Bitdefender®

TOTAL SECURITY MULTI-DEVICE 2018

HANDLEIDING

Bitdefender Total Security Multi-Device 2018
Handleiding

Publication date 06/10/2018

Copyright© 2018 Bitdefender

Kennisgevingen

Alle rechten voorbehouden. Geen enkel deel van dit boek mag worden gereproduceerd of overgedragen in enige vorm of door enig middel, hetzij elektronisch of mechanisch, met inbegrip van het fotokopiëren, opnemen, gegevensopslag of het opslaan in een retrievalsysteem zonder de schriftelijke toestemming van een erkende vertegenwoordiger van Bitdefender. Het overnemen van korte citaten in besprekingen is alleen mogelijk als de bron van het citaat wordt vermeld. De inhoud mag op geen enkele manier worden gewijzigd.

Waarschuwing en voorbehoud. Dit product en de bijbehorende documentatie worden beschermd door copyright. De informatie in dit document wordt verschaft "zoals hij is", zonder enige garantie. Hoewel er alle voorzorgsmaatregelen zijn genomen bij de voorbereiding van dit document, hebben de auteurs geen enkele wettelijke verantwoordelijkheid aan welke persoon of entiteit dan ook met betrekking tot enig verlies of schade, direct of indirect veroorzaakt of vermeend veroorzaakt door de gegevens in dit werk.

Dit boek bevat links naar websites van derden die niet onder het beheer van Bitdefender staan. Bitdefender is daarom niet verantwoordelijk voor de inhoud van deze gelinkte sites. Als u een dergelijke website bezoekt, doet u dit op eigen risico. Bitdefender verschaft deze links enkel voor uw gemak en het opnemen van de link houdt niet in dat Bitdefender de inhoud van de site van de derde partij onderschrijft of er enige verantwoordelijkheid voor accepteert.

Handelsmerken. Deze publicatie kan namen van handelsmerken vermelden. Alle geregistreerde en niet-geregistreerde handelsmerken in dit document zijn de exclusieve eigendom van hun respectievelijke eigenaars en worden met respect erkend.

Bitdefender

Inhoudsopgave

Over deze gids x
1. Voor wie is deze handleiding bedoeld? x
2. Zo gebruikt u deze handleiding x

Total Security voor pc 1

1. Installatie 2
1.1. Voorbereiden voor installatie 2
1.2. Systeemvereisten 2
1.3. Uw Bitdefender-product installeren 4

2. Aan de slag 11
2.1. De basisfuncties 11
2.1.1. Problemen aan het oplossen 13
2.1.2. Notificaties 15
2.1.3. Autopilot 16
2.1.4. Profielen 17
2.1.5. Wachtwoordbeveiligde Bitdefender-instellingen 18
2.1.6. Anonieme gebruiksrapporten 19
2.1.7. Kennisgevingen speciale aanbiedingen 19
2.2. Bitdefender-interface 20
2.2.1. Systeemvakpictogram 20
2.2.2. Hoofdvenster 22
2.2.3. De Bitdefender-secties 26
2.2.4. Beveiligingswidget 30
2.2.5. Activiteit 32
2.3. Bitdefender Central 36
2.3.1. Mijn abonnementen 37
2.3.2. Mijn apparaten 39
2.3.3. Activiteit 42
2.3.4. Mijn account 43
2.3.5. Notificaties 44
2.4. Bitdefender up-to-date houden 44
2.4.1. Controleren of Bitdefender up-to-date is 45
2.4.2. Een update uitvoeren 45
2.4.3. De automatische update in- of uitschakelen 46
2.4.4. De update-instellingen aanpassen 46
2.4.5. Doorlopende updates 48

3. Zo werkt het 49
3.1. Installatie 49
3.1.1. Hoe installeer ik Bitdefender op een tweede computer? 49
3.1.2. Hoe kan ik Bitdefender opnieuw installeren? 49
3.1.3. Waar kan ik mijn Bitdefender-product van downloaden? 50
3.1.4. Hoe kan ik de taal van mijn Bitdefender-product veranderen? 51
3.1.5. Hoe gebruik ik mijn Bitdefender-abonnement na een Windows-upgrade? 53
3.1.6. Hoe kan ik upgraden naar de recentste Bitdefender-versie? 55

3.2. Abonnementen . . . 56
3.2.1. Hoe activeer ik het Bitdefender-abonnement met een licentiesleutel? . . . 56
3.3. Bitdefender Central . . . 57
3.3.1. Hoe meld ik me aan op Bitdefender Central terwijl ik een andere online account gebruik? . . . 57
3.3.2. Hoe schakel ik Bitdefender Central-hulpberichten uit? . . . 58
3.3.3. Ik ben het wachtwoord dat ik voor mijn Bitdefender-account heb gekozen, vergeten. Hoe kan ik het terugstellen? . . . 58
3.3.4. Hoe kan ik de aanmeldsessies van mijn Bitdefender-account beheren? . . . 59
3.4. Scannen met Bitdefender . . . 59
3.4.1. Een bestand of map scannen . . . 59
3.4.2. Hoe kan ik mijn systeem scannen? . . . 60
3.4.3. Hoe plan ik een scan? . . . 60
3.4.4. Een aangepaste scantaak maken . . . 61
3.4.5. Een map uitsluiten van de scan . . . 62
3.4.6. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt? . . . 62
3.4.7. Hoe kan ik controleren welke bedreigingen Bitdefender heeft gedetecteerd? . . . 64
3.5. Ouderlijk Adviseur . . . 64
3.5.1. Mijn kinderen beschermen tegen online bedreigingen . . . 64
3.5.2. Hoe blokkeer ik de toegang van mijn kind tot een website? . . . 66
3.5.3. Hoe verhinder ik dat mijn kind een spel speelt? . . . 66
3.5.4. Hoe voorkom ik dat mijn kind in contact komt met onbetrouwbare personen? . . . 67
3.5.5. Hoe kan ik een lokatie als veilig of beperkt instellen voor mijn kind? . . . 68
3.5.6. Hoe blokkeer ik de toegang van mijn kind tot de toegekende apparaten tijdens schooldagen? . . . 70
3.5.7. Hoe blokkeer ik de toegang van mijn kind tot de toegekende apparaten tijdens schoolnachten? . . . 69
3.5.8. Hoe blokkeer ik de toegang van mijn kind tot de toegekende apparaten tijdens het weekend? . . . 70
3.5.9. Hoe kan een kindprofiel worden verwijderd . . . 71
3.6. Privacy bescherming . . . 71
3.6.1. Hoe kan ik controleren of mij online transactie beveiligd is? . . . 71
3.6.2. Wat kan ik doen als mijn apparaat gestolen is? . . . 72
3.6.3. Bestandskluizen gebruiken . . . 72
3.6.4. Hoe kan ik een bestand definitief verwijderen met Bitdefender? . . . 74
3.6.5. Hoe zorg ik ervoor dat mijn webcam niet gehackt wordt? . . . 75
3.7. Optimalisatiehulpmiddelen . . . 75
3.7.1. Mijn systeemprestaties verbeteren . . . 75
3.7.2. Hoe kan ik de opstarttijd van mijn systeem verbeteren? . . . 76
3.8. Nuttige informatie . . . 77
3.8.1. Hoe test ik mijn beveiligingsoplossing? . . . 77
3.8.2. Hoe kan ik Bitdefender verwijderen? . . . 78
3.8.3. Hoe kan ik Bitdefender VPN verwijderen? . . . 79
3.8.4. Hoe kan ik de computer automatisch afsluiten nadat het scannen is voltooid? . . . 79
3.8.5. Bitdefender configureren voor het gebruik van een proxy-internetverbinding . . . 80

3.8.6. Gebruik ik een 32- of 64-bits versie van Windows? . . . 81
3.8.7. Verborgen objecten weergeven in Windows . . . 82
3.8.8. Andere beveiligingsoplossingen verwijderen . . . 83
3.8.9. Opnieuw opstarten in Veilige modus . . . 84

4. Uw beveiliging beheren . . . 86
4.1. Antivirusbeveiliging . . . 86
4.1.1. Scannen bij toegang (real time-beveiliging) . . . 87
4.1.2. Scannen op aanvraag . . . 92
4.1.3. Automatisch scannen van verwisselbare media . . . 102
4.1.4. Gastbestand scannen . . . 104
4.1.5. Scanuitsluitingen configureren . . . 104
4.1.6. Bestanden in quarantaine beheren . . . 107
4.2. Advanced Threat Defense . . . 108
4.3. Webbeveiliging . . . 110
4.4. Antispam . . . 113
4.4.1. Antispam-begrippen . . . 114
4.4.2. De antispambeveiliging in- of uitschakelen . . . 115
4.4.3. De antispam-werkbalk in het venster van uw e-mailclient gebruiken . . . 115
4.4.4. De Vriendenlijst configureren . . . 118
4.4.5. Spammerslijst configureren . . . 119
4.4.6. De lokale antispamfilters configureren . . . 120
4.4.7. De cloudinstellingen configureren . . . 121
4.5. Firewall . . . 122
4.5.1. De regels beheren . . . 123
4.5.2. Verbindingsinstellingen beheren . . . 126
4.5.3. Geavanceerde instellingen configureren . . . 127
4.6. Kwetsbaarheid . . . 128
4.6.1. Uw systeem scannen op kwetsbaarheden . . . 128
4.6.2. De automatische kwetsbaarheidsbewaking gebruiken . . . 130
4.6.3. Wi-Fi Security Advisor . . . 132
4.7. Webcambeveiliging . . . 135
4.8. Veilige bestanden . . . 138
4.8.1. Veilige bestanden in- of uitschakelen . . . 138
4.8.2. Persoonlijke bestanden beschermen tegen ransomware-aanvallen. . . . 139
4.8.3. Toegang tot toepassingen aan het configureren . . . 140
4.8.4. Bescherming bij opstarten . . . 140
4.9. Bestandscodering . . . 141
4.10. Beveiliging Wachtwoordbeheerder voor uw gegevens . . . 146
4.11. VPN . . . 153
4.12. Safepay beveiliging voor online transacties . . . 156
4.13. Data bescherming . . . 161
4.14. Ouderlijk Adviseur . . . 162
4.14.1. Naar Ouderlijk Adviseur gaan - MIJN KINDEREN . . . 162
4.14.2. Het profiel van uw kind toevoegen . . . 163
4.14.3. Profielen in Ouderlijk Adviseur configureren . . . 169
4.15. Anti-Theft voor mobiele apparaten . . . 175
4.16. USB Immunizer . . . 177

5. Systeemoptimalisatie . . . 179

5.1. Extra . . . 179
5.1.1. De snelheid van uw systeem optimaliseren in een enkele klik . . . 179
5.1.2. De opstarttijd van uw pc aan het optimaliseren . . . 180
5.1.3. Uw schijf optimaliseren . . . 181
5.2. Profielen . . . 183
5.2.1. Werkprofiel . . . 184
5.2.2. Filmprofiel . . . 185
5.2.3. Gameprofiel . . . 187
5.2.4. Openbaar Wi-Fi-profiel . . . 188
5.2.5. Profiel batterijmodus . . . 188
5.2.6. Real-Time Optimalisering . . . 189

6. Problemen oplossen . . . 191
6.1. Algemene problemen oplossen . . . 191
6.1.1. Mijn systeem lijkt traag . . . 191
6.1.2. Het scannen start niet . . . 193
6.1.3. Ik kan een bepaalde toepassing niet meer gebruiken . . . 195
6.1.4. Wat moet u doen als Bitdefender een veilige website of online toepassing blokkeert . . . 196
6.1.5. Wat moet ik doen indien Bitdefender een veilige toepassing als ransomware beschouwt? . . . 197
6.1.6. Ik kan geen verbinding maken met het internet . . . 197
6.1.7. Ik kan geen toegang krijgen tot een apparaat op mijn netwerk. . . . 198
6.1.8. Mijn internetverbinding is langzaam . . . 200
6.1.9. Bitdefender updaten bij een langzame internetverbinding . . . 202
6.1.10. De Bitdefender-services reageren niet . . . 202
6.1.11. De antispamfilter werkt niet goed . . . 203
6.1.12. De Autofill-functie in mijn Portefeuille werkt niet . . . 208
6.1.13. Het verwijderen van Bitdefender is mislukt . . . 209
6.1.14. Mijn systeem start niet op na het installeren van Bitdefender . . . 210
6.2. Bedreigingen van uw systeem verwijderen . . . 213
6.2.1. Bitdefender Reddingsmodus (Reddingsomgeving in Windows 10) . . . 214
6.2.2. Wat moet er gebeuren wanneer Bitdefender bedreigingen op uw computer vindt? . . . 218
6.2.3. Een bedreiging in een archief opruimen . . . 219
6.2.4. Een bedreiging in een e-mailarchief opruimen . . . 220
6.2.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is? . . . 221
6.2.6. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek? . . . 222
6.2.7. Wat zijn de overgeslagen items in het scanlogboek? . . . 222
6.2.8. Wat zijn de overgecomprimeerde bestanden in het scanlogboek? . . . 223
6.2.9. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd? . . . 223

Antivirus voor Mac . . . 224

7. Installeren en verwijderen . . . 225
7.1. Systeemvereisten . . . 225
7.2. Bitdefender Antivirus for Mac installeren . . . 225
7.2.1. Installatieprocedure . . . 226
7.3. Bitdefender Antivirus for Mac verwijderen . . . 230

8. Aan de slag 231
8.1. Over Bitdefender Antivirus for Mac 231
8.2. Bitdefender Antivirus for Mac starten 231
8.3. Hoofdvenster Toepassing 232
8.4. Dock-symbool toepassing 233

9. Bescherming tegen schadelijke software 235
9.1. Aanbevelingen 235
9.2. Uw Mac scannen 236
9.3. Autopilot in- of uitschakelen 237
9.4. Bescherming Time Machine 237
9.5. Scanwizard 239
9.6. Problemen oplossen 239
9.7. Webbeveiliging 241
9.8. Updates 242
9.8.1. Zelf een update uitvoeren 243
9.8.2. Updates downloaden via een proxyserver 243
9.8.3. Productupdates 243
9.8.4. Informatie over Bitdefender Antivirus for Mac vinden 244

10. Voorkeuren instellen 245
10.1. Voorkeuren weergeven 245
10.2. Accountinfo 245
10.3. Beschermingsvoorkeuren 246
10.3.1. Uitsluitingen 248
10.4. Veilige bestanden 249
10.4.1. Toepassingen beheren 251
10.5. Geschiedenis 251
10.6. Quarantaine 252

11. VPN 274
11.1. Over VPN 254
11.2. VPN Installeren 254
11.3. VPN Openen 255
11.4. Interface 255
11.5. Abonnementen 275

12. Bitdefender Central 258
12.1. Over Bitdefender Central 258
12.2. Naar Bitdefender Central gaan 258
12.3. Mijn abonnementen 259
12.3.1. Abonnement activeren 259
12.3.2. Abonnement kopen 259
12.4. Mijn apparaten 260
12.4.1. Uw apparaten aanpassen 260
12.4.2. Beheer op afstand 261

13. Veelgestelde vragen 263

Mobile Security voor iOS 268

14. Wat is Bitdefender Mobile Security for iOS 269
15. Aan de slag 270
16. VPN 274
16.1. Abonnementen 275
17. Accountprivacy 277
18. Anti-Theft-functies 279
19. Bitdefender account 283

Mobile Security voor Android 285

20. Beschermingsfuncties 286
21. Aan de slag 287
22. Malwarescanner 292
23. Accountprivacy 295
24. Webbeveiliging 297
25. VPN 299
26. Anti-Theft-functies 303
27. App Lock 309
28. Rapporten 314
29. WearON 315
30. Instellingen 316
31. Info 317
32. Bitdefender Central 318
33. Veelgestelde vragen 322

Contact opnemen met ons 328

34. Hulp vragen 329
34.1. Telefonische ondersteuning: 331
35. Online bronnen 333
35.1. Ondersteuningscentrum voor Bitdefender 333
35.2. Bitdefender Ondersteuningsforum 334
35.3. HOTforSecurity-portaal 334
36. Contactinformatie 335
36.1. Webadressen 335
36.2. Lokale verdelers 335

36.3. Bitdefender-kantoren 335
Woordenlijst 339

Over deze gids

1. Voor wie is deze handleiding bedoeld?

Uw Bitdefender Total Security Multi-Device 2018-abonnement kan tot 10 verschillende pc's, Macs, iOS and Android-smarthphones en tablets beschermen. Het beheer van de beschermde apparaten gebeurt via een Bitdefender-account, die moet gekoppeld zijn aan een actief abonnement.

Deze gids biedt ondersteuning bij de installatie en het gebruik van de producten in uw abonnement: Bitdefender Total Security 2018, Bitdefender Antivirus for Mac, Bitdefender Mobile Security for iOS en Bitdefender Mobile Security voor Android-apparaten.

U kunt hier lezen hoe u Bitdefender moet configureren op de verschillende apparaten om ze tegen allerlei dreigingen te beschermen.

2. Zo gebruikt u deze handleiding

Deze gids is georganiseerd rond de vier producten in Bitdefender Total Security Multi-Device 2018:

- “Total Security voor pc” (p. 1)

  Leer hoe u het product op uw Windows-pc's en -laptops moet gebruiken.

- “Antivirus voor Mac” (p. 224)

  Leer hoe u het product op uw Macs moet gebruiken.

- “Mobile Security voor iOS” (p. 268)

  Leer hoe u het product op uw iOS-smartphones en -tablets moet gebruiken.

- “Mobile Security voor Android” (p. 285)

  Leer hoe u het product op uw Android-smartphones en -tablets moet gebruiken.

- “Contact opnemen met ons” (p. 328)

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

TOTAL SECURITY VOOR PC

1. INSTALLATIE

1.1. Voorbereiden voor installatie

Voordat u Bitdefender Total Security 2018 installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de computer waarop u Bitdefender wilt installeren, voldoet aan de minimale systeemvereisten. Als de computer niet voldoet aan alle minimale systeemvereisten, wordt Bitdefender niet geïnstalleerd. Als het programma als is geïnstalleerd, zal het niet goed werken en zal het systeem vertragen en instabiel worden. Raadpleeg "*Systeemvereisten*" (p. 225) voor een complete lijst van systeemvereisten.
- Meld u aan bij de computer met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de computer. Indien iets wordt opgemerkt tijdens het Bitdefender-installatieproces, zult u een bericht krijgen om het te verwijderen. Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Defender zal uitgeschakeld zijn tijdens de installatie.
- Schakel alle firewall-programma's die mogelijk op uw computer 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 computer verbonden te laten met Internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

1.2. Systeemvereisten

U kan Bitdefender Total Security 2018 uitsluitend installeren op computers met de volgende besturingssystemen:

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

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

Opmerking

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

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

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

Minimale systeemvereisten

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

Aanbevolen systeemvereisten

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

Softwarevereisten

Om Bitdefender te kunnen gebruiken, evenals alle functies ervan, moet uw computer 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

- Skype 6.3 en hoger
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 en hoger

1.3. Uw Bitdefender-product installeren

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

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

Installeren vanaf Bitdefender Central

Via de Bitdefender Central kunt u de installatiekit die met het aangekochte abonnement overeenkomt, downloaden. Zodra het installatieproces voltooid is, is Bitdefender Total Security 2018 geactiveerd.

Om Bitdefender Total Security 2018 te downloaden via Bitdefender Central:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Apparaten** en klik dan op **LOKALE BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

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

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

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

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

Als een niet-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 computer opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Het Bitdefender Total Security 2018 installatiepakket wordt voortdurend bijgewerkt.

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

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Total Security 2018 te installeren.

Stap 1 - Installatie Bitdefender

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 Total Security 2018.

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

In deze stap kunnen twee bijkomende taken uitgevoerd worden:

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

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

Stap 2 - Installatie bezig

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

Kritieke zones op uw systeem worden gescand op bedreigingen, de nieuwste versies van de toepassingsbestanden worden gedownload en geïnstalleerd en de services van Bitdefender worden gestart. Deze stap kan enkele minuten duren. Klik op **SCAN OVERSLAAN** indien u het systeem later wilt scannen. Voor meer informatie over een lopende systeemscan, raadpleeg *"Een systeemscan uitvoeren"* (p. 94).

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. Klik op **STARTEN MET Bitdefender** om verder te gaan.

Stap 4 - Aan de slag

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

Klik op **VOLTOOIEN** om naar de Bitdefender Total Security 2018-interface te gaan.

Installeren vanaf de installatiedisk

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

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

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

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

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

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

Als een niet-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 computer opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Opmerking

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

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Total Security 2018 te installeren.

Stap 1 - Installatie Bitdefender

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 Total Security 2018.

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

In deze stap kunnen twee bijkomende taken uitgevoerd worden:

- Zorg ervoor dat de optie **Anonieme rapporten verzenden** geactiveerd blijft. Door deze optie toe te staan, worden rapporten met informatie over uw gebruik van het product naar de Bitdefender-servers verzonden. Deze

informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen. Merk op dat deze rapporten geen vertrouwelijke informatie bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen gebruikt worden.

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

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

Stap 2 - Installatie bezig

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

Cruciale gebieden op uw systeem worden gescand op bedreigingen en de Bitdefender-diensten worden gestart. Deze stap kan enkele minuten duren. Klik op **SCAN OVERSLAAN** indien u het systeem later wilt scannen. Voor meer informatie over een lopende systeemscan, raadpleeg "*Een systeemscan uitvoeren*" (p. 94).

Stap 3 - Installatie voltooid

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. Klik op **STARTEN MET Bitdefender** om verder te gaan.

Stap 4 - 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*" (p. 36) voor meer informatie.

Ga verder volgens uw situatie.

Ik wil een Bitdefender-account maken

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

De gegevens die u hier opgeeft, worden vertrouwelijk behandeld.

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

Lees de Servicevoorwaarden van Bitdefender voor u verder gaat.

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

Ik heb al een Bitdefender-account

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

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

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

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

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

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

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

Stap 5 - Uw product activeren

Opmerking

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

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

Ga verder volgens uw situatie:

- Ik heb een activeringscode

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

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

     Opmerking

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

  2. **Ik wil graag Bitdefender evalueren**

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

Stap 6 - Aan de slag

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

Klik op **VOLTOOIEN** om naar de Bitdefender Total Security 2018-interface te gaan.

2. AAN DE SLAG

2.1. De basisfuncties

Nadat u Bitdefender Total Security 2018 hebt geïnstalleerd, wordt uw computer 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. 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 slachtoffer kan worden van toekomstige cyberaanvallen. Installeer en gebruik de "*VPN*" (p. 153) app om dergelijke betreurenswaardige situaties te vermijden.

U kunt uw wachtwoorden en online accounts bijhouden door ze op te slaan met "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 146) in een portefeuille Met één enkel hoofdwachtwoord kunt u uw privacy beschermen tegen indringers die mogelijk proberen om uw geld af te troggelen.

"*Webcambeveiliging*" (p. 135)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*" (p. 132).

Uw persoonlijke bestanden die lokaal opgeslagen zijn, zoals documenten, foto's of filmpjes en ook uw bestanden in de cloud kunnen nu veilig blijven,

ver weg van de gevaarlijkste bedreigingen van tegenwoordig, namelijk ransomware. Voor informatie over hoe u persoonlijke bestanden naar een veilige plaats kunt brengen, lees "*Veilige bestanden*" (p. 138).

Speel games of kijk films terwijl u werkt, Bitdefender kan u een voortdurende gebruikerservaring bieden door onderhoudstaken uit te stellen, onderbrekingen te elimineren en de visuele effecten van het systeem af te stellen. U kunt van dit alles profiteren door "*Profielen*" (p. 183).

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*" (p. 15) 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 computer en gegevens te beschermen.

Om de online functies van Bitdefender Total Security 2018 te gebruiken en uw abonnementen en toestellen te beheren, gaat u naar uw Bitdefender-account. Zie "*Bitdefender Central*" (p. 36) voor meer informatie.

In het "*Zo werkt het*" (p. 49) deel vindt u stap-voor-stap instructies over het uitvoeren van vaak voorkomende taken. Indien u problemen ondervindt bij het gebruik van Bitdefender, controleer dan het "*Algemene problemen oplossen*" (p. 191)deel met mogelijke oplossingen voor de problemen die het vaakst voorkomen.

Open het Bitdefender-venster.

Om naar de hoofdinterface van Bitdefender Total Security 2018 te gaan, volgt u de stappen hieronder:

- In **Windows 7**:
  1. Klik op **Start** en ga naar **Alle Programma's**.
  2. Klik op **Bitdefender 2018**.
  3. Klik op **Bitdefender Total Security 2018** of, sneller, dubbelklik op het pictogram van Bitdefender in het systeemvak.
- In **Windows 8 en Windows 8.1**:

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

- In **Windows 10**:

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

Meer informatie over het Bitdefender-venster en -pictogram in het systeemvak, vindt u op "*Bitdefender-interface*" (p. 20).

2.1.1. Problemen aan het oplossen

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

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

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

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

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

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

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

Wizard beveiligingsproblemen

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

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

   Als u een specifiek probleem niet meteen wilt oplossen, schakelt u het overeenkomende selectievakje uit. U wordt gevraagd op te geven hoelang het oplossen van het probleem kan worden uitgesteld. Kies de gewenste optie in het menu en klik op **OK**. Kies **Permanent** om de bewaking van de respectieve problemencategorie te stoppen.

   De status van het probleem verandert naar **Uitgesteld** en er wordt geen actie ondernomen om het probleem op te lossen.
3. Om de geselecteerde problemen op te lossen, klikt u op **Herstellen**. Sommige problemen worden onmiddellijk opgelost. Bij andere problemen wordt u geholpen door een wizard om ze op te lossen.

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

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

Statuswaarschuwingen configureren

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

- Antivirus
- Firewall
- Update
- Browserveiligheid

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

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

2.1.2. Notificaties

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

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

Om naar de Kennisgevingenlogs te gaan, klikt u op het pictogram in de linkerzijbalk van de Bitdefender-interface. Telkens wanneer zich een kritiek evenement voordoet, kunt u een teller opmerken op de -icoon.

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

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

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

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

2.1.3. Autopilot

Voor alle gebruikers die van hun beveiligingsoplossing alleen vragen dat ze worden beschermd zonder te worden gehinderd, werd Bitdefender Total Security 2018 ontworpen met een ingebouwde Autopilot-modus.

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

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

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

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

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

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

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

2.1.4. Profielen

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

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

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

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

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

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

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

Profiel batterijmodus

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

Automatische activatie van profielen configureren

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

Om Bitdefender toestemming te geven om profielen te activeren:

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

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

Om een profiel manueel te activeren, klik op de AAN/UIT-knop. U kunt slechts één profiel manueel activeren per keer.

Voor meer informatie over Profielen, ga naar"*Profielen*" (p. 183)

2.1.5. Wachtwoordbeveiligde Bitdefender-instellingen

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

Wachtwoordbescherming configureren voor de Bitdefender-instellingen:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Schakel in het **ALGEMEEN**-venster de **Wachtwoordbescherming** in door op de bijhorende schakelaar te klikken.
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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Schakel in het **ALGEMEEN**-venster de Wachtwoordbescherming uit door op de bijhorende schakelaar te klikken.
3. Voer het wachtwoord in en klik op **OK**.

Opmerking

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

2.1.6. Anonieme gebruiksrapporten

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

Indien u geen Anonieme gebruikersrapporten meer wil verzenden:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **GEAVANCEERD**.
3. Klik op de bijhorende AAN/UIT-schakelaar.

2.1.7. 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 op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het venster **ALGEMEEN** klikt u op de overeenkomstige AAN/UIT-schakelaar.

De optie speciale aanbiedingen en productmeldingen is standaard ingeschakeld.

2.2. Bitdefender-interface

Bitdefender Total Security 2018 voldoet niet alleen aan de behoeften van beginnende computergebruikers, maar ook aan de eisen van bijzonder technische gebruikers. De grafische gebruikersinterface is ontworpen zodat elke categorie gebruikers deze probleemloos kunnen gebruiken.

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

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

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

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

2.2.1. Systeemvakpictogram

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

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

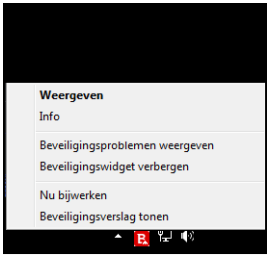
- In **Windows 7, Windows 8 en Windows 8.1**:

1. Klik onderaan rechts op het scherm op de pijl ▲.
2. Klik op **Aanpassen...** om het venster met de systeemvakpictogrammen te openen.
3. Selecteer de optie **Pictogrammen en meldingen weergeven** voor het pictogram **Bitdefender-agent**.

- In **Windows 10**:

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

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



Systeemvakpictogram

- **Weergeven** - opent het hoofdvenster van Bitdefender.
- **Over** - opent een venster met informatie over Bitdefender, over waar u hulp vindt in geval van problemen, waar u de Abonnementsovereenkomst kunt herlezen en waar u de Onderdelen van Derden alsook ons Privacybeleid kunt bekijken.
- **Alle veiligheidsproblemen weergeven** - helpt u de huidige zwakke punten in de beveiliging te verwijderen. Als de optie niet beschikbaar is, moeten er geen problemen worden opgelost. Zie "*Problemen aan het oplossen*" (p. 13) voor meer informatie.
- **Beveiligingswidget tonen/verbergen** - hiermee schakelt u de Beveiligingswidget in/uit.
- **Update nu** - start een directe update. U kunt de updatestatus volgen in het paneel Update van het hoofdvenster van Bitdefender.
- **Beveiligingsverslag tonen** - opent een venster waarin u een wekelijkse status een aanbevelingen voor uw systeem kunt zien. U kunt de aanbevelingen opvolgen om uw systeemveiligheid te verbeteren.

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

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

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

2.2.2. Hoofdvenster

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

Het venster is geordend in vier hoofdgebieden:

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

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

Actieknoppen toegang tot functiegebied
: Hier kunt u verschillende taken lanceren om uw systeem beschermd te houden en met optimale snelheid te werken. U kunt ook naar de Bitdefender-functies gaan om het product zelf te configureren.

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

Statusgebied

Het statusgebied bevat de volgende elementen:

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

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

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

  Door ergens binnen het gebied van de beveiligingsstatus te klikken, gaat u naar een wizard die u helpt om gemakkelijk bedreigingen van uw computer te verwijderen. Zie "*Problemen aan het oplossen*" (p. 13) voor meer informatie.

- Met **AUTOPILOT** kunt u optimale bescherming inschakelen en genieten van een volledig geruisloze beveiliging. Zie "*Autopilot*" (p. 16) voor meer informatie.
- Via **NU UPDATEN** kunt u een productupdate laten lopen wanneer u maar wilt, zodat u de meest recente informatiedatabase over bedreigingen hebt. Zie "*Bitdefender up-to-date houden*" (p. 44) voor meer informatie.
- **Actief Profiel** geeft het huidige profiel weer dat geactiveerd is in uw Bitdefender-product. Zie "*Profielen*" (p. 183) voor meer informatie.

Linkerzijbalk

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

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

- **Bescherming**. De actieknoppen **Snelle Scan** en **Kwetsbaarheidsscan** worden zichtbaar in de linkerbenedenhoek van de Bitdefender-interface. Ook informatie over geblokkeerde applicaties, opgespoorde bedreigingen en aanvallen wordt zichtbaar. Klik op de koppeling **FUNCTIES BEKIJKEN** om naar het configuratiegebied te gaan.

- **Privacy**. De actieknoppen **Safepay** en **VPN** worden zichtbaar in de linkerbenedenhoek van de Bitdefender-interface. Ook informatie over gedetecteerde portefeuilles en bestandskluizen wordt weergegeven. Klik op de koppeling **FUNCTIES BEKIJKEN** om naar het configuratiegebied te gaan.

- **Extra**. De actieknoppen **OneClickOptimizer** en **StartupOptimizer** worden zichtbaar in de linkerbenedenhoek van de Bitdefender-interface. U kunt ook de functie Antidiefstal gebruiken en de functie **Disk Cleanup** kan worden opgestart en onnodige bestanden kunnen worden verwijderd, om meer ruimte vrij te maken voor nieuwe gegevens.

- **Activiteit**. Van hieruit kunt u de productactiviteit van de voorbije 30 dagen bekijken en naar het veiligheidsrapport gaan dat om de zeven dagen wordt gegenereerd.

- **Kennisgevingen**. Van hieruit hebt u toegang tot de gegenereerde kennisgevingen.

- **Account**. Details over Bitdefender-account en lopend abonnement zijn beschikbaar. Ga naar uw Bitdefender-account om uw abonnement te controleren en beveiligingstaken uit te voeren op de toestellen die u beheert.

- **Instellingen**. Van hieruit hebt u toegang tot de algemene instellingen.

- **Ondersteuning**. Van hieruit kunt u, wanneer u hulp nodig hebt bij het aanpakken van een probleem met uw Bitdefender Total Security 2018, contact opnemen met de Technische ondersteuning van Bitdefender.

Actieknoppen toegang tot functiegebied

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

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

- **Snelle scan**. Voer een snelle scan uit om er zeker van te zijn dat uw computer vrij is van bedreigingen.
- **Analyse op Kwetsbaarheden**. Scan uw computer op kwetsbaarheden om zeker te zijn dat alle geïnstalleerde toepassingen, samen met het Besturingssysteem, bijgewerkt zijn en correct werken.
- **Safepay**. Open Bitdefender Safepay™ om uw gevoelige gegevens te beschermen terwijl u online transacties uitvoert.
- **VPN**. Open Bitdefender VPN om een bijkomende beschermingslaag toe te voegen wanneer u verbonden bent met het internet.
- **One-Click Optimizer**. Maak schijfruimte vrij, herstel registerfouten en beveilig uw privacy door bestanden te verwijderen die niet langer dienstig zijn met een enkele klik op een knop.
- **Startup Optimizer**. Verkort uw systeemboottijd door te verhinderen dat onnodige applicaties bij het opstarten worden uitgevoerd.

Onderste balk

Om aanvullende apparaten te beginnen beschermen:

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

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

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

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

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

- Bitdefender Total Security 2018 op Windows-apparaten.
- Bitdefender-antivirus voor Mac op macOS X-apparaten.

- Bitdefender Mobiele beveiliging op Android-gebaseerde toestellen.
- Bitdefender Mobiele beveiliging op iOS-apparaten.
- Bitdefender Ouderlijk adviseur op macOS, iOS en Android-apparaten.

2.2.3. 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 op de linkerzijbalk van de Bitdefender-interface:

- Beveiliging
- Privacy
- Extra

Beveiliging

In het gebied Bescherming kunt u uw geavanceerde veiligheidsinstellingen configureren, vrienden en spammers beheren, de instellingen van de netwerkverbinding bekijken en aanpassen, de eigenschappen van Veilige bestanden en webbescherming instellen, potentiële systeemkwetsbaarheden bekijken en oplossen en de veiligheid van de draadloze netwerken waarmee u verbonden bent, 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
- Reddingsmodus (Reddingsomgeving in Windows 10)

Raadpleeg "*Antivirusbeveiliging*" (p. 86) voor meer informatie over scantaken en het configureren van de antivirusbeveiliging.

WEBBEVEILIGING

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

Meer informatie over het configureren van Bitdefender om uw webactiviteit te beschermen, vindt u op "*Webbeveiliging*" (p. 110).

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*" (p. 122).

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 "*Advanced Threat Defense*" (p. 108).

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*" (p. 113).

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

Klik op **Wi-Fi-beveiligingsadviseur** om de lijst te bekijken van de draadloze netwerken waarmee u een verbinding maakt, samen met onze reputatiebeoordeling voor elk daarvan en de actie die u kunt ondernemen om veilig te blijven voor potentiële nieuwsgierigen.

Meer informatie over het configureren van de kwetsbaarheidsbeveiliging vindt u onder "*Kwetsbaarheid*" (p. 128).

VEILIGE BESTANDEN

De Veilige bestanden zorgen ervoor dat uw persoonlijke bestanden beschermd blijven tegen ransomware-aanvallen.

Meer informatie over het configureren van Veilige bestanden om uw persoonlijke bestanden te beschermen tegen ransomware-aanvallen, vindt u op "*Veilige bestanden*" (p. 138).

Privacy

In het gedeelte Privacy kunt u de Bitdefender VPN-app openen, uw persoonlijke gegevens versleutelen, uw online transacties beschermen, uw webcam en browsingervaring 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*" (p. 153).

CODEREN FILE

Maak gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer waar u uw confidentiële en gevoelige documenten veilig kunt opslaan.

Voor meer informatie over hoe u gecodeerde wachtwoordbeveiligde logical drives (of kluizen) kunt aanmaken op uw computer, gaat u naar "*Bestandscodering*" (p. 141).

WEBCAMBEVEILIGING

Bitdefender-webcambeveiliging zorgt ervoor dat uw webcam geen risico loopt door onbetrouwbare toepassingen de toegang te weigeren.

Voor meer informatie over hoe u uw systeem beschermd houdt tegen ongewenste toegang, lees "*Webcambeveiliging*" (p. 135).

Wachtwoordmanager

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

Meer informatie over het configureren van Wachtwoordbeheerder, vindt u onder "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 146).

SAFEPAY

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

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

Meer informatie over Bitdefender Safepay™ vindt u onder "*Safepay beveiliging voor online transacties*" (p. 156).

OUDERLIJK TOEZICHT

Bitdefender Ouderlijk adviseur stelt u in staat bij te houden wat uw kind doet op de computer. In geval van ongeschikte content kunt u besluiten de toegang tot internet of tot specifieke toepassingen te beperken.

Klik op **Configureren** in het panel Ouderlijk Adviseur 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 Wachtwoordbeheerder, vindt u onder "*Ouderlijk Adviseur*" (p. 162).

GEG. BEVEILIGING

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

Meer informatie over het configureren van de Gegevensbeveiliging vindt u onder "*Data bescherming*" (p. 161).

Extra

In het gedeelte Extra kunt u de snelheid van uw systeem verbeteren en uw apparaten beheren.

Tune-Up

Bitdefender Total Security 2018 biedt niet alleen beveiliging, maar helpt u ook optimale prestaties van uw computer te behouden.

In de Tune-Up-functie kunt u naar een aantal bruikbare hulpmiddelen gaan:

- One-Click Optimizer
- Startup Optimizer
- Schijf opschoning

Meer informatie over de hulpprogramma's voor het optimaliseren van de prestaties, vindt u onder "*Extra*" (p. 179).

Antidiefstal

Bitdefender Antidiefstal beschermt uw computer en gegevens tegen diefstal of verlies. In geval iets dergelijks voorvalt, stelt dit u in staat uw computer op afstand te lokaliseren of vergrendelen. U kunt ook alle aanwezige gegevens van uw systeem wissen.

Bitdefender Antidiefstal biedt de volgende functies:

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

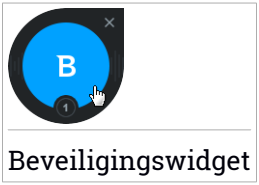
Meer informatie over hoe u uw systeem uit verkeerde handen houdt, vindt u onder "*Anti-Theft voor mobiele apparaten*" (p. 175).

2.2.4. Beveiligingswidget

Beveiligingswidget is de snelle en eenvoudige manier voor het bewaken en beheren van Bitdefender Total Security 2018. Wanneer u deze kleine en weinig opdringerige widget toevoegt aan uw bureaublad, kunt u op elk ogenblik kritieke informatie zien en belangrijke taken uitvoeren.

- het hoofdvenster van Bitdefender openen.
- Scanactiviteit bewaken in real time.

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



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

Kritieke problemen beïnvloeden de beveiliging van uw systeem.

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

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

Uw systeem is beveiligd.

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

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

De onderzijde van de widget toont de teller van de ongelezen gebeurtenissen (het aantal openstaande gebeurtenissen dat is gemeld door Bitdefender, als er zijn). Klik op de gebeurtenissenteller, bijvoorbeeld 1 voor één ongelezen

gebeurtenis, om het venster Kennisgevingen te openen. Zie "*Notificaties*" (p. 15) voor meer informatie.

Bestanden en mappen scannen

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

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

Beveiligingswidget tonen/verbergen

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

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

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

De Bitdefender-veiligheidswidget is standaard uitgeschakeld.

2.2.5. Activiteit

Het Activiteitenvenster geeft informatie over de acties die de voorbije 30 dagen door Bitdefender op uw apparaat werden ondernomen. Hier kunt u controleren welke toepassingen, bedreigingen en aanvallen werden

geblokkeerd tijdens deze periode en of er ransomeware-pogingen werden ondernomen.

Bovendien kunt u naar het Bitdefender Central activiteitsoverzicht gaan als u op de bijhorende koppeling klikt.

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

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

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

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

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

    Meer informatie over antivirusbeveiliging vindt u onder "*Antivirusbeveiliging*" (p. 86).
  - **Gescande webpagina's**

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

    Meer informatie over Webbeveiliging vindt u onder "*Webbeveiliging*" (p. 110).
  - **Kwetsbaarheden**

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

    Meer informatie over de Kwetsbaarheidsscan vindt u onder "*Kwetsbaarheid*" (p. 128).

- **Gebeurtenissentijdlijn**

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

  Voor meer informatie over een gedetailleerd verslag of gebeurtenissen over de activiteit op uw computer zie "*Notificaties*" (p. 15).

- **Privacy** gebied - weergave van informatie met betrekking tot uw systeemprivacy.

  - **Bestanden in Kluis**

    Stelt u in staat te zien hoeveel bestanden zijn beveiligd tegen ongewenste toegang.

