** om de wizard te sluiten.

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 werd gedetecteerd, verandert de kleur van de statusbalk naar rood. Zie *Problemen oplossen* (p. 24) voor meer informatie over mogelijke problemen en hun oplossingen.

Bitdefender Autopilot handelt als uw persoonlijke beveiligingsadviseur om u tijdens uw verschillende activiteiten een effectieve werking en verbeterde bescherming te bieden. Naargelang de activiteiten die u uitvoert, u werkt bijvoorbeeld of u voert online transacties uit, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat. Hiermee kunt u de voordelen van de functies die in de toepassing van Bitdefender Antivirus for Mac inbegrepen zijn, ontdekken, en ervan genieten.

Vanuit het navigatiemenu aan de linkerkant hebt u toegang tot de Bitdefender-onderdelen voor gedetailleerde configuratie en geavanceerde beheerstaken (tabbladen **Bescherming** en **Privacy**), notificaties, uw Bitdefender-account en het gebied Voorkeuren. U kunt ons eveneens contacteren (**Help** tab) voor ondersteuning indien u vragen hebt of indien er iets onverwachts verschijnt.

2.4. Dock-symbool toepassing

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 bedreigingen. Als u een bestand of een map naar het Dock-symbool sleept, wordt het bestand of de map onmiddellijk gescand.

Dock-symbool

2.5. Navigatiemenu

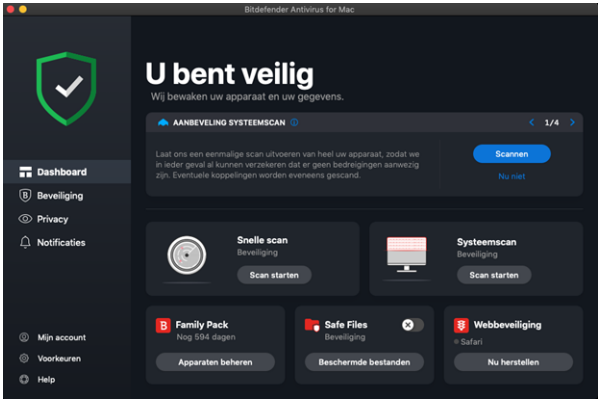
Aan de linkerkant op de Bitdefender-interface staat het navigatiemenu waarmee u snel toegang krijgt tot de functies van Bitdefender voor het gebruik van uw product. De beschikbare tabbladen in dit gebied zijn:

- **Dashboard**. Vanuit het Dashboard kunt u beveiligingsproblemen snel oplossen, aanbevelingen op basis van de systeemvereisten en gebruiksprofielen bekijken, snelle acties uitvoeren en naar uw Bitdefender-account gaan om de apparaten die u aan uw Bitdefender-abonnement hebt toegevoegd, te beheren.
- **Bescherming**. Vanuit Bescherming kunt u antivirusscans opstarten, bestanden toevoegen aan de lijst met uitzonderingen, bestanden en toepassingen beschermen tegen ransomware-aanvallen, uw Time Machine back-ups beveiligen en de bescherming tijdens het surfen configureren.
- **Privacy**. Van hier kunt u de Bitdefender VPN-app openen en de Anti-tracker extensie installeren in uw webbrowser.
- **Kennisgevingen**. Vanuit Notificaties kunt u informatie zien over de ondernomen acties voor de gescande bestanden.
- **Mijn account**. Van hier kunt u naar uw Bitdefender-account gaan om uw abonnementen te controleren en beveiligingstaken uit te voeren op de toestellen die u beheert. Er zijn eveneens details beschikbaar over de Bitdefender-account en de lopende abonnementen.
- **Voorkeuren**. Vanuit Voorkeuren kunt u de Bitdefender-instellingen configureren.
- **Help**. Vanuit Ondersteuning kunt u de afdeling Technische ondersteuning contacteren wanneer u hulp nodig hebt om problemen met uw Bitdefender-product op te lossen. U kunt ons ook feedback sturen om ons te helpen het product te verbeteren.

2.6. Donkere modus

Om uw ogen te beschermen tegen verblindend licht wanneer u 's avonds of in het donker werkt, ondersteunt Bitdefender Antivirus for Mac de donkere modus voor Mojave 10.14 en later. De kleuren van de interface werden geoptimaliseerd zodat u uw Mac kunt gebruiken zonder uw ogen te

vermoeien. De interface van Bitdefender Antivirus for Mac past zich aan volgens de weergave-instellingen van uw apparaat.



Donkere modus

3. BESCHERMING TEGEN SCHADELIJKE SOFTWARE

Dit hoofdstuk bevat de volgende onderwerpen:

- *Aanbevelingen* (p. 12)
- *Uw Mac scannen* (p. 13)
- *Scanwizard* (p. 14)
- *Quarantaine* (p. 15)
- *Bitdefender Shield (realtime bescherming)* (p. 16)
- *Uitzonderingen scannen* (p. 16)
- *Webbescherming* (p. 17)
- *Anti-tracker* (p. 19)
- *Veilige Bestanden* (p. 21)
- *Bescherming Time Machine* (p. 23)
- *Problemen oplossen* (p. 24)
- *Notificaties* (p. 25)
- *Updates* (p. 26)

3.1. Aanbevelingen

Om uw systeem beschermd te houden tegen bedreigingen en te voorkomen dat andere systemen onbedoeld geïnfecteerd worden, gelden de volgende aanbevelingen:

- Houd **Bitdefender Shield** ingeschakeld, zodat de systeembestanden automatisch gescand worden door Bitdefender Antivirus for Mac.
- Zorg dat uw Bitdefender Antivirus for Mac-product bijgewerkt blijft met de nieuwste informatie over bedreigingen en productupdates.
- Controleer regelmatig of er problemen worden gemeld door Bitdefender Antivirus for Mac, en los deze problemen op. Zie *Problemen oplossen* (p. 24) voor meer informatie.
- Check the detailed log of events concerning the Bitdefender Antivirus for Mac activity on your computer. Wanneer er iets belangrijks gebeurt aangaande de beveiliging van uw systeem of gegevens, wordt een nieuw

bericht toegevoegd aan het gebied Bitdefender Notificaties. Zie *Notificaties* (p. 25) 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. 32) voor meer informatie.

