Bitdefender ANTIVIRUS PLUS

HANDLEIDING

Bitdefender Antivirus Plus

Handleiding

Publicatiedatum 04/12/2023

Juridische kennisgeving

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Voor wie is deze handleiding bedoeld?

Deze handleiding is bedoeld voor alle Windows-gebruikers die Bitdefender Antivirus Plusvoor hebben gekozen als een beveiligingsoplossing voor hun computers. De informatie die in dit boek wordt geleverd is niet alleen geschikt voor geavanceerde computergebruikers, maar is ook gemakkelijk te begrijpen door iedereen die met een Windows-pc kan werken.

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

Wij wensen u veel aangenaam en nuttig leesplezier.

Hoe deze handleiding te gebruiken

Deze gids is opgebouwd rond een aantal belangrijke onderwerpen:

Aan de slag (pagina 13)

Ga aan de slag met Bitdefender Antivirus Plus en zijn gebruikersinterface.

Uw beveiliging beheren (pagina 46)

Leer hoe u Bitdefender Antivirus Plus kunt gebruiken om uzelf te beschermen tegen kwaadaardige software.

Zo werkt het (pagina 103)

Meer informatie over Bitdefender Antivirus Plus.

Hulp vragen (pagina 151)

Waar te zoeken en waar te vragen om hulp als er iets onverwachts gebeurt.

Conventies die in deze gids worden gebruikt

Typografische conventies

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

Weergave	Beschrijving
`voorbeeld-syntaxis`	Voorbeelden van syntaxis worden weergegeven in een `niet-proportioneel lettertype`.
https://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Over deze gids (pagina 1)	Dit is een interne koppeling naar een locatie in het document.
`bestandsnaam`	Namen van bestanden en mappen worden weergegeven in een `niet-proportioneel lettertype`.
optie	Alle productopties worden **vet** weergegeven.
trefwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

Waarschuwingen

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

Opmerking

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

Belangrijk

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

Waarschuwing

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

Verzoek om commentaar

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

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

1. INSTALLATIE

1.1. Voorbereiden voor installatie

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

- Controleer of de apparaat waarop u Bitdefenderwilt installeren, voldoet aan de minimale systeemvereisten. Als de apparaat niet aan alle systeemvereisten voldoet, wordt het Bitdefender niet geïnstalleerd, of als het toch geïnstalleerd wordt, zal het niet goed werken en zal het systeem vertragen en instabiel worden. Raadpleeg Systeemvereisten (pagina 3) voor een complete lijst van systeemvereisten.
- Meld u aan bij de apparaat met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de apparaat. 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.
- Schakel alle firewall-programma's die mogelijk op uw apparaat worden uitgevoerd uit of verwijder ze. Als u twee firewallprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Firewall zal uitgeschakeld zijn tijdens de installatie.
- Het wordt aanbevolen uw apparaat 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.

1.2. Systeemvereisten

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

- Windows 7 met Service Pack 1

- Windows 8
- Windows 8.1
- Windows 10
- 2,5 GB beschikbare vrije ruimte op de harde schijf (ten minste 800 MB op de systeemschijf)
- 2 GB geheugen (RAM)

Belangrijk
Systeemprestaties kunnen worden beïnvloed voor apparaten die CPU's van een oudere generatie hebben.

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

- Klik in **Windows 7**, met de rechtermuisknop op **Mijn Computer** op het bureaublad, en selecteer dan **Eigenschappen** uit 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. In **Windows 8.1**, zoek **Deze pc**.
  Selecteer **Eigenschappen** in het onderste menu. Zoek in **Systeem** naar informatie over uw systeemtype.
- Typ in **Windows 10 Systeem** in het zoekvak op de taakbalk en klik op het pictogram ervan. Kijk in het **Systeem** gebied om informatie te vinden over uw systeemtype.

1.3. Softwarevereisten

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

- Microsoft Edge 40 en hoger
- Internet Explorer 10 en hoger
- Mozilla Firefox 51 en hoger
- Google Chrome 34 en hoger
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 en hoger

1.4. Uw Bitdefender-product installeren

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

Indien uw aankoop van toepassing is op meer dan één apparaat, herhaalt u het installatieproces en activeert u uw product op elke apparaat met dezelfde account. De account die u moet gebruiken, is deze die uw actieve abonnement van Bitdefender bevat.

1.4.1. Installeer 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 geactiveerd.

Om Bitdefender Antivirus Plus te downloaden van Bitdefender Central:

1. Ga naar **Bitdefender Central**.
2. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:
   - **Dit apparaat beschermen**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Sla het installatiebestand op.
   - **Bescherm andere apparaten**
     a. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
     b. Klik op **DOWNLOADKOPPELING VERZENDEN**.
     c. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**.
     De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

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

4. 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 minimale systeemvereisten 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-compatibele beveiligingsoplossing 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 apparaat opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Het installatiepakket voor Bitdefender Total Security wordt voortdurend bijgewerkt.

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

Zodra de installatie gevalideerd is, verschijnt de installatiewizard. Volg de stappen om Bitdefender Antivirus Plus te installeren.

Step 1 - Bitdefender installatie

Voordat u verdergaat met de installatie, moet u akkoord gaan met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Antivirus Plus.

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

In deze stap kunnen twee bijkomende taken uitgevoerd worden:

- Zorg ervoor dat de optie **Productrapporten 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.

Klik op **INSTALLEREN** om het installatieproces van uw Bitdefender-product te starten.

Stap 2 - Installatieproces

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

Stap 3 - Installatie voltooid

Uw Bitdefender-product werd met succes geïnstalleerd.

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie een actieve bedreiging wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn.

Stap 4 - Apparaatanalyse

U wordt vervolgens gevraagd of u een analyse wilt uitvoeren van uw apparaat, om te verzekeren dat het veilig is. Tijdens deze stap zal Bitdefender kritieke systeemgebieden scannen. Klik op **Apparaatanalyse starten** om het te starten.

U kunt de scaninterface verbergen door te klikken op **Scan uitvoeren op de achtergrond**. Daarna kiest u of u op de hoogte wilt worden gebracht wanneer de scan is voltooid, of niet.

Wanneer de scan voltooid is, klikt u op **Bitdefender-interface openen**.

> **Opmerking**
> Indien u de scan niet wilt laten uitvoeren, klikt u gewoon op **Overslaan**.

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-interface te gaan.

1.4.2. 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 minimale systeemvereisten 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-compatibele beveiligingsoplossing 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 apparaat opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Het installatiepakket voor Bitdefender Total Security wordt voortdurend bijgewerkt.

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

Zodra de installatie gevalideerd is, verschijnt de installatiewizard. Volg de stappen om Bitdefender Antivirus Plus te installeren.

Stap 1 - Bitdefender Installatie

Voordat u doorgaat met de installatie, moet u akkoord gaan met de abonnementsovereenkomst. Neem even de tijd om de abonnementsovereenkomst te lezen, aangezien deze de algemene voorwaarden bevat waaronder u mag gebruiken Bitdefender Antivirus Plus.

Als u niet akkoord gaat met deze voorwaarden, sluit u het venster. Het installatieproces wordt afgebroken en u verlaat de installatie.

Bij deze stap kunnen twee extra taken worden uitgevoerd:

- Houd de **Stuur productrapporten** optie ingeschakeld. Door deze optie toe te staan, worden rapporten met informatie over hoe u het product gebruikt naar de Bitdefender-servers verzonden. Deze informatie is essentieel voor het verbeteren van het product en kan ons helpen om in de toekomst een betere ervaring te bieden. Merk op dat deze rapporten geen vertrouwelijke gegevens bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen worden gebruikt.
- Selecteer de taal waarin u het product wilt installeren.

Klik **INSTALLEREN** om het installatieproces van uw Bitdefender-product te starten.

Stap 2 - Installatie bezig

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

Stap 3 - Installatie voltooid

Er wordt een samenvatting van de installatie weergegeven. Als er tijdens de installatie een actieve dreiging is gedetecteerd en verwijderd, kan het nodig zijn het systeem opnieuw op te starten.

Stap 4 - Apparaatanalyse

U wordt nu gevraagd of u een analyse van uw apparaat wilt uitvoeren om er zeker van te zijn dat het veilig is. Tijdens deze stap scant Bitdefender kritieke systeemgebieden. Klik **Start apparaatanalyse** om het te initiëren.

U kunt de scaninterface verbergen door op te klikken **Scan op de achtergrond uitvoeren**. Kies daarna of u op de hoogte wilt worden gehouden wanneer de scan is voltooid of niet.

Wanneer de scan voltooid is, klikt u op **Verdergaan met account maken**.

> **Opmerking**
> Als u de scan niet wilt uitvoeren, kunt u ook gewoon op klikken **Overslaan**.

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. Zie Bitdefender Central (pagina 29) voor meer informatie.

Ga verder volgens uw situatie.

- **Ik wil een Bitdefender-account maken**

  1. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft, worden vertrouwelijk behandeld. Het wachtwoord moet minstens 8 tekens lang zijn, minstens één nummer of symbool en kleine letters en hoofdletters bevatten.
  2. Voordat u verdergaat, moet u de Gebruiksvoorwaarden aanvaarden. De Gebruiksvoorwaarden bevatten de voorwaarden waaronder u Bitdefender mag gebruiken; lees ze dus grondig door.
     U kunt eveneens het Privacybeleid lezen.
  3. Clik op **ACCOUNT MAKEN**.

     > **Opmerking**
     > Eens de account is aangemaakt, kunt u het gebruikte e-mailadres en wachtwoord gebruiken om in te loggen op uw account op https://central.bitdefender.com, of op de Bitdefender Central-app, indien de app geïnstalleerd is op een van uw Android- of iOS-apparaten. Ga naar Google Play, zoek Bitdefender Central op en tik op de installatie-optie om de Bitdefender Central-app voor Android te installeren. Ga naar de App Store, zoek Bitdefender Central op en tik op de installatie-optie om de Bitdefender Central-app voor iOS te installeren.

- **Ik heb al een Bitdefender-account**

  1. Klik op **Aanmelden**.

2. Voer het e-mailadres in het daarvoor bestemde veld en klik daarna op **VOLGENDE**.
3. Voer uw wachtwoord in en klik op **AANMELDEN**.
   Bent u het wachtwoord voor uw account kwijt of wilt u het gewoon opnieuw instellen:
   a. Klik op **Wachtwoord vergeten?**.
   b. Voer uw e-mailadres in en klik op **VOLGENDE**.
   c. Controleer uw e-mailaccount, voer de beveiligingscode in die u ontvangen hebt en klik op **VOLGENDE**.
      Of u kunt in de e-mail die we naar u gestuurd hebben, klikken op **Wachtwoord wijzigen**.
   d. Typ het nieuwe wachtwoord dat u wilt instellen, en typ het nogmaals. Klik op **OPSLAAN**.

   Opmerking
   Als u al een MyBitdefender-account hebt, kunt u deze gebruiken om u aan te melden bij uw Bitdefender-account. Als u uw wachtwoord bent vergeten, moet u eerst naar https://my.bitdefender.com gaan om het opnieuw in te stellen. Gebruik vervolgens de bijgewerkte inloggegevens 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 **DOORGAAN**.

     > **Opmerking**
     > U vindt uw activatiecode:
     >
     > - op het cd/dvd-label.
     > - op de productregistratiekaart.
     > - in de online aankoop e-mail.

  2. **Ik wil Bitdefender evalueren**
     In dat geval kunt u het product gedurende 30 dagen gebruiken. Om de proefperiode te beginnen, selecteert u **Ik heb geen abonnement, ik wil het product gratis uitproberen**, en klik dan op **DOORGAAN**.

Stap 7 - Aan de slag

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

Klik **FINISH** om toegang te krijgen tot de Bitdefender Antivirus Plus koppel.

2. AAN DE SLAG

2.1. De basisfuncties

Nadat u Bitdefender Antivirus Plus hebt geïnstalleerd, wordt uw apparaat beschermd tegen alle types bedreigingen (zoals malware, spyware, ransomware, exploits, botnets en Trojaanse paarden) en internetbedreigingen (zoals hackers, phishing en spam).

De toepassing gebruikt de Photontechnologie om de snelheid en prestaties van het scanproces van de bedreigingen 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.

Zonder bescherming verbinden met de publieke draadloze netwerken van luchthavens, winkelcentra, cafés of hotels kan gevaarlijk zijn voor uw apparaat en uw gegevens. Dit is voornamelijk omdat fraudeurs uw activiteit kunnen volgen en het beste moment kunnen uitkiezen om uw persoonlijke gegevens te stelen, maar ook omdat iedereen uw IP-adres kan zien, waardoor uw toestel het slachtoffer kan worden van toekomstige cyberaanvallen. Installeer en gebruik de VPN app om dergelijke betreurenswaardige situaties te vermijden.

Webcambeveiliging voorkomt dat onbetrouwbare toepassingen zich een toegang verschaffen tot uw videocamera om zo elke hackpoging te voorkomen. Op basis van de gebruikerskeuze van het Bitdefender zal de toegang van populaire toepassingen tot uw webcam toegestaan of geblokkeerd worden.

Om u te beschermen tegen potentiële nieuwsgierigen en spionnen wanneer uw apparaat verbonden is met een onbeveiligd netwerk, analyseert Bitdefender het beveiligingsniveau ervan en beveelt u indien nodig aan om de veiligheid van uw online activiteiten een boost te geven. Voor instructies over hoe u uw persoonlijke gegevens veilig kunt houden, verwijzen we naar Wi-Fi Security Advisor (pagina 75).

Bestanden die door ransomware worden versleuteld, kunnen nu worden hersteld zonder losgeld te moeten geven. Voor informatie over hoe u versleutelde bestanden kunt herstellen, raadpleeg Ransomware-remediëring (pagina 79).

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 (pagina 15).

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. Zie Notificaties (pagina 14) voor meer informatie.

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 apparaat en gegevens te beschermen.

Om de online functies van Bitdefender Antivirus Plus te gebruiken en uw abonnementen en toestellen te beheren, gaat u naar uw Bitdefender-account. Zie Bitdefender Central (pagina 29) voor meer informatie.

In de sectie Zo werkt het (pagina 103) vindt u stapsgewijze instructies voor het uitvoeren van veelvoorkomende taken. Als u problemen ondervindt tijdens het gebruik van Bitdefender, raadpleeg dan de sectie Algemene problemen oplossen (pagina 131) voor mogelijke oplossingen voor de meest voorkomende problemen.

2.1.1. Notificaties

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw apparaat. Wanneer er iets gebeurt dat van belang is voor de veiligheid van uw systeem of uw gegevens, wordt er een nieuw bericht toegevoegd aan Bitdefender Notifications, net zoals er nieuwe e-mails verschijnen in uw Postvak IN.

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

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

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

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

Klik op elke tab om meer details te lezen over de gegenereerde gebeurtenissen. Er wordt beperkte informatie weergegeven als u een keer op elke titel van een gebeurtenis klikt, namelijk: een korte beschrijving, de actie die Bitdefender heeft ondernomen wanneer ze zich voordeed en de datum en tijd van de gebeurtenis. Er kunnen opties worden geboden voor het ondernemen van verdere actie.

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

2.1.2. 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 lopende apps door tijdelijk de beveiligingsinstellingen 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.

Spelprofiel

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

Openbaar wifi-profiel

Past productinstellingen toe om te genieten van volledige bescherming, terwijl u verbonden bent met een onveilig draadloos netwerk.

Batterijmodusprofiel

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

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.

Wanneer u de **Profielen** voor het eerst opent, wordt u gevraagd om automatische profielen te activeren. Om dat te doen, klikt u gewoon op **INSCHAKELEN** in het weergegeven venster.

U kunt ook klikken op **NU NIET** indien u de voorziening op een later tijdstip wilt inschakelen.

Om Bitdefender toe te laten profielen automatisch te activeren:

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
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.

Schakel de overeenstemmende schakelaar in om een profiel manueel te activeren. Van de eerste drie profielen kan er slechts één tegelijkertijd handmatig worden geactiveerd.

Voor meer informatie over Profielen, ga naar profielen (pagina 94).

2.1.3. Wachtwoordbeveiligde Bitdefender-instellingen

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

Wachtwoordbescherming configureren voor de Bitdefender-instellingen:

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Instellingen**.
2. Schakel in het venster **Algemeen Wachtwoordbeveiliging** in.
3. 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 **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Schakel in het venster **Algemeen Wachtwoordbeveiliging** uit.
3. Voer het wachtwoord in en klik op **OK**.

> **Opmerking**
> Klik op **Wachtwoord wijzigen** om het wachtwoord van uw product te wijzigen. 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.

2.1.4. Productrapporten

Productrapporten bevatten informatie over hoe u het Bitdefender-product dat u geïnstalleerd hebt, gebruikt. Deze informatie is van essentieel belang

om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden.

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

Indien u tijdens de installatieprocedure hebt beslist om dergelijke rapporten naar de Bitdefender-servers te versturen en dit nu wilt stopzetten:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer het tabblad **Geavanceerd**.
3. Schakel **Productrapporten** uit.

2.1.5. Kennisgevingen speciale aanbiedingen

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

Om kennisgevingen voor speciale aanbiedingen in of uit te schakelen:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Schakel de overeenkomende schakelaar in venster **Algemeen** in of uit.

De optie speciale aanbiedingen en productmeldingen is standaard ingeschakeld.

2.2. Bitdefender-interface

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

Om door de Bitdefender-interface te gaan, wordt een inleidingswizard getoond met informatie over hoe u moet omgaan met het product en hoe u het moet configureren. Dit wordt in de linkerbovenhoek weergegeven. Selecteer het juiste pijltje om de gids voort te zetten of **Rondleiding overslaan** om de wizard te sluiten.

De Bitdefender-**systeemvakicoon** is altijd beschikbaar, ongeacht of u het hoofdvenster wilt openen, een productupdate wilt uitvoeren of informatie wilt bekijken over de geïnstalleerde versie.