    Voor meer informatie over hoe u gecodeerde wachtwoordbeveiligde logical drives (of kluizen) kunt aanmaken op uw computer, gaat u naar "*Bestandscodering*" (p. 141).

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

  - **Vrijgemaakte ruimte**

    Stelt u in staat om weer te geven hoeveel ruimte is opgeschoond gedurende het systeemoptimaliseringsproces. Bitdefender gebruikt Tune-Up om te helpen uw systeemsnelheid te verbeteren.

    Voor meer informatie over Tune-Up, ga naar "*Extra*" (p. 179).

  - **Accu bespaard**

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

    Meer informatie over het profiel Accumodus vindt u onder "*Profiel batterijmodus*" (p. 188).

  - **Geoptimaliseerde apps**

    Hiermee kunt u het aantal toepassingen zien dat u onder de Profielen hebt gebruikt.

    Voor meer informatie over Profielen, ga naar "*Profielen*" (p. 183).

Het beveiligingsverslag controleren

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

Om het beveiligingsverslag te controleren:

1. Naar het verslag gaan:

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

     Klik op de koppeling **Veiligheidsverslag** in de rechterbenedenhoek van het venster Activiteitenverslag.

   - Rechterklik op het pictogram van het Bitdefender in het systeemvak en selecteer **Beveiligingsverslag tonen**.

   - Zodra het verslag volledig is, ontvangt u een pop-up-melding. Klik op **Tonen** om naar het activiteitenverslag te gaan.

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

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

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

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

De melding Beveiligingsverslag aan- of uitzetten

De melding Beveiligingsverslag aan- of uitzetten:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het venster **ALGEMEEN** klikt u op de overeenkomstige AAN/UIT-schakelaar.

   De melding Beveiligingsverslag is standaard ingeschakeld.

2.3. Bitdefender Central

Bitdefender Central is het webplatform waar u toegang hebt tot de online functies en diensten van het product en waar u van op afstand belantrijke taken kunt uitvoeren op toestellen waar Bitdefender op geïnstalleerd is. kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar https://central.bitdefender.com te gaan. Zodra u aangemeld bent, kunt u beginnen met het volgende:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:
  - Bitdefender Total Security 2018
  - Bitdefender Antivirus voor Mac
  - Bitdefender Mobile Security voor Android
  - Bitdefender Mobile Security voor iOS
  - Bitdefender Parental Advisor
- 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 adviseur voor de apparaten van uw kinderen en bewaak hun activiteiten, waar u ook bent.

- Ga naar het Activiteit-rapport om de status van uw huidige abonnement en de apparaten in uw netwerk te bekijken en indien nodig de prestaties van uw Windows-apparaten van op afstand te verbeteren.

Naar Bitdefender Central gaan

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

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

2.3.1. 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. Ga naar Bitdefender Central.
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).

Een nieuw apparaat toevoegen

Indien uw abonnement meer dan één toestel dekt, kunt u een nieuw toestel toevoegen en uw Bitdefender Total Security 2018 erop installeren, als volgt:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Apparaten** en klik dan op **LOKALE BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

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

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

Abonnement verlengen

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

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

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

Abonnement activeren

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

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

Een abonnement activeren met een activatiecode:

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

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

2.3.2. Mijn apparaten

Vanaf het paneel **Mijn apparaten** van Bitdefender Central kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en verbinding hebben met internet. De 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.

Klik op het uitklappijltje in de rechterbovenhoek van het scherm om de lijst van uw apparaten weer te geven naargelang hun status of hun gebruikers.

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

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

4. Selecteer **Instellingen**.
5. Voer een nieuwe naam in het veld **Naam apparaat** in en klik op **OPSLAAN**.

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

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

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Klik op **Eigenaar toevoegen**, vul de bijbehorende velden in. Pas het profiel aan met de toevoeging van een foto en de instelling van een geboortedatum.
6. Klik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en klik op **Toewijzen**.

Bitdefender van op afstand op een apparaat updaten:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ 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, komen de volgende tabbladen beschikbaar:

- **Bedieningspaneel**. In dit venster vindt u gegevens over het geselecteerde apparaat, kunt u de beveiligingsstatus en de Bitdefender VPN-status nakijken en kunt u nagaan hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus kan groen zijn (dan zijn er

geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Klik voor meer informatie op het uitklappijltje in het bovenste statusgebied indien uw apparaat problemen ondervindt. Van hieruit kunt u problemen manueel oplossen die de veiligheid van uw toestellen aantasten.

- **Bescherming**. Vanuit dit venster kunt u van op afstand een Snelle of Systeemscan uitvoeren op uw toestellen. Klik op de **SCAN**-knop om het proces te starten. U kunt ook nagaan wanneer de laatste scan werd uitgevoerd op het toestel en van de laatste scan met de belangrijkste informatie is er een verslag beschikbaar.Voor meer informatie over deze twee scanprocessen, verwijzen we naar "*Een systeemscan uitvoeren*" (p. 94) en naar "*Een snelle scan uitvoeren*" (p. 93).
- **Optimizer**. Hier kunt u de prestaties van een toestel van op afstand verbeteren door snel te scanne, te detecteren en nutteloze bestanden op te schonen. Klik op de **START**-knop en selecteer daarna de gebieden die u wilt optimaliseren. Klik opnieuw op de **START**-knop om het optimalisatieproces te starten. Klik op de koppeling **Meer details** om naar een gedetailleerd rapport over de opgeloste problemen te gaan.

  U kunt ook het opstarten van uw toestel verbeteren door die applicaties op te sporen die veel systeemcapaciteit verbruiken. Klik op de **MEER DETAILS**-knop en kies vervolgens wat u wilt doen met de gedetecteerde applicaties. Voor meer details over deze functies, ga naar "*De snelheid van uw systeem optimaliseren in een enkele klik*" (p. 179) en "*De opstarttijd van uw pc aan het optimaliseren*" (p. 180).
- **Antidiefstal**. In geval van misplaatsing, diefstal of verlies, kunt u uw toestel met de Antidiefstalfunctie lokaliseren en van op afstand actie ondernemen. Klik op **LOKALISEREN** om te weten waar het toestel zich bevindt. De laatst gekende positie zal worden weergegeven, samen met de tijd en datum. Zie "*Anti-Theft voor mobiele apparaten*" (p. 175) voor meer informatie over deze functie.
- **Kwetsbaarheid**. Om de eventuele kwetsbaarheid van een toestel te controleren, zoals ontbrekende Window-updates, verouderde applicaties of zwakke wachtwoorden, klik op de **SCAN**-knop in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet van op afstand afgehandeld worden. Indien er een kwetsbaarheid wordt opgemerkt, moet u een nieuwe scan op het toestel laten lopen en daarna de aanbevolen acties ondernemen. Klik op **Meer details** om naar een gedetailleerd rapport over

de gevonden problemen te gaan. Zie "*Kwetsbaarheid*" (p. 128) voor meer informatie over deze functie.

2.3.3. Activiteit

Het activiteitengedeelte in Bitdefender Central is enkel toegankelijk voor de gebruikers die een Bitdefender Family Pack 2018- of Bitdefender Total Security Multi-Device 2018-abonnement hebben dat aan hun accounts gekoppeld is. De bedoeling ervan is te rapporteren hoe Bitdefender de apparaten waarop het geïnstalleerd is, de voorbije dagen heeft beschermd en informatie te tonen over het bijhorende abonnement.

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

- **Bescherming**. Hier kunt u informatie bekijken over de bestanden, toepassingen en URL's die werden geblokkeerd wegens verdacht gedrag. Om u te tonen wanneer de problemen zijn opgetreden, geven grafieken de verzamelde gegevens weer, verdeeld in dagen en het aantal gedetecteerde dreigingen. Bovendien kunt u de muis over de weergegevens informatie bewegen om het aantal gedetecteerde dreigingen te kennen.

  Onderaan de kaart ziet u de naam van het apparaat met het hoogste aantal dreigingen.

- **Tune-Up**. Van hieruit kunt u de prestaties optimaliseren van de Windows-apparaten waarop u het Bitdefender Total Security 2018-product hebt geïnstalleerd. De weergegeven informatie is gebaseerd op de optimalisatiefunctie voor opstart, die toont welke toepassingen er actief zijn tijdens het opstarten van het systeem en u het gedrag ervan in deze stap laat beheren. Afhankelijk van de beslissingen die de gemeenschap neemt door toepassing van het **Uitstellen**-commando, worden enkel de drie bovenste apparaten weergegeven. Klik op **Toepassen** om de voorgestelde wijzigingen aan te brengen op het geselecteerde apparaat.

  Klik op de koppeling die het aantal gedetecteerde toepassingen weergeeft en de gewonnen tijd om de beslissingen van andere Bitdefender-gebruikers te bekijken. Details over de tijd die uw systeem nodig heeft om op te starten, worden de tijd die de apps nodig hebben bij het opstarten en de geoptimaliseerde tijd weergegeven. Selecteer **ALLES UITSTELLLEN** indien u wilt verhinderen dat ze tijdens het opstarten actief zijn. Voor meer informatie over de optimalisatiefunctie tijdens het opstarten van Bitdefender, ga naar "*De opstarttijd van uw pc aan het optimaliseren*" (p. 180).

Opmerking
Indien er geen Bitdefender-bescherming op uw Windows-apparaten geïnstalleerd is, zal de **Tune-Up**-kaart geen informatie bevatten.

- **Abonnement**. Hier ziet u hoeveel apparaten onder uw abonnement vallen en op hoeveel apparaten u de Bitdefender-bescherming hebt geïnstalleerd. Om Bitdefender op andere apparaten te installeren, klikt u onder het besturingssysteem dat u wenst op de knop **INSTALLEREN** en volgt u de vereiste stappen.

  De naam van het gebruikte abonnement wordt weergegeven met een gekleurde stip:

  - Paars - uw abonnement is actief.
  - Rood - uw abonnement verloopt binnenkort. We bevelen u aan het zo snel mogelijk te verlengen zodat u uw apparaten beschermd houdt.

  Klik op de koppeling **Meer informatie** om naar de pagina **Abonnementen** te gaan, waar u gedetailleerde informatie kunt bekijken over uw actieve abonnement.

2.3.4. Mijn account

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

Zodra u in de rechterbovenhoek van het scherm op de -icoon klikt en **Mijn account** kiest, krijgt u de volgende tabs:

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

2.3.5. Notificaties

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

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

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

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

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

- Als uw computer een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in "*Bitdefender configureren voor het gebruik van een proxy-internetverbinding*" (p. 80).
- Er kunnen fouten optreden tijdens het downloaden van updates bij een trage internetverbinding. Om te weten hoe u dergelijke fouten herstelt, ga naar "*Bitdefender updaten bij een langzame internetverbinding*" (p. 202).
- Als u met het Internet bent verbonden via een inbelverbinding, dan adviseren wij Bitdefender regelmatig handmatig te updaten. Zie "*Een update uitvoeren*" (p. 45) 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, controleert u de **Beveiligingsstatus** links van het Statusgebied.

Controleer de updategebeurtenissen voor gedetailleerde informatie over de laatste updates:

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

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

2.4.2. Een update uitvoeren

Om updates uit te voeren is een internetverbinding vereist.

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

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

De 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 computer opnieuw op te starten wanneer de update is voltooid. Wij adviseren dit zo snel mogelijk te doen.

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

Bitdefender van op afstand op een apparaat updaten:

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

3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ 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 op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **UPDATE**.
3. Klik op de bijhorende AAN/UIT-schakelaar.
4. Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kunt de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart.

Waarschuwing

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

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

Update-frequentie

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

Update-locatie

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

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

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

Regels voor behandelen updates

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

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

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

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

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 zullen enkel geleverd worden aan gebruikers bij wie Bitdefender 2017 geïnstalleerd is.

3. ZO WERKT HET

3.1. Installatie

3.1.1. Hoe installeer ik Bitdefender op een tweede computer?

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

Bitdefender op een tweede computer installeren:

1. Klik op de koppeling **OP EEN ANDER APPARAAT INSTALLEREN** in de rechterbenedenhoek van de Bitdefender-interface.

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

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

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

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

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

3.1.2. 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.

Indien een van de vermelde situaties op jou van toepassing is, volg dan deze stappen:

- In **Windows 7**:

  1. Klik op **Start** en ga naar **Alle Programma's**.

2. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
3. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
4. U moet de computer opnieuw opstarten om het proces te voltooien.

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

1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
4. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
5. U moet de computer opnieuw opstarten om het proces te voltooien.

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op de **Systeem**-icoon in Instellingen, selecteer dan **Apps & functies**.
3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **OPNIEUW INSTALLEREN**.
6. U moet de computer 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.

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

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

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

Bitdefender installeren via Bitdefender Central:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Apparaten** en klik dan op **LOKALE BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:
   - **DOWNLOADEN**

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

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

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

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

Om Bitdefender in een andere taal:

1. Bitdefender verwijderen door het volgen van deze stappen:
   - In **Windows 7**:
     a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
     b. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
     c. Klik op **VERWIJDEREN** in het venster dat verschijnt.
     d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8 en Windows 8.1**:
  a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  c. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  d. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  e. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:
  a. Klik op **Start**, klik dan op Instellingen.
  b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  c. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  e. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  f. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

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

        Klik op de knop en sla het installatiebestand op.

- **Op een ander apparaat**

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

4. Start het gedownloade Bitdefender-programma.

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

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

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

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

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

Er kunnen zich twee gevallen voordoen:

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

  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. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
    3. Klik op **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 Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
4. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
5. 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 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
6. 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.

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.

- U hebt uw systeem gewijzigd en u wilt doorgaan met het gebruik van de beveiliging van Bitdefender. Daarvoor moet u het product opnieuw installeren met gebruikmaking van de nieuwste versie.

  Om dit probleem op te lossen:

  1. Download het installatiebestand:
     a. Ga naar Bitdefender Central.
     b. Selecteer het paneel **Apparaten** en klik dan op **LOKALE BESCHERMING INSTALLEREN**.
     c. Kies een van de twee beschikbare opties:
        - **DOWNLOADEN**

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

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

  Raadpleeg "*Bitdefender Antivirus for Mac installeren*" (p. 225) voor meer informatie over het Bitdefender-installatieproces.

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

Vanaf Bitdefender 2018 kunt u upgraden naar de recentste versie zonder dat de manuele procedure voor de-installeren en opnieuw installeren moet gevolgd worden. 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 2017 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 tot de computer opnieuw opstart.

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:http://www.bitdefender.nl/Downloads/. De activatie is enkel mogelijk met een geldig abonnement.

3.2. Abonnementen

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

Indien u een geldige licentiesleutel hebt en u deze wilt gebruiken om een abonnement voor Bitdefender Total Security 2018 te activeren, hebt u twee keuzes:

- U hebt een upgrade gedaan voor een vorige Bitdefender-versie naar de nieuwe:
  1. Zodra de upgrade naar Bitdefender Total Security 2018 voltooid is, wordt u gevraagd u aan te melden op uw Bitdefender-account.
  2. Klik op **Aanmelden** en voer het e-mailadres en het wachtwoord van uw Bitdefender-account in.
  3. Klik op **AANMELDEN** om door te gaan.
  4. Er verschijnt een kennisgeving die u meldt dat een abonnement werd aangemaakt op uw accountscherm. Het aangemaakte abonnement zal geldig zijn voor de resterende dagen op uw licentiesleutel en voor hetzelfde aantal gebruikers.

     Toestellen die eerdere versies van Bitdefender gebruiken en geregistreerd zijn met de licentiesleutel, die u naar een abonnement hebt geconverteerd, moeten het product activerenmet dezelfde Bitdefender-account.

- Bitdefender werd eerder nog niet op het systeem geïnstalleerd:
  1. Zodra het installatieproces voltooid is, wordt u gevraagd u aan te melden op uw Bitdefender-account.
  2. Klik op **Aanmelden** en voer het e-mailadres en het wachtwoord van uw Bitdefender-account in.
  3. Klik op **AANMELDEN** om verder te gaan en daarna op de knop **VOLTOOIEN** om naar de Bitdefender Total Security 2018-interface te gaan.
  4. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  5. Klik op de koppeling **Activatiecode**.

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

3.3. Bitdefender Central

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

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

Een andere account met succes gebruiken:

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

Opmerking
Het Bitdefender-product van uw toestel verandert automatisch volgens het abonnement dat verbonden is met de nieuwe Bitdefender-account.

Als er geen beschikbaar abonnement gekoppeld is aan de Bitdefender-account, of als u deze wilt overzetten naar de vorige account, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in deel *"Hulp vragen"* (p. 329).

3.3.2. Hoe schakel ik Bitdefender Central-hulpberichten uit?

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

Indien u deze berichten niet meer wil zien:

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

3.3.3. 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:

- Vanuit de Bitdefender-interface:

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

     Er verschijnt een nieuw venster.
  3. Klik op de link **Mijn wachtwoord vergeten**.
  4. Typ het e-mailadres dat u hebt gebruikt om Bitdefender-account aan te maken en klik op de knop **WACHTWOORD VERGETEN**.
  5. Controleer uw e-mail en klik op de verschafte knop.

     Het venster Bitdefender WACHTWOORD TERUGSTELLEN gaat open.

6. Voer uw e-mailadres en het nieuwe wachtwoord in het overeenkomstige veld in. Het wachtwoord moet minstens 8 karakters lang zijn en cijfers bevatten.
7. Klik op de knop **WACHTWOORD TERUGSTELLEN**.

- Vanuit uw webbrowser:

1. Ga naar https://central.bitdefender.com.
2. Klik op de link **Mijn wachtwoord vergeten**.
3. Tik uw e-mailadres in en klik vervolgens op de knop **WACHTWOORD VERGETEN**.
4. 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.

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

3.4. Scannen met Bitdefender

3.4.1. Een bestand of map scannen

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

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

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

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

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

3.4.2. Hoe kan ik mijn systeem scannen?

Om een volledige scan van het systeem uit te voeren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **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 "*Antivirusscanwizard*" (p. 97) voor meer informatie.

3.4.3. Hoe plan ik een scan?

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

Een scan plannen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **Scans beheren**.

4. Om het scantype te kiezen dat u wilt plannen, volledige systeemscan of snelle scan, klikt u op **Scanopties**.

   U kunt ook een scantype aanmaken om aan uw behoeften aan te passen door op **Nieuwe aangepaste taak** te klikken.

5. Activeer de **Planning**-schakelaar.

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

   - Bij opstarten systeem
   - Eenmalig
   - Periodiek

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

3.4.4. Een aangepaste scantaak maken

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

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

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

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

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

6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.
7. Gebruik de overeenkomstige schakelaar indien u een planning wilt instellen voor uw scantaak.

8. Klik op **Scan starten** en volg de scanwizard om de scan te voltooien. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.
9. Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

3.4.5. Een map uitsluiten van de scan

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

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

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

Om een map toe te voegen aan de lijst Uitsluitingen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Klik op het tabblad **UITSLUITINGEN**.
5. Klik op het uitklapmenu **Lijst van bestanden en mappen die uitgesloten worden voor de scan** en klik vervolgens op de knop **TOEVOEGEN**.
6. Klik op **OVERLOPEN**, selecteer de map die uit de scan wilt uitsluiten en kies vervolgens het type scan waar ze uit moet uitgesloten worden.
7. Klik op **Toevoegen** om de wijzigingen op te slaan en het venster te sluiten.

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

Er kunnen gevallen zijn waarbij Bitdefender een rechtmatig bestand verkeerdelijk markeert als een bedreiging (vals positief). Om deze fout te

corrigeren, voegt u het bestand toe aan het gebied Uitsluitingen van Bitdefender:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.

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

   b. Klik op de koppeling **FUNCTIES BEKIJKEN**.

   c. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.

   d. Klik in het venster **SCHILD** op de schakelaar AAN/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*" (p. 82).

3. Het bestand herstellen vanaf het quarantainegebied:

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

   b. Klik op de koppeling **FUNCTIES BEKIJKEN**.

   c. In het **ANTIVIRUS**-panel klikt u op **Quarantaine**.

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

4. Het bestand toevoegen aan de lijst Uitsluitingen. Om te weten hoe u dit kunt doen, ga naar "*Een map uitsluiten van de scan*" (p. 62).

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*" (p. 329).

3.4.7. 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.

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

Een scanlog of een gedetecteerde infectie later bekijken:

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

   Hier vindt u alle gebeurtenissen van scans op 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.

3.5. Ouderlijk Adviseur

3.5.1. Mijn kinderen beschermen tegen online bedreigingen

Met Ouderlijk Adviseur van Bitdefender kunt u de toegang tot internet en specifieke toepassingen beperken en voorkomen dat uw kinderen ongepaste inhoud bekijken wanneer u niet in de buurt bent.

De Ouderlijk adviseur configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het panel **OUDERLIJK ADVISEUR** klikt u op **Configureren**.

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

4. De overzichtspagina van Ouderlijk adviseur wordt geopend. Hier kunt u de instellingen voor Ouderlijk Adviseur controleren en configureren.
5. Klik op **PROFIEL TOEVOEGEN** in het rechtergedeelte van het **MIJN KINDEREN**-venster.
6. Voer specifieke informatie in de overeenkomstige velden in, zoals: naam en geboortedatum. Om een profielfoto toe te voegen, klikt u op de koppeling **Bestand kiezen**. Klik op **VOLGENDE STAP** om door te gaan.

   Op basis van normen voor de ontwikkeling van kinderen, laadt de geboortedatum van het kind instellingen voor het doorzoeken van het internet die als geschikt geacht worden voor deze leeftijdcategorie.
7. Indien Bitdefender Total Security 2018 al op het apparaat van uw kind geïnstalleerd is, selecteer dit apparaat uit de beschikbare lijst en selecteer de account die u wenst te controleren. Klik op **OPSLAAN**.

   Indien uw kind een Android- of iOS-toestel gebruikt en de toepassing Bitdefender Ouderlijk adviseur nog niet geïnstalleerd is, klikt u op **APPARAAT TOEVOEGEN**. Indien uw kind een Mac-apparaat gebruikt en de Bitdefender Antivirus for Mac-app niet geïnstalleerd is, klikt u op dezelfde knop. Selecteer het besturingssysteem waarop u de app wenst te installeren en klik op **VOLGENDE STAP** om verder te gaan.
8. Voer het e-mailadres in waar we de downloadkoppeling voor de installatie van de toepassing Ouderlijke Adviseur voor het Bitdefender-toepassing heen moeten sturen en klik vervolgens op **INSTALLATIEKOPPELING VERZENDEN**.

Controleer de activiteiten van uw kinderen en wijzig de instellingen voor Ouderlijk Adviseur via Bitdefender-account vanaf elke computer of elk mobiel apparaat met internetverbinding.

Belangrijk

Op toestellen die op Windows gebaseerd zijn, hebt u in uw abonnement opgenomen dat Bitdefender Total Security 2018 moet gedownload en geïnstalleerd worden.
Op macOS-apparaten moet het Bitdefender Antivirus for Mac-product gedownload en geïnstalleerd worden.
Op Android en iOS-apparaten moet de toepassing Ouderlijk Adviseur van Bitdefender gedownload en geïnstalleerd worden.

3.5.2. Hoe blokkeer ik de toegang van mijn kind tot een website?

Via Ouderlijk Adviseur van Bitdefender kunt u de inhoud die uw kind bekijkt met zijn apparaat controleren en de toegang tot een website blokkeren.

Om de toegang tot een website te blokkeren, moet u deze toevoegen tot de Uistluitingelijst, als volgt:

1. Ga naar https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk Adviseur** om het dashboard te openen.
4. Selecteer het profiel van uw kind in het **MIJN KINDEREN**-venster.
5. Klik op het tabblad **Websites**.
6. Klik op de knop **BEHEREN**.
7. Voer de webpagina die u wilt blokkeren in het overeenkomstige veld in.
8. Klik op **Toestaan** of **Blokkeren**.
9. Klik op **VOLTOOIEN** om de wijzigingen op te slaan.

Opmerking
Er kunnen enkel beperkingen ingesteld worden voor Android- en Windows-apparaten.

3.5.3. Hoe verhinder ik dat mijn kind een spel speelt?

Met Bitdefender Ouderlijk Adviseur hebt u het beheer over de inhoud waarvoor uw kind toegang hebben wanneer ze de computer gebruiken.

Toegang tot een game blokkeren:

1. Ga naar https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk Adviseur** om het dashboard te openen.
4. Selecteer het profiel van uw kind in het **MIJN KINDEREN**-venster.
5. Selecteer het tabblad **Toepassingen**.

   Er wordt een lijst met kaarten weergegeven. De kaarten vertegenwoordigen de apps die uw kind gebruikt.

6. Selecteer de kaart met de app die u uw kind niet langer wilt laten gebruiken.

   De markeringssymbool dat verschijnt toont dat uw kind de app niet zal kunnen gebruiken.

3.5.4. Hoe voorkom ik dat mijn kind in contact komt met onbetrouwbare personen?

Ouderlijk Adviseur van Bitdefender biedt u de mogelijkheid om telefoonoproepen van ongekende telefoonnummers of van vrienden uit de telefoonlijst van uw kind te blokkeren.

Om een specifiek contact op een Android-apparaat met daarop Bitdefender Ouderlijk adviseur geïnstalleerd te blokkeren:

1. Ga naar https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk Adviseur** om het dashboard te openen.
4. Selecteer het profiel van het kind waarvoor u beperkingen wilt instellen.
5. Selecteer het tabblad **Telefooncontacten**.

   Er wordt een lijst met kaarten weergegeven. Op deze kaart staan de contacten op de telefoon van uw kind.
6. Selecteer de kaart met het telefoonnummer dat u wilt blokkeren.

   Het markeringssymbool dat verschijnt, geeft aan dat uw kind niet zal bereikt worden via het geselecteerde telefoonnummer.

Om een specifiek contact op een Android-apparaat met waar Bitdefender Ouderlijk adviseur niet op geïnstalleerd is, te blokkeren:

1. Ga naar https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk Adviseur** om het dashboard te openen.
4. Selecteer het profiel van het kind waarvoor u beperkingen wilt instellen.
5. Klik op de gewenste kaart op de koppeling **Ouderlijk adviseur installeren op een apparaat**.
6. Klik op **APPARAAT TOEVOEGEN** in het venster dat verschijnt.

7. De **Bitdefender Ouderlijk adviseur voor Android**-optie is standaard geselecteerd. Klik op **VOLGENDE STAP** om verder te gaan en installeer vervolgens de app op het gewenste apparaat.
8. Selecteer het tabblad **Telefooncontacten**.

   Er wordt een lijst met kaarten weergegeven. De kaarten staan voor de contacten uit de Android-smartphone van uw kind.
9. Selecteer de kaart met het telefoonnummer dat u wilt blokkeren.

   Het markeringssymbool dat verschijnt, geeft aan dat uw kind niet zal bereikt worden via het geselecteerde telefoonnummer.

Om ongekende telefoonnummers te blokkeren, activeert u de schakelaar **Interactie zonder ID beller blokkeren**.

Opmerking
Er kunnen enkel beperkingen voor telefoongesprekken ingesteld worden voor Android-apparaten die aan het profiel van uw kind werden toegevoegd.

3.5.5. Hoe kan ik een lokatie als veilig of beperkt instellen voor mijn kind?

Met Ouderlijke Adviseur van Bitdefender kunt u een lokatie als veilig of beperkt instellen voor uw kind.

Een locatie instellen:

1. Ga naar https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk Adviseur** om het dashboard te openen.
4. Selecteer het profiel van uw kind in het **MIJN KINDEREN**-venster.
5. Selecteer het tabblad **Locatie kind**.
6. Klik op **Apparaten** in het rooster van het **Locatie kind**-venster.
7. Klik op **APPARATEN KIEZEN** en selecteer vervolgens het apparaat dat u wenst te configureren.
8. Klik in het **Gebieden**-venster op de knop **GEBIED TOEVOEGEN**.
9. Kies het type locatie, **VEILIG** or **BEPERKT**.

10. Tik een geldige naam in voor het gebied waar uw kind al dan niet toegang toe heeft.
11. Stel het bereik in dat moet worden toegepast voor controle via de glijder **Radius**.
12. Klik op **GEBIED TOEVOEGEN** om uw instellingen op te slaan.

Wanneer u een beperkte lokatie als veilig wilt instellen of een veilige lokatie als beperkt wilt instellen, klik erop en selecteer vervolgens de knop **GEBIED BEWERKEN**. Afhankelijk van de wijziging die u wilt doorvoeren, selecteert u de optie **VEILIG** of **BEPERKT** en klikt u op **GEBIED BIJWERKEN**.

3.5.6. Hoe blokkeer ik de toegang van mijn kind tot de toegekende apparaten tijdens schooldagen?

Via Bitdefender Ouderlijk toezicht kunt u de toegang van uw kind tot de toegekende apparaten beperken tijdens de schooluren en op momenten dat huiswerk moet gemaakt worden.

Om beperkingen te programmeren:

1. Open het paneel van Ouderlijk Adviseur vanaf Bitdefender Central.
2. Vanuit het venster **MIJN KINDEREN** selecteert u het profiel van het kind waar u beperkingen op wenst toe te passen.
3. Selecteer het tabblad **Tijdschema**.
4. In het gebied **BEPERKINGEN OVERDAG** klikt u op **SPECIFIEK**.
5. Selecteer het vakje **Tijdsbeperkingen schooldagen**.
6. Selecteer de tijdsintervallen in het rooster waarbinnen toegang moet geblokkeerd worden.

Opmerking
Er kunnen enkel beperkingen ingesteld worden voor Android- en Windows-apparaten.

3.5.7. Hoe blokkeer ik de toegang van mijn kind tot de toegekende apparaten tijdens schoolnachten?

Via Bitdefender Ouderlijk adviseur kunt u de toegang van uw kind tot de toegekende apparaten tijdens de schoolnachten beperken.

Om beperkingen te programmeren:

1. Open het paneel van Ouderlijk Adviseur vanaf Bitdefender Central.
2. Vanuit het venster **MIJN KINDEREN** selecteert u het profiel van het kind waar u beperkingen op wenst toe te passen.
3. Selecteer het tabblad **Tijdschema**.
4. Selecteer in het gebied **Bedtijd** het vakje **Schoolnachten**.
5. Gebruik de pijltjes naar boven of beneden in de bijhorende vakjes om de tijdsintervallen waarin de toegang moet geblokkeerd worden, te bepalen.

Opmerking
Er kunnen enkel beperkingen ingesteld worden voor Android- en Windows-apparaten.

3.5.8. Hoe blokkeer ik de toegang van mijn kind tot de toegekende apparaten tijdens het weekend?

Via Bitdefender Ouderlijk adviseur kunt u de toegang van uw kind tot de toegekende apparaten tijdens de weekenddagen en -nachten beperken.

Om beperkingen te programmeren:

1. Open het paneel van Ouderlijk Adviseur vanaf Bitdefender Central.
2. Vanuit het venster **MIJN KINDEREN** selecteert u het profiel van het kind waar u beperkingen op wenst toe te passen.
3. Selecteer het tabblad **Tijdschema**.
4. Selecteer in het gebied **Bedtijd** het vakje **Weekendnachten**.
5. Gebruik de pijltjes naar boven of beneden in de bijhorende vakjes om de tijdsintervallen waarin de toegang moet geblokkeerd worden, te bepalen.
6. In het gebied **LIMIETEN OVERDAG** krijgt u de volgende opties:
   - **CUMULATIEF**
     a. Selecteer het vakje **Tijdsbeperkingen weekends**.
     b. Sleep de balkjes langs de schaal naar de gewenste lengte dat toegang tot de apparaten toegestaan is.
   - **SPECIFIEK**
     a. Selecteer het vakje **Tijdsbeperkingen weekends**.

b. Selecteer de tijdsintervallen in het rooster waarbinnen toegang moet geblokkeerd worden.

Merk op dat de instellingen **CUMULATIEF** en **SPECIFIEK** niet bedoeld zijn om samen te werken.

Opmerking
Er kunnen enkel beperkingen ingesteld worden voor Android- en Windows-apparaten.

3.5.9. Hoe kan een kindprofiel worden verwijderd

Indien u een bestaand kindprofiel wenst te verwijderen:

1. Ga naar https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk Adviseur** om het dashboard te openen.
4. Klik op de ⋮ -icoon in het profiel van het kind dat uw wilt verwijderen en kies vervolgens **Verwijderen**.

3.6. Privacy bescherming

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

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

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

Uw online activiteit veilig en privé houden:

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

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

3.6.2. 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. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
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.
   - **Waarschuwing** - een waarschuwing op het toestel verzenden.
   - **Vergrendelen** - Vergrendel uw computer en stel een numerieke PINcode in om hem te ontgrendelen. U kunt ook de overeenkomstige optie activeren om Bitdefender snapshots te laten maken van de persoon die uw apparaat probeert te openen.
   - **Wissen** - verwijder alle gegevens van uw computer.

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

   - **Toon IP** - geeft het laatste IP-adres voor het geselecteerde apparaat weer.

3.6.3. Bestandskluizen gebruiken

Met Bitdefender Bestandskluis kunt u gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer maken waar u uw confidentiële en gevoelige documenten veilig kunt opslaan. De kluis is in

werkelijkheid een bestand dat op de lokale harde schijf is opgeslagen met de extensie .bvd.

Wanneer u een bestandskluis maakt, zijn twee aspecten belangrijk: de grootte en het wachtwoord. De standaardgrootte van 100 MB zou moeten voldoende zijn voor uw persoonlijke documenten, Excel-bestanden en andere gelijksoortige gegevens. Voor video's of andere grote bestanden kunt u echter meer ruimte nodig hebben.

Om uw vertrouwelijke of gevoelige bestanden of mappen veilig op te slaan in Bitdefender-bestandskluizen:

- **Maak een bestandskluis en stel er een sterk wachtwoord voor in.**

  Om een kluis te maken en te openen, klikt u met de rechtermuisknop in een leeg gebied op het bureaublad of in een map op uw computer. Wijs vervolgens **Bitdefender** > **Bitdefender Bestandskluis** aan en selecteer **Bestandskluis maken**.

  Er verschijnt een nieuw venster. Ga als volgt te werk:

  1. Klik op **Bladeren** , selecteer de plaats van de kluis en sla het kluisbestand op met de door u gewenste naam.
  2. Kies een schijfletter in het menu. Als u de kluis opent, verschijnt een virtuele schijf met de geselecteered schijfletter in **Deze computer**.
  3. Typ het wachtwoord voor de kluis in de velden **Wachtwoord** en **Bevestigen** in.
  4. Als u de standaardgrootte (100 MB) van de kluis wilt veranderen, gebruikt u de pijltjes omhoog en omlaag in het uitklapmenu van de **Kluisgrootte (MB)**.
  5. Klik op **Maken**.

  Opmerking
  Als u de kluis opent, verschijnt een vituele schijf in **Deze computer**. De schijf heeft de schijfletter die is toegewezen aan de kluis.

- **Voeg de bestanden of mappen die u wilt beveiligen toe aan de kluis.**

  Om een bestand aan een kluis toe te voegen, moet u eerst de kluis openen.

  1. Blader naar het bvd-kluisbestand.

2. Klik met de rechtermuisknop op het kluisbestand, selecteer Bitdefender Bestandskluis en selecteer **Openen**.
3. In het venster dat verschijnt, voert u het wachtwoord in, selecteert u de letter van de drive waar u de kluis aan toe wilt kennen en klikt u op **OK**.

U kunt nu via Windows Verkenner bewerkingen uitvoeren op het station dat overeenkomt met de gewenste bestandskluis, net zoals bij een gewoon station. Om een bestand aan een open kluis toe te voegen, kunt u ook met de rechtermuisknop op een bestand klikken, Bitdefender bestandskluis aanwijzen en **Toevoegen aan bestandskluis** selecteren.

- **Houd de kluis op elk ogenblik vergrendeld.**

  Open alleen kluizen als de toegang vereist is of als u hun inhoud moet beheren. Om een kluis te vergrendelen, klikt u met de rechtermuisknop op het overeenkomende virtuele schijfstation onder **Deze computer**. Wijs vervolgens **Bitdefender Bestandskluis** aan en selecteer **Vergrendelen**.

- **Zorg dat u het bvd-kluisbestand niet verwijdert.**

  Wanneer u het bestand verwijderd, wordt ook de inhoud van de kluis verwijderd.

Raadpleeg "*Bestandscodering*" (p. 141) voor meer informatie over het werken met bestandskluizen.

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

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

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

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

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

3.6.5. 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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **WEBCAMBESCHERMING**-panel klikt u op **Webcamtoegang**.

   De lijst met de toepassingen die toegang tot uw camera gevraagd hebben, wordt weergegeven.
4. Ga naar de toepassing die u toegang wilt toestaan of weigeren en klik daarna op de bijhorende schakelaar.

   Om te zien wat andere Bitdefender-gebruikers hebben gekozen om met deze geselecteerde toepassing te doen, klik op de icoon . U zult een melding krijgen telkens wanneer een van de opgelijste toepassingen werd geblokkeerd door de Bitdefender-gebruikers, wat de status van Autopilot ook is.

Om manueel toepassingen aan deze lijst toe te voegen, klik op de koppeling **Een nieuwe toepassing aan de lijst toevoegen**.

3.7. Optimalisatiehulpmiddelen

3.7.1. Mijn systeemprestaties verbeteren

De systeemprestaties zijn niet alleen afhankelijk van hardwareconfiguratie, zoals de CPU-belasting, het geheugengebruik en de harde schijfruimte. Deze is ook gekoppeld aan uw softwareconfiguratie en uw gegevensbeheer.

Dit zijn de belangrijkste acties die u kunt ondernemen met Bitdefender om de snelheid en prestaties van uw systeem te verbeteren:

- "*De prestaties van uw systeem optimaliseren in een enkele klik*" (p. 76)
- "*Scan uw systeem periodiek*" (p. 76)

De prestaties van uw systeem optimaliseren in een enkele klik

De optie OneClick Optimizer bespaart u waardevolle tijd als u een snelle manier wilt om uw systeemprestaties te verbeteren door snel scannen, detecteren en schoonmaken van nutteloze bestanden.

Om het OneClick Optimizer-proces te starten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **OneClick Optimizer**.
3. Laat Bitdefender naar bestanden zoeken die kunnen worden verwijderd en klik dan op de knop **OPTIMALISEREN** om het proces te voltooien.

Meer informatie over het verbeteren van de snelheid van uw computer in een enkele klik vindt u onder "*De snelheid van uw systeem optimaliseren in een enkele klik*" (p. 179).

Scan uw systeem periodiek

De snelheid en het algemene gedrag van uw systeem kan ook worden beïnvloed door bedreigingen.

Zorg dat u uw systeem periodiek scant, maar minstens eenmaal per week.

Het is aanbevolen de systeemscan te gebruiken omdat hiermee wordt gescand op alle types bedreigingen die de beveiliging van uw systeem in gevaar brengen en dit type scan ook binnen de archieven scant.

De Systeemscan starten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **Systeemscan**.
4. Volg de stappen van de wizard.

3.7.2. Hoe kan ik de opstarttijd van mijn systeem verbeteren?

Van onnodige toepassingen die de opstarttijd hinderlijk vertragen als u uw pc aanzet kan het openen worden uitgeschakeld of uitgesteld met de Startup Optimizer waardoor u waardevolle tijd wint.

De Startup Optimizer gebruiken:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **Startup Optimizer**.
3. Selecteer de toepassingen die u wilt uitstellen bij het opstarten van het systeem.

U vindt meer informatie over het optimaliseren van de opstarttijd van uw pc onder "*De opstarttijd van uw pc aan het optimaliseren*" (p. 180).

3.8. Nuttige informatie

3.8.1. 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*" (p. 329).

3.8.2. Hoe kan ik Bitdefender verwijderen?

Als u uw Bitdefender Total Security 2018 wilt verwijderen:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  4. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:
  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Opmerking

Deze procedure voor opnieuw installeren verwijdert uw persoonlijke instellingen permanent.

3.8.3. 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 op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. Zoek **Bitdefender VPN** en selecteer **Verwijderen**.

     Wacht tot de de-installatieproces is voltooid.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. Zoek **Bitdefender VPN** en selecteer **Verwijderen**.

     Wacht tot de de-installatieproces is voltooid.
- In **Windows 10**:
  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. Zoek **Bitdefender VPN** en selecteer **Verwijderen**.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

     Wacht tot de de-installatieproces is voltooid.

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

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

Omwille van deze reden biedt Bitdefender u de mogelijkheid 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 op de computer en wilt naar bed. U wilt dat Bitdefender uw volledig systeem controleert op bedreigingen.

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

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

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

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Zie "*Antivirusscanwizard*" (p. 97) voor meer informatie.

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

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

Belangrijk

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

Uw proxy-instellingen beheren:

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

     Opmerking
     Bitdefender kan proxy-instellingen van de populairste browsers importeren, inclusief de nieuwste versies van 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 een verbinding te maken met de proxyserver.
     - **Gebruikersnaam** - voer een gebruikersnaam in die wordt herkend door de proxy.
     - **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

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

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

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

- In **Windows 7**:
  1. Klik op **Start**.

2. Zoek **Computer** in het menu **Start**.
3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
4. Kijk onder **Systeem** om de informatie over uw systeem te controleren.

- In **Windows 8**:
  1. Zoek vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm) en rechterklik op het pictogram ervan.

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

3.8.7. 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 **Beheerpaneel**.

   In **Windows 8 en Windows 8.1**: Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Selecteer **Mapopties**.
3. Ga naar het tabblad **Weergave**.
4. Selecteer **Verborgen bestanden en mappen weergeven**.
5. Vink **Extensies voor bekende bestandstypen verbergen** uit.
6. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.