3.2. Uw Mac scannen

De functie **Bitdefender Shield** bewaakt de geïnstalleerde toepassingen op regelmatige basis, zoekt naar gebeurtenissen die op bedreigingen lijken en verhindert dat nieuwe bedreigingen uw systeem kunnen binnendringen, maar u kunt daarnaast ook op elk gewenst moment uw Mac of specifieke bestanden 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. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Selecteer het tabblad **Antivirus**.
3. Klik op een van de drie scanknoppen om de gewenste scan uit te voeren.
   - **Snelle scan** - controleert op de aanwezigheid van bedreigingen op de meest kwetsbare locaties van uw systeem (bijvoorbeeld de mappen met documenten, downloads, downloads van e-mails en tijdelijke bestanden van elke gebruiker).

- **Systeemscan** - voert een uitgebreide controle uit op dreigingen voor het volledige systeem. Ook alle geactiveerde volumes worden gescand.

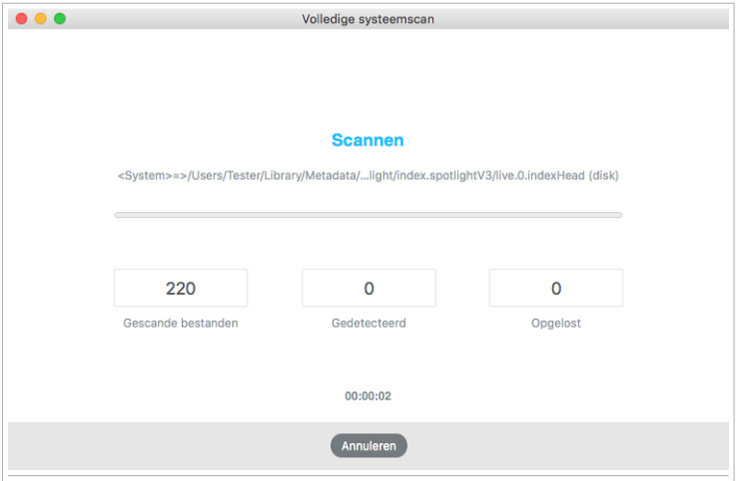
  > **Opmerking**
  >
  > Afhankelijk van de grootte van uw harde schijf kan een scan van het volledige systeem veel tijd in beslag nemen (soms wel een uur, of nog langer). Om de systeemprestaties niet te beïnvloeden, is het aan te raden geen volledige scans te starten terwijl u complexe taken (zoals videobewerking)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

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

U kunt ook een Systeemscan of Snelle Scan starten vanuit het Dashboard.

3.3. Scanwizard

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



Scan wordt uitgevoerd

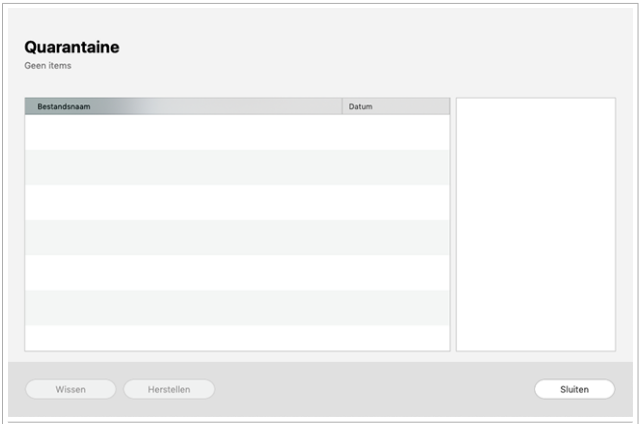
Tijdens elke scan wordt realtime informatie weergegeven over gedetecteerde en verwijderde dreigingen.

Wacht tot Bitdefender Antivirus for Mac klaar is met scannen.

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

3.4. Quarantaine

Bitdefender Antivirus for Mac kan geïnfecteerde of verdachte bestanden verplaatsen naar een speciaal beveiligde map, de zogeheten quarantaine. Wanneer een bedreiging in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.



Bestanden in quarantaine

Het venster Quarantaine toont alle bestanden die momenteel geïsoleerd zijn in de Quarantaine-map.

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

Om een lijst te zien met alle items in quarantaine:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.

2. Het venster **Antivirus** opent.

   Klik op **Openen** in het paneel **Quarantaine**.

3.5. Bitdefender Shield (realtime bescherming)

Bitdefender biedt realtime bescherming tegen een brede waaier aan bedreigingen door alle geïnstalleerde toepassingen en hun bijgewerkte versies en nieuwe en gewijzigde bestanden te scannen.

Om de realtime bescherming uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Voorkeuren**.
2. Schakel **Bitdefender Shield** in het venster **Bescherming** uit.

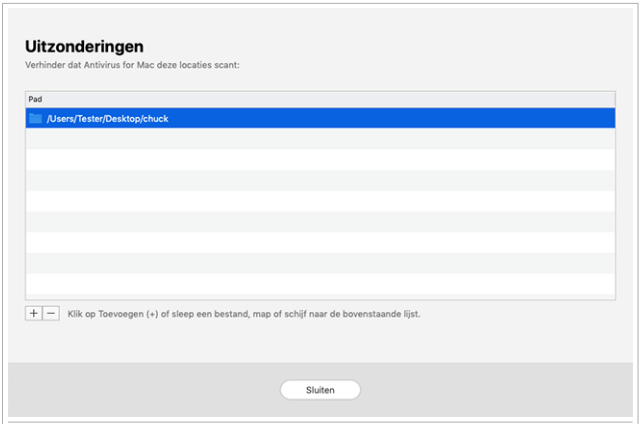
Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen bedreigingen.

3.6. Uitzonderingen 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



Uitzonderingen scannen

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

Om naar de lijst met uitzonderingen te gaan:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Het venster **Antivirus** opent.

   Klik op **Openen** in het paneel **Uitzonderingen**.

U kunt een uitzondering op twee manieren instellen:

- Sleep een bestand, map of volume naar de lijst met Uitzonderingen.
- Klik op de knop met het +-teken (+) onder de lijst met uitzonderingen. Kies vervolgens het bestand, de map of het volume dat van het scannen moet worden uitgesloten.

