Bitdefender®

ANTIVIRUS PLUS 2017

HANDLEIDING

Bitdefender Antivirus Plus 2017
Handleiding

Publication date 05/10/2017

Kennisgevingen

Bitdefender

Inhoudsopgave

INSTALLATIE

1. VOORBEREIDEN VOOR INSTALLATIE

Voordat u Bitdefender Antivirus Plus 2017 installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de computer waarop u Bitdefender wilt installeren, voldoet aan de minimale systeemvereisten. Als de computer niet voldoet aan alle minimale systeemvereisten, wordt Bitdefender niet geïnstalleerd. Als het programma als is geïnstalleerd, zal het niet goed werken en zal het systeem vertragen en instabiel worden. Raadpleeg "*Systeemvereisten*" (p. 3) voor een complete lijst van systeemvereisten.
- Meld u aan bij de computer met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de computer. Indien iets wordt opgemerkt tijdens het Bitdefender-installatieproces, zult u een bericht krijgen om het te verwijderen. Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Defender zal uitgeschakeld zijn tijdens de installatie.
- Het wordt aanbevolen uw computer verbonden te laten met Internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

2. SYSTEEMVEREISTEN

U kan Bitdefender Antivirus Plus 2017 uitsluitend installeren op computers met de volgende besturingssystemen:

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

Controleer vóór de installatie of uw computer voldoet aan de minimum systeemvereisten.

Opmerking

Om na te gaan welk Windows-besturingssysteem op uw computer wordt uitgevoerd en voor hardwaregegevens:

- In **Windows 7**, gebruikt u een rechtermuisklik op **Mijn Computer** op het bureaublad en daarna selecteert u **Eigenschappen** in het menu.
- Zoek in **Windows 8** vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm) en rechterklik op het pictogram ervan. Zoek in **Windows 8.1**, naar **Deze computer**.

  Selecteer **Eigenschappen** in het onderste menu. Zoek in **Systeem** naar informatie over uw systeemtype.
- In **Windows 10**, typt u **Systeem** in het zoekveld in de taakbalk en klikt u op het pictogram ervan. Zoek in **Systeem** naar informatie over uw systeemtype.

2.1. Minimale systeemvereisten

- 1.5 GB beschikbare harde schijfruimte
- Dual Core 1,6 GHz processor
- 1 Gb geheugen (RAM)

2.2. Aanbevolen systeemvereisten

- 2 Gb beschikbare vrije ruimte op de harddisk (ten minste 800 Mb op de systeemschijf)
- Intel CORE Duo (2 GHz) of equivalente processor
- 2 GB geheugen (RAM)

2.3. Softwarevereisten

Om Bitdefender te kunnen gebruiken, evenals alle functies ervan, moet uw computer voldoen aan de volgende softwarevereisten:

- Internet Explorer 10 of hoger
- Mozilla Firefox 30 of hoger
- Google Chrome 34 of hoger
- Skype 6.3 of hoger

3. UW BITDEFENDER-PRODUCT INSTALLEREN

U kunt Bitdefender installeren vanaf de installatiedisk of via de web installer die u naar uw computer kunt downloaden vanaf de Bitdefender Central.

Indien uw aankoop voor meer dan één computer is (u kocht bijvoorbeeld Bitdefender Antivirus Plus 2017 voor 3 PC's), herhaal het installatieproces dan en activeer uw product met dezelfde account op elke computer. De account die u moet gebruiken, is deze die uw actieve abonnement van Bitdefender bevat.

3.1. Installeren vanaf Bitdefender Central

Via de Bitdefender Central kunt u de installatiekit die met het aangekochte abonnement overeenkomt, downloaden. Zodra het installatieproces voltooid is, is Bitdefender Antivirus Plus 2017 geactiveerd.

Om Bitdefender Antivirus Plus 2017 te downloaden via Bitdefender Central:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik in het venster **MIJN APPARATEN** op **Bitdefender INSTALLEREN**.
4. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

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

     Selecteer **Windows** om uw Bitdefender-product te downloaden en klik vervolgens op **VERDERGAAN**. Voer een e-mailadres in in het overeenkomstige veld en klik op **VERZENDEN**.
5. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

Als uw systeem niet voldoet aan de minimumvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibel antivirusprogramma of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw computer opnieuw moeten opstarten om het verwijderen van de gedetecteerde antivirusprogramma's te voltooien.

Het Bitdefender Antivirus Plus 2017 installatiepakket wordt voortdurend bijgewerkt.

Opmerking
Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Antivirus Plus 2017 te installeren.

Stap 1 - Installatie Bitdefender

In het Bitdefender-installatiescherm kunt u kiezen welk type installatie u wenst uit te voeren.

Voor een volledig probleemloze installatie-ervaring, klikt u gewoon op de knop **INSTALLEREN**. Bitdefender zal worden geïnstalleerd in de standaardlocatie en met de standaardinstellingen en u zult rechtstreeks naar Stap 3 van de wizard gaan.

Als u de installatie-instellingen wilt configureren, klikt u op **AANGEPASTE INSTALLATIE**.

In deze stap kunnen drie bijkomende taken uitgevoerd worden:

- Lees de Overeenkomst voor de eindgebruiker voor u met de installatie verder gaat. De licentieovereenkomst bevat de voorwaarden en bepalingen voor uw gebruik van Bitdefender Antivirus Plus 2017.

  Sluit het venster als u niet akkoord gaat met deze voorwaarden. Het installatieproces wordt afgebroken en u verlaat de installatie.

- Zorg ervoor dat de optie **Anonieme rapporten verzenden** geactiveerd blijft. Door deze optie toe te staan, worden rapporten met informatie over uw gebruik van het product naar de Bitdefender-servers verzonden. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen. Merk op

dat deze rapporten geen vertrouwelijke gegevens, zoals uw naam of IP-adres, bevatten en niet zullen worden gebruikt voor commerciële doeleinden.

- Selecteer de taal waarin u het product wenst te installeren.

Stap 2 - Installatie-instellingen aanpassen

> **Opmerking**
> Deze stap verschijnt alleen indien u er tijdens de vorige stap voor hebt gekozen de installatie aan te passen.

De volgende opties zijn beschikbaar:

Installatiepad
Standaard wordt Bitdefender Antivirus Plus 2017 geïnstalleerd in C:\Program Files\Bitdefender\Bitdefender 2017. Als u het installatiepad wilt wijzigen, klikt u op **WIJZIGEN** en selecteert u de map waarin u Bitdefender wilt installeren.

Proxy-instellingen configureren
Bitdefender Antivirus Plus 2017 vereist internettoegang om het product te activeren, beveiliging en productupdates, opsporingscomponenten in de cloud enz. te downloaden. Als u een Proxyverbinding gebruikt in plaats van een directe internetverbinding, activeert u de bijhorende schakelaar en configureert u de proxy-instellingen.

De instellingen kunnen worden geïmporteerd vanaf de standaardbrowser of u kunt ze handmatig invoeren.

Computer scannen tijdens installatie
Schakel deze optie uit indien u niet wilt dat uw systeem wordt gescand tijdens de installatie van het Bitdefender-product.

Klik op **INSTALLEREN** om uw voorkeuren te bevestigen en begin met de installatie. Indien u zich bedenkt, klik op de **BACK**-knop.

Stap 3 - Installatie bezig

Wacht tot de installatie is voltooid. Er wordt gedetailleerde informatie over de voortgang weergegeven.

Kritieke zones op uw systeem worden gescand op virussen, de nieuwste versies van de toepassingsbestanden worden gedownload en geïnstalleerd

en de services van Bitdefender worden gestart. Deze stap kan enkele minuten duren.

Stap 4 - Installatie voltooid

Uw Bitdefender-product werd met succes geïnstalleerd.

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie actieve malware wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn. Klik op **STARTEN MET Bitdefender** om verder te gaan.

Stap 5 - Aan de slag

In het venster **Aan de slag** kunt u de details van uw abonnement bekijken.

Klik op **VOLTOOIEN** om naar de Bitdefender Antivirus Plus 2017-interface te gaan.

3.2. Installeren vanaf de installatiedisk

Om Bitdefender te installeren vanaf de installatieschijf, plaatst u de schijf in het optische station.

Binnen enkele seconden moet een installatiescherm verschijnen. Volg de instructies om de installatie te starten.

Indien het installatiescherm niet verschijnt, gebruik Windows Explorer om naar de rootdirectory van de schijf te gaan en dubbelklik op het bestand autorun.exe.

Indien uw internetsnelheid traag is of uw systeem niet met het internet verbonden is, klikt u op de knop **Installeren vanaf cd/dvd**. In dat geval zal het Bitdefender-product dat op de disk beschikbaar is, geïnstalleerd worden, terwijl een nieuwere versie zal gedownload worden vanaf de Bitdefender-servers via de productupdate.

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

Als uw systeem niet voldoet aan de minimumvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibel antivirusprogramma of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw computer opnieuw moeten opstarten om het verwijderen van de gedetecteerde antivirusprogramma's te voltooien.

Opmerking
Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Antivirus Plus 2017 te installeren.

Stap 1 - Installatie Bitdefender

In het Bitdefender-installatiescherm kunt u kiezen welk type installatie u wenst uit te voeren.

Voor een volledig probleemloze installatie-ervaring, klikt u gewoon op de knop **INSTALLEREN**. Bitdefender zal worden geïnstalleerd in de standaardlocatie en met de standaardinstellingen en u zult rechtstreeks naar Stap 3 van de wizard gaan.

Als u de installatie-instellingen wilt configureren, klikt u op **AANGEPASTE INSTALLATIE**.

In deze stap kunnen drie bijkomende taken uitgevoerd worden:

- Lees de Overeenkomst voor de eindgebruiker voor u met de installatie verder gaat. De licentieovereenkomst bevat de voorwaarden en bepalingen voor uw gebruik van Bitdefender Antivirus Plus 2017.

  Sluit het venster als u niet akkoord gaat met deze voorwaarden. Het installatieproces wordt afgebroken en u verlaat de installatie.

- Zorg ervoor dat de optie **Anonieme rapporten verzenden** geactiveerd blijft. Door deze optie toe te staan, worden rapporten met informatie over uw gebruik van het product naar de Bitdefender-servers verzonden. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen. Merk op dat deze rapporten geen vertrouwelijke informatie bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen gebruikt worden.

- Selecteer de taal waarin u het product wenst te installeren.

Stap 2 - Installatie-instellingen aanpassen

> **Opmerking**
> Deze stap verschijnt alleen indien u er tijdens de vorige stap voor hebt gekozen de installatie aan te passen.

De volgende opties zijn beschikbaar:

Installatiepad
Standaard wordt Bitdefender Antivirus Plus 2017 geïnstalleerd in C:\Program Files\Bitdefender\Bitdefender 2017\. Als u het installatiepad wilt wijzigen, klikt u op **WIJZIGEN** en selecteert u de map waarin u Bitdefender wilt installeren.

Proxy-instellingen configureren
Bitdefender Antivirus Plus 2017 vereist internettoegang om het product te activeren, beveiliging en productupdates, opsporingscomponenten in de cloud enz. te downloaden. Als u een Proxyverbinding gebruikt in plaats van een directe internetverbinding, activeert u de bijhorende schakelaar en configureert u de proxy-instellingen.

De instellingen kunnen worden geïmporteerd vanaf de standaardbrowser of u kunt ze handmatig invoeren.

Computer scannen tijdens installatie
Schakel deze optie uit indien u niet wilt dat uw systeem wordt gescand tijdens de installatie van het Bitdefender-product.

Klik op **INSTALLEREN** om uw voorkeuren te bevestigen en begin met de installatie. Indien u zich bedenkt, klik op de **BACK**-knop.

Stap 3 - Installatie bezig

Wacht tot de installatie is voltooid. Er wordt gedetailleerde informatie over de voortgang weergegeven.

Cruciale gebieden op uw systeem worden gescand op virussen en de Bitdefender-diensten worden gestart. Deze stap kan enkele minuten duren.

Stap 4 - Installatie voltooid

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie actieve malware wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn. Klik op **STARTEN MET Bitdefender** om verder te gaan.

Stap 5 - Bitdefender-account

Als u de initiële setup hebt voltooid, verschijnt het Bitdefender-account scherm. U hebt een Bitdefender-account nodig om het product te activeren en de online functies te kunnen gebruiken. Meer informatie vindt u onder "*Bitdefender Central*" (p. 38).

Ga verder volgens uw situatie.

Ik wil een Bitdefender-account maken

Voer de gevraagde informatie in en klik op **ACCOUNT AANMAKEN**.

De gegevens die u hier opgeeft, worden vertrouwelijk behandeld.

Het wachtwoord moet minstens 8 karakters lang zijn en een cijfer bevatten.

Lees de Servicevoorwaarden van Bitdefender voor u verder gaat.

Opmerking

Zodra de account is gemaakt, kunt u het opgegeven e-mailadres en wachtwoord gebruiken om op uw account in te loggen via https://central.bitdefender.com.

Ik heb al een Bitdefender-account

Klik op **Aanmelden** en voer het e-mailadres en het wachtwoord van uw Bitdefender-account in.

Klik op **AANMELDEN** om door te gaan.
Indien u het wachtwoord voor uw account vergeten bent of het reeds ingestelde wachtwoord wenst terug te stellen, klik op de koppeling **Wachtwoord vergeten**. Voer uw e-mailadres in en klik daarna op de knop **WACHTWOORD TERUGSTELLEN**. Controleer uw e-mailaccount en volg de instructies om een nieuw wachtwoord in te stellen voor uw Bitdefender-account.

Opmerking
Indien u al een MyBitdefender-account hebt, kunt u deze gebruiken om u aan te melden in uw Bitdefender-account. Indien u uw wachtwoord vergeten bent, moet u eerst naar https://my.bitdefender.com gaan om het terug te stellen. Gebruik daarna de aangepaste gegevens om u aan te melden bij uw Bitdefender-account.

Ik wil mij aanmelden met mijn Microsoft-, Facebook- of Google-account

Om u aan te melden met uw Microsoft-, Facebook- of Google-account:

1. Selecteer de service die u wilt gebruiken. U wordt omgeleid naar de aanmeldingspagina van die service.
2. Volg de instructies die door de geselecteerde service worden gegeven om uw account te koppelen aan Bitdefender.

Opmerking
Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

Stap 6 - Uw product activeren

Opmerking
Deze stap verschijnt indien u gekozen hebt om een nieuwe Bitdefender-account aan te maken in de vorige stap, of indien u zich hebt aangemeld met een account waarop een verlopen abonnement van toepassing is.

Er is een werkende internetverbinding vereist om de activering van uw product te voltooien.

Ga verder volgens uw situatie:

- Ik heb een activeringscode

  Activeer het product in dit geval door de volgende stappen te volgen:

  1. Voer de activatiecode in het veld **Ik heb een activatiecode** in en klik daarna op **VERDERGAAN**.

     Opmerking
     U vindt uw activatiecode:
     - op het cd/dvd-label.
     - op de productregistratiekaart.

- in de online aankoop e-mail.

2. **Ik wil graag Bitdefender evalueren**

   In dit geval kunt u het product gedurende 30 dagen gebruiken. Om met de proefperiode te starten, selecteert u **Ik heb geen abonnement, ik wil het product gratis uitproberen** en klik daarna op **VERDERGAAN**.

Stap 7 - Aan de slag

In het venster **Aan de slag** kunt u de details van uw abonnement bekijken.

Klik op **VOLTOOIEN** om naar de Bitdefender Antivirus Plus 2017-interface te gaan.

AAN DE SLAG

4. DE BASISFUNCTIES

Nadat u Bitdefender Antivirus Plus 2017 hebt geïnstalleerd, wordt uw computer beschermd tegen alle types malware (zoals virussen, spyware en Trojaanse paarden).

De toepassing gebruikt de Photontechnologie om de snelheid en prestaties van het anti-malware scanproces te versterken. Het werkt door de gebruikspatronen van uw systeemtoepassingen te leren om te weten wat en wanneer er moet worden gescand, om zo de invloed op de systeemprestaties te minimaliseren.

U kunt de "*Auto Pilot*" (p. 19) inschakelen om te genieten van een complete stille beveiliging en u hoeft geen instellingen te configureren. U kunt echter voordeel halen uit de Bitdefender-instellingen om uw beveiliging fijn af te stemmen en te verbeteren.

Wanneer uw toestel verbonden is met een onbeveiligd draadloos netwerk, zal Bitdefender dit identificeren en bescherming activeren om potentiële nieuwsgierigen en spionnen buiten te houden. Voor instructies over hoe u uw persoonlijke gegevens veilig kunt houden, verwijzen we naar "*Wi-Fi Security Advisor*" (p. 112).

Speel games of kijk films terwijl u werkt, Bitdefender kan u een voortdurende gebruikerservaring bieden door onderhoudstaken uit te stellen, onderbrekingen te elimineren en de visuele effecten van het systeem af te stellen. U kunt van dit alles profiteren door "*Profielen*" (p. 136).

Bitdefender zal de meeste beslissingen met betrekking tot de beveiliging voor u nemen en zal zelden pop-upwaarschuwingen weergeven. Details over acties die worden ondernomen en informatie over de programmabediening zijn beschikbaar in het venster Kennisgevingen. Meer informatie vindt u onder "*Notificaties*" (p. 18).

Het is aanbevolen Bitdefender af en toe te openen en eventuele bestaande problemen te herstellen. U zult mogelijk specifieke Bitdefender-componenten moeten configureren of preventieve acties ondernemen om uw computer en gegevens te beschermen.

Om de online functies van Bitdefender Antivirus Plus 2017 te gebruiken en uw abonnementen en toestellen te beheren, gaat u naar uw Bitdefender-account. Meer informatie vindt u onder "*Bitdefender Central*" (p. 38).

In het “Zo werkt het” (p. 48) deel vindt u stap-voor-stap instructies over het uitvoeren van vaak voorkomende taken. Indien u problemen ondervindt bij het gebruik van Bitdefender, controleer dan het “*Algemene problemen oplossen*” (p. 144)deel met mogelijke oplossingen voor de problemen die het vaakst voorkomen.

4.1. Open het Bitdefender-venster.

Om naar de hoofdinterface van Bitdefender Antivirus Plus 2017 te gaan, volgt u de stappen hieronder:

- In **Windows 7**:
  1. Klik op **Start** en ga naar **Alle Programma's**.
  2. Klik op **Bitdefender 2017**.
  3. Klik op **Bitdefender Antivirus Plus 2017** of, sneller, dubbelklik op het pictogram van Bitdefender in het systeemvak.
- In **Windows 8 en Windows 8.1**:

  Zoek Bitdefender Antivirus Plus 2017 vanuit het Windows-startscherm (u kunt bijvoorbeeld beginnen met het typen van "Bitdefender", rechtstreeks in het startscherm) en klik op het pictogram ervan. U kunt ook de Desktop-app openen en dubbelklikken op het pictogram van Bitdefender in het systeemvak.
- In **Windows 10**:

  Typ "Bitdefender" in het zoekveld in de taakbalk en klik dan op het pictogram ervan. Een andere mogelijkheid is het dubbelklikken op het pictogram van Bitdefender in het systeemvak.

Meer informatie over het Bitdefender-venster en -pictogram in het systeemvak, vindt u op “*Bitdefender-interface*” (p. 24).

4.2. Problemen aan het oplossen

Bitdefender gebruikt een systeem voor het opsporen van problemen en brengt u op de hoogte van de problemen die de veiligheid van uw computer en gegevens kunnen beïnvloeden. Standaard bewaakt het programma alleen een reeks problemen die als zeer belangrijk worden beschouwd. U kunt dit echter configureren volgens uw behoeften, waarbij u specifieke problemen kunt kiezen waarvan u op de hoogte wilt worden gebracht.

De gedetecteerde problemen bevatten belangrijke beveiligingsinstellingen die worden uitgeschakeld en andere omstandigheden die een beveiligingsrisico kunnen betekenen. Ze zijn gegroepeerd in twee categorieën:

- **Kritieke problemen** - verhinderen dat Bitdefender u beveiligt tegen malware of vormen een belangrijk beveiligingsrisico.
- **Minder belangrijke (niet-kritieke) problemen** - kan uw beveiliging in de nabije toekomst beïnvloeden.

Het Bitdefender-pictogram in het systeemvak geeft problemen in behandeling aan door de kleur als volgt te wijzigen:

Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.
Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.

Als u de muiscursor over het pictogram beweegt, verschijnt bovendien een pop-up dat het bestaan van problemen in behandeling bevestigt.

Wanneer u de Bitdefender-interface opent, geeft het gebied Beveiligingsstatus in de werkbalk bovenaan de aard van de problemen die uw systeem beïnvloeden aan.

4.2.1. Wizard beveiligingsproblemen

Volg de wizard **Beveiligingsproblemen** om de gedetecteerde problemen op te lossen.

1. Voer een van de volgende bewerkingen uit om de wizard te openen:
   - Klik met de rechtermuisknop op het Bitdefender-pictogram in het systeemvak en kies **Alle veiligheidsproblemen weergeven**.
   - Open de Bitdefender-interface en klik ergens binnen de Beveiligingsstatus in de bovenste werkbalk.
2. U kunt de problemen zien die de veiligheid van uw computer en gegevens beïnvloeden. Alle huidige problemen zijn geselecteerd om te worden opgelost.

   Als u een specifiek probleem niet meteen wilt oplossen, schakelt u het overeenkomende selectievakje uit. U wordt gevraagd op te geven hoelang het oplossen van het probleem kan worden uitgesteld. Kies de gewenste

optie in het menu en klik op **OK**. Kies **Permanent** om de bewaking van de respectieve problemencategorie te stoppen.

De status van het probleem verandert naar **Uitgesteld** en er wordt geen actie ondernomen om het probleem op te lossen.

3. Om de geselecteerde problemen op te lossen, klikt u op **Herstellen**. Sommige problemen worden onmiddellijk opgelost. Bij andere problemen wordt u geholpen door een wizard om ze op te lossen.

De problemen die deze wizard u helpt oplossen kunnen in deze hoofdcategorieën worden gegroepeerd.

- **Uitgeschakelde beveiligingsinstellingen.** Dergelijke problemen worden onmiddellijk opgelost door hun respectievelijke beveiligingsinstellingen in te schakelen.
- **Preventieve beveiligingstaken die u moet uitvoeren.** Wanneer u dergelijke problemen oplost, helpt een wizard u bij het voltooien van de taak.

4.2.2. Statuswaarschuwingen configureren

Bitdefender kan u informeren wanneer er problemen worden gedetecteerd in de verrichtingen van de volgende programmaonderdelen:

- Antivirus
- Update
- Browserveiligheid

U kunt het waarschuwingssysteem configureren om optimaal te voldoen aan uw beveiligingsbehoeften door te kiezen over welke problemen u op de hoogte wilt worden gebracht. Volg deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **GEAVANCEERD**.
3. Klik op de link **Statuswaarschuwingen configureren**.
4. Klik op de schakelaars om de statuswaarschuwingen volgens uw voorkeuren in of uit te schakelen.

4.3. Notificaties

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw computer. Wanneer er iets belangrijks

gebeurt met de veiligheid van uw systeem of gegevens, wordt er een nieuw bericht toegevoegd aan Kennisgevingen van het Bitdefender, net zoals er nieuwe e-mails verschijnen in uw Postvak IN.

Kennisgevingen zijn een belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging. U kunt met behulp van het Geschiedenis-logbestand bijvoorbeeld heel gemakkelijk zien of de laatste update is geslaagd en of er malware of kwetsbaarheden op uw computer werden aangetroffen. Daarnaast kunt u zo nodig verdere acties ondernemen of acties die door Bitdefender zijn ondernomen, wijzigen.

Om naar de Kennisgevingenlogs te gaan, klikt u op het pictogram in de linkerzijbalk van de Bitdefender-interface. 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.

4.4. Auto Pilot

Voor alle gebruikers die van hun beveiligingsoplossing alleen vragen dat ze worden beschermd zonder te worden gehinderd, werd Bitdefender Antivirus Plus 2017 ontworpen met een ingebouwde Autopilot-modus.

Wanneer u in de modus Autopilot bent, past Bitdefender een optimale beveiligingsconfiguratie toe en neemt de toepassing alle beslissingen met betrekking tot de beveiliging voor u. Dit betekent dat u geen pop-upberichten of waarschuwingen zult zien en dat u geen enkele instelling zult moeten configureren.

In de modus Autopilot, lost Bitdefender automatisch kritieke problemen op en beheert het op de achtergrond:

- Antivirusbeveiliging, geleverd door Scannen bij toegang en Doorlopend scannen.
- Webbeveiliging.
- Automatische updates.

Om de Automatische piloot uit te schakelen, klikt u op de **AUTOPILOT**-schakelaar in de bovenste takenbalk van de Bitdefender-interface.

Zolang Auto pilot is ingeschakeld, verandert het Bitdefender-pictogram in het systeemvak naar .

Belangrijk
Wanneer Autopilot is ingeschakeld en u instellingen die door deze toepassing worden beheerd wijzigt, zal Auto Pilot worden uitgeschakeld.

Open het venster Kennisgevingen om de geschiedenis te zien van acties die door Bitdefender zijn ondernomen terwijl Autopilot is ingeschakeld.

4.5. Profielen

Sommige computeractiviteiten, zoals online games of videopresentaties, vereisen een hoger reactievermogen en hoge prestaties van het systeem zonder onderbrekingen. Wanneer uw laptop werkt op batterijvermogen, is het aanbevolen minder dringende bewerkingen die extra stroom zullen verbruiken, worden uitgesteld tot de laptop opnieuw op de netstroom is aangesloten.

Bitdefender Profielen kent meer systeemvermogen toe aan de toepassingen die worden uitgevoerd door de beveiligingsinstellingen tijdelijk te veranderen en de systeemconfiguratie aan te passen. Als gevolg daarvan is de systeeminvloed op uw activiteit beperkt.

Om zich aan verschillende activiteiten aan te passen, komt Bitdefender met de volgende profielen:

Werkprofiel
: Optimaliseert uw werk op efficiënte wijze door het product en de systeeminstellingen te herkennen en aan te passen.

Filmprofiel
: Versterkt visuele effecten en elimineert onderbrekingen bij het kijken naar films.

Gameprofiel
: Versterkt visuele effecten en elimineert onderbrekingen bij het spelen van games.

Openbaar Wi-Fi-profiel
: Past productinstellingen toe om te genieten van volledige bescherming, terwijl u verbonden bent met een onveilig draadloos netwerk.

Profiel batterijmodus
: Past productinstellingen toe en houdt achtergrondactiviteit tegen om uw accuduur te verlengen.

4.5.1. Automatische activatie van profielen configureren

Voor een gebruiksvriendelijke ervaring kunt u Bitdefender configureren om uw werkprofiel te beheren. In dit geval detecteert Bitdefender automatisch de activiteit die u uitvoert en past systeem- en productoptimalisatie-instellingen toe.

Om Bitdefender toestemming te geven om profielen te activeren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Gebruik de bijhorende schakelaar om **Profielen automatisch activeren** in te schakelen.

Indien u niet wenst dat de Profielen automatisch worden geactiveerd, zet u de schakelaar uit.

Meer informatie over Profielen vindt u onder"*Profielen*" (p. 136)

4.6. Wachtwoordbeveiligde Bitdefender-instellingen

Als u niet de enige persoon met beheermachtigingen bent die deze computer gebruikt, raden wij u aan uw Bitdefender-instellingen te beveiligen met een wachtwoord.

Wachtwoordbescherming configureren voor de Bitdefender-instellingen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **ALGEMEEN**.
3. Schakel de wachtwoordbescherming in door op de overeenkomende schakelaar te klikken.
4. Voer het wachtwoord in de twee velden in en klik op **OK**. Het wachtwoord moet minstens 8 tekens lang zijn.

