Bitdefender®
ANTIVIRUS FOR MAC

GEBRUIKSAAN WIJZING

Bitdefender Antivirus for Mac

Handleiding

Publicatiedatum 11/24/2022

Juridische kennisgeving

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

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 dreigingen en andere schadelijke software, zodat u maximaal profijt hebt van uw Bitdefender.

We wensen u veel leesplezier met deze handleiding.

Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Aan de slag (pagina 11)

Aan de slag met Bitdefender Antivirus for Mac en zijn gebruikersinterface.

Bescherming tegen schadelijke software (pagina 15)

Leer hoe u Bitdefender Antivirus for Mac kunt gebruiken om uzelf te beschermen tegen schadelijke software.

Voorkeuren instellen (pagina 36)

Krijg meer informatie over de voorkeuren van Bitdefender Antivirus for Mac.

Hulp vragen (pagina 54)

Ontdek waar u hulp moet zoeken indien er zich onverwacht een probleem voordoet.

Conventies die in deze gids worden gebruikt

Typografische conventies

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

Weergave	Beschrijving
`voorbeeld-syntaxis`	Voorbeelden van syntaxis worden weergegeven in een `niet-proportioneel lettertype`.
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.
Over deze gids (pagina 1)	Dit is een interne koppeling naar een locatie in het document.
`bestandsnaam`	Namen van bestanden en mappen worden weergegeven in een `niet-proportioneel lettertype`.
optie	Alle productopties worden **vet** weergegeven.
trefwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

Waarschuwingen

De waarschuwingen zijn grafisch gemarkeerde opmerkingen in de tekst die extra informatie over de huidige paragraaf onder de aandacht brengen.

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-kritieke, 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.

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. WAT IS 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. INSTALLEREN EN VERWIJDEREN

Dit hoofdstuk bevat de volgende onderwerpen:

2.1. 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 op het Apple-symbool in de linkerbovenhoek van het scherm en kies Over **Deze Mac**. In het venster dat verschijnt, ziet u de versie van uw besturingssysteem en andere nuttige informatie. Klik op **Systeemrapport** voor gedetailleerde hardware-informatie.

2.2. Bitdefender Antivirus for Mac installeren

De Bitdefender Antivirus for Mac app kan als volgt worden geïnstalleerd vanuit 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.

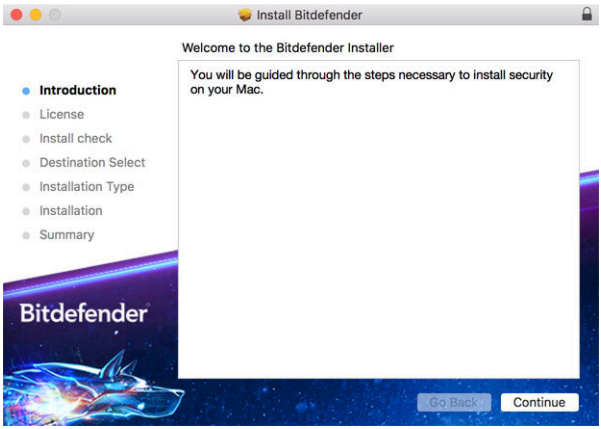
4. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
5. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Sla het installatiebestand op.
   - **Bescherm andere apparaten**
     a. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
     b. Klik op **DOWNLOADKOPPELING VERZENDEN**.
     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.

2.2.1. Installatieprocedure

Om Bitdefender Antivirus for Mac te installeren:

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



Klik op **Doorgaan**.

Stap 2 - Abonnementsovereenkomst lezen

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.

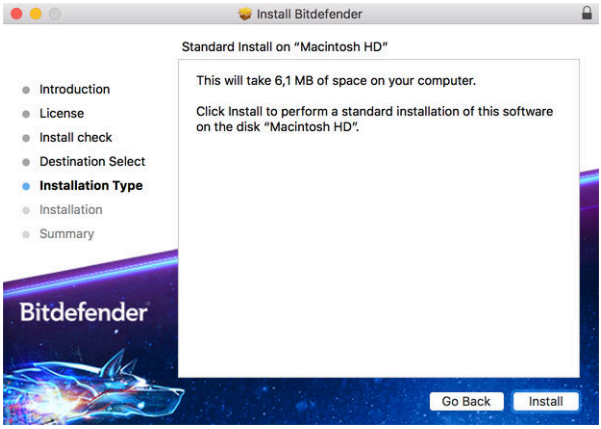
Vanuit dit venster kunt u ook de taal waarin u het product wilt installeren, selecteren.

Klik op **Doorgaan**, en klik dan 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.

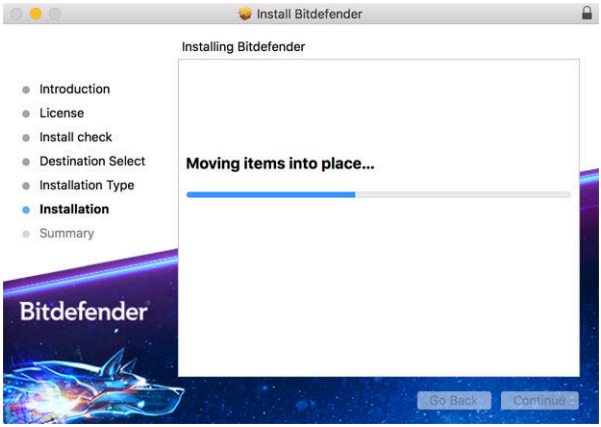
Stap 3 - Installatie starten



Bitdefender Antivirus for Mac wordt geïnstalleerd in `Macintosh HD/Library/Bitdefender`. Het installatiepad kan niet worden gewijzigd.