7. Klik op **Toepassen**, klik daarna op **OK**.

In **Windows 10**:

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

3.8.8. Andere beveiligingsoplossingen verwijderen

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

Wanneer u meer dan één beveiligingsoplossing op dezelfde computer gebruikt, wordt het systeem onstabiel. Het installatieprogramma van Bitdefender Total Security 2018 detecteert automatisch andere beveiligingsprogramma's en biedt u de mogelijkheid om ze te verwijderen.

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

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

2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
3. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
4. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

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

3.8.9. 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 de computer opnieuw.

2. Druk meerdere keren op de **F8**-toets voordat Windows wordt gestart om toegang te krijgen tot het opstartmenu.
3. Selecteer **Veilige modus** in het opstartmenu of **Veilige modus met netwerkmogelijkheden** als u internettoegang wenst.
4. Druk op **Enter** en wacht terwijl Windows wordt geladen in Veilige modus.
5. Dit proces eindigt met een bevestigingsbericht. Klik op **OK** om te bevestigen.
6. Om Windows normaal te starten, hoeft u alleen het systeem opnieuw op te starten.

- In **Windows 8, Windows 8.1 en Windows 10**:

1. Lanceer **Systeemconfiguratie** in Windows door tegelijk op de toetsen **Windows + R** op uw keyboard te drukken.
2. Schrijf **msconfig** in het dialoogvenster **Openen** en klik daarna op **OK**.
3. Selecteer het tabblad **Opstarten**.
4. In het gebied **Opstartopties** vinkt u het vakje **Veilig opstarten** aan.
5. Klik op **Netwerk** en vervolgens op **OK**.
6. Klik op **OK** in het venster **Systeemconfiguratie** dat u vertelt dat het systeem opnieuw moet worden opgestart om de wijzigingen die u hebt ingesteld, door te voeren.

   Uw systeem wordt opnieuw opgestart in Veilige modus met Netwerk.

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

4. UW BEVEILIGING BEHEREN

4.1. Antivirusbeveiliging

Bitdefender beveiligt uw computer 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 computer 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 computer zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend. Zie "*Automatisch scannen van verwisselbare media*" (p. 102) voor meer informatie.

Geavanceerde gebruikers kunnen scanuitsluitingen configureren als ze niet willen dat er specifieke bestanden of bestandstypes worden gescand. Zie "*Scanuitsluitingen configureren*" (p. 104) 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*" (p. 107) voor meer informatie.

Als uw computer werd geïnfecteerd door bedreigingen, moet u *"Bedreigingen van uw systeem verwijderen"* (p. 213) raadplegen. Om u te helpen bij het opruimen van de bedreigingen die niet kan worden verwijderd van het Windows-besturingssysteem op uw computer, biedt Bitdefender u de *"Bitdefender Reddingsmodus (Reddingsomgeving in Windows 10)"* (p. 214). Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van bedreigingen, waarmee u uw computer onafhankelijk van Windows kunt opstarten. Wanneer de computer in de Helpmodus is (Helpomgeving in Windows 10), zijn Windows-bedreigingen inactief, zodat ze gemakkelijk kunnen worden verwijderd.

4.1.1. Scannen bij toegang (real time-beveiliging)

Bitdefender verschaft voortdurende, realtime beveiliging tegen een uitgebreide serie 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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Klik in het venster **SCHILD** op de schakelaar AAN/UIT.
5. Indien u bescherming in reële tijd wenst uit te schakelen, verschijnt een waarschuwingsscherm. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart. De realtime beveiliging wordt automatisch ingeschakeld als de geselecteerde tijd verloopt.

Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen 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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Klik in het venster **SCHILD** op het accordeonmenu **GEAVANCEERDE INSTELLINGEN TONEN**.

   Er verschijnt een venster met vakken.
5. Scrol naar beneden in het venster om de scaninstellingen te configureren zoals nodig.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

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

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

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

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

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

  Indien u beslist om deze optie te gebruiken, schakel ze in en versleep daarna de balk langs de schaal om een maximale toegelaten grootte (in MB) in te stellen voor archieven die bij toegang moeten gescand worden.

- **Scan e-mails.** Om te voorkomen dat bedreigingen naar uw computer worden gedownload, scant Bitdefender automatisch inkomende en uitgaande e-mails.

  Hoewel dit niet aanbevolen is, kunt u de scan voor bedreigingen voor e-mails uitschakelen om de systeemprestaties te verbeteren. Indien u de overeenkomstige scanopties uitschakelt, sullen de e-mails en bestanden die u ontvangt, niet worden gescand. Daardoor kunnen geïnfecteerde bestanden op uw computer worden opgeslagen. Dit is geen belangrijke bedreiging omdat de real time-beveiliging de bedreiging zal blokkeren wanneer u probeert toegang te krijgen tot de geïnfecteerde bestanden (openen, verplaatsen, kopiëren of uitvoeren).

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten. Als een bedreiging het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden

en het is mogelijk dat u dan uw systeem niet meer kunt starten en geen toegang meer hebt tot uw gegevens.

- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Scannen op keyloggers.** Selecteer deze optie om uw systeem te scannen op keyloggers. Keyloggers slaan op wat u op uw toetsenbord intypt en zenden via Internet verslagen naar een kwaadwillend persoon (hacker). De hacker kan gevoelige informatie uit de gestolen data halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.
- **Scannen bij opstarting systeem.** Selecteer de optie **Vroege opstartscan** om uw systeem te scannen bij het opstarten, zodra alle kritieke diensten geladen zijn. De bedoeling van deze functie is 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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Klik in het venster **SCHILD** op het accordeonmenu **GEAVANCEERDE INSTELLINGEN TONEN**.

   Er verschijnt een venster met vakken.
5. Scrol naar beneden in het venster tot u de optie **Acties na voltooiing van de scan** ziet.
6. Configureer de scaninstellingen zoals dat nodig is.

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

Neem gepaste acties

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

- **Geïnfecteerde bestanden.** Bestanden die als 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*" (p. 107) 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 bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update voor bedreigingen uitgegeven zodat de bedreiging kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het

archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Naar quarantaine
Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie "*Bestanden in quarantaine beheren*" (p. 107) 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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Klik in het venster **SCHILD** op het accordeonmenu **GEAVANCEERDE INSTELLINGEN TONEN**.

   Er verschijnt een venster met vakken.
5. Scrol naar beneden in het venster tot u de optie **Instellingen terugstellen** ziet. Selecteer deze optie om de antivirusinstellingen terug te stellen naar fabrieksinstellingen.

4.1.2. Scannen op aanvraag

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

Het risico bestaat dat een bedreiging zich reeds in uw systeem heeft genesteld voordat u Bitdefender installeert. Het is dan ook een bijzonder

goed idee uw computer meteen te scannen op aanwezige bedreigingen nadat u Bitdefender hebt geïnstalleerd. En het is absoluut een goed idee om uw computer 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 computer scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren. Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

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

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

Een systeemscan uitvoeren

De systeemscan scant de volledige computer 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 computer 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 computer 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*" (p. 44) voor meer informatie.
- Alle open programma's afsluiten

Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren. Zie "*Een aangepaste scan configureren*" (p. 94) voor meer informatie.

Een systeemscan lanceren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **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 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 aangepaste scan configureren

Een aangepaste, gedetailleerde scan configureren en lanceren:

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

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

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

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

   b. U kunt ook deze algemene opties configureren:

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

   c. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.
6. Indien u een planning voor uw scantaak wenst in te stellen, gebruik de **Planning**-schakelaar in het **Basis**-venster. Selecteer een van de overeenkomstige opties om een planning in te stellen:
   - Bij opstarten systeem
   - Eenmalig
   - Periodiek

7. Klik op **Scannen starten** en volg de Antivirusscanwizard om het scannen te voltooien. Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.
8. Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

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

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

dat de real time-beveiliging is ingeschakeld. Het is echter aanbevolen deze optie te gebruiken om eventuele potentiële bedreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke bedreiging gaat.

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

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

Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map, kies Bitdefender en selecteer **Scannen met**

Bitdefender), verschijnt de Antivirusscanwizard van Bitdefender. Volg de wizard om het scannen te voltooien.

Opmerking

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

Stap 1 - Scan uitvoeren

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

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

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

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

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

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

Stap 2 – Acties kiezen

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

Opmerking

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

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de 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 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*" (p. 107) 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 bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update uitgegeven zodat de bedreiging kan worden verwijderd.

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

Wissen

Verwijdert gedetecteerde bestanden van de schijf.

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

Geen actie nemen

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

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

Stap 3 – Overzicht

Wanneer Bitdefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster. Als u uitgebreide informatie over het scanproces wenst, klikt u op **LOGBOEK WEERGEVEN** om het scanlogboek weer te geven. Het logbestand wordt aangemaakt in .xml-formaat en kan lokaal worden opgeslagen via de knop **Log opslaan** en een locatie te kiezen.

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*" (p. 213).

Scanlogboeken controleren

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

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

Een scanlog of een gedetecteerde infectie later bekijken:

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

   Hier vindt u alle gebeurtenissen van scans op 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.

4.1.3. Automatisch scannen van verwisselbare media

Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw computer en scant dit op de achtergrond wanneer de Autoscan-optie geactiveerd is. Dit is aanbevolen om infecties van uw computer door bedreigingen te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

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

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

Hoe werkt het?

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

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

Als Auto Pilot is uitgeschakeld:

1. U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.
2. In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde 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.

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

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een 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*" (p. 213).

Scan verwisselbare media beheren

Automatische scans van verwisselbare media beheren:

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

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

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.

4.1.4. Gastbestand scannen

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

Om scan-gastbestanden te configureren:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **GEAVANCEERD**.
3. Klik op de bijhorende AAN/UIT-schakelaar.

4.1.5. Scanuitsluitingen configureren

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

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

Opmerking

Uitsluitingen komen NIET in aanmerking voor systeem- en contextueel scannen. Systeemscan via een scanner op verzoek biedt u de mogelijkheid om het volledige systeem te analyseren op schadelijke dreigingen die de veiligheid van uw gegevens in gevaar kunnen brengen. 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

Specifieke bestanden en mappen uitsluiten van het scannen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Klik op het uitklapmenu **Lijst van bestanden en mappen die uitgesloten worden voor de scan**. In het venster dat verschijnt, kunt u de bestanden en mappen die van het scannen zijn uitgesloten, beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik op de knop **ADD**.
   b. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**. Daarnaast kunt u ook het pad naar het bestand of de map in het bewerkingsveld typen (of kopiëren en plakken).
   c. Het geselecteerde bestand of de geselecteerde map wordt standaard uitgesloten van Scannen bij toegang en Scannen bij aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.
   d. Klik op **Toevoegen**.

Bestandsextensies uitsluiten van het scannen

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

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

Bestandsextensies uitsluiten van het scannen:

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

      txt;avi;jpg

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

Scanuitsluitingen beheren

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

Scanuitsluitingen beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
4. Selecteer het tabblad **UITSLUITINGEN**.
5. Gebruik de opties in het uitklapmenu **Lijst van bestanden en mappen die uitgesloten worden voor het scannen** om uitsluitingen voor scans te beheren.
6. Klik op een van de beschikbare koppelingen om scanuitsluitingen te verwijderen of te bewerken. Ga als volgt te werk:

- Om een gegeven uit de lijst te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.
- Om een gegeven in de tabel te bewerken, dubbelklikt u op dit item (of selecteert u het en klikt u op de knop **BEWERKEN**). Er verschijnt een nieuw venster. Hierin kunt u de extensie van het pad dat moet worden uitgesloten en het type scan waarvoor u het wilt uitsluiten wijzigen volgens uw voorkeur. Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.

4.1.6. 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.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update uitgegeven zodat de bedreiging kan worden verwijderd.

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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **Quarantaine**.

   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 database van malware-handtekeningen

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.

Voeg verdachte bestanden die in quarantaine staan toe voor analyse

Houd deze optie ingeschakeld om bestanden in quarantaine automatisch naar Bitdefender te verzenden. De voorbeeldbestanden worden geanalyseerd door de bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update voor bedreigingen uitgegeven zodat de bedreiging kan worden verwijderd.

Inhoud ouder dan 30 dagen verwijderen

Bestanden in quarantaine die ouder zijn dan 30 dagen worden automatisch verwijderd.

Maak uitzondering aan voor herstelde bestanden

De bestanden die u vanuit quarantaine herstelt, worden zonder reparatie teruggezet naar hun oorspronkelijke locatie, en worden automatisch uitgesloten uit volgende scans.

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 **HERSTELLEN**.

4.2. Advanced Threat Defense

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 bedreigingen.

Geavanceerde dreigingscontrole bewaakt voortdurend de toepassingen die op de computer 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.

Om veiligheidsredenen zult u telkens wanneer een ransomware-aanval wordt opgespoord en geblokkeerd een melding ontvangen, zelfs als de Autopilot ingeschakeld is.

Advanced Threat Defense in- of uitschakelen

Advanced Threat Defense in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Ga naar het **ADVANCED THREAT DEFENSE**-venster en klik op de AAN/UIT-schakelaar.

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.

Gedetecteerde ransomware-aanvallen controleren

Om de door Advanced Threat Defense opgespoorde ransomware-aanvallen te controleren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Ga naar het **ADVANCED THREAT DEFENSE**-venster en klik op **Bescherming tegen ransomware**.
4. De eerste keer dat u Ransomware-bescherming gebruikt, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.

   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.

Opgespoorde verdachte apps controleren

Om de door Advanced Threat Defense opgespoorde verdachte apps te controleren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Ga naar het **ADVANCED THREAT DEFENSE**-venster en klik op **Verdediging dreiging**.
4. De eerste keer dat u Threat Defense gebruikt, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.

   De apps die de voorbije 90 dagen als dreigingen werden opgespoord en geblokkeerd, worden getoond. Om meer informatie te lezen over een app, het pad van het schadelijke proces en of het onschadelijk maken met succes werd uitgevoerd, kunt u er gewoon op klikken.

Processen toevoegen aan uitsluitingen

U kunt uitsluitingsregels configureren voor vertrouwde toepassingen zodat Advanced Threat Defense ze niet blokkeert als ze acties uitvoeren die op bedreigingen lijken. Advanced Threat Defense blijft de uitgesloten toepassingen bewaken.

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ADVANCED THREAT DEFENSE**-panel.
4. In het venster **WITTE LIJST** klikt u op **Toepassingen toevoegen aan de witte lijst**.
5. Zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.

   Om iets uit de lijst te verwijderen, klik op de knop **Verwijderen** ernaast.

4.3. Webbeveiliging

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

Bitdefender biedt realtime webbeveiliging voor:

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

De webbeveiligingsinstellingen configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **WEBBESCHERMING**-panel.

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

- Scan HTTP-verkeer 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 bevat mogelijke gevaarlijke onderdelen. Wees voorzichtig als deze pagina toch wilt bezoeken.

  Dit is een pagina die u veilig kunt bezoeken.

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

  Search Advisor beoordeelt de koppelingen die zijn geplaatst op de volgende online sociale netwerkservices:
  - Facebook
  - Twitter
- SSL aan het scannen

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

- Bescherming tegen fraude.
- Bescherming tegen phishing.

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

Om websites via de webbescherming van Bitdefender te configureren en beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **WEBBESCHERMING**-panel klikt u op **Witte lijst**.
4. In het tekstvak **URL toevoegen** tikt u de naam van de website in die u aan de witte lijst wilt toevoegen. Daarna klikt u op **Toevoegen**.

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

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

Bitdefender waarschuwt in de browser

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

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

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

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

4.4. Antispam

Spam is een term die wordt gebruikt voor het beschrijven van ongewenste e-mail. Spam is een groeiend probleem voor zowel individuele gebruikers als bedrijven. Het is niet mooi, u wilt niet dat uw kinderen het zien, u kunt erdoor ontslagen worden (omdat u teveel tijd verspilt of omdat u porno ontvangt op zakelijke e-mailadres) en u kunt niet verhinderen dat men u deze berichten blijft zenden. De op één na beste oplossing ligt dus voor de hand: de ontvangst van dergelijke berichten blokkeren. Jammer genoeg komen spamberichten voor in allerlei vormen en formaten en op zeer grote schaal.

Bitdefender Antispam gebruikt opmerkelijke technologische innovaties en industriestandaard antispamfilters om spam op te sporen voordat deze het Postvak IN van de gebruiker bereikt. Zie "*Antispam-begrippen*" (p. 114) voor meer informatie.

De antispambeveiliging van Bitdefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol. POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver.

Opmerking
Bitdefender biedt geen antispambeveiliging voor e-mailaccounts die u aanspreekt via een e-mailservice op Internet.

De spamberichten die door Bitdefender worden gedetecteerd, zijn gemarkeerd met de prefix [spam] in de onderwerpregel. Bitdefender verplaatst spamberichten automatisch naar een specifieke map, zoals hieronder beschreven:

- In Microsoft Outlook worden spamberichten verplaatst naar een map **Spam** die zich in de map **Verwijderde items** bevindt. Er wordt een **Spam**-map aangemaakt wanneer een e-mailbericht als spam wordt aangemerkt.
- In Mozilla Thunderbird worden spamberichten verplaatst naar een map **Spam** die zich in de map **Trash** bevindt. Er wordt een **Spam**-map aangemaakt wanneer een e-mailbericht als spam wordt aangemerkt.

Als u andere e-mailclients gebruikt, moet u een regel maken om e-mailberichten met de markering [spam] door Bitdefender te laten verplaatsen naar een aangepaste quarantainemap. Indien de mappen Verwijderde items of Prullenbak worden verwijderd, zal de Spam-map ook

verwijderd worden. Er zal echter een nieuwe Spam-map aangemaakt worden zodra er opnieuw een e-mailbericht als spam wordt aangemerkt.

4.4.1. Antispam-begrippen

Antispam-filters

DeBitdefender-Antispam-engine omvat cloud-beveiliging en andere, verschillende filters die ervoor zorgen dat uw postvak spamvrij blijft, zoals Vriendenlijst, Spammerslijst en Charsetfilter.

Vriendenlijst / Spammerslijst

De meeste mensen communiceren regelmatig met een groep mensen of ontvangen zelfs berichten van bedrijven of organisaties op hetzelfde domein. Wanneer u gebruik maakt van **vrienden- of spammerslijsten**, kunt u gemakkelijk een indeling maken van de mensen van wie u e-mails wilt ontvangen, ongeacht de inhoud (vrienden), of van de mensen van wie u nooit meer wilt horen (spammers).

Opmerking

Wij raden u aan de namen en e-mailadressen van uw vrienden toe te voegen aan de **Vriendenlijst**. Bitdefenderblokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

Tekensetfilter

Veel spamberichten zijn geschreven in Cyrillische en/of Aziatische tekensets. De tekensetfilter detecteert dit type berichten en labelt ze als SPAM.

Antispamgebruik

De Bitdefender Antispam-engine gebruikt alle antispamfilters samen om vast te stellen of een bepaald e-mailbericht in uw **Postvak IN** moet belanden.

Elke e-mail die van het internet komt, wordt eerst vergeleken met de Vriendenlijst/Spammerslijst filter. Als het adres van de afzender in de Vriendenlijst wordt gevonden, wordt de e-mail rechtstreeks naar uw **Postvak IN** verplaatst.

In het andere geval zal de filter Spammerslijst de e-mail overnemen om het adres van de afzender te controleren in zijn lijst. Als er een treffer wordt

gevonden, wordt de e-mail gelabeld als SPAM en naar de map **Spam** verplaatst.

Anders zal de Tekensetfilter controleren of de e-mail in Cyrillische of Aziatische tekens is geschreven. Als dat het geval is, wordt de e-mail gelabeld als SPAM en verplaatst naar de map **Spam**.

Opmerking

Als de e-mail het label SEXUALLY EXPLICIT vermeldt in de onderwerpregel, zal Bitdefender dit bericht als SPAM beschouwen.

Ondersteunde e-mailclients en protocollen

Antispam bescherming is aanwezig voor alle POP3/SMTP e-mailclients. De Bitdefender Antispam werkbalk is echter alleen geïntegreerd in:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 en hoger

4.4.2. De antispambeveiliging in- of uitschakelen

Antispambeveiliging is standaard ingeschakeld.

De Antispam-functie in of uit te schakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **ANTISPAM** op de schakelaar AAN/UIT.

4.4.3. De antispam-werkbalk in het venster van uw e-mailclient gebruiken

In het bovenste gebied van het venster van de e-mailclient ziet u de werkbalk Antispam. De werkbalk Antispam helpt u de antispambeveiliging direct vanaf uw e-mailclient te beheren. U kunt Bitdefender gemakkelijk corrigeren als het programma een rechtmatig bericht als SPAM heeft gemarkeerd.

Belangrijk

Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg *"Ondersteunde e-mailclients en protocollen"* (p. 115) voor een complete lijst van ondersteunde e-mailclients.

Elke knop van de Bitdefender-werkbalk wordt hieronder uitgelegd.

Instellingen - opent een venster waarin u de antispamfilters en de werkbalkinstellingen kunt configureren.
Is spam - geeft aan dat de geselecteerde e-mail spam is. De e-mail wordt onmiddellijk naar de map **Spam** verplaatst. Als de antispam-cloud-services zijn geactiveerd, wordt het bericht verzonden naar Bitdefender Cloud voor verdere analyse.
Geen spam - geeft aan dat de geselecteerde e-mail geen spam is en dat Bitdefender het niet als dusdanig mocht labelen. De e-mail wordt van de map **Spam** verplaatst naar de map van uw **Postvak IN**. Als de antispam-cloud-services zijn geactiveerd, wordt het bericht verzonden naar Bitdefender Cloud voor verdere analyse.

Belangrijk
De knop **Geen spam** wordt actief wanneer u een bericht selecteert dat door Bitdefender als SPAM is gemarkeerd (normaal bevinden deze berichten zich in de map **Spam**).

Spammer toevoegen - voegt de afzender van de geselecteerde e-mail toe aan de spammerslijst. U zult mogelijk op **OK** moeten klikken om te bevestigen. De e-mailberichten die zijn ontvangen van adressen in de spammerslijst, worden automatisch gemarkeerd als [spam].
Vriend toevoegen - voegt de afzender van de geselecteerde e-mail toe aan de vriendenlijst. U zult mogelijk op **OK** moeten klikken om te bevestigen. U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.
Spammers - opent de **Spammerslijst** die alle e-mailadressen bevatten waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud. Zie "*Spammerslijst configureren*" (p. 119) voor meer informatie.
Vrienden - opent de **Vriendenlijst** die alle e-mailadressen bevatten waarvan u altijd e-mailberichten wilt ontvangen, ongeacht hun inhoud. Zie "*De Vriendenlijst configureren*" (p. 118) voor meer informatie.

Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet als [spam] aangemerkt moeten worden). Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.

2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer het rechtmatige bericht dat door Bitdefender verkeerdelijk is gemarkeerd als [spam].
4. Klik op de knop **Vriend toevoegen** in de antispam-werkbalk van Bitdefender om de afzender aan de vriendenlijst toe te voegen. U zult mogelijk op **OK** moeten klikken om te bevestigen. U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.
5. Klik op de knop **Geen spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Het e-mailbericht wordt verplaatst naar de map Postvak IN.

Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u gemakkelijk aanduiden welke e-mailberichten niet als spam moeten worden gedetecteerd. Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop **Is spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

Werkbalkinstellingen configureren

Om de instellingen voor antispam-instellingen voor uw e-mailklant te configureren, klikt u op de knop **Instellingen** op de werkbalk en vervolgens op het tabblad **Instellingen werkbalk**.

U hebt hier de volgende opties:

- **Markeer e-mailberichten met spam als 'gelezen'** - markeert spamberichten automatisch als gelezen, zodat u er niet door wordt gestoord als ze aankomen.
- U kunt ervoor kiezen om bevestigingsvensters al dan niet weer te geven wanneer u klikt op de knoppen **Spammer toevoegen** en **Vriend toevoegen** op de antispam-werkbalk.

Bevestigingsvensters kunnen verhinderen dat u e-mailafzenders per ongeluk toevoegt aan een Vrienden-/Spammerslijst.

4.4.4. De Vriendenlijst configureren

De **Vriendenlijst** is een lijst van alle e-mailadressen waarvan u altijd berichten wilt ontvangen, ongeacht hun inhoud. Berichten van uw vrienden worden niet als spam gelabeld, zelfs niet wanneer de inhoud op spam lijkt.

Opmerking

Elke e-mail die afkomstig is van een adres in de **Vriendenlijst**, wordt automatisch en zonder verdere verwerking in uw Postvak IN geleverd.

De Vriendenlijst configureren en beheren:

- Als u Microsoft Outlook of Thunderbird gebruikt, klikt u op de knop **Vrienden** in de antispam-werkbalk van Bitdefender.
- U kunt ook:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
  3. In het **ANTISPAM**-panel klikt u op **Vrienden beheren**.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u op de knop **Toevoegen**. Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **Toevoegen**. Syntaxis:

- @domain.com en domain.com - alle ontvangen e-mailberichten van domain.com komen in uw **Postvak IN** terecht, ongeacht hun inhoud;
- domein - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) worden als SPAM gelabeld;
- com - alle ontvangen e-mailberichten met het domeinachtervoegsel com worden als SPAM gelabeld;

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn. U kunt bijvoorbeeld het e-maildomein toevoegen van het bedrijf waarvoor u werkt of de domeinen van uw vertrouwde partners toevoegen.

Om een item uit de lijst te verwijderen, klikt u op de overeenkomende koppeling **Verwijderen**. Om alle ingangen op de lijst te verwijderen, klikt u op de knop **Lijst leegmaken**.

U kunt de vriendenlijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product. Om de vriendenlijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie .bwl hebben.

Om een eerder opgeslagen vriendenlijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende bwl-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst overschrijven**.

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

4.4.5. Spammerslijst configureren

De **Spammerslijst** is een lijst van alle e-mailadressen waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud. Alle e-mailberichten die worden ontvangen van een adres van de **Spammerslijst**, worden automatisch en zonder verdere verwerking als SPAM gelabeld.

De Spammerslijst configureren en beheren:

- Als u gebruik maakt van Microsoft Outlook of Thunderbird, klikt u op de knop **Spammers** op de Bitdefender antispam-werkbalk die in uw mailklant is geïntegreerd.
- U kunt ook:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
  3. In het **ANTISPAM**-panel klikt u op **Spammers beheren**.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u op de knop **Toevoegen**. Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **Toevoegen**. Syntaxis:

- @domain.com en domain.com - alle ontvangen e-mailberichten van domain.com komen in uw **Postvak IN** terecht, ongeacht hun inhoud;
- domein - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) worden als SPAM gelabeld;

- com - alle ontvangen e-mailberichten met het domeinachtervoegsel com worden als SPAM gelabeld.

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn.

Waarschuwing

Voeg geen domein van rechtmatige webgebaseerde e-mailservices (zoals Yahoo, Gmail, Hotmail of andere) toe aan de Spammerslijst. Anders zullen de e-mailberichten die zijn ontvangen van een geregistreerde gebruiker van een dergelijke service, als spam worden gedetecteerd. Als u bijvoorbeeld yahoo.com toevoegt aan de spammerslijst, worden alle e-mailberichten die van adressen van yahoo.com afkomstig zijn, als [spam] gemarkeerd.

Om een item uit de lijst te verwijderen, klikt u op de overeenkomende koppeling **Verwijderen**. Om alle ingangen op de lijst te verwijderen, klikt u op de knop **Lijst leegmaken**.

U kunt de spammerslijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product. Om de spammerslijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie .bwl hebben.

Om een eerder opgeslagen Spammerslijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende bwl-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst overschrijven**.

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

4.4.6. De lokale antispamfilters configureren

Zoals beschreven in "*Antispam-begrippen*" (p. 114), gebruikt Bitdefender een combinatie van verschillende antispamfilters voor het identificeren van spam. De antispamfilters zijn vooraf geconfigureerde voor een efficiënte bescherming.

Belangrijk

Afhankelijk van het feit of rechtmatige e-mails ontvangt in Aziatische of Cyrillische tekens, kunt u de instelling die dergelijke e-mails blokkeert, in- of uitschakelen. De overeenkomende instelling is uitgeschakeld in de gelokaliseerde versies van het programma die dergelijke tekensets gebruiken (bijvoorbeeld in de Russische of Chinese versie).

De lokale antispamfilters configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTISPAM**-panel.
4. Klik op de bijhorende AAN/UIT-schakelaars.

Als u Microsoft Outlook of Thunderbird gebruikt, kunt u de lokale antispamfilters direct vanaf uw e-mailklant configureren. Klik op de knop **Instellingen** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailklant) en klik vervolgens op het tabblad **Antispamfilters**.

4.4.7. De cloudinstellingen configureren

"In-the cloud"-detectie maakt gebruik van de Bitdefender Cloud-services om u efficiënte antispambeveiliging te bieden die altijd up-to-date is.

De cloudbeveiliging werkt zolang Bitdefender-antispam is ingeschakeld.

Voorbeelden van rechtmatige e-mails of spam-e-mails kunnen worden verzonden naar Bitdefender Cloud wanneer u detectiefouten of niet-gedetecteerde spam-e-mails aanduidt. Hiermee kan de antispam-detectie van Bitdefender worden verbeterd.

Configureer het verzenden van e-mailvoorbeelden naar Bitdefender Cloud door de gewenste opties te selecteren, door deze stappen te volgen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ANTISPAM**-panel.
4. In het venster **INSTELLINGEN** selecteert u de gewenste opties.

Als u Microsoft Outlook of Thunderbird gebruikt, kunt u de cloud-detectie rechtstreeks vanaf uw e-mailklant configureren. Klik op de knop **Instellingen** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailklant) en klik vervolgens op het tabblad **Cloud-instellingen**.

4.5. Firewall

De Firewall beschermt uw computer tegen inkomende en uitgaande onrechtmatige verbindingspogingen, zowel op lokale netwerken als op internet. Dit kan worden vergeleken met een wachter bij uw poort – de toepassing traceert verbindingspogingen en beslist welke moeten worden toegestaan en welke moeten worden geblokkeerd.

De Bitdefender-firewall gebruikt een reeks regels om gegevens te filteren die naar en van uw systeem zijn overgedragen.

In normale omstandigheden maakt Bitdefender automatisch een regel wanneer een toepassing toegang probeert te krijgen via internet. U kunt regels voor toepassingen ook handmatig toevoegen of bewerken.

Uit veiligheidsoverwegingen zult u telkens wanneer een potentieel schadelijke toepassing geblokkeerd wordt om het internet te gebruiken, een melding ontvangen, zelfs als de Autopilot-functie ingeschakeld is.

Bitdefender wijst automatisch een netwerktype toe aan elke netwerkverbinding die het detecteert. Afhankelijk van het netwerktype is de firewall-beveiliging ingesteld op het geschikte niveau voor elke aansluiting.

Meer informatie over de firewall-instellingen voor elk netwerktype en de manier waarop u de netwerkinstellingen kunt bewerken, vindt u onder "*Verbindingsinstellingen beheren*" (p. 126).

De firewall-beveiliging in- of uitschakelen

Firewallbescherming in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **FIREWALL** op de schakelaar AAN/UIT.

Waarschuwing

Omdat het uw computer blootstelt voor onbevoegde verbindingen, mag het uitschakelen van de firewall slechts een tijdelijke maatregel zijn. Schakel de firewall zo snel mogelijk opnieuw in.

4.5.1. De regels beheren

De firewallregels beheren die de toegang bepalen van de toepassingen tot netwerkbronnen en het internet.

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het venster **FIREWALL** op **Toegang toepassing**.
4. De eerste keer dat u Firewall gebruikt, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.

U kunt de laatste 15 programma's (processen) bekijken die door de Bitdefender-firewall en het internetnetwerk waar u mee verbonden bent, gepasseerd zijn. Om de regels die voor een specifieke toepassing werden aangemaakt te bekijken, klikt u er gewoon op en klikt u daarna op de koppeling **Toepassingsregels bekijken**. Het venster **REGELS** wordt geopend.

Voor elke regel wordt de volgende informatie weergegeven:

- **NETWERK** - het proces en de netwerkadaptertypes (thuis / kantoor, openbaar of alle) waar de regel op van toepassing is. Regels zijn automatisch gecreëerd voor het filteren van netwerk- of internettoegang via elke adapter. Standaard zijn de regels van toepassing op willekeurig welk netwerk. U kan handmatig regels creëren of bewerken voor het filteren van de netwerk- of internettoegang van een applicatie via een specifieke adapter (bijvoorbeeld een draadloze netwerkadapter)
- **PROTOCOL** - het IP-protocol waarvoor de regel geldt. Standaard zijn de regels van toepassing op willekeurig welk protocol.
- **VERKEER** - de regel is in beide richtingen van toepassing. Inkomend en uitgaand.
- **POORTEN** - het poortprotocol waarvoor de regel geldt. Standaard zijn de regels op alle poorten van toepassing.
- **IP** - het internetprotocol (IP) waarvoor de regel geldt. Standaard zijn de regels van toepassing op elk IP-adres.
- **TOEGANG** - of de toepassing al dan niet netwerk- of internettoegang krijgt onder de opgegeven omstandigheden.

Om de regels voor de geselecteerde app te bewerken of te verwijderen, klik op de icoon ***.

- **Regel bewerken** - opent een venster waarin u de huidige regel kunt bewerken.
- **Regel verwijderen** - u kunt ervoor kiezen de huidige reeks regels voor de geselecteerde app te verwijderen.

Toepassingsregels toevoegen

Om een toepassingsregel toe te voegen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **FIREWALL**-panel.
4. Klik op de koppeling **Regel toevoegen** bovenaan in het venster **REGELS**.

In het venster **INSTELLINGEN** kunt u de volgende wijzigingen toepassen:

- **Deze regel toepassen op alle toepassingen.** Activeer deze schakelaar om de aangemaakte regel toe te passen op alle toepassingen.
- **Programmapad.** Klik op **Bladeren** en selecteer de applicatie waarvoor de regel geldt.
- **Machtiging.** Selecteer een van de beschikbare machtigingen:

Machtiging	Beschrijving
Toestaan	De opgegeven toepassing zal netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.
Weigeren	De opgegeven toepassing zal geen netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.

- **Netwerktype.** Selecteer het type netwerk waarvoor de regel geldt. U kunt het type wijzigen door het vervolgkeuzemenu **Netwerktype** te openen en een van de beschikbare types in de lijst te selecteren.

Netwerktype	Beschrijving
Om het even welk netwerk	Alle verkeer tussen uw computer en andere computers, ongeacht het netwerktype toestaan.

Netwerktype	Beschrijving
Thuis/Bureau	Alle verkeer tussen uw computer en computers in het netwerk toestaan.
Openbaar	Alle verkeer blokkeren is uitgeschakeld.

- **Protocol.** Selecteer in het menu het IP-protocol waarvoor de regel geldt.
  - Als u een regel voor alle protocollen wilt laten gelden, schakelt u het selectievakje **Alle** in.
  - Als u wilt dat de regel van toepassing is op TCP, selecteert u **TCP**.
  - Als u wilt dat de regel van toepassing is op UDP, selecteert u **UDP**.
  - Als u wilt dat de regel van toepassing is op ICMP, selecteert u **ICMP**.
  - Als u wilt dat de regel van toepassing is op IGMP, selecteert u **IGMP**.
  - Indien u wilt dat de regel van toepassing is op een specifiek protocol, typt u het nummer dat aan het protocol dat u wilt filteren in het lege bewerkveld.

  Opmerking

  IP-protocolnummers worden toegewezen door de Internet Assigned Numbers Authority (IANA). U vindt de complete lijst van toegewezen IP-protocolnummers op http://www.iana.org/assignments/protocol-numbers.

- **Richting.** Selecteer in het menu de verkeersrichting waarvoor de regel geldt.

Richting	Beschrijving
Uitgaand	De regel zal alleen voor uitgaand verkeer worden toegepast.
Inkomend	De regel zal alleen voor inkomend verkeer worden toegepast.
Beide	De regel zal in beide richtingen worden toegepast.

In het venster **GEAVANCEERD** kunt u de volgende instellingen aanpassen:

- **Gewoon Lokaal Adres.** Geef het lokale IP-adres en poort waarvoor de regel geldt, op.
- **Gewoon Adres op Afstand.** Geef het externe IP-adres en poort waarvoor de regel geldt, op.

Om de huidige reeks regels te verwijderen en de standaardregels terug te stellen, klikt u op de koppeling **Regels terugstellen** bovenaan in het venster **REGELS**.

4.5.2. Verbindingsinstellingen beheren

Ongeacht of u een verbinding maakt met het internet via Wi-Fi of een Ethernet-adapter, kunt u bepalen welke instellingen van toepassing moeten zijn om veilig te navigeren. De opties waar u uit kunt kiezen, zijn:

- **Dynamisch** – het netwerktype zal automatisch ingesteld worden op basis van het profiel van het verbonden netwerk, Thuis/kantoor of Openbaar. Wanneer dit gebeurt, zullen enkel Firewall-regels voor het specifieke netwerktype of deze die gedefinieerd zijn om op alle netwerktypes te gelden, van toepassing zijn.
- **Thuis / Kantoor** – het netwerktype zal altijd Thuis / Kantoor zijn, ongeacht het profiel van het verbonden netwerk. Wanneer dit gebeurt, zullen enkel Firewall-regels voor Thuis / Kantoor of deze die gedefinieerd zijn om op alle netwerktypes te gelden, van toepassing zijn.
- **Openbaar** – het netwerktype zal altijd Openbaar zijn, ongeacht het profiel van het verbonden netwerk. Wanneer dit gebeurt, zullen enkel Firewall-regels voor Openbaar of deze die gedefinieerd zijn om op alle netwerktypes te gelden, van toepassing zijn.

Om uw netwerkadapters te configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **FIREWALL**-panel.
4. Selecteer het tabblad **NETWERKTYPE**.
5. Selecteer de instellingen die u volgens u van toepassing moeten zijn wanneer u aansluit op de volgende adapters:
   - Wi-Fi

- Ethernet

4.5.3. Geavanceerde instellingen configureren

Geavanceerde firewall-instellingen configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **FIREWALL**-panel.
4. Selecteer het tabblad **INSTELLINGEN**.

De volgende functies kunnen geconfigureerd worden:

- **Poort scans blokkeren in het netwerk** - detecteert en blokkeert pogingen om uit te vinden welke poorten open zijn.

  Poortscans worden vaak door hackers gebruikt om geopende poorten op uw computer te vinden. Als zij een minder veilige of kwetsbare poort vinden kunnen zij inbreken in uw computer.

- **Paranoïde modus** - er worden meldingen gegeven telkens wanneer een toepassing een verbinding met het internet probeert te maken. Klik op **Toestaan** of **Blokkeren**. Als de Paranoïdemodus is ingeschakeld, worden de functies Autopilot en Profielen automatisch uitgeschakeld. Paranoïdemodus kan gelijktijdig worden gebruikt met **Accumodus**.

- **Stealth-modus** - hiermee kunt u instellen of u door andere computers kunt worden gedetecteerd. Klik op **Stealth-instellingen bewerken** om te kiezen wanneer uw apparaat wel of niet zichtbaar moet zijn voor andere computers.

- **Standaardgedrag toepassing** - toestaan dat Bitdefender automatische instellingen toepast op toepassingen waarvoor geen regels gedefinieerd zijn. Klik op **Standaardregels configureren** om te kiezen of automatische instellingen moeten worden toegepast of niet.

  - Automatisch - toegang tot toepassingen zal toegestaan of geweigerd worden op basis van de automatische Firewall- en gebruikersregels.
  - Toestaan - toepassingen waarvoor geen Firewall-regel gedefinieerd werd, zullen automatisch toestemming krijgen.
  - Blokkeren - toepassingen waarvoor geen Firewall-regel gedefinieerd werd, zullen automatisch geblokkeerd worden.

4.6. Kwetsbaarheid

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

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

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

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

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

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

4.6.1. Uw systeem scannen op kwetsbaarheden

Systeemkwetsbaarheden oplossen met de optie Kwetsbaarheidscan:

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

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

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

- **Toepassings-updates**

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

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

- **Zwakke wachtwoorden van Windows-accounts**

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

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

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

- **Zwakke Wi-Fi-netwerken**

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

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

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

4.6.2. De automatische kwetsbaarheidsbewaking gebruiken

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

Zo kunt u de opgespoorde problemen controleren en verhelpen:

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

De controle-instellingen voor kwetsbaarheid configureren:

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

2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **KWETSBAARHEID** op de schakelaar AAN/UIT.

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

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

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

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

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

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

Sommige 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.

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

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

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

4.6.3. 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-Wi-Fi-netwerken
- Openbare Wi-Fi-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 op het pictogram in de linkerzijbalk van de Bitdefender-interface.

2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon ⚙ in de rechterbenedenhoek van het **KWETSBAARHEID**-panel.
4. In het venster **INSTELLINGEN** klikt u op de overeenkomstige AAN/UIT-schakelaar.