Zodra u een wachtwoord hebt ingesteld, zal iedereen die de Bitdefender-instellingen probeert te wijzigen, eerst het wachtwoord moeten opgeven.

Belangrijk

Zorg dat u uw wachtwoord onthoudt of bewaar het op een veilige plaats. Als u het wachtwoord vergeten bent, moet u het programma opnieuw installeren of contact opnemen met Bitdefender voor ondersteuning.

Wachtwoordbeveiliging verwijderen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **ALGEMEEN**.
3. Schakel de wachtwoordbescherming uit door op de overeenkomende schakelaar te klikken. Voer het wachtwoord in en klik op **OK**.

Opmerking

Om het wachtwoord van uw product te wijzigen, klikt u op de link **Wachtwoord veranderen**. Voer uw huidige wachtwoord in en klik op *OK*. In het nieuwe venster dat verschijnt, voert u het nieuwe wachtwoord in dat u voortaan wenst te gebruiken om de toegang tot uw Bitdefender-instellingen te beperken.

4.7. Anonieme gebruiksrapporten

Standaard verzendt Bitdefender rapporten met informatie over uw gebruik van het programma naar de Bitdefender-servers. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden. Merk op dat deze rapporten geen vertrouwelijke gegevens, zoals uw naam of IP-adres, bevatten en niet zullen worden gebruikt voor commerciële doeleinden.

Indien u geen Anonieme gebruikersrapporten meer wil verzenden:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **GEAVANCEERD**.
3. Klik op de bijhorende schakelaar om **Anonieme gebruikersverslagen** uit te schakelen.

4.8. Speciale aanbiedingen en productmeldingen

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.

Bovendien kunnen er productmeldingen verschijnen als u veranderingen in het product aanbrengt.

Speciale aanbiedingen en productkennisgevingen in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **ALGEMEEN**.
3. Schakel de speciale aanbiedingen en productmeldingen in of uit door op de overeenkomende schakelaar te klikken.

De optie speciale aanbiedingen en productmeldingen is standaard ingeschakeld.

5. BITDEFENDER-INTERFACE

Bitdefender Antivirus Plus 2017 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 **VOLGENDE** om de gids voort te zetten, of **Rondleiding overslaan** om de wizard te sluiten.

Om de status van het product te zien en essentiële taken uit t voeren, is het systeemvakpictogram van Bitdefender op elk ogenblik beschikbaar.

In het hoofdvenster kunt u het gedrag van het product beheren via de Autopilot, hebt u toegang tot belangrijke productinformatie en kunt u courante taken uitvoeren. In de linkerzijbalk kunt u naar uw Bitdefender-account en de Bitdefender-secties gaan voor gedetailleerde configuratietaken en geavanceerde administratieve taken.

Als u altijd een oogje wilt houden op essentiële beveiligingsinformatie en snel toegang wilt krijgen tot belangrijke instellingen, kunt u de Beveiligingswidget weergeven op het bureaublad.

5.1. Systeemvakpictogram

Om het volledige product sneller te beheren, kunt u het Bitdefender-pictogram in het systeemvak gebruiken.

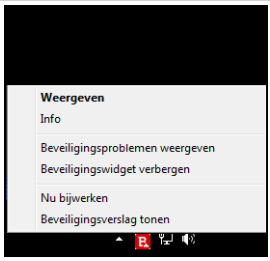
Opmerking

Het pictogram Bitdefender is mogelijk niet altijd zichtbaar. Het pictogram permanent zichtbaar maken:

- In **Windows 7, Windows 8 en Windows 8.1**:
  1. Klik onderaan rechts op het scherm op de pijl.
  2. Klik op **Aanpassen...** om het venster met de systeemvakpictogrammen te openen.
  3. Selecteer de optie **Pictogrammen en meldingen weergeven** voor het pictogram **Bitdefender-agent**.
- In **Windows 10**:

1. Klik met de rechtermuisknop op de taakbalk en selecteer **Eigenschappen**.
2. Klik op **Aanpassen** in het Taakbalkvenster.
3. Klik op de link **Selecteer welke pictogrammen op de taakbalk verschijnen** in het venster **Meldingen & acties**.
4. Schakel de schakelaar naast **Bitdefender Agent** in.

Wanneer u dubbelklikt op dit pictogram, wordt Bitdefender geopend. Door met de rechterknop op het pictogram te klikken, verschijnt een snelmenu waarmee u het Bitdefender-product snel kunt beheren.



Pictogram vak

- **Weergeven** - opent het hoofdvenster van Bitdefender.
- **Info** - opent een venster waar u informatie over Bitdefender kunt bekijken en waar u hulp kunt zoeken wanneer er zich een onverwachte gebeurtenis voordoet.
- **Alle veiligheidsproblemen weergeven** - helpt u de huidige zwakke punten in de beveiliging te verwijderen. Als de optie niet beschikbaar is, moeten er geen problemen worden opgelost. Raadpleeg "*Problemen aan het oplossen*" (p. 16) voor meer gedetailleerde informatie.
- **Beveiligingswidget tonen/verbergen** - hiermee schakelt u de Beveiligingswidget in/uit.
- **Update nu** - start een directe update. U kunt de updatestatus volgen in het paneel Update van het hoofdvenster van Bitdefender.
- **Beveiligingsverslag tonen** - opent een venster waarin u een wekelijkse status een aanbevelingen voor uw systeem kunt zien. U kunt de aanbevelingen opvolgen om uw systeemveiligheid te verbeteren.

Het systeemvakpictogram van Bitdefender brengt u door middel van een speciaal pictogram op de hoogte van problemen die uw computer beïnvloeden of van de manier waarop het product werkt. Deze symbolen zijn de volgende:

Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.
Bitdefender Autopilot is ingeschakeld.

Als Bitdefender niet werkt, verschijnt het systeemvakpictogram op een grijze achtergrond: . Dit doet zich doorgaans voor wanneer het lidmaatschap vervalt. Dit kan ook optreden wanneer de Bitdefender-services niet reageren of wanneer andere fouten de normale werking van Bitdefender beïnvloeden.

5.2. Hoofdvenster

Via het hoofdvenster van Bitdefender kunt u algemene taken uitvoeren, snel beveiligingsproblemen oplossen, informatie over het productgebruik weergeven en naar de panelen gaan van waaruit u de productinstellingen kunt configureren. U kunt het allemaal met slechts enkele klikken op de knop.

Het venster is geordend in vier hoofdgebieden:

Statusgebied
: Hier kunt u de beveiligingsstatus van uw computer controleren, een update lanceren en de Autopilot configureren.

Linkerzijbalk
: Via dit menu kunt naar uw Bitdefender-account gaan en het beheren, samen met de online eigenschappen van uw product, of omschakelen tussen de drie hoofdgedeelten van het product. Van hieruit kunt u ook naar de Kennisgevingen, het wekelijkse Beveiligingsverslag, de Algmene instellingen en het gebied Hulp & ondersteuning.

Actieknoppen en toegang tot modulegebied
: Hier kunt u verschillende taken lanceren om uw systeem beschermd te houden. U kunt ook naar de Bitdefender-modules gaan om het product zelf te configureren.

Onderste balk
: Hier kunt het Bitdefender makkelijk installeren op andere apparaten, op voorwaarde dat u voldoende licenties in uw abonnement hebt.

5.2.1. Statusgebied

Het statusgebied bevat de volgende elementen:

- **Beveiligingsstatus** aan de linkerzijde van het gebied informeert u als er problemen zijn die de beveiliging van uw computer beïnvloeden en helpt u bij het oplossen van het probleem.

  De kleur van het gebied van de beveiligingsstatus verandert afhankelijk van de gedetecteerde problemen en er worden verschillende berichten weergegeven:

  - **Het gebied wordt groen gekleurd.** Er zijn geen problemen om op te lossen. Uw computer en gegevens zijn beveiligd.
  - **Het gebied wordt geel gekleurd.** Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.
  - **Het gebied wordt rood gekleurd.** Kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet deze problemen onmiddellijk aanpakken.

  Door ergens binnen het gebied van de beveiligingsstatus te klikken, gaat u naar een wizard die u helpt om gemakkelijk bedreigingen van uw computer te verwijderen. Raadpleeg "*Problemen aan het oplossen*" (p. 16) voor meer gedetailleerde informatie.

- Met **AUTOPILOT** kunt u optimale bescherming inschakelen en genieten van een volledig geruisloze beveiliging. Raadpleeg "*Auto Pilot*" (p. 19) voor meer gedetailleerde informatie.
- Via **NU UPDATEN** kunt u een productupdate laten lopen wanneer u maar wilt, zodat u de meest recente malware-informatie hebt. Raadpleeg "*Bitdefender up-to-date houden*" (p. 44) voor meer gedetailleerde informatie.
- **Actief Profiel** geeft het profiel weer dat momenteel geactiveerd is in uw Bitdefender-product. Raadpleeg "*Profielen*" (p. 136) voor meer gedetailleerde informatie.

5.2.2. Linkerzijbalk

In de linkerzijbalk zijn er suggestieve iconen beschikbaar waarmee u naar Bitdefender-account, productsecties, activiteitenverslag, kennisgevingen, algemene instellingen en ondersteuning kunt gaan.

De namen van de pictogrammen zijn zichtbaar als u op de ≡-icoon klikt, als volgt:

- **Bescherming**. De actieknoppen **Snelle Scan** en **Kwetsbaarheidsscan** worden zichtbaar in de linkerbenedenhoek van de Bitdefender-interface. Ook informatie over geblokkeerde applicaties, opgespoorde bedreigingen en aanvallen wordt zichtbaar. Klik op de koppeling **MODULES BEKIJKEN** om naar het configuratiegebied te gaan.
- **Privacy**. De actieknopn **Safepay** wordt zichtbaar in de linkerbenedenhoek van de Bitdefender-interface. Ook informatie over gedetecteerde portefeuilles en vernietigde bestanden wordt weergegeven. Klik op de koppeling **MODULES BEKIJKEN** om naar het configuratiegebied te gaan.
- **Activiteit**. Van hieruit kunt u de productactiviteit van de voorbije 30 dagen bekijken en naar het veiligheidsrapport gaan dat om de zeven dagen wordt gegenereerd.
- **Kennisgevingen**. Van hieruit hebt u toegang tot de gegenereerde kennisgevingen.
- **Account**. Details over Bitdefender-account en lopend abonnement zijn beschikbaar. Ga naar uw Bitdefender-account om uw abonnement te controleren en beveiligingstaken uit te voeren op de toestellen die u beheert.
- **Instellingen**. Van hieruit hebt u toegang tot de algemene instellingen.
- **Ondersteuning**. Van hieruit kunt u, wanneer u hulp nodig hebt bij het aanpakken van een probleem met uw Bitdefender Antivirus Plus 2017, contact opnemen met de Technische ondersteuning van Bitdefender.

5.2.3. Actieknoppen en toegang tot modulegebied

Met de actieknoppen kunt u snel belangrijke taken lanceren. Actieknoppen worden zichtbaar in de linkerbenedenhoek van de Bitdefender-interface wanneer u een van de drie volgende secties selecteert: **Bescherming** en **Privacy** in de linkerzijbalk.

Afhankelijk van het gedeelte dat u kiest kunnen de actieknoppen die hier zichtbaar zijn, de volgende zijn:

- **Snelle scan**. Voer een snelle scan uit om er zeker van te zijn dat uw computer vrij is van malware.

- **Analyse op Kwetsbaarheden**. Scan uw computer op kwetsbaarheden om zeker te zijn dat alle geïnstalleerde toepassingen, samen met het Besturingssysteem, bijgewerkt zijn en correct werken.
- **Safepay**. Open Bitdefender Safepay™ om uw gevoelige gegevens te beschermen terwijl u online transacties uitvoert.

5.2.4. Onderste balk

Om aanvullende apparaten te beginnen beschermen:

1. Klik op de koppeling **EEN ANDER APPARAAT INSTALLEREN**.

   U wordt afgeleid naar de Bitdefender-account webpagina. Zorg ervoor dat u aangemeld bent met uw gegevens.

2. In het venster dat verschijnt, selecteert u het gewenste besturingssysteem, en klikt u op **VERDERGAAN**.

3. Voer het e-mailadres in waar we de downloadkoppeling voor de installatie van het gekozen platform heen moeten sturen.

Afhankelijk van uw keuze zullen de volgende Bitdefender-producten geïnstalleerd worden:

- Bitdefender Antivirus Plus 2017 op Windows-apparaten.
- Bitdefender-antivirus voor Mac op OS X-apparaten.
- Bitdefender Mobiele beveiliging op Android-apparaten.

5.3. De Bitdefender-secties

Het Bitdefender-product wordt geleverd met drie secties, verdeeld in nuttige modules om u beschermd te houden terwijl u werkt, op het internet surft, gamet of online betalingen wilt doen.

Wanneer u naar de modules voor een specifiek gedeelte wilt gaan of uw product wilt configureren, gaat u naar de volgende iconen op de linkerzijbalk van de Bitdefender-interface:

- Beveiliging
- Privacy

5.3.1. Beveiliging

In het gedeelte Bescherming kunt u uw beschermingsniveau configureren, de ransomware- en webbeveiligingsfuncties instellen, potentiële systeemkwetsbaarheden controleren en oplossen en de beveiliging van de draadloze netwerken waarmee u verbonden bent, beoordelen.

De modules die u in het Beveiligingsgedeelte kunt beheren zijn:

ANTIVIRUS

Antivirusbescherming is de basis van uw beveiliging. Bitdefender beschermt u in real time en op aanvraag tegen elk type malware, zoals virussen, Trojaanse paarden, spyware, adware, enz.

Via de Antivirusmodule krijgt u gemakkelijk toegang tot de volgende scantaken:

- Snelle scan
- Systeemscan
- Scans beheren
- Helpmodus

Raadpleeg "*Antivirusbeveiliging*" (p. 78) voor meer informatie over scantaken en het configureren van de antivirusbeveiliging.

WEBBEVEILIGING

Webbeveiliging helpt u om beveiligd te blijven tegen phishingaanvallen, fraudepogingen en lekken van privégegevens terwijl u op het internet surft.

Meer informatie over het configureren van Bitdefender om uw webactiviteit te beschermen, vindt u op "*Webbeveiliging*" (p. 104).

KWETSBAARHEID

De Kwetsbaarheidsmodule helpt u om uw besturingssysteem en de applicaties die u regelmatig gebruikt, up-to-date te houden en onveilige draadloze netwerken waarmee u een verbinding maakt, in het licht te stellen.

Klik op **Kwetsbaarheidsscan** in de Kwetsbaarheidsmodule om te starten met het herkennen van kritieke Windows-updates, updates van toepassingen, zwakke wachtwoorden van Windows-accounts en draadloze netwerken die niet beveiligd zijn.

Klik op **Wi-Fi-beveiligingsadviseur** om de lijst te bekijken van de draadloze netwerken waarmee u een verbinding maakt, samen met onze

reputatiebeoordeling voor elk daarvan en de actie die u kunt ondernemen om veilig te blijven voor potentiële nieuwsgierigen.

Meer informatie over het configureren van de kwetsbaarheidsbeveiliging vindt u onder "*Kwetsbaarheid*" (p. 108).

BESCHERMING TEGEN RANSOMWARE

De module Ransomware-bescherming zorgt ervoor dat uw persoonlijke bestanden beschermd blijven tegen aanvallen van online Black Hands.

Meer informatie over het configureren van Ransomware-bescherming om uw systeem te beschermen tegen ransomware-aanvallen, vindt u op "*Bescherming ransomware*" (p. 116).

5.3.2. Privacy

In het Privacygedeelte kunt u uw online transacties beschermen en uw browsingervaring veilig houden.

De modules die u in het Privacygedeelte kunt beheren, zijn:

GEG. BEVEILIGING

Met de module Databescherming kunt u bestanden permanent verwijderen.
Klik op **Bestandsvernietiging** in de gegevensbeveiligingsmodule om een wizard te starten waarmee u bestanden volledig kunt verwijderen van uw systeem.

Meer informatie over het configureren van de Gegevensbeveiliging vindt u onder "*Data bescherming*" (p. 106).

WALLET

Bitdefender is de wachtwoordbeheerder die helpt om uw wachtwoorden bij te houden, uw privacy beveiligt en een veilige online surfervaring verschaft.

Vanuit de module Wachtwoordbeheerder kunt u de volgende taken uitvoeren:

- **Portefeuille openen** - opent de bestaande Portefeuille-database.
- **Portefeuille sluiten** - sluit de bestaande Portefeuille-database.
- **Portefeuille exporteren** - staat u toe de bestaande database op te slaan op een locatie op uw systeem.

- **Nieuwe portefeuille aanmaken** - start een wizard die u in staat stelt een nieuwe Portefeuille-database aan te maken.
- **Verwijderen** - hiermee kunt u een Portefeuille-database verwijderen.
- **Instellingen** - hier kunt u de naam van uw Portefeuille-database wijzigen en een synchronisatie van de bestaande info met al uw toestellen al dan niet instellen.

Meer informatie over het configureren van Wachtwoordbeheerder, vindt u onder "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 126).

SAFEPAY

De Bitdefender Safepay™ browser helpt u om uw online bankieren, e-shopping en alle andere soorten online transacties privé en veilig te houden.

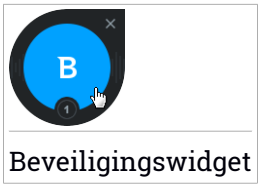
Klik op de **Safepay**-actieknop vanuit de Bitdefender-interface om te starten met het uitvoeren van online transacties in een veilige omgeving.

Meer informatie over Bitdefender Safepay™ vindt u onder "*Safepay beveiliging voor online transacties*" (p. 120).

5.4. Beveiligingswidget

Beveiligingswidget is de snelle en eenvoudige manier voor het bewaken en beheren van Bitdefender Antivirus Plus 2017. Wanneer u deze kleine en weinig opdringerige widget toevoegt aan uw bureaublad, kunt u op elk ogenblik kritieke informatie zien en belangrijke taken uitvoeren.

- het hoofdvenster van Bitdefender openen.
- Scanactiviteit bewaken in real time.
- De beveiligingsstatus van uw systeem bewaken en eventuele bestaande problemen oplossen.
- weergeven wanneer een update wordt uitgevoerd.
- Meldingen weergeven en toegang krijgen tot de recentste gebeurtenissen die zijn gemeld door Bitdefender.
- Bestanden of mappen scannen door een of meerdere items te slepen en boven de widget neer te zetten.



Beveiligingswidget

De algemene beveiligingsstatus van uw computer wordt weergegeven **in het midden** van de widget. De status wordt aangeduid door de kleur en vorm van het pictogram dat in dit gebied wordt weergegeven.


Kritieke problemen beïnvloeden de beveiliging van uw systeem.

Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld. Klik op het statuspictogram om het oplossen van de gemelde problemen te starten.


Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt. Klik op het statuspictogram om het oplossen van de gemelde problemen te starten.


Uw systeem is beveiligd.


Wanneer een scantaak op aanvraag bezig is, wordt dit geanimeerde pictogram weergegeven.

Wanneer er problemen worden gemeld, klikt u op het statuspictogram om de wizard Problemen herstellen te starten.

De onderzijde van de widget toont de teller van de ongelezen gebeurtenissen (het aantal openstaande gebeurtenissen dat is gemeld door Bitdefender, als er zijn). Klik op de gebeurtenissenteller, bijvoorbeeld 1 voor één ongelezen gebeurtenis, om het venster Kennisgevingen te openen. Meer informatie vindt u onder "*Notificaties*" (p. 18).

5.4.1. Bestanden en mappen scannen

U kunt de Beveiligingswidget gebruiken om snel bestanden en mappen te scannen. Sleep een bestand of map die u wilt scannen en zet deze neer boven de **Beveiligingswidget**.

De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten en kunnen niet worden gewijzigd. Als er geïnfecteerde bestanden worden gedetecteerd, zal Bitdefender proberen ze te desinfecteren (de malwarecode verwijderen). Als de desinfectie mislukt, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden.

5.4.2. Beveiligingswidget tonen/verbergen

Wanneer u de widget niet meer wilt zien, klikt u op .

Gebruik een van de volgende methoden om de Beveiligingswidget te herstellen:

- Vanuit het systeemvak:
  1. Klik met de rechtermuisknop op het Bitdefender-pictogram in het systeemvak.
  2. Klik op **Beveiligingswidget tonen** in het contextmenu dat verschijnt.
- Van de Bitdefender-interface:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Selecteer het tabblad **ALGEMEEN**.
  3. Schakel **Beveiligingswidget weergeven** in door op de overeenkomende schakelaar te klikken.

De Bitdefender-veiligheidswidget is standaard uitgeschakeld.

5.5. Activiteit

Het Activiteitenvenster geeft informatie over de acties die de voorbije 30 dagen door Bitdefender op uw apparaat werden ondernomen. Hier kunt u controleren welke toepassingen, bedreigingen en aanvallen werden geblokkeerd tijdens deze periode en of er ransomeware-pogingen werden ondernomen.

Het Veiligheidsrapport, dat een wekelijkse status voor uw product biedt en verschillende tips geeft om de systeembescherming te verbeteren, kunt u ook inkijken door op de bijhorende koppeling te klikken. Deze tips zijn belangrijk om de algehele beveiliging te beheren en u kunt eenvoudig de handelingen zien die u kunt uitvoeren op uw systeem.

Het verslag wordt eenmaal per week aangemaakt en het vat de relevante informatie over uw productactiviteit samen zodat u gemakkelijk kunt begrijpen welke gebeurtenissen er in dit tijdvak voorgevallen zijn.

De informatie die het beveiligingsverslag biedt, is verdeeld in twee categorieën:

- **Beveiliging** gebied - weergave van informatie met betrekking tot uw systeembeveiliging.
  - **Bestanden gescand**

    Stelt u in staat de bestanden te zien die gedurende de week zijn gescand door Bitdefender. U kunt details weergeven, zoals het aantal gescande bestanden en het aantal opgeschoonde bestanden door Bitdefender.

    Meer informatie over antivirusbeveiliging vindt u onder "*Antivirusbeveiliging*" (p. 78).
  - **Gescande webpagina's**

    Stelt u in staat het aantal door Bitdefender gescande en geblokkeerde webpagina's te controleren. Om u te beveiligen tegen het bekendmaken van persoonlijke gegevens onder het surfen, beveiligt Bitdefender uw webverkeer.

    Meer informatie over Webbeveiliging vindt u onder "*Webbeveiliging*" (p. 104).
  - **Kwetsbaarheden**

    Stelt u in staat om de systeemkwetsbaarheden gemakkelijk te identificeren en op te lossen om uw computer veiliger te maken tegen malware en hackers.

    Meer informatie over de Kwetsbaarheidsscan vindt u onder "*Kwetsbaarheid*" (p. 108).
  - **Gebeurtenissentijdlijn**

    Stelt u in staat een algeheel beeld te krijgen van alle scanprocessen en problemen hersteld door Bitdefender gedurende de week. De gebeurtenissen zijn gescheiden per dag.

    Voor meer informatie over een gedetailleerd verslag of gebeurtenissen over de activiteit op uw computer zie "*Notificaties*" (p. 18).

- **Optimalisering** gebied - geeft informatie weer met betrekking tot de opgeschoonde ruimte, geoptimaliseerde toepassingen en hoeveel computeraccu u hebt bespaard door het Profiel Accumodus te gebruiken.
  - **Accu bespaard**

    Stelt u in staat te zien hoeveel van de accu u hebt bespaard terwijl het systeem in het profiel Accumodus was.

    Meer informatie over het profiel Accumodus vindt u onder "*Profiel batterijmodus*" (p. 141).
  - **Geoptimaliseerde apps**

    Stelt u in staat het aantal toepassingen te zien dat u hebt gebruikt onder de Profielen.

    Meer informatie over Profielen vindt u onder "*Profielen*" (p. 136).

5.5.1. Het beveiligingsverslag controleren

Het Beveiligingsverslag gebruikt een systeem voor het opsporen van problemen en brengt u op de hoogte van de gebeurtenissen die de veiligheid van uw computer en gegevens kunnen beïnvloeden. De gedetecteerde problemen bevatten belangrijke beveiligingsinstellingen die worden uitgeschakeld en andere omstandigheden die een beveiligingsrisico kunnen betekenen. Als u het verslag gebruikt, kunt u specifieke Bitdefender-onderdelen configureren of preventieve acties nemen om uw computer en uw persoonlijke gegevens te beveiligen.

Om het beveiligingsverslag te controleren:

1. Naar het verslag gaan:
   - Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.

     Klik op de koppeling **Veiligheidsverslag** in de rechterbenedenhoek van het venster Activiteitenverslag.
   - Rechterklik op het pictogram van het Bitdefender in het systeemvak en selecteer **Beveiligingsverslag tonen**.
   - Zodra het verslag volledig is, ontvangt u een pop-up-melding. Klik op **Tonen** om naar het activiteitenverslag te gaan.

     Er wordt een webpagina geopend in uw webbrowser waarin u het aangemaakte verslag kunt zien.

2. Kijk bovenaan in het venster om de algehele beveiligingsstatus te zien.
3. Controleer onze aanbevelingen onderaan de pagina.

De kleur van het gebied van de beveiligingsstatus verandert afhankelijk van de gedetecteerde problemen en er worden verschillende berichten weergegeven:

- **Het gebied is groen.** Er zijn geen problemen om op te lossen. Uw computer en gegevens zijn beveiligd.
- **Het gebied is oranje.** Niet-kritieke problemen beïnvloeden de veiligheid van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.
- **Het gebied is rood.** Kritieke problemen beïnvloeden de veiligheid van uw systeem. U moet deze problemen onmiddellijk aanpakken.

5.5.2. De melding Beveiligingsverslag aan- of uitzetten

De melding Beveiligingsverslag aan- of uitzetten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **ALGEMEEN**.
3. Klik op de overeenkomende schakelaar om de melding Beveiligingsverslag aan of uit te zetten.

   De melding Beveiligingsverslag is standaard ingeschakeld.

6. BITDEFENDER CENTRAL

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

- Bitdefender downloaden en installeren op Windows,OS X en Android. De producten die beschikbaar zijn om te downloaden, zijn:
  - Bitdefender Antivirus Plus 2017
  - Bitdefender Antivirus voor Mac
  - Bitdefender Mobile Security
- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Nieuwe apparaten aan uw netwerk toevoegen en deze apparaten beheren, waar u op dat moment ook bent.

6.1. Naar Bitdefender Central gaan

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

- Vanuit het hoofdvenster van Bitdefender:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Selecteer de koppeling **Ga naar Bitdefender-centrale**.
  3. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
- Vanuit uw webbrowser:
  1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
  2. Ga naar https://central.bitdefender.com.

3. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.

6.2. Mijn abonnementen

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

6.2.1. Controleer beschikbare abonnementen

Om uw beschikbare abonnementen te controleren:

1. Ga naar Bitdefender Central.
2. Ga naar het paneel **Mijn abonnementen**.

Hier hebt u informatie over de beschikbaarheid van de abonnementen die u hebt en het aantal toestellen dat elk daarvan gebruikt.

U kunt een nieuw toestel aan een abonnement toevoegen of het vernieuwen door een abonnementenkaart te selecteren.

Opmerking
U kunt een of meer lidmaatschappen op uw account hebben, op voorwaarde dat ze voor verschillende platforms bestemd zijn (Windows, Mac OS X of Android).