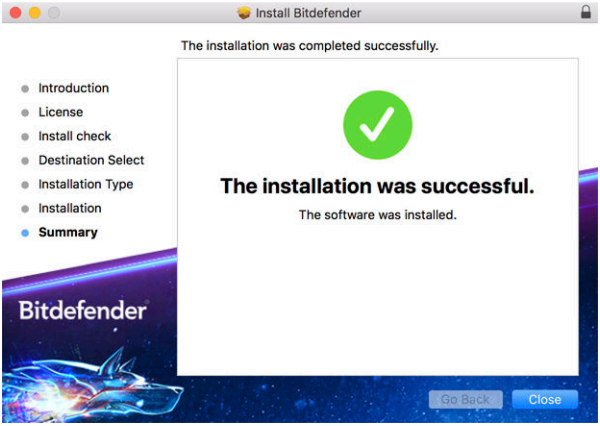
Klik op **Installeren** om de installatie te starten.

Stap 4 - Installeren van Bitdefender Antivirus for Mac



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

Stap 5 - Voltooien



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

De installatieprocedure is nu voltooid.

Belangrijk

- Als u Bitdefender Antivirus for Mac installeert op macOS High Sierra 10.13.0 of een nieuwere versie, verschijnt de melding **Systeemextensie geblokkeerd**. Deze melding informeert u dat de door Bitdefender ondertekende extensies werden geblokkeerd en handmatig moeten worden ingeschakeld. Klik op OK om door te gaan. Klik in het Bitdefender Antivirus voor Mac-venster dat verschijnt op de koppeling **Beveiliging & Privacy**. Klik op **Toestaan** in het onderste deel van het venster of selecteer de Bitdefender SRL in de lijst en klik vervolgens 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 mededeling dat u **Bitdefender volledige schijftoegang moet verlenen** en **Bitdefender moet toestaan te laden**. Volg de instructies op het scherm om het product correct te configureren.

2.3. 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 in **Programma's**, en dubbelklik dan op **BitdefenderUninstaller**.
3. Selecteer de verwijderoptie van uw voorkeur.

   Opmerking
   Als u enkel de Bitdefender VPN-app probeert te verwijderen, vink dan alleen **VPN verwijderen** aan.

4. Klik op **Verwijderen** en wacht tot de verwijdering is uitgevoerd.
5. Klik op **Sluiten** om te eindigen.

   Belangrijk
   Als er een fout optreedt, kunt u contact opnemen met het klantenserviceteam van Bitdefender zoals beschreven in Hulp vragen (pagina 54).

3. AAN DE SLAG

Dit hoofdstuk bevat de volgende onderwerpen:

3.1. Bitdefender Antivirus for Mac openen

Er zijn verschillende manieren om Bitdefender Antivirus for Mac te openen.

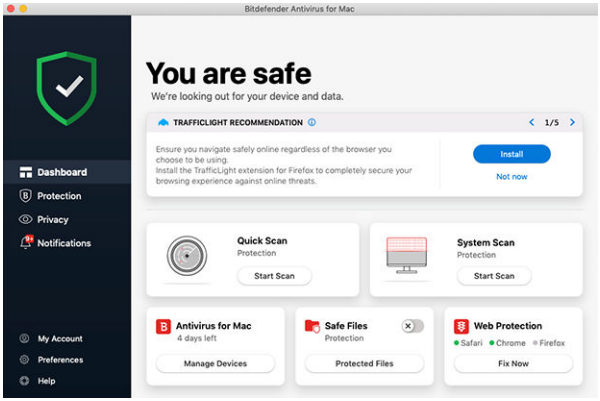
- Klik op het symbool van Bitdefender Antivirus for Mac in de Launchpad.
- Klik op het symbool in de menubalk en kies **Antivirus-interface openen**.
- Open een Finder-venster, ga naar Programma's en dubbelklik op het symbool **Bitdefender Antivirus for Mac**.

> **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 het symbool, en tik dan uw beheerdersgegevens in.
> 3. Er verschijnt een nieuw venster. Versleep het bestand **BDLDaemon** naar de lijst met toegestane toepassingen.

3.2. 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.



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 bovenaan het venster informeert u aan de hand van expliciete berichten en suggestieve kleuren over de beveiligingsstatus van het systeem. Indien Bitdefender Antivirus for Mac geen waarschuwingen bevat, is de statusbalk groen. Wanneer er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statusbalk naar rood. Raadpleeg Problemen oplossen (pagina 26) voor gedetailleerde informatie over problemen en hoe deze op te lossen.

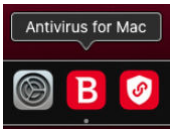
Bitdefender Autopilot is uw persoonlijke beveiligingsadviseur om u bij al uw activiteiten een effectieve werking en verhoogde bescherming te bieden. Naargelang de activiteiten die u uitvoert, of u nu werkt of online betalingen doet, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat. Hiermee kunt u de voordelen van de functies die in de toepassing Bitdefender Antivirus for Mac inbegrepen zijn, ontdekken, en ervan genieten.

Vanuit het navigatiemenu aan de linkerkant hebt u toegang tot de Bitdefender-secties voor gedetailleerde configuratie en geavanceerde beheertaken (**Bescherming** en **Privacy** tabbladen), meldingen, uw

Bitdefender-account en het **Voorkeuren** gedeelte. U kunt ook contact met ons opnemen (**Help** tabblad) voor ondersteuning in het geval u vragen hebt of er iets onverwachts verschijnt.

3.3. Dock-symbool toepassing

Het symbool van Bitdefender Antivirus for Mac is te zien in het Dock zodra u het programma opent. Het symbool in het Dock biedt u een eenvoudige manier om bestanden en mappen te scannen op dreigingen. Sleep het bestand of de map gewoon over het Dock-symbool en de scan begint onmiddellijk.