Als u een uitzondering uit de lijst wilt verwijderen, selecteert u deze in de lijst en klikt u onder de lijst met uitzonderingen op de knop met het minteken (-).

3.7. Webbescherming

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

Om de TrafficLight-extensies in te schakelen:

1. Klik op **Nu herstellen** in de kaart **Webbescherming** op het Dashboard.
2. Het venster **Webbescherming** opent.

   De gedetecteerde webbrowser die u op uw systeem geïnstalleerd hebt, verschijnt. Om de TrafficLight-extensie in uw browser te installeren, klikt u op **Extensie downloaden**.
3. U wordt doorgestuurd naar:

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

Extensie-instellingen beheren

Er zijn meerdere geavanceerde functies beschikbaar om u tegen allerlei soorten dreigingen te beschermen tijdens het surfen op het web. Om deze te gebruiken, klikt u op het TrafficLight-pictogram naast de instellingen van uw browser. Vervolgens klikt u op de knop **Instellingen**:

- **Instellingen Bitdefender TrafficLight**
  - Webbescherming: beschermt u tegen bezoeken aan websites die worden gebruikt voor malware-, phishing- en fraudeaanvallen.
  - Zoekadviseur - waarschuwt u op voorhand over riskante websites die in uw zoekresultaten worden vermeld.
- **Uitzonderingen**

  Bent u op de website die u wilt toevoegen aan de uitzonderingen, klikt u op **Huidige website aan lijst toevoegen**.

  Wilt u een andere website toevoegen, voert u het adres in het bijhorende veld in en klikt u op .

Er wordt geen waarschuwing weergegeven wanneer er bedreigingen zijn op de uitgezonderde 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. Wees voorzichtig als deze pagina toch wilt 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. Anti-tracker

Vele websites die u bezoekt, gebruiken trackers om informatie te verzamelen over uw gedrag. Ze kunnen deze informatie vervolgens delen met derden of ze kunnen de informatie gebruiken om u advertenties te laten zien die voor u relevanter zijn. Eigenaars van websites verdienen zo geld, om u gratis inhoud te kunnen bieden of om draaiende te blijven. Naast het verzamelen van informatie, kunnen trackers uw surfervaring vertragen of uw bandbreedte opgebruiken.

Als de extensie Anti-tracker van Bitdefender geactiveerd is in uw webbrowser, vermijdt u deze tracking, zorgt u dat uw gegevens privé blijven terwijl u online surft en wordt de laadtijd voor websites versneld.

De Bitdefender-extensie is compatibel met de volgende webbrowsers:

- Google Chrome
- Mozilla Firefox
- Safari

De trackers die we detecteren worden in de volgende categorieën gegroepeerd:

- **Reclame** - wordt gebruikt voor de analyse van patronen in websiteverkeer, het gedrag van gebruikers of het verkeer van bezoekers.

- **Klanteninteractie** - wordt gebruikt om de interactie van gebruikers met verschillende invoervormen, zoals chat of ondersteuning, te meten.
- **Essentieel** - wordt gebruikt om de kritieke functionaliteiten van webpagina's te monitoren.
- **Website-analytics** - wordt gebruikt om gegevens over het gebruik van webpagina's te verzamelen.
- **Sociale Media** - wordt gebruikt voor de monitoring van het sociale publiek, de activiteiten en het gebruikersengagement met verschillende sociale mediaplatformen.

Bitdefender Anti-tracker activeren

Om de Bitdefender Anti-tracker extensie te activeren in uw webbrowser:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Selecteer het tabblad **Anti-tracker**.
3. Klik op **Extensie activeren** naast de webbrowser waarvoor u de extensie wilt activeren.

3.8.1. Interface van Anti-tracker

Wanneer de extensie Anti-tracker van Bitdefender geactiveerd is, verschijnt het pictogram  naast de zoekbalk in uw webbrowser. Telkens u een website bezoekt, ziet u een teller op het pictogram: dat getal verwijst naar de gedetecteerde en geblokkeerde trackers. Voor meer details over de geblokkeerde trackers, klikt u op het pictogram om de interface te openen. U ziet, naast het aantal geblokkeerde trackers, ook hoeveel tijd de pagina nodig heeft om te laden alsook de categorieën waartoe de gedetecteerde trackers behoren. Om een lijst weer te geven van de websites die aan tracking doen, klikt u op de gewenste categorie.

Om de blokkering van trackers door Bitdefender op te heffen voor de website die u momenteel bezoekt, klikt u op **Bescherming op deze website pauzeren**. Deze instelling is enkel van toepassing zolang u de website open hebt staan en gaat terug naar zijn initiële staat zodra u de website verlaat.

Om toe te staan dat trackers van een specifieke categorie uw activiteiten volgen, klikt u op de gewenste activiteit en vervolgens op de bijhorende knop. Indien u zich bedenkt, klikt opnieuw op dezelfde knop.

3.8.2. Uitschakelen van de Bitdefender Anti-tracker

Om de Bitdefender Anti-tracker uit te schakelen in uw webbrowser:

1. Open uw webbrowser.
2. Klik op het pictogram naast de adresbalk in uw webbrowser.
3. Klik op het pictogram in de rechterbovenhoek.
4. Gebruik de bijhorende schakelaar om uit te schakelen.

   Het Bitdefender icoon wordt grijs.

3.8.3. Toestaan dat een website aan tracking doet

Wilt u dat tracking wordt toegepast wanneer u een bepaalde website bezoekt, kunt u dit adres als volgt toevoegen aan de uitzonderingen:

1. Open uw webbrowser.
2. Klik op het pictogram naast de zoekbalk.
3. Klik op het pictogram in de rechterbovenhoek.
4. Bent u op de website die u wilt toevoegen aan de uitzonderingen, klikt u op **Huidige website aan lijst toevoegen**.

   Wilt u een andere website toevoegen, voert u het adres in het bijhorende veld in en klikt u op .

3.9. 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.

Om achteraf bestanden toe te voegen aan de beschermde omgeving:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Selecteer het tabblad **Antiransomware**.
3. Klik op **Beschermde bestanden** in het gebied Veilige bestanden.
4. 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.