6.2.2. Een nieuw toestel toevoegen

Indien uw abonnement meer dan één toestel dekt, kunt u een nieuw toestel toevoegen en uw Bitdefender Antivirus Plus 2017 erop installeren, als volgt:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik in het venster **MIJN APPARATEN** op **Bitdefender INSTALLEREN**.
4. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

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

Selecteer **Windows** om uw Bitdefender-product te downloaden en klik vervolgens op **VERDERGAAN**. Voer een e-mailadres in in het overeenkomstige veld en klik op **VERZENDEN**.

5. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

6.2.3. Abonnement verlengen

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

1. Ga naar Bitdefender Central.
2. Ga naar het paneel **Mijn abonnementen**.
3. Selecteer de gewenste abonnementenkaart.
4. Klik op **VERNIEUWEN** om door te gaan.

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

6.2.4. Abonnement activeren

Een abonnement kan geactiveerd worden tijdens het installatieproces als u uw Bitdefender-account gebruikt. Samen met het activeringsproces begint het aftellen van de geldigheid.

Indien u een activeringscode hebt gekocht bij een van onze verdelers of als geschenk hebt ontvangen, kunt u de beschikbaarheid ervan toevoegen aan een bestaand Bitdefender-abonnement dat op de account beschikbaar is, op voorwaarde dat ze voor hetzelfde product geldt.

Een abonnement activeren met een activatiecode:

1. Ga naar Bitdefender Central.
2. Ga naar het paneel **Mijn abonnementen**.
3. Klik op de knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **ACTIVERINGSCODE** om door te gaan.

Het abonnement is nu geactiveerd. Ga naar het **Mijn Toestellen**-paneel en selecteer **Bitdefender INSTALLEREN** om het product op een van uw toestellen te installeren.

6.3. Mijn apparaten

Vanaf het paneel **Mijn apparaten** van Bitdefender Central kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en verbinding hebben met internet. De toestelkaarten geven de naam van het toestel weer, de beschermingsstatus en de resterende beschikbaarheid van uw abonnement.

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

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op het symbool ⋮ van de gewenste apparaatkaart en selecteer **Instellingen**.
4. Wijzig de toestelnaam in het overeenkomstige veld en selecteer vervolgens **Opslaan**.

Indien Autopilot is uitgeschakeld, kunt u deze functie activeren door op de schakelaar te klikken. Klik op **Opslaan** om de instellingen toe te passen.

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

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op het symbool ⋮ van de gewenste apparaatkaart en selecteer **Profiel**.
4. Klik op **Eigenaar toevoegen**, vul de bijbehorende velden in, stel het geslacht en de geboortedatum in en voeg eventueel een profielafbeelding toe.
5. Klik op **Toevoegen** om het profiel op te slaan.
6. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en klik op **Toewijzen**.

Bitdefender van op afstand op een apparaat updaten:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.

3. Klik op de ⋮ -icoon op de gewenste toestelkaart en selecteer vervolgens **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, komen de volgende tabbladen beschikbaar:

- **Bedieningspaneel**. In dit venster kunt u de beschermingsstatus van uw Bitdefender-producten en aantal resterende dagen op uw abonnement controleren. De beschermmingsstatus kan groen zijn als er geen probleem is met uw product, of rood als het toestel risico loopt. Als er problemen zijn die uw product aantasten, klik op **Problemen bekijken** om meer informatie te bekijken. Van hieruit kunt u problemen manueel oplossen die de veiligheid van uw toestellen aantasten.
- **Bescherming**. Vanuit dit venster kunt u van op afstand een Snelle of Systeemscan uitvoeren op uw toestellen. Klik op de **SCAN**-knop om het proces te starten. U kunt ook nagaan wanneer de laatste scan werd uitgevoerd op het toestel en van de laatste scan met de belangrijkste informatie is er een verslag beschikbaar.Voor meer informatie over deze twee scanprocessen, verwijzen we naar "*Een systeemscan uitvoeren*" (p. 86) en naar "*Een snelle scan uitvoeren*" (p. 86).
- **Kwetsbaarheid**. Om de eventuele kwetsbaarheid van een toestel te controleren, zoals ontbrekende Window-updates, verouderde applicaties of zwakke wachtwoorden, klik op de **SCAN**-knop in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet van op afstand afgehandeld worden. Indien er een kwetsbaarheid wordt opgemerkt, moet u een nieuwe scan op het toestel laten lopen en daarna de aanbevolen acties ondernemen. Klik op **Meer details** om naar een gedetailleerd rapport over de gevonden problemen te gaan. Voor meer informatie over deze functie, verwijzen we naar "*Kwetsbaarheid*" (p. 108).

6.4. Mijn account

In **Mijn Account** kunt u uw profiel personaliseren, het wachtwoord van uw account wijzigen, de aanmeldsessies en de Bitdefender Central-helpberichten beheren.

OnZodra u in de rechterbovenhoek van het scherm op de 👤-icoon klikt, krijgt u de volgende tabs:

- **Profiel** - hier kunt u accountinformatie toevoegen en bewerken.
- **Wachtwoord wijzigen** - van hieruit kunt u het wachtwoord bij uw account wijzigen.
- **Sessiebeheer** - hier kunt u de recentste inactieve en actieve aanmeldsessies die op apparaten van uw account lopen, bekijken en beheren.
- **Instellingen** - hier kunt u de helpberichten van de Bitdefender Central in- en uitschakelen en beslissen of u al dan niet een bericht wenst te ontvangen wanneer er foto's gemaakt worden op uw apparaten.

6.5. Notificaties

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.

7. BITDEFENDER UP-TO-DATE HOUDEN

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

Als u via breedband of DSL verbonden bent met het Internet, zal Bitdefender deze taak op zich nemen. Standaard controleert het of er updates zijn als u uw computer aanzet en ieder **uur** daarna. Als er een update beschikbaar is, wordt deze automatisch gedownload en op uw computer geïnstalleerd.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden en tegelijkertijd wordt elk zwak punt uitgesloten.

Belangrijk
Houd Automatische update ingeschakeld om u te beschermen tegen de laatste bedreigingen.

In sommige specifieke situaties is uw tussenkomst vereist om de bescherming van uw Bitdefender up-to-date te houden:

- Als uw computer een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in "*Bitdefender configureren voor het gebruik van een proxy-internetverbinding*" (p. 71).
- Er kunnen fouten optreden tijdens het downloaden van updates bij een trage internetverbinding. Raadpleeg "*Bitdefender updaten bij een langzame internetverbinding*" (p. 151) voor meer informatie over het oplossen van dergelijke fouten.
- Als u met het Internet bent verbonden via een inbelverbinding, dan adviseren wij Bitdefender regelmatig handmatig te updaten. Meer informatie vindt u onder "*Een update uitvoeren*" (p. 45).

7.1. Controleren of Bitdefender up-to-date is

Om het tijdstip van de laatste update van uw Bitdefender te controleren, controleert u de **Beveiligingsstatus** links van het Statusgebied.

Controleer de updategebeurtenissen voor gedetailleerde informatie over de laatste updates:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste update.

U kunt uitzoeken wanneer updates werden gestart en u kunt informatie over de updates weergeven (of ze al dan niet gelukt zijn, of het opnieuw opstarten is vereist om de installatie te voltooien, enz.); Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

7.2. Een update uitvoeren

Om updates uit te voeren is een internetverbinding vereist.

Voer een van de volgende bewerkingen uit om een update te starten:

- Open de Bitdefender-interface en klik op de koppeling **NU UPDATEN** onder de status van uw programma.
- Klik met de rechtermuisknop op het Bitdefender pictogram in het systeemvak en selecteer **Nu bijwerken**.

De module Update maakt een verbinding met de updateserver van Bitdefender en controleert op updates. Als een update is gedetecteerd, wordt u gevraagd de update te bevestigen, of wordt de update automatisch uitgevoerd, afhankelijk van de Update-instellingen.

> **Belangrijk**
> Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. Wij adviseren dit zo snel mogelijk te doen.

U kunt ook van op afstand updates uitvoeren op uw apparaten, op voorwaarde dat ze ingeschakeld zijn en met het internet verbonden zijn.

Bitdefender van op afstand op een apparaat updaten:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de -icoon op de gewenste toestelkaart en selecteer vervolgens **Update**.

7.3. De automatische update in- of uitschakelen

De automatische update in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **UPDATE**.
3. Klik op de bijhorende schakelaar om de Automatische Update in of uit te schakelen.
4. Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kunt de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de automatische update zo kort mogelijk uit te schakelen. Als Bitdefender niet regelmatig wordt geüpdatet, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

7.4. De update-instellingen aanpassen

De updates kunnen worden uitgevoerd vanaf het lokale netwerk, via het Internet, rechtstreeks of via een proxyserver. Bitdefender zal standaard elk uur via het Internet controleren op updates en de beschikbare updates zonder enige waarschuwing installeren.

De standaardinstellingen voor de update zijn geschikt voor de meeste gebruikers en u hoeft ze normaal niet te wijzigen.

De update-instellingen aanpassen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **UPDATE** en pas de instellingen volgens uw voorkeuren aan.

Update-frequentie

Bitdefender is zo geconfigureerd dat het elk uur controleert op updates. Om de updatefrequentie te wijzigen, sleept u de glijder langs de schaal om de gewenste tijd in te stellen wanneer de update moet plaatsvinden.

Update-locatie

Bitdefender is geconfigureerd om een update uit te voeren vanaf de Bitdefender-updateservers op Internet. De updatelocatie is een algemeen internetadres dat automatisch wordt omgeleid naar dichtstbijzijnde Bitdefender-updateserver in uw regio.

Wijzig de updatelocatie niet tenzij u dit wordt aangeraden door een Bitdefender-vertegenwoordiger of door uw netwerkbeheerder (als u verbonden bent met een kantoornetwerk).

U kunt terugkeren naar de algemene locatie voor internetupdates door op **STANDAARD** te klikken.

Regels voor behandelen updates

U hebt de keuze uit drie manieren voor het downloaden en installeren van de updates.

- **Stille update** - Bitdefender downloadt en installeert de update automatisch.
- **Herinneren voor het downloaden** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.
- **Herinneren voor het installeren** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

Voor sommige updates moet het systeem opnieuw worden opgestart om de installatie te voltooien. Als een update het opnieuw opstarten van het systeem vereist, blijft Bitdefender werken met de oude bestanden tot de gebruikers de computer opnieuw opstart. Hiermee wordt voorkomen dat de Bitdefender-update het werk van de gebruiker hinder.

Als u een vraag om bevestiging wilt wanneer een update het opnieuw opstarten van het systeem vereist, schakelt u de optie **Opnieuw opstarten uitstellen** uit door op de overeenkomende schakelaar te klikken.

ZO WERKT HET

8. INSTALLATIE

8.1. Hoe installeer ik Bitdefender op een tweede computer?

Indien de abonnement dat u hebt gekocht meer dan één computer dekt, kunt u uw Bitdefender-account gebruiken om een tweede pc te activeren.

Bitdefender op een tweede computer installeren:

1. Klik op de koppeling **EEN ANDER APPARAAT INSTALLEREN**.

   U wordt afgeleid naar de Bitdefender-account webpagina. Zorg ervoor dat u aangemeld bent met uw gegevens.

2. In het venster dat verschijnt, selecteert u het gewenste besturingssysteem, en klikt u op **VERDERGAAN**.

3. Voer het e-mailadres in waar we de downloadkoppeling voor de installatie van het gekozen platform heen moeten sturen.

4. Start het gedownloade Bitdefender-programma. Wacht tot het installatieproces is voltooid en sluit het venster.

Het nieuwe toestel waarop u het Bitdefender-product hebt geïnstalleerd, zal op uw Bitdefender Central-bedieningspaneel verschijnen.

8.2. Wanneer moet ik Bitdefender opnieuw installeren?

In sommige situaties zult u mogelijk uw Bitdefender-product opnieuw moeten installeren.

Typische situaties waarin u Bitdefender opnieuw moet installeren, zijn ondermeer de volgende:

- u hebt het besturingssysteem opnieuw geïnstalleerd..
- u hebt een nieuwe computer aangeschaft.
- u wilt de weergavetaal van de Bitdefender-interface wijzigen.

Om Bitdefender opnieuw te installeren, kunt u de installatieschijf gebruiken die u hebt aangeschaft of kunt u een nieuwe versie downloaden via Bitdefender Central.

Raadpleeg "*Uw Bitdefender-product installeren*" (p. 5) voor meer informatie over het Bitdefender-installatieproces.

8.3. Waar kan ik mijn Bitdefender-product van downloaden?

U kunt Bitdefender installeren vanaf de installatiedisk of via de web installer die u naar uw computer kunt downloaden vanaf uw computer via het Bitdefender Central-platform.

Opmerking
Voordat u de kit uitvoert, raden we aan om antivirusoplossingen op uw systeem te verwijderen. Wanneer u meer dan één beveiligingsoplossing op dezelfde computer gebruikt, wordt het systeem onstabiel.

Bitdefender installeren via Bitdefender Central:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik in het venster **MIJN APPARATEN** op **Bitdefender INSTALLEREN**.
4. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

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

     Selecteer **Windows** om uw Bitdefender-product te downloaden en klik vervolgens op **VERDERGAAN**. Voer een e-mailadres in in het overeenkomstige veld en klik op **VERZENDEN**.
5. Start het gedownloade Bitdefender-programma.

8.4. Hoe kan ik de taal van mijn Bitdefender-product veranderen?

Indien u Bitdefender in een andere taal wilt gebruiken, moet u het product opnieuw installeren met de juiste taal.

Om Bitdefender in een andere taal:

1. Bitdefender verwijderen door het volgen van deze stappen:

- In **Windows 7**:
  a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  b. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
  c. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
     - Bestanden in quarantaine
     - Wallets
  d. Klik op **VERDERGAAN**.
  e. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
  d. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
     - Bestanden in quarantaine
     - Wallets
  e. Klik op **VERDERGAAN**.
  f. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:
  a. Klik op **Start**, klik dan op Instellingen.
  b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
  d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

e. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

- Bestanden in quarantaine
- Wallets

f. Klik op **VERDERGAAN**.

g. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

2. De taal van Bitdefender Central wijzigen:
   a. Ga naar Bitdefender Central.
   b. Klik bovenaan rechts op het scherm op de icoon.
   c. Klik op **Mijn account** in het schuifmenu.
   d. Selecteer het tabblad **Profiel**.
   e. Selecteer een taal uit de uitklaplijst **Taal** en klik op **OPSLAAN**.
3. Download het installatiebestand:
   a. Selecteer het paneel **Mijn apparaten**.
   b. Klik in het venster **MIJN APPARATEN** op **Bitdefender INSTALLEREN**.
   c. Kies een van de twee beschikbare opties:

- **DOWNLOADEN**

  Klik op de knop en sla het installatiebestand op.

- **Op een ander apparaat**

  Selecteer **Windows** om uw Bitdefender-product te downloaden en klik vervolgens op **VERDERGAAN**. Voer een e-mailadres in in het overeenkomstige veld en klik op **VERZENDEN**.

4. Start het gedownloade Bitdefender-programma.

8.5. Hoe gebruik ik mijn Bitdefender-abonnement na een Windows-upgrade?

Deze situatie doet zich voor wanneer u uw besturingssysteem upgrade en verder wilt gaan met het gebruik van uw Bitdefender-abonnement.

Als u een vorige versie van Bitdefender gebruikt, kunt u gratis upgraden naar de nieuwste Bitdefender op de volgende wijze:

- Van een vorige Bitdefender Antivirusversie naar de nieuwste Bitdefender Antivirus die beschikbaar is.
- Van een vorige Bitdefender Internet Security versie naar de nieuwste Bitdefender Internet Security die beschikbaar is.
- Van een vorige Bitdefender Total Security versie naar de nieuwste Bitdefender Total Security die beschikbaar is.

Er kunnen zich twee gevallen voordoen:

- U hebt het besturingssysteem bijgewerkt met gebruikmaking van Windows Update en u merkt dat Bitdefender niet langer werkt.

  In dit geval moet u het product opnieuw installeren met gebruikmaking van de nieuwste versie die beschikbaar is.

  Om dit probleem op te lossen:

  1. Bitdefender verwijderen door het volgen van deze stappen:
     - In **Windows 7**:
       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
       b. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
       c. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
          - Bestanden in quarantaine
          - Wallets
       d. Klik op **VERDERGAAN**.
       e. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8 en Windows 8.1**:
       a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
       b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.

c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

d. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

- Bestanden in quarantaine
- Wallets

e. Klik op **VERDERGAAN**.

f. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:

a. Klik op **Start**, klik dan op Instellingen.

b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.

c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

e. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

- Bestanden in quarantaine
- Wallets

f. Klik op **VERDERGAAN**.

g. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

2. Download het installatiebestand:

a. Ga naar Bitdefender Central.

b. Selecteer het paneel **Mijn apparaten**.

c. Klik in het venster **MIJN APPARATEN** op **Bitdefender INSTALLEREN**.

d. Kies een van de twee beschikbare opties:

- **DOWNLOADEN**

  Klik op de knop en sla het installatiebestand op.

- **Op een ander apparaat**

  Selecteer **Windows** om uw Bitdefender-product te downloaden en klik vervolgens op **VERDERGAAN**. Voer een e-mailadres in in het overeenkomstige veld en klik op **VERZENDEN**.

3. Start het gedownloade Bitdefender-programma.

- U hebt uw systeem gewijzigd en u wilt doorgaan met het gebruik van de beveiliging van Bitdefender.

  Daarvoor moet u het product opnieuw installeren met gebruikmaking van de nieuwste versie.

  Om dit probleem op te lossen:

  1. Download het installatiebestand:
     a. Ga naar Bitdefender Central.
     b. Selecteer het paneel **Mijn apparaten**.
     c. Klik in het venster **MIJN APPARATEN** op **Bitdefender INSTALLEREN**.
     d. Kies een van de twee beschikbare opties:

        - **DOWNLOADEN**

          Klik op de knop en sla het installatiebestand op.

        - **Op een ander apparaat**

          Selecteer **Windows** om uw Bitdefender-product te downloaden en klik vervolgens op **VERDERGAAN**. Voer een e-mailadres in in het overeenkomstige veld en klik op **VERZENDEN**.

  2. Start het gedownloade Bitdefender-programma.

  Raadpleeg "*Uw Bitdefender-product installeren*" (p. 5) voor meer informatie over het Bitdefender-installatieproces.

8.6. Hoe herstel ik Bitdefender?

Indien u uw Bitdefender Antivirus Plus 2017 wilt herstellen vanuit het Windows-startmenu:

- In **Windows 7**:

  1. Klik op **Start** en ga naar **Alle Programma's**.
  2. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

3. Klik op **HERSTELLEN** in het venster dat verschijnt.

   Dit kan enkele minuten duren.

4. U moet de computer opnieuw opstarten om het proces te voltooien.

- In **Windows 8 en Windows 8.1**:

1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
3. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
4. Klik op **HERSTELLEN** in het venster dat verschijnt.

   Dit kan enkele minuten duren.

5. U moet de computer opnieuw opstarten om het proces te voltooien.

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op de **Systeem**-icoon in Instellingen, selecteer dan **Apps & functies**.
3. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **HERSTELLEN**.

   Dit kan enkele minuten duren.

6. U moet de computer opnieuw opstarten om het proces te voltooien.

9. ABONNEMENTEN

9.1. Hoe activeer ik het Bitdefender-abonnement met een licentiesleutel?

Indien u een geldige licentiesleutel hebt en u deze wilt gebruiken om een abonnement voor Bitdefender Antivirus Plus 2017 te activeren, hebt u twee keuzes:

- U hebt een upgrade gedaan voor een vorige Bitdefender-versie naar de nieuwe:
  1. Zodra de upgrade naar Bitdefender Antivirus Plus 2017 voltooid is, wordt u gevraagd u aan te melden op uw Bitdefender-account.
  2. Klik op **Aanmelden** en voer het e-mailadres en het wachtwoord van uw Bitdefender-account in.
  3. Klik op **AANMELDEN** om door te gaan.
  4. Er verschijnt een kennisgeving die u meldt dat een abonnement werd aangemaakt op uw accountscherm. Het aangemaakte abonnement zal geldig zijn voor de resterende dagen op uw licentiesleutel en voor hetzelfde aantal gebruikers.

     Toestellen die eerdere versies van Bitdefender gebruiken en geregistreerd zijn met de licentiesleutel, die u naar een abonnement hebt geconverteerd, moeten het product activerenmet dezelfde Bitdefender-account.
- Bitdefender werd eerder nog niet op het systeem geïnstalleerd:
  1. Zodra het installatieproces voltooid is, wordt u gevraagd u aan te melden op uw Bitdefender-account.
  2. Klik op **Aanmelden** en voer het e-mailadres en het wachtwoord van uw Bitdefender-account in.
  3. Klik op **AANMELDEN** om verder te gaan en daarna op de knop **VOLTOOIEN** om naar de Bitdefender Antivirus Plus 2017-interface te gaan.
  4. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  5. Selecteer de koppeling **Activatiecode**.

Er verschijnt een nieuw venster.

6. Klik op de koppeling **Ontvang nu uw GRATIS upgrade!**.
7. Voer uw licentiesleutel in het overeenkomende veld in en klik op **MIJN PRODUCT UPGRADEN**. Een abonnement met dezelfde beschikbaarheid en aantal gebruikers van uw licentiesleutel is verbonden met uw account.

10. BITDEFENDER CENTRAL

10.1. Hoe meld ik me aan op Bitdefender Central terwijl ik een andere online account gebruik?

U hebt een nieuwe Bitdefender-account aangemaakt en u wilt deze van nu af aan gebruiken.

Een andere account met succes gebruiken:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op **VERANDEREN VAN ACCOUNT** om de account die aan de computer is gekoppeld, te wijzigen.
3. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in en klik dan op **AANMELDEN**.

> **Opmerking**
> Het Bitdefender-product van uw toestel verandert automatisch volgens het abonnement dat verbonden is met de nieuwe Bitdefender-account.
> Als er geen beschikbaar abonnement gekoppeld is aan de Bitdefender-account, of als u deze wilt overzetten naar de vorige account, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in deel "*Hulp vragen*" (p. 169).

10.2. Hoe schakel ik Bitdefender Central-hulpberichten uit?

Om u te helpen begrijpen waar elke optie in Bitdefender Central nuttig voor is, worden hulpberichten op de overzichtspagina weergegeven.

Indien u deze berichten niet meer wil zien:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Mijn account** in het schuifmenu.
4. Selecteer het tabblad **Instellingen**.
5. Schakel de optie **Hulpberichten in/uitschakelen** uit.

10.3. Hoe kan ik de snapshots die op mijn apparaten genomen zijn, niet meer zien?

Om de op uw apparaten gemaakte fotosnaps niet langer zichtbaar te maken:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Mijn account** in het schuifmenu.
4. Selecteer het tabblad **Instellingen**.
5. Inactiveer de optie **Snapshots die met uw apparaten zijn gemaakt, tonen/niet tonen**.

10.4. Ik ben het wachtwoord dat ik voor mijn Bitdefender-account heb gekozen, vergeten. Hoe kan ik het terugstellen?

Er zijn twee mogelijkheden om een nieuw wachtwoord in te stellen voor uw Bitdefender-account:

- Vanuit de Bitdefender-interface:

  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de knop **SWITCH ACCOUNT**.

     Er verschijnt een nieuw venster.
  3. Klik op de link **Mijn wachtwoord vergeten**.
  4. Typ het e-mailadres dat u hebt gebruikt om Bitdefender-account aan te maken en klik op de knop **WACHTWOORD VERGETEN**.
  5. Controleer uw e-mail en klik op de verschafte knop.
  6. Typ uw e-mailadres in het overeenkomende veld in.
  7. Typ het nieuwe wachtwoord. Het wachtwoord moet minstens 8 karakters lang zijn en cijfers bevatten.
  8. Klik op de knop **WACHTWOORD TERUGSTELLEN**.

- Vanuit uw Bitdefender-account:

  1. Ga naar Bitdefender Central.

2. Klik bovenaan rechts op het scherm op de icoon.
3. Klik op **Mijn account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord wijzigen**.
5. Typ het oude wachtwoord in het veld **Oud wachtwoord** in.
6. Tik het nieuwe wachtwoord dat u voor uw account wilt gebruiken in het veld **Nieuw wachtwoord** in.
7. Klik op de knop **WACHTWOORD WIJZIGEN**.

Om naar uw Bitdefender-account te gaan tikt u voortaan uw e-mailadres en het wachtwoord in dat u net ingesteld hebt.

10.5. Hoe kan ik de aanmeldsessies van mijn Bitdefender-account beheren?

In uw Bitdefender-account kunt u de recentste inactieve en actieve aanmeldsessies op de apparaten van uw account bekijken. Bovendien kunt u van op afstand afmelden via deze stappen:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon.
3. Klik op **Mijn account** in het schuifmenu.
4. Selecteer het tabblad **Sessiebeheer**.
5. In **Actieve sessies** selecteert u de optie **AFMELDEN** naast het apparaat waar u de aanmeldsessie wenst stop te zetten.

11. SCANNEN MET BITDEFENDER

11.1. Een bestand of map scannen

De eenvoudigste manier om een bestand of map te scannen is klikken met de rechtermuisknop op het object dat u wilt scannen, Bitdefender aanwijzen en **Scannen met Bitdefender** te selecteren in het menu.

Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Typische situaties voor het gebruik van deze scanmethode zijn ondermeer de volgende:

- U vermoedt dat een specifiek bestand of een specifieke map geïnfecteerd is.
- Wanneer u bestanden waarvan u denkt dat ze mogelijk gevaarlijk zijn, downloadt van Internet.
- Scan een netwerkshare voordat u bestanden naar uw computer kopieert.

11.2. Hoe kan ik mijn systeem scannen?

Om een volledige scan van het systeem uit te voeren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Systeemscan**.
4. Volg de Systeemscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.

   Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Meer informatie vindt u onder "*Antivirusscanwizard*" (p. 90).

11.3. Hoe plan ik een scan?

U kunt uw Bitdefender-product instellen om belangrijke systeemlocaties te beginnen scannen wanneer u niet voor de computer zit.

Een scan plannen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Scans beheren**.
4. Om het scantype te kiezen dat u wilt plannen, volledige systeemscan of snelle scan, klikt u op **Scanopties**.

   U kunt ook een scantype aanmaken om aan uw behoeften aan te passen door op **Nieuwe aangepaste taak** te klikken.
5. Activeer de **Planning**-schakelaar.

   Selecteer een van de overeenkomstige opties om een planning in te stellen:

   - Bij opstarten systeem
   - Eenmalig
   - Periodiek

In het **Doelen scannen**-venster kunt u locaties selecteren die u wilt scannen.

11.4. Een aangepaste scantaak maken

Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

Ga als volgt te werk om een aangepaste scantaak te maken:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Scans beheren**.
4. Klik op **Nieuwe taak op maat**. Voer onder de tab **Basis** een naam in voor de scan en selecteer de locaties die gescand moeten worden.
5. Klik op de tab **Geavanceerd** als u de scanopties in detail wilt configureren.

U kunt de scanopties gemakkelijk configureren door het scanniveau aan te passen. Sleep de schuifregelaar langs de schaal om het gewenste scanniveau in te stellen.

U kunt er ook voor kiezen de computer uit te schakelen wanneer de scan is voltooid en er geen bedreigingen zijn gevonden. Denk eraan dat dit, telkens wanneer u deze taak uitvoert, het standaard gedrag zal zijn.

6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.
7. Gebruik de overeenkomstige schakelaar indien u een planning wilt instellen voor uw scantaak.
8. Klik op **Scan starten** en volg de scanwizard om de scan te voltooien. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.
9. Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

11.5. Een map uitsluiten van de scan

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen.