3.4. Navigatiemenu

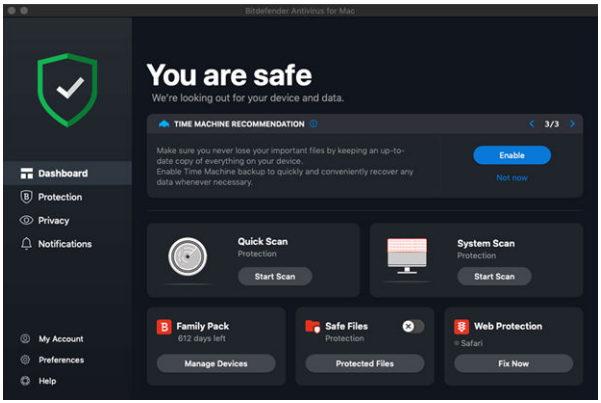
Aan de linkerkant op de Bitdefender-interface staat het navigatiemenu waarmee u snel toegang krijgt tot de functies van Bitdefender voor het gebruik van uw product. Dit zijn de tabbladen die in dit gebied beschikbaar zijn:

- **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**. Vanaf hier kunt u de Bitdefender VPN-app openen en de Anti-tracker-extensie in uw webbrowser installeren.
- **Meldingen**. Van hieruit kunt u details zien over de acties die op gescande bestanden zijn ondernomen.

- **Mijn Account**. Vanaf hier kunt u zien met welk Bitdefender-account en -abonnement uw apparaat wordt beschermd, en kunt indien nodig van account wisselen.
- **Voorkeuren**. Van hieruit 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.

3.5. 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.



4. BESCHERMING TEGEN SCHADELIJKE SOFTWARE

Dit hoofdstuk bevat de volgende onderwerpen:

4.1. Beste praktische toepassingen

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 systeembestanden automatisch worden gescand door Bitdefender Antivirus for Mac.
- Zorg dat uw Bitdefender Antivirus for Mac-product bijgewerkt blijft met de nieuwste informatie over bedreigingen en productupdates.
- Controleer en herstel regelmatig de problemen die door Bitdefender Antivirus for Mac worden gemeld. Raadpleeg Problemen oplossen (pagina 26) voor gedetailleerde informatie.
- Bekijk de gedetailleerde activiteitenlogboeken van Bitdefender Antivirus for Mac op uw computer. Wanneer er iets belangrijks gebeurt

aangaande de beveiliging van uw systeem of gegevens, wordt een nieuw bericht toegevoegd aan het gebied Meldingen van Bitdefender. Raadpleeg Notificaties (pagina 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 (pagina 36) voor meer informatie.

4.2. 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.

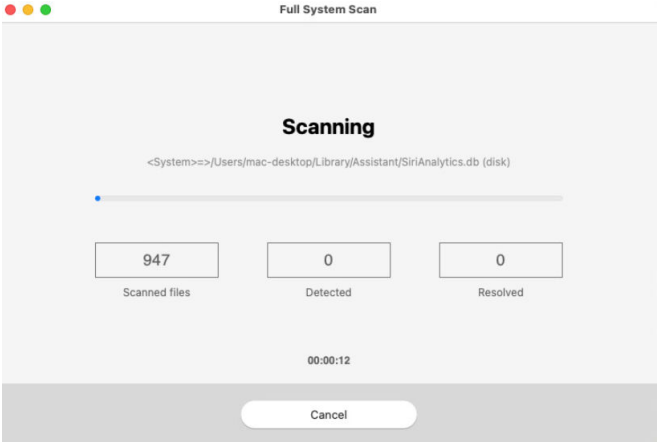
  > **Opmerking**
  > Afhankelijk van de grootte van uw harde schijf kan een scan van het volledige systeem veel tijd in beslag nemen (soms wel een uur, of nog langer). Om de systeemprestaties niet te beïnvloeden, is het aan te raden geen volledige scans te starten terwijl u complexe taken (zoals videobewerking) 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.

4.3. Scanwizard

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



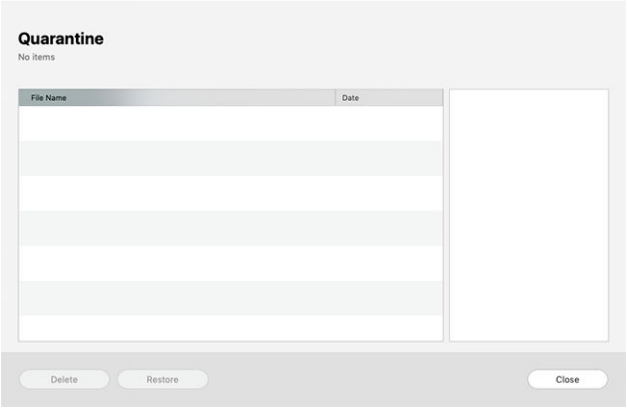
Tijdens elke scan wordt realtime informatie weergegeven over gedetecteerde en verwijderde dreigingen.

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.

4.4. 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.



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 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 **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik op **Openen** in het paneel **Quarantaine**.

