F-Secure Anti-Virus 2013

Inhoud

Hoofdstuk 1: Installatie.....5

Voordat u het product voor de eerste keer installeert.....6
Het product voor de eerste keer installeren.....6
Toepassingen installeren en upgraden.....6
Help en ondersteuning.....7

Hoofdstuk 2: Aan de slag.....9

Automatische updates gebruiken.....10
De updatestatus controleren.....10
De verbindingsinstellingen voor internet wijzigen.....10
De status van Real-time Protection Network controleren.....11
Hoe ziet u wat een product heeft gedaan?.....11
Meldinggeschiedenis weergeven.....11
Instellingen voor meldigen wijzigen.....11
Real-time Protection Network.....12
Wat is Real-time Protection Network.....12
Voordelen van Real-time Protection Network.....12
Welke gegevens u bijdraagt.....13
Hoe wij uw privacy beschermen.....14
Bijdragen aan het Real-time Protection Network.....14
Vragen over Real-time Protection Network.....15
Hoe weet ik dat mijn abonnement geldig is?.....15
Actiecentrum.....15
Een abonnement activeren.....16

Hoofdstuk 3: Inleiding.....17

De algemene status van mijn beveiliging weergeven.....18
De productstatistieken weergeven.....18
De productupdates verwerken.....19
Databaseversies weergeven.....19
Instellingen voor mobiele breedbandverbinding wijzigen.....19
Wat zijn virussen en andere malware?.....20
Virussen.....20
Spyware.....20
Rootkits.....21
Riskware.....21

Hoofdstuk 4: De computer beschermen tegen malware.....23
Hoe kan ik mijn computer scannen?.....24
Bestanden automatisch scannen.....24
Bestanden handmatig scannen.....26
E-mails scannen.....29
De scanresultaten weergeven.....30
Bestanden van de scan uitsluiten.....30
Bestandstypen uitsluiten.....30
Bestanden uitsluiten op locatie.....31
Uitgesloten toepassingen weergeven.....31
Hoe kan isolatie worden gebruikt?.....32
Items in quarantaine weergeven.....33
Geïsoleerde items herstellen.....33
Wat is DeepGuard?.....33
DeepGuard in- of uitschakelen.....34
Toepassingen toestaan die door DeepGuard zijn geblokkeerd.....34
DeepGuard in de compatibiliteitsmodus gebruiken.....34
Wat te doen met waarschuwingen van verdacht gedrag.....35

Hoofdstuk

1

Installatie

Onderwerpen:

- *Voordat u het product voor de eerste keer installeert*
- *Het product voor de eerste keer installeren*
- *Toepassingen installeren en upgraden*
- *Help en ondersteuning*

Voordat u het product voor de eerste keer installeert

Bedankt dat u voor F-Secure hebt gekozen.

U hebt het volgende nodig om het product te installeren:

- De installatie-cd of een installatiepakket. Als u een netbook zonder cd-station gebruikt, kunt u het installatiepakket downloaden van *www.f-secure.com/netbook*.
- Uw abonnementscode.
- Een internetverbinding.

Als u een beveiligingsproduct van een andere aanbieder gebruikt, zal de installer proberen deze automatisch te verwijderen. Als dit niet gebeurt, verwijder het product dan handmatig.

Opmerking: Als u meer dan één account hebt op de computer, meld u dan aan met beheerdersrechten voor de installatie.

Het product voor de eerste keer installeren

Instructies voor het installeren van het product.

Volg de instructies om het product te installeren.

1. Plaats de CD of dubbelklik op de installer die u hebt gedownload.

   Als de cd niet automatisch start, gaat u naar de Windows Verkenner, dubbelklikt u op het pictogram van de cd-rom en dubbelklikt u op het installatiebestand om de installatie te starten.

2. Volg de instructies op het scherm.

   - Als u het product op een cd-rom hebt aangeschaft in een winkel, staat de abonnementscode op de omslag van de gids voor snelle installatie.
   - Als u het product hebt gedownload van de F-Secure eStore, staat de abonnementscode in de bevestigingse-mail van de inkooporder.

   Uw computer moet mogelijk opnieuw opstarten voordat uw abonnement kan worden gevalideerd en de nieuwste updates van internet kunnen worden gedownload. Als u vanaf de cd installeert, verwijder dan de cd voordat u uw computer opnieuw opstart.

Toepassingen installeren en upgraden

Instructies voor het activeren van uw nieuwe abonnement.

Volg deze instructies om uw nieuwe abonnement te activeren of een nieuwe toepassingen te installeren met het startpaneel:

Opmerking: U vindt het pictogram voor het startpaneel in het systeemvak van Windows.

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu geopend.
2. Selecteer **Mijn abonnementen weergeven**
3. Ga naar de pagina **Abonnementsstatus** onder **Mijn abonnementen** en ga naar **Abonnement activeren**.
   Het venster **Abonnement activeren** wordt weergegeven.

4. Voer uw abonnementscode voor de toepassing in en klik op **OK**.
5. Klik op **Sluiten** nadat uw abonnement is gevalideerd en geactiveerd.
6. Ga naar de pagina **Installatiestatus** onder **Mijn abonnementen**. Als de installatie niet automatisch start, volgt u deze instructies:
   a) Klik op **Installeren**.
   Het installatievenster wordt geopend.
   b) Klik op **Volgende**.
   De toepassing is gedownload en de installatie start.
   c) Wanneer de installatie is voltooid, klikt u op **Sluiten**.

Het nieuwe abonnement is geactiveerd.

Help en ondersteuning

U hebt toegang tot de help van dit product via internet door op het Help-pictogram te klikken of door op F1 te drukken in een willekeurig venster van het product.

Nadat u uw licentie hebt geregistreerd, hebt u recht op aanvullende services zoals gratis productupdates en productondersteuning. U kunt zich registreren op *www.f-secure.com/register*.

Hoofdstuk

2

Aan de slag

Onderwerpen:

- *Automatische updates gebruiken*
- *Hoe ziet u wat een product heeft gedaan?*
- *Real-time Protection Network*
- *Hoe weet ik dat mijn abonnement geldig is?*

Informatie over hoe u aan de slag kunt met het product.

In dit gedeelte wordt beschreven hoe u de algemene instellingen kunt wijzigen en uw abonnementen kunt beheren via het startpaneel.

De algemene instellingen van het startpaneel zijn instellingen die van toepassing zijn op alle programma's die zijn geïnstalleerd op het startpaneel. In plaats van de instellingen apart te wijzigen in elk programma, kunt u eenvoudig de algemene instellingen bewerken, die vervolgens door alle geïnstalleerde programma's worden gebruikt.

De algemene instellingen van het startpaneel omvatten:

- Downloads, waar u informatie kunt weergeven over welke updates zijn gedownload en handmatig kunt controleren of er nieuwe updates beschikbaar zijn.
- Verbindingsinstellingen, waar u kunt wijzigen hoe de computer verbinding maakt met internet.
- Meldingen, waar u eerdere meldingen kunt weergeven en kunt instellen wat voor meldingen u wilt weergeven.
- Privacy-instellingen, waar u kunt selecteren of de computer verbinding mag maken met het Real-time Protection Network.

U kunt ook uw abonnementen beheren voor geïnstalleerde programma's via het startpaneel.

Automatische updates gebruiken

Automatische updates zorgen ervoor dat de beveiliging van uw computer wordt bijgewerkt.

Het product haalt de laatste updates op voor uw computer wanneer u verbinding hebt met internet. Het detecteert het netwerkverkeer en stoort het andere internetgebruik niet, zelfs niet wanneer het netwerk langzaam is.

De updatestatus controleren

Datum en tijd van de nieuwste update weergeven.

Wanneer automatische updates zijn ingeschakeld, ontvangt het product automatisch de nieuwste updates wanneer u verbinding maakt met internet.

Controleren of u beschikt over de nieuwste updates:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.
2. Selecteer **Algemene instellingen openen**.
3. Selecteer **Automatische updates** > **Downloads**.
4. Klik op **Nu controleren**.
   Het product maakt verbinding met internet en controleert op nieuwe updates. Als de beveiliging niet is bijgewerkt, worden de nieuwste updates gedownload.

   Opmerking: Als u een modem gebruikt of een ISDN-verbinding met internet hebt, moet de verbinding actief zijn als u op updates wilt controleren.