Uitsluitingen zijn bedoeld voor gebruikers met een gevorderde computerkennis en alleen in de volgende situaties:

- U hebt een grote map op uw systeem waarin u films en muziek bewaart.
- U hebt een groot archief op uw systeem waarin u verschillende gegevens bewaart.
- U bewaart een map waarin u verschillende types software en toepassingen installeert voor testdoeleinden. Het scannen van de map kan resulteren in het verlies van bepaalde gegevens.

De map aan de lijst Uitsluitingen toevoegen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **UITSLUITINGEN**.

5. Klik op het uitklapmenu **Lijst van bestanden en mappen die uitgesloten worden voor de scan**.
6. Klik op de knop **ADD**.
7. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**.
8. Klik op **Toevoegen** om de wijzigingen op te slaan en het venster te sluiten.

11.6. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt?

Er kunnen gevallen zijn waarbij Bitdefender een rechtmatig bestand verkeerdelijk markeert als een bedreiging (vals positief). Om deze fout te corrigeren, voegt u het bestand toe aan het gebied Uitsluitingen van Bitdefender:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Selecteer de koppeling **MODULES BEKIJKEN**.
   c. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
   d. In het tabblad **SCHILD** klikt u op de bijhorende schakelaar om On-access scanning uit te schakelen.

      Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart.
2. Verborgen objecten weergeven in Windows. Raadpleeg "*Verborgen objecten weergeven in Windows*" (p. 72) voor meer informatie hierover.
3. Het bestand herstellen vanaf het quarantainegebied:
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Selecteer de koppeling **MODULES BEKIJKEN**.
   c. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.

d. Selecteer het tabblad **QUARANTAINE**.

e. Selecteer het bestand en klik op **HERSTEL**.

4. Het bestand toevoegen aan de lijst Uitsluitingen. Raadpleeg "*Een map uitsluiten van de scan*" (p. 64) voor meer informatie hierover.
5. Schakel de real time antivirusbeveiliging van Bitdefender in.
6. Neem contact op met de medewerkers van onze ondersteuningsdienst zodat wij de detectiehandtekening kunnen verwijderen. Raadpleeg "*Hulp vragen*" (p. 169) voor meer informatie hierover.

11.7. Hoe kan ik controleren welke virussen Bitdefender heeft gedetecteerd?

Telkens wanneer een scan wordt uitgevoerd, wordt een scanlogboek gemaakt en registreert Bitdefender de verwijderde problemen.

Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **LOGBOEK WEERGEVEN** te klikken.

Een scanlog of een gedetecteerde infectie later bekijken:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste scan.

   Hier vindt u alle gebeurtenissen van scans op malware, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
3. In de kennisgevingenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een kennisgeving om details erover weer te geven.
4. Klik op **LOGBOEK WEERGEVEN** om het scanlogboek te openen.

12. PRIVACYBEHEER

12.1. Hoe kan ik controleren of mij online transactie beveiligd is?

Als u wilt controleren of uw online bewerkingen privé blijven, kunt u de browser die door Bitdefender is geleverd, gebruiken voor het beschermen van uw transacties en toepassingen voor thuisbankieren.

Bitdefender Safepay™ is een beveiligde browser die is ontwikkeld om uw creditcardgegevens, accountnummer of andere vertrouwelijke gegevens die u mogelijk invoert bij toegang tot verschillende online locaties, te beschermen.

Uw online activiteit veilig en privé houden:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **Safepay**.
3. Klik op de knop om toegang te krijgen tot het **virtuele toetsenbord**.

   Gebruik het **virtuele toetsenbord** wanneer u vertrouwelijke informatie, zoals uw wachtwoorden, invoert.

12.2. Hoe kan ik een bestand definitief verwijderen met Bitdefender?

Als u een bestand definitief van uw systeem wilt verwijderen, moet u de gegevens fysiek verwijderen van uw harde schijf.

De Bestandsvernietiging van Bitdefender zal u helpen om bestanden of mappen snel permanent te verwijderen van uw computer via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u definitief wilt verwijderen, wijs Bitdefender aan en selecteer **Bestandsvernietiging**.
2. Er wordt een bevestigingsvenster weergegeven. Klik op **JA, VERWIJDEREN** om de wizard Bestandsvernietiging te starten.

   Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.
3. De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

13. NUTTIGE INFORMATIE

13.1. Hoe kan ik mijn antivirusoplossing testen?

Om er zeker van te zijn dat uw Bitdefender-product correct werkt, raden we u aan de Eicartest te gebruiken.

Met de Eicartest kunt u uw antivirusbeveiliging controleren met gebruikmaking van een veilig bestand dat hiervoor is ontwikkeld.

Uw antivirusoplossing testen:

1. Download de test van de officiële webpagina van de EICAR-organisatie http://www.eicar.org/.
2. Klik op de tab **Antimalware Testbestand**.
3. Klik in het menu aan de linkerzijde op **Downloaden**.
4. Vanuit **Downloadgedeelte met gebruikmaking van standaardprotocol http** klikt u op het testbestand **eicar.com**.
5. U zult erover worden geïnformeerd dat de pagina waar u heen probeert te gaan het EICAR-Testbestand bevat (geen virus).

   Indien u klikt op **Ik begrijp de risico's, breng me er toch heen**, dat start de download van de test en een Bitdefender-pop-up informeert u dat er een virus is gedetecteerd.

   Klik op **Meer details** om meer informatie over deze handeling te krijgen.

Indien u geen Bitdefender-waarschuwing wilt ontvangen, raden we u aan om contact op te nemen met Bitdefender voor ondersteuning zoals beschreven in deel "*Hulp vragen*" (p. 169).

13.2. Hoe kan ik Bitdefender verwijderen?

Als u uw Bitdefender Antivirus Plus 2017 wilt verwijderen:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

- Bestanden in quarantaine
- Wallets

4. Klik op **VERDERGAAN**.
5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8 en Windows 8.1**:

1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
3. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
4. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
   - Bestanden in quarantaine
   - Wallets
5. Klik op **VERDERGAAN**.
6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
3. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
   - Bestanden in quarantaine
   - Wallets
6. Klik op **VERDERGAAN**.

7. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

13.3. Hoe kan ik de computer automatisch afsluiten nadat het scannen is voltooid?

Bitdefender biedt meerdere scantaken die u kunt gebruiken om zeker te zijn dat uw systeem niet is geïnfecteerd door malware. Het scannen van de volledige computer kan langer duren, afhankelijk van de hardware- en softwareconfiguratie van uw systeem.

Omwille van deze reden biedt Bitdefender u de mogelijkheid Bitdefender te configureren om uw systeem af te sluiten zodra het scannen is voltooid.

Overweeg dit voorbeeld: u bent klaar met uw werk op de computer en wilt naar bed. U wilt dat Bitdefender uw volledig systeem controleert op malware.

In dat geval kunt u Bitdefender op de volgende manier instellen om het systeem uit te schakelen nadat de scan is voltooid.

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Scans beheren**.
4. Klik in het venster **SCANTAKEN BEHEREN** op **Nieuwe aangepaste taak** om een naam in te voeren voor de scan en selecteer de locaties die gescand moeten worden.
5. Klik op de tab **Geavanceerd** als u de scanopties in detail wilt configureren.
6. Kies om de computer uit te schakelen wanneer de scan is voltooid en er geen bedreigingen zijn gevonden.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.
8. Klik op de **Scan starten**-knop om uw systeem te scannen.

Als er geen bedreigingen zijn gevonden, wordt de computer uitgeschakeld.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Meer informatie vindt u onder “*Antivirusscanwizard*” (p. 90).

13.4. Bitdefender configureren voor het gebruik van een proxy-internetverbinding

Als uw computer een internetverbinding maakt via een proxyserver, moet u Bitdefender configureren met de proxy-instellingen. Bitdefender zal standaard de proxy-instellingen van uw systeem automatisch detecteren en importeren.

Belangrijk
Internetverbindingen bij u thuis gebruiken doorgaans geen proxyserver. Als vuistregel is het aanbevolen de proxyverbindingsinstellingen van uw Bitdefender-programma te controleren en te configureren wanneer de updates niet werken. Als Bitdefender een update kan uitvoeren, dan is de toepassing correct geconfigureerd voor het maken van een internetverbinding.

Uw proxy-instellingen beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **GEAVANCEERD**.
3. Schakel het proxygebruik in door op de schakelaar te klikken.
4. Klik op de koppeling **Proxy's beheren**.
5. Er zijn twee opties voor het instellen van de proxy-instellingen:
   - **Proxy-instellingen van de standaardbrowser importeren** - proxy-instellingen van de huidige gebruiker, opgehaald van de standaardbrowser. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.

     Opmerking
     Bitdefender kan proxy-instellingen van de populairste browsers importeren, inclusief de nieuwste versies van Internet Explorer, Mozilla Firefox en Google Chrome.

   - **Proxy-instellingen aanpassen** - proxy-instellingen die u zelf kunt configureren. U moet de volgende instellingen definiëren:
     - **Adres** - voer het IP-adres van de proxyserver in.
     - **Poort** - voer de poort in die Bitdefender gebruikt om een verbinding te maken met de proxyserver.

- **Gebruikersnaam** - voer een gebruikersnaam in die wordt herkend door de proxy.
- **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.

6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Bitdefender gebruikt de beschikbare proxy-instellingen tot er een internetverbinding kan worden gemaakt.

13.5. Gebruik ik een 32- of 64-bits versie van Windows?

Nagaan of u een besturingssysteem van 32 bits of 64 bits hebt:

- In **Windows 7**:
  1. Klik op **Start**.
  2. Zoek **Computer** in het menu **Start**.
  3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
  4. Kijk onder **Systeem** om de informatie over uw systeem te controleren.
- In **Windows 8**:
  1. Zoek vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm) en rechterklik op het pictogram ervan.

     Zoek in **Windows 8.1**, naar **Deze computer**.
  2. Selecteer **Eigenschappen** in het onderste menu.
  3. Kijk in Systeem om uw systeemtype te zien.
- In **Windows 10**:
  1. Typ "Systeem" in het zoekveld in de taakbalk en klik op het pictogram ervan.
  2. Kijk bij Systeem om informatie over uw systeemtype te vinden.

13.6. Verborgen objecten weergeven in Windows

Deze stappen zijn nuttig in de gevallen waarin u te maken krijgt met een malware en u de geïnfecteerde bestanden die kunnen verborgen zijn, te vinden en te verwijderen.

Volg deze stappen om verborgen objecten weer te geven in Windows.

1. Klik op **Start**, ga naar **Beheerpaneel**.

   In **Windows 8 en Windows 8.1**: Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.

2. Selecteer **Mapopties**.
3. Ga naar het tabblad **Weergave**.
4. Selecteer **Verborgen bestanden en mappen weergeven**.
5. Vink **Extensies voor bekende bestandstypen verbergen** uit.
6. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.
7. Klik op **Toepassen**, klik daarna op **OK**.

In **Windows 10**:

1. Typ "Verborgen bestanden en mappen tonen" in het zoekveld in de taakbalk en klik op het pictogram ervan.
2. Selecteer **Verborgen bestanden, mappen en drives tonen**.
3. Vink **Extensies voor bekende bestandstypen verbergen** uit.
4. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.
5. Klik op **Toepassen**, klik daarna op **OK**.

13.7. Andere beveiligingsoplossingen verwijderen

De hoofdreden voor het gebruik van een beveiligingsoplossing is het bieden van bescherming en veiligheid voor uw gegevens. Maar wat gebeurt er als er meerdere beveiligingsproducten aanwezig zijn op hetzelfde systeem?

Wanneer u meer dan één beveiligingsoplossing op dezelfde computer gebruikt, wordt het systeem onstabiel. Het installatieprogramma van Bitdefender Antivirus Plus 2017 detecteert automatisch andere beveiligingsprogramma's en biedt u de mogelijkheid om ze te verwijderen.

Indien u de andere beveiligingsoplossingen niet hebt verwijderd tijdens de eerste installatie:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
  4. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:
  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Als u de andere beveiligingsoplossing niet van uw systeem kunt verwijderen, kunt u het hulpprogramma voor het verwijderen ophalen van de website van de verkoper of direct met hem contact opnemen voor richtlijnen betreffende het verwijderen.

13.8. Opnieuw opstarten in Veilige modus

De Veilige modus is een diagnostische gebruiksmodus die hoofdzakelijk wordt gebruikt om problemen op te lossen die de normale werking van Windows beïnvloeden. Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot virussen die verhinderen dat Windows normaal wordt gestart. In de Veilige modus werken slechts enkele toepassingen en laadt Windows alleen de basisbesturingsprogramma's en een minimum aan componenten van het besturingssysteem. Daarom zijn de meeste virussen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Windows in Veilige modus starten:

- In **Windows 7**:
  1. Start de computer opnieuw.
  2. Druk meerdere keren op de **F8**-toets voordat Windows wordt gestart om toegang te krijgen tot het opstartmenu.
  3. Selecteer **Veilige modus** in het opstartmenu of **Veilige modus met netwerkmogelijkheden** als u internettoegang wenst.
  4. Druk op **Enter** en wacht terwijl Windows wordt geladen in Veilige modus.
  5. Dit proces eindigt met een bevestigingsbericht. Klik op **OK** om te bevestigen.
  6. Om Windows normaal te starten, hoeft u alleen het systeem opnieuw op te starten.
- In **Windows 8, Windows 8.1 en Windows 10**:
  1. Lanceer **Systeemconfiguratie** in Windows door tegelijk op de toetsen **Windows + R** op uw keyboard te drukken.
  2. Schrijf **msconfig** in het dialoogvenster **Openen** en klik daarna op **OK**.
  3. Selecteer het tabblad **Opstarten**.
  4. In het gebied **Opstartopties** vinkt u het vakje **Veilig opstarten** aan.
  5. Klik op **Netwerk** en vervolgens op **OK**.
  6. Klik op **OK** in het venster **Systeemconfiguratie** dat u vertelt dat het systeem opnieuw moet worden opgestart om de wijzigingen die u hebt ingesteld, door te voeren.

Uw systeem wordt opnieuw opgestart in Veilige modus met Netwerk.

Om opnieuw op te starten normale modus, zet u de instellingen terug door de **Systeemoperati** opnieuw te lanceren en het vakje **Veilig opstarten** terug uit te vinken. Klik op **OK** en daarna op **Opnieuw opstarten**. Wacht tot de nieuwe instellingen toegepast zijn.

UW BEVEILIGING BEHEREN

14. ANTIVIRUSBEVEILIGING

Bitdefender beveiligt uw computer tegen alle types malware (virussen, Trojanen, spyware, rootkits, enz.). De Bitdefender-bescherming is ingedeeld in twee categorieën:

- Scannen bij toegang - verhindert dat nieuwe malware-bedreigingen uw systeem binnenkomen. Bitdefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.

  Met Scannen bij toegang bent u zeker van bescherming in real time tegen malware, een essentieel onderdeel van elk computerbeveiligingsprogramma.

  Belangrijk
  Houd **Scannen bij toegang** ingeschakeld om te verhinderen dat virussen uw computer infecteren.

- Scannen op aanvraag - hiermee kan u malware die al op uw systeem aanwezig is, detecteren en verwijderen. Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert het station, de map of het bestand dat Bitdefender moet scannen, en Bitdefender doet dat - op aanvraag.

Bitdefender scant automatisch alle verwisselbare media die op de computer zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend. Meer informatie vindt u onder "*Automatisch scannen van verwisselbare media*" (p. 94).

Geavanceerde gebruikers kunnen scanuitsluitingen configureren als ze niet willen dat er specifieke bestanden of bestandstypes worden gescand. Meer informatie vindt u onder "*Scanuitsluitingen configureren*" (p. 97).

Wanneer een virus of andere malware wordt gedetecteerd, zal Bitdefender automatisch proberen de malwarecode uit het geïnfecteerde bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd. Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 99).

Als uw computer werd geïnfecteerd door malware, moet u "*Malware van uw systeem verwijderen*" (p. 159) raadplegen. Om u te helpen bij het opruimen van

de malware die niet kan worden verwijderd van het Windows-besturingssysteem op uw computer, biedt Bitdefender u de Helpmodus. Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van malware, waarmee u uw computer onafhankelijk van Windows kunt opstarten. Wanneer de computer start in de Helpmodus, is de Windows-malware inactief zodat deze gemakkelijk kan worden verwijderd.

Om u te beschermen tegen ransomware en onbekende boosaardige toepassingen, gebruikt Bitdefender Actief dreigingsbeheer, een geavanceerde heuristische technologie die de toepassingen die op uw systeem worden uitgevoerd, doorlopend bewaakt. Actief dreigingsbeheer blokkeert automatisch toepassingen die zich als malware gedragen, om te verhinderen dat ze uw computer beschadigen. In sommige gevallen kunnen rechtmatige toepassingen worden geblokkeerd. In dergelijke situaties kunt u Actief dreigingsbeheer zo configureren dat het die toepassingen niet opnieuw blokkeert, door uitsluitingsregels aan te maken. Raadpleeg *"Actief dreigingsbeheer" (p. 101)* voor meer informatie.

14.1. Scannen bij toegang (real time-beveiliging)

Bitdefender verschaft voortdurende, realtime beveiliging tegen een uitgebreide serie malwarebedreigingen door alle bestanden en e-mailberichten waar toegang toe wordt gezocht te scannen.

De standaardinstellingen voor de real time-beveiliging, garanderen een goede beveiliging tegen malware, met een minimale impact op de systeemprestaties. U kunt de instellingen voor de real time-beveiliging gemakkelijk wijzigen volgens uw behoeften door naar een van de vooraf gedefinieerde beveiligingsniveaus te schakelen. Als u een geavanceerde gebruiker bent, kunt u de scaninstellingen in detail configureren door een aangepast beveiligingsniveau te maken.

14.1.1. De real time-beveiliging in- of uitschakelen

De bescherming tegen malware in reële tijd in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.

4. In het venster **SCHILD** klikt u op de bijhorende schakelaar om On-access scanning uit te schakelen.
5. Indien u bescherming in reële tijd wenst uit te schakelen, verschijnt een waarschuwingsscherm. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart. De realtime beveiliging wordt automatisch ingeschakeld als de geselecteerde tijd verloopt.

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 malware-bedreigingen.

14.1.2. Het real time-beveiligingsniveau aanpassen

Het real time-beveiligingsniveau definieert de scaninstellingen voor real time-beveiliging. U kunt de instellingen voor de real time-beveiliging gemakkelijk wijzigen volgens uw behoeften door naar een van de vooraf gedefinieerde beveiligingsniveaus te schakelen.

Het real time-beveiligingsniveau aanpassen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Sleep in het venster **SCHILD** de schuifregelaar langs de schaal om het gewenste beveiligingsniveau in te stellen. Gebruik de beschrijving aan de rechterzijde van de schaal om het beveiligingsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

14.1.3. De instellingen voor de realtime beveiliging configureren

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden. U kunt de instellingen voor de real

time-beveiliging in detail configureren door een aangepast beschermingsniveau te maken.

De instellingen voor de realtime beveiliging configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Sleep de scannerschuifregelaar van **On-access scannen** naar het niveau **AANGEPAST**.

   Er verschijnt een nieuw venster.
5. Configureer de scaninstellingen zoals dat nodig is.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de woordenlijst. U kunt ook nuttige informatie vinden door op het Internet te zoeken.
- **Scanopties voor geopende bestanden.** U kunt Bitdefender instellen om alleen alle geopende bestanden of toepassingen (programmabestanden) te scannen. Het scannen van alle geopende bestanden biedt de beste beveiliging, terwijl het scannen van toepassingen alleen kan worden gebruikt voor betere systeemprestaties.

  Standaard komen zowel lokale mappen als zaken die via het netwerk worden gedeeld in aanmerking voor scannen bij toegang. Voor betere systeemprestaties kunt u netwerklocaties uitsluiten van scannen bij toegang.

  Toepassingen (of programmabestanden) zijn veel kwetsbaarder voor malwareaanvallen dan andere bestandstypen. Deze categorie bevat de volgende bestandsextensies:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf;

mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Binnen archieven scannen.** Het scannen binnenin de archieven verloopt langzaam en is een veeleisend proces, waardoor het niet aanbevolen is voor de real time-beveiliging. Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem. De malware kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.

  Als u beslist deze optie te gebruiken, kunt u een maximaal geaccepteerde groottelimiet instellen voor archieven die bij toegang moeten worden gescand. Schakel het overeenkomende selectievakje in en typ de maximale archiefgrootte (in MB).

- **Scanopties voor e-mail en HTTP-verkeer.** Om te verhinderen dat er malware wordt gedownload naar uw computer, scant Bitdefender automatische de volgende ingangspunten van malware:
  - binnenkomende en uitgaande e-mails
  - HTTP-verkeer

  Het scannen van het webverkeer kan het surfen op het weg iets vertragen, maar het zal malware blokkeren die afkomstig is van Internet, inclusief downloads tijdens het passeren.

  Hoewel dit niet aanbevolen is, kunt u de antivirusscan van e-mails of het web uitschakelen om de systeemprestaties te verbeteren. Als u de overeenkomende scanopties uitschakelt, woden de e-mails en bestanden die zijn ontvangen of gedownload via Internet niet gescand, waardoor geïnfecteerde bestanden op uw computer moeten worden opgeslagen. Dit is geen belangrijke bedreiging omdat de real time-beveiliging de malware zal blokkeren wanneer u probeert toegang te krijgen tot de geïnfecteerde bestanden (openen, verplaatsen, kopiëren of uitvoeren).

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de

vereiste computercode om het opstartproces te starten. Als een virus het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kun starten en geen toegang meer hebt tot uw gegevens.

- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Scannen op keyloggers.** Selecteer deze optie om uw systeem te scannen op keyloggers. Keyloggers slaan op wat u op uw toetsenbord intypt en zenden via Internet verslagen naar een kwaadwillend persoon (hacker). De hacker kan gevoelige informatie uit de gestolen data halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.
- **Scannen bij opstarting systeem.** Selecteer de optie **Vroege opstartscan** om uw systeem te scannen bij het opstarten, zodra alle kritieke diensten geladen zijn. De bedoeling van deze functie is uw virusdetectie bij de opstarting van het systeem te verbeteren en de opstarttijd van uw systeem te verkorten.

Acties die worden ondernomen op gedetecteerde malware

U kunt de acties die door de realtime beveiliging worden genomen configureren.

De acties configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Sleep de scannerschuifregelaar van **On-access scannen** naar het niveau **AANGEPAST**.

   Er verschijnt een nieuw venster.
5. Selecteer het **Acties**-tabblad en configureer de scaninstellingen volgens uw behoeften.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

De volgende acties kunnen worden ondernomen door de realtime beveiliging in Bitdefender:

Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een malwarehandtekening in de database van malwarehandtekeningen van Bitdefender. Bitdefender zal automatisch proberen de malwarecode van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd.

  Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 99).

  Belangrijk

  Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** Soms worden bestanden door de heuristische analyse aangemerkt als 'verdacht'. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat hiervoor geen standaard desinfectieroutine bestaat. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.

  Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen

op voorwaarde dat het programma het archief met de schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Naar quarantaine
Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 99).

Toegang weigeren
Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.

14.1.4. De standaardinstellingen herstellen

De standaardinstellingen voor de real time-beveiliging, garanderen een goede beveiliging tegen malware, met een minimale impact op de systeemprestaties.

De standaard real time-beveiligingsinstellingen herstellen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Sleep de scannerschuifregelaar van **On-access scannen** naar het niveau **NORMAAL**.

14.2. Scannen op aanvraag

Bitdefender heeft als hoofddoel uw computer vrij te houden van virussen. Dit wordt gedaan door nieuwe virussen uit uw computer weg te houden en door uw e-mailberichten en alle nieuwe bestanden, die u downloadt of kopieert naar uw systeem, te scannen.

Het risico bestaat dat een virus zich reeds in uw systeem heeft genesteld voordat u Bitdefender installeert. Het is dan ook een bijzonder goed idee uw computer meteen te scannen op aanwezige virussen nadat u Bitdefender hebt geïnstalleerd. En het is absoluut een goed idee om uw computer regelmatig te scannen op virussen.

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand. U kunt de computer scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren. Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

14.2.1. Een bestand of map scannen op malware

U moet bestanden en mappen scannen wanneer u vermoedt dat ze geïnfecteerd zijn. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen, kies **Bitdefender** en selecteer **Scannen met Bitdefender**. De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

14.2.2. Een snelle scan uitvoeren

Quick Scan gebruikt in-the-cloud scanning om malware die op uw PC wordt uitgevoerd, te detecteren. Het uitvoeren van een Snelle scan duurt doorgaans minder dan één minuut en gebruikt slechts een fractie van het systeemgeheugen dat nodig is door een regelmatige virusscan.

Een snelle scan starten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Snelle scan**.
4. Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Het kan ook sneller: klik op de -icoon op de linkerzijbalk van de Bitdefender-interface en klik daarna op de actieknop **Snelle Scan**.

14.2.3. Een systeemscan uitvoeren

De systeemscan scant de volledige computer op alle types malware die de beveiliging bedreigen, zoals virussen, spyware, adware, rootkits en andere.

Opmerking
Omdat **Systeemscan** een grondige scan van het complete systeem uitvoert, kan de scan even duren. Het is daarom aanbevolen deze taak uit te voeren wanneer u de computer niet gebruikt.

Voordat u een systeemscan uitvoert, wordt het volgende aanbevolen:

- Controleer of de malwarehandtekeningen van Bitdefender up-to-date zijn. Het scannen van uw computer met een oude handtekeningendatabase kan verhinderen dat Bitdefender nieuwe malware die sinds de laatste update is gevonden, detecteert. Meer informatie vindt u onder "*Bitdefender up-to-date houden*" (p. 44).
- Alle open programma's afsluiten

Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren. Meer informatie vindt u onder "*Een aangepaste scan configureren*" (p. 87).

Een systeemscan lanceren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Systeemscan**.
4. Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

14.2.4. Een aangepaste scan configureren

Een aangepaste, gedetailleerde scan configureren en lanceren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS**-module selecteert u **Scans beheren**.
4. Klik op de knop **Nieuwe aangepaste taak**. Voer onder de tab **Basis** een naam in voor de scan en selecteer de locaties die gescand moeten worden.
5. Klik op de tab **Geavanceerd** als u de scanopties in detail wilt configureren. Er verschijnt een nieuw venster. Volg deze stappen:

a. U kunt de scanopties gemakkelijk configureren door het scanniveau aan te passen. Sleep de schuifregelaar langs de schaal om het gewenste scanniveau in te stellen. Gebruik de beschrijving aan de rechterzijde van de schaal om het scanniveau te identificeren dat beter beantwoordt aan uw behoeften.

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden. Klik op **Aangepast** om de scanopties in detail te configureren. Aan het einde van dit gedeelte vindt u informatie over deze opties.

b. U kunt ook deze algemene opties configureren:

- **De taak uitvoeren met lage prioriteit .** Verlaagt de prioriteit van het geselecteerde scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
- **Scanwizard minimaliseren naar systeemvak .** Minimaliseert het scanvenster naar het systeemvak. Dubbelklik op het pictogram Bitdefender om het programma te openen.
- Geef de actie op die moet worden ondernomen als er geen bedreigingen zijn gevonden.

c. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

6. Indien u een planning voor uw scantaak wenst in te stellen, gebruik de **Planning**-schakelaar in het **Basis**-venster. Selecteer een van de overeenkomstige opties om een planning in te stellen:
   - Bij opstarten systeem
   - Eenmalig
   - Periodiek
7. Klik op **Scannen starten** en volg de Antivirusscanwizard om het scannen te voltooien. Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.
8. Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de woordenlijst. U kunt ook nuttige informatie vinden door op het Internet te zoeken.
- **Bestanden scannen.** U kunt Bitdefender instellen om alleen alle types bestanden of toepassingen (programmabestanden) te scannen. Het scannen van alle bestanden biedt de beste beveiliging, terwijl het scannen van toepassingen alleen kan worden gebruikt om een snellere scan uit te voeren.