4.5. 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:

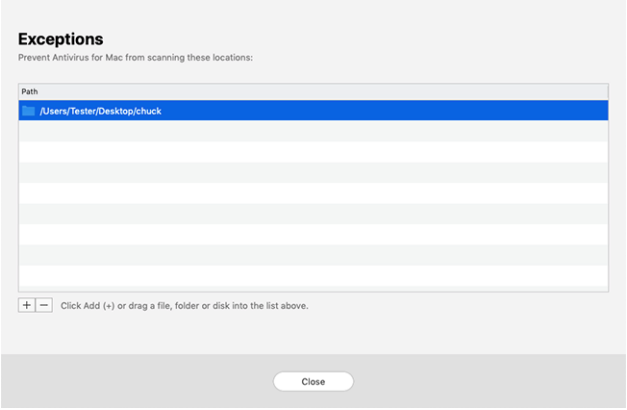
1. Klik in het navigatiemenu in de Bitdefender-interface op **Voorkeuren**.
2. Schakel **Bitdefender Shield** uit in het venster **Bescherming**.

> **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.

4.6. 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



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

Om naar de lijst met uitzonderingen te gaan:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. 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 (-).

4.7. Webbeveiliging

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

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

4.7.1. 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 op 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.

4.7.2. Uitbreidingsinstellingen 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**:

- **Bitdefender TrafficLight Instellingen**
  - 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.

4.7.3. 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 veilige pagina om te bezoeken. U kunt uw werk voortzetten.

⚠ Deze webpagina kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.

⛔ U moet de webpagina onmiddellijk verlaten omdat deze malware of andere dreigingen bevat.

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

4.8. 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 Bitdefender Anti-tracker-extensie 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.

4.8.1. 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.

4.8.2. Interface van Anti-tracker

Wanneer de Bitdefender Anti-tracker-extensie is geactiveerd, verschijnt het symbool naast de zoekbalk in uw webbrowser. Telkens wanneer u een website bezoekt, kunt u op het symbool een teller zien die verwijst naar de gedetecteerde en geblokkeerde trackers. Om meer details over de geblokkeerde trackers te bekijken, klikt u op het symbool om de interface te openen. Naast het aantal geblokkeerde trackers kunt u de tijd zien die nodig is om de pagina te laden en de categorieën waartoe de gedetecteerde trackers behoren. Om de lijst met websites die tracken te bekijken, 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.

4.8.3. Bitdefender Anti-tracker uitschakelen

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

1. Open uw webbrowser.
2. Klik op het symbool naast de adresbalk in uw webbrowser.
3. Klik op het symbool in de rechterbovenhoek.
4. Gebruik de bijhorende schakelaar om uit te schakelen.
   Het Bitdefender-pictogram wordt dan grijs.

4.8.4. 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 symbool naast de zoekbalk.
3. Klik op de pictogram in de rechterbovenhoek.
4. Als u zich op de website bevindt waarop u uitzonderingen wilt toevoegen, klikt u op **Voeg de huidige website toe aan de lijst**.
   Als u nog een website wilt toevoegen, typt u het adres in het overeenkomstige veld en klikt u op .

4.9. Safe Files

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 Safe Files 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 **Bescherming** in het navigatiemenu op de Bitdefender-interface.
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**.

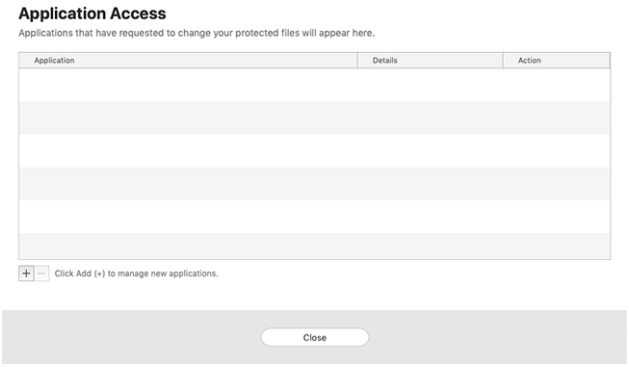
4.9.1. Toegang applicatie

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 **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Anti-ransomware** tabblad.
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.



4.10. 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.

4.10.1. 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 de **Anti-ransomware** tabblad.
3. Schakel de schakelaar **Time Machine Bescherming** in of uit.

4.11. 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.

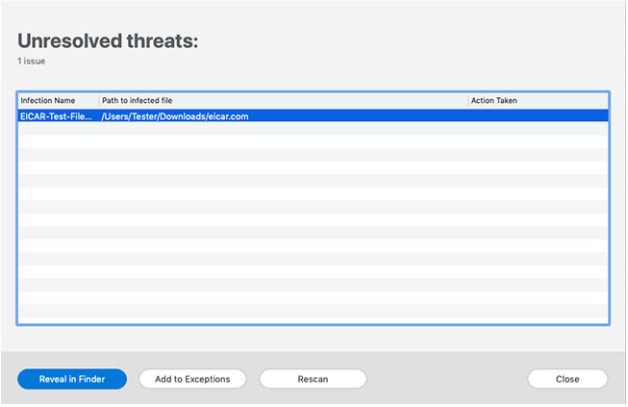
Onder andere deze problemen kunnen worden gemeld:

- 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.



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 verwijderen**. Onderneem deze actie om de infecties handmatig te verwijderen.
- **Toevoegen aan uitzonderingen**. Deze actie is niet beschikbaar voor dreigingen die worden gevonden in archieven.

4.12. Notificaties

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw computer. Wanneer er iets gebeurt dat van belang is voor de veiligheid van uw systeem of uw gegevens, wordt er een nieuw bericht toegevoegd aan het gebied Meldingen van 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.

4.13. Updates

Er worden dagelijks 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 up-to-date is, kan het de nieuwste dreigingen die door Bitdefender Labs zijn ontdekt, niet detecteren en verwijderen.

4.13.1. 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. 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.

4.13.2. 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.

4.13.3. 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.

4.13.4. Informatie vinden over Bitdefender Antivirus for Mac

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. Bitdefender Antivirus for Mac openen.
2. Klik op Bitdefender Antivirus for Mac in de menubalk en kies **Over Antivirus for Mac**.