Thuis-Wi-Fi-netwerk configureren

Uw thuisnetwerk beginnen configureren:

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

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

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

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

Openbare Wi-Fi

Terwijl u met een onbeveiligd of onveilig draadloos netwerk verbonden bent, wordt het openbare Wi-Fi-profiel geactiveerd. Terwijl u in dit profiel werkt, is Bitdefender Total Security 2018 ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Advanced Threat Defense is ingeschakeld
- De Bitdefender-firewalle is ingeschakeld en de volgende instellingen worden toegepast op uw draadloze adapter.
  - Geheime modus - AAN
  - Netwerktype - Openbaar
- De volgende instellingen van Webbescherming zijn ingeschakeld:

- SSL scannen
- Bescherming tegen fraude
- Bescherming tegen phishing

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

Informatie controleren over Wi-Fi-netwerken

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

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

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

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

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

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

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

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

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

4.7. Webcambeveiliging

Het is geen nieuws meer dat hackers uw webcam kunnen overnemen om u te bespioneren. Er zijn oplossingen om u te beschermen, zoals het terugdraaien van de privileges van de toepassing, het uitschakelen van de ingebouwde camera van het apparaat en de webcam bedekken, maar ze zijn niet zo praktisch. Om verdere pogingen om toegang te krijgen tot uw privacy houdt Bitdefender-webcambeveiliging toezicht op de toepassingen die toegang proberen te krijgen tot uw camera en blokkeert ze deze die niet als betrouwbaar werden aangeduid.

Als veiligheidsmaatregel zult u telkens wanneer een onbetrouwbare toepassing probeert om toegang te krijgen tot uw camera, een melding krijgen, zelfs wanneer de Autopilot is ingeschakeld.

Uw Webcambeveiliging in- of uitschakelen

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **WEBCAMBESCHERMING** op de schakelaar AAN/UIT.

Webcambeveiliging configureren

U kunt instellen welke regels er moeten toegepast worden wanneer een toepassing probeert om zich toegang te verschaffen tot uw camera. Volg hiervoor deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **WEBCAMBESCHERMING**-panel.

Blokkeringsregels toepassing

- **Alle toegang tot de webcam blokkeren** - geen enkele toepassing zal toegang krijgen tot uw webcam.
- **Toegang tot de webcam door browsers blokkeren** - behalve Internet Explorer en Microsoft Edge zal geen enkele internetbrowser toegang krijgen tot uw webcam. Gezien de procedure voor apps in de Windows Store om volgens eenzelfde proces te draaien, kunnen Internet Explorer en Microsoft Edge door Bitdefender niet als internetbrowsers geïdentificeerd worden. Daarom worden ze uit deze instelling uitgesloten.
- **Toegang voor toepassingen tot webcam instellen volgens de gebruikersvoorkeuren van Bitdefender** - indien de meerderheid van de Bitdefender-gebruikers een populaire toepassing als schadeloos beschouwen, zal de toegang tot de webcam automatisch ingesteld worden op Toestaan. Indien een populaire toepassing door de meesten als gevaarlijk wordt beschouwd, zal de toegang automatisch ingesteld worden op Geblokkeerd.

  U zult telkens ingelicht worden wanneer uw geïnstalleerde toepassingen door de meerderheid van de Bitdefender-gebruikers als geblokkeerd werden ingesteld, zelfs als de Autopilot-functie is ingeschakeld.

Notificaties

- **Melden wanneer toegestane toepassingen een verbinding maken met de webcam** - u ontvangt telkens een melding wanneer een toegestane toepassing zich toegang verschaft tot uw webcam, zelfs als de Autopilot-functie is ingeschakeld.

Toepassingen toevoegen tot de lijst van Webcambeveiliging

Toepassingen die proberen om een verbinding te maken met uw webcam worden automatisch opgespoord en afhankelijk van hun gedag en de keuze van de gemeenschap, wordt hun toegang toegestaan of geweigerd. U kunt echter zelf manueel beginnen configureren welke actie moet worden ondernomen. Volg hiervoor de volgende stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **WEBCAMBESCHERMING**-panel klikt u op **Webcamtoegang**.
4. De eerste keer dat u Webcam-bescherming gebruikt, krijgt u een inleiding.
5. Klik op de gewenste link:
   - **Selecteer Windows Store-toepassingen om toe te voegen aan de lijst van permissies** - een lijst met de gedetecteerde Windows Store-toepassingen wordt weergegeven. Zet de schakelaars naast de toepassingen die u wilt toevoegen aan de lijst, aan.
   - **Begin toepassingen toe te voegen aan de lijst voor webcam-toegang** - ga naar het bestand .exe dat u wilt toevoegen aan de lijst, en klik op **OK**.

     Om nog toepassingen toe te voegen, klik op de koppeling **Een nieuwe toepassing toevoegen aan de lijst**.

Klik op de schakelaar Toegang toegestaan/Toegang geblokkeerd.

Om te zien wat Bitdefender-gebruikers hebben gekozen om met deze geselecteerde toepassing te doen, klik op de icoon .

De toepassingen die toegang tot uw camera vragen verschijnt in dit venster, samen met het tijdstip van laatste activiteit.

U zult een melding krijgen telkens wanneer een van de toegestane toepassingen werd geblokkeerd door de Bitdefender-gebruikers, wat de status van Autopilot ook is.

4.8. Veilige bestanden

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

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

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

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

Met Bitdefender Veilige bestanden kunt u persoonlijke bestanden, zoals documenten, foto's of films beschermen tegen ransomware.

Opmerking
Advanced Threat Defense en Veilige bestanden zijn twee beschermingslagen tegen ransomware. Advanced Threat Defense is de functie die ransomware-aanvallen in volle actie tegenhouden op de kritieke zones van uw systeem, terwijl Veilige bestanden ervoor zorgt dat geen enkel belangrijk bestand op uw computer versleuteld wordt.

4.8.1. Veilige bestanden in- of uitschakelen

Om de functie Veilige bestanden in of uit te schakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **VEILIGE BESTANDEN** op de schakelaar AAN/UIT.

Telkens wanneer een applicatie probeert om naar een van de beschermde bestanden te gaan, wordt een Bitdefender pop-up weergegeven. U kunt de toegang toestaan of blokkeren.

Opmerking
De functie Veilige bestanden is niet standaard geactiveerd.

4.8.2. Persoonlijke bestanden beschermen tegen ransomware-aanvallen.

Indien u persoonlijke bestanden veilig wilt onderbrengen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het venster **VEILIGE BESTANDEN** op **Beschermde mappen**.
4. De eerste keer dat u Beschermde Mappen gebruikt, krijgt u een inleiding. Klik op **MEER MAPPEN BESCHERMEN** om verder te gaan.
5. Selecteer de map die u wilt beschermen en klik op **OK**.

   Om mappen toe te voegen, klik op de koppeling **Meer mappen beschermen**. U kunt ook mappen naar dit venster verslepen.

Standaard worden de mappen Afbeeldingen, Video's, Muziek, Bureaublad en Downloads beschermd tegen aanvallen van dreigingen. Persoonlijke gegevens die in online bestandshostingdiensten worden opgeslagen, zoals Box, Dropbox, Google Drive en OneDrive worden ook opgenomen in de beschermingsomgeving, op voorwaarde dat hun applicaties op het systeem geïnstalleerd zijn.

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

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

4.8.3. Toegang tot toepassingen aan het configureren

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het venster **VEILIGE BESTANDEN** op **Toegang toepassing**.
4. De appsdie verzocht hebben om bestanden in uw beschermde mappen te wijzigen, worden hier vermeld. Klik op de Toestaan-schakelaar naast de toepassing waarvan u zeker bent dat ze veilig is.

In hetzelfde venster kunt u ransomwarebescherming uitschakelen voor specifieke toepassingen door op de schakelaar Blokkeren te klikken.

Indien u nieuwe toepassingen aan de lijst wilt toevoegen, klikt u op de koppeling **Een nieuwe toepassing aan de lijst toevoegen**.

4.8.4. Bescherming bij opstarten

Het is bekend dat heel wat kwaadwillige apps zo ingesteld zijn dat ze uitgevoerd worden tijdens het opstarten van het systeem, iets wat een computer erg veel schade kan toebrengen. Bitdefender-boottijdbescherming scant alle cruciale systeemgebieden voordat alle bestanden worden geladen, zonder enige impact op het systeem.

Bescherming bij het opstarten uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **VEILIGE BESTANDEN**-panel.
4. Klik op de schakelaar AAN/UIT.

Opmerking
Toepassingen die werden toegevoegd aan uitsluitingen zullen gescand worden en dienovereenkomstig verwerkt.

4.9. Bestandscodering

Met Bestandscodering van Bitdefender kunt u gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer maken waar u uw confidentiële en gevoelige documenten veilig kunt opslaan. De in de kluizen opgeslagen data zijn alleen toegankelijk voor gebruikers die het wachtwoord kennen.

Met het wachtwoord kan u een kluis openen, data erin opslaan en de kluis weer sluiten zonder dat de beveiliging in gevaar komt. Als en kluis open is, kan u nieuwe bestanden toevoegen, huidige bestanden openen of bewerken.

De kluis is een bestand dat is opgeslagen op de lokale harde schijf met de extensie bvd. Ofschoon de fysieke bestanden die de kluisschijven vormen, geopend kunnen worden door een ander besturingssysteem (zoals Linux), kan de informatie erop niet niet gelezen worden doordat deze is gecrypteerd.

Bestandskluizen kunnen worden beheerd vanaf het Bitdefender-venster of via het Windows-snelmenu en de logical drive die aan de kluis is gekoppeld.

Bestandskluizen beheren

Om uw bestandskluizen van Bitdefender te beheren, klikt u op de -icoon op de linkerzijbalk van de Bitdefender-interface.

De bestaande bestandskluizen verschijnen in het panel **Bestandskluizen**.

Bestandskluizen maken

Om een nieuwe kluis aan te maken:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op **Nieuwe bestandskluis aanmaken** in het paneel **BESTANDSCODERING**.
4. Geef de plaats en de naam van de bestandskluis op.
   - Voer de naam van het kluisbestand in het overeenkomende veld in.
   - Klik op **Bladeren** , selecteer de plaats van de kluis en sla het kluisbestand op met de door u gewenste naam.

5. Kies een schijfletter in het overeenkomende menu. Als u de kluis opent, verschijnt een virtuele schijf met de geselecteered schijfletter in Deze computer.
6. Als u de standaardgrootte (100 MB) van de kluis wilt veranderen, gebruikt u de pijltjes omhoog en omlaag in het uitklapmenu van de **Kluisgrootte (MB)**.
7. Typ het gewenste wachtwoord voor de kluis in de velden **Wachtwoord** en **Wachtwoord bevestigen** in. Het wachtwoord moet minstens 8 tekens bevatten. Iedereen die probeert de kluis te openen en naar de bestanden erin te gaan, moet het wachtwoord opgeven.
8. Klik op **Maken**.

Bitdefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om het probleem op te lossen.

Om een kluis sneller aan te maken, klikt u met de rechtermuisknop op uw bureaublad of in een map op uw computer. Wijs vervolgens **Bitdefender** > **Bitdefender Bestandskluis** aan en selecteer **Bestandskluis maken**.

Opmerking
Het kan nuttig zijn alle bestandssafes op te slaan op dezelfde locatie. Hierdoor kunt u ze sneller vinden.

Een bestandskluis importeren

Om een plaatselijk opgeslagen bestandskluis te importeren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Selecteer in het panel **BESTANDSCODERING Kluis importeren**.
4. Zoek de locatie van uw kluisen selecteer deze (het .bvd-bestand).
5. Klik op **Openen**.

Bestandskluizen openen

Om bestanden die zijn opgeslagen in een kluis te openen en te bewerken, moet u de kluis openen. Als u de kluis opent, verschijnt een vituele schijf in Deze computer. De schijf heeft de schijfletter die is toegewezen aan de kluis.

Een kluis openen:

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

   De bestaande bestandskluizen verschijnen in het panel **Bestandskluizen**.
2. Klik op de koppeling **Kluizen bekijken** en selecteer vervolgens de kluis die u wilt openen.
3. Klik op de **Ontsluiten**-knop en voer daarna het vereiste wachtwoord in.
4. Klik op **OK** en daarna op de **Openen**-knop om uw kluis te openen.

Bitdefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen.

Om een kluis sneller te openen, zoekt u op uw computer naar het bvd-bestand dat de kluis voorstelt die u wilt openen. Klik met de rechtermuisknop op het bestand, selecteer **Bitdefender Bestandskluis** en klik op **Openen**. Voer het vereiste wachtwoord in en klik op **OK**.

Bestanden toevoegen aan kluizen

Voordat u bestanden of mappen aan een safe kunt toevoegen, moet u de safe openen.

Nieuwe bestanden toevoegen aan uw kluis:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **BESTANDSCODERING**-panel.
4. Selecteer in het **MIJN KLUIZEN**-venster de kluis die u wilt openen.
5. Klik op de **Ontsluiten**-knop en voer daarna het vereiste wachtwoord in.
6. Klik op de **Openen**-knop om uw kluis te openen.
7. Voeg bestanden of mappen toe, zoals u normaal zou doen in Window (u kunt bijvoorbeeld kopiëren en plakken).

Om bestanden sneller an uw kluis toe te voegen, klikt u met de rechtermuisknop op het bestand of de map die u naar de kluis wilt kopiëren,

selecteert u **Bitdefender Bestandskluis** en klikt u op **Toevoegen aan Bestandskluis**.

- Als er slechts één safe open is, wordt het bestand of de map direct naar die safe gekopieerd.
- Als er meerdere safes open zijn, wordt u gevraagd de safe te kiezen waarnaar u het item wilt kopiëren. Selecteer in het menu de stationsletter die overeenkomt met de gewenste safe en klik op **OK** om het item te kopiëren.

Kluizen vergrendelen

Als u klaar bent met het werken in een bestandskluis, moet u de kluis vergrendelen om uw data te beveiligen. Door de safe te vergrendelen, verdwijnt het overeenkomende schijfstation uit Deze computer. Hierdoor worden de gegevens die in de safe zijn opgeslagen, volledig geblokkeerd.

Een kluis afsluiten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. In het panel **Bestandskluizen** selecteert u **Kluizen bekijken**.
3. Selecteer in het **MIJN KLUIZEN**-venster de kluis die u wilt vergrendelen.
4. Klik op de knop **Vergrendelen**.

Bitdefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om het probleem op te lossen.

Om een kluis sneller te vergrendelen klikt u op het .bvd-bestand dat de kluis voorstelt. Selecteer **BitdefenderBestandskluis** en klik op **Vergrendelen**.

Bestanden verwijderen uit kluizen

Om bestanden of mappen uit een safe te verwijderen, moet de safe open zijn. Bestanden of mappen uit een kluis verwijderen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **BESTANDSCODERING**-panel.

4. Selecteer in het **MIJN KLUIZEN**-venster de kluis waarvan u bestanden wilt verwijderen.
5. Klik op de **Ontgrendelen**-knop indien deze vergrendeld is.
6. Klik op de knop **Openen**.

   Verwijder bestanden of mappen zoals u dat gewoon bent in Windows (klik bijvoorbeeld met de rechtermuisknop op een bestand dat u wilt Verwijderen en selecteer **Verwijderen**).

Het kluiswachtwoord wijzigen

Het wachtwoord beveiligt de inhoud van een safe tegen onbevoegde toegang. Alleen gebruikers die het wachtwoord kennen, kunnen de safe openen en krijgen toegang tot de documenten en gegevens die in de safe zijn opgeslagen.

De safe moet vergrendeld zijn voordat u het wachtwoord kunt wijzigen. Het wachtwoord van een kluis wijzigen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **BESTANDSCODERING**-panel.
4. Selecteer in het **MIJN KLUIZEN**-venster de kluis waarvoor u het wachtwoord wilt wijzigen.
5. Klik op de knop **Instellingen**.
6. Typ het huidige wachtwoord in het veld **Oud wachtwoord**.
7. Voer het nieuwe wachtwoord voor de kluis in de velden **Nieuw wachtwoord** en **Nieuw wachtwoord bevestigen** in.

   Opmerking
   Het wachtwoord moet minstens 8 tekens bevatten. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

Bitdefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om het probleem op te lossen.

Om het wachtwoord van een kluis sneller te wijzigen, zoekt u op uw computer het .bvd-bestand dat voor de kluis staat. Klik met de rechtermuisknop op het bestand, selecteer **Bitdefender Bestandskluis** en klik op **Wachtwoord kluis wijzigen**.

4.10. Beveiliging Wachtwoordbeheerder voor uw gegevens

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

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

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

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

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

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

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

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

Wachtwoordbeheerder beveiligt de volgende persoonlijke gegevens:

- Persoonlijke gegevens, zoals het e-mailadres of het telefoonnummer

- Logingegevens voor de websites
- Bankrekeninggegevens of het creditcardnummer
- Toegangsgegevens naar de e-mailaccounts
- Wachtwoorden voor de toepassingen
- Wachtwoorden voor de Wi-Fi-netwerken

Maak een nieuwe Wallet database aan

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

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

Importeer een bestaande database

Om een plaatselijk opgeslagen database te importeren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **Portefeuille** op **Nieuwe portefeuille aanmaken**.
4. Klik op de knop **Vanuit doel**.
5. Ga naar de locatie op uw apparaat waar u de Wallet-database wenst op te slaan, en kies er vervolgens een naam voor.
6. Klik op **Openen**.
7. Geef uw Portefeuille een naam en voer het wachtwoord dat bij de aanmaak werd toegekend, in.
8. Klik op **Importeren**.
9. Selecteer de programma's van waaruit u de Portefeuille legitimatiebewijzen wenst te laten importeren, en klik dan op de knop **Voltooien**.

De Portefeuille-database exporteren

Uw Portefeuilledatabase exporteren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op het panel **Portefeuille** op **Mijn portefeuilles**.
4. Klik op de ⋮ -icoon op de gewenste portefeuille en selecteer vervolgens **Exporteren**.
5. Zoek de locatie van uw portefeuilledatabase en selecteer deze (het .db-bestand).
6. Klik op **Opslaan**.

Opmerking

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

Synchroniseer uw portefeuilles in de cloud

De portefeuillesynchronisatie in de cloud in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op het panel **Portefeuille** op **Mijn portefeuilles**.
4. Klik op de -icoon op de gewenste portefeuille en selecteer vervolgens **Instellingen**.
5. Kies de gewenste optie in het venster dat verschijnt en klik vervolgens op **Opslaan**.

Opmerking

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

Uw Portefeuille-gegevens beheren

Uw wachtwoorden beheren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op het panel **Portefeuille** op **Mijn portefeuilles**.
4. Selecteer de gewenste Portefeuilledatabase uit het venster **MIJN PORTEFEUILLES** en klik vervolgens op de **PORTEFEUILLE ACTIVEREN**-knop.
5. Voer het hoofdwachtwoord in en klik op **OK**.

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

- Identiteit
- Websites
- Online bank

- E-mails
- Toepas.
- Wi-Fi-netw.

De gegevens aanvullen / bewerken

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

De Wachtwoordbeheerderbeveiliging in- of uitschakelen

De bescherming van Wachtwoordmanager in- of uitschakelen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het panel **PORTEFEUILLE** op de schakelaar AAN/UIT.

De instellingen voor Wachtwoordbeheerder beheren

Het hoofdwachtwoord in detail configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **PORTEFEUILLE**-panel.
4. Selecteer het tabblad **VEILIGHEIDSINSTELLINGEN**.

De volgende opties zijn beschikbaar:

- **Mijn masterwachtwoord vragen wanneer ik inlog op mijn pc** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot de computer.

- **Mijn masterwachtwoord vragen wanneer ik mijn browsers en toepassingen open** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot een browser of toepassing.
- **Mijn masterwachtwoord niet vragen** - u wordt niet gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot de computer, een browser of een toepassing.
- **Portefeuille automatisch vergrendelen wanneer ik mijn PC onverwacht verlaat** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u na 15 minuten terugkeert naar de computer.

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

Verbeter uw ervaring

Om de browsers of toepassingen waarin u de wachtwoordmanager wilt integreren te selecteren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **PORTEFEUILLE**-panel.
4. Selecteer het tabblad **PLUG-INS**.

   Kies een toepassing om de Wachtwoordbeheerder te gebruiken en verbeter uw ervaring:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Autofill configureren

De functie Autofill maakt het u gemakkelijk om verbinding te maken met uw favoriete websites of om in te loggen op uw online accounts. De eerste keer

dat u uw certificaten en persoonlijke gegevens invoert in uw webbrowser, worden ze automatisch beveiligd in de Portefeuille.

Om de **Autofill**-instellingen te configureren:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **PORTEFEUILLE**-panel.
4. Selecteer het tabblad **AUTOFILL-INSTELLINGEN**.
5. De volgende opties configureren:
   - **Configureren hoe Wallet uw gegevens beveiligt.**:
     - **Inloggegevens automatisch opslaan in Portefeuille** - de logingegevens en andere herkenbare gegevens zoals uw persoonlijke en creditcardgegevens worden automatisch opgeslagen en bijgewerkt in de Portefeuille.
     - **Vraag me elke keer** - u wordt elke keer gevraagd of u uw gegevens aan de Portefeuille wilt toevoegen.
     - **Niet opslaan, ik werk de gegevens handmatig bij** - de gegevens kunnen alleen handmatig aan de Portefeuille worden toegevoegd.
   - **Inlogreferenties automatisch aanvullen**:
     - **Autofill logingegevens elke keer** - de gegevens worden automatisch in de browser ingevuld.
   - **Autofill formulieren**:
     - **Geef mijn in te vullen opties aan als ik een pagina met formulieren bezoek** - een pop-up met de invulopties verschijnt telkens wanneer Bitdefender detecteert dat u een online betaling wilt uitvoeren of wilt intekenen.

De Wachtwoordbeheerder beheren vanuit uw browser

U kunt de informatie Wachtwoordbeheerder gemakkelijk beheren vanuit uw browser, zodat u alle belangrijke gegevens bij de hand hebt. De invoegtoepassing Bitdefender wordt ondersteund door de volgende browsers:

Google Chrome, Internet Explorer en Mozilla Firefox, en hij is ook geïntegreerd in Safepay.

Om naar de Portefeuille-extensie van Bitdefender te gaan, opent u uw webbrowser, accepteert de installatie van de invoegtoepassing en klikt op het pictogram op de taakbalk.

De Portefeuille-extensie van Bitdefender bevat de volgende opties:

- Portefeuille openen - opent de Portefeuille.
- Portefeuille vergrendelen - vergrendelt de portefeuille.
- Websites - opent een submenu met alle logins van de websites die in Portefeuille zijn opgeslagen. Klik op **Website toevoegen** om de nieuwe websites aan de lijst toe te voegen.
- Formulieren invullen - opent een submenu met de gegevens die u voor een speciale categorie hebt toegevoegd. Van hieruit kunt u nieuwe gegevens aan uw Portefeuille toevoegen.
- Wachtwoordgenerator - hiermee kunt u willekeurige wachtwoorden genereren die u voor nieuwe of bestaande accounts kunt gebruiken. Klik op **Geavanceerde instellingen tonen** om de complexiteit van het wachtwoord aan te passen.
- Instellingen - opent het instellingenvenster van Wachtwoordbeheerder.
- Probleem melden - meldt elk willekeurig probleem dat u ondervindt met Wachtwoordbeheerder van Bitdefender

4.11. VPN

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

Opmerking

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

VPN Installeren

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op **VPN Activeren** in het paneel **VPN**.
4. Lees de **Abonnementsovereenkomst** in het venster met de beschrijving van de VPN-app en klik vervolgens op **Bitdefender VPN ACTIVEREN**.

   Wacht even totdat de bestanden gedownload en geïnstalleerd zijn.
5. 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.

VPN Openen

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

- Vanuit het systeemvak
  1. Rechtsklik op het icoon in het systeemvak en klik vervolgens op **Tonen**.
- Van de Bitdefender-interface:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de actieknop **VPN**.

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"* (p. 275).

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 uw verbinding worden aan de onderkant van de interface de verstreken tijd en het IP-adres dat automatisch toegewezen werd aan uw apparaat weergegeven.

Om meer opties te bekijken, ga naar **Menu** door linksboven op het icoon ≡ te klikken. 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.
- **Instellingen** – u kunt het gedrag van uw product aanpassen naargelang uw noden:
  - ontvang notificaties wanneer de VPN automatisch verbindt of de verbinding verbreekt
  - VPN-app automatisch uitvoeren bij opstart van Windows
  - de VPN-app automatisch opstarten wanneer uw toestel met een onbeveiligd draadloos netwerk verbindt
- **Upgraden naar Premium** - indien u de gratis versie gebruikt, kunt u hier upgraden naar premium.
- **Ondersteuning** - u wordt doorgestuurd naar ons platform Ondersteuningscentrum, waar u een nuttig artikel kunt lezen over hoe u Bitdefender VPN gebruikt.
- **Over deze versie** - informatie over de geïnstalleerde versie.

Abonnementen

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

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

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

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het abonnement voor Bitdefender Total Security 2018: u kunt het dus gedurende de hele geldigheid ervan gebruiken, ongeacht de status van het abonnement van de beveiligingsoplossing. Indien het Bitdefender Premium VPN-abonnement vervalt, maar indien het abonnement voor Bitdefender Total Security 2018 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.

4.12. Safepay beveiliging voor online transacties

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

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

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

Voor de beste privacybeveiliging is Bitdefender-Wachtwoordbeheerder geïntegreerd in Bitdefender Safepay™ om uw gegevens te beveiligen wanneer u naar persoonlijke online plaatsen gaat. Zie *"Beveiliging Wachtwoordbeheerder voor uw gegevens"* (p. 146) 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 computer is verbonden met onbeveiligde Wi-Fi-netwerken.
- Het ondersteunt bookmarks en stelt u in staat om te surfen tussen uw favoriete bank/winkelsites.
- Het is niet beperkt tot bankieren en online winkelen. Elke website kan worden geopend in Bitdefender Safepay™.

Bitdefender Safepay™ gebruiken

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

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

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

3. Klik op **Bitdefender Safepay™**.

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

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

- In **Windows 10**:

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

Opmerking

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

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

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

- belangrijke informatie afdrukken door te klikken op .

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

Instellingen configureren

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

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

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

  Domeinenlijst
  Kies hoe Bitdefender Safepay™ zich gedraagt als u websites van specifieke domeinen bezoekt in uw gewone webbrowser door ze toe te voegen aan de domeinenlijst en het gedrag voor elk van hen te selecteren:
  - Automatisch openen in Bitdefender Safepay™.
  - Bitdefender u elke keer laten vragen wat u wilt doen.
  - Bitdefender Safepay™ nooit gebruiken wanneer er een pagina van het domein wordt bezocht in een gewone browser.

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

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

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

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

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

Plug-ins beheren

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

Certificaten beheren

U kunt certificaten van uw systeem importeren naar een certificatenwinkel.

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

Virtueel Toetsenbord automatisch starten bij wachtwoordvelden

Het Virtuele toetsenbord verschijnt automatisch wanneer een wachtwoordveld wordt geselecteerd.

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

Vraag om bevestiging voor u gaat afdrukken

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

Favorieten beheren

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

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

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

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

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

gaat. De URL wordt ook toegevoegd aan de Domeinenlijst op de instellingen-pagina.

4.13. Data bescherming

Bestanden definitief verwijderen

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

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

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

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

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het panel **GEGEVENSBEVEILIGING** klikt u op **Bestandsvernietiging**.
4. 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 het vernietigen van de bestanden heeft voltooid.

c. **Samenvatting resultaten**

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

4.14. Ouderlijk Adviseur

Via de functie Ouderlijk Adviseur kunt u de toegang tot het internet en tot specifieke applicaties voor elk appparaat waarop de functie geïnstalleerd is, controleren. Zodra u Ouderlijk Adviseur hebt geconfigureerd, kunt u makkelijk nagaan wat uw kind doet op het apparaat dat hij gebruikt en waar hij de voorbije 24 uur is geweest. Bovendien geeft de app u statistieken over zijn activiteiten en interesses om beter in te schatten waar uw kind mee bezig is.

U hebt alleen een computer met internettoegang en een webbrowser nodig.

U kunt Ouderlijk Adviseur configureren voor het blokkeren van:

- ongeschikte webpagina's.
- applicaties zoals spelletjes, chatten, programma's die bestanden uitwisselen en dergelijke.
- specifieke contacten die niet telefonisch in contact mogen komen met uw kind.

Controleer de activiteiten van uw kinderen en wijzig de instellingen voor Ouderlijk Adviseur via Bitdefender-account vanaf elke computer of elk mobiel apparaat met internetverbinding.

4.14.1. Naar Ouderlijk Adviseur gaan - MIJN KINDEREN

Zodra u het gedeelte Ouderlijk Adviseur hebt geopend, is het venster **MIJN KINDEREN** beschikbaar. Hier kunt u alle profielen die u voor uw kinderen hebt aangemaakt, bekijken en bewerken. De profielen worden weergegeven als profielkaarten, zodat u ze snel kunt beheren en hun status in een oogopslag kunt controleren.

Zodra u een profiel creëert, kunt u meer gedetailleerde instellingen aanpassen om de toegang tot het internet en tot specifieke applicaties voor uw kinderen controleren.

U krijgt toegang tot de instellingen voor Ouderlijk Adviseur vanaf uw Bitdefender Central op elke computer of elk mobiel apparaat met een internetverbinding.

Ga naar uw Bitdefender-account.

- Op elk apparaat met internettoegang:
  1. Ga naar Bitdefender Central.
  2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
  3. Selecteer de functie **Ouderlijk Adviseur**.
  4. In het **MIJN KINDEREN**-venster dat verschijnt, kunt u de profielen van Ouderlijk Adviseur voor elk apparaat configureren.
- Vanuit uw Bitdefender-interface:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
  3. In het panel **OUDERLIJK ADVISEUR** klikt u op **Configureren**.

     U wordt afgeleid naar de Bitdefender-account webpagina. Zorg ervoor dat u aangemeld bent met uw gegevens.
  4. Selecteer de functie **Ouderlijk Adviseur**.
  5. In het **MIJN KINDEREN**-venster dat verschijnt, kunt u de profielen van Ouderlijk Adviseur voor elk apparaat configureren.

Opmerking
Zorg dat u bij de computer bent aangemeld met een beheerdersaccount. Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Adviseur openen en configureren.

4.14.2. Het profiel van uw kind toevoegen

Om de activiteiten van uw kind te beginnen volgen, moet u een profiel configureren en Ouderlijk Adviseur Agent van Bitdefender installeren op apparaten die hij gebruikt.

Om het profiel van uw kind aan Ouderlijk Adviseur toe te voegen:

1. Open het paneel van Ouderlijk Adviseur vanaf Bitdefender Central.

2. Klik op **PROFIEL TOEVOEGEN** in het rechtergedeelte van het **MIJN KINDEREN**-venster.
3. Voer specifieke informatie in de overeenkomstige velden in, zoals: naam en geboortedatum. Om een profielfoto toe te voegen, klikt u op de koppeling **Bestand kiezen**. Klik op **VOLGENDE STAP** om door te gaan.

   Op basis van normen voor de ontwikkeling van kinderen, laadt de geboortedatum van het kind instellingen voor het doorzoeken van het internet die als geschikt geacht worden voor deze leeftijdcategorie.
4. Indien Bitdefender Total Security 2018 al op het apparaat van uw kind geïnstalleerd is, selecteer dit apparaat uit de beschikbare lijst en selecteer de account die u wenst te controleren. Klik op **OPSLAAN**.

   Indien uw kind een Android- of iOS-toestel gebruikt en de toepassing Bitdefender Ouderlijk adviseur nog niet geïnstalleerd is, klikt u op **APPARAAT TOEVOEGEN**. Indien uw kind een Mac-apparaat gebruikt en de Bitdefender Antivirus for Mac-app niet geïnstalleerd is, klikt u op dezelfde knop. Selecteer het besturingssysteem waarop u de app wenst te installeren en klik op **VOLGENDE STAP** om verder te gaan.
5. Voer het e-mailadres in waar we de downloadkoppeling voor de installatie van de toepassing Ouderlijke Adviseur voor het Bitdefender-toepassing heen moeten sturen en klik vervolgens op **INSTALLATIEKOPPELING VERZENDEN**.

Belangrijk

Op toestellen die op Windows gebaseerd zijn, hebt u in uw abonnement opgenomen dat Bitdefender Total Security 2018 moet gedownload en geïnstalleerd worden.
Op macOS-apparaten moet het Bitdefender Antivirus for Mac-product gedownload en geïnstalleerd worden.
Op Android en iOS-apparaten moet de toepassing Ouderlijk Adviseur van Bitdefender gedownload en geïnstalleerd worden.

Meerdere toestellen aan hetzelfde profiel toekennen

U kunt meerdere toestellen aan hetzelfde profiel toekennen, zodat dezelfde beperkingen worden toegepast. Dit doet u zo:

1. Ga naar Bitdefender Central.
2. Selecteer de functie Ouderlijk Adviseur.

3. Klik op de ⋮ -icoon op de gewenste profielkaart en selecteer vervolgens **Apparaten**.
4. Selecteer uit de lijst de beschikbare apparaten waar u het profiel aan wilt toekennen.

   Indien uw kind een Android- of iOS-toestel gebruikt en de toepassing Bitdefender Ouderlijk adviseur nog niet geïnstalleerd is, klikt u op **APPARAAT TOEVOEGEN**. Indien uw kind een Mac-apparaat gebruikt en de Bitdefender Antivirus for Mac-app niet geïnstalleerd is, klikt u op dezelfde knop. Selecteer het besturingssysteem waarop u de app wenst te installeren en klik op **VOLGENDE STAP** om verder te gaan.

   Voer het e-mailadres in waar we de downloadkoppeling voor de installatie van de toepassing Ouderlijke Adviseur voor het Bitdefender-toepassing heen moeten sturen en klik vervolgens op **INSTALLATIEKOPPELING VERZENDEN**.
5. Nadat u het installatieproces hebt voltooid op het nieuwe toestel, selecteert u het uit de lijst om het profiel toe te passen.
6. Selecteer **OPSLAAN**.

Ouderlijk Adviseur koppelen aan Bitdefender Central

Om de online activiteiten van uw kind op Android en iOS te bewaken, moet u zijn apparaat koppelen aan uw Bitdefender-account door in te loggen op de account vanuit de app.

Om een apparaat te koppelen aan uw Bitdefender-account:

- Op **Android**:
  1. Selecteer de knop die verschijnt in het e-mailbericht dat door onze server wordt verstuurd. U wordt doorgestuurd naar Google Play Store.

     Indien u ervoor koos om via uw Bitdefender-account geen downloadkoppeling te versturen naar het e-mailadres van uw kind, gaat u naar Google Play en zoekt u naar de app in Bitdefender Ouderlijk adviseur.
  2. Tik op **INSTALLEREN** in het Bitdefender Parental Advisor-venster en tik vervolgens op **ACCEPTEREN** indien u gevraagd wordt om toelatingen toe te staan. Bitdefender heeft toelatingen nodig om u op de hoogte te

houden van de activiteit van uw kind. Als ze niet worden geaccepteerd, zal de app niet geïnstalleerd worden.

3. Open de app Ouderlijk Adviseur.
4. Lees de **Abonnementsovereenkomst** en tik vervolgens op **VERDERGAAN**.
5. Log in op uw bestaande Bitdefender-account of meld u aan met een Google-account.

   Indien u geen Bitdefender-account hebt, kunt u ervoor kiezen een nieuwe account aan te maken via de betreffende optie.
6. Tik op **GA NAAR INSTELLINGEN** om naar het scherm te gaan waar u de Toegankelijkheidsoptie kunt inschakelen voor de app. Volg de instructies op het scherm om de app correct te configureren.
7. Tik op **GA NAAR INSTELLINGEN** om naar het scherm te gaan waar u de optie Gebruikstoegang Inschakelen kunt inschakelen voor de app. Volg de instructies op het scherm om de app correct te configureren.
8. Tik op **GA NAAR INSTELLINGEN** om naar het scherm te gaan waar u de optie Beheerdersrechten Apparaat Activeren kunt inschakelen voor de app. Volg de instructies op het scherm om de app correct te configureren.

   Zo zal uw kind de Ouderlijk Adviseur Agent niet kunnen de-installeren.
9. Tik op **KLAAR** om het installatieproces te beëindigen.

Opmerking

Op Android 4.4 en latere versies, moeten op Bitdefender, om de sms-berichten van uw kind te kunnen bijhouden, de instellingen van de ingebouwde Android Messages-app gewijzigd worden. We bevelen u aan om **Ja** te kiezen in het dialoogvenster dat verschijnt nadat u in de app op **KLAAR** hebt getikt.

- Op **iOS**:

1. Selecteer de knop die verschijnt in het e-mailbericht dat door onze server naar u wordt verstuurd en installeer vervolgens de app.
2. Open de app Ouderlijk Adviseur.
3. Er wordt een introductiewizard weergegeven met details over de producteigenschappen. Tik op **Volgende** om verder te gaan.

4. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
5. Geef toestemming voor toegang tot de locatie van het apparaat, zodat Bitdefender het kan vinden.
6. Geef de app toestemming om meldingen te verzenden.
7. Wijs het apparaat toe aan het profiel van uw kind.

De activiteit van de kind bewaken

Met Bitdefender kunt u volgen wat uw kinderen online doen.

Zo kunt u altijd exact uitvinden welke websites ze hebben bezocht, welke toepassingen ze hebben gebruikt of welke activiteiten door Ouderlijk Adviseur werden geblokkeerd.

Afhankelijk van de instellingen die u invoert, kunnen de verslagen gedetailleerde informatie bevatten voor elke gebeurtenis, bijvoorbeeld:

- De status van de gebeurtenis.
- De ernst van de kennisgeving.
- De apparaatnaam.
- De datum en het tijdstip waarop de gebeurtenis is opgetreden.

Voor het bewaken van het internetverkeer, de geopende toepassingen of de Facebook-activiteit voor uw kind:

1. Open het paneel van Ouderlijk Adviseur vanaf Bitdefender Central.
2. Selecteer de gewenste apparatenkaart.

   In het venster **Activiteit** kunt u de informatie bekijken die u interesseert. U kunt ook de koppeling op de kaart van het gevolgde apparaat **Activiteit van vandaag bekijken** selecteren, om u naar het **Activiteit**-venster te brengen.

De Algemene instellingen configureren

Standaard worden de activiteiten van uw kinderen bijgehouden wanneer u Ouderlijk Adviseur activeert.

Om e-mailmeldingen te ontvangen:

1. Open het paneel van Ouderlijk Adviseur vanaf Bitdefender Central.

2. Selecteer het tabblad **Instellingen** in de rechterbovenhoek.
3. De overeenkomende optie om activiteitsverslagen te ontvangen inschakelen.
4. Voer het e-mailadres in waarnaar de e-mailmeldingen moeten worden verzonden.
5. E-mailmeldingen ontvangen voor het volgende:
   - Geblokkeerde websites
   - Geblokkeerde apps
   - Zones met beperkte toegang
   - Oproep of sms ontvangen van een geblokkeerd telefoonnummer
   - Verwijdering van Parental Advisor Facebook-app
6. Klik op **OPSLAAN**.

Een profiel bewerken

Om een bestaand profiel te bewerken:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Ouderlijk Adviseur**.
3. Klik op de ⋮ -icoon op de gewenste profielkaart en selecteer vervolgens **Bewerken**.
4. Nadat u de gewenste instellingen hebt aangepast, selecteert u **OPSLAAN**.

Een profiel verwijderen

Om een bestaand profiel te verwijderen:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Ouderlijk Adviseur**.
3. Klik op de ⋮ -icoon op de gewenste profielkaart en selecteer vervolgens **Verwijderen**.
4. Bevestig uw keuze.

4.14.3. Profielen in Ouderlijk Adviseur configureren

Om uw kind te beginnen volgen, moet u een profiel aan het apparaat toestellen, waarop Ouderlijk Adviseur Agent van het Bitdefender geïnstalleerd is.

Nadat u een profiel hebt toegevoegd voor uw kind, kunt u meer gedetailleerde instellingen aanpassen om de toegang tot het internet en specifieke toepassingen te volgen en controleren.

Om een profiel te beginnen configureren, selecteert u de gewenste profielkaart uit het **MIJN KINDEREN**-venster.

Klik op een tabblad om de overeenkomende functie van Ouderlijk Adviseur te configureren voor het apparaat:

- Activiteit - geeft alle activiteiten, interesses, lokaties en interacties met vrienden vanaf vandaag weer.
- Toepassingen - biedt u de mogelijkheid om de toegang tot bepaalde applicaties, zoals games, berichtensoftware, films enz. te blokkeren.
- Websites - hiermee kunt uw webnavigatie filteren.
- Telefooncontacten - hier kunt u bepalen welke contacten uit de lijst van uw vrienden toestemming hebben om via de telefoon met uw kind in contact te treden.
- Locatie kind - hier kunt u locaties instellen die al dan niet veilig zijn voor uw kind.
- Sociaal - hier kunt u de toegang tot sociale netwerken blokkeren.
- Tijdschema - hiermee kunt u de toegang tot de apparaten die u in het profiel van uw kind hebt aangeduid, blokkeren.

Activiteit

Het Activiteit-venster geeft u gedetailleerde informatie over de activiteiten van uw kinderen van de voorbije 24 uur, zowel thuis als elders. Om activiteiten van de voorbije dagen te bekijken, klikt u op de kalendericoon in de linkerbovenhoek van het venster.

Afhankelijk van de activiteit kan dit venster informatie bevatten over:

- **Lokaties** - hier kunt u de lokaties zien waar uw kind in de loop van de dag was.

- **Interesses** - hier vindt u informatie over de categorieën websites die uw kind heeft bezocht. Klik op de koppeling **Ongepaste inhoud bekijken** om toegang tot specifieke interesses toe te staan of te weigeren.
- **Sociale interactie** - hier kunt u zien met welke contactpersonen uw kind heeft gecommuniceerd. Klik op de koppeling **Contacten beheren** om de contacten te selecteren met wie u kind al dan niet in contact mag blijven.
- **Toepassingen** - hier kunt u zien welke toepassingen uw kind heeft gebruikt. Klik op de koppeling **App-beperkingen overlopen** om de toegang tot specifieke toepassingen te blokkeren of toe te staan.
- **Activiteit tijdens de dag** - hier kunt u zien hoeveel tijd uw kind online heeft doorgebracht op alle aan uw kind toegekende apparaten en de plaats waar hij/zij actief was. De verzamelde informatie heeft betrekking op de dag van vandaag.