Het hoofdvenster geeft informatie over uw beveiligingsstatus. Op basis van het gebruik en de noden van uw apparaat geeft **Autopilot** hier verschillende soorten aanbevelingen weer om u te helpen de beveiliging en prestaties van uw apparaat te verbeteren. En u kunt de snelle acties die u het vaakst gebruikt, toevoegen, zodat u ze altijd bij de hand hebt.

Vanuit het navigatiemenu aan de linkerzijde, kunt u naar de secties instellingen, notificaties en **Bitdefender** gaan voor gedetailleerde configuratietaken en geavanceerde administratieve taken.

Vanuit het bovengedeelte van de hoofdinterface hebt u toegang tot uw **Bitdefender-account**. U kunt ons ook contacteren voor ondersteuning indien u vragen hebt of indien er iets onverwacht gebeurt.

2.2.1. Systeemvakpictogram

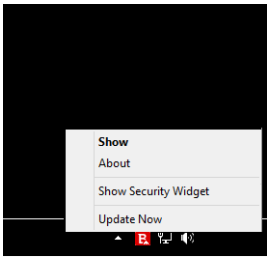
Om het volledige product sneller te beheren, kunt u het Bitdefender -pictogram in het systeemvak gebruiken.

Opmerking
Het Bitdefender-pictogram is mogelijk niet altijd zichtbaar. Om het pictogram permanent te laten verschijnen:

- In **Windows 7, Windows 8 en Windows 8.1**
  1. Klik op de pijl in de rechterbenedenhoek van het scherm.
  2. Klik op **Aanpassen...** om het venster met de systeemvakpictogrammen te openen.
  3. Selecteer de optie **Pictogrammen en meldingen weergeven** voor het pictogram van de **Bitdefender-agent**.
- In **Windows 10**
  1. Klik met de rechtermuisknop op de taakbalk en selecteer **Taakbalkinstellingen**.
  2. Scroll omlaag en klik op de link **Selecteer welke pictogrammen op de taakbalk** verschijnen onder **Systeemvak**.
  3. 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.

- **Weergeven** - opent het hoofdvenster van Bitdefender.
- **Over** - opent een venster met informatie over Bitdefender, over waar u hulp vindt in geval van problemen en waar u de Abonnementsovereenkomst, Onderdelen van Derde partijen alsook ons Privacybeleid kunt bekijken.
- **Update nu** - start een directe update. U kunt de updatestatus volgen in het paneel Update van het hoofdvenster van **Bitdefender**.



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

Er zijn geen problemen met de veiligheid van uw systeem.

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

Als Bitdefender niet werkt, verschijnt het systeemvakpictogram op een grijze achtergrond: . Dit gebeurt meestal wanneer het abonnement afloopt. Het kan ook voorkomen wanneer de Bitdefender-services niet reageren of wanneer andere fouten de normale werking van Bitdefender beïnvloeden.

2.2.2. Navigatiemenu

Aan de linkerzijde van de Bitdefender-interface vindt u het navigatiemenu waarmee u snel toegang krijgt tot alle Bitdefender-functies en -tools om uw product te beheren. De beschikbare tabbladen in dit gebied zijn:

- **Dashboard**. Van hier kunt u beveiligingsproblemen snel oplossen, aanbevelingen naargelang uw systeemnoden en gebruikspatronen weergeven, snelle acties uitvoeren en Bitdefender op andere apparaten installeren.
- **Bescherming**. Hier kunt u antivirusscans starten en configureren, Firewall-instellingen openen, gegevens herstellen indien ze werden versleuteld door ransomware en bescherming configureren wanneer u surft online.
- **Privacy**. Hier kunt u wachtwoordbeheerders aanmaken voor online accounts, de toegang tot uw webcam beschermen, online betalingen in beveiligde omgevingen uitvoeren, de VPN-app openen en uw kinderen beschermen door hun online activiteit op te volgen en te beperken.
- **Hulpprogramma's**. Van hieruit kunt u de snelheid van het systeem verbeteren en de antidiefstalfunctie voor uw apparaten configureren.
- **Meldingen**. Van hieruit hebt u toegang tot de gegenereerde kennisgevingen.
- **Instellingen**. Van hieruit hebt u toegang tot de algemene instellingen.
- **Ondersteuning**. Vanaf hier kunt u, wanneer u hulp nodig hebt bij het oplossen van een situatie met uw Bitdefender Antivirus Plus, contact opnemen met de afdeling Technische Ondersteuning van Bitdefender.
- **Mijn account**. Van hier kunt u naar uw Bitdefender-account gaan om uw abonnementen te controleren en beveiligingstaken uit te voeren op de toestellen die u beheert. Er zijn eveneens details beschikbaar over de Bitdefender-account en de lopende abonnementen.

2.2.3. Dashboard

Via het Dashboardvenster kunt u algemene taken uitvoeren, snel beveiligingsproblemen oplossen, informatie over het productgebruik weergeven en naar de panelen gaan van waar u de productinstellingen kunt configureren.

U kunt het allemaal met slechts enkele klikken op de knop.

Het venster is geordend in drie hoofdgebieden:

Gebied beveiligingsstatus

Hier controleert u de beveiligingsstatus van uw apparaat.

Autopilot

Hier kunt u de aanbevelingen voor Autopilot nagaan om de juiste werking van het systeem te verzekeren.

Snelle acties

Hier kunt u verschillende taken lanceren om uw systeem beschermd te houden en met optimale snelheid te werken. U kunt het Bitdefender eveneens installeren op andere toestellen, op voorwaarde dat u voldoende licenties hebt in uw abonnement.

Gebied beveiligingsstatus

Bitdefender gebruikt een systeem voor het opsporen van problemen en brengt u op de hoogte van de problemen die de veiligheid van uw apparaat en gegevens kunnen beïnvloeden. De gedetecteerde problemen bevatten belangrijke beveiligingsinstellingen die worden uitgeschakeld en andere omstandigheden die een beveiligingsrisico kunnen betekenen.

Wanneer problemen de beveiliging van uw apparaat aantasten, verandert de status die aan de bovenzijde van de **Bitdefender-interface** staat, naar rood. De weergegeven status geeft de aard van de problemen aan die uw systeem aantasten. Daarnaast verandert de **systeemvak**-icoon naar en als u de muiscursor over de icoon beweegt, verschijnt er een pop-up die bevestigt dat er problemen zijn.

Vermits de gedetecteerde problemen kunnen verhinderen dat Bitdefender u tegen bedreigingen beschermt of een belangrijk beveiligingsrisico kunnen inhouden, raden we aan dat u aandachtig bent en de problemen zo snel mogelijk oplost. Klik op de knop naast het gedetecteerde probleem om het probleem op te lossen.

Autopilot

Bitdefender Autopilot is uw persoonlijke beveiligingsadviseur om u bij al uw activiteiten een effectieve werking en verhoogde bescherming te bieden. Naargelang de activiteiten die u uitvoert, of u nu werkt, online betalingen doet, films bekijkt of spelletjes speelt, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat.

De voorgestelde aanbevelingen kunnen ook betrekking hebben op acties die u moet uitvoeren om ervoor te zorgen dat uw product aan volle capaciteit blijft werken.

Klik op de overeenkomende knop om de voorgestelde functie in gebruik te nemen of om verbeteringen door te voeren.

Uitschakelen van Autopilot-meldingen

Om uw aandacht te vestigen op de Autopilot-aanbevelingen, is het Bitdefender-product zo ingesteld om u via een pop-up op de hoogte te brengen.

Om de Autopilot-notificaties uit te schakelen:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Schakel in het venster **Algemeen Aanbeveling meldingen** uit.

Snelle acties

Met snelle acties kunt u taken opstarten die u belangrijk vindt om uw systeem te beschermen en aan de optimale snelheid te laten werken.

Bitdefender biedt standaard enkele snelle acties die u kunt vervangen met de acties die u zelf het vaakst gebruikt. Om een snelle actie te vervangen:

1. Klik op de icoon in de rechterbovenhoek van de kaart die u wilt verwijderen.
2. Wijs de taak aan die u aan de hoofdinterface wilt toevoegen en klik op **TOEVOEGEN**.

De taken die u aan de hoofdinterface kunt toevoegen, zijn:

- **Snelle scan**. Voer een snelle scan uit om mogelijke dreigingen op uw apparaat onmiddellijk te detecteren.
- **Systeemscan**. Voer een systeemscan uit om ervoor te zorgen dat uw apparaat vrij is van dreigingen.
- **Kwetsbaarheidsscan**. Scan uw apparaat op kwetsbaarheden om te verzekeren dat alle geïnstalleerde apps, samen met het besturingssysteem, bijgewerkt zijn en correct werken.
- **Wi-Fi Security Advisor**. Open het venster Wifi Beveiligingsadviseur binnen de module Kwetsbaarheid.
- **OpenSafepay**. Open Bitdefender Safepay™ om uw gevoelige gegevens te beschermen terwijl u online transacties uitvoert.

- **Open VPN**. Open Bitdefender VPN om een bijkomende beschermingslaag toe te voegen wanneer u verbonden bent met het internet.
- **Bestandsvernietiging**. Start de tool Bestandsvernietiging op om sporen van gevoelige gegevens van uw apparaat te verwijderen.
- **Open OneClick Optimizer**. Maak schijfruimte vrij, herstel registerfouten en beveilig uw privacy door bestanden die niet langer dienstig zijn in een enkele klik te verwijderen.

Om bijkomende toestellen te beginnen beschermen met Bitdefender:

1. Klik op **Een ander apparaat installeren**.
   Er verschijnt een nieuw venster op uw scherm.
2. Klik op **DOWNLOADKOPPELING DELEN**.
3. Volg de stappen op het scherm om Bitdefender te installeren.

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

- Bitdefender Antivirus Plus op Windows-apparaten.
- Bitdefender Antivirus for Mac op macOS X-apparaten.
- Bitdefender Mobile Security op Android-apparaten.
- Bitdefender Mobile Security op iOS-apparaten.

2.2.4. De Bitdefender-secties

Het product van Bitdefender heeft drie secties, verdeeld in nuttige functies om u te helpen beveiligd te blijven terwijl u werkt, op het web surft of online betalingen uitvoert, de snelheid van uw systeem verbetert en nog veel meer.

Wanneer u naar de functies voor een specifiek gedeelte wilt gaan of uw product wilt configureren, gaat u naar de volgende iconen in het navigatiemenu van de **Bitdefender-interface**:

- **Bescherming**
- **Privacy**
- **Hulpprogramma's**

Beveiliging

In het gebied Bescherming kunt u uw geavanceerde beveiligingsinstellingen configureren, vrienden en spammers beheren, de instellingen van de netwerkverbinding weergeven en bewerken, de voorzieningen voor Online Threat Preventie instellen, potentiële systeemkwetsbaarheden bekijken en oplossen en de beveiliging van de draadloze netwerken waarmee u verbinding maakt, beoordelen.

De functies 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 bedreiging, zoals malware, Trojaanse paarden, spyware, adware enz.

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

- Snelle scan
- Systeemscan
- Scans beheren
- Noodomgeving

Raadpleeg Antivirusbeveiliging (pagina 46) voor meer informatie over scantaken en het configureren van de antivirusbeveiliging.

ONLINE THREAT PREVENTION

Online Threat Prevention helpt u om beschermd te blijven tegen phishing-aanvallen, 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 Preventie van online bedreigingen (pagina 68).

FIREWALL

De firewall beschermt u terwijl u verbonden bent met netwerken en internet door alle verbindingspogingen te filteren.

Meer informatie over de firewallconfiguratie, vindt u onder Firewall.

ADVANCED THREAT DEFENSE

Geavanceerde Dreigingsverdediging beschermt uw systeem actief tegen bedreigingen zoals ransomware, spyware en Trojaanse paarden door het

gedrag van alle geïnstalleerde toepassingen te analyseren. Verdachte processen worden geïdentificeerd en indien nodig geblokkeerd.

Voor meer informatie over hoe u uw systeem beschermd houdt tegen bedreigingen, lees Geavanceerde bescherming tegen bedreigingen (pagina 66).

ANTISPAM

De Bitdefender-antispamfunctie zorgt ervoor dat uw Postvak IN vrij blijft van ongewenste e-mails door het POP3-mailverkeer te filteren.

Meer informatie over antispambeveiliging vindt u onder Antispam.

KWETSBAARHEID

De Kwetsbaarheidsfunctie 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 **Openen** in de module Kwetsbaarheden om de voorzieningen ervan te openen.

Met de **Kwetsbaarheidsscan** kunt u kritieke Windows-updates, updates van toepassingen, zwakke wachtwoorden van Windows-accounts en draadloze netwerken die niet beveiligd zijn, identificeren. Klik op **Scan starten** om een scan uit te voeren voor uw apparaat.

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 (pagina 71).

RANSOMWARE-REMEDIËRING

De functie Ransomware-remediëring helpt u bestanden herstellen indien ze door ransomware worden versleuteld.

Voor meer informatie over hoe u versleutelde bestanden kunt herstellen, raadpleeg Ransomware-remediëring (pagina 79).

Privacy

In het gedeelte Privacy kunt u de Bitdefender VPN-app openen, uw persoonlijke gegevens versleutelen, uw online transacties beschermen, uw

webcam en surfervaring beveiligen en uw kinderen beschermen door hun online activiteit te volgen en te beperken.

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

VPN

VPN beveiligt uw online activiteit en verbergt uw IP-adres telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. U kunt bovendien ook inhoud bekijken die in bepaalde gebieden afgeschermd wordt.

Voor meer informatie over deze functie, raadpleeg VPN (pagina 84).

VIDEO- & AUDIOBEVEILIGING

Video- & audiobeveiliging houdt uw webcam buiten gevaar door de toegang tot onbetrouwbare apps te blokkeren en u te waarschuwen als apps toegang proberen te krijgen tot uw microfoon.

Voor meer informatie over hoe u uw webcam kunt beveiligen tegen ongewenste toegang en hoe het Bitdefender ingesteld kan worden om u te waarschuwen over uw microfoonactiviteit, zie Video- & audiobeveiliging.

SAFEPAY

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

Voor meer informatie over Bitdefender Safepay™, zie Safepay beveiliging voor online transacties (pagina 87).

OUDERLIJK TOEZICHT

Met Ouderlijk Toezicht van Bitdefender kunt u controleren wat uw kinderen op hun apparaat doen. In geval van ongepaste inhoud kunt u beslissen om hun toegang tot het internet of tot specifieke apps te beperken.

Klik op **Configureren** in het panel Ouderlijk toezicht om te starten met het configureren van de toestellen van uw kinderen en het bewaken van hun activiteit, waar u ook bent.

Meer informatie over het configureren van Ouderlijk toezicht vindt u onder Ouderlijk toezicht.

ANTI-TRACKER

De functie Anti-tracker helpt u om tracering te vermijden zodat uw data privé blijven terwijl uw browser online is. Het verkort ook de tijd die nodig is om websites te laden.

Raadpleeg voor meer informatie over de functie Anti-tracker Anti-tracker.

Hulpprogramma's

In het gedeelte Hulpprogramma's kunt u de snelheid van uw systeem verbeteren en uw apparaten beheren.

OneClick Optimizer

Bitdefender Total Security biedt niet alleen beveiliging, maar helpt u ook de prestaties van uw apparaat in vorm te houden.

Onze OneClick Optimizer helpt u, in één eenvoudige stap, onnodige bestanden te vinden en te verwijderen van uw apparaat.

Voor meer informatie hierover, raadpleegt u OneClick Optimizer.

Anti-Theft

Bitdefender Antidiefstal beschermt uw apparaat en gegevens tegen diefstal of verlies. In dat geval kunt u uw apparaat op afstand lokaliseren of vergrendelen. U kunt ook alle in uw systeem aanwezige gegevens wissen.

Bitdefender Antidiefstal biedt de volgende functies:

- Lokaliseren op afstand
- Vergrendelen op afstand
- Wissen op afstand
- Waarschuwing op afstand

Meer informatie over hoe u uw systeem uit verkeerde handen houdt, vindt u onder Device Anti-Theft.

Gegevensbeveiliging

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

Voor meer informatie hierover, zie Data bescherming (pagina 101).

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.

Voor meer informatie over deze functie, zie profielen (pagina 94).

2.2.5. Producttaal wijzigen

De interface van Bitdefender is beschikbaar in meerdere talen. U kunt de taal aan de hand van de volgende stappen aanpassen:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het venster **Algemeen** op **Taal veranderen**.
3. Selecteer de gewenste taal uit de lijst en klik op **OPSLAAN**.
4. Wacht even tot de instellingen toegepast zijn.

2.3. Bitdefender Central

2.3.1. Over Bitdefender CENTRAL

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

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

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

Zodra u aangemeld bent, kunt u beginnen met het volgende:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:

- De Bitdefender Windows-productlijn
- Bitdefender Antivirus for Mac
- Bitdefender Mobile Security for Android
- Bitdefender Mobile Security for iOS

- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Nieuwe apparaten aan uw netwerk toevoegen en deze apparaten beheren, waar u op dat moment ook bent.
- Bescherm de netwerktoestellen en hun gegevens tegen diefstal of verlies met **Antidiefstal**.
- Configureer de instellingen voor **Ouderlijk toezicht** voor de apparaten van uw kinderen en volg hun activiteiten, waar u ook bent.

2.3.2. Toegang tot Bitdefender Central

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

- Vanuit de hoofdinterface van Bitdefender:
  1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Mijn account**.
  2. Klik op **Ga naar Bitdefender Central**.
  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. Log in op uw account met uw e-mailadres en wachtwoord.

- Vanaf uw Android- of iOS-apparaat:
  1. Open de Bitdefender Central-app die u hebt geïnstalleerd.