  Toepassingen (of programmabestanden) zijn veel kwetsbaarder voor malwareaanvallen dan andere bestandstypen. Deze categorie bevat de volgende bestandsextensies: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scanopties voor archieven.** Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem. De malware kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld. Het is echter aanbevolen deze optie te gebruiken om eventuele potentiële bedreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke bedreiging gaat.

  Opmerking
  Als gearchiveerde bestanden worden gescand, duurt het scannen langer en worden er meer systeembronnen gebruikt.

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten. Als een virus het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kun starten en geen toegang meer hebt tot uw gegevens.
- **Geheugen scannen.** Selecteer deze optie om programma's te scannen die worden uitgevoerd in uw systeemgeheugen.
- **Register scannen.** Selecteer deze optie voor het scannen van registersleutels. Het Windows-register is een database die de configuratie-instellingen en opties opslaat voor de componenten van het Windows-besturingssysteem, evenals voor geïnstalleerde toepassingen.
- **Cookies scannen.** Selecteer deze opties om de cookies te scannen die via browsers op uw computers zijn opgeslagen.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Commerciële keyloggers negeren.** Selecteer deze opties als u commerciële keylogger-software op uw computer hebt geïnstalleerd en deze software gebruikt. Commerciële keyloggers zijn rechtmatige computerbewakingsprogramma's waarvan de basisfunctie eruit bestaat alles wat op het toetsenbord wordt getypt, te registreren.
- **Scannen op rootkits.** Selecteer deze optie om te scannen op rootkits en verborgen objecten die dergelijke software gebruiken.

14.2.5. Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map, kies Bitdefender en selecteer **Scannen met Bitdefender**), verschijnt de Antivirusscanwizard van Bitdefender. Volg de wizard om het scannen te voltooien.

Opmerking

Als de scanwizard niet verschijnt, kan de scan worden geconfigureerd om stil te worden uitgevoerd op de achtergrond. Zoek het pictogram voor de scanvoortgang in het systeemvak. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Stap 1 - Scan uitvoeren

Bitdefender start het scannen van de geselecteerde objecten. U ziet real time-informatie over de scanstatus en statistieken (inclusief de verstreken tijd, een schatting van de resterende tijd en het aantal gedetecteerde bedreigingen).

Wacht tot Bitdefender klaar is met scannen. Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

De scan stoppen of pauzeren. U kunt het scannen op elk ogenblik stoppen door op **STOP** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard. Klik op **PAUZE** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **HERVATTEN**.

Wachtwoordbeveiligde archieven. Wanneer een met een wachtwoord beschermd archief wordt gedetecteerd, kunt u afhankelijk van de scaninstellingen worden gevraagd het wachtwoord op te geven. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. De volgende opties zijn beschikbaar:

- **Wachtwoord.** Als u wilt dat Bitdefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren. Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Geen wachtwoord vragen en dit object overslaan bij het scannen.** Selecteer deze optie om het scannen van dit archief over te slaan.
- **Alle wachtwoordbeveiligde items overslaan zonder ze te scannen.** Selecteer deze optie als u niet wilt worden lastig gevallen met betrekking tot wachtwoordbeveiligde archieven. Bitdefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

Kies de gewenste optie en klik op **OK** om door te gaan met scannen.

Stap 2 – Acties kiezen

Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

Opmerking

Wanneer u een snelle scan of een systeemscan uitvoert, neemt Bitdefender automatisch de aanbevolen acties op bestanden die zijn gedetecteerd tijdens de scan. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de malware waarmee ze zijn geïnfecteerd. Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kan een algemene actie selecteren die moet worden genomen voor alle groepen problemen of u kan afzonderlijke acties voor elke groep problemen selecteren. Een of meerdere van de volgende opties kunnen in het menu verschijnen.

Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een malwarehandtekening in de database van malwarehandtekeningen van Bitdefender. Bitdefender zal automatisch proberen de malwarecode van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd.

  Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 99).

  Belangrijk

  Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** Soms worden bestanden door de heuristische analyse aangemerkt als 'verdacht'. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat hiervoor geen standaard desinfectieroutine bestaat. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.

  Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Wissen

Verwijdert gedetecteerde bestanden van de schijf.

Als er geïnfecteerde bestanden samen met schone bestanden in een archief zijn opgeslagen, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen en het archief opnieuw op te bouwen met de schone bestanden. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Geen actie nemen

Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.

Klik op **Doorgaan** om de aangegeven acties toe te passen.

Stap 3 – Overzicht

Wanneer Bitdefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster. Als u uitgebreide informatie over het scanproces wenst, klikt u op **LOGBOEK WEERGEVEN** om het scanlogboek weer te geven.

Belangrijk

In de meeste gevallen desinfecteert Bitdefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Er zijn echter problemen die niet automatisch kunnen worden opgelost. Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien. Meer informatie en instructies over het handmatig verwijderen van malware, vindt u onder "*Malware van uw systeem verwijderen*" (p. 159).

14.2.6. Scanlogboeken controleren

Telkens wanneer er een scan wordt uitgevoerd, wordt er een scanverslag aangemaakt en Bitdefender slaat de gedetecteerde problemen op in het Antivirusvenster. Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **LOGBOEK WEERGEVEN** te klikken.

Een scanlog of een gedetecteerde infectie later bekijken:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste scan.

   Hier vindt u alle gebeurtenissen van scans op malware, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
3. In de kennisgevingenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een kennisgeving om details erover weer te geven.
4. Klik op **LOGBOEK WEERGEVEN** om het scanlogboek te openen.

14.3. Automatisch scannen van verwisselbare media

Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw computer en scant dit op de achtergrond. Dit is aanbevolen om infecties van uw computer door virussen en andere malware te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

- Cd's/dvd's
- USB-opslagapparaten, zoals flashpennen en externe harde schijven
- toegewezen (externe) netwerkstations

U kunt het automatisch scannen afzonderlijk configureren voor elke categorie opslagapparaten. Automatisch scannen van toegewezen netwerkstations is standaard uitgeschakeld.

14.3.1. Hoe werkt het?

Wanneer Bitdefender een verwisselbaar opslagapparaat detecteert, start het programma met scannen op malware op de achtergrond (op voorwaarde dat de automatische scan is ingeschakeld voor dat type apparaat). Een Bitdefender-scanpictogram verschijnt in het systeemvak. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Als Auto Pilot is ingeschakeld, wordt u niet gehinderd door herinnering aan de scan. De scan wordt alleen geregistreerd en de informatie over de scan zal beschikbaar zijn in het venster Kennisgevingen.

Als Auto Pilot is uitgeschakeld:

1. U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.
2. In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde malware of isoleert het programma geïnfecteerde bestanden in quarantaine. Als er na de scan niet opgeloste bedreigingen zijn, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

   Opmerking
   Houd ermee rekening dat er geen actie kan worden ondernomen op geïnfecteerde of verdachte bestanden die op cd's/dvd's zijn gevonden. Zo kan er ook geen actie worden ondernemen op geïnfecteerde of verdachte bestanden die zijn gedetecteerd op toegewezen netwerkstations als u niet over de geschikte privileges beschikt.

3. Nadat de scan is voltooid, wordt het venster met de scanresultaten weergegeven om u te laten weten of u de bestanden op de verwisselbare media veilig kunt openen.

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een door malware geïnfecteerde cd/dvd gebruikt. De malware kan niet van de schijf worden verwijderd (het medium is alleen-lezen). Zorg dat de real time-beveiliging is ingeschakeld om te verhinderen dat malware zich over uw systeem verspreidt. De beste werkwijze is het kopiëren van alle waardevolle gegevens van de schijf naar uw systeem en ze daarna verwijderen van de schijf.

- In sommige gevallen zal Bitdefender niet in staat zijn malware te verwijderen uit specifieke bestanden vanwege wettelijke of technische beperkingen. Een voorbeeld hiervan zijn bestanden die gearchiveerd zijn met een eigen technologie (dit is te wijten aan het feit dat het archief niet correct opnieuw kan worden gemaakt).

  Raadpleeg *"Malware van uw systeem verwijderen"* (p. 159) voor meer informatie over het omgaan met malware.

14.3.2. Scan verwisselbare media beheren

Automatische scans van verwisselbare media beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **DRIVES EN APPARATEN**.

Voor de beste beveiliging is het aanbevolen het automatisch scannen in te schakelen voor alle types verwisselbare opslagapparaten.

De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, probeert Bitdefender ze te desinfecteren (de malwarecode verwijderen) of ze naar quarantaine te verplaatsen. Als beide acties mislukken, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden. De scanopties zijn standaard en u kunt ze niet wijzigen.

14.4. Gastbestand scannen

Het gastbestand zit standaard in de installatie van uw besturingssysteem en wordt gebruik om hostnamen aan IP-adressen te koppelen, telkens wanneer u een nieuwe webpagina bezoekt, een verbinding maakt met een FTP of andere internetservers. Het is een gewoon tekstbestand en kwaadaardige programma's zouden het kunnen wijzigen. Geavanceerde gebruikers weten hoe ze het moeten gebruiken om vervelende advertenties, banners, cookies van derden of overvallers te blokkeren.

Om scan-gastbestanden te configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.

2. Klik op het tabblad **GEAVANCEERD**.
3. Klik op de bijhorende schakelaar om scan gastbestand in of uit te schakelen.

14.5. Scanuitsluitingen configureren

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen. Deze functie is bedoeld om te vermijden dat u in uw werk wordt gestoord en kan ook helpen de systeemprestaties te verbeteren. Uitsluitingen zijn voorzien voor gebruikers die over een gevorderde computerkennis beschikken. Als u deze kennis niet hebt, kunt u de aanbevelingen van een expert van Bitdefender volgen.

U kunt uitsluitingen configureren die u wilt toepassen op Scannen bij toegang of Scannen op aanvraag afzonderlijk, of op beide scantypes tegelijk. De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing worden geopend.

Opmerking

Uitsluitingen komen NIET in aanmerking voor contextueel scannen. Contextueel scannen is een type van scannen op aanvraag. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **Scannen met Bitdefender**.

14.5.1. Bestanden en mappen uitsluiten van het scannen

Specifieke bestanden en mappen uitsluiten van het scannen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Klik op het uitklapmenu **Lijst van bestanden en mappen die uitgesloten worden voor de scan**. In het venster dat verschijnt, kunt u de bestanden en mappen die van het scannen zijn uitgesloten, beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik op de knop **ADD**.

b. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**. Daarnaast kunt u ook het pad naar het bestand of de map in het bewerkingsveld typen (of kopiëren en plakken).

c. Het geselecteerde bestand of de geselecteerde map wordt standaard uitgesloten van Scannen bij toegang en Scannen bij aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.

d. Klik op **Toevoegen**.

14.5.2. Bestandsextensies uitsluiten van het scannen

Wanneer u een bestandsextensie uitsluit van de scan, zal Bitdefender niet langer bestanden met die extensie scannen, ongeacht hun locatie op uw computer. De uitsluiting is ook van toepassing op bestanden op verwisselbare media, zoals cd's, dvd's, USB-opslagapparaten of netwerkstations.

Belangrijk
Ga voorzichtig te werk wanneer u extensies uitsluit van het scannen, want dergelijke uitsluitingen kunnen uw computer kwetsbaar maken voor malware.

Bestandsextensies uitsluiten van het scannen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Klik op het uitklapmenu **Lijst van extensies die uitgesloten worden voor de scan**. In het venster dat verschijnt, kunt u de bestandsextensies die van het scannen zijn uitgesloten, beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik op de knop **ADD**.
   b. Voer de extensies in die u wilt uitsluiten van het scannen en scheid ze van elkaar met puntkomma's (;). Hier is een voorbeeld:

      txt;avi;jpg

c. Alle bestanden met de opgegeven extensies worden standaard uitgesloten van Scannen bij toegang en Scannen op aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.

d. Klik op **Toevoegen**.

14.5.3. Scanuitsluitingen beheren

Als de geconfigureerde scanuitsluitingen niet langer nodig zijn, is het aanbevolen dat u ze verwijdert of dat u scanuitsluitingen uitschakelt.

Scanuitsluitingen beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Gebruik de opties in het uitklapmenu **Lijst van bestanden en mappen die uitgesloten worden voor het scannen** om uitsluitingen voor scans te beheren.
6. Klik op een van de beschikbare koppelingen om scanuitsluitingen te verwijderen of te bewerken. Ga als volgt te werk:
   - Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **VERWIJDEREN**.
   - Om een gegeven in de tabel te bewerken, dubbelklikt u op dit item (of selecteert u het en klikt u op de knop **BEWERKEN**). Er verschijnt een nieuw venster. Hierin kunt u de extensie van het pad dat moet worden uitgesloten en het type scan waarvoor u het wilt uitsluiten wijzigen volgens uw voorkeur. Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.

14.6. Bestanden in quarantaine beheren

Bitdefender isoleert de door malware geïnfecteerde bestanden die het niet kan desinfecteren en de verdachte bestanden in een beveiligd gebied dat de quarantaine wordt genoemd. Wanneer een virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

Daarnaast scant Bitdefender de bestanden in quarantaine na elke update van malware-handtekening. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

De bestanden in quarantaine controleren en beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **QUARANTAINE**.
5. Bestanden in quarantaine worden automatisch beheerd door Bitdefender op basis van de standaard quarantaine-instellingen. Hoewel dit niet aanbevolen is, kunt u de quarantaine-instellingen aanpassen volgens uw voorkeur.

   Quarantaine opnieuw scannen na updaten van virusdefinities
   Houd deze optie ingeschakeld om bestanden in quarantaine automatisch te scannen na elke update van de virusdefinities. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

   Voeg verdachte bestanden die in quarantaine staan toe voor verdere analyses
   Houd deze optie ingeschakeld om bestanden in quarantaine automatisch naar Bitdefender te verzenden. De voorbeeldbestanden worden geanalyseerd door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

   Inhoud ouder dan {30} dagen verwijderen
   Standaard worden bestanden in quarantaine die ouder zijn dan 30 dagen, automatisch verwijderd. Als u dit interval wilt wijzigen, geeft u een nieuwe waarde op in het overeenkomende veld. Typ 0 om het automatisch verwijderen van oude bestanden in quarantaine uit te schakelen.

6. Om een bestand in quarantaine te verwijderen, selecteert u het en klikt u op de knop **VERWIJDEREN**. Als u een bestand uit de quarantaine wilt terugzetten naar de oorspronkelijke locatie, selecteert u het bestand en klikt u op **HERSTELLEN**.

14.7. Actief dreigingsbeheer

Bitdefender Actief dreigingsbeheer is een innovatieve proactieve detectietechnologie die geavanceerde heuristische methoden gebruikt voor het in real time detecteren van ransomware en andere nieuwe potentiële bedreigingen.

Actief dreigingsbeheer bewaakt voortdurend de toepassingen die op de computer worden uitgevoerd en zoekt naar acties die op malware lijken. Elk van deze acties krijgt een score en voor elk proces wordt een algemene score berekend. Wanneer de algemene score voor een proces een bepaalde drempel bereikt, wordt het proces beschouwd als schadelijk en wordt het automatisch geblokkeerd.

Als Autopilot uit is, wordt u op de hoogte gebracht via een pop-upvenster over de gedetecteerde ransomware of geblokkeerde toepassing. Anders wordt de toepassing geblokkeerd zonder enige melding. U kunt controleren welke toepassingen zijn gedetecteerd door Actief dreigingsbeheer in het venster Kennisgevingen.

14.7.1. Gedetecteerde toepassingen controleren

De applicaties die werden gedetecteerd door Active Threat Control controleren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de Active Threat Control-scan.
3. Als u de toepassing vertrouwt, kunt u Actief dreigingsbeheer configureren om deze niet meer te blokkeren door op **TOESTAAN EN BEWAKEN** te klikken. Actief dreigingsbeheer blijft de uitgesloten toepassingen bewaken. Als voor een uitgesloten toepassing wordt gedetecteerd dat deze verdachte activiteiten uitvoert, wordt de gebeurtenis eenvoudigweg gemeld en gerapporteerd aan Bitdefender Cloud als detectiefout.

14.7.2. Actief dreigingsbeheer in- of uitschakelen

Active Threat Control in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. In het venster **SCHILD** klikt u op de bijhorende schakelaar om Active Threat Control in of uit te schakelen.

14.7.3. De bescherming van Actief dreigingsbeheer aanpassen

Als u merkt dat Actief dreigingsbeheer vaak rechtmatige toepassingen detecteert, moet u een toegeeflijker beveiligingsniveau instellen.

Om de bescherming van het Actief dreigingsbeheer aan te passen, verschuift u de glijder op de schaal naar het gewenste beschermingsniveau.

Gebruik de beschrijving aan de rechterzijde van de schaal om het beveiligingsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

Opmerking

Wanneer u het beveiligingsniveau hoger instelt, zal Actief dreigingsbeheer minder tekenen van malware-achtig gedrag nodig hebben om een proces te rapporteren. Dit zal leiden tot een hoger aantal gerapporteerde toepassingen en tegelijkertijd tot een grotere waarschijnlijkheid van fout-positieven (veilige toepassingen die worden gedetecteerd als kwaadaardig).

14.7.4. Uitgesloten processen beheren

U kunt de uitsluitingsregels configureren voor vertrouwde toepassingen zodat Actief dreigingsbeheer ze niet blokkeert als ze acties uitvoeren die op malware lijken. Actief dreigingsbeheer blijft de uitgesloten toepassingen bewaken. Als voor een uitgesloten toepassing wordt gedetecteerd dat deze verdachte activiteiten uitvoert, wordt de gebeurtenis eenvoudigweg gemeld en gerapporteerd aan Bitdefender Cloud als detectiefout.

Procesuitsluitingen van de Active Threat Control beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.

2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Klik op het uitklapmenu **Lijst van processen die uitgesloten worden voor de scan**.

   Van hieruit kunt u de procesuitsluitingen voor de Active Threat Control beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik op de knop **ADD**.
   b. Klik op **Bladeren**, zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.
   c. Houd de optie **Toestaan** geselecteerd om te verhinderen dat Actief dreigingsbeheer de toepassing blokkeert.
   d. Klik op **Toevoegen**.
7. Ga als volgt te werk om uitsluitingen te verwijderen of te bewerken:
   - Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **VERWIJDEREN**.
   - Om een gegeven in de tabel te bewerken, dubbelklikt u op dit item (of selecteert u het) en klikt u op de knop **BEWERKEN**. Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.

15. WEBBEVEILIGING

Bitdefender Webbeveiliging garandeert een veilige surfervaring door u te waarschuwen over mogelijke kwaadaardige websites.

Bitdefender biedt realtime webbeveiliging voor:

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

De webbeveiligingsinstellingen configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **WEBBESCHERMING**-module.

Klik op de schakelaars om deze optie in of uit te schakelen.

- Search advisor is een component die de resultaten van uw zoekopdrachten en de koppelingen die op websites van sociale netwerken zijn geplaatst, beoordeelt door naast elk resultaat een pictogram te plaatsen.

  U mag deze webpagina niet bezoeken.

  Deze webpagina bevat mogelijke gevaarlijke onderdelen. Wees voorzichtig als deze pagina toch wilt bezoeken.

  Dit is een pagina die u veilig kunt bezoeken.

  Search Advisor beoordeelt de zoekresultaten van de volgende zoekmachines op Internet:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor beoordeelt de koppelingen die zijn geplaatst op de volgende online sociale netwerkservices:

- Facebook
- Twitter

- SSL aan het scannen

  Meer verfijnde aanvallen kunnen gebruik maken van beveiligd webverkeer om hun slachtoffers te misleiden. Het is daarom aanbevolen SSL scannen in te schakelen.

- Bescherming tegen fraude.
- Bescherming tegen phishing.

U kunt een lijst opmaken van websites die niet zullen worden gescand door de antimalware, antiphishing en antifraude-engines van Bitdefender. De lijst mag websites bevatten die u volledig vertrouwt. Voeg bijvoorbeeld de websites toe waar u regelmatig online winkelt.

Voor het configureren en beheren van websites met gebruikmaking van webbeveiliging van Bitdefender klikt u op de link **Witte lijst**. Er verschijnt een nieuw venster.

Om een site toe te voegen aan de Witte lijst, geeft u het adres van de site op in het overeenkomende veld en kikt u op **Toevoegen**.

Om een website uit de lijst te verwijderen, selecteert u de site in de lijst en klikt u op de overeenkomende koppeling **Verwijderen**.

Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

15.1. Bitdefender waarschuwt in de browser

Telkens wanneer u een website bezoekt die als onveilig is geclassificeerd, wordt de website geblokkeerd en wordt een waarschuwingspagina weergegeven in uw browser.

De pagina bevat informatie, zoals de URL van de website en de gedetecteerde bedreiging.

U moet beslissen wat u vervolgens wilt doen. De volgende opties zijn beschikbaar:

- Navigeer weg van de webpagina door te klikken op **Breng me terug naar de veiligheid**.
- U kunt ondanks de waarschuwing naar de webpagina gaan door op **Ik begrijp het risico, laat me er toch heengaan** te klikken.

16. DATA BESCHERMING

16.1. Bestanden definitief verwijderen

Wanneer u een bestand verwijdert, is het niet langer toegankelijk met de normale middelen. Het bestand blijft echter opgeslagen op de harde schijf tot het wordt overschreven wanneer nieuwe bestanden worden gekopieerd.

Bitdefender Bestandsvernietiging helpt om gegevens permanent te verwijderen door ze fysisch te wissen van uw harde schijf.

Volg deze stappen om bestanden of mappen snel permanent verwijderen van uw computer via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u permanent wilt verwijderen.
2. Selecteer **Bitdefender** > **Bestandsvernietiging** in het contextmenu dat verschijnt.
3. Er wordt een bevestigingsvenster weergegeven. Klik op **JA, VERWIJDEREN** om de wizard Bestandsvernietiging te starten. Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.
4. De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

U kunt bestanden ook vernietigen via de Bitdefender-interface, als volgt:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de module **GEGEVENSBEVEILIGING** selecteert u **Bestandsvernietiging**.
4. Volg de wizard Bestandsvernietiging:
   a. Klik op de knop **BESTANDEN TOEVOEGEN...** om de bestanden of mappen die u permanent wenst te verwijderen, toe te voegen.

      U kunt deze bestanden of mappen ook naar dit venster slepen.

   b. Klik op **BESTANDEN PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.

      Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.

   c. **Samenvatting resultaten**

De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

17. KWETSBAARHEID

Een belangrijke stap bij het beschermen van uw computer tegen kwaadwillende acties en applicaties is het up-to-date houden van het besturingssysteem en van de applicaties die u regelmatig gebruikt. Bovendien: om ongeoorloofde fysieke toegang tot uw computer te voorkomen, moeten sterke wachtwoorden (wachtwoorden die niet makkelijk kunnen geraden worden) geconfigureerd worden voor elke Windows-gebruikersaccount en voor de Wi-Fi-netwerken waarmee u een verbinding maakt.

Bitdefender controleert uw systeem automatisch op kwetsbaarheden en breng u hiervan op de hoogte. Dit scant naar het volgende:

- verouderde toepassingen op uw computer.
- ontbrekende Windows-updates.
- zwakke wachtwoorden voor Windows-gebruikersaccounts.
- onbeveiligde draadloze netwerken en routers.

Bitdefender biedt twee eenvoudige manieren om de kwetsbaarheden van uw systeem op te lossen:

- U kunt uw systeem scannen op kwetsbaarheden en ze stapsgewijs repareren met de optie **Kwetsbaarheidscan**.
- Met de automatische kwetsbaarheidsbewaking kunt u de gedetecteerde kwetsbaarheden controleren en oplossen in het venster Kennisgevingen.

Het is aanbevolen de systeemkwetsbaarheden om de week of twee weken te controleren en op te lossen.

17.1. Uw systeem scannen op kwetsbaarheden

Systeemkwetsbaarheden oplossen met de optie Kwetsbaarheidscan:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **Kwetsbaarheidsscan**.
3. Wacht tot Bitdefender uw systeem op kwetsbaarheden heeft gecontroleerd. Om het scanproces te stoppen, klikt u op de knop **Overslaan** bovenaan op het venster.
   - **Kritieke Windows updates**

Klik op **Details weergeven** om de lijst te zien van kritieke Windows updates die momenteel niet zijn geïnstalleerd op uw computer.

Klik op **Updates installeren** om de installatie van de geselecteerde updates te starten. De installatie van de updates kan even duren en voor sommige updates zal het nodig zijn het systeem opnieuw op te starten om de installatie te voltooien. Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

- **Toepassings-updates**

  Als een applicatie niet up-to-date is, klik dan op de **Nieuwe versie downloaden**-koppeling om de laatste versie te downloaden.

  Klik op **Details weergeven** om informatie over de toepassing die moet worden bijgewerkt te zien.

- **Zwakke wachtwoorden van Windows-accounts**

  U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw computer en de beschermingsniveaus van de wachtwoorden.

  Klik op **Wachtwoord wijzigen bij aanmelden** om een nieuw wachtwoord in te stellen voor uw systeem.

  Klik op **Details weergeven** om de zwakke wachtwoorden te wijzigen. U kunt kiezen om de gebruiker te vragen het wachtwoord te wijzigen bij de volgende aanmelding of u kunt het wachtwoord zelf onmiddellijk wijzigen. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

- **Zwakke Wi-Fi-netwerken**

  Klik **Details weergeven** voor meer informatie over het draadloze netwerk waarmee u verbonden bent. Indien wordt aanbevolen om een sterker wachtwoord in te stellen voor uw thuisnetwerk, klikt u op de daarbijhorende koppeling.

  Wanneer andere aanbevelingen beschikbaar zijn, volt u de instructies zodat u zeker bent dat uw thuisnetwerk veilig blijft tegen de indiscrete blikken van hackers.

In de rechter bovenhoek van het venster kunt u de resultaten filteren volgens uw voorkeuren.

17.2. De automatische kwetsbaarheidsbewaking gebruiken

Bitdefender scant uw systeem regelmatig op de achtergrond op kwetsbaarheden en houdt gegevens bij van de gevonden problemen in het venster Kennisgevingen.

Zo kunt u de opgespoorde problemen controleren en verhelpen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de Kwetsbaarheidsscan.
3. U kunt gedetailleerde informatie betreffende de gedetecteerde kwetsbaarheden van het systeem zien. Afhankelijk van het probleem, gaat u als volgt te werk om een specifieke kwetsbaarheid te herstellen:
   - Als er Windows-updates beschikbaar zijn, klikt u op **INSTALLEREN**.
   - Indien automatische Windows Update geïnactiveerd is? klikt u op **ACTIVEREN**.
   - Als een toepassing verouderd is, klikt u op **NU BIJWERKEN** om een koppeling te zoeken naar de webpagina van de verkoper vanaf waar u de nieuwste versie van die toepassing kunt installeren.
   - Als een Windows-gebruikersaccount een zwak wachtwoord heeft, klikt u op **WACHTWOORD WIJZIGEN** om de gebruiker te forceren het wachtwoord te wijzigen bij de volgende aanmelding of wijzigt u zelf het wachtwoord. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).
   - Als de Windows-functie Autorun is ingeschakeld, klikt u op **VERHELPEN** om de functie uit te schakelen.
   - Indien de router die u hebt geconfigureerd een zwak wachtwoord heeft ingevoerd, klikt u op **WACHTWOORD WIJZIGEN** om naar de interface te gaan, waar u een sterk wachtwoord kunt instellen.
   - Indien het netwerk waar u mee verbonden bent, kwetsbaarheden heeft die uw systeem kunnen bedreigen, klik op **WIFI-SETTINGS**.