Applicaties

Het Toepassingen-venster helpt u om te voorkomen dat applicaties lopen. Games, media en messaging software, maar ook andere categorieën van software kunnen op deze manier worden geblokkeerd.

De functie kan geactiveerd of geïnactiveerd worden met de hiertoe bestemde schakelaar.

Toepassingsbeheer configureren voor een specifieke gebruikersaccount:

1. Er wordt een lijst met kaarten weergegeven. De kaarten vertegenwoordigen de apps die uw kind gebruikt.
2. Selecteer de kaart met de app die u uw kind niet langer wilt laten gebruiken.

   De markeringssymbool dat verschijnt toont dat uw kind de app niet zal kunnen gebruiken.

Websites

Het Websites-venster helpt u om websites met ongepaste inhoud te blokkeren. Websites waarop video's, games, media en messaging-software worden gehoost, maar ook andere categorieën van negatieve inhoud, kunnen op deze manier geblokkeerd worden.

De functie kan geactiveerd of geïnactiveerd worden met de hiertoe bestemde schakelaar.

Afhankelijk van de leeftijd die u voor uw kind instelt, wordt de Interesses-lijst standaard voorzien van een selectie geactiveerde categorieën. Om de toegang tot een specifieke categorie toe te staan of te weigeren, klikt u erop.

Het markeringssymbool dat verschijnt, geeft aan dat uw kind de inhoud met betrekking tot een specifieke categorie niet zal kunnen openen.

Een website toestaan of blokkeren

Om de toegang tot bepaalde webpagina's te beperken of toe te staan, moet u ze als volgt aan de Uitsluitingen-lijst toevoegen:

1. Klik op de knop **BEHEREN**.
2. Tik de webpagina die u wilt toestaan of blokkeren in het overeenkomstige veld in.
3. Klik op **Toestaan** of **Blokkeren**.
4. Klik op **VOLTOOIEN** om de wijzigingen op te slaan.

Opmerking

Toegangsbeperkingen voor websites kunnen enkel ingesteld worden voor Windows-, Android- en macOS-apparaten die toegevoegd zijn aan het profiel van uw kind.

Telefooncontacten

Het Telefooncontacten-venster biedt u de mogelijkheid om te bepalen welke vrienden uit de lijst van uw kind al dan niet toestemming hebben om via de telefoon met hem in contact te treden.

Om een specifiek telefoonnummer van een contact te beperken, moet u aan het profiel van uw kind eerst het Android-apparaat dat het gebruikt, toevoegen, aan de hand van de volgende stappen:

1. Selecteer het tabblad **Ouderlijk Adviseur** in Bitdefender Central.
2. Klik op de gewenste kaart op de koppeling **Ouderlijk adviseur installeren op een apparaat**.
3. Klik op **APPARAAT TOEVOEGEN** in het venster dat verschijnt.
4. De **Bitdefender Ouderlijk adviseur voor Android**-optie is standaard geselecteerd. Klik op **VOLGENDE STAP** om door te gaan.
5. Selecteer het profiel van het kind waarvoor u beperkingen wilt instellen.

6. Selecteer het tabblad **Telefooncontacten**.

   Er wordt een lijst met kaarten weergegeven. De kaarten staan voor de contacten uit de Android-smartphone van uw kind.

7. Selecteer de kaart met het telefoonnummer dat u wilt blokkeren.

   Het markeringssymbool dat verschijnt, geeft aan dat uw kind niet zal bereikt worden via het geselecteerde telefoonnummer.

Om ongekende telefoonnummers te blokkeren, activeert u de schakelaar **Interactie zonder ID beller blokkeren**.

Opmerking
Er kunnen enkel beperkingen voor telefoongesprekken ingesteld worden voor Android-apparaten die aan het profiel van uw kind werden toegevoegd.

Locatie van kind

Bekijk de huidige locatie van uw apparaat op Google Maps. De locatie wordt elke 5 seconden vernieuwd, dus u kunt deze volgen indien hij in beweging is.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen:

- Als GPS is ingeschakeld op het apparaat, kan de locatie worden bepaald tot op enkele meters, zolang deze binnen het bereik van GPS-satellieten is (dus niet in een gebouw).
- Indien het apparaat binnenshuis is, kan de locatie tot op binnen tientallen meters worden bepaald indien Wi-Fi is ingeschakeld en er beschikbare draadloze netwerken in de omtrek zijn.
- Anders worden alleen gegevens van het mobiele netwerk gebruikt om de locatie te bepalen, waardoor de nauwkeurigheid beperkt blijft tot enkele honderden meters.

Locatie & Veilige check-in configureren

Om zeker te zijn dat uw kind naar bepaalde lokaties gaat, kunt u een lijst met veilige en onveilige plaatsen aanmaken. Telkens wanneer hij alleen een vooraf ingestelde zone betreedt, verschijnt er in de Ouderlijk Adviseur-app een melding die vraagt om te bevestigen dat hij veilig is. Door op **IK BEN VEILIG AANGEKOMEN** te tikken, krijgt u via een melding in uw Bitdefender-account een melding dat de eindbestemming bereikt werd.

Indien uw kind geen bevestiging geeft, kunt u nog steeds het overzicht van zijn locatie in de loop van de dag bekijken door zijn profiel te openen in uw Bitdefender-account.

Om een lokatie te configureren:

1. Klik op **Apparaten** in het rooster van het **Locatie kind**-venster.
2. Klik op **APPARATEN KIEZEN** en selecteer vervolgens het apparaat dat u wenst te configureren.
3. Klik in het **Gebieden**-venster op de knop **GEBIED TOEVOEGEN**.
4. Kies het type locatie, **VEILIG** or **BEPERKT**.
5. Tik een geldige naam in voor het gebied waar uw kind al dan niet toegang toe heeft.
6. Stel het bereik in dat moet worden toegepast voor controle via de glijder **Radius**.
7. Klik op **GEBIED TOEVOEGEN** om uw instellingen op te slaan. U wordt gevraagd of uw kinderen al dan niet alleen zullen reizen. Bevestig met Ja of Neen.

Opmerking
De locatietracker kan gebruikt worden om Android- en iOS-apparaten te volgen waarop de Bitdefender Ouderlijk adviseur op geïnstalleerd is.

Sociaal

Ouderlijk Adviseur volgt de Facebook-account van uw kind en rapporteert de belangrijkste activiteiten die plaatsvinden.

Deze online activiteiten worden gecontroleerd en u wordt gewaarschuwd als ze een bedreiging voor de privacy van uw kind blijken te zijn.

De bewaakte elementen van de online account omvatten:

- Accountgegevens
- Pagina's liken
- geüploade foto's

Om de Facebook-bescherming voor een specifieke gebruikersaccount te configureren, tikt u het e-mailadres van de kinderaccount waarop u toezicht houdt in en klikt u vervolgens op **VERZENDEN**.

Licht uw kind in over uw intenties en vraag het om de knop **ACCOUNT BESCHERMEN** die van ons in zijn e-mailberichten ontvangt, aan te klikken.

Om naar de Facebook-account onder toezicht te gaan, klikt u op de koppeling **Bekijken op Facebook**.

Om te stoppen met het bewaken van de account, gebruikt u de knop **ACCOUNT LOSKOPPELEN** bovenaan.

Om via e-mail op de hoogte gebracht te worden wanneer uw kind de Ouderlijk adviseur-app van zijn toestel verwijdert, vinkt u het bijhorende vakje aan.

Tijdschema

Met het Tijdschema-venster kunt u de toegang tot de apparaten die u in het profiel van uw kind hebt aangeduid, blokkeren. Er kunnen op elk uur tijdens de schooltijd en tijdens het weekend beperkingen worden ingesteld, enkel voor Android- en Windows-apparaten.

Om tijdsbeperkingen tijdens de nacht te configureren:

1. Selecteer in het gebied **BEDRIJD** de vakjes **Schoolnachten** en **Weekendnachten**.
2. Klik op de ⊗-icoon vanuit de overeenkomstige vakjes en gebruik vervolgens de pijltjes omhoog en omlaag om de tijdsintervallen in te stellen tijdens dewelke de toegang moet geblokkeerd worden.

Om tijdsbeperkingen tijdens de dag te configureren:

1. In het gebied **LIMIETEN OVERDAG** krijgt u de volgende opties:
   - **CUMULATIEF**
     a. Selecteer de vakjes **Tijdslimieten schooltijd** en **Tijdslimieten weekends**.
     b. Sleep de balkjes langs de schaal naar de gewenste lengte dat toegang tot de apparaten toegestaan is.
   - **SPECIFIEK**
     a. Selecteer de vakjes **Tijdslimieten schooltijd** en **Tijdslimieten weekends**.
     b. Selecteer de tijdsintervallen in het rooster waarbinnen toegang moet geblokkeerd worden.

Opmerking
De instellingen **CUMULATIEF** en **SPECIFIEK** zijn zo ontworpen dat ze onafhankelijk van elkaar werken.

4.15. Anti-Theft voor mobiele apparaten

Diefstal van laptops is een belangrijk probleem dat individuele personen en bedrijven evenzeer schaadt. De gegevens die men verliest kan zelfs voor nog meer schade zorgen dan het verliezen van de hardware zelf en kan op zowel financieel als emotioneel gebied belangrijk zijn.

Er zijn maar weinig mensen die de juiste stappen nemen om hun belangrijke persoonlijke, zakelijke en financiële gegevens te beveiligen voor het geval ze gestolen of verloren worden.

Bitdefender Antidiefstal helpt u om beter voorbereid te zijn op een dergelijk gebeuren en stelt u in staat om op afstand uw laptop te lokaliseren of te vergrendelen en om zelfs alle gegevens ervan te wissen, mocht uw laptop ooit tegen uw wil worden meegenomen.

Om de Antidiefstalfuncties te gebruiken, moet er worden voldaan aan de volgende minimale vereisten:

- De bevelen kunnen enkel verzonden worden vanuit de Bitdefender-account.
- De laptop moet zijn verbonden met Internet om de opdrachten te kunnen ontvangen.

Antidiefstalfuncties werken op de volgende manier:

Zoeken

Bekijk de locatie van uw apparaat op Google Maps.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen. De locatie wordt tot op enkele tientallen meters nauwkeurig bepaald als Wi-Fi is ingeschakeld op uw laptop en er draadloze netwerken in de omgeving zijn.

Als de laptop verbonden is met een LAN-kabel zonder dat er een Wi-Fi-locatie beschikbaar is, wordt de locatie bepaald op basis van het IP-adres, en dat is veel minder nauwkeurig.

Waarschuwingen

Een waarschuwing van op afstand op het toestel verzenden.

De functie is enkel beschikbaar op mobiele toestellen.

Vergrendelen

Uw laptop vergrendelen en een PIN van 4 cijfers instellen om hem te ontgrendelen. Wanneer u de opdracht **Vergrendelen** verzendt, start het systeem opnieuw op en opnieuw inloggen op Windows is alleen mogelijk als de juiste PIN die u hebt ingesteld, wordt ingevoerd.

Indien u wilt dat Bitdefender foto's maakt van de persoon die probeert om uw laptop te openen, moet u het bijhorende vakje aanvinken. De gemaakt foto's worden gemaakt met de frontcamera en samen met de tijdmarkering weergegeven op de overzichtspagina van de Antidiefstal. Alleen de twee recentste foto's worden opgeslagen.

Deze actie is alleen beschikbaar op laptops die aan de voorkant beschikken over een camera.

Wissen

Alle gegevens van uw systeem verwijderen. Wanneer u de opdracht **Wissen** verzendt, start de laptop opnieuw op en worden de gegevens op alle delen van de harde schijf gewist.

IP tonen

Toont het laatste IP-adres voor het geselecteerde apparaat. Klik op **TOON IP** om dit zichtbaar te maken.

Antidiefstal wordt geactiveerd na de installatie en is uitsluitend toegankelijk via uw Bitdefender-account vanaf elk apparaat met een internetverbinding, waar u ook bent.

De Antidiefstalfuncties gebruiken

Om naar de Antidiefstalfuncties te gaan, gebruikt u een van de volgende mogelijkheden:

- Vanuit het hoofdvenster van Bitdefender:
  1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
  2. Klik op de actieknop **Antidiefstal**.
  3. In het Bitdefender Central-venster dat verschijnt, klikt u op de gewenste toetstelkaart en selecteert u **Antidiefstal**.
- Op elk apparaat met internettoegang:
  1. Open een internetbrowser en ga naar: https://central.bitdefender.com.

2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Selecteer het paneel **Mijn apparaten**.
4. Klik op de gewenste toestelkaart en selecteer vervolgens **Antidiefstal**.
5. Selecteer de functie die u wilt gebruiken:

   Toon IP - geeft het laatste IP-adres van uw apparaat weer.
   Lokaliseren - geef de locatie van uw apparaat weer in Google Maps.
   Waarschuwing - een waarschuwing op het toestel verzenden.
   Vergrendelen - vergrendel uw laptop en stel een pincode in die moet worden ingevoerd voordat het apparaat kan worden ontgrendeld.
   Wissen - wis alle gegevens van uw laptop.

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

4.16. USB Immunizer

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

Helaas kan deze functie ook worden gebruikt door bedreigingen om automatisch te starten en zo in uw computer te infiltreren vanaf media die beschreven kunnen worden, zoals USB-sticks en geheugenkaarten die via kaartlezers worden verbonden. De afgelopen jaren zijn er talloze op Autorun gebaseerde aanvallen aangemaakt.

Met USB Immunizer kunt u voorkomen dat een willekeurige NTFS, FAT32 of FAT-geformatteerde USB-stick ooit nog automatisch 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-computer.

Om een USB-apparaat te immuniseren:

1. Verbind de USB-stick met uw computer.

2. Blader op uw computer naar de locatie van het verwijderbare opslagapparaat en rechterklik op het pictogram ervan.
3. Ga in het contextuele menu naar **Bitdefender** en selecteer **Deze schijf immuniseren**.

Opmerking
Als het station al immuun is gemaakt, verschijnt het bericht **Het USB-apparaat wordt beveiligd tegen op autorun gebaseerde bedreigingen** in plaats van de optie Immuniseren.

Om te voorkomen dat uw computer bedreigingen start vanaf USB-apparaten die niet immuun zijn gemaakt, kunt u de media autorun-functie uitschakelen. Zie "*De automatische kwetsbaarheidsbewaking gebruiken*" (p. 130) voor meer informatie.

5. SYSTEEMOPTIMALISATIE

5.1. Extra

Bitdefender wordt geleverd met een Extra-gedeelte dat u helpt de integriteit van uw systeem te behouden. De aangeboden hulpmiddelen voor het onderhoud zijn van cruciaal belang voor de verbetering van de reactiviteit van uw systeem en het efficiënte beheer van de harde schijfruimte.

Bitdefender stelt u de volgende hulpmiddelen voor optimalisering van PC's voor:

- OneClick Optimizer analyseert en verbetert uw systeemsnelheid door talrijke taken uit te voeren d.m.v. een enkele klik op een knop.
- Startup Optimizer beperkt de opstarttijd van uw systeem door te voorkomen dat onnodige toepassingen worden geladen als de pc wordt opgestart.
- Disk Cleanup identificeert de bestanden die de hoofdoorzaak kunnen zijn voor het gebrek aan ruimte op uw schijf, en geeft u de mogelijkheid te beslissen of u de bestanden houdt of niet.

5.1.1. De snelheid van uw systeem optimaliseren in een enkele klik

Problemen als storingen van de harddisk, overgebleven registerbestanden en browsergeschiedenis kunnen uw computer vertragen en dat kan vervelend voor u worden. Deze kunnen nu allemaal worden opgelost met een enkele klik op een knop.

OneClick Optimizer stelt u in staat nutteloze bestanden te herkennen en te verwijderen door talloze opschoontaken tegelijk uit te voeren.

Om het OneClick Optimizer-proces te starten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **OneClick Optimizer**.
   a. **Analyseren**

      Wacht tot Bitdefender het zoeken naar systeemproblemen heeft voltooid.

      - Disk Cleanup - identificeert onnodige bestanden en mappen.

- Opruiming Register - herkent ongeldige of verlopen referenties in het register van Windows.
- Privacy Opruiming - herkent tijdelijke internetbestanden en cookies, browsercache en geschiedenis.

Het aantal gevonden problemen wordt weergegeven. Klik op de koppeling **Details weergeven** om ze te bekijken voordat u doorgaat met het opruimproces. Klik op **OPTIMALISEREN** om door te gaan.

b. **Bezig met optimaliseren**

Wacht tot Bitdefender het optimaliseren van uw systeem heeft voltooid.

c. **Problemen**

Hier kunt u het resultaat van de bewerking bekijken.

Wanneer u uitgebreide informatie wilt over het optimaliseringsproces, klikt u op de knop **GEDETAILLEERD VERSLAG WEERGEVEN**.

5.1.2. De opstarttijd van uw pc aan het optimaliseren

Een lange opstarttijd is een echt probleem veroorzaakt doordat toepassingen zijn ingesteld om te worden uitgevoerd zonder dat dat nodig is. Het wachten van een paar minuten tot een systeem is opgestart, kan u waardevolle tijd en productiviteit kosten.

Het venster Startup Optimizer geeft weer welke toepassingen worden uitgevoerd tijdens het opstarten van het systeem en laat u hun gedrag beheren in deze stap.

Om het Startup Optimizer-proces te starten:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **Startup Optimizer**.

a. **Toepassingen selecteren**

U kunt een lijst met toepassingen die bij het opstarten worden uitgevoerd zien. Selecteer de toepassingen die u bij het opstarten wilt uitschakelen of uitstellen.

b. **Gebruikersgroepkeuze**

Zien wat andere gebruikers van Bitdefender hebben besloten te doen met de app die u hebt geselecteerd.

c. **Opstarttijd systeem**

Controleer de schuif bovenaan het venster om te zien hoeveel tijd zowel uw systeem als de geselecteerde toepassingen nodig hebben om te worden uitgevoerd bij het opstarten.

Opnieuw opstarten van het systeem is vereist om informatie te kunnen ophalen over de opstarttijd van systeem en toepassingen.

d. **Opstartstatus**

- **Aan.** Selecteer deze optie als u wilt dat een toepassing wordt uitgevoerd bij het opstarten van het systeem. Deze optie is standaard ingeschakeld.
- **Uitstel.** Selecteer deze optie om het uitvoeren van een programma bij het opstarten van het systeem uit te stellen. Dit betekent dat de geselecteerde toepassingen starten met vijf minuten vertraging nadat de gebruiker inlogt op het systeem. De functie **Uitstellen** is vooraf bepaald en kan niet worden geconfigureerd door de gebruiker.
- **Uitschakelen.** Selecteer deze optie om het uitvoeren van een programma bij het opstarten van het systeem uit te schakelen.

e. **Resultaten**

Informatie zoals de geschatte systeemopstarttijd na het uitstellen of uitschakelen van programma's wordt weergegeven.

Opnieuw opstarten van het systeem kan vereist zijn om al deze info te zien.

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

Opmerking

In geval uw abonnement verloopt of u besluit om Bitdefender te de-installeren, worden de programma's waarvan u een stop had gepland bij het opstarten hersteld tot hun standaardopstartinstellingen.

5.1.3. Uw schijf optimaliseren

Onnodige bestanden en mappen die schijfruimte innemen, kunnen ervoor zorgen dat uw systeem trager wordt. Daarom is het aanbevolen om uw systeemsnelheid te verbeteren door regelmatig een opruiming uit te voeren.

Bitdefender Disk Cleanup helpt u uw schijfruimte te optimaliseren door de bestanden te identificeren die de hoofdoorzaak kunnen zijn voor het gebrek

aan ruimte op uw schijf. Daarnaast hebt u ook de mogelijkheid om te beslissen wat u gaat doen met de geïdentificeerde bestanden.

Om uw systeem op te ruimen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de actieknop **Schijfopruiming**.
3. De eerste keer dat u Disk Cleanup gebruikt, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.

   a. **Drives en apparaten**

   U ziet een lijst van de beschikbare schijven. Naast Windows-schijven worden ook externe harde schijven en USB-apparaten gescand en in de lijst weergegeven. Klik op **STATION ANALYSEREN** vanuit het schijfgebied dat u wilt opruimen.

   b. **Station aan het analyseren**

   De geselecteerde drive is geanalyseerd. Wacht tot Bitdefender het zoeken naar grote bestanden en mappen heeft voltooid.

   c. **Problemen**

   Hier kunt u de resultaten van de bewerking bekijken. Gebruik het uitklappijltje **FILTEREN OP** in de linkerzijde van het venster om te kiezen in welke volgorde u de resultaten wilt zien. U kunt de resultaten op maat filteren (van 10 MB tot meer dan 5 GB) of op type (de bestanden worden per extensie in verschillende mappen geplaatst).

   Selecteer de bestanden die u wenst te verwijderen en klik vervolgens op **KEUZE BEVESTIGEN** om het verwijderproces op te starten.

   Beschermde en belangrijke bestanden verantwoordelijk voor de werking van uw systeem worden ook geïdentificeerd, maar kunnen niet worden geselecteerd of verwijderd.

   Klik op de icoon om toegang te krijgen tot de mappen die behoren tot de geselecteerde bestanden.

   d. **Bevestig uw selectie**

   De lijst met de geselecteerde bestanden wordt weergegeven. Controleer nogmaals dat u deze bestanden niet meer nodig hebt, want eens u verdergaat, kunnen deze niet meer uit de Prullenbak worden gehaald. Bevestig uw keuze door op **VERWIJDEREN** te klikken.

e. **Samenvatting resultaten**

De status van het proces wordt als volgt weergegeven:

Alle geselecteerde bestanden werden verwijderd.

Een of meer van de geselecteerde bestanden kon niet worden verwijderd **of** geen van de geselecteerde bestanden kon worden verwijderd.

Klik op **VOLTOOIEN** om het venster te sluiten.

5.2. Profielen

Dagelijkse werkactiviteiten, films kijken of games spelen kan het systeem vertragen, met name wanneer ze tegelijkertijd worden uitgevoerd met het Windows-updateproces en onderhoudstaken. Met Bitdefender kunt u nu uw voorkeursprofiel kiezen en toepassen. Het maakt systeemafstellingen om de prestaties van specifieke geïnstalleerde toepassingen te verbeteren.

Bitdefender verschaft de volgende profielen:

- Werkprofiel
- Filmprofiel
- Gameprofiel
- Openbaar Wi-Fi-profiel
- Profiel batterijmodus

Als u besluit om **Profielen** niet te gebruiken, wordt er een standaardprofiel ingeschakeld genaamd **Standaard** dat geen optimalisering verschaft aan uw systeem.

Afhankelijk van uw activiteit worden de volgende productinstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Alle Bitdefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Automatische Update wordt uitgesteld.
- Geplande scans zijn uitgesteld.
- 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 Total Security 2018 ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Advanced Threat Defense is ingeschakeld
- De Bitdefender-firewalle is ingeschakeld en de volgende instellingen worden toegepast op uw draadloze adapter.
  - Geheime modus - AAN
  - Netwerktype - Openbaar
- De volgende instellingen van Webbescherming zijn ingeschakeld:
  - SSL scannen
  - Bescherming tegen fraude
  - Bescherming tegen phishing

5.2.1. Werkprofiel

Meerdere taken uitvoeren op het werk, zoals het verzenden van e-mails, een videogesprek hebben met collega's op afstand of werken met designtoepassingen kan invloed hebben op uw systeemprestaties. Werkprofiel is ontworpen om u te helpen uw werkefficiëntie te verbeteren, door een aantal diensten op de achtergrond en onderhoudstaken uit te schakelen.

Werkprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Werkprofiel zit:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. 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 start, kunt u de toepassing handmatig toevoegen aan de **Toepassingenlijst**.

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

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.
4. In het venster **WERKPROFIEL** klikt u op de link **Toepassingenlijst**.
5. Klik op **Toevoegen** om een nieuwe toepassing toe te voegen aan de **Toepassingenlijst**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

5.2.2. Filmprofiel

Het weergeven van videocontent in HD-kwaliteit, zoals HD-films, vereist belangrijke systeemvermogens. Filmprofiel stelt het systeem- en de productinstellingen af zodat u kunt genieten van een ononderbroken en vloeiende filmervaring.

Filmprofiel configureren

Om de te nemen handelingen te configureren terwijl u in Filmprofiel bent:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
4. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor videospelers boosten
   - Productinstellingen voor Filmprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen
   - Instellingen vermogensplan voor films afstellen.
5. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig videospelers toevoegen aan de lijst Filmprofiel

Indien Bitdefender niet automatisch naar Filmprofiel overschakelt wanneer u een bepaalde videospeler start, kunt u de toepassing handmatig toevoegen aan de **Spelerslijst**.

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
4. In het venster **FILMPROFIEL** klikt u op de link **Spelerslijst**.
5. Klik op **Toevoegen** om een nieuwe toepassing toe te voegen aan de **Spelerslijst**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

5.2.3. Gameprofiel

Genieten van een ononderbroken game-ervaring heeft alles te maken met het verminderen van systeemolaadtijden en het beperken van vertraging. Door gebruik te maken van gedragsheuristiek tegelijk met een lijst van bekende games, kan Bitdefender automatisch uitgevoerde games detecteren en uw systeemvermogen optimaliseren zodat u kunt genieten van uw gametijd.

Gameprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Gameprofiel zit:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Klik op de knop **CONFIGUREREN** in het gebied Gameprofiel.
4. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor games boosten
   - Productinstellingen voor Gameprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen
   - Instellingen vermogensplan voor games afstellen.
5. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig games aan de Spellijst toevoegen

Indien Bitdefender niet automatisch naar het Gameprofiel overschakelt wanneer u een bepaalde game of toepassing start, kunt u de toepassing handmatig toevoegen aan de **Spellijst**.

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Klik op de knop **CONFIGUREREN** in het gebied Gameprofiel.
4. In het venster **GAMEPROFIEL** klikt u op de link **Spellijst**.

5. Klik op **Toevoegen** om een nieuwe game toe te voegen aan de **Spellijst**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de game, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

5.2.4. Openbaar Wi-Fi-profiel

E-mailberichten verzenden, gevoelige logingegevens invoeren of online winkelen terwijl u met onveilige draadloze netwerken verbonden bent, kan uw persoonlijke gegevens in gevaar brengen. Openbaar Wi-Fi-profiel past de productinstellingen aan, zodat u online betalingen kunt uitvoeren en gevoelige informatie kunt gebruiken in een beveiligde omgeving.

Openbaar Wi-Fi-profiel configureren

Om Bitdefender configureren zodat productinstellingen worden toegepast wanneer u verbonden bent met een onveilig draadloos netwerk:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. 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 op **Opslaan**.

5.2.5. Profiel batterijmodus

Het profiel Accumodus is speciaal ontworpen voor laptop- en tabletgebruikers. Het doel ervan is om de invloed op vermogensverbruik van zowel systeem als Bitdefender te beperken als het accuniveau lager is dan de standaardconsumptie van deze die u selecteert.

Profiel Accumodus aan het configureren

Om het profiel Accumodus te configureren:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.
3. Klik op de knop **CONFIGUREREN** in het gebied Profiel Batterijmodus.

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

Tik een geldige waarde in het vakje in of selecteer er een met de pijltjes omhoog en om laag om in te stellen wanneer het systeem moet beginnen werken in Batterijmodus. Standaard is de modus geactiveerd als het accuniveau onder de 30% komt.

De volgende productinstellingen worden toegepast als Bitdefender in het profiel Accumodus handelt:

- Bitdefender Automatische Update is uitgesteld.
- Geplande scans zijn uitgesteld.
- Beveiligingswidget is uitgeschakeld.

Bitdefender detecteert wanneer uw laptop overschakelt op accuvoeding en afhankelijk van het accuniveau gaat het dan automatisch over op de Accumodus. Op dezelfde manier verlaat Bitdefender automatisch de Accumodus, als de laptop niet langer op de accu werkt.

5.2.6. Real-Time Optimalisering

Bitdefender Real-Time Optimalisering is een plug-in die uw systeemprestaties geruisloos verbetert, op de achtergrond, en garandeert dat u niet wordt onderbroken terwijl u in een profielmodus bent. Afhankelijk van de CPU-belasting bewaakt de plug-in alle processen en richt zich op die processen die een hogere belasting aannemen om ze aan te passen aan uw behoeften.

Om Realtime-optimalisatie in of uit te schakelen:

1. Klik op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Selecteer het tabblad **PROFIELEN**.

3. 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.

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.

- "*Mijn systeem lijkt traag*" (p. 191)
- "*Het scannen start niet*" (p. 193)
- "*Ik kan een bepaalde toepassing niet meer gebruiken*" (p. 195)
- "*Wat moet u doen als Bitdefender een veilige website of online toepassing blokkeert*" (p. 196)
- "*Wat moet ik doen indien Bitdefender een veilige toepassing als ransomware beschouwt?*" (p. 197)
- "*Bitdefender updaten bij een langzame internetverbinding*" (p. 202)
- "*De Bitdefender-services reageren niet*" (p. 202)
- "*De antispamfilter werkt niet goed*" (p. 203)
- "*De Autofill-functie in mijn Portefeuille werkt niet*" (p. 208)
- "*Het verwijderen van Bitdefender is mislukt*" (p. 209)
- "*Mijn systeem start niet op na het installeren van Bitdefender*" (p. 210)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Hulp vragen*" (p. 329).

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"* (p. 83) voor meer informatie.

- **Er is niet voldaan aan de minimale systeemvereisten voor het uitvoeren van Bitdefender.**

  Als uw apparaat niet voldoet aan de minimale systeemvereisten, wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn. Zie "Minimale systeemvereisten" (p. 3) voor meer informatie.

- **U hebt toepassingen geïnstalleerd die u niet gebruikt**.

  Elke computer 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 bedreigingen. 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 bedreigingen die de veiligheid van uw systeem in gevaar brengen.

  De Systeemscan starten:

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

3. In het **ANTIVIRUS**-panel klikt u op **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 op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
    2. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
    3. Klik op **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 Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
    2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
    3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
    4. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    5. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
  - In **Windows 10**:
    1. Klik op **Start**, klik dan op Instellingen.
    2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
    3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
    4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
    5. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.

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

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.

- **Bitdefender is niet de enige beveiligingsoplossing die op uw systeem is geïnstalleerd**.

  In dit geval:

  1. Verwijder de andere beveiligingsoplossing. Zie *"Andere beveiligingsoplossingen verwijderen"* (p. 83) voor meer informatie.
  2. Bitdefender opnieuw installeren
     - In **Windows 7**:
       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
       b. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
       c. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       d. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8 en Windows 8.1**:
       a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
       b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
       c. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
       d. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       e. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:
  a. Klik op **Start**, klik dan op Instellingen.
  b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  c. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  e. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  f. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.

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.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

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 respectieve toepassing uitsluiten van de bewaking door Advanced Threat Defense.

Het programma aan de lijst Uitsluitingen toevoegen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **ADVANCED THREAT DEFENSE**-panel.
4. In het venster **WITTE LIJST** klikt u op **Toepassingen toevoegen aan de witte lijst**.
5. Zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

6.1.4. Wat moet u doen als Bitdefender een veilige website of online toepassing blokkeert

Bitdefender biedt een veilige websurfervaring door al het webverkeer te filteren en alle kwaadaardige content te blokkeren. Het is echter mogelijk dat Bitdefender een veilige website of online toepassing als onveilig beschouwd, wat tot gevolg heeft dat Bitdefender HTTP-verkeer zo scant dat het onterecht wordt geblokkeerd.

Als de zelfde pagina of toepassing herhaaldelijk geblokkeerd blijft, dan dan deze worden toegevoegd aan een witte lijst zodat hij niet wordt gescand door de engines van Bitdefender, waardoor een meer vloeiendere ervaring van websurfen wordt gegarandeerd.

Een website toevoegen aan de **Witte lijst**:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **WEBBESCHERMING**-panel klikt u op **Witte lijst**.

4. Geef het adres van de geblokkeerde website of online toepassing in het juiste veld in en klik op **Toevoegen**.
5. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Alleen websites en toepassingen die u volledig vertrouwt zouden moeten worden toegevoegd aan deze lijst. Ze worden uitgesloten van scannen door de volgende engines: bedreiging, phishing en fraude.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

6.1.5. Wat moet ik doen indien Bitdefender een veilige toepassing als ransomware beschouwt?

Ransomware is een kwaadaardig programma dat geld probeert te verdienen van gebruikers door hun kwestbare systemen af te sluiten. Om uw systeem veilig te houden tegen tegenslagen, geeft Bitdefender u de mogelijkheid om persoonlijke bestanden te beveiligen.

Wanneer een toepassing een van uw beschermde bestanden probeert te wijzigen of te verwijderen, zal dit als onveilig worden beschouwd en zal Bitdefender de functionaliteit ervan blokkeren.

Indien een dergelijke toepassing wordt toegevoegd aan de lijst van niet-vertrouwde toepassingen, en u zeker weet dat het veilig is om de toepassing te gebruiken, volgt u deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik in het venster **VEILIGE BESTANDEN** op **Toegang toepassing**.
4. De appsdie verzocht hebben om bestanden in uw beschermde mappen te wijzigen, worden hier vermeld. Klik op de Toestaan-schakelaar naast de toepassing waarvan u zeker bent dat ze veilig is.

6.1.6. Ik kan geen verbinding maken met het internet

Het is mogelijk dat een programma of een webbrowser, na het installeren van Bitdefender, geen verbinding meer kan maken met Internet of geen toegang meer krijgt tot de netwerkdiensten.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van de respectieve softwaretoepassing automatisch toe te staan.

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **FIREWALL**-panel.
4. Selecteer het tabblad **REGELS**.
5. Om een app-regel toe te voegen, klik op de koppeling **Regel toevoegen**.
6. Een nieuw venster verschijnt waarin u de details kunt toevoegen. Verzeker u ervan alle beschikbare netwerktypes te selecteren en in de sectie **Toestemming Toestaan** te selecteren.

Sluit Bitdefender, open de softwaretoepassing en probeert opnieuw een verbinding te maken met internet.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

6.1.7. Ik kan geen toegang krijgen tot een apparaat op mijn netwerk.

Afhankelijk van het netwerk waarmee u verbonden bent, kan de Bitdefender-firewall de verbinding tussen uw systeem en een ander apparaat (zoals een andere computer of printer) blokkeren. Hierdoor zult u mogelijk niet langer bestanden kunnen delen of afdrukken.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van het respectieve apparaat automatisch toe te staan. U doet dat als volgt:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. Klik op de icoon in de rechterbenedenhoek van het **FIREWALL**-panel.
4. Klik op de koppeling **Regel toevoegen** bovenaan in het venster **REGELS**.
5. In het venster **INSTELLINGEN** schakelt u de optie **Deze regel toepassen op alle toepassingen** in.

6. Klik op het tabblad **GEAVANCEERD**.
7. Tik in het vakje **Aangepast afstandsadres** het IP-adres in van de computer of de printer waar u onbeperkte toegang toe wenst.

Als u nog steeds geen verbinding kunt maken met het apparaat, wordt het probleem mogelijk niet veroorzaakt door Bitdefender.

Controleer op andere potentiële oorzaken, zoals hieronder:

- De firewall op de andere computer kan het delen van bestanden en printers met uw computer blokkeren.
  - Als de Windows Firewall wordt gebruikt, kan deze worden geconfigureerd om het delen van bestanden en printers als volgt toe te staan:
    - In **Windows 7**:
      1. Klik op **Start**, ga naar **Configuratiescherm** en selecteer **Systeem en Beveiliging**.
      2. Ga naar **Windows Firewall** en klik daarna op **Een programma toestaan via Windows Firewall**.
      3. Selecteer het vakje **Bestands- en printerdeling**.
    - 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 **Systeem en Beveiliging**, ga naar **Windows Firewall** en selecteer **Een app toegang geven via Windows Firewall**.
      3. Selecteer het vakje **Bestands- en printerdeling** en klik daarna op **OK**.
    - In **Windows 10**:
      1. Typ "Een app via Windows Firewall toestaan" in het zoekveld in de taakbalk en klik op het pictogram ervan.
      2. Klik op **Instellingen wijzigen**.
      3. In de lijst **Toegestane apps en functies** selecteert u het vakje **Delen van Bestand en Printer** en klikt u daarna op **OK**.
  - Als er een ander firewall-programma wordt gebruikt, moet u de documenten of het Help-bestand van dit programma raadplegen.

- Algemene omstandigheden die het gebruik van of verbinden met de gedeelde printer kunnen verhinderen:
  - U moet zich mogelijk aanmelden bij een Windows-beheerdersaccount om toegang te krijgen tot de gedeelde printer.
  - Er zijn machtigingen ingesteld voor de gedeelde printer om de toegang alleen toe te staan tot specifieke computers en gebruikers. Als u uw printer deelt, moet u de machtigingen controleren die voor de printer zijn ingesteld om te zien of de gebruiker op de andere computer toegang heeft tot de printer. Als u probeert een verbinding te maken met een gedeelde printer, moet u bij de gebruiker op de andere computer controleren of u de machtiging hebt om een verbinding te maken met de printer.
  - De printer die op uw computer of op de andere computer is aangesloten, wordt niet gedeeld.
  - De gedeelde printer is niet toegevoegd aan de computer.

  Opmerking
  Om te leren hoe u het delen van printers kunt beheren (een printer delen, machtigingen voor een printer instellen of verwijderen, verbinden met een netwerkprinter of met een gedeelde printer), gaat u naar Windows Help en ondersteuning (klik in het menu Start op **Help en ondersteuning**).

- De toegang tot de netwerkprinter is mogelijk beperkt tot specifieke computers of gebruikers. Raadpleeg de netwerkbeheerder om uit te vinden of u de machtiging hebt om een verbinding te maken met die printer.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

6.1.8. Mijn internetverbinding is langzaam

Deze situatie kan zich voordoen nadat u Bitdefender hebt geïnstalleerd. Het probleem kan zijn veroorzaakt door fouten in de Bitdefender-firewallconfiguratie.

Om deze problemen op te lossen:

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

3. In het panel **FIREWALL** klikt u op de schakelaar AAN/UIT om de functie uit te schakelen.
4. Controleer of uw internetverbinding verbetert wanneer de Bitdefender-firewall is uitgeschakeld.
   - Als u nog steeds een langzame internetverbinding kunt maken, wordt het probleem mogelijk niet veroorzaakt door Bitdefender. Neem contact op met uw internet-provider om te controleren of de verbinding werkt aan hun kant.

     Als u van uw internet-provider de bevestiging ontvangt dat de verbinding aan hun zijde werkt en het probleem zich blijft voordoen, neemt u contact op met Bitdefender zoals beschreven in sectie "*Hulp vragen*" (p. 329).
   - Als de internetverbinding is verbeterd na het uitschakelen van de Bitdefender-firewall:

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

     b. Klik op de koppeling **FUNCTIES BEKIJKEN**.

     c. Klik op de icoon in de rechterbenedenhoek van het **FIREWALL**-panel.

     d. Ga naar het tabblad **NETWERKADAPTERS** en stel uw internetverbinding in op **Thuis/Kantoor**.

     e. In het tabblad **GEAVANCEERDE INSTELLINGEN** klikt u op de schakelaar om **Poortscans in het netwerk blokkeren** uit te schakelen.

     In de ruimte **Stealth-modus** klikt u op **Stealth-verbindingen bewerken**. Schakel de Stealth-modus in voor de netwerkadapter waar u mee verbonden bent.

     f. Sluit Bitdefender, start het systeem opnieuw op en controleer de snelheid van de internetverbinding.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

6.1.9. 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 op het ⚙ pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op het tabblad **UPDATE**.
3. Selecteer naast **Update procesregels Herinneren voor het downloaden** in het vervolgkeuzemenu.
4. Ga terug naar het hoofdvenster en klik op de link **NU UPDATEN**.
5. Selecteer alleen **Updates handtekeningen** en klik vervolgens op **OK**.
6. Bitdefender downloadt en installeert enkel de informatie-database voor bedreigingen.

6.1.10. De Bitdefender-services reageren niet

Dit artikel helpt u bij het oplossen van de foutmelding **Bitdefender-services reageren niet**. U kunt deze fout aantreffen als volgt:

- Het Bitdefender-pictogram in het systeemvak wordt grijs weergegeven en u krijgt een melding dat de Bitdefender-services niet reageren.
- Het Bitdefender-venster geeft aan dat de Bitdefender-services niet reageren.

De fout kan worden veroorzaakt door een van de volgende omstandigheden:

- tijdelijke communicatiefouten tussen de Bitdefender-services.
- sommige Bitdefender-services zijn gestopt.
- andere beveiligingsoplossingen worden op hetzelfde ogenblik als Bitdefender uitgevoerd.

Probeer de volgende oplossingen om deze fouten op te lossen:

1. Wacht enkele ogenblikken en kijk of er iets verandert. De fout kan tijdelijk zijn.
2. Start de computer opnieuw op en wacht enkele ogenblikken tot Bitdefender is geladen. Open Bitdefender om te zien of de fout blijft bestaan. Het

probleem wordt doorgaans opgelost door de computer opnieuw op te starten.

3. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van Bitdefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens Bitdefender opnieuw te installeren.

   Zie "*Andere beveiligingsoplossingen verwijderen*" (p. 83) voor meer informatie.