3.9.1. Toegang toepassingen

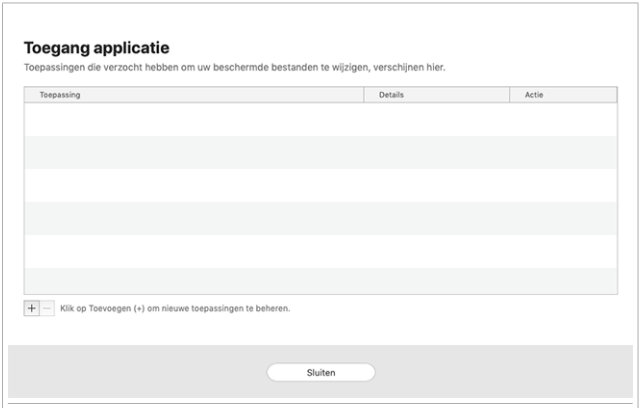
De applicaties die proberen om beschermde bestanden te wijzigen of verwijderen kunnen aangeduid worden als potentieel onveilig en toegevoegd aan de lijst Geblokkeerde applicaties. Indien een applicatie geblokkeerd werd en u zeker bent dat dit normaal gedrag is, kunt u ze toestaan via de volgende stappen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Selecteer het tabblad **Antiransomware**.
3. Klik op **Toegang toepassingen** in het gebied Veilige bestanden.

4. Wijzig de status naast de geblokkeerde toepassing 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.



Veilige Bestanden

3.10. 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.

Raadpleeg de Apple-ondersteuningspagina voor instructies indien u items van een Time Machine back-up moet herstellen.

Time Machine Protection in- of uitschakelen

Om Time Machine Bescherming in of uit te schakelen:

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Bescherming**.
2. Selecteer het tabblad **Antiransomware**.
3. Schakel de schakelaar **Time Machine Bescherming** in of uit.

3.11. Problemen oplossen

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.

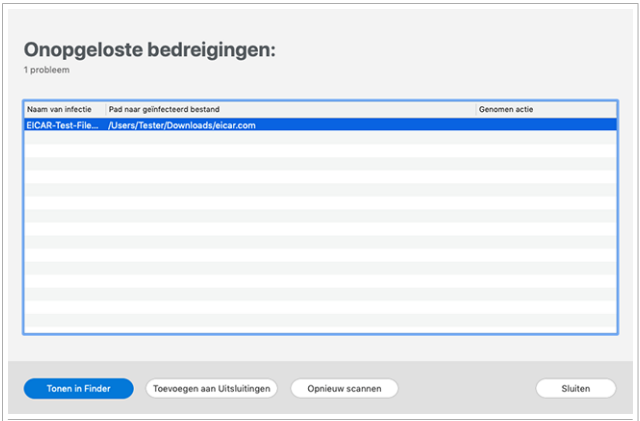
Als u de problemen oplost die door Bitdefender Antivirus for Mac worden gemeld, weet u zeker dat uw systeem en uw gegevens altijd veilig zijn.

Onder andere deze problemen kunnen worden gemeld:

- De nieuwe informatie-update voor bedreigingen werd niet gedownload van onze servers.
- Er werden bedreigingen op uw systeem gedetecteerd en het product kan ze niet automatisch desinfecteren.
- De realtime bescherming is uitgeschakeld.

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

1. Als er geen waarschuwingen van Bitdefender zijn, is de statusbalk groen. Als er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statusbalk naar rood.
2. Lees de beschrijving voor meer informatie.
3. Wanneer er een probleem wordt gedetecteerd, klikt u op de overeenkomstige knop om een actie te ondernemen.



Het venster Niet-opgeloste dreigingen

De lijst met onopgeloste bedreigingen wordt bijgewerkt na elke systeemscan, ongeacht of de scan automatisch werd uitgevoerd of door u werd opgestart.

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

- Handmatig wissen. Kies deze actie als u besmettingen handmatig wilt verwijderen.
- Toevoegen aan Uitsluitingen. Deze actie is niet beschikbaar voor bedreigingen die worden aangetroffen binnen archieven.

3.12. Notificaties

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw computer. Wanneer er iets belangrijks gebeurt met de veiligheid van uw systeem of gegevens, wordt er een nieuw bericht toegevoegd aan Kennisgevingen van het Bitdefender, net zoals er nieuwe e-mails verschijnen in uw Postvak IN.

Kennisgevingen zijn een belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging. U kunt bijvoorbeeld heel gemakkelijk controleren of een update is geslaagd, of er bedreigingen of kwetsbaarheden op uw computer werden aangetroffen enz. Daarnaast kunt u zo nodig verdere acties ondernemen of acties die door Bitdefender zijn ondernomen, wijzigen.

Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties** om de Notificatielog te bekijken. Telkens wanneer zich een kritiek evenement voordoet, kunt u een teller opmerken op de 

-icoon.

Afhankelijk van het type en de ernst worden kennisgevingen gegroepeerd in:

- **Kritieke** gebeurtenissen wijzen op kritieke problemen. U moet ze onmiddellijk controleren.
- Gebeurtenissen van het type **Waarschuwing** wijzen op niet-kritieke problemen. U moet ze controleren en herstellen wanneer u tijd hebt.
- Gebeurtenissen van het type **Informatie** duiden op een geslaagde bewerking.

Klik op elke tab om meer details te lezen over de gegenereerde gebeurtenissen. Er wordt beperkte informatie weergegeven als u een keer op elke titel van een gebeurtenis klikt, namelijk: een korte beschrijving, de

actie die Bitdefender heeft ondernomen wanneer ze zich voordeed en de datum en tijd van de gebeurtenis. Er kunnen opties worden geboden voor het ondernemen van verdere actie.

Om u te helpen geregistreerde gebeurtenissen gemakkelijker te beheren, biedt het venster Kennisgevingen opties waarmee alle gebeurtenissen in dat deel kunnen worden verwijderd of gemarkeerd als gelezen.

3.13. Updates

Elke dag worden er nieuwe bedreigingen gevonden en geïdentificeerd. Daarom is het erg belangrijk om Bitdefender Antivirus for Mac bij te werken met de nieuwste updates van bedreigingsinformatie.