De controle-instellingen voor kwetsbaarheid configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **KWETSBAARHEID**-module.
4. Klik op de bijhorende schakelaar om Kwetsbaarheidscan in of uit te schakelen.

   Belangrijk
   Om automatisch op de hoogte te worden gebracht over kwetsbaarheden van het systeem of de toepassing, moet u de optie **Kwetsbaarheid** ingeschakeld houden.

5. Kies de systeemkwetsbaarheden die u regelmatig wilt controleren met de overeenkomende schakelaars.

   Kritieke Windows updates
   Controleer of uw Windows-besturingssysteem over de laatste kritieke beveiligingsupdates van Microsoft beschikt.

   Toepassings-updates
   Controleer of toepassingen geïnstalleerd op uw systeem up-to-date zijn. Verouderde toepassingen kunnen door kwaadaardige software worden misbruikt, waardoor uw PC kwetsbaar wordt voor aanvallen van buitenaf.

   Zwakke wachtw.
   Controleer of de wachtwoorden van de Windows-accounts en routers die op het systeem zijn geconfigureerd, gemakkelijk te raden zijn. Het instellen van moeilijk te raden wachtwoorden (sterke wachtwoorden) maakt het bijzonder moeilijk voor hackers om in uw systeem in te breken. Een sterk wachtwoord bevat hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, $ of @).

   Autorun media
   Controleer de status van de Windows-functie Autorun. Met deze functie kunnen toepassingen automatisch worden gestart vanaf cd's, dvd,'s, USB-stations of andere externe apparaten.

   Sommige malwaretypes gebruiken Autorun om zich automatisch te verspreiden van de verwisselbare media naar de PC. Daarom is het aanbevolen deze Windows-functie uit te schakelen.

Notifications Wi-Fi Security Advisor

Controleer of het draadloze thuisnetwerk waarmee u verbonden bent al dan niet veilig is en of er kwetsbaarheden zijn. Controleer ook of het wachtwoord van uw thuisrouter sterk genoeg is en hoe u het veiliger kunt maken.

De meeste onbeveiligde draadloze netwerken zijn niet veilig, waardoor de indiscrete ogen van hackers toegang krijgen tot uw persoonlijke activiteiten.

Opmerking
Als u de bewaking van een specifieke kwetsbaarheid uitschakelt, worden verwante problemen niet langer opgenomen in het venster Kennisgevingen.

17.3. Wi-Fi Security Advisor

Als u onderweg bent, in een coffee shop gaat werken of in de luchthaven wacht, kan het de snelste oplossing zijn om een verbinding te maken met een openbaar draadloos netwerk om betalingen te doen, e-mails te lezen of sociale netwerkaccounts te raadplegen. Maar er kunnen nieuwsgierige ogen zijn, die uw persoonlijke gegevens proberen te stelen en kijken hoe de informatie door het netwerk heen druppelt.

Persoonlijke gegevens zijn de wachtwoorden en gebruikersnamen die u gebruikt om naar uw online accounts te gaan, zoals e-mails, bankrekeningen, sociale media-accounts, maar ook de berichten die u verzendt.

Gewoonlijk zijn openbare draadloze netwerken niet veilig, aangezien ze geen wachtwoord vragen om u aan te melden, en als dat wel het geval is, kan het wachtwoord ter beschikking gesteld worden van iedereen die een verbinding wil maken. Bovendien kunnen er kwaadaardige of honingpotnetwerken zijn, die een doelwit vormen voor cybercriminelen.

Om u te beschermen tegen de gevaren van onveilige of onversleutelde openbare draadloze hotspots, analyseert Bitdefender Wi-Fi Security Advisor hoe veilig een draadloos netwerk is, en indien nodig beveelt hij u aan om Bitdefender Safepay™ te gebruiken met inschakeling van de Wi-Fi Hotspot.

De Bitdefender Wi-Fi Security Advisor geeft u informatie over:

- Thuis-Wi-Fi-netwerken
- Openbare Wi-Fi-netwerken

17.3.1. De meldingen van Wi-Fi Security Advisor aan- of uitzetten

Om de meldingen van Wi-Fi Security Advisor aan of uit te zetten

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **KWETSBAARHEID**-module.
4. Klik op de overeenkomende schakelaar om de meldingen van **Wi-Fi Security Adviser** aan of uit te zetten.

17.3.2. Thuis-Wi-Fi-netwerk configureren

Uw thuisnetwerk beginnen configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer in de module **KWETSBAARHEID Wi-Fi-Security Advisor**.
4. In het tabblad **THUIS-WI-FI** klikt u op de knop **THUIS-WI-FI SELECTEREN**.

   Er wordt een lijst weergegeven met de draadloze netwerken waarmee u tot nu toe een verbinding hebt gemaakt.
5. Duid uw thuisnetwerk aan en klik daarna op **SELECTEREN**.

Indien een thuisnetwerk als onbeveiligd of onveilig wordt beschouwd, worden configuratieaanbevelingen weergegeven om de beveiliging te verbeteren.

Om het draadloze netwerk dat u als thuisnetwerk hebt ingesteld, te verwijderen, klikt u op de knop **VERWIJDEREN**.

17.3.3. Openbare Wi-Fi

Terwijl u met een onbeveiligd of onveilig draadloos netwerk verbonden bent, wordt het openbare Wi-Fi-profiel geactiveerd. Terwijl u in dit profiel werkt, is Bitdefender Antivirus Plus 2017 ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Actief dreigingsbeheer is ingeschakeld
- De volgende instellingen van Webbescherming zijn ingeschakeld:

- SSL scannen
- Bescherming tegen fraude
- Bescherming tegen phishing

- Er is een knop beschikbaar die Bitdefender Safepay™ opent. In dit geval is de Hotspot-bescherming voor onbeveiligde netwerken standaard geactiveerd.

17.3.4. Informatie controleren over Wi-Fi-netwerken

Om informatie te controleren over de draadloze netwerken, verbindt u zich gewoonlijk met:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer in de module **KWETSBAARHEID Wi-Fi-Security Advisor**.
4. Afhankelijk van de informatie die u nodig hebt, selecteert u een van de volgende twee tabbladen: **THUIS-WI-FI** of **OPENBARE WI-FI**.
5. Klik op **Details bekijken** naast het netwerk waar u meer informatie over wenst.

Er zijn drie types draadloze netwerken gefilterd naargelang belang. Elk type wordt aangeduid door een specifiek pictogram:

Wi-Fi is onveilig - betekent dat het beveiligingsniveau van het netwerk laag is. Dit betekent dat er een hoog risico bestaat als u het gebruikt en het is niet aanbevolen om betalingen uit te voeren of bankrekeningen te controleren zonder extra bescherming. In dergelijke situaties bevelen wij u aan om Bitdefender Safepay™ met Hotspot-bescherming voor onveilige netwerken geactiveerd.

Wi-Fi is niet veilig - betekent dat het beveiligingsniveau van het netwerk matig is. Dit betekent dat het kwetsbaarheden kan bevatten en het is niet aanbevolen om betalingen uit te voeren of bankrekeningen te controleren zonder extra bescherming. In dergelijke situaties bevelen wij u aan om Bitdefender Safepay™ met Hotspot-bescherming voor onveilige netwerken geactiveerd.

Wi-Fi is veilig - betekent dat het netwerk dat u gebruikt, veilig is. In dit geval kunt gevoelige gegevens gebruiken om online bewerkingen uit te voeren.

Als u op de koppeling **Informatie bekijken** in het gebied van elk netwerk klikt, worden de volgende gegevens weergegeven:

- **Beveiligd** - hier kunt u bekijken of het geselecteerde netwerk al dan niet beveiligd is. Onbeveiligde netwerken kunnen de gegevens die u gebruikt, toegankelijk laten.
- **Type versleuteling** - hier kunt u bekijken welk type versleuteling wordt gebruikt door het geselecteerde netwerk. Bepaalde versleutelingstypes zijn mogelijk niet veilig. Daarom bevelen we u sterk aan om informatie over het weergegeven versleutelingstype te controleren, zodat u zeker bent dat u beschermd bent terwijl u op het internet surft.
- **Kanaal/Frequentie** - hier kunt u de frequentie van het kanaal bekijken dat het geselecteerde netwerk gebruikt.
- **Wachtwoordkwaliteit** - hier kunt u bekijken hoe sterk het wachtwoord is. Merk op dat de netwerken met een zwak wachtwoord een doelwit vormen voor cybercriminelen.
- **Type aanmelding** - hier kunt u bekijken of het geselecteerde netwerk al dan niet beschermd is met een wachtwoord. Het is sterk aanbevolen om enkel een verbinding te maken met netwerken die een sterk wachtwoord hebben.
- **Type authentificatie** - hier kunt u bekijken welk type authentificatie wordt gebruikt door het geselecteerde netwerk.

Zorg ervoor dat de optie **Melden** geactiveerd blijft, zodat u meldingen krijgt, telkens wanneer uw systeem met dit netwerk een verbinding maakt.

18. BESCHERMING RANSOMWARE

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.

De infectie kan verspreid worden via spam-e-mails, door bijlagen te downloaden of door besmette websites te bezoeken en schadelijke applicatie ste installeren zonder dat de gebruiker weet wat er met zijn systeem gebeurt.

Ransomware kan een of meer van de volgende gedragingen vertonen, die verhinderen dat de gebruiker naar zijn systeem kan gaan:

- Versleuteling van gevoelige en persoonlijke bestanden zonder de mogelijkheid te bieden om ze te ontsleutelen tot het slachtoffer er losgeld voor betaalt.
- Vergrendelt het computerscherm en geeft een bericht weer dat om geld vraagt. In dat geval is er geen enkel bestand versleuteld, de gebruiker wordt enkel gedwongen om de betaling uit te voeren.
- Blokkeert applicaties zodat ze niet kunnen uitgevoerd worden.

Aan de hand van de recentste technologie beschermt Bitdefender Ransomware-bescherming de systeemintegriteit door cruciale systeemgebieden te beschermen tegen schade zonder het systeem te belasten. U kunt uw persoonlijke bestanden, zoals documenten, foto's, filmpjes of bestanden die u in de cloud opslaat, die u in de cloud opslaat, echter ook beschermen.

18.1. De Ransomware-bescherming in- of uitschakelen

De module Bescherming tegen Ransomware uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **BESCHERMING TEGEN RANSOMWARE**-module.

4. Klik op de bijhorende schakelaar om de **Bescherming tegen Ransomware** in of uit te schakelen.

Telkens wanneer een applicatie probeert om naar een beschermd bestand te gaan, wordt een Bitdefender pop-up weergegeven. U kunt de toegang toestaan of weigeren.

18.2. Persoonlijke bestanden beschermen tegen ransomware-aanvallen.

Indien u persoonlijke bestanden veilig wilt onderbrengen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **BESCHERMING TEGEN RANSOMWARE**-module.
4. Klik op de knop **ADD**.
5. Ga naar de map die u wilt beschermen en klik daarna op **OK** om de geselecteerde map aan de beschermde omgeving toe te voegen.

Standaard worden de mappen Documenten, Foto's, Video's, Muziek, Bureaublad, Openbare documenten, Openbare foto's, Openbare video's, Openbare muziek en Openbaar bureaublad beschermd tegen malware-aanvallen.

> **Opmerking**
> Aangepaste mappen kunnen enkel beschermd worden voor huidige gebruikers. Systeem- en applicatiebestanden kunnen niet aan uitzonderingen toegevoegd worden.

18.3. Vertrouwde applicaties configureren

Ransomware-bescherming inactiveren voor specifieke toepassingen, maar enkel deze die u vertrouwt mogen aan de lijst toegevoegd worden.

Betrouwbare applicaties toevoegen aan uitsluitingen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.

3. In de **BESCHERMING TEGEN RANSOMWARE**-module selecteert u **Vertrouwde applicaties**.
4. Klik op **Toevoegen** en overloop de applicaties die u wilt beschermen.
5. Klik op **OK** om de geselecteerde applicatie toe te voegen aan de beschermingsomgeving.

18.4. Geblokkeerde applicaties configureren

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 uitsluiten via de volgende stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **BESCHERMING TEGEN RANSOMWARE**-module selecteert u **Geblokkeerde applicaties**.
4. Klik op **Toestaan** en overloop de applicatie waarvan u zeker bent dat ze veilig is.
5. Klik op **OK** om de geselecteerde applicatie toe te voegen aan de betrouwbare lijst.

18.5. Bescherming bij opstarten

Het is bekend dat heel wat malware-applicaties zo ingesteld zijn dat ze uitgevoerd worden tijdens het opstarten van het systeem, iets wat een computer erg veel schade kan toebrengen. Bitdefender-boottijdbescherming scant alle cruciale systeemgebieden voordat alle bestanden worden geladen, zonder enige impact op het systeem. Tegelijkertijd wordt bescherming geboden tegen bepaalde aanvallen die gebaseerd zijn op de uitvoering van de stack- of heapcode of code-injecties of haken binnen bepaalde cruciale dynamische bibliotheken.

Bescherming bij het opstarten uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.

3. Selecteer de icoon in de rechterbovenhoek van de **BESCHERMING TEGEN RANSOMWARE**-module.
4. Klik op de bijhorende schakelaar om de **Bescherming bij opstarten** in of uit te schakelen.

19. SAFEPAY BEVEILIGING VOOR ONLINE TRANSACTIES

De computer wordt in snel tempo het hoofdhulpmiddel voor winkelen en bankieren. Facturen betalen, geld overmaken, bijna alles wat u zich maar voor kunt stellen kopen, dat alles is nooit sneller en gemakkelijker geweest.

Dit houdt in het verzenden via Internet van persoonlijke gegevens, account- en creditcardgegevens, wachtwoorden en andere soorten privégegevens, met andere woorden, precies het soort gegevensstroom waar cybercriminelen graag gebruik van maken. Hackers zijn meedogenloos in hun pogingen deze gegevens te stelen, dus u kunt nooit voorzichtig genoeg zijn als het om het beveiligen van online transacties gaat.

Bitdefender Safepay™ is allereerst een beveiligde browser, een verzegelde omgeving, die is bestemd voor het privé en veilig houden van online bankieren, e-shopping en andere soorten online transacties.

Voor de beste privacybeveiliging is Bitdefender-Wachtwoordbeheerder geïntegreerd in Bitdefender Safepay™ om uw gegevens te beveiligen wanneer u naar persoonlijke online plaatsen gaat. Meer informatie vindt u onder "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 126).

Bitdefender Safepay™ biedt de volgende functies:

- Het blokkeert de toegang tot uw desktop en elke poging snapshots van uw scherm te maken.
- Het beveiligt uw geheime wachtwoorden als u online surft met Wachtwoordbeheerder.
- Het verschaft een virtueel toetsenbord dat het, als het wordt gebruikt, onmogelijk maakt voor hackers uw aanslagen te lezen.
- Het is volledig onafhankelijk van uw andere browsers.
- Het biedt een ingebouwde hotspotbeveiliging die kan worden gebruikt wanneer uw computer is verbonden met onbeveiligde Wi-Fi-netwerken.
- Het ondersteunt bookmarks en stelt u in staat om te surfen tussen uw favoriete bank/winkelsites.
- Het is niet beperkt tot bankieren en online winkelen. Elke website kan worden geopend in Bitdefender Safepay™.

19.1. Bitdefender Safepay™ gebruiken

Standaard detecteert Bitdefender wanneer u naar een online banksite of online winkel in een willekeurige browser op uw computer surft en het vraagt u deze site te starten in Bitdefender Safepay™.

Om naar de hoofdinterfae van Bitdefender Safepay™ te gaan, gebruikt u een van de volgende manieren:

- Vanuit de Bitdefender-interface:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de actieknop **Safepay**.
- Voor Windows:
  - In **Windows 7**:
    1. Klik op **Start** en ga naar **Alle Programma's**.
    2. Klik op **Bitdefender**.
    3. Klik op **Bitdefender Safepay™**.
  - In **Windows 8 en Windows 8.1**:

    Zoek Bitdefender Safepay™ vanuit het Windows-startscherm (u kunt bijvoorbeeld beginnen met het typen van "Bitdefender Safepay™", rechtstreeks in het startscherm) en klik op het pictogram.
  - In **Windows 10**:

    Typ "Bitdefender Safepay™" in het zoekveld in de taakbalk en klik op het pictogram ervan.

Opmerking

Als de Adobe Flash Player plug-in niet is geïnstalleerd of verouderd is, wordt er een Bitdefender-bericht weergegeven. Klik op de overeenkomstige knop om door te gaan.
Nadat het installatieproces is voltooid, dient u handmatig de Bitdefender Safepay™-browser te heropenen om verder te gaan met uw werk.

Indien u gewend bent aan webbrowsers, zult u geen moeite hebben Bitdefender Safepay™ te gebruiken - het ziet eruit en gedraagt zich als een gewone browser:

- geef de URL's op in de adresbalk van de sites waar u heen wilt gaan.

- voeg tabs toe om meerdere websites te bezoeken in het Bitdefender Safepay™-venster door te klikken op .
- surf terug en vooruit en vernieuw pagina's met gebruikmaking van respectievelijk .
- ga naar Bitdefender Safepay™ instellingen door te klikken op en kies **Instellingen**.
- beveilig uw wachtwoorden met Wachtwoordbeheerder door te klikken op .
- beheer uw favorieten door te klikken op naast de adresbalk.
- het virtuele toetsenbord openen door te klikken op .
- vergroot of verklein de browserafmetingen door gelijktijdig te drukken op de toetsen **Ctrl** en **+/-** op het numerieke toetsenbord.
- informatie bekijken over uw Bitdefender-product door te klikken op en kies **Over...**.
- belangrijke informatie afdrukken door te klikken op .

Opmerking
Om om te schakelen tussen Bitdefender Safepay™ en Windows desktop, drukt u op de toetsen **Alt+Tab** of klikt u op de knop **Minimaliseren**.

19.2. Instellingen configureren

Klik op en kies **Instellingen** om Bitdefender Safepay™ te configureren:

- In de **Algemene instellingen** kunt u het volgende instellen:

  Gedrag van Bitdefender Safepay™
  Kies wat u wilt dat er gebeurt als u naar een online winkel of site voor online bankieren gaat in uw gewone webbrowser:
  - Websites automatisch openen in Safepay.
  - Me aanraden Safepay te gebruiken.
  - Me niet aanraden Safepay te gebruiken.

  Domeinenlijst
  Kies hoe Bitdefender Safepay™ zich gedraagt als u websites van specifieke domeinen bezoekt in uw gewone webbrowser door ze toe te voegen aan de domeinenlijst en het gedrag voor elk van hen te selecteren:

- Automatisch openen in Bitdefender Safepay™.
- Bitdefender u elke keer laten vragen wat u wilt doen.
- Bitdefender Safepay™ nooit gebruiken wanneer er een pagina van het domein wordt bezocht in een gewone browser.

Pop-ups blokkeren

U kunt ervoor kiezen om pop-ups te blokkeren door te klikken op de overeenkomende schakelaar.

U kunt ook een lijst aanmaken met websites waarvan u pop-ups toestaat. De lijst mag websites bevatten die u volledig vertrouwt.

Om een site toe te voegen aan de lijst, geeft u het adres van de site op in het overeenkomende veld en klikt u op **Domein toevoegen**.

Om een website uit de lijst te verwijderen, selecteert u het X-je bij het gewenste gegeven.

Hotspot-bescherming activeren

U kunt een extra beschermingslaag activeren wanneer u verbonden bent met onbeveiligde WiFi-netwerken door deze functie te activeren.

Ga naar "*Hotspotbeveiliging voor onbeveiligde netwerken*" (p. 124) voor meer informatie.

- In het gebied **Geavanceerde instellingen** zijn de volgende opties beschikbaar:

Plug-ins beheren

U kunt kiezen of u specifieke plug-ins in Bitdefender Safepay™ wenst te activeren of inactiveren.

Certificaten beheren

U kunt certificaten van uw systeem importeren naar een certificatenwinkel.

Selecteer **Certificaten importeren** en volg de wizard om de certificaten te gebruiken in Bitdefender Safepay™.

Virtueel Toetsenbord automatisch starten bij wachtwoordvelden

Het Virtuele toetsenbord verschijnt automatisch wanneer een wachtwoordveld wordt geselecteerd.

Gebruik de bijhorende schakelaar om de functie te activeren of inactiveren.

Vraag om bevestiging voor u gaat afdrukken
Activeer deze optie indien u uw bevestiging wenst te geven voordat het afdrukproces start.

19.3. Favorieten beheren

Indien u de automatische detectie van sommige of alle websites hebt uitgeschakeld, of Bitdefender detecteert bepaalde websites eenvoudigweg niet, dan kunt u favorieten toevoegen aan Bitdefender Safepay™ zodat u favoriete websites in de toekomst eenvoudig kunt starten.

Volg deze stappen om een URL toe te voegen aan Bitdefender Safepay™-favorieten:

1. Klik op de -icoon naast de adresbalk om de pagina met favorieten te openen.

   Opmerking
   De pagina met favorieten is standaard geopend als u Bitdefender Safepay™ start.

2. Klik op de knop **+** om een nieuwe favoriete pagina toe te voegen.
3. Voer de URL en de titel van de favoriete pagina in en klik op **Aanmaken**. Vink de optie **Automatisch openen in Safepay** aan indien u de gemarkeerde pagina wilt openen met Bitdefender Safepay™, telkens als u er naartoe gaat. De URL wordt ook toegevoegd aan de Domeinenlijst op de instellingen-pagina.

19.4. Hotspotbeveiliging voor onbeveiligde netwerken

Als u Bitdefender Safepay™ gebruikt terwijl u bent verbonden met onbeveiligde Wi-Fi-netwerken (bijvoorbeeld een openbare hotspot), dan wordt er een extra beveiligingslaag geboden door de functie 'Hotspotbeveiliging'. Deze service versleutelt internetcommunicatie via onbeveiligde verbindingen en helpt u daarmee om uw privacy te bewaren, via welk netwerk u ook bent verbonden.

De Hotspot-bescherming werkt enkel als uw computer verbonden is met een onbeveiligd netwerk.

De beveiligde verbinding wordt geïnitialiseerd en er wordt een bericht weergegeven in het Bitdefender Safepay™-venster wanneer de verbinding

tot stand is gebracht. Het symbool verschijnt voor de URL in de adresbalk om u te helpen beveiligde verbindingen gemakkelijk te herkennen.

U moet de handeling mogelijk accepteren.

20. BEVEILIGING WACHTWOORDBEHEERDER VOOR UW GEGEVENS

We gebruiken onze computers om online te winkelen of onze rekeningen te betalen, om in te loggen op platforms van sociale media of op toepassingen voor instant messaging.

Maar zoals iedereen weet, is het niet altijd gemakkelijk om het wachtwoord te onthouden!

En we zijn niet voorzichtig als we online surfen, onze persoonlijke gegevens, zoals ons e-mailadres, onze ID van instant messaging of onze creditcardgegevens kunnen in gevaar komen.

Het bewaren van uw wachtwoorden of uw persoonlijke gegevens of een vel papier of in de computer kan gevaarlijk zijn, want ze kunnen worden gezien en gebruikt door mensen die deze gegevens willen stelen en gebruiken. En elk wachtwoord dat u hebt ingesteld voor uw online accounts of voor uw favoriete websites onthouden, is geen gemakkelijke taak.

Is er daarom een manier om ervan verzekerd te zijn dat we onze wachtwoorden vinden wanneer we ze nodig hebben? En kunnen we verzekerd blijven dat onze geheime wachtwoorden altijd veilig zijn?

Wachtwoordbeheerder helpt om uw wachtwoorden bij te houden, beveilgt uw privacy en bezorgt een veilige online surfervaring.

Door het gebruik van een enkel masterwachtwoord om naar uw gegevens te gaan, maakt Wachtwoordbeheerder het gemakkelijk voor u om uw wachtwoorden veilig te houden in een Portefeuille.

Om de beste beveiliging voor uw online activiteiten te bieden, is Wachtwoordbeheerder geïntegreerd met Bitdefender Safepay™ en verschaft een samengebundelde oplossing voor de verschillende wegen waarop uw persoonlijke gegevens in gevaar kunnen komen.

Wachtwoordbeheerder beveiligt de volgende persoonlijke gegevens:

- Persoonlijke gegevens, zoals het e-mailadres of het telefoonnummer
- Logingegevens voor de websites
- Bankrekeninggegevens of het creditcardnummer
- Toegangsgegevens naar de e-mailaccounts

- Wachtwoorden voor de toepassingen
- Wachtwoorden voor de Wi-Fi-netwerken

20.1. Maak een nieuwe Wallet database aan

Bitdefender-portefeuille is de plek waar u uw persoonlijke gegevens kunt opslaan. Voor een makkelijkere browserervaring moet u een als volgt een Portefeuilledatabase aanleggen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de module **WACHTWOORDMANAGER** selecteert u **Nieuwe portefeuille aanmaken**.
4. Selecteer de knop **Nieuw aanmaken**.
5. Typ de vereiste informatie in de overeenkomende velden.
   - Portefeuillelabel instellen - tik een unieke naam in voor de database van uw Portefeuille
   - Masterwachtwoord - tik een wachtwoord in voor uw Portefeuille.
   - Tik het wachtwoord opnieuw in - tik het wachtwoord dat u hebt ingesteld opnieuw in.
   - Hint - tik een hint in om het wachtwoord te herinneren.
6. Klik op **Doorgaan**.
7. In deze stap kunt u kiezen om uw informatie in de cloud op te slaan. Indien u Ja selecteert, blijft bankinformatie lokaal op uw toestel opgeslagen. Kies de gewenste optie en klik daarna op **Verdergaan**.
8. Selecteer de webbrowser waarvan u de gegevens van wilt importeren.
9. Klik op **Voltooien**.

20.2. Importeer een bestaande database

Om een plaatselijk opgeslagen database te importeren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.

3. In de module **WACHTWOORDMANAGER** selecteert u **Nieuwe portefeuille aanmaken**.
4. Selecteer de knop **Vanuit doel**.
5. Zoek de locatie van uw portefeuilledatabase en selecteer deze (het .db-bestand).
6. Klik op **Openen**.
7. Geef uw Portefeuille een naam en voer het wachtwoord dat bij de aanmaak werd toegekend, in.
8. Klik op **Importeren**.
9. Selecteer de programma's van waaruit u de Portefeuille legitimatiebewijzen wenst te laten importeren, en klik dan op de knop **Voltooien**.

20.3. De Portefeuille-database exporteren

Uw Portefeuilledatabase exporteren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de module **WACHTWOORDMANAGER** selecteert u **Mijn portefeuille**.
4. Klik op de -icoon op de gewenste portefeuille en selecteer vervolgens **Exporteren**.
5. Zoek de locatie van uw portefeuilledatabase en selecteer deze (het .db-bestand).
6. Klik op **Opslaan**.

> **Opmerking**
> De Portefeuille moet geopend zijn om de **Exporteren**-optie beschikbaar te maken.
> Indien de portefeuille die u moet exporteren vergrendeld is, klikt u op de knop **PORTEFEUILLE ACTIVEREN** en voert u het wachtwoord in dat werd aangemaakt van bij het begin.

20.4. Synchroniseer uw portefeuilles in de cloud

De portefeuillesynchronisatie in de cloud in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de module **WACHTWOORDMANAGER** selecteert u **Mijn portefeuille**.
4. Klik op de -icoon op de gewenste portefeuille en selecteer vervolgens **Instellingen**.
5. Kies de gewenste optie in het venster dat verschijnt en klik vervolgens op **Opslaan**.

Opmerking
De Portefeuille moet geopend zijn om de **Exporteren**-optie beschikbaar te maken.
Indien de portefeuille die u moet synchroniseren, vergrendeld is, klikt u op de knop **PORTEFEUILLE ACTIVEREN** en voert u het wachtwoord in dat werd aangemaakt van bij het begin.

