

## Test beveiligingssoftware



# VEILIGHEID VAAK SCHIJN

Met een virusscanner en een firewall waar u jaarlijks voor betaalt, waant u zich misschien veilig. Dat is lang niet altijd terecht, blijkt uit de nieuwste test van beveiligingspakketten.

Een virusscanner en firewall staan standaard op het boodschappenlijstje van elke nieuwe computerkoper. Want als er al een versie voorgeïnstalleerd op de pc of notebook staat, is dat een 30-dagen-‘verleidversie’: hopelijk schaft u daarna de volledige versie aan. Maar wie denkt dat elk pakket tegenwoordig wel in orde is, heeft het helaas bij het verkeerde eind.

Virussen hebben er de afgelopen jaren heel wat nieuwe familieleden bij gekregen. De maffiafamilie, ook wel ‘malware’ genoemd, bestaat nu ook uit onder andere Trojaanse paarden, spyware en rootkits (zie het kader op pagina 13). Allemaal nieuwe bedreigingen, met elk talloze varianten, bedacht om de beveiliging te slim af te zijn. Virusscanners zijn malwarescanners geworden.

Hoe goed zijn de nieuwste beveiligingspakketten hierop ingesteld? In onze nieuwste test zitten der tien beveiligingspakketten (malwarescanner plus firewall). Daar hebben we twee bekende gratis virusscanners, van Alwil en Avira, aan toegevoegd, want waarom zou je betalen als gratis goed genoeg is? Bitdefender heeft ook een gratis virusscanner, maar die scant niet aan de poort, alleen op aanvraag. Die is daarom niet meegenomen.

We hebben een lijstje met eisen opgesteld waar een goed beveiligingspakket aan moet voldoen.

Een goed pakket:

- doet uiteraard wat het moet doen, dus malware herkennen en opruimen, en kan van onbekende bestanden ook redelijk voorspellen of het malware is;
- heeft een firewall die de poorten goed bewaakt en verbergt voor buitenstaanders;
- vertraagt het systeem minimaal;
- scant nog voor installatie de harde schijf, laat zich eenvoudig installeren en laat geen resten achter na deïnstallatie;
- is eenvoudig te bedienen, neemt zelf zo veel mogelijk beslissingen en valt de gebruiker zo min mogelijk lastig, en dan in duidelijke taal;
- scant regelmatig zelf de computer op malware en doet daar geen uren over;
- heeft slim gekozen standaardinstellingen, die een goede balans zijn tussen veiligheid enerzijds, en snelheid en gebruiksgemak anderzijds.

Klinkt eenvoudig, nietwaar? Helaas is er geen enkel pakket dat op alle punten goed scoort.

### LACHWEKKEND

Zeven pakketten laten zoveel door dat de naam 'beveiligingspakket' eigenlijk lachwekkend is. Als norm gold dat een goed pakket 98% van de mal-

## Kosten

Op de gratis virusscanners na, betaalt u voor een pakket met een licentie voor virusupdates voor een beperkte periode, meestal een jaar. Om daarna beschermd te blijven, moet u de licentie verlengen, wat vaak even duur is als een volledig nieuw pakket.

ware tegen moet houden. Geen enkel pakket haalt die score voor alle soorten malware, maar CA en Microsoft zijn werkelijk zo lek als een mandje. CA liet 30% van alle Trojaanse paarden door en maar liefst 70% van alle bootvirussen. Microsoft onderschepte minder dan een op de tien macrovirussen. De gratis scanners presteerden ook onvoldoende. Slechts twee pakketten hebben de verdedigingslinie in de volle breedte op orde: Gdata en F-Secure. Maar ook zij waarschuwen niet of zelden voor phishing sites, zoals nagemaakte banksites. Dat doet alleen Norton goed.

### VIJF UUR

Interessant was de vraag of de scanners in staat zijn om aan bestanden die niet op de zwarte lijst staan, te zien of het om malware gaat. Van de 15

### DE TOP-3:



1 Gdata Internet Security 2008

2 Bitdefender Internet Security 2008



3 F-Secure Internet Security 2008

## Wat en hoe

Alle pakketten zijn onderzocht op een doorsnee Windows XP-computer met SP2 voorzien van alle updates, een Intel P4 3 GHz processor en 1 GB intern geheugen. Indien mogelijk hebben we de doos gekocht, anders gedownload. Alle pakketten zijn getest met de standaardinstellingen en de laatste virusupdates. Het malwarecollectief dat de computer belaagde, bestond uit onder meer 543 Trojaanse paarden, 21 rootkits, 346 wormen, 48 macrovirussen, 124 bestandsvirussen, 40 bootvirussen en 35 stuks spyware. In totaal ruim 1709 stuks malware, waarvan 15 gloednieuwe virussen. Het testoordeel kon niet meer dan 10 punten hoger zijn dan het oordeel voor malwaredetectie. Spamfilters en andere eventuele extra's zijn niet beoordeeld.

virussen die de pakketten niet kenden omdat 'virusupdates ophalen' was uitgezet, herkenden de beste pakketten nog niet de helft, en Trend Micro zelfs geen een. Dat laat maar weer eens zien hoe afhankelijk virusscanners zijn van updates.