De verbindingsinstellingen voor internet wijzigen

Meestal is het niet nodig om de standaardinstellingen te wijzigen, maar u kunt instellen hoe de server verbinding maakt met internet zodat u automatisch updates kunt ontvangen.

De verbindingsinstellingen voor internet wijzigen:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.
2. Selecteer **Algemene instellingen openen**.
3. Selecteer **Automatische updates** > **Verbinding**.
4. Selecteer in de lijst **Internetverbinding** hoe de computer is verbonden met internet.
   - Selecteer **Altijd uitgaan van actieve verbinding** als u een permanente netwerkverbinding hebt.

     Opmerking: Als de computer geen permanente netwerkverbinding heeft en is ingesteld voor inbellen op aanvraag, kan er meerdere keren worden ingebeld als u **Altijd uitgaan van actieve verbinding** selecteert.
   - Selecteer **Verbinding detecteren** om alleen updates op te halen als het product vaststelt dat er een actieve netwerkverbinding beschikbaar is.
   - Selecteer **Verkeer detecteren** om alleen updates op te halen wanneer het product vaststelt dat er ander netwerkverkeer is.

     Tip: Als u een ongebruikelijke hardwareconfiguratie hebt die ervoor zorgt dat met de instelling **Verbinding detecteren** wordt vastgesteld dat u een actieve netwerkverbinding hebt, zelfs als dit niet het geval is, moet u **Verkeer detecteren** selecteren.

5. Selecteer bij **HTTP-proxy** of uw computer wel of geen *proxyserver* gebruikt om verbinding te maken met internet.
   - Selecteer **Geen HTTP-proxy** als uw computer rechtstreeks is verbonden met internet.
   - Selecteer **HTTP-proxy handmatig configureren** om de instellingen voor *HTTP-proxy* in te stellen.
   - Selecteer **HTTP-proxy van mijn browser gebruiken** om dezelfde *HTTP-proxy*-instellingen te gebruiken die u hebt opgegeven in uw webbrowser.

De status van Real-time Protection Network controleren

Veel productfuncties zijn afhankelijk van de verbinding van Real-time Protection Network om correct te kunnen functioneren.

Als er netwerkproblemen zijn of als uw firewall verkeer van Real-time Protection Network blokkeert, is de status 'verbinding is verbroken'. Als er geen productfuncties zijn geïnstalleerd waarvoor toegang tot Real-time Protection Network is vereist, is de status 'niet in gebruik.

De status controleren:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.
2. Selecteer **Algemene instellingen openen**.
3. Selecteer **Automatische updates** > **Verbinding**.

Onder **Real-time Protection Network** wordt de huidige status van Real-time Protection Network weergegeven.

Hoe ziet u wat een product heeft gedaan?

U kunt zien welke acties het product heeft genomen om uw computer te beschermen op de pagina **Meldingen**.

Het product geeft een melding weer wanneer een actie wordt uitgevoerd, bijvoorbeeld wanneer er een virus wordt gevonden dat wordt geblokkeerd. Sommige meldingen worden mogelijk ook door uw serviceprovider verzonden, bijvoorbeeld om u te laten weten dat er nieuwe services beschikbaar zijn.

Meldinggeschiedenis weergeven

U kunt zien welke meldingen zijn weergegeven in de meldingengeschiedenis

De meldingengeschiedenis weergeven:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.
2. Selecteer **Algemene instellingen openen**.
3. Selecteer **Overige** > **Meldingen**.
4. Klik op **Meldingengeschiedenis weergeven**.
   De lijst met de meldingengeschiedenis wordt weergegeven.

Instellingen voor meldigen wijzigen

U kunt selecteren welk type meldingen u wilt dat het product weergeeft.

De instellingen voor meldingen wijzigen:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.

2. Selecteer **Algemene instellingen openen**.
3. Selecteer **Overige** > **Meldingen**.
4. Schakel het selectievakje **Programmaberichten toestaan** in of uit om programmaberichten in of uit te schakelen.

   Als deze instelling is ingeschakeld, geeft het product meldingen weer van de geïnstalleerde programma's.
5. Schakel het selectievakje **Promotieberichten toestaan** in of uit om promotieberichten in of uit te schakelen.
6. Klik op **OK**.

Real-time Protection Network

Dit document beschrijft Real-time Protection Network, een online service van F-Secure Corporation, waarbij schone toepassingen en website worden geïdentificeerd en tegelijkertijd bescherming wordt geboden tegen malware en websitemisbruik.

Wat is Real-time Protection Network

Real-time Protection Network is een online service die een snelle oplossing biedt tegen de meest recente dreigingen op het internet.

Als bijdrager aan het Real-time Protection Network kunt u ons helpen de bescherming te vergroten tegen nieuwe en opkomende dreigingen. Real-time Protection Network verzamelt statistieken van bepaalde onbekende, schadelijke of verdachte toepassingen en wat ze doen op uw apparaat. Deze gegevens zijn anoniem en worden verzonden naar F-Secure Corporation voor gecombineerde analyse. Wij gebruiken de geanalyseerde informatie om de beveiliging op uw apparaat te verbeteren tegen de nieuwste dreigingen en schadelijke bestanden.

Hoe Real-time Protection Network werkt

Als een bijdrager aan het Real-time Protection Network kunt u informatie leveren over onbekende toepassingen en websites en over schadelijke toepassingen en misbruik op websites. Real-time Protection Network houdt uw webactiviteit niet bij en verzamelt geen informatie over websites die zijn geanalyseerd. Het verzamelt geen gegevens over schone toepassingen die zijn geïnstalleerd op uw computer.

Als u deze gegevens niet wilt indienen, verzamelt Real-time Protection Network geen informatie over geïnstalleerde toepassingen of bezochte websites. Het product moet echter op de F-Secure-servers de reputatie van toepassingen, websites, berichten en andere objecten navragen. Het navragen wordt gedaan met een cryptografische controlesom waarbij het gevraagde object zelf niet wordt verzonden naar F-Secure. Wij houden geen gegevens bij per gebruiker; alleen de teller van het bestand of de website wordt verhoogd.

Het is onmogelijk om al het netwerkverkeer naar Real-time Protection Network te stoppen, aangezien dit een wezenlijk deel uitmaakt van de bescherming die het product biedt.

Voordelen van Real-time Protection Network

Met Real-time Protection Network heeft u de beschikking over snellere en meer nauwkeurige bescherming tegen de meest recente bedreigingen en u ontvangt geen onnodige waarschuwingen voor verdachte toepassingen die niet kwaadaardig zijn.

Als een bijdrager aan het Real-time Protection Network kunt u ons helpen nieuwe en niet-gedetecteerde malware te vinden en mogelijke foute positieven te verwijderen uit onze database met virusdefinities.

Alle deelnemers in Real-time Protection Network helpen elkaar. Wanneer Real-time Protection Network een verdachte toepassing vindt op uw apparaat, kunt u voordeel halen uit de analyse wanneer dezelfde toepassing al eerder op andere apparaten is gevonden. Real-time Protection Network verbetert de algemene prestaties van uw apparaat, aangezien het geïnstalleerde beveiligingsproduct de toepassingen niet meer hoeft te

scannen die door Real-time Protection Network zijn geanalyseerd en schoon zijn bevonden. Daarnaast worden gegevens over kwaadaardige websites en ongevraagde bulkberichten gedeeld over Real-time Protection Network en kunnen wij u meer nauwkeurige bescherming bieden tegen websitemisbruik en spamberichten.

Hoe meer mensen bijdragen aan het Real-time Protection Network, hoe beter individuele deelnemers worden beschermd.

Welke gegevens u bijdraagt

Als een bijdrager aan het Real-time Protection Network levert u informatie over toepassingen die zijn opgeslagen op uw apparaat en de websites die u bezoekt, zodat het Real-time Protection Network bescherming kan leveren tegen de nieuwste schadelijke toepassingen en verdachte websites.

Bestandsreputatie analyseren

Real-time Protection Network verzamelt alleen gegevens van toepassingen waarvan de reputatie onbekend is en van bestanden die verdacht zijn of waarvan bekend is dat ze malware zijn.

Real-time Protection Network verzamelt anonieme informatie van schone en verdachte toepassingen op uw apparaat. Real-time Protection Network verzamelt alleen informatie over uitvoerbare bestanden (zoals Portable Executable-bestanden op het Windows-platform met de extensie .cpl, .exe, .dll, .ocx, .sys, .scr, and .drv).