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

2.3.3. Twee-factorenauthenticatie

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

Twee-factorenauthenticatie activeren

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

Om de twee-factorenauthenticatie te activeren:

1. Toegang Bitdefender Centraal.
2. Klik op het pictogram rechtsboven op het scherm.
3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Klik op **2-Factorauthenticatie**.
6. Kik op **AAN DE SLAG**.
   Kies een van de volgende methodes:
   - **Authenticator App** - gebruik een authenticator app om een code te genereren telkens u zich wilt aanmelden op uw Bitdefender account.
     Als u een authenticator app zou willen, gebruiken, maar u niet zeker weet welke te kiezen, is er een lijst beschikbaar van de authentication apps die we aanbevelen.
     a. Klik op **AUTHENTICATOR APP GEBRUIKEN** om te starten.
     b. Om u aan te melden op een op Android of iOS gebaseerd apparaat, gebruik dat dan om de QR code te scannen.

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

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

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

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

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

  c. Klik op **ACTIVEREN**.

  d. U krijgt tien activeringscodes. U kunt de lijst kopiëren, downloaden of afdrukken en deze gebruiken in het geval u uw e-mailadres verliest of u zich niet meer kunt aanmelden. Elke code kan slechts één keer gebruikt worden.

  e. Klik op **GEREED**.

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

1. Klik op **TWEE-FACTORENAUTHENTICATIE UITSCHAKELEN**.
2. Controleer uw app of e-mailaccount en tik de code in die u hebt ontvangen.
   In het geval u ervoor hebt gekozen om de authenticatiecode te ontvangen via e-mail, hebt u vijf minuten om uw e-mailaccount te controleren en de gegenereerde code in te tikken. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.
3. Bevestig uw keuze.

2.3.4. Betrouwbare apparaten toevoegen

Om ervoor te zorgen dat alleen u toegang hebt tot uw Bitdefender account, is het mogelijk dat we eerst een veiligheidscode vragen. Als u deze stap zou willen overslaan telkens u verbinding maakt vanaf hetzelfde apparaat, raden we u aan dit te benoemen als een betrouwbaar apparaat.

Om toestellen toe te voegen als betrouwbare apparaten:

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

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

2.3.5. Activiteit

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

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

- **Mijn apparaten.** Hier kunt u het aantal aangesloten apparaten en hun beschermingsstatus bekijken. Om problemen met de gedetecteerde apparaten op afstand op te lossen, klikt u op **Problemen oplossen** en vervolgens op **SCANNEN EN PROBLEMEN OPLOSSEN**.
  Om details te zien over de gedetecteerde problemen, klikt u op **Problemen bekijken**.
  Informatie over de gedetecteerde bedreigingen kan voor iOS-apparaten niet worden opgehaald.
- **Dreigingen geblokkeerd.** Hier ziet u een grafiek met de algemene statistieken, met inbegrip van informatie over de bedreigingen die de voorbije 24 uur en 7 dagen werden geblokkeerd. De weergegeven informatie wordt opgehaald naargelang het schadelijke gedrag dat in de bestanden, toepassingen en url's werd gedetecteerd.
- **Topgebruikers met geblokkeerde bedreigingen.** Hier ziet u de gebruikers waarbij de meeste bedreigingen werden gevonden.
- **Topapparaten met geblokkeerde bedreigingen.** Hier ziet u de apparaten waarop de meeste bedreigingen werden gevonden.

2.3.6. Mijn abonnementen

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

Controleer beschikbare abonnementen

Zo controleert u uw beschikbare abonnementen:

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

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

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

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

Abonnement activeren

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

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

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

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Klik op de knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **ACTIVEREN** om door te gaan.

Het abonnement is nu geactiveerd.

Abonnement verlengen

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

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

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

2.3.7. Mijn apparaten

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

Toevoeging van een nieuw apparaat

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

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel en tik vervolgens op **INSTALLEER BESCHERMING**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
   - **Bescherm andere apparaten**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
     Druk op **DOWNLOADKOPPELING VERZENDEN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL**

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

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

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

Uw apparaten aanpassen

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

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

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

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Klik op **Eigenaar toevoegen** en vul de bijbehorende velden in. Pas het profiel aan: voeg een foto toe, selecteer een geboortedatum en voeg een e-mailadres en geboortedatum toe.
6. Klik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en klik op **TOEWIJZEN**.

Beheer op afstand

Bitdefender van op afstand op een apparaat updaten:

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

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

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

- **Dashboard.** In dit venster kunt u de gegevens van het geselecteerde apparaat bekijken, de beschermingsstatus en de Bitdefender VPN-status controleren en nakijken hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus is altijd groen (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Wanneer er problemen zijn met uw apparaat, klik dan op het uitklappijltje in het bovenste statusgebied voor meer details. Hier kunt u
- **Bescherming.** In dit tabblad kunt u op afstand een snelle of systeemscan uitvoeren op uw apparaten. Klik op de knop **Scan** om de scan te starten. U kunt ook zien wanneer de laatste scan op het apparaat is uitgevoerd en er is een rapport beschikbaar met de belangrijkste gegevens van de laatste scan.
- **Optimalisatie.** Hier kunt u op afstand de prestaties van een apparaat verbeteren door snel te scannen, nutteloze bestanden te detecteren en op te schonen. Klik op de **START** knop, en selecteer vervolgens de gebieden die u wilt optimaliseren. Klik nogmaals op de knop **START** om het optimalisatieproces te starten. Klik op **Meer details** voor een gedetailleerd rapport over de opgeloste problemen.
- **Anti-diefstal.** In geval van misplaatsing, diefstal of verlies kunt u met de anti-diefstalfunctie uw apparaat lokaliseren en op afstand acties ondernemen. Klik op **LOKALISEREN** om de positie van het apparaat te achterhalen. De laatst bekende positie wordt weergegeven, samen met de tijd en datum.

- **Kwetsbaarheid.** Om een apparaat te controleren op kwetsbaarheden zoals ontbrekende Windows-updates, verouderde apps of zwakke wachtwoorden klikt u op de knop **SCANNEN** in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet op afstand worden verholpen. Als er een kwetsbaarheid wordt gevonden, moet u een nieuwe scan uitvoeren op het apparaat en vervolgens de aanbevolen acties ondernemen. Klik op **Meer details** voor een gedetailleerd rapport over de gevonden problemen.

2.3.8. Meldingen

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

2.4. Bitdefender up-to-date houden

Elke dag worden er nieuwe bedreigingen gevonden en geïdentificeerd. Daarom is het heel belangrijk om Bitdefender up to date te houden met de nieuwste informatiedatabase voor bedreigingen.

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 apparaat aanzet en ieder **uur** daarna. Als er een update beschikbaar is, wordt deze automatisch gedownload en op uw apparaat geïnstalleerd.

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

> **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 apparaat een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in .
- Als u met het Internet bent verbonden via een inbelverbinding, dan adviseren wij Bitdefender regelmatig handmatig te updaten. Zie voor meer informatie.

2.4.1. Controleren of Bitdefender up-to-date is

Om het tijdstip van de laatste update van uw Bitdefender te controleren:

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

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.

2.4.2. Een update uitvoeren

Om updates uit te voeren is een internetverbinding vereist.

Om een update te starten, klikt u met de rechtermuisknop op het Bitdefender-pictogram in het **systeemvak** en selecteert u vervolgens **Nu updaten**.

De functie 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 apparaat opnieuw op te starten wanneer de update is voltooid. Wij raden aan 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 vanop afstand op een Windows-apparaat updaten:

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

2.4.3. De automatische update in- of uitschakelen

De automatische update in- of uitschakelen:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Klik op het tabblad **Update**.
3. Schakel de overeenkomende schakelaar in of uit.

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, of tot het systeem opnieuw wordt opgestart.

   Waarschuwing
   Dit is een kritiek beveiligingsprobleem. Wij adviseren 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.

2.4.4. 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 **Instellingen** in het navigatiemenu op 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.

Regels voor behandelen updates

Telkens wanneer er een update beschikbaar is, zal Bitdefender de update automatisch downloaden en invoeren zonder notificaties weer te geven. Schakel de optie **Stille update** uit indien u een notificatie wilt ontvangen telkens wanneer er een nieuwe update beschikbaar is.

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 apparaat opnieuw opstart. Hiermee wordt voorkomen dat de Bitdefender-update het werk van de gebruiker hinder.

Schakel **Opstartnotificatie** in als u verzocht wilt worden uw toestel terug op te starten wanneer een update dat vereist.

2.4.5. Doorlopende updates

Om zeker te zijn dat u de recentste versie gebruikt, controleert uw Bitdefender automatisch of er productupdates zijn. Deze updates kunnen nieuwe functies en verbeteringen hebben, productproblemen verhelpen of u een automatische upgrade naar een nieuwe versie bezorgen. Wanneer de nieuwe Bitdefender-versie via een update arriveert, worden persoonlijke instellingen opgeslagen en wordt de verwijderings- en herinstallatieprocedure overgeslagen.

Voor deze updates moet u het systeem opnieuw opstarten om de installatie van nieuwe bestanden te activeren. Nadat de productupdate voltooid is, verschijnt een popup-venster met de melding dat het systeem opnieuw moet worden opgestart. Indien u deze kennisgeving niet hebt gezien, kunt u ofwel klikken op **NU OPNIEUW OPSTARTEN** in het venster **Kennisgevingen** waar de recentste update wordt vermeld, of het systeem manueel opnieuw opstarten.

> **Opmerking**
> De updates met nieuwe functies en verbeteringen worden enkel aan gebruikers geleverd bij wie Bitdefender 2020 geïnstalleerd is.

2.5. Smart voice assistance

Als u de slimme luidspreker Amazon Alexa of de Google Assistant-app gebruikt, kunt u spraakopdrachten geven om een reeks taken uit te voeren of informatie te controleren op de apparaten waarop Bitdefender is geïnstalleerd. Zo kunt u scan- en optimalisatietaken uitvoeren, het internet op de aangesloten apparaten pauzeren, de status van uw huidige abonnement controleren of de locaties of online activiteiten van uw kinderen controleren. Raadpleeg Spraakopdrachten voor interactie met Bitdefender (pagina 44) voor de volledige lijst met spraakopdrachten die u kunt starten.

2.5.1. Instellen van spraakopdrachten

De spraakopdrachten van Bitdefender kunnen worden geconfigureerd voor:

- **Google Home app aan**
  - Android 5.0 en hoger
  - iOS 10.0 en nieuwer
  - Chromebooks
- **Amazon Alexa app aan**
  - Echo
  - Echo Dot
  - Echo Show
  - Echo Spot
  - Fire TV Cube

Instellen van Amazon Alexa-spraakopdrachten voor Bitdefender

Om de spraakopdrachten van Bitdefender in te stellen op Amazon Alexa:

1. Open de Amazon Alexa app.
2. Tik op het **Menu** pictogram, en ga dan naar **Vaardigheden**.
3. Zoek naar Bitdefender.
4. Tik op **Bitdefender** en tik dan op **INSCHAKELEN**.
5. U wordt gevraagd in te loggen op uw Bitdefender-account.
   Tik uw gebruikersnaam en uw wachtwoord in, en tik op **INLOGGEN**.

Zodra de synchronisatie van Bitdefender met uw Amazon Alexa is voltooid, krijgt u uitleg over de spraakopdrachten die u kunt gebruiken om taken te starten of om informatie te controleren over de apparaten waarop Bitdefender is geïnstalleerd.

Als u wilt dat de assistent u de lijst met alle beschikbare spraakopdrachten of vaardigheden geeft, zeg dan **HELP MIJ**.

Instellen van Google Home-spraakopdrachten voor Bitdefender

Om de spraakopdrachten op Google Home in te stellen:

1. Open de toepassing Google Home.
2. Tik op Menu in de linkerbovenhoek van het Beginscherm en tik vervolgens op **Verkennen**.
3. Zoek naar Bitdefender.
4. Tik op **Bitdefender** en tik dan op **Link**.
5. U wordt gevraagd om u aan te melden bij uw Bitdefender-account. Typ uw gebruikersnaam en uw wachtwoord en tik vervolgens op **AANMELDEN**.

Zodra de synchronisatie van Bitdefender met Google Home is voltooid, krijgt u uitleg over de spraakopdrachten die u kunt gebruiken om taken te starten of om informatie te controleren over de apparaten waarop Bitdefender is geïnstalleerd.

Wanneer u de assistent nodig heeft om u bijvoorbeeld de lijst met alle beschikbare spraakopdrachten of vaardigheden te geven **HELP ME**.

2.5.2. Spraakopdrachten voor interactie met Bitdefender

Om de spraakopdrachten van Bitdefender te openen:

- Op Amazon Alexa: **Alexa, open Bitdefender**
- Op Google Home: **OK Google, praat met Bitdefender**

Om de spraakopdrachten van Bitdefender te starten:

- Op Amazon Alexa: **Alexa, vraag het aan Bitdefender**
- Op Google Home: **OK, Google, vraag het aan Bitdefender**

De vragen en taken die u kunt starten zodra de Bitdefender-assistent is geopend, zijn:

- Hoe is mijn activiteit vandaag?
- Wat is de status van mijn abonnement?
- Optimaliseer mijn apparaten. (Deze opdracht start OneClick Optimizer op de aangesloten Windows-apparaten).
- Voer een snelle scan uit op mijn [apparaattype]. (Als apparaattype kunt u laptop, computer, telefoon of tablet zeggen).

Als u Ouderlijk Toezicht hebt ingesteld op de apparaten van uw kinderen, zijn de vragen en taken die u kunt starten zodra de Bitdefender-assistent is geopend:

- Pauzeer de internetverbinding voor [profielnaam].
- Hervat de internetverbinding voor [profielnaam].
- Zoek mijn kind.
- Waar is mijn kind?
- Hoeveel tijd besteedde mijn kind aan zijn/haar apparaten?
- Hoelang heeft mijn kind vandaag Facebook gebruikt?
- Hoelang heeft mijn kind vandaag Instagram gebruikt?

Als u meer Ouderlijk Toezichtprofielen heeft, kunt u de naam van uw kind in de opdracht vermelden. Bijvoorbeeld, **Zoek Jennifer**.

3. UW BEVEILIGING BEHEREN

3.1. Antivirusbeveiliging

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

- **Scannen bij toegang** - verhindert dat nieuwe 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 bedreigingen, een essentieel onderdeel van elk computerbeveiligingsprogramma.

  > **Belangrijk**
  > Houd **Scannen bij toegang** ingeschakeld om te verhinderen dat bedreigingen uw apparaat infecteren.

- **Scannen op aanvraag** - hiermee kunt u de bedreiging 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 apparaat zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend. Zie Automatisch scannen van verwisselbare media (pagina 60) voor meer informatie.

Geavanceerde gebruikers kunnen scanuitzonderingen configureren als ze niet willen dat specifieke bestanden of bestandstypes worden gescand. Zie Scanuitsluitingen configureren (pagina 63) voor meer informatie.

Wanneer een bedreiging wordt gedetecteerd, zal Bitdefender automatisch proberen de kwaadwillige code 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. Zie Bestanden in quarantaine beheren (pagina 65) voor meer informatie.

Als uw apparaat werd geïnfecteerd door bedreigingen, moet u Bedreigingen van uw systeem verwijderen (pagina 143) raadplegen. Om u te helpen bij het opruimen van de bedreigingen die niet kan worden verwijderd van het Windows-besturingssysteem op uw apparaat, biedt Bitdefender u de Reddingsomgeving (pagina 144). Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van bedreigingen, waarmee u uw apparaat onafhankelijk van Windows kunt opstarten. Wanneer het apparaat in de Noodomgeving wordt gebruikt, zijn Windows-dreigingen niet actief, waardoor het makkelijker is om ze te verwijderen.

3.1.1. Scannen bij toegang (real time-beveiliging)

Bitdefender biedt realtime bescherming tegen een breed gamma bedreigingen door alle bestanden en e-mailberichten waar toegang toe wordt gezocht, te scannen.

De real time-beveiliging in- of uitschakelen

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

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Bescherming**.
2. Klik in het deelvenster **ANTIVIRUS** op **Openen**.
3. Schakel in het venster **Geavanceerd Bitdefender Shield** in of uit.
4. 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 bedreigingen.

De geavanceerde 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.

Om degeavanceerde instellingen voor de realtime beveiliging te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. In het venster **Geavanceerd** kunt u de scaninstellingen configureren.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- **Scan alleen toepassingen.** U kunt Bitdefender instellen om alleen geopende apps te scannen.
- **Scan potentieel ongewenste toepassingen.** Selecteer deze optie om te scannen op ongewenste toepassingen. Een potentieel ongewenste toepassing (PUA) of potentieel ongewenst programma (PUP) is software die meestal gebundeld wordt met freeware software en pop-ups weergeeft of een werkbalk installeert in de standaard browser. Sommige veranderen de startpagina of de zoekmachine, andere laten verschillende processen op de achtergrond lopen die de pc vertragen of tonen talrijke advertenties. Deze programma's kunnen worden geïnstalleerd zonder uw toestemming (ook wel adware genoemd) of worden standaard opgenomen in de express installatiekit (advertentie-gesteund).
- **Scripts scannen.** Met de functie Scripts scannen kan Bitdefender powershellscripts en office-documenten scannen die scriptgebaseerde malware zou kunnen bevatten.
- **Gedeelde netwerken scannen.** Om een extern netwerk vanaf uw apparaat veilig te gebruiken, raden we aan dat u de optie Gedeelde netwerken scannen ingeschakeld laat.
- **Procesgeheugen scannen.** Scant op kwaadaardige activiteiten in het geheugen van lopende processen.
- **Opdrachtregel scannen.** Scant de opdrachtregel van nieuw opgestarte toepassingen om bestandsloze aanvallen te voorkomen.
- **Archieven scannen.** Het scannen binnen archieven is een traag proces dat veel middelen vergt, en dat daarom niet wordt aanbevolen voor real

time-beveiliging. Archieven met geïnfecteerde bestanden vormen geen onmiddellijke dreiging voor de veiligheid van uw systeem. De dreiging kan uw systeem pas aantasten als het geïnfecteerde bestand wordt uitgepakt uit het archief en wordt uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.