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel "*Hulp vragen*" (p. 329).

6.1.11. De antispamfilter werkt niet goed

Dit artikel helpt u bij het oplossen van de volgende problemen met betrekking tot de werking van de antispamfilter van Bitdefender:

- Een aantal rechtmatige e-mailberichten wordt gemarkeerd als [spam]..
- Talrijke spamberichten worden niet als dusdanig gemarkeerd door de antispam-filter.
- De antispam-filter detecteert geen enkel spambericht.

Rechtmatige berichten worden gemarkeerd als [spam]

Rechtmatige berichten worden als [spam] gemarkeerd omdat ze eruit zien als spam voor de antispamfilter van Bitdefender. U kunt dit probleem oplossen door de antispamfilter op de goede manier te configureren.

Bitdefender voegt de ontvangers van uw e-mailberichten automatisch toe aan uw vriendenlijst. De e-mailberichten die zijn ontvangen van de contactpersonen in de vriendenlijst, worden beschouwd als rechtmatig. Ze worden niet gecontroleerd door de antispamfilter en worden daarom ook nooit gemarkeerd als [spam].

De automatische configuratie van de vriendenlijst verhindert niet dat er detectiefouten optreden in deze situaties:

- U ontvangt veel gevraagde commerciële e-mail omdat u zich op verschillende websites hebt geabonneerd. In dit geval bestaat de oplossing eruit de e-mailadressen waarvan u dergelijke e-mailberichten ontvangt, toe te voegen aan de vriendenlijst.

- Een belangrijk deel van uw rechtmatige e-mail komt van mensen naar wie u nog nooit een e-mail hebt gestuurd, zoals klanten, potentiële zakenpartners en anderen. In dit geval zijn andere oplossingen vereist.

  Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, worden de detectiefouten aangegeven.

Opmerking
Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg *"Ondersteunde e-mailclients en protocollen"* (p. 115) voor een complete lijst van ondersteunde e-mailclients.

Contactpersonen toevoegen aan de vriendenlijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van rechtmatige berichten gemakkelijk toevoegen aan de vriendenlijst. Volg deze stappen:

1. Selecteer in uw e-mailclient een e-mailbericht van de afzender die u wilt toevoegen aan de vriendenlijst.
2. Klik op de knop **Vriend toevoegen** in de antispam-werkbalk van Bitdefender.
3. U wordt gevraagd de adressen die aan de vriendenlijst zijn toegevoegd, te bevestigen. Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.

Als u een andere e-mailclient gebruikt, kunt u contactpersonen toevoegen aan de vriendenlijst vanaf de Bitdefender-interface. Volg deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTISPAM**-panel klikt u op **Vrienden beheren**.

   Er wordt een configuratievenster weergegeven.
4. Voer het e-mailadres in waarop u e-mailberichten wilt ontvangen en klik daarna op **Toevoegen**. U kunt zoveel e-mailadressen toevoegen als u wilt.
5. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet als [spam] aangemerkt moeten worden). Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer het rechtmatige bericht dat door Bitdefender verkeerdelijk is gemarkeerd als [spam].
4. Klik op de knop **Vriend toevoegen** in de antispam-werkbalk van Bitdefender om de afzender aan de vriendenlijst toe te voegen. U zult mogelijk op **OK** moeten klikken om te bevestigen. U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.
5. Klik op de knop **Geen spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Het e-mailbericht wordt verplaatst naar de map Postvak IN.

Veel spamberichten worden niet gedetecteerd

Als u veel spamberichten ontvangt die niet als [spam] zijn gemarkeerd, moet u de antispamfilter van Bitdefender configureren om de efficiëntie te verbeteren.

Probeer de volgende oplossingen:

1. Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, worden niet-gedetecteerde spamberichten aangegeven.

   ### Opmerking

   Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg *"Ondersteunde e-mailclients en protocollen"* (p. 115) voor een complete lijst van ondersteunde e-mailclients.

2. Spammers toevoegen aan de spammerslijst. De e-mailberichten die zijn ontvangen van adressen in de spammerslijst, worden automatisch gemarkeerd als [spam].

Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u gemakkelijk aanduiden welke e-mailberichten niet als spam moeten worden gedetecteerd. Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop **Is spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

Spammers toevoegen aan de spammerslijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van de spamberichten gemakkelijk toevoegen aan de spammerslijst. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer de berichten die door Bitdefender zijn gemarkeerd als [spam].
4. Klik op de knop **Spammer toevoegen** in de antispam-werkbalk van Bitdefender.
5. U wordt gevraagd de adressen die aan de spammerslijst zijn toegevoegd, te bevestigen. Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

Als u een andere e-mailclient gebruikt, kunt u spammers handmatig toevoegen aan de spammerslijst vanaf de Bitdefender-interface. Het is handig om dit alleen te doen wanneer u meerdere spamberichten hebt ontvangen van hetzelfde e-mailadres. Volg deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTISPAM**-panel klikt u op **Spammers beheren**.

   Er wordt een configuratievenster weergegeven.

4. Voer het e-mailadres van de scanner in en klik daarna op **Toevoegen**. U kunt zoveel e-mailadressen toevoegen als u wilt.
5. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

De antispamfilter detecteert geen enkel spambericht

Als er een spambericht als [spam] is gemarkeerd, kan er een probleem zijn met de antispamfilter van Bitdefender. Voordat u dit probleem probeert op te lossen, moet u controleren of het niet wordt veroorzaakt door een van de volgende omstandigheden:

- De antispambeveiliging wordt mogelijk uitgeschakeld. Om de status van de antispambescherming te controleren, klikt u op de -icoon in de linkerzijbalk van de Bitdefender-interface en selecteert u vervolgens de koppeling **FUNCTIES WEERGEVEN**. Klik op het tandrad in het paneel **ANTISPAM** en zoek daarna in het bovenste gedeelte van het venster om na te gaan of de functie geactiveerd is.

  Als Antispam is uitgeschakeld, is dit de oorzaak van uw probleem. Klik op de bijhorende schakelaar om uw Antispambescherming in te schakelen.
- De antispambeveiliging van Bitdefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol. Dit betekent het volgende:
  - E-mailberichten die zijn ontvangen via op het web gebaseerde e-mailservices (zoals Yahoo, Gmail, Hotmail of andere), worden op spam gefilterd door Bitdefender.
  - Als uw e-mailclient is geconfigureerd om e-mailberichten te ontvangen met een ander protocol dan POP3 (bijv. IMAP4), controleert de antispamfilter van Bitdefender deze berichten niet op spam.

  Opmerking

  POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver. Als u het protocol dat uw e-mailclient gebruikt om e-mailberichten te downloaden niet kent, kunt u dat vragen aan de persoon die uw e-mailclient heeft geconfigureerd.
- Bitdefender Total Security 2018 scant geen POP3-verkeer van Lotus Notes.

Een mogelijke oplossing is het repareren of opnieuw installeren van het product. Het is echter mogelijk dat u contact wilt opnemen met Bitdefender voor ondersteuning, zoals beschreven in sectie "*Hulp vragen*" (p. 329).

6.1.12. De Autofill-functie in mijn Portefeuille werkt niet

U hebt uw online gegevens opgeslagen in uw Bitdefender-Wachtwoordmanager en u hebt opgemerkt dat autofill niet werkt. Meestal doet dit probleem zich voor wanneer de Bitdefender-Portefeuille-extensie niet is geïnstalleerd in uw browser.

Om deze situatie op te lossen, volgt u deze stappen:

- In **Internet Explorer:**
  1. Open Internet Explorer.
  2. Klik op Extra.
  3. Klik op Invoegtoepassingen beheren.
  4. Klik op Werkbalken en Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.
- In **Mozilla Firefox:**
  1. Open Mozilla Firefox.
  2. Klik op Extra.
  3. Klik op Add-ons.
  4. Klik op Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.
- In **Google Chrome:**
  1. Open Google Chrome.
  2. Ga naar het Menu-pictogram.
  3. Klik op Extra.
  4. Klik op Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.

Opmerking
De add-on zal worden ingeschakeld nadat u uw webbrowser opnieuw hebt opgestart.

Controleer nu of de autofill-functie in Portefeuille werkt voor uw online accounts.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

6.1.13. Het verwijderen van Bitdefender is mislukt

Indien u uw Bitdefender-product wilt verwijderen en u merkt dat het proces blijft hangen of het systeem bevriest, klik dan op **Annuleren** om de handeling af te breken. Start het systeem opnieuw op als dit niet werkt.

Als het verwijderen mislukt, kunnen er enkele registersleutels en bestanden van Bitdefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van Bitdefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden.

Om Bitdefender helemaal van uw systeem te verwijderen:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
  4. Klik op **VERWIJDEREN** in het venster dat verschijnt.

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

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
3. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **VERWIJDEREN** in het venster dat verschijnt.
6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

6.1.14. 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"* (p. 84).
  2. Bitdefender verwijderen van uw systeem:

     - In **Windows 7**:

       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.

b. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.

c. Klik op **VERWIJDEREN** in het venster dat verschijnt.

d. Wacht tot het verwijderen 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 Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.

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

c. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.

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

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

f. Start uw systeem opnieuw op in normale modus.

- In **Windows 10**:

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

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

c. **Bitdefender Total Security 2018** vinden en **De-installeren** selecteren.

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

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

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

g. Start uw systeem opnieuw op in normale modus.

3. Uw Bitdefender reïnstalleren.

- **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**

Om dit probleem op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 84).
2. Verwijder de andere beveiligingsoplossing van uw systeem:
   - In **Windows 7**:
     a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
     b. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
     c. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
   - In **Windows 8 en Windows 8.1**:
     a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
     b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
     c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
     d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
   - In **Windows 10**:
     a. Klik op **Start**, klik dan op Instellingen.
     b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
     c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
     d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

   Om andere software correct te verwijderen, gaat u naar de betreffende website en voert u het hulpprogramma voor het verwijderen uit of neemt u contact op met ons voor de richtlijnen voor het verwijderen.

3. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

U hebt de bovenstaande stappen al gevolgd en de situatie is niet opgelost.

Om dit probleem op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 84).
2. Gebruik de optie Systeemherstel van Windows om de computer te herstellen naar een eerdere datum voordat u het product Bitdefender installeert.
3. Start het systeem opnieuw op in de normale modus en neem contact op met onze experts voor hulp, zoals beschreven in deel "*Hulp vragen*" (p. 329).

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.

- "*Bitdefender Reddingsmodus (Reddingsomgeving in Windows 10)*" (p. 214)
- "*Wat moet er gebeuren wanneer Bitdefender bedreigingen op uw computer vindt?*" (p. 218)
- "*Een bedreiging in een archief opruimen*" (p. 219)
- "*Een bedreiging in een e-mailarchief opruimen*" (p. 220)
- "*Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?*" (p. 221)
- "*Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?*" (p. 222)
- "*Wat zijn de overgeslagen items in het scanlogboek?*" (p. 222)
- "*Wat zijn de overgecomprimeerde bestanden in het scanlogboek?*" (p. 223)

- *"Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?"* (p. 223)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk *"Hulp vragen"* (p. 329).

6.2.1. Bitdefender Reddingsmodus (Reddingsomgeving in Windows 10)

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

Zodra Bitdefender Total Security 2018 geïnstalleerd is op **Windows 7, Window 8 en Windows 8.1** en het Bitdefender Rescue Mode Image-bestand gedownload is, kan Rescue Mode gebruikt worden, zelfs als u niet langer in Windows kunt opstarten.

In Windows 10, is de Bitdefender Rescue-omgeving geïntegreerd met Windows RE. Dit betekent dat er geen Rescue Mode-beeld moet gedownload worden op dit besturingssysteem en de functie kan niet gebruikt worden als er opstartproblemen zijn. Om het systeem op te schonen voordat er Windows-diensten worden geladen, bevelen we aan om de Bitdefender Rescue-cd te gebruiken.

Bitdefender Rescue-cd is een gratis tool die uw computer scant en opschoont wanneer u vermoedt dat een bedreiging de werking ervan aantast. Nuttige artikelen met informatie over hoe u deze moet creëren en gebruiken, vindt u op het Bitdefender-ondersteuningplatform op https://www.bitdefender.com/support/consumer.html.

Het Bitdefender Rescue Mode-beeld downloaden

Om Rescue Mode te kunnen gebruiken in **Windows 7, Windows 8 en Windows 8.1** moet u eerst het afbeeldingsbestand downloaden als volgt:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **Rescue Mode**.

4. Klik op **JA** in het bevestigingsvenster dat verschijnt om uw computer opnieuw op te starten

   Wacht tot het Bitdefender Rescue Mode Image-bestand werd gedownload van de Bitdefender-servers. Zodra het downloadproces beëindigd is, zal de computer opnieuw opstarten.

   Er verschijnt een menu waarin u wordt gevraagd een besturingssysteem te selecteren. Bij deze stap kunt u ervoor kiezen uw systeem op te starten in Rescue-modus of in normale modus.

Opmerking
Wegens de integratie met Windows Recovery Environment in **Windows 10** moet er op dit besturingssysteem geen Rescue Mode-beeld gedownload worden.

Uw systeem opstarten in Rescue Mode in Windows 7, Windows 8 en Windows 8.1.

U kunt de Helpmodus op één of twee manieren openen:

Vanuit de Bitdefender-interface

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **Rescue Mode**.
4. Klik op **JA** in het bevestigingsvenster dat verschijnt om uw computer opnieuw op te starten
5. Nadat de computer opnieuw is opgestart, verschijnt een menu waarin u wordt gevraagd een besturingssysteem te selecteren. Kies **Bitdefender Helpmodus** om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
6. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt. Druk vervolgens opnieuw op **Enter**.

   Bitdefender-Helpmodus wordt binnen enkele ogenblikken geladen.

Start uw computer direct op in de Helpmodus

Als Windows niet langer start, kunt u met de onderstaande stappen uw computer direct opstarten in de Helpmodus van Bitdefender:

- In **Windows 7**:
  1. Druk op de **F8**-toets tot het scherm **Geavanceerde opstartopties** verschijnt.
  2. Gebruik de pijltoetsen om Bitdefender Rescue Mode te selecteren en druk daarna op **Enter**.

     Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.
- In **Windows 8 en Windows 8.1**:
  1. Druk op de **Shift**-toets tot het scherm **Geavanceerde opstartopties** verschijnt.
  2. Selecteer de optie **Een ander besturingssysteem kiezen** en daarna Bitdefender Rescue Mode.

     Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.

Opmerking

Het is enkel mogelijk uw computer in Rescue-modus te starten indien er een Rescue Mode Image-bestand vooraf werd gedownload zoals beschreven in "Het Bitdefender Rescue Mode-beeld downloaden" (p. 214).

Uw systeem opstarten in Rescue Environment van Windows 10

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

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. Klik op de koppeling **FUNCTIES BEKIJKEN**.
3. In het **ANTIVIRUS**-panel klikt u op **Rescue Environment**.
4. Klik op **Herstarten** in het venster dat verschijnt.

   Bitdefender-Rescue Environment wordt binnen enkele ogenblikken geladen.

Uw systeem scannen in Rescue-modus (Rescue Environment in Windows 10)

Om uw systeem te scannen in Rescue-modus (Rescue Environment):

- In **Windows 7, Windows 8 en Windows 8.1**:
  1. Open de Helpmodus zoals beschreven in "Uw systeem opstarten in Rescue Mode in Windows 7, Windows 8 en Windows 8.1." (p. 215).
  2. Het Bitdefender-logo verschijnt en het kopiëren van de beveiligingsoplossing-engines wordt gestart.
  3. Een welkomstvenster wordt weergegeven. Klik op **Doorgaan**.
  4. Een update van de informatie-database voor bedreigingen werd opgestart.
  5. Nadat de update is voltooid, verschijnt het venster van de antivirusscanner van Bitdefender voor scannen op aanvraag.
  6. Klik op **Nu scannen**, selecteer het scandoel in het venster dat verschijnt en klik daarna op **Openen** om het scannen te starten.

     Het is aanbevolen de volledige Windows-partitie te scannen.

     Opmerking
     Wanneer u in de Helpmodus werkt, krijgt u te maken met partitienamen van het Linux-type. Schijfpartities zullen verschijnen als sda1 die waarschijnlijk overeenstemmen met het station (C:) Partitie van het Windows-type, sda2 overeenkomend met (D:) enz.

  7. Wacht tot de scan is voltooid. Volg de instructies om een gedetecteerde bedreiging te verwijderen.
  8. Om de Helpmodus af te sluiten, klikt u met de rechtermuisknop in een leeg gebied op het bureaublad. Selecteer vervolgens **Verlaten** in het menu dat verschijnt en kies vervolgens of u de computer opnieuw wilt opstarten of uitschakelen.
- In **Windows 10**:
  1. Ga naar de Rescue Environment, zoals beschreven in "Uw systeem opstarten in Rescue Environment van Windows 10" (p. 216).
  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 er gebeuren wanneer Bitdefender bedreigingen op uw computer vindt?

U kunt op een van de volgende manieren te weten komen dat er een bedreiging aanwezig is op uw computer:

- U hebt uw computer gescand en Bitdefender heeft geïnfecteerde items gevonden.
- Een bedreigingswaarschuwing laat u weten dat Bitdefender een of meerdere bedreigingen op uw computer 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-antivirusbeveiliging van Bitdefender uit.
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Klik op de koppeling **FUNCTIES BEKIJKEN**.
   c. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
   d. Klik in het venster **SCHILD** op de schakelaar AAN/UIT.

2. Verborgen objecten weergeven in Windows. Om te weten hoe u dit kunt doen, ga naar "*Verborgen objecten weergeven in Windows*" (p. 82).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real time antivirusbeveiliging van Bitdefender in.

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

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 84).
2. Verborgen objecten weergeven in Windows. Om te weten hoe u dit kunt doen, ga naar "*Verborgen objecten weergeven in Windows*" (p. 82).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Start uw systeem opnieuw op en ga naar de normale modus.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

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-antivirusbeveiliging van Bitdefender uit.
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Klik op de koppeling **FUNCTIES BEKIJKEN**.
   c. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
   d. Klik in het venster **SCHILD** op de schakelaar AAN/UIT.
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 de sectie "*Hulp vragen*" (p. 329).

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-antivirusbeveiliging van Bitdefender uit.
   a. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
   b. Klik op de koppeling **FUNCTIES BEKIJKEN**.
   c. Klik op de icoon in de rechterbenedenhoek van het **ANTIVIRUS**-paneel.
   d. Klik in het venster **SCHILD** op de schakelaar AAN/UIT.
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 antivirusbeveiliging van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 329).

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 "*Hoe kan ik mijn systeem scannen?*" (p. 60).
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*" (p. 329).

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 computer beschermd te houden. Als u die bestanden wilt scannen met Bitdefender, moet u contact opnemen met de productfabrikant voor meer informatie over die bestanden.

Wij raden u aan deze bestanden te negeren omdat ze geen bedreiging vormen voor uw systeem.

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 systeemgeheugen 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 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.

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.

ANTIVIRUS VOOR MAC

7. INSTALLEREN EN VERWIJDEREN

Dit hoofdstuk bevat de volgende onderwerpen:

- "*Systeemvereisten*" (p. 225)
- "*Bitdefender Antivirus for Mac installeren*" (p. 225)
- "*Bitdefender Antivirus for Mac verwijderen*" (p. 230)

7.1. Systeemvereisten

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

Uw Mac moet bovendien aan deze bijkomende vereisten voldoen:

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

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

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

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

7.2. Bitdefender Antivirus for Mac installeren

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

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

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

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

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

7.2.1. Installatieprocedure

Zo installeert u Bitdefender Antivirus for Mac:

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

Stap 1 - Welkomstvenster

Welkomstvenster

Klik op **Doorgaan**.

Stap 2 - Abonnementsovereenkomst lezen

Lees de Abonnementsovereenkomst

Voordat u verdergaan met de installatie, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Antivirus for Mac.

Klik op **Doorgaan** en vervolgens op **Akkoord**.

Belangrijk

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

Stap 3 - Installatie starten

Installatie starten

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

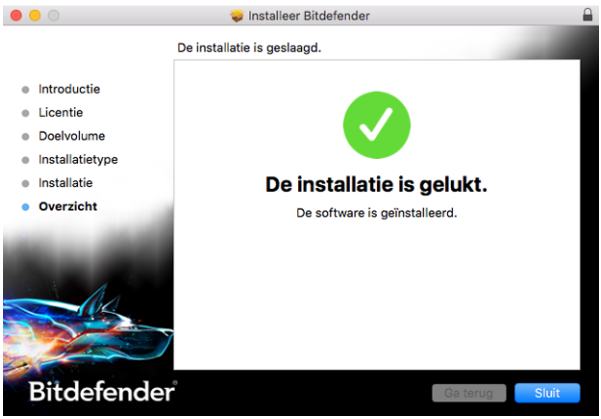
Klik op **Installeren** om de installatie te starten.

Stap 4 - Bitdefender Antivirus for Mac installeren

Bitdefender Antivirus for Mac installeren

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

Stap 5 - Voltooien



Voltooien

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

De installatieprocedure is nu voltooid.

Belangrijk

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

Wanneer u Bitdefender Antivirus for Mac voor het eerst installeert, verschijnen de wizards Veilige bestanden en Time Machine Protection. Zie "*Veilige bestanden*" (p. 249) eb "*Bescherming Time Machine*" (p. 237) voor meer informatie.

U krijgt een inleiding in de VPN-functie. Klik op **Volgende** om door te gaan. Zie "*VPN*" (p. 274) voor meer informatie.

7.3. Bitdefender Antivirus for Mac verwijderen

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

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster en ga naar de map Programma's.
2. Open de Bitdefender-map en dubbelklik op BitdefenderUninstaller.
3. Klik op **Verwijderen** en wacht tot de verwijdering is uitgevoerd.
4. Klik op **Sluiten**.

Belangrijk

Als er problemen optreden, kunt u contact opnemen met Bitdefender Klantenondersteuning volgens de aanwijzingen in "*Hulp vragen*" (p. 329).

8. AAN DE SLAG

Dit hoofdstuk bevat de volgende onderwerpen:

- "*Over Bitdefender Antivirus for Mac*" (p. 231)
- "*Bitdefender Antivirus for Mac starten*" (p. 231)
- "*Hoofdvenster Toepassing*" (p. 232)
- "*Dock-symbool toepassing*" (p. 233)

8.1. Over Bitdefender Antivirus for Mac

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

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

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

8.2. Bitdefender Antivirus for Mac starten

U kunt Bitdefender Antivirus for Mac op verschillende manieren starten:

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

8.3. Hoofdvenster Toepassing

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

Hoofdvenster Toepassing

De functie **Autopiloot**, rechtsboven in het hoofdvenster, bewaakt voortdurend alle programma's die op de computer actief zijn, zoekt naar activiteiten die op bedreigingen kunnen wijzen en verhindert dat nieuwe bedreigingen tot uw systeem kunnen doordringen.

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

De statusbalk boven in het venster geeft informatie over de beveiligingsstatus van het systeem in de vorm van tekstberichten met een kleurcodering. Als er geen waarschuwingen van Bitdefender Antivirus for Mac zijn, is de statusbalk groen. Als er een veiligheidsprobleem is gedetecteerd, wordt de statusbalk in de kleur geel weergegeven. Klik op de knop **Problemen weergeven** om te zien welke problemen de beveiliging van uw systeem in gevaar brengen. Zie "*Problemen oplossen*" (p. 239) voor meer informatie over mogelijke problemen en hun oplossingen.

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

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

Zie "*Uw Mac scannen*" (p. 236) voor meer informatie.

Onder de scanknoppen zijn de volgende opties beschikbaar:

- **Webbeveiliging** - filtert al het webverkeer en blokkeert schadelijke content, zodat u veilig op het web kunt surfen. Zie "*Webbeveiliging*" (p. 241) voor meer informatie.
- **Ga naar Bitdefender-account** - klik rechtsonder in het hoofdvenster op de koppeling **Ga naar uw account** om uw Bitdefender-account te openen. Zie "*Bitdefender Central*" (p. 258) voor meer informatie.
- **Aantal resterende dagen** - hier ziet u hoe lang het nog duurt voordat uw abonnement verloopt. Als de einddatum niet meer veraf is, kunt u op de koppeling klikken om een webpagina te openen voor het verlengen van uw abonnement.
- **Kopen** - hiermee gaat u naar de Bitdefender-website, waar u aanbiedingen kunt bekijken of een abonnement kunt nemen.
- **Feedback** - opent een nieuw berichtvenster in uw standaard e-mailclient, zodat u ons een e-mail kunt sturen.

8.4. Dock-symbool toepassing

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

Dock-symbool

9. BESCHERMING TEGEN SCHADELIJKE SOFTWARE

Dit hoofdstuk bevat de volgende onderwerpen:

- "*Aanbevelingen*" (p. 235)
- "*Uw Mac scannen*" (p. 236)
- "*Autopilot in- of uitschakelen*" (p. 237)
- "*Bescherming Time Machine*" (p. 237)
- "*Scanwizard*" (p. 239)
- "*Problemen oplossen*" (p. 239)
- "*Webbeveiliging*" (p. 241)
- "*Updates*" (p. 242)

9.1. Aanbevelingen

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

- Zorg dat **Autopilot** altijd ingeschakeld is, zodat de systeembestanden automatisch door Bitdefender Antivirus for Mac worden gescand.
- Zorg dat uw Bitdefender Antivirus for Mac-product altijd over de nieuwste bedreigingsinformatie en productupdates beschikt, door **Autopiloot** ingeschakeld te laten.
- Controleer regelmatig of er problemen worden gemeld door Bitdefender Antivirus for Mac, en los deze problemen op. Zie "*Problemen oplossen*" (p. 239) voor meer informatie.
- Check the detailed log of events concerning the Bitdefender Antivirus for Mac activity on your computer. Telkens er iets gebeurt dat van belang is voor de beveiliging van uw systeem of data, wordt een nieuw bericht toegevoegd aan de Bitdefender-geschiedenis. Zie "*Geschiedenis*" (p. 251) voor meer informatie.
- Volg ook de volgende adviezen op:

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

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

Verder hoeft u niets te doen of in te stellen. Als u dit wilt, kunt u de instellingen en voorkeuren van het programma aan uw wensen aanpassen. Zie "*Voorkeuren instellen*" (p. 245) voor meer informatie.

9.2. Uw Mac scannen

De functie **Autopiloot** bewaakt voortdurend alle toepassingen die op uw computer worden uitgevoerd, zoekt naar gebeurtenissen die op bedreigingen wijzen en verhindert dat nieuwe bedreigingen uw systeem kunnen binnendringen, maar u kunt daarnaast ook op elk gewenst moment uw Mac of specifieke bestanden scannen.

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

U kunt een scan ook op deze manier starten:

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

Opmerking

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

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

9.3. Autopilot in- of uitschakelen

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

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

Waarschuwing

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

9.4. Bescherming Time Machine

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

De wizard Time Machine Protection

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

De wizard Time Machine Protection

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

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

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

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

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

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

Zo activeert u Bitdefender Time Machine Protection voor uw backups:

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

   Er wordt een bevestigingsvenster weergegeven.

2. Klik op **Sluiten**.

Time Machine Protection in- of uitschakelen

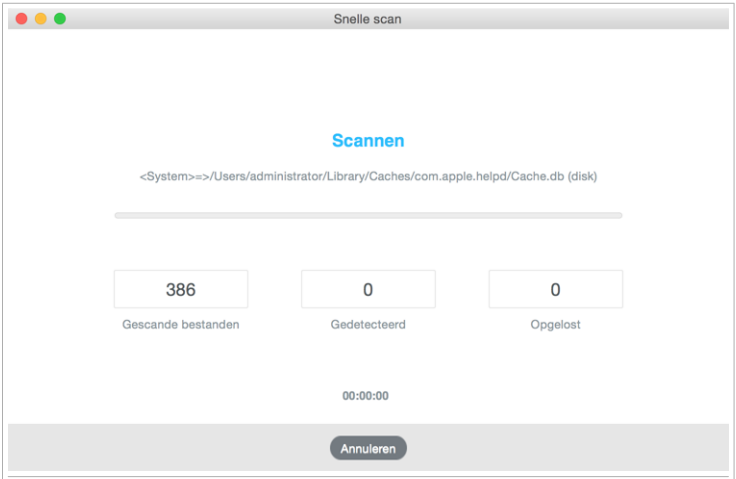
Zo schakelt u Time Machine Protection in of uit:

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

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

9.5. Scanwizard

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



Scan wordt uitgevoerd

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

Wacht tot Bitdefender Antivirus for Mac klaar is met scannen.

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

9.6. Problemen oplossen

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

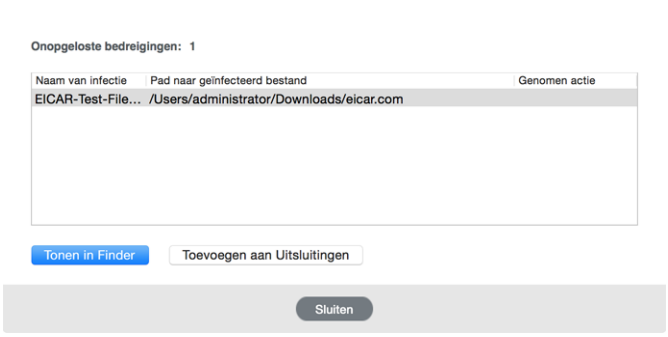
Als u de problemen oplost die door Bitdefender Antivirus for Mac worden gemeld, weet u zeker dat uw systeem en uw gegevens altijd veilig zijn.

Onder andere deze problemen kunnen worden gemeld:

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

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

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



Het venster Niet-opgeloste dreigingen

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

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

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

- Toevoegen aan uitsluitingen. Deze actie is niet beschikbaar voor bedreigingen die worden aangetroffen binnen archieven.

9.7. Webbeveiliging

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

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

TrafficLight-extensies inschakelen

Zo schakelt u de TrafficLight-extensies in:

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

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

Extensie-instellingen beheren

Er zijn meerdere geavanceerde functies beschikbaar om u tegen allerlei soorten dreigingen te beschermen tijdens het surfen op het web. Om deze functies te gebruiken: klik op het icoon TrafficLight naast de instellingen van uw browser en dan op **Instellingen**:

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

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

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

- **Witte lijst**

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

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

Paginabeoordelingen en waarschuwingen

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

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

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

9.8. Updates

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

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

De updates van de bedreigingsinformatie gebeuren 'on the fly', wat betekent dat de bestanden die moeten worden bijgewerkt, geleidelijk worden

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

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

9.8.1. Zelf een update uitvoeren

U kunt altijd handmatig een update uitvoeren.

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

Zo voert u handmatig een update uit:

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

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

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

9.8.2. Updates downloaden via een proxyserver

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

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

9.8.3. Productupdates

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

Het is mogelijk dat u voor deze updates het systeem opnieuw moet opstarten om de installatie van nieuwe bestanden te activeren. Als het voor een productupdate noodzakelijk is het systeem opnieuw op te starten, blijft Bitdefender Antivirus for Mac de oude bestanden gebruiken zolang u de computer nog niet opnieuw hebt opgestart. U kunt dan gewoon doorwerken tijdens het updateproces.

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

9.8.4. Informatie over Bitdefender Antivirus for Mac vinden

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

Om naar het venster Over te gaan:

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

10. VOORKEUREN INSTELLEN

Dit hoofdstuk bevat de volgende onderwerpen:

- "*Voorkeuren weergeven*" (p. 245)
- "*Accountinfo*" (p. 245)
- "*Beschermingsvoorkeuren*" (p. 246)
- "*Uitsluitingen*" (p. 248)
- "*Veilige bestanden*" (p. 249)
- "*Geschiedenis*" (p. 251)
- "*Quarantaine*" (p. 252)

10.1. Voorkeuren weergeven

Zo opent u het voorkeurenvenster van Bitdefender Antivirus for Mac:

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

10.2. Accountinfo

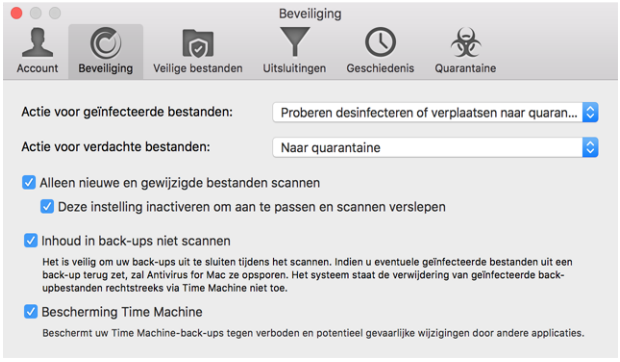
Het venster Accountinfo toont informatie over uw abonnement en uw Bitdefender-account.

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

Vanuit dit venster kunt u ook de optie **Mijn Aanbiedingen** (de)selecteren. Door de optie te selecteren, krijgt u notificaties telkens Bitdefender een speciaal aanbod heeft voor u.

10.3. Beschermingsvoorkeuren

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



Beschermingsvoorkeuren

- **Actie voor geïnfecteerde objecten.** Wanneer een bedreiging wordt gedetecteerd, zal Bitdefender Antivirus for Mac 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 in quarantaine geplaatst om verdere besmetting te voorkomen.

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

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

- **Actie voor verdachte objecten.** Soms worden bestanden door de heuristische analyse aangemerkt als 'verdacht'. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat hiervoor geen standaard desinfectieroutine bestaat.

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

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

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

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

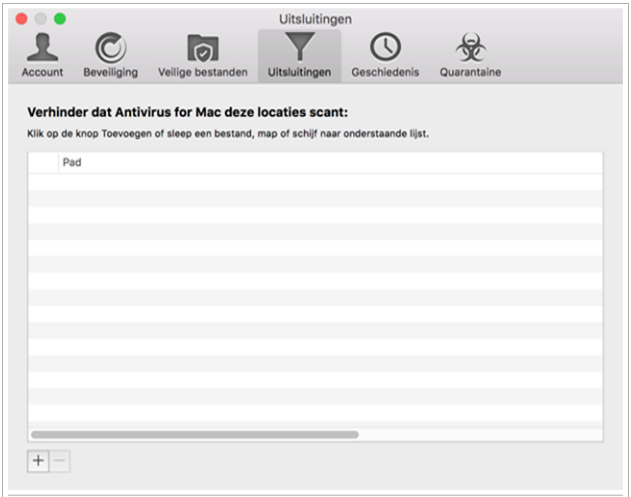
- **Inhoud in back-ups niet scannen.** Selecteer dit aankruisvak als u niet wilt dat backup-bestanden worden gescand. Als een geïnfecteerd backup-bestand later wordt teruggezet, wordt dit automatisch door Bitdefender Antivirus for Mac gedetecteerd en zal de juiste actie worden ondernomen.

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

10.3.1. Uitsluitingen

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

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



Uitsluitingen

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

U kunt een uitsluiting op twee manieren instellen:

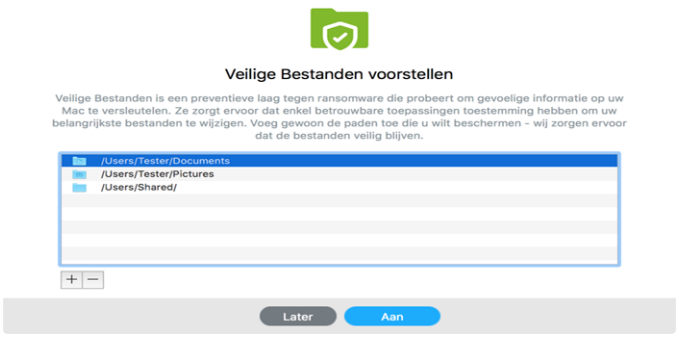
- Sleep een bestand, map of volume naar de lijst Uitsluitingen.
- Klik onder de lijst Uitsluitingen op de knop met het plusteken (+). Selecteer vervolgens het bestand, de map of het volume dat u van het scannen wilt uitsluiten.

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

10.4. Veilige bestanden

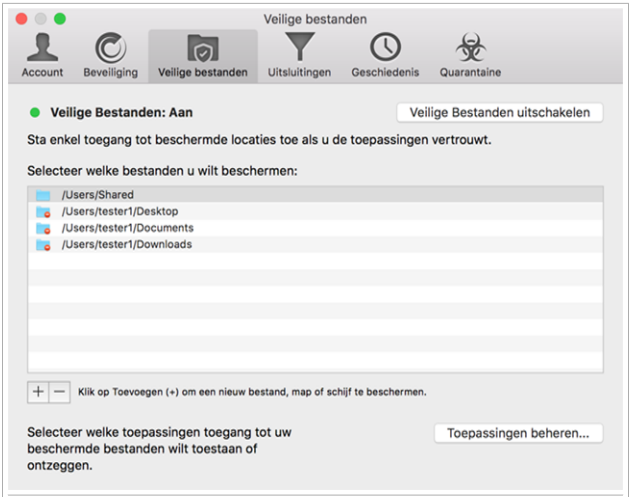
Ransomoware is een schadelijke software die kwestbare systemen aanvalt door ze te vergrendelen en later om geld te vragen zodat de gebruiker terug de controle over zijn systeem te krijgen. Deze schadelijke software handelt op een intelligente manier door valse berichten weer te geven zodat de gebruiker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

Gebruik makend van de recentste technologie garandeert Bitdefender systeemintegriteit door kritieke systeemgebieden te beschermen tegen ransomwareaanvallen zonder het systeem te belasten. Mogelijks wilt u echter ook uw persoonlijke bestanden beschermen, zoals documenten, foto's of films tegen ongeoorloofde toegang door onbetrouwbare apps. Met Bitdefender Veilige bestanden kunt u persoonlijke bestanden op een veilige plek bewaren en zelf configureren welke apps toestemming mogen krijgen om wijzigingen aan te brengen in de beschermde bestanden en welke niet.



Wizard Veilige bestanden

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



Veilige bestanden

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

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

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

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

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

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

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

10.4.1. Toepassingen beheren

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

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

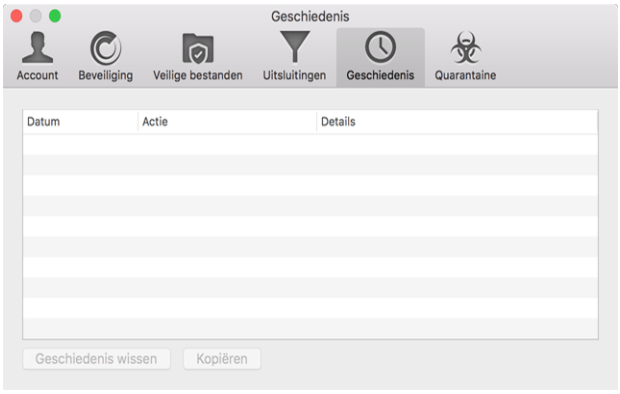
Gebruik de versleepmethode of klik op het +-teken (+) om meer apps aan de lijst toe te voegen.

10.5. Geschiedenis

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

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

Er worden gegevens over de activiteiten van het product weergegeven.



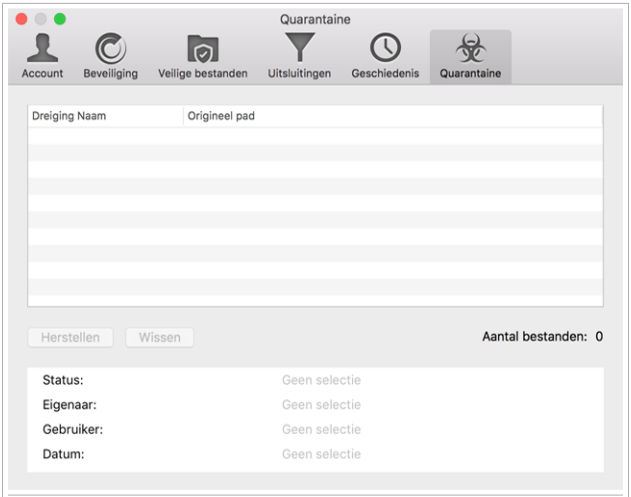
Geschiedenis

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

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

10.6. Quarantaine

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



Bestanden in quarantaine

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

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

11. VPN

Dit hoofdstuk bevat de volgende onderwerpen:

- "*Over VPN*" (p. 254)
- "*VPN Installeren*" (p. 254)
- "*VPN Openen*" (p. 255)
- "VPN-interface" (p. 255)
- "*Abonnementen*" (p. 275)

11.1. Over VPN

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

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

Opmerking

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

11.2. VPN Installeren

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

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

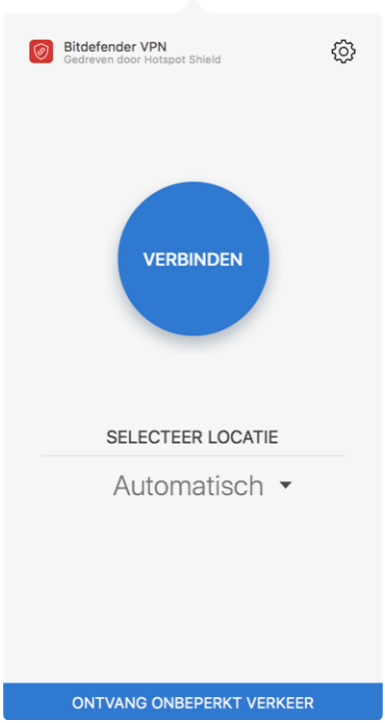
11.3. VPN Openen

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

11.4. 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, door de locatie te selecteren in de lijst **LOCATIE SELECTEREN**. Voor meer info over VPN-abonnementen, raadpleeg "*Abonnementen*" (p. 275).