20.5. Uw Portefeuille-gegevens beheren

Uw wachtwoorden beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de module **WACHTWOORDMANAGER** selecteert u **Mijn portefeuille**.
4. Selecteer de gewenste Portefeuilledatabase uit het venster **MIJN PORTEFEUILLES** en klik vervolgens op de **PORTEFEUILLE ACTIVEREN**-knop.
5. Voer het hoofdwachtwoord in en klik op **OK**.

Er verschijnt een nieuw venster. Selecteer de gewenste categorie in het bovenste deel van het venster:

- Identiteit
- Websites
- Online bank
- E-mails
- Applicaties

- Wi-Fi-netw.

De gegevens aanvullen / bewerken

- Om een nieuw wachtwoord toe te voegen, kiest u de gewenste categorie bovenaan en klikt u op **+ Item toevoegen**, vul de gegevens in de betreffende velden in en klik op de knop Opslaan.
- Om een gegeven in de tabel te bewerken, selecteert u het gegeven en klikt u op de knop **Bewerken**.
- Om een invoer te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**.

20.6. De Wachtwoordbeheerderbeveiliging in- of uitschakelen

De bescherming van Wachtwoordmanager in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **WACHTWOORDMANAGER**-module.
4. Gebruik de bijhorende schakelaar om de Wachtwoordmanager in of uit te schakelen.

20.7. De instellingen voor Wachtwoordbeheerder beheren

Het hoofdwachtwoord in detail configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **WACHTWOORDMANAGER**-module.
4. Selecteer het tabblad **VEILIGHEIDSINSTELLINGEN**.

De volgende opties zijn beschikbaar:

- **Mijn masterwachtwoord vragen wanneer ik inlog op mijn pc** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot de computer.
- **Mijn masterwachtwoord vragen wanneer ik mijn browsers en toepassingen open** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot een browser of toepassing.
- **Portefeuille automatisch vergrendelen wanneer ik mijn PC onverwacht verlaat** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u na 15 minuten terugkeert naar de computer.

Belangrijk
Zorg dat u uw masterwachtwoord onthoudt of bewaar het op een veilige plaats. Als u het wachtwoord vergeten bent, moet u het programma opnieuw installeren of contact opnemen met Bitdefender voor ondersteuning.

Verbeter uw ervaring

Om de browsers of toepassingen waarin u de wachtwoordmanager wilt integreren te selecteren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **WACHTWOORDMANAGER**-module.
4. Selecteer het tabblad **PLUG-INS**.

   Kies een toepassing om de Wachtwoordbeheerder te gebruiken en verbeter uw ervaring:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Autofill configureren

De functie Autofill maakt het u gemakkelijk om verbinding te maken met uw favoriete websites of om in te loggen op uw online accounts. De eerste keer

dat u uw certificaten en persoonlijke gegevens invoert in uw webbrowser, worden ze automatisch beveiligd in de Portefeuille.

Om de **Autofill**-instellingen te configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **WACHTWOORDMANAGER**-module.
4. Selecteer het tabblad **AUTOFILL-INSTELLINGEN**.
5. De volgende opties configureren:
   - **Configureren hoe Wallet uw gegevens beveiligt.**:
     - **Inloggegevens automatisch opslaan in Portefeuille** - de logingegevens en andere herkenbare gegevens zoals uw persoonlijke en creditcardgegevens worden automatisch opgeslagen en bijgewerkt in de Portefeuille.
     - **Vraag me elke keer** - u wordt elke keer gevraagd of u uw gegevens aan de Portefeuille wilt toevoegen.
     - **Niet opslaan, ik werk de gegevens handmatig bij** - de gegevens kunnen alleen handmatig aan de Portefeuille worden toegevoegd.
   - **Inlogreferenties automatisch aanvullen**:
     - **Autofill logingegevens elke keer** - de gegevens worden automatisch in de browser ingevuld.
   - **Autofill formulieren**:
     - **Geef mijn in te vullen opties aan als ik een pagina met formulieren bezoek** - een pop-up met de invulopties verschijnt telkens wanneer Bitdefender detecteert dat u een online betaling wilt uitvoeren of wilt intekenen.

De Wachtwoordbeheerder beheren vanuit uw browser

U kunt de informatie Wachtwoordbeheerder gemakkelijk beheren vanuit uw browser, zodat u alle belangrijke gegevens bij de hand hebt. De invoegtoepassing Bitdefender wordt ondersteund door de volgende browsers: Google Chrome, Internet Explorer en Mozilla Firefox, en hij is ook geïntegreerd in Safepay.

Om naar de Portefeuille-extensie van Bitdefender te gaan, opent u uw webbrowser, accepteert de installatie van de invoegtoepassing en klikt op het  pictogram op de taakbalk.

De Portefeuille-extensie van Bitdefender bevat de volgende opties:

- Portefeuille openen - opent de Portefeuille.
- Portefeuille vergrendelen - vergrendelt de portefeuille.
- Websites - opent een submenu met alle logins van de websites die in Portefeuille zijn opgeslagen. Klik op **Website toevoegen** om de nieuwe websites aan de lijst toe te voegen.
- Formulieren invullen - opent een submenu met de gegevens die u voor een speciale categorie hebt toegevoegd. Van hieruit kunt u nieuwe gegevens aan uw Portefeuille toevoegen.
- Wachtwoordgenerator - hiermee kunt u willekeurige wachtwoorden genereren die u voor nieuwe of bestaande accounts kunt gebruiken. Klik op **Geavanceerde instellingen tonen** om de complexiteit van het wachtwoord aan te passen.
- Instellingen - opent het instellingenvenster van Wachtwoordbeheerder.
- Probleem melden - meldt elk willekeurig probleem dat u ondervindt met Wachtwoordbeheerder van Bitdefender

21. BITDEFENDER USB IMMUNIZER

De Autorun-functie die is ingebouwd in Windows-besturingssystemen is een heel handig hulpmiddel waardoor computers automatisch een bestand kunnen uitvoeren vanaf media die zijn verbonden met deze computers. Software-installaties bijvoorbeeld kunnen automatisch starten als er een cd in de cd-lezer wordt geschoven.

Helaas kan deze functie ook worden gebruikt door malware om automatisch te starten en zo in uw computer te infiltreren vanaf media die beschreven kunnen worden, zoals USB-sticks en geheugenkaarten die via kaartlezers worden verbonden. De afgelopen jaren zijn er talloze op Autorun gebaseerde aanvallen aangemaakt.

Met USB Immunizer kunt u voorkomen dat een willekeurige NTFS, FAT32 of FAT-geformatteerde USB-stick ooit nog automatisch malware uitvoert. Zodra een USB-apparaat immuun is gemaakt, kan malware het niet langer configureren om een bepaalde toepassing uit te voeren wanneer het apparaat wordt verbonden met een Windows-computer.

Om een USB-apparaat te immuniseren:

1. Verbind de USB-stick met uw computer.
2. Blader op uw computer naar de locatie van het verwijderbare opslagapparaat en rechterklik op het pictogram ervan.
3. Ga in het contextuele menu naar **Bitdefender** en selecteer **Deze schijf immuniseren**.

> **Opmerking**
> Als het station al immuun is gemaakt, verschijnt het bericht **Het USB-apparaat wordt beveiligd tegen op autorun gebaseerde malware** in plaats van de optie Immuniseren.

Om te voorkomen dat uw computer malware start vanaf USB-apparaten die niet immuun zijn gemaakt, kunt u de media autorun-functie uitschakelen. Meer informatie vindt u onder "*De automatische kwetsbaarheidsbewaking gebruiken*" (p. 110).

SYSTEEMOPTIMALISATIE

22. PROFIELEN

Dagelijkse werkactiviteiten, films kijken of games spelen kan het systeem vertragen, met name wanneer ze tegelijkertijd worden uitgevoerd met het Windows-updateproces en onderhoudstaken. Met Bitdefender kunt u nu uw voorkeursprofiel kiezen en toepassen. Het maakt systeemafstellingen om de prestaties van specifieke geïnstalleerde toepassingen te verbeteren.

Bitdefender verschaft de volgende profielen:

- Werkprofiel
- Filmprofiel
- Gameprofiel
- Openbaar Wi-Fi-profiel
- Profiel batterijmodus

Als u besluit om **Profielen** niet te gebruiken, wordt er een standaardprofiel ingeschakeld genaamd **Standaard** dat geen optimalisering verschaft aan uw systeem.

Afhankelijk van uw activiteit worden de volgende productinstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Alle Bitdefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Automatische Update wordt uitgesteld.
- Geplande scans zijn uitgesteld.
- Search Advisor is uitgeschakeld.
- Speciale aanbiedingen en productmeldingen zijn uitgeschakeld.

Afhankelijk van uw activiteit worden de volgende systeeminstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Automatische Windows-updates zijn uitgesteld.
- Windows-waarschuwingen en pop-ups zijn uitgeschakeld.
- Onnodige programma's op de achtergrond worden gestaakt.
- Visuele effecten worden afgesteld voor de beste prestaties.
- Onderhoudstaken worden uitgesteld.

- Instellingen voor het vermogen worden aangepast.

Terwijl u in het Openbare Wi-Fi-profiel werkt, is Bitdefender Antivirus Plus 2017 ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Actief dreigingsbeheer is ingeschakeld
- De volgende instellingen van Webbescherming zijn ingeschakeld:
  - SSL scannen
  - Bescherming tegen fraude
  - Bescherming tegen phishing

22.1. Werkprofiel

Meerdere taken uitvoeren op het werk, zoals het verzenden van e-mails, een videogesprek hebben met collega's op afstand of werken met designtoepassingen kan invloed hebben op uw systeemprestaties. Werkprofiel is ontworpen om u te helpen uw werkefficiëntie te verbeteren, door een aantal diensten op de achtergrond en onderhoudstaken uit te schakelen.

Werkprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Werkprofiel zit:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.
5. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties boosten op werktoepassingen
   - Productinstellingen voor Werkprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen
6. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig toepassingen toevoegen aan de lijst Werkprofiel

Indien Bitdefender niet automatisch naar Werkprofiel overschakelt wanneer u een bepaalde werktoepassing start, kunt u de toepassing handmatig toevoegen aan de **Toepassingenlijst**.

Om handmatig toepassingen toe te voegen aan de Toepassingenlijst in Werkprofiel:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.
5. In het venster **WERKPROFIEL** klikt u op de link **Toepassingenlijst**.
6. Klik op **Toevoegen** om een nieuwe toepassing toe te voegen aan de **Toepassingenlijst**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

22.2. Filmprofiel

Het weergeven van videocontent in HD-kwaliteit, zoals HD-films, vereist belangrijke systeemvermogens. Filmprofiel stelt het systeem- en de productinstellingen af zodat u kunt genieten van een ononderbroken en vloeiende filmervaring.

Filmprofiel configureren

Om de te nemen handelingen te configureren terwijl u in Filmprofiel bent:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
5. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor videospelers boosten

- Productinstellingen voor Filmprofiel optimaliseren
- Programma's op de achtergrond en onderhoudstaken uitstellen
- Automatische Windows-updates uitstellen
- Instellingen vermogensplan voor films afstellen.

6. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig videospelers toevoegen aan de lijst Filmprofiel

Indien Bitdefender niet automatisch naar Filmprofiel overschakelt wanneer u een bepaalde videospeler start, kunt u de toepassing handmatig toevoegen aan de **Spelerslijst**.

Om handmatig videospelers toe te voegen aan de Spelerslijst in Filmprofiel:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
5. In het venster **FILMPROFIEL** klikt u op de link **Spelerslijst**.
6. Klik op **Toevoegen** om een nieuwe toepassing toe te voegen aan de **Spelerslijst**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

22.3. Gameprofiel

Genieten van een ononderbroken game-ervaring heeft alles te maken met het verminderen van systeemolaadtijden en het beperken van vertraging. Door gebruik te maken van gedragsheuristiek tegelijk met een lijst van bekende games, kan Bitdefender automatisch uitgevoerde games detecteren en uw systeemvermogen optimaliseren zodat u kunt genieten van uw gametijd.

Gameprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Gameprofiel zit:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.

2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Gameprofiel.
5. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor games boosten
   - Productinstellingen voor Gameprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen
   - Instellingen vermogensplan voor games afstellen.
6. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig games aan de Spellijst toevoegen

Indien Bitdefender niet automatisch naar het Gameprofiel overschakelt wanneer u een bepaalde game of toepassing start, kunt u de toepassing handmatig toevoegen aan de **Spellijst**.

Om handmatig games aan de Spellijst toe te voegen in het Gameprofiel:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Gameprofiel.
5. In het venster **GAMEPROFIEL** klikt u op de link **Spellijst**.
6. Klik op **Toevoegen** om een nieuwe game toe te voegen aan de **Spellijst**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de game, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

22.4. Openbaar Wi-Fi-profiel

E-mailberichten verzenden, gevoelige logingegevens invoeren of online winkelen terwijl u met onveilige draadloze netwerken verbonden bent, kan uw persoonlijke gegevens in gevaar brengen. Openbaar Wi-Fi-profiel past de

productinstellingen aan, zodat u online betalingen kunt uitvoeren en gevoelige informatie kunt gebruiken in een beveiligde omgeving.

Openbaar Wi-Fi-profiel configureren

Om Bitdefender configureren zodat productinstellingen worden toegepast wanneer u verbonden bent met een onveilig draadloos netwerk:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Openbaar Wi-Fi-profiel.
5. Laat het vakje **Pas de productinstellingen aan om de bescherming te stimuleren bij verbinding met een onveilig openbaar Wi-Fi-netwerk** aangevinkt.
6. Klik op **Opslaan**.

22.5. Profiel batterijmodus

Het profiel Accumodus is speciaal ontworpen voor laptop- en tabletgebruikers. Het doel ervan is om de invloed op vermogensverbruik van zowel systeem als Bitdefender te beperken als het accuniveau lager is dan de standaardconsumptie van deze die u selecteert.

Profiel Accumodus aan het configureren

Om het profiel Accumodus te configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Zorg ervoor dat de optie **Profielen** ingeschakeld is.
4. Klik op de knop **CONFIGUREREN** in het gebied Profiel Batterijmodus.
5. Kies de afstellingen voor het systeem die moeten worden toegepast door de volgende opties aan te vinken:
   - Productinstellingen voor Accumodus optimaliseren.
   - Programma's op de achtergrond en onderhoudstaken uitstellen.

- Automatische Windows-updates uitstellen.
- Instellingen vermogensplan voor Accumodus afstellen.
- Externe apparaten en netwerkpoorten uitschakelen.

6. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Tik een geldige waarde in het vakje in of selecteer er een met de pijltjes omhoog en om laag om in te stellen wanneer het systeem moet beginnen werken in Batterijmodus. Standaard is de modus geactiveerd als het accuniveau onder de 30% komt.

De volgende productinstellingen worden toegepast als Bitdefender in het profiel Accumodus handelt:

- Bitdefender Automatische Update is uitgesteld.
- Geplande scans zijn uitgesteld.
- Beveiligingswidget is uitgeschakeld.

Bitdefender detecteert wanneer uw laptop overschakelt op accuvoeding en afhankelijk van het accuniveau gaat het dan automatisch over op de Accumodus. Op dezelfde manier verlaat Bitdefender automatisch de Accumodus, als de laptop niet langer op de accu werkt.

22.6. Real-Time Optimalisering

Bitdefender Real-Time Optimalisering is een plug-in die uw systeemprestaties geruisloos verbetert, op de achtergrond, en garandeert dat u niet wordt onderbroken terwijl u in een profielmodus bent. Afhankelijk van de CPU-belasting bewaakt de plug-in alle processen en richt zich op die processen die een hogere belasting aannemen om ze aan te passen aan uw behoeften.

Om Realtime-optimalisatie in of uit te schakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Gebruik de bijhorende schakelaar om de Optimalisatie in reële tijd in of uit te schakelen.

PROBLEMEN OPLOSSEN

23. ALGEMENE PROBLEMEN OPLOSSEN

Dit hoofdstuk beschrijft enkele problemen die zich kunnen voordoen terwijl u Bitdefender gebruikt en biedt u mogelijke oplossingen voor deze problemen. De meeste problemen kunnen worden opgelost door de juiste configuratie van de productinstellingen.

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Hulp vragen*" (p. 169).

23.1. Mijn systeem lijkt traag

Na het installeren van beveiligingssoftware kan er doorgaans een lichte vertraging van het systeem merkbaar zijn. Dit is normaal tot in zekere mate.

Als u een aanzienlijke vertraging opmerkt, kan dit probleem verschijnen door de volgende redenen:

- **Bitdefender is niet het enige beveiligingsprogramma dat op uw systeem is geïnstalleerd.**

  Hoewel Bitdefender de beveiligingsprogramma's verwijdert die tijdens de installatie zijn gevonden, is het aanbevolen elk ander antivirusprogramma

dat u mogelijk gebruikt voordat u Bitdefender installeert, te verwijderen. Meer informatie vindt u onder "*Andere beveiligingsoplossingen verwijderen*" (p. 73).

- **Er is niet voldaan aan de minimale systeemvereisten voor het uitvoeren van Bitdefender.**

  Als uw apparaat niet voldoet aan de minimale systeemvereisten, wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn. Meer informatie vindt u onder "*Minimale systeemvereisten*" (p. 3).

- **U hebt toepassingen geïnstalleerd die u niet gebruikt**.

  Elke computer heeft programma's of toepassingen die u niet gebruikt. En veel ongewenste programma's worden op de achtergrond uitgevoerd en nemen schijfruimte en geheugen in. De-installeer een programma als u het niet gebruikt. Dit geldt ook voor andere vooraf geïnstalleerde software of evaluatietoepassingen die u hebt vergeten te verwijderen.

  > **Belangrijk**
  > Indien u vermoedt dat een programma of toepassing een essentieel deel van uw besturingssysteem uitmaakt, verwijder het dan niet en neem contact op met Bitdefender-klantenservice voor hulp.

- **Uw systeem is mogelijk geïnfecteerd**.

  De snelheid en het algemene gedrag van uw systeem kan ook worden beïnvloed door malware. Spyware, virussen, Trojaanse paarden en adware eisen allemaal hun tol op de prestaties van uw computer. Zorg dat u uw systeem periodiek scant, maar minstens eenmaal per week. Het wordt aanbevolen om Bitdefender Systeemscan te gebruiken want deze scant op alle typen malware die de veiligheid van uw systeem bedreigen.

  De Systeemscan starten:

  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de koppeling **MODULES BEKIJKEN**.
  3. In de **ANTIVIRUS**-module selecteert u **Systeemscan**.
  4. Volg de stappen van de wizard.

23.2. Het scannen start niet

Dit probleemtype kan twee hoofdoorzaken hebben:

- **Een eerder installatie van Bitdefender die niet volledig werd verwijderd of een ongeldige Bitdefender-installatie**.

  In dit geval:

  1. Bitdefender volledig van het systeem verwijderen:
     - In **Windows 7**:
       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
       b. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
       c. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
          - Bestanden in quarantaine
          - Wallets
       d. Klik op **VERDERGAAN**.
       e. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8 en Windows 8.1**:
       a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
       b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
       c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
       d. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
          - Bestanden in quarantaine
          - Wallets
       e. Klik op **VERDERGAAN**.
       f. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 10**:

a. Klik op **Start**, klik dan op Instellingen.

b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.

c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

e. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

- Bestanden in quarantaine
- Wallets

f. Klik op **VERDERGAAN**.

g. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

2. Uw Bitdefender reïnstalleren.

- **Bitdefender is niet de enige beveiligingsoplossing die op uw systeem is geïnstalleerd**.

  In dit geval:

  1. Verwijder de andere beveiligingsoplossing. Meer informatie vindt u onder "*Andere beveiligingsoplossingen verwijderen*" (p. 73).
  2. Bitdefender volledig van het systeem verwijderen:
     - In **Windows 7**:

       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.

       b. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

       c. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

       - Bestanden in quarantaine
       - Wallets

       d. Klik op **VERDERGAAN**.

e. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8 en Windows 8.1**:

  a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.

  b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.

  c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

  d. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

  - Bestanden in quarantaine
  - Wallets

  e. Klik op **VERDERGAAN**.

  f. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:

  a. Klik op **Start**, klik dan op Instellingen.

  b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.

  c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

  d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

  e. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

  - Bestanden in quarantaine
  - Wallets

  f. Klik op **VERDERGAAN**.

  g. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

3. Uw Bitdefender reïnstalleren.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

23.3. Ik kan de toepassing niet meer gebruiken

Dit probleem doet zich voor wanneer u probeert een programma te gebruiken dat normaal werkte vóór de installatie van Bitdefender.

Na installatie van Bitdefender kunt u een van deze situaties tegenkomen:

- U kunt van Bitdefender een bericht ontvangen met de melding dat het programma probeert een wijziging aan te brengen aan het systeem.
- U kunt een foutbericht ontvangen van het programma dat u probeert te gebruiken.

Dit soort situatie doet zich voor wanneer Actief dreigingsbeheer sommige toepassingen verkeerdelijk identificeert als kwaadaardig.

Actief dreigingsbeheer is een Bitdefender-module die de toepassingen op uw systeem voortdurend bewaakt en programma's met een potentieel boosaardig gedrag rapporteert. Omdat deze functie op een heuristisch systeem is gebaseerd, kunnen er gevallen zijn waarbij rechtmatige toepassingen worden gerapporteerd door Actief dreigingsbeheer.

Wanneer deze situatie zich voordoet, kunt u de respectieve toepassing uitsluiten van de bewaking door Actief dreigingsbeheer.

Het programma aan de lijst Uitsluitingen toevoegen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Klik op het uitklapmenu **Lijst van processen die uitgesloten worden voor de scan**. In het venster dat verschijnt, kunt u de uitsluitingen voor het proces Actief dreigingsbeheer beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik op de knop **ADD**.
   b. Klik op **Bladeren**, zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.

c. Houd de optie **Toestaan** geselecteerd om te verhinderen dat Actief dreigingsbeheer de toepassing blokkeert.

d. Klik op **Toevoegen**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

23.4. Wat moet u doen als Bitdefender een veilige website of online toepassing blokkeert

Bitdefender biedt een veilige websurfervaring door al het webverkeer te filteren en alle kwaadaardige content te blokkeren. Het is echter mogelijk dat Bitdefender een veilige website of online toepassing als onveilig beschouwd, wat tot gevolg heeft dat Bitdefender HTTP-verkeer zo scant dat het onterecht wordt geblokkeerd.

Als de zelfde pagina of toepassing herhaaldelijk geblokkeerd blijft, dan dan deze worden toegevoegd aan een witte lijst zodat hij niet wordt gescand door de engines van Bitdefender, waardoor een meer vloeiendere ervaring van websurfen wordt gegarandeerd.

Een website toevoegen aan de **Witte lijst**:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. Selecteer de icoon in de rechterbovenhoek van de **WEBBESCHERMING**-module.
4. Klik op de koppeling **Witte lijst**.
5. Geef het adres van de geblokkeerde website of online toepassing aan in het overeenkomende veld en klik op **Toevoegen**.
6. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Alleen websites en toepassingen die u volledig vertrouwt zouden moeten worden toegevoegd aan deze lijst. Ze worden uitgesloten van scannen door de volgende engines: malware, phishing en fraude.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

23.5. Wat moet ik doen indien Bitdefender een veilige toepassing als ransomware beschouwt?

Ransomware is een kwaadaardig programma dat geld probeert te verdienen van gebruikers door hun kwestbare systemen af te sluiten. Om uw systeem veilig te houden tegen tegenslagen, geeft Bitdefender u de mogelijkheid om persoonlijke bestanden te beveiligen.

Wanneer een toepassing een van uw beschermde bestanden probeert te wijzigen of te verwijderen, zal dit als onveilig worden beschouwd en zal Bitdefender de functionaliteit ervan blokkeren.

Indien een dergelijke toepassing wordt toegevoegd aan de lijst met onbetrouwbare toepassingen en u zeker bent dat u ze veilig kunt gebruiken, volgt u deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **BESCHERMING TEGEN RANSOMWARE**-module selecteert u **Geblokkeerde applicaties**.
4. Klik op **Toestaan** en overloop de applicatie waarvan u zeker bent dat ze veilig is.
5. Klik op **OK** om de geselecteerde applicatie toe te voegen aan de betrouwbare lijst.

23.6. Bitdefender updaten bij een langzame internetverbinding

Als u een langzame internetverbinding hebt (zoals een inbelverbinding), kunnen er fouten optreden tijdens het updaten.

Uw systeem up-to-date houden met de recentste Bitdefender-malwarehandtekeningen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **UPDATE**.
3. Selecteer naast **Update procesregels Herinneren voor het downloaden** in het vervolgkeuzemenu.

4. Ga terug naar het hoofdvenster en klik op de **Update** actieknop van de Bitdefender-interface.
5. Selecteer alleen **Updates handtekeningen** en klik vervolgens op **OK**.
6. Bitdefender zal alleen de updates van de malwarehandtekeningen downloaden en installeren.

23.7. De Bitdefender-services reageren niet

Dit artikel helpt u bij het oplossen van de foutmelding **Bitdefender-services reageren niet**. U kunt deze fout aantreffen als volgt:

- Het Bitdefender-pictogram in het systeemvak wordt grijs weergegeven en u krijgt een melding dat de Bitdefender-services niet reageren.
- Het Bitdefender-venster geeft aan dat de Bitdefender-services niet reageren.

De fout kan worden veroorzaakt door een van de volgende omstandigheden:

- tijdelijke communicatiefouten tussen de Bitdefender-services.
- sommige Bitdefender-services zijn gestopt.
- andere beveiligingsoplossingen worden op hetzelfde ogenblik als Bitdefender uitgevoerd.

Probeer de volgende oplossingen om deze fouten op te lossen:

1. Wacht enkele ogenblikken en kijk of er iets verandert. De fout kan tijdelijk zijn.
2. Start de computer opnieuw op en wacht enkele ogenblikken tot Bitdefender is geladen. Open Bitdefender om te zien of de fout blijft bestaan. Het probleem wordt doorgaans opgelost door de computer opnieuw op te starten.
3. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van Bitdefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens Bitdefender opnieuw te installeren.

   Meer informatie vindt u onder "*Andere beveiligingsoplossingen verwijderen*" (p. 73).

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel "*Hulp vragen*" (p. 169).

23.8. De Autofill-functie in mijn Portefeuille werkt niet

U hebt uw online gegevens opgeslagen in uw Bitdefender-Wachtwoordmanager en u hebt opgemerkt dat autofill niet werkt. Meestal doet dit probleem zich voor wanneer de Bitdefender-Portefeuille-extensie niet is geïnstalleerd in uw browser.

Om deze situatie op te lossen, volgt u deze stappen:

- In **Internet Explorer:**
  1. Open Internet Explorer.
  2. Klik op Extra.
  3. Klik op Invoegtoepassingen beheren.
  4. Klik op Werkbalken en Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.
- In **Mozilla Firefox:**
  1. Open Mozilla Firefox.
  2. Klik op Extra.
  3. Klik op Add-ons.
  4. Klik op Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.
- In **Google Chrome:**
  1. Open Google Chrome.
  2. Ga naar het Menu-pictogram.
  3. Klik op Instellingen.
  4. Klik op Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.

Opmerking
De add-on zal worden ingeschakeld nadat u uw webbrowser opnieuw hebt opgestart.

Controleer nu of de autofill-functie in Portefeuille werkt voor uw online accounts.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

23.9. Het verwijderen van Bitdefender is mislukt

Indien u uw Bitdefender-product wilt verwijderen en u merkt dat het proces blijft hangen of het systeem bevriest, klik dan op **Annuleren** om de handeling af te breken. Start het systeem opnieuw op als dit niet werkt.