Beslist u om deze optie te gebruiken, schakel deze dan in en versleep de schuifregelaar langs de schaal om archieven die groter zijn dan een bepaalde waarde in MB (Megabytes) uit te sluiten.

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de opstartsectoren van uw harde schijf te scannen. Deze sector van de harde schijf bevat de noodzakelijke computercode om het opstartproces te starten. Wanneer een dreiging de opstartsector infecteert, kan de schijf ontoegankelijk worden en kunt u uw systeem niet opstarten en geen toegang krijgen 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.
- **Keyloggers scannen.** Selecteer deze optie om uw systeem te scannen op keylogger apps. 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 gegevens halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.
- **Vroege opstartscan.** 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 om de detectie van bedreigingen bij de opstart van het systeem te verbeteren en de opstarttijd van uw systeem te verkorten.

Acties die worden ondernomen op gedetecteerde bedreigingen

U kunt de acties die door de realtime bescherming worden genomen configureren aan de hand van de volgende stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.

3. In het venster **Geavanceerd** scrolt u naar beneden tot u de optie **Dreigingsacties** ziet.
4. Configureer de scaninstellingen zoals dat nodig is.

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

Neem gepaste actie

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

- **Geïnfecteerde bestanden.** Bestanden die als besmet zijn gedetecteerd, komen overeen met een stukje bedreigingsinformatie gevonden in de informatiedatabase voor bedreigingen van Bitdefender. Bitdefender zal automatisch proberen de kwaadaardige code 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. Zie Bestanden in quarantaine beheren (pagina 65) voor meer informatie.

  > **Belangrijk**
  > Voor specifieke types bedreigingen 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 dreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een dreiging wordt bevestigd, wordt een informatie-update voor dreigingen uitgegeven zodat de dreiging 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 verplaatsen

Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie Bestanden in quarantaine beheren (pagina 65) voor meer informatie.

Toegang weigeren

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

De standaardinstellingen herstellen

De standaardinstellingen voor de realtime-beveiliging garanderen een goede beveiliging tegen bedreigingen, met een minimale impact op de systeemprestaties.

De standaard real time-beveiligingsinstellingen herstellen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Scrol naar beneden in het venster **Geavanceerd** tot u de optie **Geavanceerde instellingen terugstellen** ziet. Selecteer deze optie om de antivirusinstellingen terug te stellen naar fabrieksinstellingen.

3.1.2. Scannen op aanvraag

Bitdefender heeft als hoofddoel uw apparaat vrij te houden van bedreigingen. Dit wordt gedaan door nieuwe bedreigingen uit uw apparaat 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 bedreiging zich reeds in uw systeem heeft genesteld voordat u Bitdefender installeert. Het is dan ook een bijzonder goed idee uw apparaat meteen te scannen op aanwezige bedreigingen nadat u Bitdefender hebt geïnstalleerd. En het is absoluut een goed idee om uw apparaat regelmatig te scannen op bedreigingen.

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand. U kunt de apparaat 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 apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

Een bestand of map scannen op bedreigingen

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.

Een snelle scan uitvoeren

Quick Scan gebruikt in-the-cloud scanning om bedreigingen die op uw systeem worden uitgevoerd, te detecteren. Het uitvoeren van een Snelle scan duurt doorgaans minder dan een minuut en gebruikt slechts een fractie van het systeemgeheugen dat gewone antivirusscans gebruiken.

Een snelle scan starten:

1. Klik in het navigatiemenu in de Bitdefender-interface op Bescherming.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op de **Scan uitvoeren** knop naast **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.

Een systeemscan uitvoeren

De systeemscan scant de volledige apparaten op alle types bedreigingen die de beveiliging in gevaar brengen, zoals malware, 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 apparaten niet gebruikt.

Voordat u een systeemscan uitvoert, wordt het volgende aanbevolen:

- Zorg ervoor dat Bitdefender up to date is met de informatiedatabase voor bedreigingen. Het scannen van uw apparaat met een oude informatiedatabase voor bedreigingen kan verhinderen dat Bitdefender nieuwe bedreigingen die sinds de laatste update zijn gevonden, detecteert. Zie Bitdefender up-to-date houden (pagina 39) voor meer informatie.
- Alle open programma's afsluiten

Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren. Zie Een aangepaste scan configureren (pagina 53) voor meer informatie.

Een systeemscan lanceren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op de **Scan uitvoeren** knop naast **Systeemscan**.
4. De eerste keer dat u de Systeemscan uitvoert, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.
5. Volg de Antivirus Scan-wizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op gedetecteerde bestanden. Als er onopgeloste bedreigingen blijven, wordt u gevraagd de acties te kiezen die u daarop wilt ondernemen.

Een aangepaste scan configureren

In het venster **Scans beheren** kunt u Bitdefender zo instellen dat het scans uitvoert wanneer u denkt dat uw apparaat op mogelijke bedreigingen

moet worden gecontroleerd. U kunt ervoor kiezen om een **Systeemscan** of **Snelle scan** in te plannen, of u kunt een aangepaste scan aanmaken.

Om een nieuwe aangepaste scan in detail te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op **+Scan aanmaken**.
4. Voer in het veld **Taaknaam** een naam in voor de scan, selecteer vervolgens de locaties die u wilt laten scannen, en klik op **Volgende**.
5. Configureer deze algemene opties:
   - **Scan alleen toepassingen.** U kunt Bitdefender zo instellen dat alleen geopende apps worden gescand.
   - **Prioriteit scantaak.** U kunt kiezen welke impact een scanprocedure mag hebben op de prestaties van uw systeem.
     - Auto - De prioriteit van de scanprocedure hangt af van de systeemactiviteit. Om te verzekeren dat de scanprocedure geen invloed heeft op de systeemactiviteit, beslist Bitdefender of de scanprocedure met een hoge of lage prioriteit moet worden uitgevoerd.
     - Hoog - De prioriteit van de scanprocedure is hoog. Door deze optie te selecteren, laat u andere programma's trager werken, en verkort u de tijd die nodig is om de scanprocedure te voltooien.
     - Laag - De prioriteit van de scanprocedure is laag. Door deze optie te selecteren, laat u andere programma's sneller werken, en verlengt u de tijd die nodig is om de scanprocedure te voltooien.
   - **Acties na het scannen.** Kies welke actie Bitdefender moet ondernemen als er geen bedreigingen zijn gevonden:
     - Venster met samenvatting weergeven
     - Apparaat uitschakelen
     - Scanvenster sluiten
6. Als u de scanopties in detail wilt configureren, klikt u op **Geavanceerde opties weergeven**. U vindt informatie over de vermelde scans aan het einde van dit gedeelte.

Klik op **Volgende**.

7. U kunt **Scantaak inplannen** indien gewenst inschakelen, en dan kiezen wanneer de aangepaste scan die u hebt gemaakt, moet beginnen.
   - ❍ Bij opstarten systeem
   - ❍ Dagelijks
   - ❍ Maandelijks
   - ❍ Wekelijks

   Kiest u Dagelijks, Maandelijks of Wekelijks, versleept u de schuifregelaar op de schaal om te kiezen wanneer de ingeplande scan moet starten.
8. Klik op **OPSLAAN** om de instellingen op te slaan en sluit het configuratievenster.
   Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Indien er tijdens de scanprocedure bedreigingen worden gevonden, wordt u gevraagd de acties te kiezen die in verband met de gedetecteerde bestanden moeten worden ondernomen.

Informatie over de scanopties

Misschien vindt u deze informatie nuttig:

- ❍ 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.
- ❍ **Scan mogelijk ongewenste applicaties.** Selecteer deze optie om te scannen op ongewenste toepassingen. Een mogelijk ongewenste applicatie (PUA) of mogelijk ongewenst programma (PUP) is software die meestal wordt meegeleverd met freeware software en die pop-ups weergeeft of een werkbalk installeert in de standaardbrowser. Sommigen van hen zullen de startpagina of de zoekmachine wijzigen, anderen zullen verschillende processen op de achtergrond uitvoeren die de pc vertragen of zullen talloze advertenties weergeven. Deze programma's kunnen zonder uw toestemming worden geïnstalleerd (ook wel adware genoemd) of worden standaard opgenomen in de kit voor snelle installatie (ondersteund door advertenties).
- ❍ **Archieven scannen.** Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke dreiging voor de beveiliging van uw systeem. De dreiging 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 dreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke dreiging gaat.

Versleep de schuifregelaar langs de schaal om archieven die groter zijn dan een bepaalde waarde in MB (Megabytes) uit te sluiten.

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

- **Scan alleen nieuwe en gewijzigde bestanden.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algehele reactietijd van het systeem aanzienlijk verbeteren met een minimum aan beveiliging.
- **Scan opstartsectoren.** U kunt Bitdefender instellen om de opstartsectoren van uw harde schijf te scannen. Deze sector van de harde schijf bevat de benodigde computercode om het opstartproces te starten. Wanneer een dreiging de opstartsector infecteert, kan de schijf ontoegankelijk worden en kunt u mogelijk uw systeem niet meer opstarten en geen toegang krijgen 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 apps.
- **Cookies scannen.** Selecteer deze opties om de cookies te scannen die via browsers op uw computers zijn opgeslagen.
- **Keyloggers scannen.** Selecteer deze optie om uw systeem te scannen op keylogger-apps. Keyloggers registreren wat u op uw toetsenbord typt en sturen rapporten via internet naar een kwaadwillende persoon (hacker). De hacker kan uit de gestolen gegevens gevoelige informatie halen, zoals bankrekeningnummers en wachtwoorden, en daarmee persoonlijke voordelen behalen.

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 het scannen beëindigt. 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 bedreigingen 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, afhankelijk van het type gedetecteerd bestand:

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een stuk dreigingsinformatie dat is gevonden in de Bitdefender Threat Information Database. Bitdefender zal automatisch proberen de kwaadaardige code uit het geïnfecteerde bestand te verwijderen en het originele bestand te reconstrueren. Deze operatie wordt desinfectie genoemd.
  Bestanden die niet kunnen worden gedesinfecteerd, worden in quarantaine geplaatst om de infectie in te dammen. In quarantaine geplaatste bestanden kunnen niet worden uitgevoerd of geopend; daarom verdwijnt het risico om besmet te raken. Voor meer informatie, zie Bestanden in quarantaine beheren (pagina 65).

> **Belangrijk**
> Voor bepaalde soorten bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig kwaadaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand van de schijf verwijderd.

- **Verdachte documenten.** Bestanden worden door de heuristische analyse als verdacht gedetecteerd. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat er geen desinfectieroutine beschikbaar is. Ze worden in quarantaine geplaatst om een mogelijke infectie te voorkomen.
  Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de dreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een dreiging wordt bevestigd, wordt een informatie-update uitgegeven zodat de dreiging kan worden verwijderd.
- **Archieven met geïnfecteerde bestanden.**
  - 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 het archief met de schone bestanden kan reconstrueren. Als archiefreconstructie niet mogelijk is, wordt u geïnformeerd dat er geen actie kan worden ondernomen om te voorkomen dat schone bestanden verloren gaan.

Verwijderen

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 ondernemen

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 een bedreiging vindt u onder Bedreigingen van uw systeem verwijderen (pagina 143).

3.1.3. 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 **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste scan.
   Hier vindt u alle gebeurtenissen van scans op bedreigingen, 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.

3.1.4. Automatisch scannen van verwisselbare media

Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw apparaat en scant dit op de achtergrond

wanneer de Autoscan-optie geactiveerd is. Dit is aanbevolen om infecties van uw apparaat door bedreigingen te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

- Cd's/dvd's
- USB-sticks 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.

Hoe werkt het?

Wanneer Bitdefender een verwisselbaar opslagapparaat detecteert, begint het het apparaat te scannen op bedreigingen (op voorwaarde dat de automatische scan voor dat type apparaat is ingeschakeld). U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.

Een Bitdefender-scanpictogram verschijnt in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

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.

In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde bedreigingen 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.

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een cd/dvd gebruikt die besmet is met een bedreiging. De bedreiging kan niet van de schijf worden verwijderd

(het medium is alleen-lezen). Zorg dat de real time-beveiliging is ingeschakeld om te verhinderen dat bedreigingen zich over uw systeem verspreiden. 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 bedreigingen 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).
  Om te weten hoe u met bedreigingen moet omgaan, ga naar Bedreigingen van uw systeem verwijderen (pagina 143).

Scan verwisselbare media beheren

Automatische scans van verwisselbare media beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Selecteer het venster **Instellingen**.

De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, probeert Bitdefender ze te desinfecteren (de kwaadaardige code 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.

Voor de beste beveiliging is het aanbevolen om de geselecteerde optie van **Autoscan** in te schakelen voor alle types verwisselbare opslagapparaten.

3.1.5. 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 **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Geavanceerd** tabblad.
3. Schakel **Gastbestand scannen** in of uit.

3.1.6. 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 Bitdefender-vertegenwoordiger volgen.

U kunt de 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**
> Uitzonderingen 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**.

Bestanden en mappen uitsluiten van het scannen

Om specifieke bestanden en mappen van het scannen uit te sluiten:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer in het overeenkomende veld het pad in van de map die u wilt uitsluiten van het scannen.
   U kunt ook naar de map navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer de map en klik op **OK**.

6. Schakel de schakelaar naast de beschermingsvoorziening die de map niet moet scannen, in. Er zijn drie opties:
   - Antivirus
   - Preventie van online dreigingen
   - Advanced Threat Defense
7. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Bestandsextensies uitsluiten van scannen

Wanneer u een bestandsextensie uitsluit van de scan, zal Bitdefender bestanden met die extensie niet meer scannen, ongeacht hun locatie op uw apparaat. 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 apparaat kwetsbaar maken voor bedreigingen.

Om bestandsextensies uit te sluiten van het scannen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. In de **Instellingen** venster, klik **Uitzonderingen beheren**.
4. Klik **+Voeg een uitzondering toe**.
5. Voer de extensies in die u van het scannen wilt uitsluiten met een puntje ervoor, en scheid ze van elkaar met puntkomma's (;).
   ```
   txt;avi;jpg
   ```
6. Schakel de schakelaar naast de beschermingsvoorziening die de extensie niet moet scannen, in.
7. Klik op **Opslaan**.

Scanuitsluitingen beheren

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

Om scanuitsluitingen te beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**. Er wordt een lijst met al uw uitzonderingen weergegeven.
4. Klik op een van de beschikbare knoppen om scanuitzonderingen te verwijderen of te bewerken. Ga als volgt te werk:
   - Om iets uit de lijst te verwijderen, klik op de knop ernaast.
   - Om een gegeven in de tabel te bewerken, klikt u ernaast op de knop **Bewerken**. Er verschijnt een nieuw venster. Hierin kunt u de extensie of het pad dat moet worden uitgezonderd, wijzigen, alsook de beveiligingsvoorziening die de extensie of het pad moet uitsluiten. Breng de nodige wijzigingen aan en klik daarna op **WIJZIGEN**.

3.1.7. Bestanden in quarantaine beheren

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

Standaard worden in quarantaine geplaatste bestanden automatisch naar Bitdefender Labs gestuurd om te worden geanalyseerd door de Bitdefender-bedreigingsonderzoekers. Als de aanwezigheid van een dreiging wordt bevestigd, wordt er een informatie-update vrijgegeven om de dreiging te kunnen verwijderen.

Daarnaast scant Bitdefender de bestanden in quarantaine telkens de informatiedatabase voor bedreigingen geüpdatet wordt. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

De bestanden in quarantaine controleren en beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Ga naar het venster **Instellingen**.
   Hier ziet u de naam van de bestanden in quarantaine, alsook hun oorspronkelijke locatie en de naam van de gedetecteerde bedreigingen.

4. Bestanden in quarantaine worden automatisch beheerd door Bitdefender op basis van de standaard quarantaine-instellingen.
   Hoewel dit niet wordt aanbevolen, kunt u de quarantaine-instellingen aanpassen volgens uw voorkeur door te klikken op **Instellingen weergeven**.
   Klik op de schakelaars om deze optie in of uit te schakelen.
   Quarantaine opnieuw scannen na update van informatie over bedreigingen
   Houd deze optie ingeschakeld om bestanden in quarantaine automatisch te scannen na elke update van de informatiedatabase voor bedreigingen. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.
   Inhoud ouder dan 30 dagen verwijderen
   Bestanden in quarantaine die ouder zijn dan 30 dagen worden automatisch verwijderd.
   Maak uitzonderingen aan voor herstelde bestanden
   De bestanden die u vanuit quarantaine herstelt, worden zonder reparatie teruggezet naar hun oorspronkelijke locatie, en worden voor volgende scans automatisch uitgesloten.
5. 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 **Terugzetten**.

3.2. Geavanceerde bescherming tegen bedreigingen

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

Geavanceerde dreigingscontrole bewaakt voortdurend de toepassingen die op de apparaat worden uitgevoerd en zoekt naar acties die op bedreigingen lijken. Elk van deze acties krijgt een score en voor elk proces wordt een algemene score berekend.

Als veiligheidsmaatregel wordt u op de hoogte gesteld telkens er bedreigingen of mogelijk kwaadwillige processen worden gedetecteerd en geblokkeerd.

3.2.1. Advanced Threat Defense in- of uitschakelen

Advanced Threat Defense in- of uitschakelen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **ADVANCED THREAT DEFENSE** op **Openen**.
3. Ga naar het venster **Instellingen** en klik op de schakelaar naast **Bitdefender Advanced Threat Defense**.

> **Opmerking**
> Om uw systeem beschermd te houden tegen ransomware en andere bedreigingen, bevelen we u aan Advanced Threat Defense zo weinig mogelijk uit te schakelen.