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



VPN-interface

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

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

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

11.5. Abonnementen

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

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

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

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

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

12. BITDEFENDER CENTRAL

Dit hoofdstuk bevat de volgende onderwerpen:

- "*Over Bitdefender Central*" (p. 258)
- "*Mijn abonnementen*" (p. 259)
- "*Mijn apparaten*" (p. 260)

12.1. Over Bitdefender Central

Bitdefender Central is het webplatform waar u toegang hebt tot de online functies en diensten van het product en waar u van op afstand belantrijke taken kunt uitvoeren op toestellen waar Bitdefender op geïnstalleerd is. kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar https://central.bitdefender.com te gaan. Zodra u toegang hebt, kunt u beginnen met het volgende:

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

12.2. Naar Bitdefender Central gaan

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

- Vanuit het hoofdvenster van Bitdefender Antivirus for Mac:

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

- Vanuit uw webbrowser:
  1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
  2. Ga naar https://central.bitdefender.com.
  3. Log in op uw account met uw e-mailadres en wachtwoord.

12.3. Mijn abonnementen

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

12.3.1. Abonnement activeren

Een abonnement kan geactiveerd worden tijdens het installatieproces als u uw Bitdefender-account gebruikt. De geldigheidsduur van het abonnement begint te lopen vanaf het moment van activering.

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

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

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

Het abonnement is nu geactiveerd.

Zie "*Bitdefender Antivirus for Mac installeren*" (p. 225) voor informatie over het installeren van het product op uw apparaten.

12.3.2. Abonnement kopen

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

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

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

12.4. Mijn apparaten

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

12.4.1. Uw apparaten aanpassen

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

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

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

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

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

12.4.2. Beheer op afstand

Bitdefender van op afstand op een apparaat updaten:

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

Om de functie Autopiloot vanop afstand in te schakelen:

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

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

- **Bedieningspaneel**. In dit venster vindt u gegevens over het geselecteerde apparaat, kunt u de beveiligingsstatus nakijken en kunt u nagaan hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus kan groen zijn (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Klik voor meer informatie op het uitklappijltje in het bovenste statusgebied indien uw apparaat problemen ondervindt. Van

hieruit kunt u problemen manueel oplossen die de veiligheid van uw toestellen aantasten.

- **Bescherming**. In dit tabblad kunt u op afstand een Snelle scan of een Volledige scan uitvoeren op uw apparaten. Klik op de **SCAN**-knop om het proces te starten. U kunt ook nagaan wanneer de laatste scan werd uitgevoerd op het toestel en van de laatste scan met de belangrijkste informatie is er een verslag beschikbaar. Zie "*Uw Mac scannen*" (p. 236) voor meer informatie over deze twee scanprocessen.

13. VEELGESTELDE VRAGEN

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

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

1. Volg de onderstaande stappen om een Bitdefender-account aan te maken:
   - Ga naar https://central.bitdefender.com.
   - Voer de gevraagde informatie in en klik op de knop **Account aanmaken**.

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

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

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

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

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

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

1. Ga naar Bitdefender Central.
2. Klik linksboven in het venster op het symbool ≡ en selecteer vervolgens het paneel **Mijn abonnementen**.
3. Klik op de knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **Activeren** om door te gaan.

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

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

De niet-opgeloste problemen kunnen betrekking hebben op:

- Archieven met beperkte toegang (bijvoorbeeld xar of rar)

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

- Postbussen met beperkte toegang (bijvoorbeeld Thunderbird)

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

- Inhoud in backups

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

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

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

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

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

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

   Er worden gegevens over de activiteiten van het product weergegeven.

Kan ik Bitdefender Antivirus for Mac bijwerken via een proxyserver?

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

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

Hoe kan ik Bitdefender Antivirus for Mac verwijderen?

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster en ga naar de map Programma's.
2. Open de Bitdefender-map en dubbelklik op BitdefenderUninstaller.
3. Klik op **Verwijderen** en wacht tot de verwijdering is uitgevoerd.
4. Klik op **Sluiten**.

Belangrijk

Als er problemen optreden, kunt u contact opnemen met Bitdefender Klantenondersteuning volgens de aanwijzingen in *"Hulp vragen"* (p. 329).

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

- Zo verwijdert u de TrafficLight-extensies uit Mozilla Firefox:
  1. Open Mozilla Firefox.
  2. Ga naar **Extra** en selecteer **Add-ons**.
  3. Selecteer **Extensies** in de linkerkolom.

4. Selecteer de extensie en klik op **Verwijderen**.
5. Start de browser opnieuw om de verwijdering te voltooien.

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

Wanneer moet ik Bitdefender VPN gebruiken?

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

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

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

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met

onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

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

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

MOBILE SECURITY VOOR IOS

14. WAT IS BITDEFENDER MOBILE SECURITY FOR IOS

Online activiteiten zoals facturen betalen, vakanties boeken of goederen en diensten kopen zijn eenvoudig en zonder gedoe. Maar naarmate zoveel activiteiten op het internet geëvolueerd zijn, zijn er grote risico's aan verbonden en als beveiligingsgegevens genegeerd worden, kunnen persoonsgegevens gehackt worden. En wat is er belangrijker dan de bescherming van uw gegevens in online accounts en op uw persoonlijke smartphone?

Dankzij Bitdefender Mobile Security for iOS kunt u:

- Bescherm uw data wanneer u onbeveiligde draadloze netwerken gebruikt.
- Controleren of er lekken zijn ontstaan in de online rekeningen die u dagelijks gebruikt.
- Uw apparaat opsporen als u het kwijt bent of als het gestolen werd, vergrendelen en de data erop verwijderen.

Bitdefender Mobile Security for iOS wordt gratis geleverd en moet geactiveerd worden met een Bitdefender-account.

15. AAN DE SLAG

Apparaatvereisten

Bitdefender Mobile Security for iOS werkt op iPhones met iOS 10 en hoger en vereist een actieve internetverbinding om geactiveerd te worden en om na te gaan of er datalekken zijn op uw online accounts.

Bitdefender Mobile Security for iOS installeren

- **Vanuit Bitdefender Central**
  - Op iOS
    1. Ga naar https://central.bitdefender.com.
    2. Log in op uw Bitdefender-account.
    3. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **Mijn apparaten**.
    4. Tik op **LOKALE BESCHERMING INSTALLEREN**.
    5. Selecteer Bitdefender Mobile Security in de lijst en tik op **Ga naar App Store**.
    6. Tik op **INSTALLEREN** in het scherm van de App Store.
  - Op Windows, macOS, Android
    1. Ga naar https://central.bitdefender.com.
    2. Log in op uw Bitdefender-account.
    3. Druk op de icoon ☰ in de linkerbovenhoek van het scherm en klik dan op **Mijn Apparaten**.
    4. Druk op **LOKALE BESCHERMING INSTALLEREN**.
    5. Klik voor Windows en macOS op de link **Op een ander apparaat**.

       Tik op Android op **Wilt u andere apparaten beschermen?**.
    6. Kies **iOS**.
    7. Selecteer **Bitdefender Mobile Security** in de lijst en tik op **Doorgaan**.
    8. Typ een e-mailadres in het daarvoor bestemde veld en tik daarna op **Verzenden**.

9. Ga vanop uw iOS-apparaat naar uw e-mailaccount en tik in de e-mail die u van onze servers ontvangt op **HAAL HET UIT DE AppStore**.

   U wordt doorgestuurd naar de **App Store**-app.

10. Tik op **INSTALLEREN** in het scherm van de App Store.

- **Vanaf App Store**

  Zoek naar Bitdefender Mobile Security for iOS om de app te vinden en te installeren.

Om de installatieprocedure te vervolledigen, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Mobile Security for iOS.

Tik op **Verdergaan** om verder te gaan naar het volgende venster.

Log in op uw Bitdefender-account

Om Bitdefender Mobile Security for iOS te gebruiken, moet u uw apparaat aan een Bitdefender-, Facebook-, Google- of Microsoft-account koppelen door vanuit de app in te loggen op uw account. De eerste keer dat u de app opent, wordt u gevraagd u aan te melden op een account.

Zo koppelt u uw apparaat aan een Bitdefender-account:

1. Geef in de overeenkomstige velden het e-mailadres en wachtwoord in van uw Bitdefender-account. Hebt u geen Bitdefender-account en wenst u er een aan te maken, klik op de daartoe bestemde link.
2. Tik op **Inloggen**.

Om in te loggen via een Facebook-, Google- of Microsoft-account, geeft u de dienst die u wilt gebruiken in bij **OF LOG IN MET**. U wordt doorgestuurd naar de inlogpagina van de gewenste dienst. Volg de instructies om uw account te linken met Bitdefender Mobile Security for iOS.

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.

Wizard

De eerste keer dat u de app opent, wordt een introductiewizard over de producteigenschappen gestart. Selecteer **VOLGENDE** om de gids voort te zetten, of **Overslaan** om de wizard te sluiten.

Dashboard

Tik op het pictogram van Bitdefender Mobile Security for iOS in de App Drawer van uw apparaat, zodat de applicatie-interface wordt geopend.

De eerste keer dat u de app opent, wordt u gevraagd om Bitdefender toe te staan u notificaties te sturen. Tik op **Toestaan** om op de hoogte te blijven telkens Bitdefender iets over uw app moet communiceren. Om de Bitdefender-notificaties te beheren, gaat u naar Instellingen > Notificaties > Mobiele Beveiliging.

Om toegang te krijgen tot de informatie die u nodig hebt, tikt u op de bijhorende icoon onder in het scherm.

VPN
Versleutelt internetcommunicatie, om uw privacy te verzekeren ongeacht welk netwerk u gebruikt. Zie "*VPN*" (p. 274) voor meer informatie.

Accountprivacy
Ga na of er lekken zijn in uw e-mailaccounts. Zie "*Accountprivacy*" (p. 277) voor meer informatie.

Antidiefstal
Spoor uw apparaat op en vergrendel het om te voorkomen dat uw persoonlijke gegevens in de verkeerde handen terechtkomen. Zie "*Anti-Theft-functies*" (p. 279) voor meer informatie.

Om andere opties te bekijken, tik op de -icoon van uw apparaat terwijl de toepassing op het startscherm staat. U ziet de volgende opties verschijnen:

- Aankopen herstellen - van hier kunt u teruggaan naar het Premium VPN-abonnement dat u aangekocht heeft via uw iTunes-account.
- Starten - hier kunt u de snelle rondleiding over het product opstarten.
- Feedback - hier lanceert u het standaard e-mailprogramma om ons feedback te sturen over de toepassing.

- Info toepassing - hier hebt u toegang tot informatie over de geïnstalleerde versie alsook de Abonnementsovereenkomst, het Privacybeleid en de naleving van de Open source-licenties.

16. VPN

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

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

Opmerking

Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de functie Bitdefender VPN voor het eerst probeert te gebruiken. Door het gebruik van de functie 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

Om Bitdefender VPN in te schakelen:

1. Tik op de -icoon onder in het scherm.
2. Klik op **Verbinden** telkens u bescherming wenst wanneer u verbonden bent met een onbeveiligd draadloos netwerk.

   Tik op **Verbreken** wanneer u de verbinding wilt verbreken.

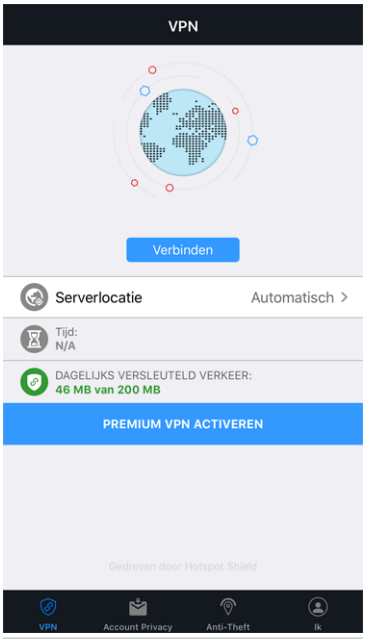
Opmerking

De eerste keer dat u VPN inschakelt, wordt u gevraagd Bitdefender toe te staan VPN-configuraties in te stellen die het netwerkverkeer zullen monitoren. Tik op **Toestaan** om verder te gaan. Indien er een authenticatiemethode (vingerafdruk of pincode) werd ingesteld om uw smartphone te beschermen, dient u deze te gebruiken.

Het icoon VPN verschijnt in de statusbalk wanneer VPN actief is.

Om uw batterij te sparen, raden we aan VPN uit te schakelen wanneer u dit niet gebruikt.

Indien u een premium-abonnement heeft en u de server naar wens wilt veranderen, tik op **Locatie Server** in de VPN-interface en selecteer vervolgens de locatie die u wenst. Voor meer info over VPN-abonnementen, raadpleeg *"Abonnementen"* (p. 275).



VPN

16.1. 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 tikken op de knop **PREMIUM VPN ACTIVEREN** die beschikbaar is in het VPN-venster.

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het abonnement voor Bitdefender Mobile Security for iOS: u kunt het dus gedurende de hele geldigheid ervan gebruiken. Indien het Bitdefender Premium VPN-abonnement vervalt, gaat u automatisch 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.

17. ACCOUNTPRIVACY

Bitdefender-accountprivacy gaat na of er data werd gelekt in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende apps of websites. De data die in een account opgeslagen is, kan gaan om wachtwoorden, credit card-informatie of bankrekeninginformatie en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op privacy.

De privacystatus van een account wordt weergegeven na de validering.

Om na te gaan of er lekken zijn op een van uw rekeningen, tik op **Scannen op lekken**.

Om vanaf nu persoonlijke informatie veilig te houden:

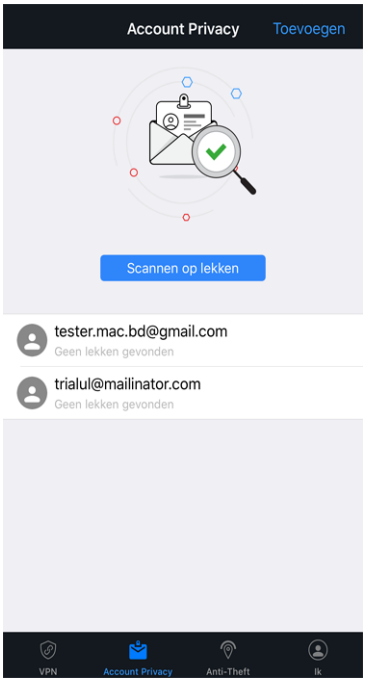
1. Tik op de -icoon onder in het scherm.
2. Tik op **Toevoegen** rechtsboven in het scherm.
3. Typ uw e-mailadres in het daarvoor bestemde veld en tik daarna op **Volgende**.

   Bitdefender moet deze account valideren voordat persoonlijke informatie wordt weergegeven. Daarom werd een e-mailbericht met valideringscode verzonden naar het opgegeven e-mailadres.
4. Controleer uw Postvak IN en tik vervolgens de ontvangen code in het vakje **Accountprivacy** van uw app in. Indien u de bevestigingse-mail niet in uw Postvak IN vindt, controleer ook uw Ongewenste mail.

   De privacystatus van de gevalideerde account wordt weergegeven.

Indien er in een van uw accounts worden gevonden, bevelen we u aan het wachtwoord zo snel mogelijk te wijzigen. Om een sterk en veilig wachtwoord te creëren, kunt u deze tips in gedachten houden:

- Zorg ervoor dat het minstens acht karakters lang is.
- Gebruik kleine letters en hoofdletters.
- Voeg ten minste een cijfer of symbool toe, zoals #, @, % of !.



Accountprivacy

18. ANTI-THEFT-FUNCTIES

Bitdefender helpt u bij het terugvinden van uw apparaat en kan verhinderen dat uw gegevens in verkeerde handen vallen.

Hiervoor hoeft u alleen maar Anti-Theft te activeren op het apparaat. Als het nodig blijkt te zijn, kunt u vervolgens vanuit elke webbrowser toegang krijgen tot **Bitdefender Central**.

Bitdefender Mobile Security for iOS biedt de volgende Anti-Theft-functies:

Lokalisering op afstand

Bekijk de huidige locatie van uw apparaat op Maps.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen:

- Als GPS is ingeschakeld op het apparaat, kan de locatie worden bepaald tot op enkele meters, zolang deze binnen het bereik van GPS-satellieten is (dus niet in een gebouw).
- Indien het apparaat binnenshuis is, kan de locatie tot op binnen tientallen meters worden bepaald indien Wi-Fi is ingeschakeld en er beschikbare draadloze netwerken in de omtrek zijn.
- Anders worden alleen gegevens van het mobiele netwerk gebruikt om de locatie te bepalen, waardoor de nauwkeurigheid beperkt blijft tot enkele honderden meters.

Vergrendelen op afstand

Vergrendel het scherm van uw apparaat op afstand.

Wissen op afstand

U kunt alle persoonlijke gegevens op uw apparaat op afstand wissen als het apparaat niet langer in uw bezit is.

Anti-Theft activeren

Om de antidiefstalfuncties te activeren:

1. Tik op de -icoon onder in het scherm.
2. Activeer de schakelaar.
3. Geef toegang tot de locatie van uw toestel, zodat Bitdefender het kan opsporen als het verloren raakt of gestolen wordt. Deze notificatie

verschijnt enkel wanneer u Bitdefender Antidiefstal voor het eerst activeert. Om de toegang tot Bitdefender te beheren, gaat u naar Instellingen > Privacy > Locatie diensten > Mobiele Beveiliging.

4. De eerste keer dat u de Antidiefstalfunctie inschakelt op uw toestel, dient u ook een MDM-profiel (Mobile Device Management) te installeren. Om dit te doen, volgt u deze stappen:

   a. Tik op **Toestaan** om terug te gaan naar het gebied Instellingen.

   b. Tik op **Installeren** om het MDM-profiel (Mobile Device Management)te installeren dat Bitdefender nodig heeft om het activeringsproces voort te zetten.

      Indien er een pincode is ingesteld om uw smartphone te beschermen, dient u deze in te geven.

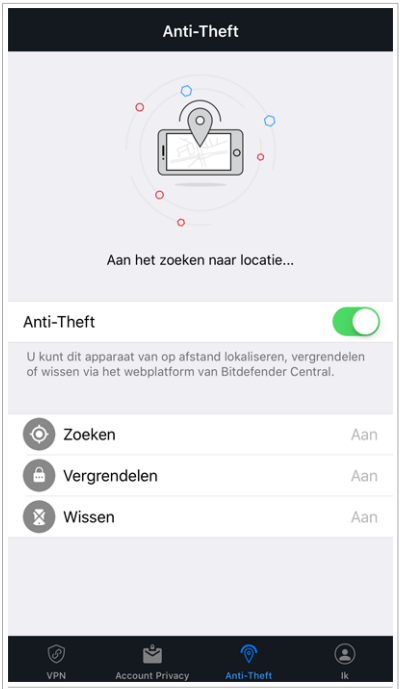
   c. Lees de informatie over de CA Root Certificate en Mobile Device Management.

   d. Tik op **Installeren** als u akkoord gaat met de bepalingen.

   e. Tik op **Vertrouwen** in de waarschuwing Extern Beheer en vervolgens op **Klaar** om het venster te sluiten.

Opmerking

Indien de installatie van het huidige Bitdefender MDM-profiel mislukt, is het mogelijk dat er al een ouder MDM-profiel geïnstalleerd is en verwijderd moet worden. Om dit te doen, gaat u naar Instellingen > Algemeen > Toestelbeheer > Bitdefender. Selecteer het getesteerde profiel en tik op **Verwijderen Beheer**. Indien er een pincode is ingesteld om uw smartphone te beschermen, dient u deze in te geven. Tik nogmaals op **Verwijderen Beheer** om uw keuze te bevestigen. bevestigen. Probeer Antidiefstal nogmaals te activeren. Stuur een e-mail naar ons team via bdios@bitdefender.com indien het probleem blijft aanhouden.



Antidiefstal

Webbeheer: Anti-Theft-functies gebruiken vanuit Bitdefender Central

Zo opent u de Anti-Theft-functies vanuit uw Bitdefender-account:

1. Ga naar https://central.bitdefender.com.
2. Log in op uw Bitdefender-account.
3. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **Mijn apparaten**.
4. Tik op de gewenste apparaatkaart en dan op het tabblad **Antidiefstal**.
5. Tik in het onderste veld van het venster op de icoon van de functie die u wilt gebruiken:

   Toon IP - geeft het laatste IP-adres voor het geselecteerde apparaat weer.
   Lokaliseren - geef de locatie van uw apparaat weer op Maps.

Vergrendelen - vergrendel uw apparaat en stel een pincode in die moet worden ingevoerd voordat het apparaat kan worden ontgrendeld.
Wissen - wis alle gegevens van uw apparaat.

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

19. BITDEFENDER ACCOUNT

Een Bitdefender-account is een vereiste om Bitdefender Mobile Security for iOS te activeren. Wanneer u toegang wenst tot de online functies en diensten van het product, of op afstand belangrijke taken uit te voeren op apparaten waarop Bitdefender geïnstalleerd is, kunt u zich vanuit elke computer of mobiel apparaat met internetverbinding aanmelden. Ga naar https://central.bitdefender.com.

Mijn apparaten

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

Om uw apparaten makkelijk te identificeren, kunt u de naam van het apparaat aanpassen en aan elk apparaat een eigenaar toekennen of aanmaken:

1. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **Mijn apparaten**.
2. Tik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm. De volgende opties zijn beschikbaar:
   - **Instellingen** - van hieruit kunt u de naam van het geselecteerde apparaat wijzigen.
   - **Profiel** - van hieruit kan een profiel toegekend worden aan het geselecteerde apparaat. Tik op **Eigenaar toevoegen**, vul dan de bijhorende velden in. Stel naam, e-mailadres, telefoonnummer, geboortedatum in en u kunt zelfs een profielfoto toevoegen.
   - **Verwijderen** - hier kunt u een profiel, samen met het toegewezen apparaat, verwijderen van uw Bitdefender-account.

Inloggen met een andere Bitdefender-account

Om in te loggen met een andere Bitdefender-account:

1. Tik op de -icoon onder in het scherm.

2. Tik op de ••• -icoon rechtsboven in het scherm.
3. Tik op **Uitloggen**.
4. Geef in de overeenkomstige velden het e-mailadres en wachtwoord in van uw Bitdefender-account.
5. Tik op **Inloggen**.

MOBILE SECURITY VOOR ANDROID

20. BESCHERMINGSFUNCTIES

Bitdefender Mobile Security beschermt uw Android-apparaat door middel van de volgende functies:

- Malwarescanner
- Accountprivacy
- Webbeveiliging
- VPN
- Anti-Theft, met:
  - Lokalisering op afstand
  - Apparaatvergrendeling op afstand
  - Gegevens wissen op afstand
  - Apparaatwaarschuwingen op afstand
- App Lock
- Rapporten
- WearON

U kunt gedurende 14 dagen gratis gebruikmaken van de functies van het product. Na afloop van deze periode dient u de volledige versie aan te schaffen voor blijvende bescherming van uw mobiele apparaat.

21. AAN DE SLAG

Apparaatvereisten

Bitdefender Mobile Security werkt op alle apparaten met Android 4.0.3 of hoger. Voor bedreiging-scans via de cloud is een actieve internetverbinding nodig.

Bitdefender Mobile Security installeren

- **Vanuit Bitdefender Central**
  - Android
    1. Ga naar https://central.bitdefender.com.
    2. Log in op uw Bitdefender-account.
    3. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **Mijn apparaten**.
    4. Tik op **LOKALE BESCHERMING INSTALLEREN**.
    5. Selecteer **Bitdefender Mobile Security** in de lijst en tik op **Ga naar Google Play**.
    6. Tik in het scherm van Google Play op **Installeren**.
  - Windows, macOS, iOS
    1. Ga naar https://central.bitdefender.com.
    2. Log in op uw Bitdefender-account.
    3. Druk op de icoon ☰ in de linkerbovenhoek van het scherm en klik dan op **Mijn Apparaten**.
    4. Druk op **LOKALE BESCHERMING INSTALLEREN**.
    5. Klik voor Windows en macOS op de link **Op een ander apparaat**.

       Tik op iOS op **Wilt u andere apparaten beschermen?**.
    6. Kies **Android**.
    7. Selecteer **Bitdefender Mobile Security** uit de lijst en klik dan op **DOORGAAN**.

8. Voer een e-mailadres in het passende veld in en klik daarna op **VERZENDEN**.
9. Open uw e-mailaccount op uw Android-apparaat en tik op de knop **Kopen bij Google Play**.

   U wordt doorgestuurd naar de **Google Play**-app.
10. Tik in het scherm van Google Play op **Installeren**.

- **Vanuit Google Play**

  Zoek naar Bitdefender Mobile Security om de app te vinden en te installeren.

  In plaats daarvan kunt u ook de QR-code scannen:

QR-code

Om de installatieprocedure te vervolledigen, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Mobile Security.

Tik op **VERDERGAAN** om verder te gaan naar het volgende venster.

Log in op uw Bitdefender-account

Om Bitdefender Mobile Security te gebruiken, moet u uw apparaat aan een Bitdefender-, Facebook-, Google- of Microsoft-account koppelen door vanuit de app in te loggen op uw account. De eerste keer dat u de app opent, wordt u gevraagd u aan te melden op een account.

Als u Bitdefender Mobile Security vanaf uw Bitdefender-account hebt geïnstalleerd, zal de app proberen om automatisch op deze account in te loggen.

Zo koppelt u uw apparaat aan een Bitdefender-account:

1. Open Bitdefender Mobile Security.
2. Geef in de overeenkomstige velden het e-mailadres en wachtwoord in van uw Bitdefender-account. Hebt u geen Bitdefender-account en wenst u er een aan te maken, klik op de daartoe bestemde link.
3. Tik op **Inloggen**.

Om in te loggen via een Facebook-, Google- of Microsoft-account, geeft u de dienst die u wilt gebruiken in bij **OF LOG IN MET**. U wordt doorgestuurd naar de inlogpagina van de gewenste dienst. Volg de instructies om uw account te linken met Bitdefender Mobile Security.

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.

Bitdefender Mobile Security activeren

U moet Bitdefender Mobile Security activeren met behulp van een abonnement, dat aangeeft hoe lang u dit product mag gebruiken. Wanneer het abonnement verlopen is, zal de app niet meer werken en is uw apparaat niet langer beschermd.

Zo activeert u Bitdefender Mobile Security:

1. Open Bitdefender Mobile Security.
2. De app toont informatie over de huidige status van uw abonnement.

   Tik op **Ik heb een code**.
3. Typ een activeringscode in het desbetreffende veld en tik op **Activeren**.

Zo verlengt u uw huidige abonnement:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Mijn account** uit de lijst.
3. Voer onder **Abonnement verlengen** een activeringscode in en tik op **Activeren**.

   U kunt uw huidige abonnement ook verlengen door gebruik te maken van een van de aanbiedingen.

Dashboard

Tik op het pictogram van Bitdefender Mobile Security in de App Drawer van uw apparaat, zodat de applicatie-interface wordt geopend.

Het Dashboard toont informatie over de beveiligingsstatus van uw apparaat en stelt u in staat alle beveiligingsfuncties gemakkelijk te beheren.

Als er een procedure actief is of als u actie moet ondernemen, wordt er in het Dashboard een kaart weergegeven met meer informatie en mogelijke acties.

Via de **Menu**-knop linksboven in het scherm kunt u de functies van Bitdefender Mobile Security gebruiken en van de ene sectie naar de andere navigeren:

Malwarescanner
Hiermee kunt u zelf een scan starten en de optie Opslag scannen in- of uitschakelen. Zie "*Malwarescanner*" (p. 292) voor meer informatie.

Accountprivacy
Controleer of er data gelekt werd in uw online accounts. Zie "*Accountprivacy*" (p. 295) voor meer informatie.

Webbeveiliging
Hiermee kunt u de functie voor Webbescherming in- of uitschakelen. Zie "*Webbeveiliging*" (p. 297) voor meer informatie.

VPN
Versleutelt internetcommunicatie, om uw privacy te verzekeren ongeacht welk netwerk u gebruikt. Zie "*VPN*" (p. 299) voor meer informatie.

Antidiefstal
Hiermee kunt u de Anti-Theft-functies in- of uitschakelen en instellingen configureren. Zie "*Anti-Theft-functies*" (p. 303) voor meer informatie.

App Lock
Hiermee kunt u de geïnstalleerde apps beveiligen door een pincode in te stellen. Zie "*App Lock*" (p. 309) voor meer informatie.

Rapporten
Hier wordt een logboek bijgehouden van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten op uw apparaat. Zie "*Rapporten*" (p. 314) voor meer informatie.

WearON

Deze functie communiceert met uw smartwatch om uw telefoon terug te vinden als deze is zoekgeraakt. Zie "*WearON*" (p. 315) voor meer informatie.

22. MALWARESCANNER

Bitdefender beschermt uw apparaat en uw gegevens tegen schadelijke apps, door scans uit te voeren tijdens de installatie van nieuwe apps. U kunt ook handmatig een scan starten.

Opmerking
Zorg dat uw mobiele apparaat verbonden is met internet. Als uw apparaat geen internetverbinding heeft, kan de scan niet worden gestart.

- **Scannen bij installatie**

  Zodra u een nieuwe app installeert, wordt deze automatisch door Bitdefender Mobile Security gescand met behulp van cloud-technologie. Deze scanprocedure wordt herhaald wanneer u een update van de geïnstalleerde apps uitvoert.

  Dit type scan wordt uitgevoerd via de Autopilot-functie. Autopilot is een intelligente scanner die alle geïnstalleerde of bijgewerkte apps scant en bedreigingen elimineert.

  Als een geïnstalleerde app schadelijk blijkt te zijn, verschijnt er een waarschuwing met het advies de app te verwijderen. Tik dan op **Verwijderen** om naar het verwijderingsscherm voor de app te gaan.

- **Scannen op aanvraag**

  Wanneer u wilt controleren of u alle apps op uw apparaat veilig kunt gebruiken, kunt u een scan op aanvraag uitvoeren.

  Om een scan te starten, tikt u in de Malwarescanner-kaart van het Dashboard op de knop **Scan starten**.

  In plaats hiervan kunt u ook op deze manier een scan starten:

  1. Open Bitdefender Mobile Security.
  2. Tik op de **Menu**-knop en selecteer **Malwarescanner** uit de lijst.
  3. Tik op **Scan starten**.

  Opmerking
  In Android 6 zijn extra machtigingen vereist voor de Malware Scanner-functie. Nadat u de knop **Scan starten** hebt ingedrukt, selecteert u **Toestaan** voor de volgende items:

- **Antivirus** toestaan om telefoongesprekken te starten en te beheren?
- **Antivirus** toegang geven tot foto's, media en bestanden op uw apparaat?

De voortgang van de scan wordt weergegeven. U kunt de scan op elk gewenst moment afbreken.

Malwarescan

Bitdefender Mobile Security scant normaal gesproken het interne geheugen van uw apparaat met inbegrip van een eventueel aanwezige SD-kaart (de "opslag"). Hierdoor worden ook schadelijke apps op de geheugenkaart opgespoord voordat ze schade kunnen aanrichten.

Zo kunt u Opslag scannen in- of uitschakelen:

1. Open Bitdefender Mobile Security.

2. Tik op de **Menu**-knop en selecteer **Malwarescanner** uit de lijst.
3. Tik op de bijbehorende schakelaar.

U kunt Opslag scannen ook vanuit **Instellingen** in- of uitschakelen door eerst op de knop en daarna op de bijbehorende schakelaar te tikken.

Als er schadelijke apps worden aangetroffen, krijgt u hier bericht over. U kunt deze apps dan verwijderen via de knop **Verwijderen**.

De Malwarescanner-kaart geeft de status van uw apparaat weer. Zolang het apparaat veilig is, is de kaart groen. Wanneer er een scan moet worden uitgevoerd of als u actie moet ondernemen, wordt de kaart rood.

23. ACCOUNTPRIVACY

Bitdefender-accountprivacy gaat na of er data werd gelekt in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende apps of websites. De data die in een account opgeslagen is, kan gaan om wachtwoorden, credit card-informatie of bankrekeninginformatie en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op privacy.

De privacystatus van een account wordt weergegeven na de validering.

Automatische nieuwe controles zijn geprogrammeerd om in de achtergrond uitgevoerd te worden, maar u kunt ook dagelijks manuele scans lanceren.

Telkens wanneer er nieuwe lekken werden ontdekt in verband met de gevalideerde e-mailaccounts, worden meldingen weergegeven.

Om vanaf nu persoonlijke informatie veilig te houden:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Accountprivacy** uit de lijst.
3. Tik op de blauwe cirkel onderaan rechts op het scherm.
4. Typ uw e-mailadres in het daarvoor bestemde veld en tik daarna op **VOLGENDE**.

   Bitdefender moet deze account valideren voordat persoonlijke informatie wordt weergegeven. Daarom werd een e-mailbericht met valideringscode verzonden naar het opgegeven e-mailadres.
5. Controleer uw Postvak IN en tik vervolgens de ontvangen code in het vakje **Accountprivacy** van uw app in. Indien u de bevestigingse-mail niet in uw Postvak IN vindt, controleer uw Ongewenste mail.

   De privacystatus van de gevalideerde account wordt weergegeven.

Indien er in een van uw accounts worden gevonden, bevelen we u aan het wachtwoord zo snel mogelijk te wijzigen. Om een sterk en veilig wachtwoord te creëren, kunt u deze tips in gedachten houden:

- Zorg ervoor dat het minstens acht karakters lang is.
- Gebruik kleine letters en hoofdletters.
- Voeg ten minste een cijfer of symbool toe, zoals #, @, % of !.

Eens u een account die deel uitmaakte van een privacy-schending beveiligd hebt, kunt u de wijzigingen bevestigen door de geïdentificeerde lekken aan te duiden als **Opgelost**. Om dit te doen:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Accountprivacy** uit de lijst.
3. Tik op de account die u net beveiligd hebt.
4. In het gebied **Lekken**, sleep naar links op de lek waarvoor u de account beveiligd hebt.
5. Tik op de icoon .
6. De kaart **Aanduiden als opgelost** verschijnt.

   Tik op **BEVESTIGEN** om te bevestigen dat de account beveiligd is.

Wanneer alle gedetecteerde lekken aangeduid zijn als **Opgelost**, wordt de account niet langer gemarkeerd als gelekt, tot er een nieuw lek wordt ontdekt.

24. WEBBEVEILIGING

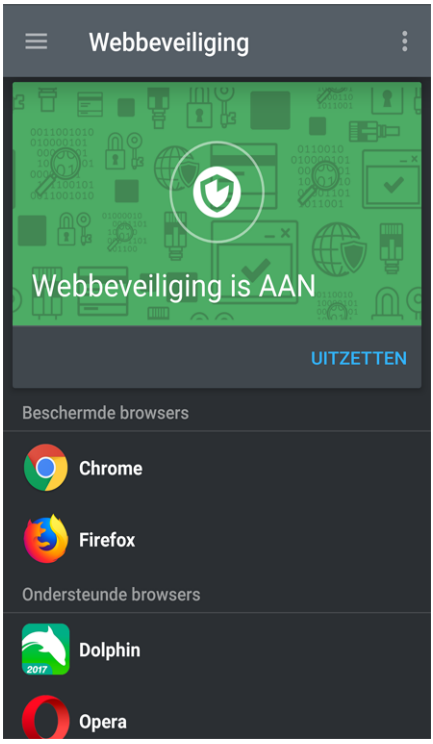
Web Protection gebruikt de cloudservices van Bitdefender om de webpagina's te controleren die u bezoekt met de standaard Android-browser, Google Chrome, Firefox, Opera, Opera Mini en/of Dolphin. Een volledig overzicht van ondersteunde webbrowsers is te vinden in het gedeelte Web Protection.

Als een URL verwijst naar een website waarvan bekend is dat deze spyware of virussen bevat of voor phishing of fraude wordt gebruikt, wordt de webpagina tijdelijk geblokkeerd en verschijnt er een waarschuwing.

U kunt dan zelf beslissen of u de webpagina toch wilt bezoeken of wilt terugkeren naar een veilige pagina.

Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Webbeveiliging. Geef de functie toestemming om zich te registreren als een Toegankelijkheid-service en tik op **Aanzetten** wanneer hierom wordt gevraagd. Tik op **Antivirus** en zet de schakelaar aan. Bevestig vervolgens dat u toestemming geeft voor de toegang.



Webbeveiliging

25. VPN

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

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

Opmerking

Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de functie Bitdefender VPN voor het eerst probeert te gebruiken. Door het gebruik van de functie 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.

Er zijn twee manieren om Bitdefender VPN in of uit te schakelen:

- Tik op de knop aan/uit in de VPN-kaart op het Dashboard.

  De status van Bitdefender VPN wordt weergegeven.

- Tik op de **Menu**-knop en selecteer **VPN** uit de lijst.

  Tik op **VERBINDEN** telkens u bescherming wenst wanneer u verbonden bent met een onbeveiligd draadloos netwerk.

  Tik op **VERBREKEN** wanneer u de verbinding wilt verbreken.

Opmerking

De eerste keer dat u VPN opstart, zal u worden gevraagd Bitdefender toe te laten een VPN verbinding op te zetten die het netwerkverkeer zal monitoren. Tik op **OK** om verder te gaan.

Het icoon verschijnt in de statusbalk wanneer Bitdefender VPN actief is.

Om uw batterij te sparen, raden we aan de VPN-functie uit te schakelen wanneer u dit niet gebruikt.

Indien u een premium-abonnement hebt en u de server naar wens wilt veranderen, tik op **LOCATIE KIEZEN** in de VPN-functie en selecteer vervolgens de locatie die u wenst. Voor meer info over VPN-abonnementen, raadpleeg "Abonnementen" (p. 301).

VPN

Tik op **MEER DETAILS** in de VPN-kaart op het Dashboard om toegang te krijgen tot de functie waar u het volgende kunt:

- Bekijk hoeveel dataverkeer u over hebt van uw dagelijkse quotum of upgrade naar de premium-versie - Info beschikbaar in de gratis versie.

- Kies de server waarmee u wilt verbinden en bekijk hoelang uw abonnement nog geldig is - Info beschikbaar in de Premium VPN-versie.

VPN Instellingen

Tik op de knop in het menu van de VPN functie, selecteer vervolgens **Instellingen** voor de geavanceerde configuratie-opties van uw VPN.

In VPN **Instellingen** kunt u de volgende opties configureren:

- Snelle toegang VPN notificatie - u krijgt een notificatie in de statusbalk waarmee u VPN snel kunt inschakelen.
- Notificatie bij verbinding met een open Wi-Fi - u krijgt, in de statusbalk, een notificatie om VPN te gebruiken telkens u verbindt met een open Wi-Fi netwerk.
- Notificatie bij het bezoeken van een website voor internetbankieren - telkens u een website voor internetbankieren bezoekt, krijgt u in de statusbalk een notificatie om VPN te gebruiken.

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 tikken op de knop **PREMIUM VPN ACTIVEREN** die beschikbaar is het Dashboard of in het VPN-venster.

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het abonnement voor Bitdefender Mobile Security: u kunt het dus gedurende de hele geldigheid ervan gebruiken, onafhankelijk van de status van het beschermingabonnement. Indien het Bitdefender Premium VPN-abonnement vervalt, maar indien het abonnement voor Bitdefender Mobile Security 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.

26. ANTI-THEFT-FUNCTIES

Bitdefender helpt u bij het terugvinden van uw apparaat en kan verhinderen dat uw gegevens in verkeerde handen vallen.

Hiervoor hoeft u alleen maar Anti-Theft te activeren op het apparaat. Als het nodig blijkt te zijn, kunt u vervolgens vanuit elke webbrowser toegang krijgen tot **Bitdefender Central**.

Zelfs als u geen internettoegang hebt, kunt u uw apparaat en uw gegevens beschermen door vanaf een mobiele telefoon **sms-opdrachten** naar uw apparaat te sturen.

Bitdefender Mobile Security biedt de volgende Anti-Theft-functies:

Lokalisering op afstand

Bekijk de huidige locatie van uw apparaat in Google Maps. De locatie wordt elke 5 seconden vernieuwd, dus u kunt deze volgen indien hij in beweging is.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen:

- Als GPS is ingeschakeld op het apparaat, kan de locatie worden bepaald tot op enkele meters, zolang deze binnen het bereik van GPS-satellieten is (dus niet in een gebouw).
- Indien het apparaat binnenshuis is, kan de locatie tot op binnen tientallen meters worden bepaald indien Wi-Fi is ingeschakeld en er beschikbare draadloze netwerken in de omtrek zijn.
- Anders worden alleen gegevens van het mobiele netwerk gebruikt om de locatie te bepalen, waardoor de nauwkeurigheid beperkt blijft tot enkele honderden meters.

IP tonen

Toont het laatste IP-adres voor het geselecteerde apparaat. Tik op **IP tonen** om deze informatie zichtbaar te maken.

Wissen op afstand

U kunt alle persoonlijke gegevens op uw apparaat op afstand wissen als het apparaat niet langer in uw bezit is.

Vergrendelen op afstand

Vergrendel het scherm van uw apparaat en stel een numerieke pincode in, die moet worden ingevoerd om het scherm te ontgrendelen.

Waarschuwing naar apparaat sturen (Scream-functie)

U kunt op afstand een bericht op het scherm van het apparaat laten weergeven, of een luid geluidssignaal laten afspelen via de luidspreker van het apparaat.

Als het apparaat is zoekgeraakt, kunt u een bericht op het scherm van het apparaat weergeven, zodat de eerlijke vinder weet hoe hij of zij u kan bereiken.