Als het verwijderen mislukt, kunnen er enkele registersleutels en bestanden van Bitdefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van Bitdefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden.

Om Bitdefender helemaal van uw systeem te verwijderen:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
     - Bestanden in quarantaine
     - Wallets
  4. Klik op **VERDERGAAN**.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

4. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
   - Bestanden in quarantaine
   - Wallets
5. Klik op **VERDERGAAN**.
6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:
  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
     - Bestanden in quarantaine
     - Wallets
  6. Klik op **VERDERGAAN**.
  7. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

23.10. Mijn systeem start niet op na het installeren van Bitdefender

Als u Bitdefender net hebt geïnstalleerd en het systeem niet langer opnieuw kunt opstarten in de normale modus, kunnen er verschillende redenen zijn voor dit probleem.

Dit wordt zee waarschijnlijk veroorzaakt door een eerdere installatie van Bitdefender die niet goed werd verwijderd of door een andere beveiligingsoplossing die nog steeds op het systeem aanwezig is.

U kunt elke situatie op de volgende manier aanpakken:

- **U had eerder een versie van Bitdefender en hebt deze niet correct verwijderd.**

  Om dit probleem op te lossen:

  1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 75) voor meer informatie hierover.
  2. Bitdefender verwijderen van uw systeem:
     - In **Windows 7**:
       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
       b. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
       c. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
          - Bestanden in quarantaine
          - Wallets
       d. Klik op **VERDERGAAN**.
       e. Wacht tot de de-installatieproces is voltooid.
       f. Start uw systeem opnieuw op in normale modus.
     - In **Windows 8 en Windows 8.1**:
       a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
       b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
       c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.
       d. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:
          - Bestanden in quarantaine
          - Wallets
       e. Klik op **VERDERGAAN**.

f. Wacht tot de de-installatieproces is voltooid.

g. Start uw systeem opnieuw op in normale modus.

- In **Windows 10**:

a. Klik op **Start**, klik dan op Instellingen.

b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.

c. **Bitdefender Antivirus Plus 2017** vinden en **De-installeren** selecteren.

d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

e. Klik op **VERWIJDEREN** in het venster dat verschijnt en kies welke gegevens moeten bewaard worden voor een latere installatie:

- Bestanden in quarantaine
- Wallets

f. Klik op **VERDERGAAN**.

g. Wacht tot de de-installatieproces is voltooid.

h. Start uw systeem opnieuw op in normale modus.

3. Uw Bitdefender reïnstalleren.

- **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**

Om dit probleem op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 75) voor meer informatie hierover.
2. Verwijder de andere beveiligingsoplossing van uw systeem:

- In **Windows 7**:

a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.

b. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

c. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8 en Windows 8.1**:
  a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:
  a. Klik op **Start**, klik dan op Instellingen.
  b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Om andere software correct te verwijderen, gaat u naar de betreffende website en voert u het hulpprogramma voor het verwijderen uit of neemt u contact op met ons voor de richtlijnen voor het verwijderen.

3. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

U hebt de bovenstaande stappen al gevolgd en de situatie is niet opgelost.

Om dit probleem op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 75) voor meer informatie hierover.
2. Gebruik de optie Systeemherstel van Windows om de computer te herstellen naar een eerdere datum voordat u het product Bitdefender installeert.
3. Start het systeem opnieuw op in de normale modus en neem contact op met onze experts voor hulp, zoals beschreven in deel "*Hulp vragen*" (p. 169).

24. MALWARE VAN UW SYSTEEM VERWIJDEREN

Malware kan uw systeem op heel wat verschillende manieren beïnvloeden en de benadering van Bitdefender is afhankelijk van het type malware-aanval. Omdat virussen vaak hun gedrag veranderen, is het moeilijk een patroon vast te stellen voor hun gedrag en hun acties.

Er zijn situaties wanneer Bitdefender de malwareinfectie niet automatisch kan verwijderen van uw systeem. In dergelijke gevallen is uw tussenkomst vereist.

- "*Helpmodus Bitdefender*" (p. 159)
- "*Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt?*" (p. 162)
- "*Een virus in een archief opruimen*" (p. 163)
- "*Een virus in een e-mailarchief opruimen*" (p. 165)
- "*Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?*" (p. 166)
- "*Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?*" (p. 166)
- "*Wat zijn de overgeslagen items in het scanlogboek?*" (p. 167)
- "*Wat zijn de overgecomprimeerde bestanden in het scanlogboek?*" (p. 167)
- "*Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?*" (p. 167)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Hulp vragen*" (p. 169).

24.1. Helpmodus Bitdefender

Helpmodus is een Bitdefender-functie waarmee u alle bestaande harde schijfpartities buiten uw besturingssysteem kunt scannen en desinfecteren.

Zodra Bitdefender Antivirus Plus 2017 geïnstalleerd en het Bitdefender Rescue Image-bestand gedownload is, kan Rescue Mode gebruikt worden, zelfs als u niet langer in Windows kunt opstarten.

Bezig met downloaden van Bitdefender Rescue Image

Om de Rescue-modus te kunnen gebruiken, moet u het beeldbestand eerst downloaden, als volgt:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS** module selecteert u **Helpmodus**.
4. Klik op **JA** in het bevestigingsvenster dat verschijnt om uw computer opnieuw op te starten

   Wacht tot het Bitdefender Rescue Image-bestand werd gedownload van de Bitdefender-servers. Zodra het downloadproces beëindigd is, zal de computer opnieuw opstarten.

   Er verschijnt een menu waarin u wordt gevraagd een besturingssysteem te selecteren. Bij deze stap kunt u ervoor kiezen uw systeem op te starten in Rescue-modus of in normale modus.

Uw systeem starten in de Helpmodus

U kunt de Helpmodus op één of twee manieren openen:

Vanuit de Bitdefender-interface

Om rechtstreeks via Bitdefender naar Helpmodus te gaan:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **MODULES BEKIJKEN**.
3. In de **ANTIVIRUS** module selecteert u **Helpmodus**.
4. Klik op **JA** in het bevestigingsvenster dat verschijnt om uw computer opnieuw op te starten
5. Nadat de computer opnieuw is opgestart, verschijnt een menu waarin u wordt gevraagd een besturingssysteem te selecteren. Kies **Bitdefender Helpmodus** om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
6. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt. Druk vervolgens opnieuw op **Enter**.

Bitdefender-Helpmodus wordt binnen enkele ogenblikken geladen.

Start uw computer direct op in de Helpmodus

Als Windows niet langer start, kunt u met de onderstaande stappen uw computer direct opstarten in de Helpmodus van Bitdefender:

1. Start / herstart uw computer en druk op uw toetsenbord op de **spatiebalk** voordat het Windows-logo verschijnt.
2. Er verschijnt een menu waarin u wordt gevraagd een besturingssysteem voor het opstarten te selecteren. Druk op **TAB** om naar het gebied Tools. Kies **Bitdefender Rescue Image** en druk op de **Enter**-toets om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
3. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt. Druk vervolgens opnieuw op **Enter**.

   Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.

Uw systeem scannen in de Helpmodus

Uw systeem scannen in de Helpmodus:

1. Open de Helpmodus zoals beschreven in “Uw systeem starten in de Helpmodus” (p. 160).
2. Het Bitdefender-logo verschijnt en het kopiëren van de antivirus-engines wordt gestart.
3. Een welkomstvenster wordt weergegeven. Klik op **Doorgaan**.
4. Er is een update van de antivirushandtekeningen gestart.
5. Nadat de update is voltooid, verschijnt het venster van de antivirusscanner van Bitdefender voor scannen op aanvraag.
6. Klik op **Nu scannen**, selecteer het scandoel in het venster dat verschijnt en klik daarna op **Openen** om het scannen te starten.

   Het is aanbevolen de volledige Windows-partitie te scannen.

> **Opmerking**
> Wanneer u in de Helpmodus werkt, krijgt u te maken met partitienamen van het Linux-type. Schijfpartities zullen verschijnen als `sda1` die

waarschijnlijk overeenstemmen met het station (C:) Partitie van het Windows-type, sda2 overeenkomend met (D:) enz.

7. Wacht tot de scan is voltooid. Volg de instructies als er malware is gedetecteerd, om de bedreiging te verwijderen.
8. Om de Helpmodus af te sluiten, klikt u met de rechtermuisknop in een leeg gebied op het bureaublad. Selecteer vervolgens **Verlaten** in het menu dat verschijnt en kies vervolgens of u de computer opnieuw wilt opstarten of uitschakelen.

24.2. Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt?

U kunt op een van de volgende manieren controleren of er een virus op uw computer aanwezig is:

- U hebt uw computer gescand en Bitdefender heeft geïnfecteerde items gevonden.
- Een viruswaarschuwing laat u weten dat Bitdefender een of meerdere virussen op uw computer heeft geblokkeerd.

Voer in dergelijke gevallen een update uit van Bitdefender om zeker te zijn dat u over de laatste malwarehandtekeningen beschikt en voer een systeemscan uit om het systeem te analyseren.

Selecteer de gewenste actie (desinfecteren, verwijderen, naar quarantaine verplaatsen) voor de geïnfecteerde items zodra de systeemscan is voltooid.

Waarschuwing
Als u vermoedt dat het bestand deel uitmaakt van het Windows-besturingssysteem of dat het geen geïnfecteerd bestand is, volgt u deze stappen niet en neemt u zo snel mogelijk contact op met de klantendienst van Bitdefender.

Als de geselecteerde actie niet kan worden ondernemen en het scanlogboek een infectie meldt die niet kan worden verwijderd, moet u de bestanden handmatig verwijderen.

De eerste methode kan worden gebruikt in de normale modus:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.

a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.

b. Selecteer de koppeling **MODULES BEKIJKEN**.

c. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.

d. Klik op de bijhorende schakelaar om **Scannen bij toegang** uit te schakelen.

2. Verborgen objecten weergeven in Windows. Raadpleeg "*Verborgen objecten weergeven in Windows*" (p. 72) voor meer informatie hierover.
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real time antivirusbeveiliging van Bitdefender in.

Indien de eerste methode niet werkte om de infectie te verwijderen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 75) voor meer informatie hierover.
2. Verborgen objecten weergeven in Windows. Raadpleeg "*Verborgen objecten weergeven in Windows*" (p. 72) voor meer informatie hierover.
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Start uw systeem opnieuw op en ga naar de normale modus.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

24.3. Een virus in een archief opruimen

Een archief is een bestand of een verzameling van bestanden dat is gecomprimeerd onder een speciale indeling om de benodigde schijfruimte voor het opslaan van de bestanden te beperken.

Sommige van deze formaten zijn open formaten. Hierdoor kan Bitdefender binnen deze formaten scannen en de geschikte acties ondernemen om ze te verwijderen.

Andere archiefformaten worden gedeeltelijk of volledig gesloten. Bitdefender kan alleen de aanwezigheid van virussen detecteren, maar kan geen andere acties ondernemen.

Als Bitdefender u meldt dat er een virus is gedetecteerd binnen een archief en er geen actie beschikbaar is, betekent dit dat het niet mogelijk is het virus te verwijderen vanwege beperkingen op de machtigingsinstellingen voor het archief.

Een virus dat in een archief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Identificeer het archief dat het virus bevat door een systeemscan uit te voeren.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Selecteer de koppeling **MODULES BEKIJKEN**.
   c. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
   d. In het venster **SCHILD** klikt u op de bijhorende schakelaar om **On-access scanning** uit te schakelen.
3. Ga naar de locatie van het archief en decomprimeer het met een archiveringstoepassing, zoals WinZip.
4. Identificeer het geïnfecteerde bestand en verwijder het.
5. Verwijder het originele archief zodat u zeker bent dat de infectie volledig is verwijderd.
6. Comprimeer de bestanden in een nieuw archief met een archiveringstoepassing zoals WinZip.
7. Schakel de realtime antivirusbescherming van Bitdefender in en voer een Systeemscan uit om zeker te zijn dat er geen andere infecties op het systeem aanwezig zijn.

Opmerking
Het is belangrijk dat u weet dat een virus dat is opgeslagen in een archief, geen onmiddellijke bedreiging is voor uw systeem, omdat het virus moet worden gedecomprimeerd en uitgevoerd om uw systeem te kunnen infecteren.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

24.4. Een virus in een e-mailarchief opruimen

Bitdefender kan ook virussen identificeren in e-maildatabases en e-mailarchieven die op de schijf zijn opgeslagen.

Het is soms nodig het geïnfecteerde bestand te identificeren met de informatie die is opgegeven in het scanrapport en het handmatig te verwijderen.

Een virus dat in een e-mailarchief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Scan de e-maildatabase met Bitdefender.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Selecteer de koppeling **MODULES BEKIJKEN**.
   c. Selecteer de icoon in de rechterbovenhoek van de **ANTIVIRUS**-module.
   d. Klik op de bijhorende schakelaar om **Scannen bij toegang** uit te schakelen.
3. Open het scanrapport en gebruik de identificatiegegevens (Onderwerp, Van, Aan) van de geïnfecteerde berichten om ze te zoeken in de e-mailclient.
4. De geïnfecteerde bestanden verwijderen. De meeste e-mailclients verplaatsen het verwijderde bericht ook naar een herstelmap van waar het kan worden hersteld. U moet controleren of dit bericht ook uit deze herstelmap is verwijderd.
5. Comprimeer de map die het geïnfecteerde bericht bevat.
   - In Microsoft Outlook 2007: Klik in het menu Bestand op Gegevensbestandsbeheer. Selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen. Klik nu op Compact.
   - In Microsoft Outlook 2010 / 2013: In het Bestandsmenu klikt u op Info en dan op Accountinstellingen (Accounts toevoegen en verwijderen of bestaande login-instellingen wijzigen). Klik dan op Gegevensbestand, selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen. Klik nu op Compact.

6. Schakel de real time antivirusbeveiliging van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 169).

24.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?

U kunt vermoeden dat een bestand in uw systeem gevaarlijk is, ondanks het feit dat uw Bitdefender-product het niet heeft gedetecteerd.

Om ervoor te zorgen dat uw systeem beschermd is:

1. Voer een **Systeemscan** uit met Bitdefender. Raadpleeg "*Hoe kan ik mijn systeem scannen?*" (p. 62) voor meer informatie hierover.
2. Als het scanresultaat schoon lijkt, maar u nog steeds twijfels hebt en wilt zeker zijn over het bestand, moet u contact opnemen met onze experts zodat wij u kunnen helpen.

   Raadpleeg "*Hulp vragen*" (p. 169) voor meer informatie hierover.

24.6. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?

Dit is slechts een melding die aangeeft dat Bitdefender heeft gedetecteerd dat deze bestanden ofwel door een wachtwoord ofwel door een vorm van codering zijn beveiligd.

De meest gebruikelijke items die door een wachtwoord zijn beveiligd, zijn:

- Bestanden die bij een andere beveiligingsoplossing horen.
- Bestanden die bij het besturingssysteem horen.

Om de inhoud ook daadwerkelijk te scannen, moeten deze bestanden zijn opgehaald of op een andere manier zijn gedecodeerd.

Als deze inhoud zou worden uitgepakt, zou de real time scanner van Bitdefender ze automatisch scannen om uw computer beschermd te houden. Als u die bestanden wilt scannen met Bitdefender, moet u contact opnemen met de productfabrikant voor meer informatie over die bestanden.

Wij raden u aan deze bestanden te negeren omdat ze geen bedreiging vormen voor uw systeem.

24.7. Wat zijn de overgeslagen items in het scanlogboek?

Alle bestanden die in het scanrapport als Overgeslagen worden weergegeven, zijn zuiver.

Voor betere prestaties scant Bitdefender geen bestanden die niet werden gewijzigd sinds de laatste scan.

24.8. Wat zijn de overgecomprimeerde bestanden in het scanlogboek?

Overgecomprimeerde items zijn elementen die niet kunnen worden opgehaald door de scanengine of elementen waarvoor de decoderingstijd te lang zou zijn waardoor het systeem onstabiel zou kunnen worden.

Overgecomprimeerd betekent dat het Bitdefender het scannen binnen dat archief heeft overgeslagen omdat het uitpakken ervan teveel systeemgeheugen zou in beslag nemen. De inhoud zal bij real time toegang worden gescand indien dat nodig is.

24.9. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?

Als er een geïnfecteerd bestand wordt gedetecteerd, zal Bitdefender automatisch proberen dit te desinfecteren. Als de desinfectie mislukt, wordt het bestand naar quarantaine verplaatst om de infectie in te dammen.

Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

Dit is doorgaans het geval met installatiebestanden die zijn gedownload vanaf onbetrouwbare websites. Als u zelf in een dergelijke situatie terechtkomt, downloadt u het installatiebestand vanaf de website van de fabrikant of een andere vertrouwde website.

CONTACT OPNEMEN MET ONS

25. HULP VRAGEN

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

De "*Algemene problemen oplossen*" (p. 144) sectie biedt de nodige informatie betreffende de vaakst voorkomende problemen tijdens het gebruik van dit product.

Als u geen oplossing voor uw vraag in de geleverde middelen hebt gevonden, kunt u direct contact met ons opnemen:

- "Neem direct met ons contact op vanaf uw Bitdefender-product" (p. 169)
- "Neem contact op met ons via ons online Ondersteuningscentrum" (p. 170)

Neem direct met ons contact op vanaf uw Bitdefender-product

Als u een actieve internetverbinding hebt, kunt u direct vanaf de productinterface contact opnemen met Bitdefender voor hulp.

Volg deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. U hebt de volgende opties:
   - **Productdocumentatie**

     Ga naar onze database en zoek de benodigde informatie.
   - **Contact Ondersteuning**

     Gebruik de knop **Contact opnemen met ondersteuning** om het Bitdefender ondersteuningshulpprogramma te starten en contact op te nemen met de klantendienst. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

     a. Schakel het selectievakje voor de overeenkomst en klik op **Volgende**.

b. Vul het verzendformulier in met de nodige gegevens:

i. Voer uw e-mailadres in.

ii. Voer uw volledige naam in.

iii. Voer een beschrijving in van het probleem dat zich heeft voorgedaan.

iv. Controleer de optie **Probeer het probleem opnieuw voort te brengen alvorens het door te geven** voor het geval u een productprobleem ondervindt. Doorgaan met de vereiste stappen.

c. Wacht enkele minuten terwijl Bitdefender met het product verwante informatie verzamelt. Deze informatie zal onze technici helpen een oplossing voor uw probleem te vinden.

d. Klik op **Voltooien** om de informatie te verzenden naar de klantendienst van Bitdefender. Wij nemen zo snel mogelijk contact op met u.

- **Online help vinden**

  Uw online artikelen bekijken.

Neem contact op met ons via ons online Ondersteuningscentrum

Als u de benodigde informatie niet kunt openen met het Bitdefender-product, kunt u ons online ondersteuningscentrum raadplegen:

1. Ga naar https://www.bitdefender.com/support/consumer.html.

   Het Ondersteuningscentrum van Bitdefender bevat talrijke artikelen met oplossingen voor problemen met betrekking tot Bitdefender.

2. Gebruik de zoekbalk bovenaan het venster om artikelen te vinden die een oplossing voor uw probleem bieden. Vul om te zoeken een term in de zoekbalk in en klik op **Zoeken**.

3. Lees de relevante artikelen of documenten door en pas de voorgestelde oplossingen toe.

4. Als uw probleem hiermee niet is opgelost, gaat u naar

   https://www.bitdefender.com/support/contact-us.htmlen neemt u contact op met onze experts van de ondersteuning.

25.1. Telefonische ondersteuning:

De laboratoria van Bitdefender stellen alles in het werk om de toegang tot telefonische ondersteuning te kunnen garanderen, tijdens plaatselijke werkuren van maandag tot en met vrijdag, met uitzondering van feestdagen.

Telefonische toegang tot de laboratoria van Bitdefender:

- **Belgium**: 070 35 83 04
- **Netherlands**: 020 788 61 50

Zorg voordat u ons belt dat u de volgende zaken binnen handbereik hebt:

- het licentienummer van uw Bitdefender programma. Geef dit nummer door aan een van onze technici zodat hij kan nagaan op welk type ondersteuning u recht hebt.
- de actuele versie van uw besturingssysteem.
- informatie met betrekking tot de merken en modellen van alle op uw computer aangesloten randapparaten en van de software die in het geheugen is geladen of in gebruik is.

In het geval er een virus is ontdekt, kan de technicus u vragen om een lijst met technische informatie en bepaalde bestanden door te sturen, die mogelijkerwijs nodig zijn voor het stellen van een diagnose.

Indien een technicus u om foutmeldingen vraagt, geef dan de exacte inhoud door en het moment waarop de meldingen verschenen, de activiteiten die eraan voorafgingen en de stappen die u zelf reeds hebt ondernomen om het probleem op te lossen.

De technicus zal een strikte procedure opvolgen in een poging het probleem op te sporen.

De volgende elementen vallen niet binnen de service:

- Deze technische ondersteuning heeft geen betrekking op de toepassingen, installaties, de deïnstallatie, de overdracht, preventief onderhoud, de vorming, het beheer op afstand of andere softwareconfiguraties dan diegene die tijdens de interventie specifiek door onze technicus werden vermeld.
- De installatie, de instellingen, de optimalisering en de netwerkconfiguratie of de configuratie op afstand van toepassingen die niet binnen het kader van de geldende ondersteuning vallen.

- Back-ups van software/gegevens. De klant dient zelf een back-up te maken van alle gegevens, software en bestaande programma's die aanwezig zijn op de informatiesystemen waarop onze ondersteuning van toepassing is, alvorens enige dienstprestatie te laten uitvoeren door Bitdefender.

Bitdefender KUNNEN IN GEEN GEVAL AANSPRAKELIJK WORDEN GESTELD VOOR HET VERLIES OF DE RECUPERATIE VAN GEGEVENS, PROGRAMMA'S, OF VOOR HET NIET KUNNEN BENUTTEN VAN SYSTEMEN OF VAN HET NETWERK.

Adviezen beperken zich enkel tot de gestelde vragen en zijn gebaseerd op de door de klant verschafte informatie. De problemen en mogelijke oplossingen kunnen afhangen van het type systeemomgeving en van een groot aantal andere variabelen waarvan Bitdefender niet op de hoogte zijn.

Bitdefender kunnen dan ook in geen geval aansprakelijk worden gesteld voor eventuele schade die voortvloeit uit het gebruik van de verschafte informatie.

Het kan zijn dat het systeem waarop de Bitdefender programma's moeten worden geïnstalleerd onstabiel is (eerdere virusinfecties, installatie van meerdere antivirus - of beveiligingsprogramma's, etc.). In betreffende gevallen zal een technicus u mogelijkerwijze voorstellen eerst een onderhoudsbeurt op uw systeem te laten uitvoeren, alvorens het probleem kan worden opgelost.

De technische gegevens kunnen wijzigen op het moment dat er nieuwe gegevens beschikbaar zijn. Om die reden raden Bitdefender u dan ook aan regelmatig onze site "Producten" te raadplegen, via https://www.bitdefender.nl voor upgrades, of onze site met veelgestelde vragen (FAQ) op https://www.bitdefender.nl/support/consumer/.

Bitdefender wijzen elke aansprakelijkheid af voor enige rechtstreekse, onrechtstreekse, bijzondere of accidentele schade, of voor gevolgschade die te wijten is aan het gebruik van de aan u verschafte informatie.

Indien een interventie ter plaatse noodzakelijk is, zal de technicus u meer gedetailleerde informatie verschaffen met betrekking tot de dichtstbijzijnde wederverkoper.

26. ONLINE BRONNEN

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

- Bitdefender-ondersteuningscentrum:

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

- Bitdefender-ondersteuningsforum:

  https://forum.bitdefender.com

- Het HOTforSecurity-portaal over computerbeveiliging:

  https://www.hotforsecurity.com

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

26.1. Bitdefender-ondersteuningscentrum

Het Bitdefender-ondersteuningscentrum is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over viruspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

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

Het Bitdefender-ondersteuningscentrum is op elk ogenblik beschikbaar op

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

26.2. Bitdefender-ondersteuningsforum

Het Bitdefender-ondersteuningsforum biedt Bitdefender-gebruikers een eenvoudige manier om hulp te krijgen en anderen te helpen.

Als uw Bitdefender-product niet goed werkt, als het specifieke virussen niet van uw computer kan verwijderen of als u vragen hebt over de manier waarop het werkt, kunt u uw probleem of vraag op het forum plaatsen.

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

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

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

26.3. HOTforSecurity-portaal

HOTforSecurity is een rijke bron aan informatie over computerbeveiliging. Hier leert u meer over de verschillende bedreigingen waaraan uw computer wordt blootgesteld wanneer u een verbinding met Internet maakt (malware, phishing, spam, cybercriminelen).

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

De webpagina van HOTforSecurity is te bereiken via https://www.hotforsecurity.com.

27. CONTACTINFORMATIE

Efficiënte communicatie is de sleutel naar het succes. Gedurende de laatste 16 jaar heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners steeds opnieuw te overtreffen. Aarzel niet contact op te nemen met ons als u eventuele vragen hebt.

27.1. Webadressen

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

27.2. Lokale verdelers

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

Een Bitdefender-verdeler in uw land zoeken:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.
3. Als u geen Bitdefender-verdeler in uw lang vindt, kunt u met ons contact opnemen via e-mail op sales@bitdefender.com. Schrijf uw e-mail in het Engels, zodat wij u snel kunnen helpen.

27.3. Bitdefender-kantoren

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

Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

France

Bitdefender SAS
49, Rue de la Vanne
92120 Montrouge
Telefoon: +33 (0)1 47 35 72 73
Verkoop: sales@bitdefender.fr
Technische ondersteuning: https://www.bitdefender.fr/support/nous-contacter.html
Web: https://www.bitdefender.fr

Verenigde Staten

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

Duitsland

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

Spanje

Bitdefender España, S.L.U.

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

Roemenië

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefoon verkoop: +40 21 2063470
E-mail verkoop: sales@bitdefender.ro
Technische ondersteuning: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Verenigde Arabische Emiraten

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

Woordenlijst

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.

Achterdeur

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 verkopers.

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.

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.

Archief

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.

Bestandsnaamextensie

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.

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.

Cookie

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.

Downloaden

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.

Geavanceerde aanhoudende dreiging

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 malware.

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 het virus 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.

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.

Geheugengebruik

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.

Heuristisch

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

Honingpot

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.

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 zou echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval zouden de tien spaties slechts

twee bytes nodig hebben. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

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 bijvoorbeeld op de client worden uitgevoerd, kunnen ze 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 programma dat alles vastlegt wat u typt.

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).

Macrovirus

Een type computervirus dat 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.

Mailclient

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

malware

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

Niet-heuristisch

Deze scanmethode steunt op specifieke virushandtekeningen. Het voordeel van de niet-heuristische scan is dat hij zich niet laat misleiden door iets dat kan lijken op een virus en dat hij geen vals alarm genereert.

Opdrachtregel

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

Opstartgebied:

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

Opstartitems

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 een toepassingsprogramma. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Opstartsectorvirus

Een virus dat 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 het virus actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal het virus telkens in het geheugen geactiveerd zijn.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische archiveringssysteem vanaf het begin.

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.

Photon

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van antivirusbescherming 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 virus dat zijn vorm wijzigt bij elk bestand dat hij infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kunt aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende

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

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

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

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

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met malware,

vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

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).

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 dit geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

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

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.

Trojaans paard

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

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

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 updatemodule waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Vals positief

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

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.

Virushandtekening

Het binaire patroon van een virus, dat wordt gebruikt door het antivirusprogramma om het virus te detecteren en uit te schakelen.

Worm

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