5. VPN

Dit hoofdstuk bevat de volgende onderwerpen:

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-app kan worden geïnstalleerd vanuit uw Bitdefender-product en worden gebruikt telkens wanneer u een extra beschermingslaag wilt toevoegen aan uw verbinding. De VPN dient als een tunnel tussen uw apparaat en het netwerk waarmee u verbinding maakt, en beveiligt uw verbinding, versleutelt de gegevens met behulp van encryptie op bankniveau en verbergt uw IP-adres waar u ook bent. Uw verkeer wordt omgeleid via een aparte server; zo wordt het vrijwel onmogelijk om uw apparaat te identificeren via de talloze andere apparaten die onze diensten gebruiken. Bovendien hebt u, terwijl u via Bitdefender VPN met het internet bent verbonden, toegang tot inhoud die normaal gesproken beperkt is in specifieke 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 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 Openen

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

- Klik in het navigatiemenu in de **Bitdefender-interface** op **Privacy**. Klik op **Openen** in de Bitdefender VPN-kaart.
- Klik op het symbool in de menubalk.
- Ga naar de map Toepassingen, open de map Bitdefender en dubbelklik op het Bitdefender VPN-symbool.

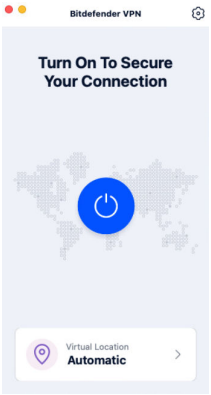
De eerste keer dat u de toepassing opent, wordt u gevraagd Bitdefender toe te staan configuraties toe te voegen. Door aan Bitdefender deze toestemming te verlenen, stemt u ermee in dat alle netwerkactiviteiten op uw apparaat worden gefilterd of gemonitord wanneer u de VPN-toepassing gebruikt.

Opmerking
De Bitdefender VPN-app kan alleen worden geïnstalleerd op macOS Sierra (10.12.6), macOS High Sierra (10.13.6) of macOS Mojave (10.14) of latere versies van het besturingssysteem.

5.3. 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 {1} {2}.

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



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** - 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:
  - **Algemeen**
    - Meldingen - Productmeldingen weergeven.
    - Een opstart uitvoeren - Bitdefender VPN automatisch starten bij het inloggen.
    - Productrapporten - Stuur anonieme productrapporten door om ons te helpen uw ervaring en beschermingsmogelijkheden te verbeteren.
  - **Geavanceerd**
    - Internet Kill-Switch - Onderbreekt tijdelijk al het internetverkeer, als de VPN-verbinding ongewild uitvalt.
    - Ad blocker en Anti-tracker - Blokkeer advertenties en trackers om te genieten van een schoner en sneller web.
    - Split tunneling - Geselecteerde websites omzeilen de VPN en verbinden rechtstreeks met het internet.

> **Opmerking**
> Klik op **Beheren** en dan **Website toevoegen** om webpagina's aan deze lijst toe te voegen.

- Autoconnect - Het VPN automatisch verbinden wanneer:
  - Aan het verbinden met een onbeveiligd of openbaar wifinetwerk.
  - Er werd een app voor peer-to-peer bestandsuitwisseling geopend.

- **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 app verlaten.

5.4. Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om de 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 staat los van het itdefender Antivirus for Mac-abonnement, wat betekent dat u het kunt gebruiken zolang het beschikbaar is, ongeacht de status van het beveiligingsabonnement. Als het Bitdefender Premium VPN-abonnement afloopt, maar het abonnement voor Bitdefender Antivirus for Mac nog steeds actief is, wordt u teruggezet naar het gratis plan.

Bitdefender VPN is een cross-platform product en is beschikbaar in de 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.

6. VOORKEUREN INSTELLEN

Dit hoofdstuk bevat de volgende onderwerpen:

6.1. Voorkeuren weergeven

Om het voorkeurenvenster van Bitdefender Antivirus for Mac te openen:

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

6.2. 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 dreigingen door alle geïnstalleerde toepassingen, hun bijgewerkte versies en nieuwe en gewijzigde bestanden te scannen. We raden u aan om Bitdefender Shield niet uit te schakelen, maar als het toch moet, doe het dan zo kort mogelijk. Als Bitdefender Shield is uitgeschakeld, bent u niet beschermd tegen dreigingen.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Schakel dit selectievakje in om Bitdefender Antivirus for Mac in te stellen om alleen bestanden te scannen die niet eerder zijn gescand of die sinds de laatste scan gewijzigd zijn.

Als u wilt, kunt u deze instelling negeren voor scans die worden gestart door middel van slepen en neerzetten. Schakel hiervoor het selectievakje uit.

- **Inhoud in back-ups niet scannen.** Schakel dit selectievakje in 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.

6.3. 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 op de gedetecteerde bestanden.

6.4. 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 **Voorkeuren** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer het tabblad **Andere**.

3. Schakel de schakelaar **Mijn aanbiedingen** in of uit.

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

7. OVER BITDEFENDER CENTRAL

Bitdefender Central is het platform dat u toegang geeft tot de online functies en diensten van het product. Vanuit dit platform kunt u vanop afstand belangrijke taken uitvoeren op de apparaten 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-app 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 voor Mac
  - De Bitdefender Windows-productlijn
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Voeg nieuwe apparaten toe aan uw netwerk en beheer deze apparaten, waar u ook bent.

7.1. Toegang tot Bitdefender Central

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 hoofdinterface 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:
  1. Open de Bitdefender Central-app die u hebt geïnstalleerd.

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

7.2. Twee-factorenauthenticatie

De twee-factorenauthenticatiemethode 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.