Verzamelde gegevens bevatten:

- het bestandspad waar de toepassing zich bevindt op uw apparaat,
- de grootte van het bestand en wanneer het is gemaakt of aangepast,
- bestandkenmerken en rechten,
- handtekeninginformatie van het bestand,
- de huidige versie van het bestand en het bedrijf dat het bestand heeft gemaakt,
- de herkomst van het bestand of de download-URL, en
- F-Secure DeepGuard en antivirusanalyseresultaten van gescande bestanden en
- andere vergelijkbare informatie.

Real-time Protection Network verzamelt nooit informatie over uw persoonlijke documenten, tenzij deze zijn geïnfecteerd. Van elk type schadelijk bestand worden de naam van de infectie en de desinfectiestatus van het bestand verzameld.

Met Real-time Protection Network kunt u ook verdachte toepassingen indienen voor analyse. Toepassingen die u opstuurt mogen alleen PE-bestanden (Portable Executable) bevatten. Real-time Protection Network verzamelt nooit informatie over uw persoonlijke documenten en ze worden nooit automatisch geüpload voor analyse.

Bestanden indienen voor analyse

Met het Real-time Protection Network kunt u ook verdachte toepassingen toevoegen om te analyseren.

U kunt afzonderlijke verdachte toepassingen handmatig toevoegen wanneer het product u vraagt dit te doen. U kunt alleen Portable Executable-bestanden toevoegen. Real-time Protection Network uploadt nooit uw persoonlijke documenten.

De reputatie van een website analyseren

Real-time Protection Network houdt uw webactiviteiten niet bij en verzamelt geen gegevens over websites die al zijn geanalyseerd. Het controleert of de bezochte websites veilig zijn terwijl u internet gebruikt. Wanneer u een website bezoekt, controleert Real-time Protection Network de veiligheid hiervan en geeft een melding als de site is gewaardeerd als verdacht of schadelijk.

Als de website die u bezoekt kwaadaardige of verdachte inhoud bevat of als er websitemisbruik bekend is, verzamelt Real-Time Protection Network de gehele URL van de site, zodat de inhoud van de webpagina kan worden geanalyseerd.

Als u naar een site gaat die nog niet is gewaardeerd, verzamelt Real-time Protection Network de domein- en subdomeinnamen, en in sommige gevallen het pad naar de bezochte pagina, zodat de site kan worden geanalyseerd en gewaardeerd. Alle URL-parameters die mogelijke herkenbare persoonlijke gegevens bevatten, worden verwijderd om uw privacy te beschermen.

Opmerking: Real-time Protection Network waardeert of analyseert geen webpagina's in particuliere netwerken, dus het verzamelt nooit persoonlijke IP-netwerkadresgegevens (bijvoorbeeld van een bedrijfsintranet).

De systeeminformatie analyseren

Real-time Protection Network verzamelt de naam en versie van uw besturingssysteem, informatie over de internetverbinding en de gebruiksstatistieken van Real-time Protection Network (bijvoorbeeld, het aantal keer dat de reputatie van een website wordt gevraagd en de gemiddelde tijd waarin het resultaat van de navraag wordt opgehaald). Hierdoor kunnen we de service controleren en verbeteren.

Hoe wij uw privacy beschermen

We dragen gegevens veilig en automatisch over en verwijderen alle persoonlijke informatie die de gegevens mogelijk bevatten.

Real-time Protection Network verwijdert identificerende gegevens voordat ze worden verzonden naar F-Secure en het codeert alle verzamelde informatie tijdens de overdracht om deze te beschermen tegen ongeautoriseerde toegang. De verzamelde informatie wordt niet apart verwerkt; de informatie wordt gegroepeerd met de informatie van andere bijdragers aan het Real-time Protection Network. Alle gegevens worden statistisch en anoniem geanalyseerd, wat betekent dat er geen gegevens aan u worden gekoppeld.

Alle informatie waardoor u mogelijk persoonlijk kunt worden herkend, wordt niet opgenomen in de verzamelde gegevens. Real-time Protection Network verzamelt geen persoonlijke IP-adressen of uw persoonlijke informatie, zoals e-mailadressen, gebruikersnamen en wachtwoorden. Hoewel we al het mogelijke doen om alle persoonlijk herkenbare gegevens te verwijderen, is het mogelijk dat er persoonlijk herkenbare gegevens achterblijven in de verzamelde gegevens. In dergelijke gevallen zullen wij niet proberen om dergelijke onbedoelde gegevens te gebruiken om u te identificeren.

We passen strenge veiligheidsmaatregelen en fysieke, administratieve en technische voorzorgsmaatregelen toe om de verzamelde gegevens te beschermen wanneer deze worden overgedragen, opgeslagen en verwerkt. Informatie wordt opgeslagen op beveiligde locaties en op servers die worden beheerd door ons. Deze bevinden zich in onze kantoorgebouwen of in de kantoorgebouwen van onze onderaannemers. Alleen bevoegd personeel heeft toegang tot de verzamelde gegevens.

F-Secure kan de verzamelde gegevens delen met zijn dochterondernemingen, onderaannemers, distributeurs en partners, maar altijd in een niet persoonlijke herkenbare, anonieme indeling.

Bijdragen aan het Real-time Protection Network

U helpt ons de Real-time Protection Network-bescherming te verbeteren door gegevens over kwaadaardige programma's en website te leveren.

U kunt ervoor kiezen om deel te namen aan het Real-time Protection Network tijdens de installatie. Met de standaardinstallatie-instellingen draagt u bij aan het Real-time Protection Network. U kunt deze instelling later in het product wijzigen.

Volg deze instructies om de instellingen voor Real-time Protection Network te wijzigen:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.

2. Selecteer **Algemene instellingen openen**.
3. Selecteer **Overige** > **Privacy**.
4. Schakel het selectievakje voor deelname in om bij te dragen aan het Real-time Protection Network.

Vragen over Real-time Protection Network

Contactgegevens voor vragen over Real-time Protection Network.

Als u verdere vragen hebt over Real-time Protection Network, neemt u contact op met:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

De nieuwste versie van dit beleid is altijd beschikbaar op onze website.

Hoe weet ik dat mijn abonnement geldig is?

Uw abonnementstype en status worden weergegeven op de pagina **Abonnementsstatus**.

Als het abonnement bijna verloopt of als uw abonnement is verlopen, verandert de algehele beveiligingsstatus van het programma op het bijbehorende startpaneelpictogram.

De geldigheid van uw abonnement controleren:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.
2. Selecteer **Mijn abonnementen weergeven**.
3. Selecteer **Abonnementsstatus** om informatie over uw abonnementen voor geïnstalleerde programma's weer te geven.
4. Selecteer **Installatiestatus** om weer te geven welke programma's kunnen worden geïnstalleerd.

Uw abonnementsstatus en de vervaldatum worden ook weergegeven op de pagina **Statistieken** van het programma. Als uw abonnement is verlopen, moet u uw abonnement verlengen om updates te blijven ontvangen en het product te blijven gebruiken.

Opmerking: Als uw abonnement is verlopen, knippert het statuspictogram op uw systeemvak.

Actiecentrum

In het actiecentrum worden belangrijke meldingen weergegeven die uw aandacht nodig hebben.

Als uw abonnement is afgelopen of op het punt staat om af te lopen, wordt u op de hoogte gesteld via het actiecentrum. De achtergrondkleur en inhoud van het bericht in het actiecentrum zijn afhankelijk van uw abonnementstype en -status:

- Als uw abonnement op het punt staat te verlopen, en er zijn gratis abonnementen beschikbaar, heeft het bericht een witte achtergrond en een knop **Activeren**.

- Als uw abonnement op het punt staat te verlopen en er zijn geen gratis abonnementen beschikbaar, heeft het bericht een gele achtergrond en de knoppen **Kopen** en **Code invoeren**. Als u al een nieuw abonnement hebt gekocht, kunt u op **Code invoeren** klikken om de abonnementscode op te geven en uw abonnement te activeren.
- Als uw abonnement is verlopen en er zijn gratis abonnementen beschikbaar, heeft het bericht een rode achtergrond en de knop **Activeren**.
- Als uw abonnement is verlopen en er zijn geen gratis abonnementen beschikbaar, heeft het bericht een rode achtergrond en de knoppen **Kopen** en **Code invoeren**. Als u al een nieuw abonnement hebt gekocht, kunt u op **Code invoeren** klikken om de abonnementscode op te geven en uw abonnement te activeren.