3.2.2. Gedetecteerde kwaadwillige aanvallen controleren

Wanneer bedreigingen of mogelijk kwaadwillige processen worden gedetecteerd, blokkeert Bitdefender deze om uw apparaat te beschermen tegen ransomware of andere malware. U kunt de lijst met gedetecteerde kwaadwillige aanvallen op elk gewenst moment controleren aan de hand van de onderstaande stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
3. Ga naar het venster **Threat Defense**.
   De aanvallen die de voorbije 90 dagen werden gedetecteerd, worden getoond. Om meer informatie te lezen over de opgespoorde ransomware, de paden van het schadelijke proces en of het onschadelijk maken met succes werd uitgevoerd, kunt u er gewoon op klikken.

3.2.3. Processen toevoegen aan uitzonderingen

U kunt uitzonderingsregels configureren voor vertrouwde toepassingen zodat Advanced Threat Defense ze niet blokkeert als ze acties uitvoeren die op bedreigingen lijken.

Om processen toe te voegen aan de uitsluitingenlijst van Advanced Threat Defense:

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

2. In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
3. In de **Instellingen** venster, klik **Uitzonderingen beheren**.
4. Klik **+Voeg een uitzondering toe**.
5. Voer het pad in van de map die u wilt uitsluiten van scannen in het overeenkomstige veld.
   U kunt ook naar het uitvoerbare bestand navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer het bestand en klik op **OK**.
6. Schakel de schakelaar naast **Advanced Threat Defense** in.
7. Klik **Redden**.

3.2.4. Detectie van exploits

Een manier voor hackers om in te breken in systemen, is misbruik maken van specifieke bugs of kwetsbaarheden in computersoftware (toepassingen of plug-ins) en hardware. Om te garanderen dat uw apparaat vrij blijft van dergelijke aanvallen, die zich meestal heel snel verspreiden, maakt Bitdefender gebruik van de meest recente anti-exploittechnologieën.

3.2.5. Detectie van exploit in- en uitschakelen

Om detectie van exploits in en uit te schakelen:

- Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
- In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
- Ga naar het venster **Instellingen** en klik op de schakelaar naast **Detectie exploits** om de voorziening in of uit te schakelen.

> **Opmerking**
> De optie Detectie van exploits is standaard ingeschakeld.

3.3. Preventie van online bedreigingen

Bitdefender Online Threat Prevention garandeert een veilige surfervaring door u te waarschuwen over mogelijke kwaadaardige websites.

Bitdefender biedt realtime bescherming tegen online bedreigingen voor:

- Internet Explorer

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

Om de instellingen van Online Threat Prevention te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **ONLINE THREAT PREVENTION** op **Instellingen**.

In de secties **Webbescherming** klikt u op de aan-uitschakelaars voor:

- Web attack prevention blokkeert bedreigingen die via het internet binnenkomen, met inbegrip van drive-by downloads.
- 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 kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.

  Dit is een veilige pagina om te 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

- Versleutelde webscan.

Meer verfijnde aanvallen kunnen gebruik maken van beveiligd webverkeer om hun slachtoffers te misleiden. We raden u dan ook aan om de optie Versleutelde Webscan ingeschakeld te laten.

- Bescherming tegen fraude.
- Bescherming tegen phishing.

Scrol naar beneden tot u bij de sectie **Network Threat Prevention** komt. Hier vindt u de optie **Network Threat Prevention**. Houd deze optie ingeschakeld om uw apparaat te beschermen tegen aanvallen van complexe malware (zoals ransomware) op basis van kwetsbaarheden.

U kunt een lijst opmaken van websites, domeinen en IP-adressen die niet zullen worden gescand door de antibedreiging-, antiphishing- en antifraude-engines van Bitdefender. De lijst dient enkel de websites, domeinen en IP-adressen te bevatten die u volledig vertrouwt.

Om websites, domeinen en IP-adressen via de functie Online Threat Prevention van Bitdefender te configureren en te beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ONLINE BEDREIGINGSPREVENTIE** paneel, klik **Instellingen**.
3. Klik op **Uitzonderingen beheren**.
4. Klik **+Voeg een uitzondering toe**.
5. Voer in het overeenkomende veld de naam van de website of van het domein of het IP-adres in dat u wilt toevoegen aan de uitzonderingen.
6. Klik op de schakelaar naast **Online Threat Prevention**.
7. Om een item uit de lijst te verwijderen, klikt u op de knop ernaast. Klik **Redden** om de wijzigingen op te slaan en het venster te sluiten.

3.3.1. 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:

- Verlaat de website door te klikken op **BRENG ME TERUG NAAR EEN VEILIGE LOCATIE**.
- Ga ondanks de waarschuwing door met uw bezoek aan de website, door te klikken op **Ik begrijp de risico's; breng me toch naar de webpagina**.
- Als u zeker bent dat de gedetecteerde website veilig is, klikt u op **INDIENEN** om deze toe te voegen aan de uitzonderingen. We raden aan dat u enkel websites toevoegt die u volledig vertrouwt.

3.4. Kwetsbaarheid

Een belangrijke stap bij het beschermen van uw apparaat 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 apparaat 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 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.

3.4.1. Uw systeem scannen op kwetsbaarheden

Om kwetsbaarheden in het systeem te detecteren, vereist Bitdefender een actieve internetverbinding.

Om uw systeem op kwetsbaarheden te scannen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **KWETSBAARHEID** op **Openen**.

3. Klik in het tabblad **Kwetsbaarheidsscan** op **Scan starten** en wacht tot Bitdefender uw systeem controleert op kwetsbaarheden. De gedetecteerde kwetsbaarheden worden gegroepeerd in drie categorieën:

   - **BESTURINGSSYSTEEM**
     - **Beveiliging van het besturingssysteem**
       Gewijzigde systeeminstellingen die uw apparaat en gegevens zouden kunnen aantasten, zoals het niet weergeven van waarschuwingen wanneer uitgevoerde bestanden zonder uw toestemming wijzigingen uitvoeren op uw systeem, of wanneer MTP-apparaten zoals telefoons of camera's verbinding maken en verschillende bewerkingen uitvoeren zonder uw medeweten.
     - **Kritieke Windows updates**
       Er wordt een lijst weergegeven met kritieke Windows-updates die niet geïnstalleerd zijn op uw computer. Het is mogelijk dat u het systeem opnieuw moet opstarten, zodat Bitdefender de installatie kan voltooien. Het kan even duren voordat de updates geïnstalleerd zijn.
     - **Zwakke Windows-accounts**
       U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw apparaat en de beschermingsniveaus van de wachtwoorden. U kunt kiezen om de gebruiker te vragen het wachtwoord te wijzigen bij de volgende aanmelding of u kunt het wachtwoord zelf onmiddellijk wijzigen. Om een nieuw wachtwoord in te stellen voor uw systeem, selecteert u **Wachtwoord nu wijzigen**.
       Om een sterk wachtwoord te maken, raden we aan dat u een combinatie gebruikt van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).
   - **TOEPASSINGEN**
     - **Browserbeveiliging**
       Wijziging in de instellingen van uw apparaat, waardoor bestanden en programma's die zijn gedownload via Internet Explorer zonder integriteitsvalidering kunnen worden uitgevoerd. Dit kan ervoor zorgen dat uw apparaat wordt aangetast.
     - **Toepassingsupdates**

Om informatie te zien over de toepassing die moet worden bijgewerkt, klikt u erop in de lijst.
Als een toepassing niet up-to-date is, klikt u op **NIEUWE VERSIE DOWNLOADEN** om de laatste versie te downloaden.

- **NETWERK**
  - **Netwerk en Inloggegevens**
    Gewijzigde systeeminstellingen zoals het automatisch verbinden met open hotspot-netwerken zonder uw medeweten of het niet afdwingen van versleuteling van uitgaand beveiligd verkeer.
  - **Wi-Fi-netwerken en routers**
    Om meer te weten over het draadloze netwerk en de router waarmee u verbinding hebt gemaakt, klikt u erop in de lijst. Als het aanbevolen wordt dat u voor uw thuisnetwerk een sterker wachtwoord kiest, zorg dan dat u onze instructies volgt, zodat u verbonden kunt blijven zonder dat u zich zorgen hoeft te maken over uw privacy.
    Wanneer andere aanbevelingen beschikbaar zijn, volt u de instructies zodat u zeker bent dat uw thuisnetwerk veilig blijft tegen de indiscrete blikken van hackers.

3.4.2. 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 **Meldingen** in het navigatiemenu op 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:
   - Klik op **Installeren** als er Windows-updates beschikbaar zijn.

- Indien automatische Windows Update geïnactiveerd is klikt u op **Activeren**.
- Als een toepassing verouderd is, klikt u op **Nu updaten** om een link 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 veranderen** 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 ingesteld, klikt u op **Wachtwoord wijzigen** om naar de interface te gaan, waar u een sterk wachtwoord kunt instellen.
- Klik op **Wifi-instellingen wijzigen** indien het netwerk waarmee u verbonden bent, kwetsbaarheden heeft die uw systeem in gevaar kunnen brengen.

De controle-instellingen voor kwetsbaarheid configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.

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

3. Ga naar het tabblad **INSTELLINGEN**
4. Kies de systeemkwetsbaarheden die u regelmatig wilt controleren met de overeenkomende schakelaars.
   Windows updates
   Controleer of uw Windows-besturingssysteem over de laatste kritieke beveiligingsupdates van Microsoft beschikt.
   Applicatie-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.

Gebruikerswachtwoorden

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 @).

Autoplay

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

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.

3.4.3. 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 VPN** te gebruiken.

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

- **Thuis-wifi-netwerken**
- **Wifi-netwerken op kantoor**
- **Openbare wifi-netwerken**

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 **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Instellingen** en schakel de optie **Wifi Beveiligingsadviseur** in of uit.

Thuis-Wi-Fi-netwerk configureren

Uw thuisnetwerk beginnen configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Wifi Beveiligingsadviseur** en klik op **Thuis-wifi**.
4. Klik in het tabblad **Thuis-wifi** op **THUIS-WIFI 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**.

Om een nieuw draadloos netwerk als thuis-wifi toe te voegen, klikt u op **Nieuwe thuis-wifi selecteren**.

Wifinetwerk op kantoor configureren

Om uw kantoornetwerk te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Wifi Beveiligingsadviseur** en klik op **Kantoor-wifi**.
4. Klik in het tabblad **Kantoor-wifi** op **KANTOOR-WIFI SELECTEREN**.
   Er wordt een lijst weergegeven met de draadloze netwerken waarmee u tot nu toe verbinding hebt gemaakt.
5. Duid het netwerk van uw kantoor aan en klik op **SELECTEREN**.

Indien een netwerk voor kantoor als onbeveiligd of onveilig wordt beschouwd, worden configuratieaanbevelingen weergegeven om de beveiliging ervan te verbeteren.

Om het draadloze netwerk dat u als netwerk voor kantoor hebt ingesteld, te verwijderen, klikt u op **VERWIJDEREN**.

Om een nieuw draadloos netwerk als kantoor-wifi toe te voegen, klikt u op **Nieuwe kantoor-wifi selecteren**.

Openbare Wifi

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 ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Advanced Threat Defense is ingeschakeld
- De Bitdefender Firewall is ingeschakeld en de volgende instellingen zijn toegepast op uw draadloze adapter:

- Stealth-modus - AAN
- Netwerktype - Openbaar

- De volgende instellingen van Online Threat Prevention zijn ingeschakeld:
  - Versleutelde webscan
  - 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.

Informatie controleren over Wi-Fi-netwerken

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

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Wifi Beveiligingsadviseur**.
4. Afhankelijk van de informatie die u nodig hebt, selecteert u een van de drie tabbladen, **Thuis-wifi**, **Kantoor-wifi** of **Openbare wifi**.
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:

Wifi 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 te gebruiken.

Wifi is niet veilig - betekent dat het beveiligingsniveau van het netwerk matig is. Dit betekent dat het kwetsbaarheden kan bevatten, en het niet aanbevolen is 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 te gebruiken.

Wifi 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.

3.5. Ransomware-remediëring

Ransomware-remediëring van Bitdefender maakt een back-up van uw bestanden zoals documenten, afbeeldingen, video's of muziek, om te verzekeren dat ze worden beschermd tegen schade of verlies in geval van versleuteling door ransomware. Telkens een ransomware-aanval wordt gedetecteerd, blokkeert Bitdefender alle processen die in de aanval zijn betrokken en start het remediëringsproces op. Zo kunt u de inhoud van al uw bestanden herstellen, zonder het gevraagde losgeld te moeten betalen

3.5.1. De Ransomware-remediëring in- of uitschakelen

Om de Ransomware-remediëring in of uit te schakelen:

1. 1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Bescherming**.
2. Schakel de schakelaar in het paneel **RANSOMWARE-REMEDIËRING** in of uit.

> **Opmerking**
> Om te verzekeren dat uw bestanden tegen ransomware worden beschermd, raden we aan dat u Ransomware-remediëring ingeschakeld laat.

3.5.2. Automatisch herstellen in- of uitschakelen

Automatisch herstellen zorgt ervoor dat uw bestanden automatisch worden hersteld in geval van versleuteling door ransomware.

Om automatisch herstellen in of uit te schakelen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **RANSOMWARE-REMEDIËRING** op **Beheren**.
3. In het venster Instellingen schakelt u de schakelaar voor **Automatisch herstellen** in of uit.

3.5.3. Bestanden bekijken die automatisch werden hersteld

Wanneer de optie **Automatisch herstellen** ingeschakeld is, herstelt Bitdefender automatisch de bestanden die door ransomware werden versleuteld. Zo kunt u zorgeloos genieten van uw apparaat, want u weet dat uw bestanden veilig zijn.

Om bestanden te bekijken die automatisch werden hersteld:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd geremedieerd en klikt u op **Herstelde bestanden**.
   De lijst met herstelde bestanden wordt weergegeven. Hier kunt u ook de locatie waar uw bestanden werden hersteld, bekijken.

3.5.4. Versleutelde bestanden handmatig herstellen

Volg deze stappen indien u de bestanden die door ransomware werden versleuteld handmatig wilt herstellen:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd gedetecteerd en klikt u op **Versleutelde bestanden**.
3. De lijst met versleutelde bestanden wordt weergegeven.
   Klik op **Bestanden herstellen** om verder te gaan.
4. Indien een deel van of het gehele herstelproces mislukt, moet u de locatie kiezen waar de ontcijferde bestanden moeten worden bewaard.
   Klik op **LOCATIE VOOR HET HERSTEL** en kies een locatie op uw pc.
5. Er wordt een bevestigingsvenster weergegeven.
   Klik op **VOLTOOIEN** om het herstelproces te beëindigen.

Bestanden met de onderstaande extensies kunnen worden hersteld, indien ze worden versleuteld:

```
.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.
bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.d
b;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.htm;.htm
l;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.m
id;.midi;.mkv;.mp3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;
.ogg;.pdf;.pkg;.php;.pl;.png;.pps;.ppt;.pptx;.ps;.psd;.
py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.t
ex;.tif;.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.
wav;.wks;.wma;.wpl;.wps;.wpd;.wsf;.z;.zip;
```

3.5.5. Toepassingen aan uitzonderingen toevoegen

U kunt de uitzonderingsregels voor vertrouwde toepassingen configureren zodat de functie Ransomware-remediëring deze niet blokkeert wanneer ze handelingen uitvoeren die op ransomware lijken.

Om toepassingen toe te voegen aan de uitzonderingenlijst van Ransomware-remediëring:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **RANSOMWARE-OPLOSSING** paneel, klik **Beheren**.

3. Ga naar het venster **Uitzonderingen** en klik op **+Een uitzondering toevoegen**.

3.6. Anti-tracker

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

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

De Bitdefender-extensie is compatibel met de volgende webbrowsers:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

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

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

3.6.1. Interface van Anti-tracker

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

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

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

3.6.2. Bitdefender Anti-tracker uitschakelen

Om de Bitdefender Anti-tracker uit te schakelen:

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

- Vanuit deBitdefender-interface:
  1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in het deelvenster **ANTI-TRACKER** op **Instellingen**.
  3. Schakel de overeenstemmende schakelaar uit naast de webbrowser waarvoor u de extensie wenst uit te schakelen.

3.6.3. Toestaan dat een website aan tracking doet

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

1. Open uw webbrowser.
2. Klik op het symbool naast de zoekbalk.
3. Klik op de pictogram in de rechterbovenhoek.
4. Bent u op de website die u wilt toevoegen aan de uitzonderingen, klikt u op **Huidige website aan lijst toevoegen**.
   Wilt u een andere website toevoegen, voert u het adres in het bijhorende veld in en klikt u op .

3.7. VPN

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

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

3.7.1. VPN Installeren

De VPN-app kan als volgt geïnstalleerd worden vanaf uw Bitdefender-interface:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **VPN** op **VPN installeren**.
3. Lees de **Abonnementsovereenkomst** in het venster met de beschrijving van de VPN-app en klik vervolgens op **BITDEFENDER VPN INSTALLEREN**.
   Wacht even totdat de bestanden gedownload en geïnstalleerd zijn.
   Als een andere VPN-toepassing wordt gedetecteerd, bevelen we aan dat u deze de-installeert. Door meerdere VPN-oplossingen te hebben, kan het systeem vertraging oplopen of kunnen er problemen ontstaan met de functionaliteit.
4. Klik op **BITDEFENDER VPN OPENEN** om het installatieproces af te ronden.

   Opmerking
   Voor de installatie van Bitdefender VPN is .Net Framework 4.5.2 of hoger noodzakelijk. Indien dit pakket niet geïnstalleerd is, verschijnt een notificatiescherm. Klik op **installeer .Net Framework** om naar een pagina te gaan waar u de nieuwste versie van deze software kunt downloaden.

3.7.2. VPN Openen

Volg een van de volgende methoden om naar de hoofdinterface van Bitdefender VPN te gaan:

- Vanuit het systeemvak
  1. Rechtsklik op het pictogram in het systeemvak en klik vervolgens op **Tonen**.
- Vanuit deBitdefender-interface
  1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in het deelvenster **VPN** op **VPN openen**.