7.2.1. Twee-factorenauthenticatie activeren

Door de twee-factorenauthenticatie 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 op het pictogram rechtsboven op het scherm.
3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.

5. Kik op **AAN DE SLAG**.
   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 **DOORGAAN**.

     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.
   In het geval u ervoor hebt gekozen om de authenticatiecode te ontvangen via e-mail, hebt u vijf minuten om uw e-mailaccount te controleren en de gegenereerde code in te tikken. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.

3. Bevestig uw keuze.

7.3. 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. Toegang Bitdefender Centraal.
2. Klik op de pictogram in de rechterbovenhoek van het scherm.
3. Klik **Bitdefender-account** in het diamenu.
4. Selecteer de **Wachtwoord en veiligheid** tabblad.
5. Klik op **Vertrouwde apparaten**.
6. De lijst van de apparaten waar Bitdefender op geïnstalleerd is, wordt weergegeven. Klik op het gewenste apparaat.

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

7.4. 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.

7.4.1. Toevoeging van een nieuw apparaat

Indien uw abonnement meer dan één toestel dekt, kunt u een nieuw toestel toevoegen en uw Bitdefender Antivirus for Mac erop installeren, als volgt:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel en tik vervolgens op **INSTALLEER BESCHERMING**.

3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
   - **Bescherm andere apparaten**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
     Druk op **DOWNLOADKOPPELING VERZENDEN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**. De gegenereerde downloadkoppeling is slechts 24 uur geldig. Indien de koppeling vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.
     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en tik vervolgens op de overeenkomstige downloadknop.
4. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

7.4.2. Uw apparaten aanpassen

Om uw apparaten beter te kunnen herkennen, kunt u de apparaatnaam aanpassen:

1. Toegang Bitdefender Centraal.
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 apparaten, om het beheer te vergemakkelijken:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.

3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram 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 lijst **Apparaateigenaar** en klik op **TOEWIJZEN**.

7.4.3. Beheer op afstand

Bitdefender van op afstand op een apparaat updaten:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram in de rechterbovenhoek van het scherm.
4. Selecteer **Update**.

Voor meer acties van op afstand en informatie over uw Bitdefender-product op een specifiek toestel, klik op de gewenste toestelkaart.

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

- **Dashboard.** In dit venster kunt u de gegevens van het geselecteerde apparaat bekijken, de beschermingsstatus en de Bitdefender VPN-status controleren 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
- **Bescherming.** In dit tabblad kunt u op afstand een snelle of systeemscan 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.

- **Optimalisatie.** Hier kunt u op afstand de prestaties van een apparaat verbeteren door snel te scannen, nutteloze bestanden te detecteren en op te schonen. Klik op de **START** knop, en selecteer vervolgens de gebieden die u wilt optimaliseren. Klik nogmaals op de knop **START** om het optimalisatieproces te starten. Klik op **Meer details** voor een gedetailleerd rapport over de opgeloste problemen.
- **Anti-diefstal.** In geval van misplaatsing, diefstal of verlies kunt u met de anti-diefstalfunctie uw apparaat lokaliseren en op afstand acties ondernemen. Klik op **LOKALISEREN** om de positie van het apparaat te achterhalen. De laatst bekende positie wordt weergegeven, samen met de tijd en datum.
- **Kwetsbaarheid.** Om een apparaat te controleren op kwetsbaarheden zoals ontbrekende Windows-updates, verouderde apps of zwakke wachtwoorden klikt u op de knop **SCANNEN** in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet op afstand worden verholpen. Als er een kwetsbaarheid wordt gevonden, moet u een nieuwe scan uitvoeren op het apparaat en vervolgens de aanbevolen acties ondernemen. Klik op **Meer details** voor een gedetailleerd rapport over de gevonden problemen.

7.5. 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 kunt u het aantal aangesloten apparaten en hun beschermingsstatus bekijken. Om problemen met de gedetecteerde apparaten op afstand op te lossen, klikt u op **Problemen oplossen** en vervolgens op **SCANNEN EN PROBLEMEN OPLOSSEN**.
  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.
- **Dreigingen 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.

7.6. Mijn abonnementen

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

7.6.1. Controleer beschikbare abonnementen

Zo controleert u uw beschikbare abonnementen:

1. Toegang Bitdefender Centraal.
2. Ga naar het paneel **Mijn abonnementen**.

Hier vindt u informatie over de beschikbaarheid van uw abonnementen en het aantal apparaten dat gebruikmaakt van deze abonnementen.

U kunt een nieuw apparaat aan een abonnement toevoegen of een abonnement verlengen door een abonnementskaart te selecteren.

> **Opmerking**
> U kunt een of meer lidmaatschappen op uw account hebben, op voorwaarde dat ze voor verschillende platforms bestemd zijn (Windows, macOS, iOS of Android).

7.6.2. 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.

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

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
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.

7.6.3. Abonnement verlengen

Indien u automatische verlenging voor uw Bitdefender-abonnement hebt uitgeschakeld, kunt u het handmatig verlengen via de volgende stappen:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Selecteer de gewenste abonnementskaart.
4. Klik op **VERLENGEN** om door te gaan.

In uw webbrowser wordt een webpagina geopend waar u uw Bitdefender-abonnement kunt verlengen.

7.7. Meldingen

Om u op de hoogte te houden van wat er gebeurt op de apparaten die aan uw account gekoppeld zijn, hebt u de -icoon ter beschikking. Zodra u erop klikt, krijgt u een algemeen beeld met informatie over de activiteit van de Bitdefender-producten die op uw apparaten geïnstalleerd zijn.