De updates van de bedreigingsinformatie gebeuren 'on the fly', wat betekent dat de bestanden die moeten worden bijgewerkt, geleidelijk worden vervangen. Zo heeft de update geen gevolgen voor de werking van het product en wordt tegelijkertijd elk zwak punt uitgesloten.

- Als Bitdefender Antivirus for Mac up-to-date is, kunnen ook de nieuwste dreigingen worden gedetecteerd en uit geïnfecteerde bestanden worden verwijderd.
- Als Bitdefender Antivirus for Mac niet is bijgewerkt, kunnen de nieuwste soorten bedreigingen die zijn ontdekt door Bitdefender Labs niet worden gedetecteerd en verwijderd.

3.13.1. Zelf een update uitvoeren

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. Klik in de menubalk op de knop **Acties**.
2. Kies **Informatiedatabase bedreigingen updaten**.

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.

3.13.2. 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 verbinding maakt met het internet via een proxyserver die authenticatie vereist, moet u regelmatig overschakelen naar een rechtstreekse internetverbinding om ervoor te zorgen dat u updates van bedreigingsinformatie ontvangt.

3.13.3. 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. Het is mogelijk dat u voor deze updates het systeem opnieuw moet opstarten om de installatie van nieuwe bestanden te activeren. 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.

3.13.4. Informatie over Bitdefender Antivirus for Mac vinden

Om informatie te vinden over de Bitdefender Antivirus for Mac-versie die u hebt geïnstalleerd, gaat u naar het venster **Over**. Daar vindt u eveneens de Abonnementsovereenkomst, het Privacybeleid en de Open source-licenties.

Om naar het venster Over te gaan:

1. Open Bitdefender Antivirus for Mac.
2. Klik in de menubalk op Bitdefender Antivirus for Mac en kies **Over Antivirus voor Mac**.

4. VPN

Dit hoofdstuk bevat de volgende onderwerpen:

- *Over VPN* (p. 28)
- *VPN Openen* (p. 28)
- *Interface* (p. 29)
- *Abonnementen* (p. 31)

4.1. 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.

4.2. VPN Openen

Er zijn drie manieren om de Bitdefender VPN-toepassing te openen:

- Klik in het navigatiemenu in de **Bitdefender-interface** op **Privacy**.

Klik op **Openen** in de Bitdefender VPN-kaart.

- Klik op het pictogram in de menubalk.
- Ga naar de map Toepassingen, open de map Bitdefender en dubbelklik op het pictogram Bitdefender VPN.

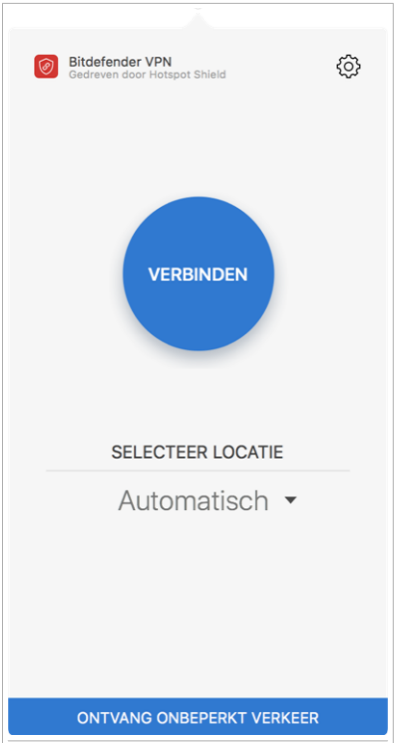
De eerste keer dat u de toepassing opent, wordt u gevraagd Bitdefender toe te staan configuraties toe te voegen. Door aan Bitdefender] deze toestemming te verlenen, stemt u ermee in dat alle netwerkactiviteiten op uw apparaat worden gefilterd of gemonitord wanneer u de VPN-toepassing gebruikt.

Opmerking
De Bitdefender VPN-app kan enkel op macOS Sierra (10.12.6), macOS High Sierra (10.13.6) of macOS Mojave (10.14 of hoger) worden geïnstalleerd.

4.3. Interface

De VPN-interface geeft de status van de app weer: verbonden of niet verbonden. Voor gebruikers met de gratis versie stelt Bitdefender de serverlocatie automatisch in op de meest geschikte server. Premium-gebruikers hebben de mogelijkheid om de serverlocatie waarmee ze wensen te verbinden, te wijzigen, door de locatie te selecteren in de lijst **Virtuele locaties**. Voor meer info over VPN-abonnementen, raadpleeg *Abonnementen* (p. 31).

Om te verbinden of om de verbinding te verbreken, klik op de status bovenaan op het scherm. Het 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 het icoon ⚙ aan de rechterbovenkant:

- **Mijn Account** - geeft details weer over uw Bitdefender-account en VPN-abonnement. 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:
  - Notificaties
  - Stel de VPN in om op te starten wanneer het systeem opgestart wordt
  - Productrapporten

- Automatisch verbinden - bevindt zich in het tabblad **Geavanceerd**; met deze voorziening kunt u de Bitdefender VPN automatisch laten verbinden wanneer u een niet-beveiligd of openbaar wifinetwerk gebruikt of wanneer een app voor peer-to-peer-bestandsuitwisseling wordt opgestart.

- **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** - de toepassing verlaten.

4.4. 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 **Upgraden** 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 beschermingabonnement. Indien het Bitdefender Premium VPN-abonnement vervalt, maar indien het abonnement voor Bitdefender Antivirus for Mac nog actief is, gaat u terug naar de gratis versie.

Bitdefender VPN is een cross-platform product, beschikbaar in Bitdefender-producten die compatibel zijn met Windows, macOS, Android en iOS. Eens u upgradet naar de premium-versie, kunt u uw abonnement op alle producten gebruiken, op voorwaarde dat u inlogt met dezelfde Bitdefender-account.

5. VOORKEUREN INSTELLEN

Dit hoofdstuk bevat de volgende onderwerpen:

- *Voorkeuren weergeven* (p. 32)
- *Beschermingsvoorkeuren* (p. 32)
- *Geavanceerde voorkeuren* (p. 33)
- *Speciale aanbieding* (p. 33)

5.1. Voorkeuren weergeven

Zo opent u het voorkeurenvenster van Bitdefender Antivirus for Mac:

1. Voer een van de volgende bewerkingen uit:
   - Klik in het navigatiemenu in de Bitdefender-interface op **Voorkeuren**.
   - Klik in de menubalk op Bitdefender Antivirus for Mac en kies **Voorkeuren**.