En als u het apparaat niet kunt vinden, terwijl het misschien vlakbij is (bijvoorbeeld ergens in huis of op kantoor), kunt u een luid geluidssignaal laten klinken via de Scream-functie. Dit werkt ook als het apparaat in de stille modus staat.

Anti-Theft activeren

Om de Anti-Theft-functies te activeren, voltooit u de configuratieprocedure vanaf de Anti-Theft-kaart in het Dashboard.

In plaats hiervan kunt u Anti-Theft ook op deze manier activeren:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Anti-Theft** uit de lijst.
3. Tik op **Aanzetten**.
4. U kunt deze functie nu als volgt activeren:

Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Anti-Theft. Voer de onderstaande stappen uit om deze functie in te schakelen:

- Tik op **Anti-Theft activeren** en tik vervolgens op **Aanzetten**.
- Ken de volgende machtigingen toe:
  a. **Antivirus** toestaan om sms-berichten te sturen en te bekijken?
  b. **Antivirus** toegang geven tot de locatie van dit apparaat?
  c. **Antivirus** toegang geven tot uw contacten?

a. **Beheerdersmachtigingen toekennen**

Deze bevoegdheden zijn absoluut noodzakelijk om de Anti-Theft-module te kunnen gebruiken. U moet daarom beheerdersbevoegdheden toekennen voordat u verder kunt gaan.

b. **Applicatie-pincode instellen**

Om er zeker van te zijn dat alleen uzelf veranderingen in de instellingen van Anti-Theft kunt aanbrengen, moet u een pincode instellen. Voordat de Anti-Theft-instellingen gewijzigd kunnen worden, moet deze pincode worden ingevoerd. Op apparaten met ondersteuning voor vingerafdrukherkenning kan ook een vingerafdrukscan worden gebruikt in plaats van de ingestelde pincode.

Opmerking
Dezelfde pincode wordt ook door App Lock gebruikt om uw geïnstalleerde apps te beschermen.

c. **Snapshot activeren**

Telkens wanneer iemand probeert uw geïnstalleerde applicaties te gebruiken terwijl de optie Snapshot ingeschakeld is, maakt Bitdefender een foto van deze persoon. Zie "Snapshot" (p. 311) voor meer informatie over deze functie.

d. **Vertrouwd nummer instellen voor Anti-Theft**

Selecteer het tabblad **Sms-beheer**, type een vertrouwd telefoonnummer of selecteer een telefoonnummer uit de lijst, en tik op **Nummer opslaan**. Het vertrouwde telefoonnummer moet ook een landcode bevatten, en kan het nummer zijn van iemand die u kent of van een andere telefoon die u gebruikt.

Wanneer een andere simkaart in uw apparaat wordt geplaatst, verstuurt Bitdefender Mobile Security automatisch een sms-bericht met informatie over het telefoonnummer van de nieuwe simkaart. Dit sms-bericht wordt verzonden naar het door u van tevoren ingestelde 'vertrouwde nummer'.

Op deze manier kunt u nog steeds sms-opdrachten naar uw telefoon sturen, ook als de simkaart is vervangen en de telefoon een nieuw nummer heeft.

Belangrijk
Dit is geen verplichte stap, maar het is wel aan te raden om tijdens de eerste configuratie een vertrouwd nummer in te stellen. Deze opdracht werkt alleen als deze is verzonden vanaf het van tevoren ingestelde vertrouwde nummer.

Nadat Anti-Theft is geactiveerd, kunt u de functies Webbeheer en Sms-beheer afzonderlijk in- of uitschakelen met behulp van de desbetreffende knoppen in het Anti-Theft-scherm.

Webbeheer: Anti-Theft-functies gebruiken vanuit Bitdefender Central

Opmerking

Voor alle Anti-Theft-functies is het noodzakelijk dat de optie **Achtergrondgegevens** bij de gegevensgebruik-instellingen van uw apparaat is ingeschakeld.

Zo opent u de Anti-Theft-functies vanuit uw Bitdefender-account:

1. Ga naar Bitdefender Central.
2. Tik linksboven in het venster op het pictogram en selecteer vervolgens **Mijn apparaten**.
3. Selecteer de gewenste apparaatkaart in het venster **Mijn apparaten**.
4. Selecteer het tabblad **Anti-Theft**.
5. Tik in het onderste veld van het venster op het pictogram en tik vervolgens op de knop voor de functie die u wilt gebruiken:

   Lokaliseren - geef de locatie van uw apparaat weer in Google Maps.
   Waarschuwing - typ een bericht om op het scherm van uw apparaat te laten weergeven en/of laat het apparaat een geluidssignaal afspelen.
   Vergrendelen - vergrendel uw apparaat en stel een pincode in die moet worden ingevoerd voordat het apparaat kan worden ontgrendeld.
   Wissen - wis alle gegevens van uw apparaat.

   ### Belangrijk

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

   IP tonen - geeft het laatste IP-adres voor het geselecteerde apparaat weer.

Sms-beheer: Anti-Theft-functies gebruiken via sms-opdrachten

Als sms-opdrachten zijn ingeschakeld, kunt u vanaf elke gewenste mobiele telefoon sms-berichten met de volgende opdrachten naar uw smartphone sturen:

- **LOCATE** - stuur een bericht met informatie over de locatie van het apparaat naar het telefoonnummer waarvandaan deze sms-opdracht is verzonden. Het bericht bevat een Google Maps-link, die kan worden geopend in de browser van de mobiele telefoon.
- **SCREAM** - speel een luid geluidssignaal af via de luidspreker van het apparaat.
- **LOCK** - vergrendel het scherm van het apparaat met de door u ingestelde pincode.
- **WIPE** - wis alle gegevens op het apparaat.

Belangrijk
Deze opdracht werkt alleen als deze is verzonden vanaf het van tevoren ingestelde vertrouwde nummer.

- **CALLME** - bel het telefoonnummer waarvandaan deze sms-opdracht is verzonden, met de luidspreker ingeschakeld. Op deze manier kunt u meeluisteren met de persoon die uw telefoon in handen heeft.
- **HELP** - stuur een bericht met een overzicht van alle beschikbare opdrachten naar het telefoonnummer waarvandaan deze sms-opdracht is verzonden.
- **SIM Change** - het vertrouwde nummer ontvangt een sms-bericht met het nieuwe telefoonnummer, zodra uw simkaart wordt vervangen door een andere. Om het telefoonnummer van uw vriend of kennis in te stellen, tikt u op **Vertrouwd nummer**. Typ het telefoonnummer inclusief de landcode, of kies de desbetreffende kaart uit de contactenlijst.

Alle sms-opdrachten moeten in deze vorm worden ingevoerd:

bd-<pincode> <opdracht>

Opmerking
De spitse haakjes dienen alleen om een variabele aan te geven en moeten zelf niet worden ingevoerd.

Een voorbeeld: als de pincode is ingesteld op 368711 en u een bericht wilt ontvangen met informatie over de locatie van uw telefoon, stuurt u deze sms-opdracht naar het telefoonnummer van uw telefoon:

BD-123456 LOCATE

27. APP LOCK

Bepaalde apps, bijvoorbeeld voor e-mail, foto's of berichten, bevatten persoonlijke informatie die u waarschijnlijk graag privé wilt houden. U kunt deze informatie beschermen door de toegang tot deze apps te beperken.

Met App Lock kunt u apps beveiligen met een speciale pincode, zodat onbevoegden deze apps niet meer kunnen gebruiken. U moet hiervoor een pincode van minimaal 4 en maximaal 8 cijfers instellen. Elke keer dat u een van de beveiligde apps wilt gebruiken, moet u deze pincode invoeren.

Op apparaten met ondersteuning voor vingerafdrukherkenning kan ook een vingerafdrukscan worden gebruikt in plaats van de ingestelde pincode.

App Lock activeren

Om de toegang tot bepaalde apps te beperken, configureert u App Lock vanaf de kaart die in het Dashboard wordt weergegeven nadat Anti-Theft is geactiveerd.

In plaats hiervan kunt u App Lock ook op deze manier activeren:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Tik op **Aanzetten** en geef Bitdefender toegang tot de gebruiksgegevens door het desbetreffende selectievakje in te schakelen.

   Opmerking
   In Android 6 zijn extra machtigingen vereist voor de functie Snapshot. Om deze functie in te schakelen, moet u **Antivirus** toestemming geven om foto's te maken en video's op te nemen.

4. Ga terug naar de app, configureer de toegangscode en tik op **Pincode instellen**.

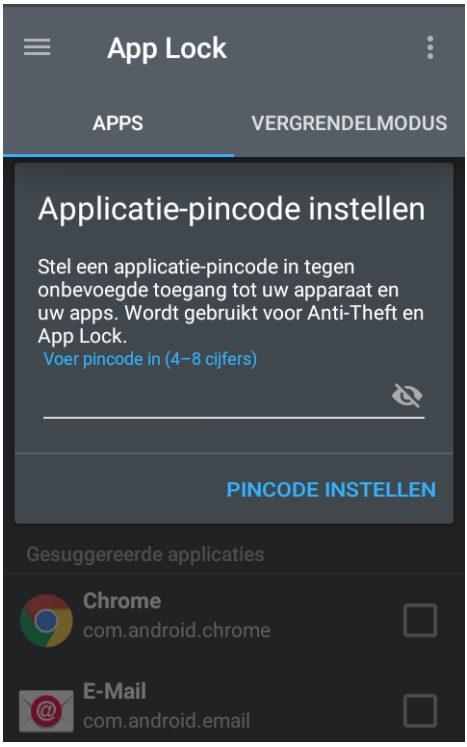
   Opmerking
   Deze stap is alleen beschikbaar als u nog geen pincode voor Anti-Theft hebt ingesteld.

5. Gebruik de optie Snapshot om indringers te betrappen die proberen toegang te krijgen tot uw persoonlijke gegevens.

6. Selecteer welke toepassingen u wilt beschermen.

Als vijf keer achter elkaar een verkeerde pincode of vingerafdruk wordt gebruikt, wordt een time-out van 30 seconden gestart. Hierdoor wordt het vrijwel onmogelijk om in de beveiligde apps in te breken.

Opmerking
Dezelfde pincode wordt ook door Anti-Theft gebruikt.



App Lock

Vergrendelmodus

Hier kunt u instellen wanneer de App Lock-functie de applicaties op uw apparaat moet beveiligen.

U kunt kiezen uit deze opties:

- **Telkens vergrendelen** - de door u geconfigureerde pincode of vingerafdruk moet bij elk gebruik van de beveiligde apps worden gebruikt.
- **Ontgrendelen tot scherm uit** - de apps zijn toegankelijk totdat het scherm wordt uitgeschakeld.
- **Korte onderbreking toestaan** - u kunt een ontgrendelde app verlaten en binnen 30 seconden weer activeren.
- **Smart Unlock activeren** - als deze optie is ingeschakeld en er verbinding is met een netwerk dat als vertrouwd is ingesteld, zijn de overige opties niet beschikbaar. Bevestiging met een pincode of vingerafdruk is dan niet nodig om toegang te krijgen tot de apps.

App Lock-instellingen

Tik op de knop in het App Lock-menu en selecteer **Instellingen** om geavanceerde configuratieopties voor App Lock weer te geven.

Met de **App Lock-instellingen** kunt u het volgende doen:

- Een snapshot laten maken na drie mislukte pogingen om de pincode in te voeren.
- Berichten vergrendelen voor nieuw geïnstalleerde apps.
- Uw pincode wijzigen.

Snapshot

Met Bitdefender-snapshot kunt u uw vrienden of verwanten op heterdaad betrappen. Op deze manier kunt u hen laten weten dat u hun nieuwsgierige ogen doorheen uw persoonlijke bestanden of de toepassingen die u gebruikt, niet op prijs stelt.

Deze functie werkt heel eenvoudig: telkens wanneer de pincode of vingerafdruk drie keer achter elkaar verkeerd wordt ingevoerd, wordt er een foto gemaakt met de camera aan de voorkant. Deze foto wordt opgeslagen met informatie over het tijdstip en de reden waarom de foto is gemaakt. U kunt deze foto later bekijken via de App Lock-functie van Bitdefender Mobile Security.

Opmerking
Deze functie is alleen beschikbaar op apparaten die aan de voorkant beschikken over een camera.

Zo configureert u de Snapshot-functie:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Tik op de knop in het App Lock-menu en selecteer **Instellingen**.
4. Activeer de schakelaar **Snapshot maken na 3 mislukte pincodepogingen**.

De foto's die tijdens het invoeren van een incorrecte pincode worden gemaakt, worden in het App Lock-menu weergegeven en kunnen in het volledige scherm worden bekeken.

U kunt de foto's ook bekijken in uw Bitdefender-account:

1. Ga naar https://central.bitdefender.com.
2. Log in op uw account.
3. Tik linksboven in het venster op het pictogram en selecteer vervolgens **Mijn apparaten**.
4. Selecteer uw apparaat in het venster **Mijn apparaten** en selecteer vervolgens het tabblad **Anti-Theft**.

   De foto's worden weergegeven.

Alleen de 3 meest recente foto's worden bewaard.

Smart Unlock

Met Smart Unlock kunt u heel eenvoudig voorkomen dat u elke keer een pincode of vingerafdrukscan nodig hebt voor de beveiligde apps.

U kunt bepaalde Wi-Fi-netwerken als 'vertrouwd' aanmerken, zodat de App Lock-blokkeringsinstellingen worden uitgeschakeld zolang u via een van deze netwerken verbonden bent met internet.

Zo activeert u de functie Smart Unlock:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.

3. Open het tabblad **Vergrendelmodus** en kies de gewenste optie.

   Het draadloze netwerk waarmee u verbonden bent, wordt weergegeven.

   Als u het momenteel gebruikte Wi-Fi-netwerk als vertrouwd netwerk wilt aanmerken, tikt u op het pictogram ⊕.

Opmerking
Deze instelling is alleen beschikbaar indien Smart Unlock is ingeschakeld.

Als u later van mening verandert, kunt u de functie weer uitschakelen. De vertrouwde Wi-Fi-netwerken worden dan niet langer vertrouwd.

28. RAPPORTEN

De Rapporten-functie houdt een uitgebreid logboek bij van gebeurtenissen met betrekking tot de scanactiviteiten op uw apparaat.

Elke keer dat er iets gebeurt dat van belang is voor de beveiliging van het apparaat, wordt een nieuw bericht toegevoegd aan de rapporten.

Zo opent u de Rapporten:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Rapporten** uit de lijst.

Het venster Rapporten bevat de volgende tabbladen:

- **Weekrapporten** - hier kunt u de beveiligingsstatus en de uitgevoerde taken van de huidige en de vorige week bekijken. Elke zondag wordt het rapport van de afgelopen week gegenereerd. U krijgt bericht wanneer het weekrapport beschikbaar is.

  Elke week wordt hier een nieuwe tip weergegeven, dus kom hier regelmatig terug om uw app zo goed mogelijk te leren gebruiken.

- **Activiteitenlogboek** - hier kunt u gedetailleerde informatie bekijken over de activiteiten van uw Bitdefender Mobile Security-app vanaf het moment van installatie op uw Android-apparaat.

  Om het huidige activiteitenlogboek te wissen, tikt u rechtsboven in het scherm op en vervolgens selecteert u **Activiteitenlogboek wissen**.

29. WEARON

Met Bitdefender WearON kunt u uw smartphone heel gemakkelijk terugvinden als u deze bent kwijtgeraakt, bijvoorbeeld op kantoor of thuis. Deze functie werkt ook als de stille modus van de telefoon actief is.

Zorg dat deze functie altijd ingeschakeld is, zodat u uw smartphone zo nodig gemakkelijk kunt terugvinden.

Opmerking
Deze functie werkt met Android 4.3 en Android Wear.

WearON activeren

Om WearON te gebruiken, koppelt u uw smartwatch aan Bitdefender Mobile Security en activeert u de WearON-functie met deze spraakopdracht:

Start:<Where is my phone>

Bitdefender WearON ondersteunt twee opdrachten:

1. **Phone Alert**

   De functie Phone Alert waarschuwt u als u te ver van uw smartphone verwijderd bent.

   Wanneer u uw smartwatch bij u hebt, detecteert deze automatisch de app op uw telefoon. Uw smartwatch gaat trillen wanneer u meer dan tien meter van de telefoon verwijderd bent.

   U kunt deze functie als volgt inschakelen: open Bitdefender Mobile Security, tik in het menu op **Algemene instellingen** en activeer de schakelaar in het gedeelte WearON.

2. **Scream**

   Uw telefoon terugvinden was nog nooit zo makkelijk. Telkens wanneer u vergeet waar u uw telefoon hebt achtergelaten, tikt u op het Scream-commando op uw uurwerk, zodat uw telefoon een geluidssignaal geeft.

30. INSTELLINGEN

Onder Instellingen kunt u de volgende opties wijzigen:

- **Pincode Beveiliging** - u kunt de pincode wijzigen die u hebt ingesteld om toepassingen of Antidiefstal-opdrachten te ontgrendelen.
- **Malware-scanner** - u kunt beslissen of de opslag moet worden gescand.
- **In-de-cloud-detectie** - u kunt beslissen of u ons rapporten stuurt die ons kunnen helpen de cloud-detectie te verbeteren.
- **Accountprivacy** - u kunt beslissen of u op de hoogte wilt blijven wanneer uw accounts niet betrokken zijn in lekken.
- **App Lock** - u kunt beslissen of u notificaties voor nieuwe toepassingen vergrendelt.
- **Snapshot** - u kunt beslissen of er een schermafdruk moet worden genomen na drie mislukte pogingen om uw toepassingen te gebruiken.
- **Antidiefstal** - u kunt het nummer dat u ingesteld hebt als vertrouwd, wijzigen, voor het geval uw toestel in vreemde handen valt.
- **Rapporten** - u kunt beslissen of u notificaties voor rapporten ontvangt.
- **Anonieme rapporten sturen** - u kunt beslissen of u ons rapporten stuurt met informatie over hoe u het product gebruikt. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen.

31. INFO

Om informatie te vinden over de Bitdefender Mobile Security-versie die u hebt geïnstalleerd, gaat u naar **Over**. Daar kunt u ons ook contacteren voor ondersteuning en vindt u de Abonnementsovereenkomst, het Privacybeleid en de Open source-licenties.

32. BITDEFENDER CENTRAL

Bitdefender Central is het webplatform waar u toegang hebt tot de online functies en diensten van het product en waar u van op afstand belantrijke taken kunt uitvoeren op toestellen waar Bitdefender op geïnstalleerd is. kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar https://central.bitdefender.com te gaan. Zodra u toegang hebt, kunt u beginnen met het volgende:

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

Inloggen op uw Bitdefender-account

Zo kunt u op uw Bitdefender-account inloggen:

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.

Mijn apparaten

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

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

1. Ga naar Bitdefender Central.
2. Tik linksboven in het venster op het pictogram en selecteer vervolgens **Mijn apparaten**.
3. Tik 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 selecteer **OPSLAAN**.

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

1. Ga naar Bitdefender Central.
2. Tik linksboven in het venster op het pictogram en selecteer vervolgens **Mijn apparaten**.
3. Tik op de gewenste apparaatkaart en vervolgens op de icoon in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Tik op **Eigenaar toevoegen**, vul de bijbehorende velden in. Pas het profiel aan met de toevoeging van een foto en de instelling van een geboortedatum.
6. Tik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en tik op **Toewijzen**.

Voor meer bewerkingen op afstand en voor meer informatie over uw Bitdefender-product op een specifiek apparaat, selecteert u de desbetreffende apparaatkaart.

Wanneer u een apparaatkaart selecteert, komen de volgende tabbladen beschikbaar:

- **Bedieningspaneel**. In dit venster vindt u gegevens over het geselecteerde apparaat, kunt u de beveiligingsstatus en de Bitdefender VPN-status nakijken en kunt u nagaan hoeveel bedreigingen de voorbije zeven dagen

werden geblokkeerd. De beschermingsstatus kan groen zijn (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Tik voor meer informatie op het uitklappijltje in het bovenste statusgebied indien uw apparaat problemen ondervindt. Van hieruit kunt u problemen manueel oplossen die de veiligheid van uw toestellen aantasten.

- **Bescherming**. In dit tabblad kunt u op afstand een scan uitvoeren op uw apparaat. Tik op de knop **Scan** om de scan te starten. U kunt ook nagaan wanneer de laatste scan werd uitgevoerd op het toestel en van de laatste scan met de belangrijkste informatie is er een verslag beschikbaar.
- **Antidiefstal**. Als uw apparaat is zoekgeraakt of gestolen, kunt u het met de Anti-Theft-functie terugvinden en op afstand opdrachten uitvoeren. Tik op **Lokaliseren** om de locatie van het apparaat te achterhalen. De laatst gekende positie zal worden weergegeven, samen met de tijd en datum. Zie "*Anti-Theft-functies*" (p. 303) voor meer informatie over deze functie.

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. Ga naar Bitdefender Central.
2. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **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.

Een nieuw apparaat toevoegen

Als uw abonnement voor meerdere apparaten geldt, kunt u een nieuw apparaat toevoegen en uw versie van Bitdefender Mobile Security op dit apparaat installeren, zoals wordt beschreven in "Bitdefender Mobile Security installeren" (p. 287).

Abonnement verlengen

Als uw abonnement nog minder dan 30 dagen geldig is en u niet voor automatische verlenging hebt gekozen, kunt u het abonnement als volgt handmatig verlengen:

1. Ga naar Bitdefender Central.
2. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **Mijn abonnementen**.
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.

33. VEELGESTELDE VRAGEN

Waarom heeft Bitdefender Mobile Security een internetverbinding nodig?

De applicatie moet met Bitdefender-servers communiceren om te kunnen bepalen of de geïnstalleerde applicaties en de bezochte webpagina's wel veilig zijn, en ook om opdrachten vanaf uw Bitdefender-account te kunnen ontvangen wanneer u de Anti-Theft-functies gebruikt.

Waarom heeft Bitdefender Mobile Security deze bevoegdheden nodig?

- Internettoegang -> nodig voor communicatie met de cloud.
- Telefoonstatus en -identiteit lezen -> wordt gebruikt om te bepalen of het apparaat verbonden is met internet en om bepaalde apparaatinformatie op te vragen, waarmee een unieke ID kan worden samengesteld voor de communicatie met de Bitdefender-cloud.
- Browserfavorieten lezen en schrijven -> de module Webbeveiliging verwijdert schadelijke websites uit uw browsergeschiedenis.
- Loggegevens lezen -> Bitdefender Mobile Security detecteert sporen van bedreigingsactiviteiten in de Android-logboeken.
- Sms, contacten, accountgegevens en externe opslag lezen en schrijven -> nodig om op afstand gegevens te kunnen wissen.
- Locatie -> nodig voor lokalisatie op afstand.
- Camera -> nodig voor Snapshot.
- Opslag -> nodig om de Malwarescanner ook de SD-kaart te laten scannen.

Waar zie ik de details over de activiteit van de toepassing?

Bitdefender Mobile Security houdt een logboek bij van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten van de applicatie. Om deze informatie weer te geven, opent u Bitdefender Mobile Security, tikt u op de **Menu**-knop en selecteert u **Rapporten** uit de lijst.

Ik ben de pincode vergeten waarmee ik mijn app heb beveiligd. Wat moet ik doen?

1. Ga naar Bitdefender Central.
2. Tik linksboven in het venster op het pictogram ☰ en selecteer vervolgens **Mijn apparaten**.

3. Tik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. De pincode wordt weergegeven in het veld **Applicatiepincode**.

Welk effect heeft Bitdefender Mobile Security op de prestaties en de batterij van mijn apparaat?

We hebben dit effect tot een minimum beperkt. De toepassing wordt enkel uitgevoerd wanneer dit van essentieel belang is - nadat u een toepassing installeert, wanneer u de interface van de toepassing gebruikt of wanneer u een beveiligingscontrole wenst. Bitdefender Mobile Security is niet op de achtergrond actief wanneer u telefoongesprekken voert, een sms-bericht invoert of een spel speelt.

Hoe kan ik App Lock uitzetten?

U kunt de App Lock-functie als zodanig niet uitzetten, maar u kunt de functie wel heel eenvoudig uitschakelen door de selectievakjes naast alle geselecteerde apps leeg te maken. (Hiervoor hebt u uw pincode of vingerafdruk nodig.).

Hoe kan ik een ander draadloos netwerk instellen als vertrouwd netwerk?

Als u een ander draadloos netwerk als vertrouwd wilt instellen:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Open het tabblad **Vergrendelmodus** en selecteer het pictogram .
4. Gebruik uw pincode of vingerafdruk om de actie te bevestigen.
5. Tik op het pictogram naast het netwerk dat u als vertrouwd wilt instellen.

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

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

1. Ga naar Bitdefender Central.
2. Tik rechtsboven op het scherm op de icoon .
3. Tik op **Mijn Account** in het schuifmenu.

4. Selecteer het tabblad **Instellingen**.
5. Inactiveer de optie **Snapshots die met uw apparaten zijn gemaakt, tonen/niet tonen**.

Hoe kan ik veilig online blijven winkelen?

Online winkelen gaat gepaard met hoge risico's als u enkele details over het hoofd ziet. Om niet het slachtoffer te worden van fraude, bevelen wij u het volgende aan:

- Houd uw beveiligingsapp up to date.
- Voer enkel online betalingen met kopersbescherming uit.
- Gebruik een VPN wanneer u een verbinding maakt met het internet via openbare en onbeveiligde draadloze netwerken.
- Wees aandachtig voor de wachtwoorden die u hebt toegekend aan uw online accounts. Ze moeten sterk zijn, met hoofdletters en kleine letters, cijfers en symbolen (@, !, %, #, etc.).
- Zorg ervoor dat de informatie die u verzendt, via veilige verbindingen gaat. De online website-extensies moet HTTPS://, zijn, niet HTTP://.

Wanneer moet ik Bitdefender VPN gebruiken?

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

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

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

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden

we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

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

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

Kan ik een andere Bitdefender-account aan mijn apparaat koppelen?

Ja, u kunt als volgt wijzigen welke Bitdefender-account aan uw apparaat is gekoppeld:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Mijn account** uit de lijst.
3. Tik op **Uitloggen** en bevestig uw keuze.
4. Tik op **Central-account gebruiken** en typ het e-mailadres en het wachtwoord voor uw nieuwe Bitdefender-account.

Wat is Apparaatbeheer?

Apparaatbeheer is een Android-functie die Bitdefender Mobile Security de benodigde bevoegdheden geeft om bepaalde taken op afstand te kunnen uitvoeren. Zonder deze bevoegdheden zou vergrendeling op afstand niet werken en zouden niet alle gegevens op afstand kunnen worden gewist. Als u de app wilt verwijderen, moet u eerst deze machtigingen intrekken via **Instellingen > Beveiliging > Apparaatbeheerders kiezen**.

Waarvoor dient het vertrouwde nummer?

Als uw telefoon in handen komt van iemand die niet van plan is de telefoon aan de rechtmatige eigenaar terug te geven, is de kans groot dat deze persoon al snel de simkaart zal vervangen. Telkens wanneer Bitdefender Mobile Security detecteeert dat een SIM-kaart in uw telefoon werd gewijzigd, stuurt het automatisch een sms met het nieuwe telefoonnummer naar het nummer dat u hebt ingesteld. Op deze manier kunt u nog steeds sms-opdrachten naar uw telefoon sturen, ook als de simkaart is vervangen en de telefoon een nieuw nummer heeft. Het vertrouwde nummer is bijvoorbeeld het

telefoonnummer van iemand die u goed kent en vertrouwt, of het nummer van een andere telefoon die in uw bezit is.

Kan het vertrouwde nummer nog worden gewijzigd nadat ik het heb ingesteld?

Ja, dat kan:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Instellingen** uit de lijst.
3. Tik in het gedeelte **Anti-Theft** op **Vertrouwd nummer**.

   U moet eerst een pincode invoeren voordat u het vertrouwde nummer kunt wijzigen.

Hoeveel kost het versturen van sms-opdrachten?

Sms-opdrachten worden verzonden als gewone sms-berichten, waarvoor u de gebruikelijke kosten van uw telefoonmaatschappij verschuldigd bent. Bitdefender brengt hiervoor verder geen kosten in rekening.

Hoe kan ik de fout "Geen Google-token" verhelpen, die zich voordoet wanneer ik inlog op Bitdefender Mobile Security?

Deze fout treedt op als het apparaat niet aan een Google-account is gekoppeld of als het apparaat wel aan een account is gekoppeld, maar er vanwege een tijdelijk probleem geen verbinding met Google gemaakt kan worden. Probeer een van de volgende oplossingen:

- Ga naar Android Instellingen > Applicaties > Applicatiebeheer > Bitdefender Mobile Security en tik op **Gegevens wissen**. Probeer vervolgens opnieuw in te loggen.
- Controleer of uw apparaat is gekoppeld aan een Google-account.

  Dit kunt u als volgt controleren: ga naar Instellingen > Accounts & synchronisatie en kijk of er een Google-account wordt weergegeven onder **Accounts beheren**. Voeg uw account toe als er geen account wordt weergegeven, start het apparaat opnieuw op en probeer opnieuw in te loggen op Bitdefender Mobile Security.
- Start het apparaat opnieuw op en probeer opnieuw in te loggen.

In welke talen is Bitdefender Mobile Security leverbaar?

Bitdefender Mobile Security is momenteel beschikbaar in deze talen:

- Braziliaans
- Tsjechisch
- Nederlands
- Engels
- Frans
- Duits
- Grieks
- Hongaars
- Italiaans
- Japans
- Koreaans
- Pools
- Portugees
- Roemeens
- Russisch
- Spaans
- Thais
- Turks
- Vietnamees

In de toekomst komen nog meer talen beschikbaar. Om de taal voor de interface van Bitdefender Mobile Security te wijzigen, gaat u naar de **Taal en toetsenbord**-instellingen van uw apparaat en stelt u het apparaat in op de gewenste taal.

CONTACT OPNEMEN MET ONS

34. HULP VRAGEN

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

De "*Algemene problemen oplossen*" (p. 191) sectie biedt de nodige informatie betreffende de vaakst voorkomende problemen tijdens het gebruik van dit product.

Als u geen oplossing voor uw vraag in de geleverde middelen hebt gevonden, kunt u direct contact met ons opnemen:

- "Neem direct met ons contact op vanaf uw Bitdefender Total Security 2018-product" (p. 329)
- "Neem contact op met ons via ons online Ondersteuningscentrum" (p. 330)

Neem direct met ons contact op vanaf uw Bitdefender Total Security 2018-product

Als u een actieve internetverbinding hebt, kunt u direct vanaf de productinterface contact opnemen met Bitdefender voor hulp.

Volg deze stappen:

1. Klik op het pictogram in de linkerzijbalk van de Bitdefender-interface.
2. U hebt de volgende opties:
   - **GEBRUIKSAANWIJZING**

     Ga naar onze database en zoek de benodigde informatie.
   - **ONDERSTEUNINGSCENTRUM**

     Raadpleeg onze online artikels en videohandleidingen.
   - **CONTACTEREN**

     Klik op **ONDERSTEUNING CONTACTEREN** om de Support Tool voor Bitdefender op te starten en de Klantendienst te contacteren.

a. Vul het verzendformulier in met de nodige gegevens:

   i. Selecteer het type probleem dat u hebt ondervonden.

   ii. Voer een beschrijving in van het probleem dat zich heeft voorgedaan.

   iii. Klik op **PROBEER DIT PROBLEEM TE REPRODUCEREN** indien u een productprobleem ondervindt. Doorgaan met de vereiste stappen.

   Wacht enkele ogenblikken terwijl Bitdefender productgerelateerde informatie verzamelt. Deze informatie zal onze technici helpen een oplossing voor uw probleem te vinden.

   iv. Klik op **TICKET BEVESTIGEN**.

b. Vul het formulier verder in met de vereiste gegevens:

   i. Voer uw volledige naam in.

   ii. Voer uw e-mailadres in.

   iii. Duid het selectievakje voor akkoord aan.

   iv. Klik op **TICKET VERSTUREN**.

   Wacht enkele ogenblikken terwijl uw ticket wordt aangemaakt en de verzamelde informatie wordt doorgestuurd naar de Klantendienst van Bitdefender.

c. Klik op **SLUITEN** om de wizard af te sluiten. Een van onze vertegenwoordigers contacteert u zo snel mogelijk.

Neem contact op met ons via ons online Ondersteuningscentrum

Als u de benodigde informatie niet kunt openen met het Bitdefender-product, kunt u ons online ondersteuningscentrum raadplegen:

1. Ga naar https://www.bitdefender.com/support/consumer.html.

   Het Ondersteuningscentrum van Bitdefender bevat talrijke artikelen met oplossingen voor problemen met betrekking tot Bitdefender.

2. Gebruik de zoekbalk bovenaan het venster om artikelen te vinden die een oplossing voor uw probleem bieden. Vul om te zoeken een term in de zoekbalk in en klik op **Zoeken**.

3. Lees de relevante artikelen of documenten door en pas de voorgestelde oplossingen toe.
4. Als uw probleem hiermee niet is opgelost, gaat u naar

   https://www.bitdefender.com/support/contact-us.htmlen neemt u contact op met onze experts van de ondersteuning.

34.1. Telefonische ondersteuning:

De laboratoria van Bitdefender stellen alles in het werk om de toegang tot telefonische ondersteuning te kunnen garanderen, tijdens plaatselijke werkuren van maandag tot en met vrijdag, met uitzondering van feestdagen.

Telefonische toegang tot de laboratoria van Bitdefender:

- **Belgium**: 070 35 83 04
- **Netherlands**: 020 788 61 50

Zorg voordat u ons belt dat u de volgende zaken binnen handbereik hebt:

- het licentienummer van uw Bitdefender programma. Geef dit nummer door aan een van onze technici zodat hij kan nagaan op welk type ondersteuning u recht hebt.
- de actuele versie van uw besturingssysteem.
- informatie met betrekking tot de merken en modellen van alle op uw computer aangesloten randapparaten en van de software die in het geheugen is geladen of in gebruik is.

In het geval er een bedreigingen is ontdekt, kan de technicus u vragen om een lijst met technische informatie en bepaalde bestanden door te sturen, die mogelijkerwijs nodig zijn voor het stellen van een diagnose.

Indien een technicus u om foutmeldingen vraagt, geef dan de exacte inhoud door en het moment waarop de meldingen verschenen, de activiteiten die eraan voorafgingen en de stappen die u zelf reeds hebt ondernomen om het probleem op te lossen.

De technicus zal een strikte procedure opvolgen in een poging het probleem op te sporen.

De volgende elementen vallen niet binnen de service:

- Deze technische ondersteuning heeft geen betrekking op de toepassingen, installaties, de deïnstallatie, de overdracht, preventief onderhoud, de

vorming, het beheer op afstand of andere softwareconfiguraties dan diegene die tijdens de interventie specifiek door onze technicus werden vermeld.

- De installatie, de instellingen, de optimalisering en de netwerkconfiguratie of de configuratie op afstand van toepassingen die niet binnen het kader van de geldende ondersteuning vallen.
- Back-ups van software/gegevens. De klant dient zelf een back-up te maken van alle gegevens, software en bestaande programma's die aanwezig zijn op de informatiesystemen waarop onze ondersteuning van toepassing is, alvorens enige dienstprestatie te laten uitvoeren door Bitdefender.

Bitdefender KUNNEN IN GEEN GEVAL AANSPRAKELIJK WORDEN GESTELD VOOR HET VERLIES OF DE RECUPERATIE VAN GEGEVENS, PROGRAMMA'S, OF VOOR HET NIET KUNNEN BENUTTEN VAN SYSTEMEN OF VAN HET NETWERK.

Adviezen beperken zich enkel tot de gestelde vragen en zijn gebaseerd op de door de klant verschafte informatie. De problemen en mogelijke oplossingen kunnen afhangen van het type systeemomgeving en van een groot aantal andere variabelen waarvan Bitdefender niet op de hoogte zijn.

Bitdefender kunnen dan ook in geen geval aansprakelijk worden gesteld voor eventuele schade die voortvloeit uit het gebruik van de verschafte informatie.

Het kan zijn dat het systeem waarop de Bitdefender programma's moeten worden geïnstalleerd onstabiel is (eerdere virusinfecties, installatie van meerdere antivirus - of beveiligingsprogramma's, etc.). In betreffende gevallen zal een technicus u mogelijkerwijze voorstellen eerst een onderhoudsbeurt op uw systeem te laten uitvoeren, alvorens het probleem kan worden opgelost.

De technische gegevens kunnen wijzigen op het moment dat er nieuwe gegevens beschikbaar zijn. Om die reden raden Bitdefender u dan ook aan regelmatig onze site "Producten" te raadplegen, via https://www.bitdefender.nl voor upgrades, of onze site met veelgestelde vragen (FAQ) op https://www.bitdefender.nl/support/consumer/.

Bitdefender wijzen elke aansprakelijkheid af voor enige rechtstreekse, onrechtstreekse, bijzondere of accidentele schade, of voor gevolgschade die te wijten is aan het gebruik van de aan u verschafte informatie.

Indien een interventie ter plaatse noodzakelijk is, zal de technicus u meer gedetailleerde informatie verschaffen met betrekking tot de dichtstbijzijnde wederverkoper.

35. ONLINE BRONNEN

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

- Ondersteuningscentrum voor Bitdefender:

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

- Ondersteuningsforum voor Bitdefender:

  https://forum.bitdefender.com

- Het HOTforSecurity-portaal over computerbeveiliging:

  https://www.hotforsecurity.com

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

35.1. Ondersteuningscentrum voor Bitdefender

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

Het Bitdefender Ondersteuningscentrum is toegankelijk voor iedereen en kan vrij worden doorzocht. De uitgebreide informatie in deze database is een van de vele middelen om Bitdefender-klanten toegang te geven tot technische kennis en waardevolle inzichten. Alle geldige aanvragen voor informatie of foutrapporten die van Bitdefender-klanten komen, vinden uiteindelijk hun weg naar het Bitdefender-ondersteuningscentrum, als rapporten over het oplossen van problemen, “spiekbriefjes” om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Ondersteuningscentrum is elk uur van de dag beschikbaar op

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

35.2. Bitdefender Ondersteuningsforum

Het Bitdefender Ondersteuningsforum biedt Bitdefender-gebruikers een eenvoudige manier om hulp te krijgen en anderen te helpen.

Als uw Bitdefender-product niet goed werkt, als het specifieke bedreigingen niet van uw computer kan verwijderen of als u vragen hebt over de manier waarop het werkt, kunt u uw probleem of vraag op het forum plaatsen.

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

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

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

35.3. HOTforSecurity-portaal

HOTforSecurity is een rijke bron aan informatie over computerbeveiliging. Hier leert u meer over de verschillende bedreigingen waaraan uw computer wordt blootgesteld wanneer u een verbinding met Internet maakt (malware, phishing, spam, cybercriminelen).

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

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

36. CONTACTINFORMATIE

Efficiënte communicatie is de sleutel naar het succes. BITDEFENDER heeft sinds 2001 een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners te overtreffen. Aarzel niet contact op te nemen met ons als u eventuele vragen hebt.

36.1. Webadressen

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

36.2. Lokale verdelers

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

Een Bitdefender-verdeler in uw land zoeken:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.
3. Als u geen Bitdefender-distributeur in uw land kunt vinden, kunt u via email rechtstreeks contact met ons opnemen via sales@bitdefender.com. Schrijf uw e-mail in het Engels zodat wij u onmiddellijk kunnen helpen.

36.3. Bitdefender-kantoren

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

Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

Belgium

Bitdefender SAS
49, Rue de la Vanne
92120 Montrouge
Telefoon: +33 (0)1 47 35 72 73
Verkoop: sales@bitdefender.com
Technische ondersteuning: https://www.bitdefender.be/support/contact-us
Web: https://www.bitdefender.be

Verenigde Staten

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

VK en Ierland

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-mail: info@bitdefender.co.uk
Telefoon: (+44) 2036 080 456
Verkoop: sales@bitdefender.co.uk
Technische ondersteuning: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Duitsland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte

Kantoor: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Verkoop: vertrieb@bitdefender.de
Technische ondersteuning: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Denemarken

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Kantoor: +45 7020 2282
Technische ondersteuning: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Spanje

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

Roemenië

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefoon verkoop: +40 21 2063470
E-mail verkoop: sales@bitdefender.ro
Technische ondersteuning: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Verenigde Arabische Emiraten

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

Woordenlijst

Abonnement

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

Achterdeur

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

Activeringscode

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

ActiveX

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

ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

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

Archief

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

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

Bedreiging

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

Bestandsnaamextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

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.

Cookie

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

Downloaden

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het

proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

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

Geavanceerde aanhoudende dreiging

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze 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.

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.

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.

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.

Honingpot

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

Informatie-update Bedreigingen

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

Ingepakte programma's

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

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

IP

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

Java-applet

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

onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

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

Keylogger

Een keylogger is een 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).

Macrovirus

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.

Mailclient

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

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.

Opdrachtregel

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

Opstartitems

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

Opstartsector

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

Opstartsectorvirus

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.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische archiveringssysteem vanaf het begin.

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

Phishing

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

Photon

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van 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 kunt aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voorzien voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

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

Ransomware

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

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

Rapportbestand

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

Rootkit

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

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

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om 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.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf.

Een harde-schijfstation leest en schrijft harde schijven.

Een diskettestation opent diskettes.

Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Script

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

Spam

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

Spyware

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

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

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

Systeemvak

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

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen.

TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Trojaans paard

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

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

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.

Vals positief

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

Virtueel PrivéNetwerk (VPN)

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

bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Worm

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