8. VEELGESTELDE VRAGEN

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

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:
   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 **MAAK ACCOUNT AAN**.
2. Download Bitdefender Antivirus for Mac als volgt:
   a. Selecteer de **Mijn apparaten** paneel en klik vervolgens op **INSTALLEER BESCHERMING**.
   b. Kies een van de twee beschikbare opties:
      - **Bescherm dit apparaat**
        i. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
        ii. Sla het installatiebestand op.
      - **Bescherm andere apparaten**
        i. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.

ii. Klik **STUUR DOWNLOADLINK**.

iii. Typ een e-mailadres in het overeenkomstige veld en klik **STUUR E-MAIL**.
Houd er rekening mee dat de gegenereerde downloadlink alleen de komende 24 uur geldig is. Als de link verloopt, moet u een nieuwe genereren door dezelfde stappen te volgen.

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

c. Voer het Bitdefender-product uit dat u hebt gedownload.

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

Als u een activeringscode hebt gekocht bij een van onze wederverkopers of als cadeau hebt gekregen, kunt u de beschikbaarheid ervan toevoegen aan uw Bitdefender-abonnement.

Volg deze stappen om een abonnement te activeren met een activeringscode:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Klik op de **ACTIVATIE CODE** en typ vervolgens de code in het overeenkomstige veld.
4. Klik **ACTIVEREN** doorgaan.

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 de geïnfecteerd bestanden later worden 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 updaten via een Proxyserver?

Bitdefender Antivirus for Mac kan alleen worden bijgewerkt via proxyservers die geen authenticatie vereisen. U hoeft geen programma-instellingen te configureren.

Als u verbinding maakt met internet via een proxyserver die authenticatie vereist, moet u regelmatig overschakelen naar een directe internetverbinding om updates over bedreigingsinformatie te verkrijgen.

Hoe verwijder ik Bitdefender Antivirus for Mac?

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 BitdefenderUninstaller.

3. Klik **Verwijderen** en wacht tot het proces is voltooid.
4. Klik **Dichtbij** af te maken.

> **Belangrijk**
> Als er een fout optreedt, kunt u contact opnemen met de Bitdefender Klantenservice zoals beschreven in Hulp vragen (pagina 54).

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

- Zo verwijdert u de TrafficLight-extensies uit Mozilla Firefox:
  1. Ga naar **Hulpprogramma's** 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 **Meer hulpprogramma's** en selecteer **Extensies**.
  3. Klik op het symbool **Verwijderen** naast de extensie die u wilt verwijderen.
  4. Klik op **Verwijderen** om de verwijdering te bevestigen.
- Volg deze stappen om Bitdefender TrafficLight uit Safari te verwijderen:
  1. Ga naar **Voorkeuren** of druk op **Command-Comma(,)**.
  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.

9. HULP VRAGEN

9.1. Hulp vragen

Bitdefender biedt zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning. Als u een probleem ondervindt of een vraag hebt over uw Bitdefender-product, kunt u verschillende online bronnen gebruiken om een oplossing of een antwoord te vinden. Tegelijkertijd kunt u contact opnemen met het klantenserviceteam van Bitdefender. Onze ondersteuningsmedewerkers zullen uw vragen tijdig beantwoorden en u de hulp bieden die u nodig hebt.

9.2. Online bronnen

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

- Bitdefender Support Center:
  https://www.bitdefender.nl/consumer/support/
- De Community van Bitdefender-experts:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

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

9.2.1. Bitdefender Support Center

Het Bitdefender Support Center 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 dreigingspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De Bitdefender Support Center 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 de Bitdefender Support Center als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Support Center is te allen tijde beschikbaar op het volgende adres: https://www.bitdefender.nl/consumer/support/.

9.2.2. De Community van Bitdefender-experts

De Community van Experts is een omgeving waar gebruikers, enthousiastelingen en fans van Bitdefender aan kunnen deelnemen, waar ze ideeën kunnen uitwisselen, elkaar kunnen ondersteunen en hun kennis en oplossingen kunnen delen. Het is ook een plaats voor brainstorming en een bron van waardevolle feedback aan onze ontwikkelingsteams. De leden van de gemeenschap zijn ervaren Bitdefender-gebruikers die in hun eigen tijd graag anderen helpen. Met hun enorme bijdrage en oprechte vrijwillige inspanningen hebben we een kennisbank gecreëerd waar gebruikers antwoorden en begeleiding kunnen vinden, maar met dat menselijke tintje.

Hier vindt u zinvolle gesprekken met mensen die Bitdefender gebruiken op hun apparaten. De gemeenschap biedt een echte band met onze leden en laat uw stem horen. Het is een plek waar u wordt aangemoedigd om deel te nemen in de wetenschap dat uw mening en inbreng worden gerespecteerd en gekoesterd. Als gewaardeerde provider streven we ernaar een ongeëvenaard niveau van snelle, accurate ondersteuning te bieden en willen we onze gebruikers dichter bij ons brengen. Wij hebben onze gemeenschap met dit doel voor ogen ontworpen.

U vindt de website van onze Community van experts hier:

https://community.bitdefender.com/en/

9.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia heeft alle informatie die u nodig hebt over de nieuwste cyberdreigingen. Dit is de plaats waar Bitdefender-experts tips en trucs delen over hoe u beschermd kunt blijven tegen hackers, datalekken, identiteitsdiefstal en pogingen tot sociale imitatie.

De webpagina van Bitdefender Cyberpedia vindt u hier:

https://www.bitdefender.com/cyberpedia/.

9.3. Contactinformatie

Efficiënte communicatie is de sleutel tot succes. Sinds 2001 heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners telkens te overtreffen. Aarzel daarom niet om rechtstreeks contact met ons op te nemen als u iets wilt vragen, via onze Bitdefender Support Center.