3.7.3. VPN-interface

De VPN-interface geeft de status van de app weer: verbonden of niet verbonden. Voor gebruikers met de gratis versie stelt Bitdefender de serverlocatie automatisch in op de meest geschikte server. Premium-gebruikers hebben de mogelijkheid de serverlocatie waarmee ze wensen

te verbinden, te wijzigen. Voor meer informatie over VPN-abonnementen, raadpleeg Abonnementen (pagina 87).

Om te verbinden of om de verbinding te verbreken: klik op de status die bovenaan het scherm wordt weergeven of rechtsklik op het icoon systeemvak. Het icoon systeemvak geeft een groen vinkje weer wanneer de VPN verbonden is, en een rood vinkje wanneer de verbinding verbroken is.

Tijdens de verbinding worden de verstreken tijd en de gebruikte bandbreedte weergegeven op het onderste gedeelte van de interface.

Om het **Menu** gebied volledig te zien, klikt u op het pictogram ☰ linksboven. U hebt hier de volgende opties:

- **Mijn Account** - geeft details weer over uw Bitdefender-account en VPN-abonnement. Klik op **Account Wisselen** indien u met een andere account wenst in te loggen.
  Klik op **Hier toevoegen** om een activeringscode voor Bitdefender Premium VPN toe te voegen.
- **Instellingen** – u kunt het gedrag van uw product aanpassen naargelang uw noden. De instellingen zijn gegroepeerd in twee categorieën:
  - **Algemeen**
    - Meldingen
    - Opstarten - kies of Bitdefender VPN bij het opstarten wordt uitgevoerd of niet
    - Productrapporten - dien anonieme productrapporten in om ons te helpen uw ervaring te verbeteren
    - Donkere modus
    - Taal
  - **Geavanceerd**
    - Internet Kill-Switch - deze voorziening onderbreekt tijdelijk al het internetverkeer indien de VPN-verbinding onbedoeld wordt verbroken. Zodra u terug online bent, wordt de verbinding opnieuw tot stand gebracht.

- Autoconnect - Verbind Bitdefender VPN automatisch wanneer u een openbaar of niet-beveiligd wifinetwerk gebruikt of wanneer een app voor peer-to-peer-bestandsuitwisseling wordt gestart

- **Ondersteuning** - u hebt toegang tot ons platform Ondersteuningscentrum, waar u artikels kunt lezen over hoe u Bitdefender VPN gebruikt of over hoe u ons feedback kunt sturen.
- **Over deze versie** - informatie over de geïnstalleerde versie.

3.7.4. Abonnementen

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

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

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

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

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

3.8. 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 ™ is in de eerste plaats een beveiligde browser, een verzegelde omgeving, ontworpen om uw internetbankieren, e-shopping en andere soorten online transacties privé en veilig te houden.

Voor de beste privacybeveiliging werd Bitdefender Password Manager geïntegreerd in Bitdefender Safepay™ om uw identificatiegegevens te beveiligen wanneer u naar persoonlijke online locaties gaat. Zie Beveiliging Wachtwoordbeheerder voor uw gegevens voor meer informatie.

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 apparaat 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™.

3.8.1. Bitdefender Safepay™ gebruiken

Standaard detecteert Bitdefender wanneer u naar een online banksite of online winkel in een willekeurige browser op uw apparaat 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 **Privacy** in het navigatiemenu op de Bitdefender-interface.

2. Klik in het deelvenster **SAFEPAY** op **Instellingen**.
3. Klik in het venster **Safepay** op **Safepay starten**.

- 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** en **Windows 11**:
    Voer "Bitdefender Safepay™" in het zoekveld in de taakbalk in en klik op de icoon ervan.

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 BitdefenderSafepay™ **instellingen** door te klikken op en te kiezen voor **Instellingen**.
- beveilig uw wachtwoorden met **Wachtwoordbeheerder** door te klikken op .
- beheer uw **favorieten** door te klikken op ☆ naast de adresbalk.
- open het virtuele toetsenbord door te klikken op .
- vergroot of verklein de browserafmetingen door gelijktijdig te drukken op de toetsen **Ctrl** en **+/-** op het numerieke toetsenbord.

- bekijk informatie over uw Bitdefender-product door te klikken op ⋯ en **Over** te kiezen.
- druk belangrijke informatie af door te klikken op ⋯ en **Afdrukken** te kiezen.

> **Opmerking**
> Om tussen Bitdefender Safepay™ en Windows-bureaublad te wisselen, drukt u op de toetsen **Alt+Tab** of klikt u in de linkerbovenhoek van het venster op de optie **Wisselen naar Bureaublad**.

3.8.2. Instellingen configureren

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

Regels voor Bitdefender Safepay toepassen voor domeinen die worden geopend

De websites die u hebt toegevoegd aan **Bladwijzers** met de optie **Automatisch openen in Safepay** ingeschakeld, verschijnen hier. Wilt u het automatisch openen met Bitdefender Safepay™ opheffen voor een website uit de lijst, klikt u op × naast het gewenste item in de kolom **Verwijderen**.

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.

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.

Klik op **IMPORTEREN** en volg de wizard om de certificaten te gebruiken in Bitdefender Safepay™.

Virtueel toetsenbord gebruiken

Het Virtuele toetsenbord verschijnt automatisch wanneer een wachtwoordveld wordt geselecteerd.

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

Bevestiging afdrukken

Activeer deze optie indien u uw bevestiging wenst te geven voordat het afdrukproces start.

3.8.3. 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 ⋯ en kies **Favorieten** 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. Geef de URL en de titel van de bladwijzer in en klik vervolgens 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.

3.8.4. Safepay-notificaties uitschakelen

Bitdefender-product is zo ingesteld dat u via een pop-up op de hoogte wordt gebracht wanneer een website voor internetbankieren wordt gedetecteerd.

Om Safepay-notificaties uit te schakelen:

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

2. In de **VEILIG** paneel, klik **Instellingen**.
3. In het venster **Instellingen** schakelt u de schakelaar naast **Safepay-notificaties** in.

3.8.5. VPN met Safepay gebruiken

Het Bitdefender-product kan zo worden ingesteld dat de VPN-app automatisch samen met Safepay wordt opgestart, zodat u uw online betalingen ook op netwerken die niet zijn beveiligd, in een veilige omgeving kunt uitvoeren.

Om de VPN-app samen met Safepay te gebruiken:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VEILIG** paneel, klik **Instellingen**.
3. In het venster **Instellingen** schakelt u de schakelaar naast **VPN gebruiken met Safepay** in.

3.9. Bitdefender USB Immunizer

De Autorun-functie die is ingebouwd in Windows-besturingssystemen is een heel handig hulpmiddel waardoor apparaten automatisch een bestand kunnen uitvoeren vanaf media die zijn verbonden met deze apparaten. Software-installaties bijvoorbeeld kunnen automatisch starten als er een cd in de cd-lezer wordt geschoven.

Helaas kan deze functie ook worden gebruikt door bedreigingen om automatisch te starten en zo in uw apparaat 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 bedreigingen uitvoert. Zodra een USB-apparaat immuun is gemaakt, kunnen bedreigingen het niet langer configureren om een bepaalde toepassing uit te voeren wanneer het apparaat wordt verbonden met een Windows-apparaat.

Om een USB-apparaat te immuniseren:

1. Verbind de USB-stick met uw apparaat.

2. Blader op uw apparaat 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 dreigingen** in plaats van de optie Immuniseren.

Om te voorkomen dat uw apparaat bedreigingen start vanaf USB-apparaten die niet immuun zijn gemaakt, kunt u de media autorun-functie uitschakelen. Zie De automatische kwetsbaarheidsbewaking gebruiken (pagina 73) voor meer informatie.

4. NUTSVOORZIENINGEN

4.1. 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:

- werk profiel
- Film profiel
- Spelprofiel
- **Openbaar wifi-profiel**
- Batterijmodusprofiel

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.
- De Antispamkenmerk is ingeschakeld.
- **Search Advisor** is uitgeschakeld.
- Meldingen bijzondere aanbiedingen 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 ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Geavanceerde bescherming tegen bedreigingen is ingeschakeld
- De Bitdefender Firewall is ingeschakeld en de volgende instellingen worden toegepast op uw draadloze adapter:
  - Stealth-modus - AAN
  - Netwerktype - Openbaar
- De volgende instellingen van Online Threat Prevention zijn ingeschakeld:
  - Versleutelde webscan
  - Bescherming tegen fraude
  - Bescherming tegen phishing

4.1.1. 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 **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.

4. 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
5. 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 opstart, kunt u de toepassing handmatig toevoegen aan de **Werktoepassingenlijst**.

Om toepassingen handmatig toe te voegen aan de Werktoepassingenlijst in Werkprofiel:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de **CONFIGUREREN** knop in het gebied Werkprofiel.
4. Klik in het venster **Instellingen Werkprofiel** op **Toepassingenlijst**.
5. Klik op **TOEVOEGEN**.
   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.

4.1.2. 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 **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
4. Kies de systeemaanpassingen die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor videospelers boosten
   - Productinstellingen voor Filmprofiel optimaliseren
   - Stel achtergrondprogramma's en onderhoudstaken uit
   - Stel automatische Windows-updates uit
   - Instellingen vermogensplan voor films afstellen.
5. Klik **REDDEN** 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 **Filmtoepassingenlijst**.

Om videospelers handmatig toe te voegen aan de Filmtoepassingenlijst in Filmprofiel:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de **CONFIGUREREN** knop in het gebied Filmprofiel.
4. Klik in het venster **Instellingen Filmprofiel** op **Spelerslijst**.
5. Klik **TOEVOEGEN**.
   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de app, selecteer het en klik **OK** om het aan de lijst toe te voegen.

4.1.3. 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 **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **Configureren** in het gebied Gameprofiel.
4. Kies de systeemaanpassingen die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor games boosten
   - Productinstellingen voor Gameprofiel optimaliseren
   - Stel achtergrondprogramma's en onderhoudstaken uit
   - Stel automatische Windows-updates uit
   - Instellingen vermogensplan voor games afstellen.
5. Klik **REDDEN** 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 **Gametoepassingenlijst**.

Om games handmatig aan de Gametoepassingenlijst toe te voegen in het Gameprofiel:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de **Configureren** knop in het spelprofielgebied.
4. Klik in het venster **Instellingen Gameprofiel** op **Spellijst**.
5. Klik **TOEVOEGEN**.

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.

4.1.4. Openbaar Wifi-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 Wifi-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 te configureren zodat productinstellingen worden toegepast wanneer u verbonden bent met een onveilig draadloos netwerk:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Openbaar Wi-Fi-profiel.
4. Laat het vakje **Pas de productinstellingen aan om de bescherming te stimuleren bij verbinding met een onveilig openbaar Wi-Fi-netwerk** aangevinkt.
5. Klik **Redden**.

4.1.5. Profiel Accumodus

Het profiel Accumodus is speciaal ontworpen voor laptop- en tabletgebruikers. Het doel ervan is om de invloed op vermogensverbruik van zowel het 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 **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.

3. Klik op de knop **Configureren** in het gebied Profiel Accumodus.
4. 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.
5. Klik **REDDEN** 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 Automatic Update is uitgesteld.
- Geplande scans worden uitgesteld.

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.

4.1.6. Realtime 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 **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.

2. In de **profielen** tabblad, klik **Instellingen**.
3. Verrol naar beneden tot u de optie Optimalisatie in reële tijd ziet, en gebruik vervolgens de bijhorende schakelaar om deze in of uit te schakelen.

4.2. Data bescherming

4.2.1. 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.

De Bitdefender File Shredder helpt u gegevens permanent te verwijderen door ze fysiek van uw harde schijf te verwijderen.

Volg deze stappen om bestanden of mappen snel permanent verwijderen van uw apparaat 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. Klik op **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.
   Wacht tot Bitdefender klaar is met het versnipperen van de bestanden.
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 **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **Gegevensbeveiliging** op **Bestandsvernietiging**.
3. Volg de wizard Bestandsvernietiging:
   a. Klik op de knop **MAPPEN 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 **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.

Wacht tot Bitdefender klaar is met het versnipperen van de bestanden.

c. **Overzicht van resultaten**
De resultaten worden weergegeven. Klik **Finish** om de wizard af te sluiten.

5. ZO WERKT HET

5.1. Installatie

5.1.1. Hoe installeer ik Bitdefender op een tweede apparaat?

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

Om Bitdefender op een tweede apparaat te installeren:

1. Klik op **Installeren op ander apparaat** in de linkerbenedenhoek van de **Bitdefender-interface**.
   Er verschijnt een nieuw venster op uw scherm.
2. Klik **DEEL DE DOWNLOADLINK**.
3. Volg de aanwijzingen op het scherm om Bitdefender te installeren.

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

5.1.2. Hoe kan ik Bitdefender opnieuw installeren?

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

- u hebt het besturingssysteem opnieuw geïnstalleerd..
- u wilt problemen oplossen die mogelijk voor vertragingen en crashes hebben gezorgd
- uw Bitdefender-product start of werkt niet naar behoren.

In het geval dat een van de vermelde situaties op u van toepassing is, volg dan deze stappen:

- In **Windows 7**:
  1. Klik **Begin** en ga naar **Alle programma's**.
  2. Zoek *Bitdefender Antivirus Plus* en selecteer **De-installeren**.
  3. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  4. U moet de apparaat 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 **De-installeren** of **Programma's en Functies**.
  3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  4. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  5. U moet het apparaat opnieuw opstarten om het proces te voltooien.
- In **Windows 10** En **Windows 11**:
  1. Klik op **Start**, klik dan op **Instellingen**.
  2. Klik op het **Systeem**-pictogram in Instellingen, selecteer dan **Apps & functies**.
  3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **HERINSTALLEREN**.
  6. U moet het apparaat opnieuw opstarten om het proces te voltooien.

> **Opmerking**
> Als u deze procedure voor opnieuw installeren volgt, worden persoonlijke instellingen opgeslagen, die in het nieuw geïnstalleerde product ook beschikbaar blijven. Andere instellingen kunnen teruggesteld worden naar hun fabrieksconfiguratie.

5.1.3. Waar kan ik mijn Bitdefender-product downloaden?

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

> **Opmerking**
> Voordat u de kit uitvoert, raden we aan om beveiligingsoplossingen die op uw systeem zijn geïnstalleerd, te verwijderen. Wanneer u meer dan één beveiligingsoplossing op dezelfde apparaat gebruikt, wordt het systeem onstabiel.

Om Bitdefender te installeren vanuit Bitdefender Central:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel en klik vervolgens op **INSTALLEER BESCHERMING**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
   - **Bescherm andere apparaten**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
     Klik **STUUR DOWNLOADLINK**. Typ een e-mailadres in het overeenkomstige veld en klik **STUUR E-MAIL**. Houd er rekening mee dat de gegenereerde downloadlink alleen de komende 24 uur geldig is. Als de link verloopt, moet u een nieuwe genereren door dezelfde stappen te volgen.
     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en klik vervolgens op de overeenkomstige downloadknop.
4. Start het gedownloade Bitdefender-programma.

5.1.4. 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 Bitdefender-versie gebruikt, kunt u gratis upgraden naar de nieuwste Bitdefender, als volgt:

- 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.
  Installeer het product in dit geval opnieuw door de volgende stappen te volgen:
  - In **Windows 7**:
    1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
    2. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
    3. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
       Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.
  - In **Windows 8** En **Windows 8.1**:
    1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
    2. Klik op **Een programma de-installeren** of **Programma's en Functies**.
    3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
    4. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
       Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.
  - In **Windows 10** En **Windows 11**:
    1. Klik **Begin**, dan klikken **Instellingen**.
    2. Klik in het gebied Instellingen op het pictogram **Systeem** en selecteer dan **Apps**.
    3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.

4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
5. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
6. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
   Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.

> **Opmerking**
> Door deze herinstallatieprocedure te volgen, worden aangepaste instellingen opgeslagen en beschikbaar in het nieuw geïnstalleerde product. Andere instellingen kunnen worden teruggeschakeld naar hun standaardconfiguratie.

- 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. Toegang Bitdefender Centraal.
     b. Selecteer de **Mijn apparaten** paneel en klik vervolgens op **INSTALLEER BESCHERMING**.
     c. Kies een van de twee beschikbare opties:
        - **Bescherm dit apparaat**
          Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
        - **Een ander apparaat beschermen**
          Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
          Klik **STUUR DOWNLOADLINK**. Typ een e-mailadres in het overeenkomstige veld en klik **STUUR E-MAIL**. Houd er rekening mee dat de gegenereerde downloadlink alleen de komende 24 uur geldig is. Als de link verloopt, moet u een nieuwe genereren door dezelfde stappen te volgen.

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

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

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

5.1.5. Hoe kan ik upgraden naar de recentste Bitdefender-versie?

Vanaf nu kunt u naar de nieuwste versie upgraden zonder de handmatige de-installatie- en installatie-procedures te volgen. Het nieuwe product, wordt meer bepaald samen met nieuwe functies en ingrijpende verbeteringen in het product, geleverd via productupdate en als u al een actieve Bitdefender-abonnement hebt, wordt het product automatisch geactiveerd.

Indien u de versie van 2020 gebruikt, kunt u naar de nieuwste versie upgraden aan de hand van de volgende stappen:

1. Klik op **NU OPNIEUW OPSTARTEN** in de kennisgeving die u ontvangt met de upgrade-informatie. Als u deze gemist hebt, ga naar het venster **Kennisgevingen**, ga naar de recentste update en klik vervolgens op de knop **NU OPNIEUW OPSTARTEN**. Wacht totdat het apparaat opnieuw is opgestart.
   Het venster **Wat is er nieuw** verschijnt, met informatie over de verbeterde en nieuwe functies.
2. Klik op de koppelingen **Meer weten** om doorgestuurd te worden naar de specifieke pagina, met meer informatie en nuttige artikels.
3. Sluit het venster **Wat is er nieuw** om naar de interface van de nieuw geïnstalleerde versie te gaan.