Opmerking: Met de koppeling **Meldingsgeschiedenis weergeven** kunt u een lijst met productmeldingen weergeven, niet eerdere actiecentrummeldingen.

Een abonnement activeren

Als u een nieuwe abonnementscode of campagnecode hebt voor een product, moet u het activeren.

To activate a subscription:

1. Klik op het startpaneel met de rechtermuisknop op het rechterpictogram.
   Er wordt een pop-upmenu weergegeven.
2. Selecteer **Mijn abonnementen weergeven**.
3. Kies een van de volgende opties:
   - Klik op **Abonnement activeren**.
   - Klik op**Actiecode activeren**.
4. Voer in het dialoogvenster dat wordt geopend uw nieuwe abonnementscode of campagnecode in en klik op **OK**.

   Tip: Als u uw abonnementscode per e-mail hebt ontvangen, kunt u de code kopiëren uit het e-mailbericht en deze in het veld plakken.

Nadat u de nieuwe abonnementscode hebt ingevoerd, wordt de geldigheidsduur van het nieuwe abonnement weergegeven op de pagina **Abonnementsstatus**.

Hoofdstuk

3

Inleiding

Onderwerpen:

- *De algemene status van mijn beveiliging weergeven*
- *De productstatistieken weergeven*
- *De productupdates verwerken*
- *Wat zijn virussen en andere malware?*

Dit product beschermt uw computer tegen virussen en andere schadelijke toepassingen.

Het product scant bestanden en analyseert toepassingen en updates automatisch. U hoeft hiervoor geen actie te ondernemen.

De algemene status van mijn beveiliging weergeven

De pagina **Status** geeft een kort overzicht van de geïnstalleerde productfuncties met de huidige status.

Open als volgt de pagina **Status**:

Klik op de hoofdpagina op **Status**.

De pagina **Status** wordt geopend.

De pictogrammen geven de status van het programma en de beveiligingsfuncties aan.

Statuspictogram	Naam status	Beschrijving
	OK	Uw computer is beveiligd. De functie is ingeschakeld en werkt correct.
	Informatie	Het product informeert u over een speciale status van een functie. De functie wordt bijvoorbeeld bijgewerkt.
	Waarschuwing	Uw computer is niet volledig beveiligd. Het product heeft bijvoorbeeld lange tijd geen updates ontvangen of de status van een functie vereist aandacht.
	Fout	Uw computer is niet beveiligd Uw abonnement is bijvoorbeeld verlopen of een kritieke functie is uitgeschakeld.
	Uit	Een niet-essentiële functie is uitgeschakeld.

De productstatistieken weergeven

U kunt zien wat het product heeft gedaan sinds de installatie op de pagina **Statistieken**.

De pagina **Statistieken** openen:

Klik op de hoofdpagina op **Statistieken**.

De pagina **Statistieken** wordt geopend.

- **Laatste voltooide updatecontrole** geeft de tijd van de laatste update weer.

- **Virus- en spywarebescherming** geeft aan hoeveel bestanden door het product zijn gescand en sinds de installatie zijn opgeschoond.
- **Toepassingen** geeft weer hoeveel toepassingen DeepGuard heeft geblokkeerd sinds de installatie.
- **Firewallverbindingen** geeft het aantal toegestane en geblokkeerde verbindingen weer sinds de installatie.
- **Spam en phishing filteren** geeft weer hoeveel e-mailberichten het product heeft gedetecteerd als geldige e-mailberichten en als spamberichten.

De productupdates verwerken

Het product werkt de beveiliging automatisch bij.

Databaseversies weergeven

De tijden van de laatste updates en versienummers worden weergeven op de pagina **Database-updates**.

De pagina **Database-updates** openen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Overige instellingen** > **Databaseversies**.

Op de pagina **Databaseversies** wordt de laatste datum weergegeven waarop de virus- en spywaredefinities zijn gedownload, DeepGuard en spam- en phishingfilters zijn bijgewerkt met de bijbehorende versienummers.

Instellingen voor mobiele breedbandverbinding wijzigen

Selecteer of u beveiligingsupdates wilt downloaden wanneer u een mobiele breedbandverbinding gebruikt.

Opmerking: Deze functie is alleen beschikbaar in Microsoft Windows 7.

Beveiligingsupdates worden standaard altijd gedownload wanneer u zich op het netwerk van uw eigen provider bevindt. De updates worden echter uitgesteld als u het netwerk van een andere provider gebruikt. Dit is omdat de prijzen van verbindingen kunnen verschillen tussen providers, bijvoorbeeld in verschillende landen. U kunt deze instelling ongewijzigd laten als u bandbreedte, en mogelijk ook kosten, wilt besparen tijdens uw bezoek.

Opmerking: Deze instelling is alleen van toepassing op mobiele breedbandverbindingen. Wanneer de computer is verbonden met een vast of draadloos netwerk, wordt het product automatisch bijgewerkt.

De instelling wijzigen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Overige instellingen** > **Mobiel breedband** > **Beveiligingsupdates downloaden**.
3. Selecteer de gewenste update-optie voor mobiele verbindingen:
   - **Alleen op het netwerk van mijn eigen provider**

     Updates worden altijd gedownload op het netwerk van uw eigen provider. Wanneer u het netwerk van een andere provider bezoekt, worden de updates uitgesteld. U kunt het beste deze optie selecteren zodat uw beveiligingsproduct up-to-date blijft voor de verwachte kosten.
   - **Nooit**

     Updates worden niet gedownload wanneer u mobiel breedband gebruikt.
   - **Altijd**

Updates worden altijd gedownload ongeacht het netwerk dat u gebruikt. Selecteer deze optie als u ervoor wilt zorgen dat de beveiliging van uw computer altijd up-to-date is ongeacht de kosten.

4. Als u zelf wilt beslissen elke keer dat u het netwerk van uw eigen provider verlaat, selecteert u **Mij dit elke keer vragen wanneer ik het netwerk van mijn provider verlaat**.

Uitgestelde beveiligingsupdates

De beveiligingsupdates kunnen mogelijk worden uitgesteld wanneer u een mobiele breedbandverbinding gebruikt buiten het netwerk van uw eigen provider.

Als dit gebeurt, ziet u de melding **Uitgesteld** in de rechterbenedenhoek van uw scherm. De updates worden uitgesteld omdat de prijzen van verbindingen kunnen variëren tussen providers, bijvoorbeeld in verschillende landen. Als u tijdens uw bezoek bandbreedte en mogelijk ook kosten wilt besparen, is het aan te raden deze instelling niet te wijzigen. Als u de instelling echter toch wilt wijzigen, druk dan op de koppeling **Wijzigen**.

Opmerking:

Deze functie is alleen beschikbaar in Microsoft Windows 7.

Wat zijn virussen en andere malware?

Malware zijn programma's die speciaal zijn ontworpen om uw computer te beschadigen, uw computer te gebruiken voor illegale doeleinden zonder uw medeweten of informatie te stelen van uw computer.

Malware kan het volgende doen:

- het beheer van uw webbrowser overnemen,
- uw zoekpogingen omleiden,
- ongewenste advertenties weergeven,
- de websites bijhouden die u bezoekt,
- persoonlijke gegevens stelen zoals uw bankgegevens,
- uw computer gebruiken om spam te verzenden en
- uw computer gebruiken om andere computers aan te vallen.

Malwareprogramma's kunnen er ook voor zorgen dat uw computer langzaam en instabiel wordt. U hebt wellicht *malware* op uw computer als deze plotseling erg langzaam wordt en vaak vastloopt.

Virussen

Een virus is meestal een programma dat zichzelf kan toevoegen aan bestanden en zichzelf kan vermenigvuldigen. Ze kunnen de inhoud van andere bestanden wijzigen zodat uw computer kan worden beschadigd.

Een *virus* is een programma dat meestal zonder uw medeweten op uw computer wordt geïnstalleerd. Daarna probeert het virus zich te vermenigvuldigen. Het virus:

- gebruikt bepaalde systeembronnen van uw computer
- kan bestanden op uw computer wijzigen of beschadigen
- probeert uw computer waarschijnlijk te gebruiken om andere computers te infecteren
- kan toestaan dat uw computer wordt gebuikt voor illegale doeleinden.

Spyware

Spyware zijn programma's die uw persoonlijke gegevens verzamelen.

Spyware kan onder andere de volgende persoonlijke gegevens verzamelen:

- internetsites die u hebt bezocht,
- e-mailadressen op uw computer,
- wachtwoorden of
- creditcardgegevens.