5.2. 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.

- **Bitdefender Shield.** Bitdefender Shield biedt realtime bescherming tegen een brede waaier aan bedreigingen door alle geïnstalleerde toepassingen en hun bijgewerkte versies en nieuwe en gewijzigde bestanden te scannen. We raden aan dat u Bitdefender Shield niet uitschakelt, maar als u dat toch moet doen, doe het dan zo weinig mogelijk. Indien Bitdefender Shield uitgeschakeld is, wordt u niet beschermd tegen bedreigingen.
- **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 bijbehorende vakje.
- **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.

5.3. Geavanceerde voorkeuren

U kunt een algemene actie kiezen voor alle problemen en verdachte items die tijdens de scan gedetecteerd werden.

Actie voor geïnfecteerde objecten

Poging tot desinfecteren of verplaatsen naar quarantaine - Indien er geïnfecteerde bestanden worden gedetecteerd, probeert Bitdefender ze te desinfecteren (schadelijke code verwijderen) of ze naar quarantaine te verplaatsen.

Geen actie ondernemen - Er wordt geen actie ondernomen voor de geïnfecteerde bestanden.

Actie voor verdachte bestanden

Bestanden naar quarantaine verplaatsen - Indien verdachte bestanden worden gedetecteerd, verplaatst Bitdefender ze naar quarantaine.

Geen actie ondernemen - Er wordt geen actie ondernomen voor de geïnfecteerde bestanden.

5.4. Speciale aanbieding

Wanneer er reclameaanbiedingen beschikbaar zijn, is het Bitdefender product zo ingesteld dat u daarvan op de hoogte wordt gesteld via een pop-upvenster. Dit geeft u de mogelijkheid om te profiteren van voordelige tarieven en om uw apparaten beveiligd te houden gedurende een langere periode.

Om kennisgevingen voor speciale aanbiedingen in of uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Voorkeuren**.
2. Selecteer het tabblad **Andere**.
3. Schakel de schakelaar **Mijn aanbiedingen** in of uit.

De optie **Mijn aanbiedingen** is standaard ingeschakeld.

6. BITDEFENDER CENTRAL

Dit hoofdstuk bevat de volgende onderwerpen:

- *Over Bitdefender Central* (p. 34)
- *Mijn abonnementen* (p. 38)
- *Mijn apparaten* (p. 38)

6.1. Over Bitdefender Central

Bitdefender Central is het platform waar u toegang hebt tot de online functies en diensten van het product en waar u vanop afstand belangrijke taken kunt uitvoeren op apparaat waarop Bitdefender is geïnstalleerd. U kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar https://central.bitdefender.com te gaan of rechtstreeks vanuit de Bitdefender Central-toepassing op Android- en iOS-apparaten.

Om de Bitdefender Central-toepassing op uw apparaten te installeren:

- **Op Android** - zoek Bitdefender Central op Google Play en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.
- **Op iOS** - zoek Bitdefender Central in de App Store en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.

Zodra u aangemeld bent, 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
- Uw Bitdefender-abonnementen beheren en verlengen.
- Nieuwe apparaten aan uw netwerk toevoegen en deze apparaten beheren, waar u op dat moment 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 het hoofdvenster van Bitdefender Antivirus for Mac:
  1. Klik rechtsonder in het scherm op de koppeling **Ga naar uw account**.
- Vanuit uw webbrowser:
  1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
  2. Ga naar https://central.bitdefender.com.
  3. Log in op uw account met uw e-mailadres en wachtwoord.
- Vanaf uw Android- of iOS-apparaat:

  Open de Bitdefender Central-toepassing die u geïnstalleerd hebt.

Opmerking
Hierin zitten de opties die u ook in de webinterface vindt.

6.3. Twee-factorenauthenticatie

De 2-Factor authenticatiemethode voegt een extra veiligheidslaag toe aan uw Bitdefender account, door een authenticatiecode te vragen bovenop uw aanmeldgegevens. Op deze manier voorkomt u dat uw account wordt overgenomen en houdt u types cyberaanvallen, zoals keyloggers, bruteforce- of woordenlijstaanvallen, af.

Twee-factorenauthenticatie activeren

Door de tweefactorenauthenticatie te activeren, maakt u uw Bitdefender account veel veiliger. Uw identiteit zal gecontroleerd worden telkens u zich aanmeldt via verschillende apparaten, hetzij om één van de Bitdefender producten te installeren, hetzij om de status van uw abonnement te controleren of vanop afstand taken uit te voeren op uw apparaten.

Om de twee-factorenauthenticatie te activeren:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .

3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Klik op **STARTEN**.

   Kies een van de volgende methodes:

   - **Authenticator App** - gebruik een authenticator app om een code te genereren telkens u zich wilt aanmelden op uw Bitdefender account.

     Als u een authenticator app zou willen, gebruiken, maar u niet zeker weet welke te kiezen, is er een lijst beschikbaar van de authentication apps die we aanbevelen.

     a. Klik op **AUTHENTICATOR APP GEBRUIKEN** om te starten.

     b. Om u aan te melden op een op Android of iOS gebaseerd apparaat, gebruik dat dan om de QR code te scannen.

        Om u aan te melden op een laptop of computer, kunt u de getoonde code manueel toevoegen.

        Klik op **VERDERGAAN**.

     c. Voer de code in die de app geeft of deze die weergegeven wordt in de vorige stap, en klik dan op **ACTIVEREN**.

   - **E-mail** - telkens u zich aanmeldt in uw Bitdefender account, zal er een verificatiecode naar het Postvak-IN van uw e-mail worden gestuurd. Controleer de e-mail en gebruik dan de code die u ontving.

     a. Klik op **E-MAIL GEBRUIKEN** om te starten.

     b. Controleer uw e-mail en tik de verstrekte code in.

     c. Klik op **Activeren**.