Gebruikers die gratis willen upgraden van Bitdefender 2016 of een lagere versie naar de nieuwste Bitdefender-versie moeten hun huidige versie verwijderen uit het controlepaneel en vervolgens het recentste installatiebestand downloaden via de Bitdefender-website op het volgende adres: https://www.bitdefender.com/Downloads/. De activatie is enkel mogelijk met een geldig abonnement.

5.2. Bitdefender Centraal

5.2.1. Hoe meldt u zich met een andere account aan voor Bitdefender-account?

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

Om succesvol in te loggen met een andere Bitdefender-account:

1. Klik op uw accountnaam in het bovenste gedeelte van de **Bitdefender-interface**.
2. Klik in de rechterbovenhoek van het scherm op **Account wisselen** om de account gelinkt aan de apparaat te wisselen.
3. Typ het e-mailadres in het overeenkomstige veld en klik vervolgens op **VOLGENDE**.
4. Typ uw wachtwoord en klik vervolgens 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 (pagina 151).

5.2.2. 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. Toegang Bitdefender Centraal.
2. Klik op de pictogram in de rechterbovenhoek van het scherm.
3. Klik op **Mijn account** in het schuifmenu.
4. Klik op **Instellingen** in het schuifmenu.
5. Schakel de optie **Hulpberichten in/uitschakelen** uit.

5.2.3. 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:

- Van de Bitdefender-interface:
  1. Klik **Mijn rekening** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in de rechterbovenhoek van het scherm op **Account wisselen**.
     Er verschijnt een nieuw venster.
  3. Voer uw e-mailadres in en klik op **VOLGENDE**.
     Er verschijnt een nieuw venster.
  4. Klik **Wachtwoord vergeten?**.
  5. Klik op **VOLGENDE**.
  6. Controleer uw e-mailaccount, typ de beveiligingscode die u hebt ontvangen en klik vervolgens op **VOLGENDE**.
     U kunt ook klikken **Verander wachtwoord** in de e-mail die we u hebben gestuurd.
  7. Typ het nieuwe wachtwoord dat u wilt instellen en typ het nogmaals. Klik **REDDEN**.

- Vanuit uw webbrowser:
  1. Ga naar: https://central.bitdefender.com.
  2. Klik op **AANMELDEN**.
  3. Typ uw e-mailadres en klik vervolgens op **VOLGENDE**.
  4. Klik **Wachtwoord vergeten?**.
  5. Klik **VOLGENDE**.
  6. Controleer uw e-mailaccount en volg de instructies om een nieuw wachtwoord in te stellen voor uw Bitdefender-account.

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

5.2.4. 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. Toegang Bitdefender Centraal.
2. Klik op de pictogram in de rechterbovenhoek van het scherm.
3. Klik op **Instellingen** in het schuifmenu.
4. Selecteer in het gebied **Actieve sessies** de optie **AFMELDEN** naast het apparaat waar u de aanmeldsessie wenst stop te zetten.

5.3. Scannen met BitDefender

5.3.1. 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 apparaat kopieert.

5.3.2. Hoe kan ik mijn systeem scannen

Om een volledige scan van het systeem uit te voeren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik op de knop **Scan uitvoeren** naast **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. Zie voor meer informatie.

5.3.3. Hoe plan ik een scan?

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

Een scan plannen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het onderste gedeelte van de interface op ··· naast het scantype dat u wilt inplannen, Systeemscan of Snelle scan, en selecteer vervolgens **Bewerken**.
   U kunt ook een scantype maken dat bij uw noden past, door te klikken op **+Scan aanmaken** naast **Scans beheren**.
4. Pas de scan aan in overeenkomst met uw noden, en klik op **Volgende**.
5. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan.
   Selecteer een van de overeenkomstige opties om een planning in te stellen:
   - Bij het opstarten van het systeem
   - Dagelijks
   - Wekelijks
   - Maandelijks

   Als u Dagelijks, Maandelijks of Wekelijks kiest, sleept u de schuifregelaar langs de schaal om de gewenste periode in te stellen wanneer de geplande scan moet starten.

Het venster **Scantaak** verschijnt als u ervoor kiest een nieuwe aangepaste scan aan te maken. Hier kunt u de locaties selecteren die u wilt laten scannen.

5.3.4. Een aangepaste scantaak maken

Als u specifieke locaties wilt scannen op uw apparaat 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. In de **ANTIVIRUS** paneel, klik **Open**.
2. Klik op **+Scan aanmaken** naast **Scans beheren**.
3. Voer in het veld Taaknaam een naam in voor de scan, selecteer vervolgens de locaties die u wilt laten scannen en klik op **VOLGENDE**.
4. Configureer deze algemene opties:
   - **Scan alleen toepassingen**. U kunt Bitdefender instellen om alleen geopende apps te scannen.
   - **Prioriteit scantaak**. U kunt kiezen welke impact een scanprocedure mag hebben op de prestaties van uw systeem.
     - Auto - De prioriteit van het scanproces hangt af van de systeemactiviteit. Om ervoor te zorgen dat het scanproces geen invloed heeft op de systeemactiviteit, zal Bitdefender beslissen of het scanproces met hoge of lage prioriteit moet worden uitgevoerd.
     - Hoog - De prioriteit van het scanproces is hoog. Door deze optie te kiezen, laat u andere programma's langzamer werken en verkort u de tijd die nodig is om het scanproces te voltooien.
     - Laag - De prioriteit van het scanproces is laag. Door deze optie te kiezen, kunt u andere programma's sneller laten werken en zal het scanproces langer duren.
   - **Acties na het scannen**. Kies welke actie Bitdefender moet ondernemen als er geen bedreigingen zijn gevonden:
     - Samenvattingsvenster tonen
     - Apparaat uitschakelen

- Sluit het scanvenster

5. Als u de scanopties in detail wilt configureren, klikt u op **Geavanceerde opties weergeven**.
   Klik **Volgende**.
6. U kunt de optie **Scantaak inplannen** inschakelen als u dat wenst. Vervolgens kiest u wanneer de aangepaste taak die u hebt gemaakt, moet worden gestart.
   - Bij het opstarten van het systeem
   - Dagelijks
   - Maandelijks
   - Wekelijks

   Als u Dagelijks, Maandelijks of Wekelijks kiest, sleept u de schuifregelaar langs de schaal om de gewenste periode in te stellen wanneer de geplande scan moet starten.
7. Klik **Redden** om de instellingen op te slaan en het configuratievenster te sluiten.
   Afhankelijk van de te scannen locaties kan de scan even duren. Als er tijdens het scanproces bedreigingen worden gevonden, wordt u gevraagd om de acties te kiezen die op de gedetecteerde bestanden moeten worden ondernomen.

Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

5.3.5. Hoe sluit ik een map uit 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.

Om een map toe te voegen aan de Uitzonderingenlijst:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik op het tabblad **Instellingen**.
4. Klik op **Uitzonderingen beheren**.
5. Klik **+Voeg een uitzondering toe**.
6. Voer het pad in van de map die u wilt uitsluiten van scannen in het overeenkomstige veld.
   U kunt ook naar de map navigeren door op de bladerknop aan de rechterkant van de interface te klikken, deze te selecteren en op te klikken **OK**.
7. Zet de schakelaar aan naast de beveiligingsfunctie die de map niet mag scannen. Er zijn drie opties:
   - Antivirus
   - Preventie van online bedreigingen
   - Geavanceerde bescherming tegen bedreigingen
8. Klik **Redden** om de wijzigingen op te slaan en het venster te sluiten.

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

Er kunnen zich gevallen voordoen waarin Bitdefender een legitiem bestand ten onrechte als een bedreiging labelt (een vals positief). Om deze fout te corrigeren, voegt u het bestand toe aan het gebied van de Bitdefender-uitzonderingen:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. Schakel in het venster **Geavanceerd Bitdefender Shield** uit.

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. Om te weten hoe u dit kunt doen, ga naar Verborgen objecten weergeven in Windows (pagina 126).
3. Het bestand herstellen vanaf het quarantainegebied:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. Ga naar het venster **Instellingen** op klik op **Quarantaine beheren**.
   d. Selecteer het bestand en klik op **HERSTEL**.
4. Voeg het bestand toe aan de Uitzonderingenlijst.
5. Schakel de real time antivirusbeveiliging van Bitdefender in.
6. Neem contact op met de medewerkers van onze ondersteuningsdienst zodat wij de detectie van de update van de bedreigingsinformatie kunnen verwijderen. Om te weten hoe u dit kunt doen, ga naar Hulp vragen (pagina 151).

5.3.7. Hoe kan ik controleren welke bedreigingen 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.

U kunt het scanlogboek rechtstreeks vanuit de scanwizard openen, zodra de scan is voltooid, door op te klikken **TOON LOGBOEK**.

Een scanlogboek of een gedetecteerde infectie op een later tijdstip controleren:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In de **Alle** selecteer op het tabblad de melding over de laatste scan.

Hier kunt u alle bedreigingsscangebeurtenissen vinden, inclusief bedreigingen die zijn gedetecteerd door scannen bij toegang, door de gebruiker gestarte scans en statuswijzigingen voor automatische scans.

3. In de notificatielijst kunt u zien welke scans recentelijk zijn uitgevoerd. Klik op een melding om er details over te bekijken.
4. Klik op **Logboek weergeven** om het scanlogboek te openen.

5.4. Privacybeheer

5.4.1. 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 enige andere vertrouwelijke gegevens die u mogelijk invoert wanneer u verschillende online locaties bezoekt, te beschermen.

Uw online activiteit veilig en privé houden:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VEILIG** paneel, klik **Instellingen**.
3. In de **Veilig betalen** venster, klik **Start Safepay**.
4. Klik op de knop om het **Virtuele toetsenbord** te openen.
   Gebruik het **virtuele toetsenbord** wanneer u vertrouwelijke informatie, zoals uw wachtwoorden, invoert.

5.4.2. Wat kan ik doen als mijn apparaat gestolen is?

Diefstal van mobiele apparaten, of het nu om een smartphone, tablet of laptop gaat, is een van de belangrijkste problemen tegenwoordig die particulieren en organisaties over de hele wereld treft.

Met Bitdefender Antidiefstal kunt u niet alleen het gestolen apparaat zoeken en vergrendelen, maar kunt u ook alle gegevens wissen om zeker te zijn dat ze niet worden gebruikt door de dief.

Naar de antidiefstalfuncties gaan vanaf uw account:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Klik op de gewenste toestelkaart en selecteer vervolgens **Antidiefstal**.
4. Selecteer de functie die u wilt gebruiken:
   - **LOKALISEREN** - geef de lokatie van uw apparaat weer op Google Maps.
     Toon IP - geeft het laatste IP-adres voor het geselecteerde apparaat weer.
   - **Waarschuwing** - een waarschuwing op het apparaat verzenden.
   - **Vergrendelen** - vergrendel uw apparaat en stel een numerieke pincode in om het te ontgrendelen. U kunt ook de overeenstemmende optie inschakelen om Bitdefender toe te staan snapshots te maken van de persoon die toegang probeert te krijgen tot uw apparaat.
   - **Wissen** - alle gegevens van uw apparaat verwijderen.

     Belangrijk
     Nadat u een apparaat hebt gewist, werken de functies van Anti-Theft niet langer.

5.4.3. 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.

Met de Bestandsvernietiger van Bitdefender kunt u bestanden of mappen op uw apparaat snel versnipperen met het contextmenu van Windows, door de volgende stappen te volgen:

1. Klik met de rechtermuisknop op het bestand of de map die u definitief wilt verwijderen, wijs Bitdefender aan en selecteer **Bestandsvernietiging**.
2. Klik **permanent verwijderen**en bevestig vervolgens dat u door wilt gaan met het proces.

Wacht tot Bitdefender klaar is met het versnipperen van de bestanden.

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

5.4.4. Hoe zorg ik ervoor dat mijn webcam niet gehackt wordt?

U kunt uw Bitdefender-product zo instellen dat u de toegang van geïnstalleerde toepassingen tot uw webcam kunt weigeren of toestaan. Volg hiervoor deze stappen:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Ga naar het venster **Webcambescherming**. U ziet er een lijst met de apps die toegang tot uw camera hebben verzocht.
4. Wijs op de app die u wilt toestaan of waarvoor u de toegang wilt weigeren, en klik vervolgens op de schakelaar ernaast, voorgesteld door een videocamera.

   Klik op het pictogram om te zien wat de andere Bitdefender-gebruikers met de geselecteerde app hebben gedaan. U wordt gewaarschuwd telkens wanneer een van de vermelde apps wordt geblokkeerd door de Bitdefender-gebruikers.

Om manueel toepassingen aan deze lijst toe te voegen, klikt op de knop **Toepassing toevoegen** en selecteert u een van beide opties.

- Van Windows Store
- Van uw apps

5.4.5. Hoe kan ik versleutelde bestanden handmatig herstellen wanneer het herstelproces faalt?

Indien de versleutelde bestanden niet automatisch worden hersteld, kunt u ze handmatig herstellen aan de hand van de volgende stappen:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In de **Alle** Selecteer op het tabblad de melding over het laatste gedetecteerde ransomware-gedrag en klik vervolgens op **Versleutelde bestanden**.

3. De lijst met de versleutelde bestanden wordt weergegeven.
   Klik op **BESTANDEN HERSTELLEN** om verder te gaan.
4. Als het gehele of een deel van het herstelproces mislukt, moet u de locatie kiezen waar de gedecodeerde bestanden moeten worden opgeslagen. Klik **Locatie herstellen**en kies vervolgens een locatie op uw pc.
5. Er verschijnt een bevestigingsvenster.
   Klik **Finish** om het herstelproces te beëindigen.

Bestanden met de volgende extensies kunnen worden hersteld als ze versleuteld worden:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

5.5. Nuttige informatie

5.5.1. Hoe test ik mijn beveiligingsoplossing?

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 beveiligingsoplossing controleren met een veilig bestand dat hiervoor is ontwikkeld.

Om uw beveiligingsoplossing te 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 worden geïnformeerd dat de pagina die u probeert te bezoeken het EICAR-Testbestand bevat (geen bedreiging).

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 bedreiging 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 (pagina 151).

5.5.2. Hoe kan ik Bitdefender verwijderen?

Als u uw {1}{2} wilt verwijderen:

- In **Windows 7**:
  1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
  2. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  4. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Een programma verwijderen** of **Programma's en functies**.
  3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  4. Klik **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:
  1. Klik op {1}Start{2}, klik dan op Instellingen.
  2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Apps**.
  3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.

4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
5. Klik **VERWIJDEREN** in het venster dat verschijnt.
6. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

> **Opmerking**
> Deze procedure voor opnieuw installeren verwijdert uw persoonlijke instellingen permanent.

5.5.3. Hoe kan ik Bitdefender VPN verwijderen?

De procedure om Bitdefender VPN te verwijderen, is vergelijkbaar met de procedure om andere programma's van uw computer te verwijderen:

- In **Windows 7**:
  1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
  2. Zoek **Bitdefender VPN** en selecteer **De-installeren**.
     Wacht tot de de-installatieproces is voltooid.
- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Verwijderen** een programma of **Programma's en functies**.
  3. Vinden **Bitdefender-VPN** en selecteer **Verwijderen**.
     Wacht tot het verwijderingsproces is voltooid.
- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**en klik vervolgens op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. Vinden **Bitdefender-VPN** en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
     Wacht tot het verwijderingsproces is voltooid.

5.5.4. Hoe verwijder ik de extensie Anti-tracker van Bitdefender?

Afhankelijk van de webbrowser die u gebruikt, volgt u deze stappen om de extensie Anti-tracker van Bitdefender te de-installeren:

- Internet Explorer
  1. Klik op naast de zoekbalk en selecteer Uitbreidingen beheren. Er verschijnt een lijst van de geïnstalleerde extensies.
  2. Klik op Anti-tracker van Bitdefender.
  3. Klik rechtsonder op **Uitschakelen**.
- Google Chrome
  1. Klik op naast de zoekbalk.
  2. Selecteer **Meer extra** en vervolgens **Extensies**.
     Er verschijnt een lijst van de geïnstalleerde extensies.
  3. Klik op **Verwijderen** in de kaart Anti-tracker van Bitdefender.
  4. Klik op **Verwijderen** in de pop-up die verschijnt.
- Mozilla Firefox
  1. Klik naast de zoekbalk.
  2. Selecteer **Uitbreidingen** en vervolgens **Extensies**.
     Er verschijnt een lijst met de geïnstalleerde extensies.
  3. Klik op en selecteer **Verwijderen**.

5.5.5. Hoe kan ik de apparaat 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 bedreigingen. Het scannen van de volledige apparaat kan langer duren, afhankelijk van de hardware- en softwareconfiguratie van uw systeem.

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

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

Om de apparaat uit te schakelen wanneer Snelle scan of Systeemscan zijn voltooid:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op ··· naast Snelle scan of Systeemscan en selecteer **Bewerken**.
4. Pas de scan aan in overeenkomst met uw noden en klik op **Volgende**.
5. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan en kies vervolgens wanneer de taak moet worden gestart.
   Als u Dagelijks, Maandelijks of Wekelijks kiest, sleept u de schuifregelaar langs de schaal om de gewenste periode in te stellen wanneer de geplande scan moet starten.
6. Klik **Redden**.

Om het apparaat uit te schakelen wanneer een aangepaste scan is voltooid:

1. Klik op ··· naast de aangepaste scan die u hebt aangemaakt.
2. Klik op **Volgende** en klik dan opnieuw op **Volgende**.
3. vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan en kies vervolgens wanneer de taak moet worden gestart.
4. Klik **Redden**.