Spyware installeert zichzelf bijna altijd zonder uw toestemming. Spyware wordt mogelijk geïnstalleerd samen met een handig programma of door u op een optie te laten klikken in een misleidend pop-upbericht.

Rootkits

Rootkits zijn programma's die het moeilijk maken om andere *malware* te vinden.

Rootkits verbergen bestanden en processen. Ze doen dit meestal om schadelijke activiteiten op uw computer te verbergen. Als een rootkit *malware* verbergt, kunt u niet eenvoudig vaststellen dat er malware op de computer staat.

Dit product bevat een rootkitscanner die gericht op rootkits zoekt, zodat *malware* niet zo makkelijk kan worden verborgen.

Riskware

Riskware is niet ontworpen om uw computer te beschadigen, maar het kan uw computer beschadigen als het onjuist wordt gebruikt.

Riskware is niet precies hetzelfde als malware. Riskware-programma's voeren een aantal handige maar mogelijk gevaarlijke functies uit.

Voorbeelden van riskware-programma's zijn:

- programma's voor chatten (zoals IRC, Internet relay chat),
- programma's voor het overdragen van bestanden via internet van een computer naar een andere,
- Telefoonprogramma's voor internet (VoIP, *Voice Over Internet Protocol*).
- Software voor toegang op afstand, zoals VNC,
- scareware, die individuen angst injagen of bedriegen zodat ze dan nep-beveiligingssoftware zullen kopen, of
- software die ontworpen is om CD-controles te omzeilen of beveiligingen te kopiëren.

Als u het programma zelf hebt geïnstalleerd en juist hebt ingesteld, is het minder schadelijk.

Als de riskware is geïnstalleerd zonder uw medeweten, is het waarschijnlijke met kwade bedoelingen geïnstalleerd en moet het worden verwijderd.

Hoofdstuk

4

De computer beschermen tegen malware

Onderwerpen:

- *Hoe kan ik mijn computer scannen?*
- *Bestanden van de scan uitsluiten*
- *Hoe kan isolatie worden gebruikt?*
- *Wat is DeepGuard?*

Virus en spyware scannen beveiligt uw computer tegen programma's die mogelijk persoonlijke gegevens stelen, uw computer beschadigen of deze voor illegale doeleinden gebruiken.

Alle soorten malware worden standaard onmiddellijk verwerkt wanneer ze worden gedetecteerd, zodat ze geen schade kunnen aanrichten.

Standaard worden tijdens een scan voor virussen en spyware uw lokale vaste schijven, alle verwisselbare media (zoals draagbare schijven of cd's) en gedownloade inhoud automatisch gescand. U kunt ook instellen dat uw e-mail automatisch worden gescand.

De scanfuncties voor virussen en spyware controleren uw computer ook op wijzigingen die kunnen duiden op *malware*. Als gevaarlijke systeemwijzigingen, zoals systeeminstellingen of pogingen om belangrijke systeemprocessen te wijzigen, worden gevonden, stopt DeepGuard dit programma omdat het waarschijnlijk *malware* is.

Hoe kan ik mijn computer scannen?

Wanneer virus en spyware scannen is ingeschakeld, wordt uw computer automatisch op schadelijke bestanden gescand. U kunt bestanden ook handmatig scannen en geplande scans instellen.

We raden u aan om virus en spyware scannen te allen tijde in te schakelen. Scan uw bestanden handmatig als u er zeker van wilt zijn dat er zich geen schadelijke bestanden op uw computer bevinden of als u bestanden wilt scannen die u hebt uitgesloten van de realtime scan.

Door een geplande scan in te stellen, verwijdert virus en spyware scannen schadelijke bestanden van uw computer op de ingestelde tijden.

Bestanden automatisch scannen

Realtime scannen beveiligt uw computer door alle bestanden te scannen wanneer ze worden geopend en door toegang te blokkeren tot bestanden die *malware* bevatten.

Wanneer uw computer een bestand probeert te openen, wordt het bestand gescand op malware door realtime scannen voordat uw computer het bestand kan openen. Als realtime scannen schadelijke inhoud vindt, wordt het bestand geïsoleerd voordat het enige schade kan aanrichten.

Is realtime scannen van invloed op de prestaties van mijn computer?

Normaal merkt u niets van het scanproces omdat het weinig tijd kost en maar weinig systeembronnen gebruikt. De hoeveelheid tijd en systeembronnen nodig voor realtime scannen zijn afhankelijk van bijvoorbeeld de inhoud, locatie en het type van het bestand.

Bestanden waarvoor het langer duurt om ze te scannen:

- Bestanden op verwisselbare media zoals cd's, dvd's en draagbare USB-stations.
- Gecomprimeerde bestanden zoals *ZIP*-bestanden.

  Opmerking: Ingepakte bestanden worden standaard niet gescand.

Realtime scannen kan uw computer trager maken in de volgende gevallen:

- u hebt een computer die niet voldoet aan de systeemvereisten of
- u opent veel bestanden op hetzelfde moment. Bijvoorbeeld, wanneer u een map opent met veel bestanden die gescand moeten worden.

Realtime scannen in- of uitschakelen

Realtime scannen ingeschakeld laten om *malware* te stoppen voordat deze uw computer kan beschadigen.

Realtime scannen in- of uitschakelen:

1. Klik op de hoofdpagina op **Status**.
2. Klik op **Instellingen op deze pagina wijzigen**.

   Opmerking: U moet beschikken over beheerdersrechten om beveiligingsfuncties uit te schakelen.

3. **Virus en spyware scannen** in- of uitschakelen.
4. Klik op **Sluiten**.

Schadelijke bestanden automatisch verwerken

Realtime scannen kan schadelijke bestanden automatisch verwerken zonder u vragen te stellen.

Realtime scannen automatisch schadelijke bestanden laten verwerken:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **Virus en spyware scannen**.
3. Selecteer **Schadelijke bestanden automatisch verwerken**.

Als u ervoor kiest schadelijke bestanden niet automatisch te verwerken, vraagt realtime scannen wat u wilt doen met een schadelijk bestand als deze is gevonden.

Spyware verwerken

Virus en spyware scannen blokkeert spyware onmiddellijk wanneer het probeert te starten.

Voordat een spywaretoepassing kan starten, blokkeert het product de toepassing en laat u beslissen wat u ermee wilt doen.

Kies een van de volgende acties wanneer spyware is gevonden:

Actie	Wat er gebeurt met de spyware
Automatisch verwerken	Het product laten beslissen wat de beste actie is om te ondernemen op basis van de gevonden spyware.
De spyware in quarantaine plaatsen	De spyware in quarantaine plaatsen zodat deze uw computer niet kan beschadigen.
De spyware verwijderen	Alle spywaregerelateerde bestanden van uw computer verwijderen.
De spyware alleen blokkeren	De toegang tot de spyware blokkeren, maar deze op uw computer houden.
De spyware van de scan uitsluiten	Spyware toestaan om te worden uitgevoerd en deze in de toekomst uitsluiten van scans.

Riskware verwerken

Virus en spyware scannen blokkeert riskware onmiddellijk wanneer deze probeert te starten.

Voordat een riskwaretoepassing kan starten, blokkeert het product de toepassing en laat u beslissen wat u ermee wilt doen.

Kies een van de volgende acties wanneer riskware is gevonden:

Actie	Wat er gebeurt met de riskware
De riskware alleen blokkeren	De toegang tot de riskware blokkeren, maar deze op uw computer houden.
De riskware in quarantaine plaatsen	De riskware in quarantaine plaatsen zodat deze uw computer niet kan beschadigen.
De riskware verwijderen	Alle riskwaregerelateerde bestanden van uw computer verwijderen.
De riskware van de scan uitsluiten	Riskware toestaan om te worden uitgevoerd en deze in de toekomst uitsluiten van scans.

Tracking cookies automatisch verwijderen

Door tracking cookies te verwijderen, weerhoudt u websites ervan om de sites die u op het internet bezoekt bij te houden.

Tracking cookies zijn kleine bestanden die websites toestaan te registeren welke websites u bezoekt. Volg deze instructies om tracking cookies buiten uw computer te houden.

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **Virus en spyware scannen**.
3. Selecteer **Traceercookies verwijderen**.
4. Klik op **OK**.

Bestanden handmatig scannen

U kunt uw bestanden handmatig scannen wanneer u bijvoorbeeld een extern apparaat met uw computer verbindt, om er zeker van te zijn dat deze geen malware bevatten.