In het geval u wilt stoppen met het gebruik van de twee-factorenauthenticatie:

1. Klik op **TWEE-FACTORENAUTHENTICATIE UITSCHAKELEN**.
2. Controleer uw app of e-mailaccount en tik de code in die u hebt ontvangen.
3. Bevestig uw keuze.

6.4. Betrouwbare apparaten toevoegen

Om ervoor te zorgen dat alleen u toegang hebt tot uw Bitdefender account, is het mogelijk dat we eerst een veiligheidscode vragen. Als u deze stap zou

willen overslaan telkens u verbinding maakt vanaf hetzelfde apparaat, raden we u aan dit te benoemen als een betrouwbaar apparaat.

Om toestellen toe te voegen als betrouwbare apparaten:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Klik op **Betrouwbare apparaten**.
6. De lijst van de apparaten waar Bitdefender op geïnstalleerd is, wordt weergegeven. Klik op de gewenste apparaat.

U kunt zo veel apparaten toevoegen als u wilt, op voorwaarde dat Bitdefender erop geïnstalleerd is en uw abonnement geldig is.

6.5. Activiteit

In de Activiteitzone hebt u toegang tot informatie over de apparaten waar Bitdefender op geïnstalleerd is.

Wanneer u naar het **Activiteiten**-venster gaat, zijn de volgende kaarten beschikbaar:

- **Mijn apparaten**. Hier ziet u het aantal geconnecteerde apparaten, samen met hun beschermingsstatus. Om problemen voor de gedetecteerde apparaten vanop afstand op te lossen, klikt u op **Problemen oplossen** en vervolgens op **PROBLEMEN SCANNEN EN HERSTELLEN**.

  Om details te zien over de gedetecteerde problemen, klikt u op **Problemen bekijken**.

  Informatie over de gedetecteerde bedreigingen kan voor iOS-apparaten niet worden opgehaald.

- **Bedreigingen geblokkeerd**. Hier ziet u een grafiek met de algemene statistieken, met inbegrip van informatie over de bedreigingen die de voorbije 24 uur en 7 dagen werden geblokkeerd. De weergegeven informatie wordt opgehaald naargelang het schadelijke gedrag dat in de bestanden, toepassingen en url's werd gedetecteerd.

- **Topgebruikers met geblokkeerde bedreigingen**. Hier ziet u de gebruikers waarbij de meeste bedreigingen werden gevonden.

- **Topapparaten met geblokkeerde bedreigingen**. Hier ziet u de apparaten waarop de meeste bedreigingen werden gevonden.

6.6. Mijn abonnementen

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

6.6.1. Abonnement activeren

Een abonnement kan geactiveerd worden tijdens het installatieproces als u uw Bitdefender-account gebruikt. 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.

Volg de onderstaande stappen om een abonnement te activeren met behulp van een activeringscode:

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 knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **Activeren** 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.

6.7. Mijn apparaten

Vanaf het paneel **Mijn apparaten** van uw Bitdefender-account kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en 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.

6.7.1. Uw apparaten aanpassen

Om uw apparaten beter te kunnen herkennen, kunt u de apparaatnaam 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**.

Om het beheer van uw apparaten te vereenvoudigen, kunt u eigenaren instellen en aan de apparaten toewijzen:

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**, 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 lijst **Apparaateigenaar** en klik op **Toewijzen**.

6.7.2. 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**.

Wanneer u op een apparaatkaart klikt, komen de volgende tabbladen beschikbaar:

- **Bedieningspaneel**. In dit venster vindt u gegevens over het geselecteerde apparaat, kunt u de beveiligingsstatus nakijken en kunt u nagaan hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus kan groen zijn (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Klik voor meer informatie op het uitklappijltje in het bovenste statusgebied indien uw apparaat problemen ondervindt. Van hieruit kunt u problemen manueel oplossen die de veiligheid van uw toestellen aantasten.
- **Bescherming**. In dit tabblad kunt u op afstand een Snelle scan of een Volledige scan uitvoeren op uw apparaten. Klik op de **SCAN**-knop om het proces te starten. U kunt ook nagaan wanneer de laatste scan werd uitgevoerd op het toestel en van de laatste scan met de belangrijkste informatie is er een verslag beschikbaar. Zie *Uw Mac scannen* (p. 13) 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 te proberen, moet u:

1. Volg de onderstaande stappen om een Bitdefender-account aan te maken:
   a. Ga naar https://central.bitdefender.com.
   b. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft, worden vertrouwelijk behandeld.
   c. Voordat u verdergaat, moet u de Gebruiksvoorwaarden aanvaarden. De Gebruiksvoorwaarden bevatten de voorwaarden waaronder u Bitdefender mag gebruiken; lees ze dus grondig door.

      U kunt eveneens het Privacybeleid lezen.
   d. Klik op **ACCOUNT AANMAKEN**.
2. Volg de onderstaande stappen om Bitdefender Antivirus for Mac te downloaden:
   a. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
   b. Kies een van de twee beschikbare opties:
      - **Bescherm dit apparaat**
        i. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
        ii. Sla het installatiebestand op.
      - **Bescherm andere apparaten**
        i. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

ii. Klik op **DOWNLOADLINK VERSTUREN**.

iii. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**.

De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

iv. Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.

c. 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.

Volg de onderstaande stappen om een abonnement te activeren met behulp van een activeringscode:

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 knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **Activeren** om door te gaan.

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 uitzonderingen** 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 logboek bij van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten van de applicatie. Om toegang te krijgen tot deze informatie, klikt u in het navigatiemenu in de interface van Bitdefender op **Notificaties**.

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 verbinding maakt met het internet via een proxyserver die authenticatie vereist, moet u regelmatig overschakelen naar een rechtstreekse internetverbinding om ervoor te zorgen dat u updates van bedreigingsinformatie ontvangt.

Hoe kan ik Bitdefender Antivirus for Mac verwijderen?

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster en ga naar de map Programma's.
2. Open de Bitdefender-map en dubbelklik op Bitdefender Uninstaller.
3. Klik op **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. 46).