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

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Zie Antivirusscanwizard (pagina 56) voor meer informatie.

5.5.6. Hoe kan ik Bitdefender configureren om een proxy-internetverbinding te gebruiken?

Als uw apparaat 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 **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Geavanceerd** tabblad.
3. Schakel **Proxyserver** in.
4. Klik op **Proxywijziging**.
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 Microsoft Edge, 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 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.

5.5.7. 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 **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.
     In **Windows 8.1**, zoek **Deze pc**.
  2. Selecteer **Eigenschappen** in het onderste menu.
  3. Kijk in Systeem om uw systeemtype te zien.

- In **Windows 10** En **Windows 11**:
  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.

5.5.8. Verborgen objecten weergeven in Windows

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

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

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

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** En **Windows 11**:

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. Duidelijk **Verberg extensies voor bekende bestandstypen**.
4. Duidelijk **Verberg beveiligde besturingssysteembestanden**.
5. Klik **Toepassen**, dan klikken **OK**.

5.5.9. 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 apparaat Bitdefender Antivirus Plusgebruikt, wordt het systeem onstabiel. Het installatieprogramma van 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 **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
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 verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Een programma verwijderen** of **Programma's en functies**.
  3. Wacht even totdat 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 verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**en klik vervolgens op Instellingen.
  2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Apps**.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  5. Wacht tot het verwijderingsproces 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.

5.5.10. 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 bedreigingen 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 bedreigingen 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 uw apparaat opnieuw op.
  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**, **Windows 10** en **Windows 11**:
  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 in normale modus, zet u de instellingen terug door de **Systeemoperatie** 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.

6. PROBLEMEN OPLOSSEN

6.1. 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 (pagina 151).

6.1.1. 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 elke andere

beveiligingsoplossing die u mogelijk gebruikt voordat u Bitdefender installeert, te verwijderen. Zie Andere beveiligingsoplossingen verwijderen (pagina 127) voor meer informatie.

- **Er is niet voldaan aan de systeemvereisten voor het uitvoeren van Bitdefender.**
  Als uw apparaat niet voldoet aan de systeemvereisten wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn. Zie Systeemvereisten (pagina 3) voor meer informatie.
- **U hebt toepassingen geïnstalleerd die u niet gebruikt.**
  Elk apparaat heeft programma's of toepassingen die niet worden 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 dreigingen. Spyware, malware, 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 types dreigingen die de veiligheid van uw systeem in gevaar brengen.
  De Systeemscan starten:
  1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
  2. In de **ANTIVIRUS** paneel, klik **Open**.
  3. Klik in het venster **Scans** op de **Scan uitvoeren** knop naast **Systeemscan**.
  4. Volg de stappen van de wizard.

6.1.2. 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.**
  Installeer Bitdefender in dat geval opnieuw:
  - In **Windows 7**:
    1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
    2. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
    3. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    4. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
  - In **Windows 8** En **Windows 8.1**:
    1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
    2. Klik **Verwijderen** een programma of **Programma's en functies**.
    3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
    4. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    5. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.
  - In **Windows 10** En **Windows 11**:
    1. Klik **Begin**, dan klikken **Instellingen**.
    2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.
    3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
    4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
    5. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.

6. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.

> **Opmerking**
> Door deze herinstallatieprocedure te volgen, worden aangepaste instellingen opgeslagen en beschikbaar in het nieuw geïnstalleerde product. Andere instellingen kunnen worden teruggezet naar hun standaardconfiguratie.

- **Bitdefender is niet het enige beveiligingsoplossing die op uw systeem is geïnstalleerd.**
  In dit geval:

  1. Verwijder de andere beveiligingsoplossing. Zie Andere beveiligingsoplossingen verwijderen (pagina 127) voor meer informatie.
  2. Bitdefender opnieuw installeren:
     - In **Windows 7**:
       a. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
       b. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
       c. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       d. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8** En **Windows 8.1**:
       a. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
       b. Klik **Verwijderen** een programma of **Programma's en functies**.
       c. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
       d. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       e. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:
  a. Klik **Begin**, dan klikken **Instellingen**.
  b. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.
  c. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  d. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  e. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt
  f. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.

> **Opmerking**
> Door deze herinstallatieprocedure te volgen, worden aangepaste instellingen opgeslagen en beschikbaar in het nieuw geïnstalleerde product. Andere instellingen kunnen worden teruggezet naar hun standaardconfiguratie.

Als deze informatie niet nuttig was, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in de sectie Hulp vragen (pagina 151).

6.1.3. Ik kan een bepaalde 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 type situatie doet zich voor wanneer Advanced Threat Defense per vergissing toepassingen als schadelijk beschouwt.

Advanced Threat Defense is een Bitdefender-functie die constant toezicht houdt op de toepassingen die op uw systeem draaien en verslag uitbrengt over deze die potentieel schadelijk gedrag vertonen. Omdat deze functie op een heuristisch systeem is gebaseerd, kunnen er gevallen zijn waarbij

rechtmatige toepassingen worden gerapporteerd door Advanced Threat Defense.

Wanneer deze situatie zich voordoet, kunt u de respectievelijke toepassing uitsluiten, zodat deze niet wordt gemonitord door Advanced Threat Defense.

Om het programma toe te voegen aan de lijst met uitsluitingen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
3. In de **Instellingen** venster, klik **Uitzonderingen beheren**.
4. Klik **+Voeg een uitzondering toe**.
5. Voer in het overeenkomende veld het pad van het uitvoerbare bestand in dat u wilt uitsluiten van het scannen.
   U kunt ook naar het uitvoerbare bestand navigeren door op de bladerknop aan de rechterkant van de interface te klikken, het te selecteren en op te klikken **OK**.
6. Zet de schakelaar ernaast aan **Geavanceerde bescherming tegen bedreigingen**.
7. Klik **Redden**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 151).

6.1.4. Wat moet u doen wanneer Bitdefender een website, domein, IP-adres of online toepassing blokkeert die veilig is

Bitdefender biedt een veilige websurfervaring door al het webverkeer te filteren en alle kwaadaardige content te blokkeren. Het is echter mogelijk dat Bitdefender een website, domein, IP-adres of online toepassing die veilig is, als onveilig beschouwt, waardoor het scannen van HTTP-verkeer door Bitdefender deze onterecht gaat blokkeren.

Als dezelfde pagina of online toepassing of hetzelfde domein of IP-adres herhaaldelijk wordt geblokkeerd, kunt u deze toevoegen aan de uitzonderingen zodat ze niet worden gescand door de engines van Bitdefender, wat een vlottere surfervaring garandeert.

Om een website toe te voegen aan **Uitzonderingen**:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ONLINE BEDREIGINGSPREVENTIE** paneel, klik **Instellingen**.
3. Klik **Beheer uitzonderingen**.
4. Klik **+Voeg een uitzondering toe**.
5. Typ in het overeenkomstige veld de naam van de website, de naam van het domein of het IP-adres dat u aan uitzonderingen wilt toevoegen.
6. Klik op de schakelaar ernaast **Preventie van online bedreigingen**.
7. Klik **Redden** om de wijzigingen op te slaan en het venster te sluiten.

U dient enkel websites, domeinen, IP-adressen en toepassingen die u volledig vertrouwt, toe te voegen aan deze lijst. Ze worden uitgesloten van het scannen door de volgende engines: bedreiging, phishing en fraude.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 151).

6.1.5. Bitdefender updaten bij een langzame internetverbinding

Als u een langzame internetverbinding hebt (zoals een inbelverbinding), kunnen er fouten optreden tijdens het updaten.

Om uw systeem up to date houden met de nieuwste Bitdefender-informatie-database voor bedreigingen:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Update** tabblad.
3. Schakel de schakelaar **Stille update** uit.
4. Wanneer een volgende update beschikbaar is, zal u worden gevraagd welke update u wilt downloaden. Selecteer enkel **Handtekeningen update**.
5. Bitdefender downloadt en installeert enkel de informatie-database voor bedreigingen.

6.1.6. 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 wordt gemeld 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 apparaat 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 apparaat 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.
   Zie Andere beveiligingsoplossingen verwijderen (pagina 127) voor meer informatie.

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel Hulp vragen (pagina 151).

6.1.7. 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 **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
  2. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  3. Klik **VERWIJDEREN** in het venster dat verschijnt.
  4. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Een programma verwijderen** of **Programma's en functies**.
  3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  4. Klik **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**en klik vervolgens op Instellingen.
  2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.
  3. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  5. Klik **VERWIJDEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

6.1.8. 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. Om te weten hoe u dit kunt doen, ga naar Opnieuw opstarten in Veilige modus (pagina 129).
  2. Bitdefender verwijderen van uw systeem:
     - In **Windows 7**:
       a. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
       b. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.
       c. Klik **VERWIJDEREN** in het venster dat verschijnt.
       d. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
       e. Start uw systeem opnieuw op in normale modus.
     - In **Windows 8** En **Windows 8.1**:
       a. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
       b. Klik **Een programma verwijderen** of **Programma's en functies**.
       c. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.

d. Klik **VERWIJDEREN** in het venster dat verschijnt.

e. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

f. Start uw systeem opnieuw op in de normale modus.

- In **Windows 10** En **Windows 11**:

  a. Klik **Begin**en klik vervolgens op Instellingen.

  b. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.

  c. Vinden **Bitdefender Antivirus Plus** en selecteer **Verwijderen**.

  d. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.

  e. Klik **VERWIJDEREN** in het venster dat verschijnt.

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

  g. Start uw systeem opnieuw op in de normale modus.

3. Uw Bitdefender-product herinstalleren.

- **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**
  Om dit op te lossen:

  1. Start uw systeem opnieuw op en ga naar Veilige modus. Raadpleeg voor meer informatie over hoe u dit doet Opnieuw opstarten in Veilige modus (pagina 129).
  2. Verwijder de andere beveiligingsoplossing van uw systeem:
     - In **Windows 7**:

       a. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.

       b. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

       c. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8** En **Windows 8.1**:

  a. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.

  b. Klik **Een programma verwijderen** of **Programma's en functies**.

  c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

  d. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:

  a. Klik **Begin**en klik vervolgens op Instellingen.

  b. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.

  c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

  d. Wacht tot het verwijderingsproces 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 op te lossen:

1. Start uw systeem opnieuw op en ga naar Veilige modus. Raadpleeg voor meer informatie over hoe u dit doet Opnieuw opstarten in Veilige modus (pagina 129).

2. Gebruik de optie Systeemherstel van Windows om de apparaat 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 (pagina 151).

6.2. Bedreigingen van uw systeem verwijderen

Bedreigingen kunnen uw systeem op heel wat verschillende manieren beïnvloeden en de benadering van Bitdefender is afhankelijk van het type bedreiging. Omdat bedreigingen vaak hun gedrag veranderen, is het moeilijk een patroon vast te stellen voor hun gedrag en hun acties.

Er zijn situaties wanneer Bitdefender de bedreigingsinfectie niet automatisch kan verwijderen van uw systeem. In dergelijke gevallen is uw tussenkomst vereist.

- Reddingsomgeving (pagina 144)
- Wat moet u doen als Bitdefender dreigingen vindt op uw apparaat? (pagina 144)
- Een bedreiging in een archief opruimen (pagina 146)
- Een bedreiging in een e-mailarchief opruimen (pagina 147)
- Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is? (pagina 148)
- Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek? (pagina 149)
- Wat zijn de overgeslagen items in het scanlogboek? (pagina 149)
- Wat zijn de overgecomprimeerde bestanden in het scanlogboek? (pagina 149)
- Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd? (pagina 150)

Als u uw probleem hier niet kunt vinden, of als de gepresenteerde oplossingen het niet oplossen, kunt u contact opnemen met de vertegenwoordigers van de technische ondersteuning van Bitdefender, zoals weergegeven in hoofdstuk Hulp vragen (pagina 151).

6.2.1. Reddingsomgeving

Helpmodus is een Bitdefender-functie waarmee u alle bestaande harde schijfpartities binnen en buiten uw besturingssysteem kunt scannen en desinfecteren.

Bitdefender Noodomgeving is geïntegreerd met Windows RE.

Uw systeem starten in de Helpmodus

U kunt enkel op de volgende manier van uw Bitdefender-product naar de Rescue Environment gaan:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik op **Openen** naast **Noodomgeving**.
4. Klik op **Herstarten** in het venster dat verschijnt.
   Bitdefender Noodomgeving wordt binnen enkele ogenblikken geladen.

Uw systeem scannen in de Noodomgeving

Om uw systeem te scannen in de Noodomgeving:

1. Ga naar de Rescue Environment, zoals beschreven in Uw systeem starten in de Helpmodus (pagina 144).
2. Het Bitdefender-scanproces start automatisch zodra het systeem is geladen in Rescue Environment.
3. Wacht tot de scan is voltooid. Volg de instructies om een gedetecteerde bedreiging te verwijderen.
4. Om Rescue Environment te verlaten, klikt u op de knop SLUITEN in het venster met de scanresultaten.

6.2.2. Wat moet u doen als Bitdefender dreigingen vindt op uw apparaat?

U ontdekt op een van de volgende manieren dat er een dreiging aanwezig is op uw apparaat:

- U hebt uw apparaat gescand en Bitdefender heeft geïnfecteerde items gevonden.

- Een bedreigingswaarschuwing laat u weten dat Bitdefender een of meerdere bedreigingen op uw apparaat heeft geblokkeerd.

Voer in dergelijke gevallen een update uit van Bitdefender om zeker te zijn dat u over de laatste informatiedatabase over bedreigingen 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 antivirusbescherming van Bitdefender uit:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. In de **Geavanceerd** venster, uitschakelen **Bitdefender-schild**.
2. Geef verborgen objecten weer in Windows. Raadpleeg voor meer informatie over hoe u dit doet Verborgen objecten weergeven in Windows (pagina 126).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real-time antivirusbescherming van Bitdefender in.

Indien de eerste methode niet werkte om de infectie te verwijderen:

1. Start uw systeem opnieuw op en ga naar Veilige modus. Raadpleeg voor meer informatie over hoe u dit doet Opnieuw opstarten in Veilige modus (pagina 129).

2. Geef verborgen objecten weer in Windows. Raadpleeg voor meer informatie over hoe u dit doet Verborgen objecten weergeven in Windows (pagina 126).
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 sectie Hulp vragen (pagina 151).

6.2.3. Een bedreiging 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 bedreigingen detecteren, maar kan geen andere acties ondernemen.

Als Bitdefender u meldt dat er een bedreiging is gedetecteerd binnen een archief en er geen actie beschikbaar is, betekent dit dat het niet mogelijk is de bedreiging te verwijderen vanwege beperkingen op de machtigingsinstellingen voor het archief.

Een bedreiging die in een archief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Identificeer het archief dat de bedreiging bevat door een systeemscan uit te voeren.
2. Schakel de real-time antivirusbescherming van Bitdefender uit:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. In de **Geavanceerd** venster, uitschakelen **Bitdefender-schild**.

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 bedreiging die is opgeslagen in een archief, geen onmiddellijke bedreiging is voor uw systeem, omdat de bedreiging 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 sectie Hulp vragen (pagina 151).

6.2.4. Een bedreiging in een e-mailarchief opruimen

Bitdefender kan ook bedreigingen identificeren in de 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 bedreiging die in een e-mailarchief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Scan de e-maildatabase met Bitdefender.
2. Schakel de real-time antivirusbescherming van Bitdefender uit:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. In de **Geavanceerd** venster, uitschakelen **Bitdefender-schild**.

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/ 2016: 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 antivirusbescherming van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 151).

6.2.5. 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. Om te weten hoe u dit kunt doen, ga naar How do I scan my system?.
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.
   Om te weten hoe u dit kunt doen, ga naar Hulp vragen (pagina 151).

6.2.6. 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 apparaat 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.

6.2.7. 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.

6.2.8. 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 systeembronnen zou in beslag nemen. De inhoud zal bij real time toegang worden gescand indien dat nodig is.

6.2.9. 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 bepaalde soorten bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig kwaadaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand van de schijf verwijderd.

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.

7. HULP VRAGEN

7.1. Hulp vragen

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

7.2. Online bronnen

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

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

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

7.2.1. Bitdefender Support Center

Het Bitdefender Support Center is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over dreigingspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De Bitdefender Support Center is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog een middel om BitDefender-klanten de technische kennis en het inzicht

te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de Bitdefender Support Center als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

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

7.2.2. De Community van Bitdefender-experts

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

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

U vindt de website van onze Community van experts hier:

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

7.2.3. Bitdefender Cyberpedia

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

De webpagina van Bitdefender Cyberpedia vindt u hier:

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

7.3. Contactinformatie

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

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

7.3.1. Lokale verdelers

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

Om een Bitdefender-verdeler te vinden in uw land:

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

WOORDENLIJST

Activeringscode

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

ActiveX

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

Advanced persistent threat

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

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden

geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd. Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archive

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

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

Backdoor

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

Boot sector

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

Boot virus

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

Botnet

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

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

Browser

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

Brute Force-aanval

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

Opdrachtregel

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

Cookies

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

Cyberpesten

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

Woordenboekaanval

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

Schijfstation

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

Download

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

E-mail

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

Gebeurtenissen

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

Exploits

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

Vals positief

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

Bestandsextensie

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

Heuristisch

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

Honeypot

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

IP

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

Java applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou

u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

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

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt. Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macro virus

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

Mail client

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

Geheugen

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

Niet-heuristisch

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

Online predatoren

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

Ingepakte programma's

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

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

Pad

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

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

Phishing

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

de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Foton

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

Polymorf virus

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

Poort

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

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

Ransomware

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

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

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

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

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

Script

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

Spam

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

Spyware

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

anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

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

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

Startup items

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

Abonnement

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

Systeemvak

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

TCP/IP

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

Dreiging

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

informatie-updates van dreigingen

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

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen op uw computer installeert.

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

Update

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

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

Virtueel privénetwerk (VPN)

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

Worm

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