De handmatige scan starten

U kunt uw hele computer of een specifieke locatie scannen op een bepaald type *malware*.

Als u alleen bepaalde typen *malware* vermoedt, kunt op dat type scannen. Als u vermoedt dat virussen op een bepaalde locatie op de computer staan, kunt u dat gedeelte scannen. Dit gaat veel sneller dan het scannen van de hele computer.

Uw computer handmatig scannen:

1. Klik op de hoofdpagina op de pijl onder **Scannen**.

   De scanopties worden weergegeven.

2. Selecteer het type scan.

   Selecteer **Scaninstellingen wijzigen** om handmatig scannen naar virussen en andere schadelijke toepassingen op uw computer te optimaliseren.

3. Als u **Selecteren wat moet worden gescand** selecteert, wordt er een venster geopend waarin u de locatie kunt selecteren.
   De **Wizard Scannen** wordt geopend.

Scantypen

U kunt uw hele computer of een specifieke locatie scannen op een bepaald type malware.

Hieronder worden de verschillende typen scan weergegeven:

Scantype	Wat wordt gescand	Wanneer te gebruiken
Virus- en spywarescan	Delen van uw computer worden gescand op virussen, spyware en riskware	Dit type scan is veel sneller dan een volledige scan. Alleen de delen van uw systeem met geïnstalleerde programmabestanden worden gescand. Dit type scan wordt aanbevolen als u snel wilt controleren of de computer schoon is, omdat het efficiënt actieve malware op uw computer kan vinden en verwijderen.
Volledige computerscan	Uw volledige computer (interne en externe vaste schijven) wordt gescand op virussen, spyware en riskware	Wanneer u zeker wilt weten dat er geen malware of riskware op uw computer staat.Dit type scan duurt het langst om te voltooien. Een combinatie van de snelle malwarescan en de scan van de vaste schijf.Er wordt ook gecontroleerd op items die mogelijk zijn verborgen door een rootkit.
Selecteren wat moet worden gescand	Een bepaald bestand, map of station scannen op virussen, spyware en riskware	Wanneer u denkt dat er op een bepaald gedeelte van uw computer malware staat; de locatie bevat bijvoorbeeld downloads van mogelijk gevaarlijke bronnen zoals P2P-netwerken voor het delen van bestanden. De duur

Scantype	Wat wordt gescand	Wanneer te gebruiken
		van de scan is afhankelijk van het formaat van het doel dat u scant. De scan wordt snel voltooid als u bijvoorbeeld een map scant die alleen een paar kleine bestanden bevat.
Rootkit-scan	Belangrijke systeemlocaties waar een verdacht item een beveiligingsprobleem kan betekenen. Scant op verborgen bestanden, mappen, stations of processen	Wanneer u denkt dat een rootkit op uw computer is geïnstalleerd. Bijvoorbeeld als er onlangs malware is gevonden op uw computer en u er zeker van wilt zijn dat er geen rootkit is geïnstalleerd.

Scannen in Windows Explorer

U kunt schijven, mappen en bestanden scannen op *virussen*, *spyware* en *riskware* in Windows Verkenner.

Een schijf, map of bestand scannen:

1. Plaats de muisaanwijzer op de schijf, map of het bestand dat u wilt scannen en klik met de rechtermuisknop.
2. Selecteer in het snelmenu **Mappen op virussen scannen**. (De naam van de optie is afhankelijk van of u een schijf, map of bestand scant.)
   Het venster **Wizard Scannen** wordt geopend en de scan wordt gestart.

Als een *virus* of *spyware* wordt gevonden, wordt u door de **Wizard Scannen** door de reinigingsprocedure geleid.

Te scannen bestanden selecteren

U kunt de bestandstypen selecteren die u wilt laten scannen op *virussen* en *spyware* in handmatige of geplande scans.

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Overige instellingen** > **Handmatig scannen**.
3. Selecteer onder **Scanopties** uit de volgende instellingen:

Alleen bekende bestandstypen scannen	Als u alleen die bestandstypen wilt scannen die de grootste kans hebben op infecties, bijvoorbeeld uitvoerbare bestanden. Als u deze optie selecteert, wordt de scan ook sneller uitgevoerd. De bestanden met de volgende extensies worden gescand: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` en `.hqx`.
In gecomprimeerde bestanden scannen	Archiefbestanden en -mappen scannen.

Geavanceerde methodiek gebruiken	Alle beschikbare methodiek gebruiken tijdens de scan om beter nieuwe of onbekende malware te kunnen vinden. **Opmerking:** Als u deze opties selecteert, duurt het scannen langer, en kunnen er meer onterechte foutmeldingen ontstaan (onschadelijke bestanden die worden aangemerkt als verdacht).

4. Klik op **OK**.

Opmerking: Uitgesloten bestanden op de lijst met uitgesloten items worden niet gescand, zelfs als u ze selecteert om hier gescand te worden.

Wat te doen als schadelijke bestanden worden gevonden

Selecteer hoe u schadelijke bestanden wilt verwerken als deze worden gevonden.

De te ondernemen actie selecteren wanneer schadelijke inhoud is gevonden tijdens handmatig scannen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Overige instellingen** > **Handmatig scannen**.
3. Kies bij **Wanneer virus of spyware wordt gevonden** een van de volgende opties:

Optie	Beschrijving
Vragen (standaard)	U kunt de te ondernemen actie selecteren voor elk item dat is gevonden tijdens handmatig scannen.
De bestanden schoonmaken	Het product probeert automatisch geïnfecteerde bestanden te desinfecteren die zijn gevonden tijdens handmatig scannen. **Opmerking:** Als het product het geïnfecteerde bestand niet kan schoonmaken, wordt het geïsoleerd (behalve als het op het netwerk of verwisselbare schijven is gevonden), zodat het de computer niet kan beschadigen.
De bestanden isoleren	Het product verplaatst schadelijke bestanden die zijn gevonden tijdens handmatig scannen in quarantaine zodat ze de computer niet kunnen beschadigen.
De bestanden verwijderen	Het product verwijdert schadelijke bestanden die zijn gevonden tijdens handmatig scannen.
Alleen rapporteren	Het product laat schadelijke bestanden die zijn gevonden tijdens handmatig scannen zoals ze zijn en registreert de detectie in het scanrapport. **Opmerking:** Als scannen in real-time is uitgeschakeld, is malware nog wel schadelijk voor uw computer als u deze optie selecteert.

Opmerking: Wanneer schadelijke bestanden zijn gevonden tijdens scannen volgens planning, worden ze automatisch schoongemaakt.

Een scan plannen

Uw computer zodanig instellen dat virussen en andere schadelijke toepassingen automatisch worden gescand en verwijderd wanneer u deze niet gebruikt of instellen dat de scan regelmatig wordt uitgevoerd om er zeker van te zijn dat uw computer schoon is.

Een scan plannen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Overige instellingen** > **Gepland scannen**.
3. **Scannen volgens planning** inschakelen.
4. Selecteer wanneer u de scan wilt laten starten.

Optie	Beschrijving
Dagelijks	Uw computer dagelijks scannen.
Wekelijks	Uw computer op geselecteerde dagen van de week scannen. Selecteer de dagen in de lijst.
Maandelijks	Uw computer op geselecteerde dagen in de maand scannen. Selecteer als volgt de dagen: 1. Selecteer één van de opties bij **Dag**. 2. Selecteer de dag van de maand in de lijst naast de geselecteerde dag.

5. Selecteer wanneer u de scan wilt starten op de geselecteerde dagen.

Optie	Beschrijving
Starttijd	De scan op de ingestelde tijd starten.
Nadat de computer niet is gebruikt gedurende	De scan starten nadat u de computer gedurende de opgegeven periode niet hebt gebruikt.

Scannen volgens planning gebruikt de handmatige scaninstellingen wanneer het uw computer scant, behalve dat het elke keer archieven scant en automatisch schadelijke bestanden schoonmaakt.

E-mails scannen

E-mail scannen beschermt u tegen schadelijke bestanden in e-mails die naar u zijn verzonden.

Virus en spyware scannen moet ingeschakeld zijn om e-mails op virussen te scannen.

Scannen van e-mail inschakelen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **Virus en spyware scannen**.
3. Selecteer **Schadelijke e-mailbijlagen verwijderen**.
4. Klik op **OK**.

Wanneer worden e-mailberichten en bijlagen gescand?