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

9.3.1. 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.

Om een Bitdefender-verdeler te vinden in uw land:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.

WOORDENLIJST

Activeringscode

Is een unieke sleutel die u in de handel kunt kopen en die gebruikt wordt om een specifiek product of een dienst te activeren. Met een activeringscode kan een geldig abonnement voor een bepaalde periode en een bepaald aantal toestellen geactiveerd worden en kunt u ook gebruiken om het abonnement te verlengen, op voorwaarde dat het voor hetzelfde product of dezelfde dienst is.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic. ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Advanced persistent threat

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze bedreiging. Het doel van een advanced persistent threat is heel lang onopgemerkt te blijven en belangrijke informatie in te kijken en te verzamelen, zonder de toestellen te beschadigen. De methode die gebruikt wordt om de bedreiging in het netwerk te brengen verloopt via een pdf-bestand of een Office-document dat er onschuldig uitziet, zoadat elke gebruiker de bestanden kan openen.

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.

Archive

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Backdoor

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Boot sector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Boot virus

Een bedreiging die de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal de bedreiging actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal de bedreigingen telkens in het geheugen geactiveerd zijn.

Botnet

Het woord "botnet" is samengesteld uit de woorden "robot" en "netwerk". Botnets zijn apparaten die met het internet verbonden zijn en met bedreigingen geïnfecteerd zijn en kunnen gebruikt worden om spammail te verzenden, data te stelen, kwetsbare apparaten van op afstand

te controleren of om spyware, ransomware en andere schadelijke bedreigingen te verspreiden. Het doel ervan is zoveel mogelijk apparaten te infecteren, bijvoorbeeld pc's, servers, mobiele of IoT-apparaten die eigendom zijn van grote bedrijven of sectoren.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. Populaire browsers omvatten Microsoft Internet Explorer, Mozilla Firefox en Google Chrome. Dit zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

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.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookies

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

Cyberpesten

Wanneer collega's of onbekenden met opzet onrechtmatige daden stellen tegenover kinderen, met de bedoeling om fysiek te kwetsen. Om emotionele schade te berokkenen, sturen de daders gemene berichten of onflatteuze foto's om hun slachtoffers af te zonderen van anderen of gefrustreerd te doen voelen.

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.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf. Een harde-schijfstation leest en schrijft harde schijven. Een diskettestation opent diskettes. Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Download

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Exploits

Een manier om misbruik te maken van verschillende bugs of kwetsbaarheden in een computer (software of hardware). Zo kunnen hackers de controle over computers of over netwerken in handen krijgen.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid. Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe bedreigingen op basis van regels. Deze scanmethode is niet gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaande bedreiging. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Honeypot

Een afleiding in uw computersysteem dat hackers aantrekt om te onderzoeken hoe ze te werk gaan en de afwijkende methodes die ze gebruiken om systeeminformatie te verzamelen, te identificeren. Bedrijven zijn steeds meer geïnteresseerd om honingpotten te implementeren en te gebruiken om hun algemene beveiligingsstatus te verbeteren.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

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).

Macro virus

Een type computerbedreiging die is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen. Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mail client

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode is gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de niet-heuristische scan is dat deze zich niet laat misleiden door iets dat kan lijken op een bedreiging en geen vals alarm genereert.

Online predatoren

Personen die minderjarigen of adolescenten met opzet willen betrekken in gesprekken, om hen zo te betrekken in illegale seksuele activiteiten. Sociale netwerken zijn de ideale plaats waar kwetsbare kinderen gemakkelijk kunnen worden verleid om seksuele activiteiten uit te voeren, online of tijdens fysieke ontmoetingen.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt, zoals wachtwoorden en

creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Foton

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van uw beveiligingsoplossing op de prestaties te beperken. Door de activiteit van uw pc's op de achtergrond te bewaken, maakt het gebruikspatronen die helpen opstart- en scanprocessen te optimaliseren.

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.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

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-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.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad,

het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een verzameling softwareprogramma's die op beheerdersniveau toegang biedt tot een systeem. Deze term werd voor het eerst gebruikt voor Unix-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die beheerdersrechten gaven aan indringers, zodat ze hun aanwezigheid konden verbergen en onzichtbaar bleven voor de echte systeembeheerders.

De belangrijkste functie van rootkits is het verbergen van processen, bestanden, logins en logbestanden. Rootkits die de hiervoor benodigde software bevatten, kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten.

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 bedreigingen of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met bedreigingen, 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.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

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 waarbij men het slachtoffer wordt van spyware is bepaalde P2P-programma's voor bestandsuitwisseling 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.

Startup items

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of apps. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Abonnement

Koopovereenkomst die u het recht heeft om een specifiek(e) product of dienst op een specifiek aantal toestellen en voor een bepaalde tijd te gebruiken. Een vervallen abonnement kan automatisch worden verlengd met gebruik van de informatie van de gebruiker tijdens de eerste aankoop.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Dreiging

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.

informatie-updates van dreigingen

Het binaire patroon van een bedreiging, gebruikt door de beveiligingsoplossing om de bedreiging te detecteren en te verwijderen.

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 naam komt uit een verhaal uit de Ilias van Homerus. De Grieken schonken hun vijanden, de Trojanen, een reusachtig houten paard, zogenaamd als vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten uit de holle romp van het paard tevoorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatefunctie waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virtueel privénetwerk (VPN)

Dit is een technologie die een tijdelijke en versleutelde rechtstreekse verbinding met een zeker netwerk over een minder beveiligd netwerk mogelijk maakt. Op die manier is het verzenden en ontvangen van data veilig en versleuteld, zodat ze moeilijk te vangen is door spionnen. Een bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Worm

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