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

- Zo verwijdert u de TrafficLight-extensies uit Mozilla Firefox:
  1. Ga naar **Extra** en selecteer **Add-ons**.
  2. Selecteer **Extensies** in de linkerkolom.
  3. Selecteer de extensie en klik op **Verwijderen**.
  4. Start de browser opnieuw om de verwijdering te voltooien.
- Zo verwijdert u de TrafficLight-extensies uit Google Chrome:
  1. Klik rechtsboven op **Meer** .
  2. Ga naar **Extra** en selecteer **Extensies**.
  3. Klik op het pictogram **Verwijderen.....** naast de extensie die u wilt verwijderen.
  4. Klik op **Verwijderen** om de verwijdering te bevestigen.
- Zo verwijdert u Bitdefender TrafficLight uit Safari:
  1. Naar **Voorkeuren** gaan op drukken op **Opdracht-Komma(,)**.
  2. Selecteer **Extensies**.

     Er verschijnt een lijst van de geïnstalleerde extensies.
  3. Selecteer de Bitdefender TrafficLight extensie, en klik dan op **Deïnstalleren**.
  4. Klik opnieuw op **Deïnstalleren** om het verwijderingsproces te bevestigen.

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om te verzekeren dat u veilig bent wanneer u surft op het web, 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 is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. 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. 46)
- *Contactinformatie* (p. 48)

8.1. Ondersteuning

Bitdefender wil zijn klanten graag de best mogelijke, snelle ondersteuning bieden. Als er een probleem is met een product van Bitdefender of als u hier iets over wilt vragen, zijn er meerdere online informatiebronnen waar u snel een oplossing of een antwoord kunt 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

De volgende online informatiebronnen zijn beschikbaar voor hulp bij eventuele problemen of vragen met betrekking tot Bitdefender.

- Bitdefender Ondersteuningscentrum:

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

- Bitdefender Ondersteuningsforum:

  https://forum.bitdefender.com

- Het HOTforSecurity-portaal over computerbeveiliging:

  https://www.hotforsecurity.com

U kunt ook altijd uw favoriete zoekmachine gebruiken om meer informatie te vinden over computerbeveiliging en over de producten van Bitdefender.

Bitdefender Ondersteuningscentrum

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

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

Het Bitdefender Ondersteuningscentrum is voor iedereen toegankelijk en kan vrijelijk worden doorzocht. De uitgebreide informatie in het Ondersteuningscentrum is een van de vele manieren waarop Bitdefender-klanten toegang kunnen krijgen tot technische kennis en achtergrondinformatie. Alle geldige informatieverzoeken en probleemmeldingen van klanten van Bitdefender komen uiteindelijk terecht in het Bitdefender Ondersteuningscentrum in de vorm van bugfix-rapporten, oplossingen of informatieve artikelen, die een aanvulling vormen op de Help-bestanden van onze producten.

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

Bitdefender Ondersteuningsforum

Via het Bitdefender Ondersteuningsforum kunnen Bitdefender-gebruikers heel gemakkelijk hulp krijgen of anderen 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.

Zoek altijd eerst op het forum om te zien of een vergelijkbare vraag of kwestie al eerder is besproken.

Het Bitdefender Ondersteuningsforum is in 5 talen (Engels, Duits, Frans, Spaans en Roemeens) beschikbaar via https://forum.bitdefender.com. 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 een verbinding met Internet maakt (malware, phishing, spam, cybercriminelen). Via een nuttig woordenboek leer u de termen kennen met betrekking tot de computerbeveiliging.

Er worden regelmatig nieuwe artikelen gepubliceerd om u op de hoogte te houden van de meest recent ontdekte bedreigingen, actuele beveiligingstrends en andere informatie over de beveiligingssector.

De webpagina van HOTforSecurity is https://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 artikelen of documenten door en pas de voorgestelde oplossingen toe.
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 naar het 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 te overtreffen. Aarzel niet contact op te nemen met ons als u eventuele vragen hebt.

8.2.1. Webadressen

Verkoopafdeling: sales@bitdefender.com
Ondersteuningscentrum:https://www.bitdefender.com/support/consumer.html
Documentatie: documentation@bitdefender.com
Lokale distributeurs:https://www.bitdefender.com/partners
Partnerprogramma: partners@bitdefender.com
Persinformatie: pr@bitdefender.com
Vacatures: jobs@bitdefender.com
Indienen van bedreigingen: virus_submission@bitdefender.com
Spammeldingen: spam_submission@bitdefender.com
Misbruikmeldingen: abuse@bitdefender.com

Website: https://www.bitdefender.be

8.2.2. Lokale distributeurs

De lokale Bitdefender-distributeurs staan klaar om alle vragen binnen hun verantwoordelijkheidsgebied te beantwoorden, zowel over commerciële als algemene zaken.

Zo vindt u een Bitdefender-distributeur in uw land:

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 email in het Engels zodat wij u onmiddellijk kunnen helpen.

8.2.3. Bitdefender-vestigingen

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:

Verenigde Staten

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
Orhideea Towers, 15A Orhideelor Street, Sector 6
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 hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

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 licentieovereenkomst.

Bedreiging

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 bedreigingen kunnen zichzelf ook dupliceren. Alle computerbedreigingen zijn door de mens gemaakt. Een eenvoudige bedreiging die zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudige bedreiging is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren. Een nog gevaarlijker type is een bedreiging die in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

Brute force-aanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door mogelijke wachtwoordcombinaties in te geven, meestal te beginnen met het meest eenvoudig te raden wachtwoord.

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt.

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 bedreiging die zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke bedreigingen moeilijk te identificeren.

Ransomware

Ransomware is een kwaadaardig programma dat geld probeert te verdienen van gebruikers door hun kwestbare systemen af te sluiten. CryptoLocker, CryptoWall en TeslaWall zijn enkele varianten die jagen op persoonlijke systemen van gebruikers.

De infectie kan verspreid worden door spam-e-mail 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.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dat geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

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 systeemgeheugen 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 kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen 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.

Woordenboekaanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door een combinatie van veel voorkomende woorden in te geven om zo mogelijke wachtwoorden te genereren. Dezelfde methode wordt gebruikt om decryptiesleutels van versleutelde berichten of documenten te raden. Woordenboekaanvallen slagen in hun opzet omdat veel mensen korte wachtwoorden gebruiken die uit slechts één woord bestaan en die makkelijk te raden zijn.

Worm

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