Scannen op virussen en spyware kan schadelijke inhoud verwijderen uit e-mail die u ontvangt.

Scannen op virussen en spyware verwijdert schadelijke e-mailberichten die worden ontvangen door e-mailprogrammas'zoals Microsoft Outlook en Outlook Express, Microsoft Mail of Mozilla Thunderbird. Het scant niet-gecodeerde e-mailberichten en bijlagen elke keer dat uw e-mailprogramma ze ontvangt van de mailserver via het POP3-protocol.

Virus en spyware scannen kan geen e-mailberichten in webmail scannen (dit gaat om e-mailtoepassingen die in uw webbrowser werken) zoals Hotmail, Yahoo!-mail of Gmail. U bent nog steeds beschermd tegen

virussen, zelfs als u schadelijke bijlagen niet verwijdert of als u webmail gebruikt. Wanneer u e-mailbijlagen opent, verwijdert realtime scannen alle schadelijke bijlagen voordat ze schade kunnen aanbrengen.

Opmerking: Realtime scannen beschermt alleen uw computer, maar niet uw vrienden. Met realtime scannen worden geen toegevoegde bestanden gescand, tenzij u de bijlage opent. Dit betekent dat als u webmail gebruikt en u een bericht doorstuurt zonder de meegezonden bijlage te openen, u mogelijk een geïnfecteerde e-mail naar uw vrienden doorstuurt.

De scanresultaten weergeven

Virus- en spywaregeschiedenis geeft alle schadelijke bestanden weer die het product heeft gevonden.

Het product kan soms niet de actie uitvoeren die u hebt geselecteerd als er iets schadelijks is gevonden. Als u er bijvoorbeeld voor kiest om bestanden schoon te maken en een bestand kan niet worden schoongemaakt, plaatst het product deze in quarantaine. U kunt deze informatie weergeven in de virus- en spywaregeschiedenis.

De geschiedenis weergeven:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **Virus en spyware scannen**.
3. Klik op **Verwijderingsgeschiedenis weergeven**.

De virus- en spywaregeschiedenis geeft de volgende informatie weer:

- datum en tijd waarop het schadelijke bestand is gevonden,
- de naam van de malware en de locatie op uw computer en
- de uitgevoerde actie.

Bestanden van de scan uitsluiten

Soms wilt u bepaalde bestanden of toepassingen van de scan uitsluiten. Uitgesloten items worden niet gescand, tenzij u deze van de lijst met uitgesloten items verwijdert.

Opmerking: Er zijn aparte lijsten met uitgesloten items voor realtime en handmatig scannen. Als u bijvoorbeeld een bestand van de realtime scan uitsluit, wordt het wel gescand bij de handmatige scan, tenzij u het ook van de handmatige scan uitsluit.

Bestandstypen uitsluiten

Als u bestanden uitsluit op type, worden bestanden met de opgegeven extensies niet gescand op schadelijke inhoud.

Bestandstypen toevoegen of verwijderen die u wilt uitsluiten:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Kies of u de bestandstypen van realtime of handmatig scannen wilt uitsluiten:
   - Selecteer **Computer Security** > **Virus en spyware scannen** om het bestandstype uit te sluiten van van real-time scannen.
   - Selecteer **Overige instellingen** > **Handmatig scannen** om het bestandstype uit te sluiten van handmatig scannen.

3. Klik op **Bestanden van de scan uitsluiten**.
4. Een bestandstype uitsluiten:
   a) Selecteer het tabblad **Bestandstypen**.
   b) Selecteer **Bestanden met de volgende extensies uitsluiten**.
   c) Geef een bestandstype dat overeenkomt met het type bestanden dat u wilt uitsluiten op in het veld naast de knop **Toevoegen**.

      Als u bestanden wilt opgeven die geen extensie hebben, typt u '.'. U kunt het jokerteken '?' gebruiken in plaats van een willekeurig teken of '*' voor een willekeurig aantal tekens.

      Als u bijvoorbeeld uitvoerbare bestanden wilt uitsluiten, typt u `exe` in het veld.
   d) Klik op **Toevoegen**.
5. Herhaal de voorgaande stap voor andere extensies die u wilt uitsluiten van het scannen op virussen.
6. Klik op **OK** om het dialoogvenster **Uitsluiten van scannen** te sluiten.
7. Klik op **OK** om de nieuwe instellingen toe te passen.

De geselecteerde bestandstypen worden van toekomstige scans uitgesloten.

Bestanden uitsluiten op locatie

Wanneer u bestanden uitsluit op locatie, worden bestanden in de opgegeven schijven of mappen niet gescand op schadelijke inhoud.

Bestandslocaties toevoegen of verwijderen die u wilt uitsluiten:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Kies of u de locatie van realtime of handmatig scannen wilt uitsluiten:
   - Selecteer **Computer** > **Virus en spyware scannen** om de locatie van realtime scannen uit te sluiten.
   - Selecteer **Computer** > **Handmatig scannen** om de locatie van handmatig scannen uit te sluiten.
3. Klik op **Bestanden van de scan uitsluiten**.
4. Een bestand, station of map uitsluiten:
   a) Selecteer het tabblad **Objecten**.
   b) Selecteer **Objecten uitsluiten (bestanden, mappen, ...)**.
   c) Klik op **Toevoegen**.
   d) Selecteer het bestand, station of de map die u wilt uitsluiten van virusscans.

      Opmerking: Sommige stations zijn mogelijk verwisslbare stations, zoals cd-, dvd- of netwerkstations. Netwerkstations en lege verwisselbare station kunnen niet worden uitgesloten.

   e) Klik op **OK**.
5. Herhaal de vorige stap om andere bestanden, stations of mappen uit te sluiten van het scannen voor virussen.
6. Klik op **OK** om het dialoogvenster **Uitsluiten van scannen** te sluiten.
7. Klik op **OK** om de nieuwe instellingen toe te passen.

De geselecteerde bestanden, schijven of mappen worden uitgesloten van toekomstige scans.

Uitgesloten toepassingen weergeven

U kunt toepassingen weergeven die u hebt uitgesloten van scans en deze verwijderen van de lijst met uitgesloten items als u ze in de toekomst wel wilt scannen.

Als realtime of handmatig scannen een toepassing detecteert die zich gedraagt als spyware of riskware, maar u weet dat deze veilig is, kunt u de toepassing uitsluiten van scannen zodat het product u er niet meer over waarschuwt.

Opmerking: Als de toepassing zich gedraagt als virus of andere kwaadaardige software, kan de toepassing niet worden uitgesloten.

U kunt toepassingen niet rechtstreeks uitsluiten. Nieuwe toepassingen verschijnen alleen op de lijst met uitgesloten items als u ze uitsluit tijdens het scannen.

Toepassingen weergeven die zijn uitgesloten van scannen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Kies of u toepassingen die zijn uitgesloten van realtime of handmatig scannen wilt weergeven:
   - Selecteer **Computer** > **Virus en spyware scannen** om toepassingen weer te geven die zijn uitgesloten van realtime scannen.
   - Selecteer **Computer** > **Handmatig scannen** om toepassingen weer te geven die zijn uitgesloten van handmatig scannen.
3. Klik op **Bestanden van de scan uitsluiten**.
4. Selecteer het tabblad **Toepassingen**.

   Opmerking: Alleen spyware- en riskware-toepassingen kunnen worden uitgesloten, virussen niet.

5. Als u de uitgesloten toepassingen nogmaals wilt scannen:
   a) Selecteer de toepassing die u in de scan wilt opnemen.
   b) Klik op **Verwijderen**.
6. Klik op **OK** om het dialoogvenster **Uitsluiten van scannen**te sluiten.
7. Klik op **OK** om af te sluiten.

Hoe kan isolatie worden gebruikt?

Isolatie is een veilige opslagplaats voor bestanden die mogelijk schadelijk zijn.

Bestanden in isolatie kunnen geen schade aanrichten aan uw computer.

U kunt *malware*, *spyware* en *riskware* in quarantaine plaatsen om ze onschadelijk te maken. U kunt toepassingen of bestanden herstellen uit quarantaine als u ze later nodig hebt.

Als u een item in isolatie niet nodig hebt, kunt u het verwijderen. Als u een item uit isolatie verwijdert, wordt het volledig van de computer verwijderd.

- In het algemeen kunt u *malware* die in isolatie is geplaatst, verwijderen.
- In de meeste gevallen kunt u *spyware* verwijderen die in isolatie is geplaatst. Het is mogelijk dat de *spyware* die in isloatie is geplaatst een deel is van een legitiem programma en dat het programma niet meer correct werkt als u het onderdeel verwijdert. Als u het programma op de computer wilt laten staan, kunt u de *spyware* die in isolatie is geplaatst weer herstellen.
- Geïsoleerde *riskware* kan een legitiem softwareprogramma zijn. Als u het programma zelf hebt geïnstalleerd kunt u het terugzetten uit de isolatie. Als de *riskware* is geïnstalleerd zonder dat u het weet, is het meestal met kwade bedoelingen geïnstalleerd en moet het worden verwijderd.

Items in quarantaine weergeven

Meer informatie over in quarantaine geplaatste items.

Gedetailleerde informatie over geïsoleerde items bekijken:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **Virus en spyware scannen**.
3. Klik op **Quarantaine weergeven**.
   Op de pagina **Quarantaine** wordt het totaalaantal items weergegeven dat is opgeslagen in quarantaine.
4. Klik op **Details** voor gedetailleerde informatie over items in quarantaine.

   U kunt de inhoud sorteren op malwarenaam of bestandspad.

   Een lijst met de eerste 100 items wordt weergegeven met het type items in quarantaine, de naam en het pad waar de bestanden zijn geïnstalleerd.
5. Als u meer informatie wilt weergeven over een item in quarantaine, klikt u op het pictogram naast het item in de kolom **Status**.

Geïsoleerde items herstellen

U kunt in quarantaine geplaatste items herstellen wanneer u ze weer nodig hebt.

U kunt in quarantaine geplaatste toepassingen of bestanden herstellen als u ze weer nodig hebt. Herstel geen in quarantaine geplaatste items tenzij u zeker weet dat ze veilig zijn. Herstelde items worden op hun oospronkelijke locatie op de computer teruggezet.

Geïsoleerde items herstellen

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **Virus en spyware scannen**.
3. Klik op **Quarantaine weergeven**.
4. Selecteer de items in quarantaine die u wilt herstellen.
5. Klik op **Herstellen**.

Wat is DeepGuard?

DeepGuard analyseert de inhoud van bestanden en het gedrag van toepassingen, en controleert toepassingen die niet vertrouwd zijn.

DeepGuard blokkeert nieuwe en niet ontdekte *virussen*, *wormen* en andere schadelijke toepassingen die wijzigingen proberen aan te brengen op uw computer, en voorkomt dat schadelijke toepassingen toegang krijgen tot internet.

Wanneer DeepGuard een nieuwe toepassing detecteert die mogelijk schadelijke wijzigingen in het systeem probeert aan te brengen, staat DeepGuard de toepassing toe te werken in een veilige zone. In de veilige zone kan de toepassing uw computer niet beschadigen. DeepGuard analyseert de wijzigingen die de toepassing heeft geprobeerd te maken en op basis hiervan wordt besloten hoe groot de kans is dat de toepassing *malware* is. Als de toepassing waarschijnlijk *malware* is, wordt het geblokkeerd door DeepGuard.

Mogelijk schadelijke systeemwijzigingen die DeepGuard detecteert bevatten:

- systeeminstelling (Windows-register) wordt gewijzigd,
- probeert belangrijke systeemprogramma's te sluiten, zoals beveiligingsprogramma's zoals dit product en
- probeert belangrijke systeembestanden te bewerken.

DeepGuard in- of uitschakelen

Houd DeepGuard ingeschakeld om te voorkomen dat verdachte toepassingen mogelijk schadelijke systeemwijzigingen aanbrengen in uw computer.

Als u Windows XP hebt, moet u ervoor zorgen dat u Service Pack 2 hebt geïnstalleerd voordat u DeepGuard inschakelt.

DeepGuard in- of uitschakelen:

1. Klik op de hoofdpagina op **Status**.
2. Klik op **Instellingen op deze pagina wijzigen**.

   Opmerking: U moet beschikken over beheerdersrechten om beveiligingsfuncties uit te schakelen.

3. **DeepGuard** in- of uitschakelen.
4. Klik op **Sluiten**.

Toepassingen toestaan die door DeepGuard zijn geblokkeerd

U kunt beheren welke toepassingen door DeepGuard worden toegestaan en geblokkeerd.

Het kan voorkomen dat DeepGuard een veilige toepassing blokkeert, zelfs als u de toepassing wilt gebruiken en weet dat deze veilig is. Dit komt doordat de toepassing systeemwijzigingen probeert aan te brengen die mogelijk schadelijk zijn. Ook hebt u wellicht per ongeluk de toepassing geblokkeerd toen een venster van DeepGuard werd weergegeven.

De door DeepGuard geblokkeerde toepassing toestaan:

1. Klik op de hoofdpagina op **Extra**.
2. Klik op **Toepassingen**.
   De lijst met **Gevolgde toepassingen** wordt weergegeven.
3. De toepassing zoeken die u wilt toestaan.

   Opmerking: U kunt op kolomkoppen klikken om de lijst te sorteren. Klik bijvoorbeeld op de kolom **Toestemming** om de lijst in groepen van toegestane en geweigerde programma's te sorteren.

4. Selecteer **Toestaan** in de kolom **Toestemming**.
5. Klik op **Sluiten**.

DeepGuard staat de toepassing weer toe om systeemwijzigingen aan te brengen.

DeepGuard in de compatibiliteitsmodus gebruiken

Voor maximale beveiliging past DeepGuard tijdelijk uitvoerende programma's aan. Sommige programma's controleren of ze niet beschadigd of aangepast zijn en zijn mogelijk niet compatibel met deze functie. Bijvoorbeeld, online games met hulpmiddelen tegen vals spelen controleren of ze niet zijn aangepast wanneer ze worden uitgevoerd. In deze gevallen kunt u de compatibiliteitsmodus inschakelen.

De compatibiliteitsmodus inschakelen:

1. Klik op de hoofdpagina op **Instellingen**.

   Opmerking: U moet beschikken over beheerdersrechten om deze instellingen te wijzigen.

2. Selecteer **Computer Security** > **DeepGuard**.
3. Selecteer **De compatibiliteitsmodus gebruiken**.
4. Klik op **OK**.

Wat te doen met waarschuwingen van verdacht gedrag

DeepGuard controleert toepassingen die niet vertrouwd zijn. Als een toepassing die wordt gecontroleerd, probeert toegang te krijgen tot internet, wijzigingen probeert aan te brengen in uw systeem of zich verdacht gedraagt, blokkeert DeepGuard de toepassing.

Als u **Waarschuw mij over verdacht gedrag** hebt geselecteerd in de DeepGuard-instellingen, waarschuwt DeepGuard u wanneer het een mogelijk schadelijke toepassing heeft gedetecteerd of wanneer u een toepassing start die een onbekende reputatie heeft.

Bepalen wat u wilt doen met de toepassing die DeepGuard heeft geblokkeerd:

1. Klik op **Details** om meer informatie over het programma weer te geven.
   Het gedeelte met details laat u het volgende zien:
   - de locatie van de toepassing,
   - de reputatie van de toepassing in Real-Time Protection Network en
   - hoe algemeen de toepassing is.
2. Bepaal of u de toepassing vertrouwt die DeepGuard heeft geblokkeerd:
   - Kies **Ik vertrouw de toepassing. Doorgaan.** als u de toepassing niet wilt blokkeren.

     De toepassing is waarschijnlijk veiliger als:
     - DeepGuard de toepassing heeft geblokkeerd als gevolg van iets dat u hebt gedaan,
     - u de toepassing herkent of
     - u de toepassing van een vertrouwde bron hebt verkregen.
   - Kies **Ik vertrouw de toepassing niet. Blijven blokkeren.** als u de toepassing wilt blijven blokkeren.

     De toepassing is waarschijnlijk minder veilig als:
     - de toepassing niet veel voorkomt,
     - de toepassing een onbekende reputatie heeft of
     - u de toepassing niet kent.
3. Als u een verdachte toepassing wilt verzenden voor analyse:
   a) Klik op **De toepassing naar F-Secure rapporteren**.
   Het product geeft de voorwaarden voor verzending weer.
   b) Klik op **Accepteren** als u akkoord gaat met de voorwaarden en het voorbeeld wilt verzenden.

   We raden u aan een voorbeeld te verzenden als:
   - DeepGuard een toepassing blokkeert waarvan u weet dat deze veilig is of
   - u vermoedt dat de toepassing mogelijk *malware* is.