Opvallend was verder dat Steganos op ons test-systeem bijna vijf uur nodig had om 3 GB aan schone bestanden te scannen. Gdata bewijst dat een goede scan niet meer dan negen minuten hoeft te duren.

## Beveiligingssoftware

## Prestaties

Merk	Product	Testoordeel	Prijs <sup>1</sup>	Malware (virus) bescherming	Prestaties firewall	Blokkeren phishing sites	(De)Installatie	Gebruiksgemak	Systeembelasting	Bijzonderheden
<b>BEVEILIGINGSPAKKETTEN</b>										
▶ <b>Gdata</b>	Internet Security 2008	69	€ 55 (€ 45)	+	+	--	+	++	-/□	HNORS
<b>Bitdefender</b>	Internet Security 2008	65	€ 60	□	+	□	+	+	-/□	HNORS
<b>F-Secure</b>	Internet Security 2008	64	€ 80	□/+	+	--	□	+	□	NORS
<b>Kaspersky</b>	Internet Security 7.0 <sup>3</sup>	58	€ 70	□/+	□	--	+	+	□	HNOS
<b>Avira</b>	Premium Security Suite	56	€ 60	-/□	+	--	□	+	+	DOS
<b>Norton</b>	Internet Security 2008	54	€ 70 (€ 50)	□	□	++	□	□	□	HNR
<b>Eset</b>	Smart Security 3.0	54	€ 80 (€ 38)	-/□	□	--	□	+	□/+	NS
<b>Steganos</b>	Internet Security 2008	49	€ 70 (€ 40)	-/□	+	--	+	+	□	DNS
<b>McAfee</b>	Internet Security Suite	49	€ 70	□	□	--	□	□	□	NOS
<b>Panda</b>	Internet Security 2008	45	€ 60	-/□	+	--	□	□	□/+	HNORS
<b>Trend Micro</b>	Internet Security 2008	45	€ 60	-/□	□	--	+	+	□/+	HNOS
<b>Microsoft</b>	Windows Live OneCare 2.0	37	€ 45	-	+	□	+	□	□/+	HN
<b>CA</b>	Internet Sec. Suite Plus 2008	30	€ 65	--/-	+	--	□	+	□	DNOS
<b>ANTIVIRUS (MALWARE) SOFTWARE</b>										
<b>Alwil</b>	Avast! 4 Home Edition	49	n.v.t.	-/□	n.v.t.	n.v.t.	□	□	+	DN
<b>Avira</b>	AntiVir Personal	47	n.v.t.	-/□	n.v.t.	--	□	□	+	D

\* 0-20 = slecht, 20-40 = matig, 40-60 = redelijk, 60-80 = goed, 80-100 = zeer goed; -- = slecht, - = matig, □ = redelijk, + = goed, ++ = zeer goed, ▶ = Beste koop

Alle: geschikt voor Windows XP en Vista, geen versie beschikbaar voor Mac OS X of Linux Ubuntu  
Prijspeiling begin april 2008

<sup>1</sup> Prijs voor volledige versie (geen upgrade) met licentie voor virusupdates voor 1 jaar voor 3 computers, behalve Kaspersky (2 computers) en Bitdefender (2 jaar). Tussen haakjes de prijs voor een licentieverlenging voor een jaar extra virusupdates, indien afwijkend van de genoemde prijs

<sup>2</sup> D = Niet in winkel te koop, alleen te downloaden  
H = Nederlandstalige papieren handleiding  
N = Nederlandstalige software  
O = Ouderlijk toezicht (ongewenste websites blokkeren)  
R = Installatie-cd is tevens reddings-cd  
S = Heeft spamfilter

<sup>3</sup> In mei komt versie 8 uit

# Soorten malware

- **Bootvirus** – virus dat zich in de opstartsector van de harde schijf nestelt, dat geladen wordt nog voordat het besturingssysteem start.
- **Macrovirus** – virus dat misbruik maakt van de programmeertaal van bijvoorbeeld Word en Excel.
- **Malware** – verzamelnaam voor alle software met kwaadaardige bedoelingen.
- **Phishing-site** – Nagemaakte site, vaak van een bank, waar u naar toe wordt gelokt (bijvoorbeeld met een mailtje) om waardevolle gegevens in te vullen.
- **Rootkit** – malware die zich zeer diep in het besturingssysteem nestelt, en

- daardoor vaak onzichtbaar wordt voor beveiligingssoftware.
- **Spyware** – software die persoonlijke gegevens verzamelt over de gebruiker, bijvoorbeeld surf- en computergedrag, en deze naar een externe partij stuurt.
- **Trojaans Paard of trojan** – malware vermomd als nuttig programmaatje, dat de computer opent voor kwaadwillenden via het internet.
- **Virus** – kwaadaardige programmacode die zich in een bestand nestelt met als doel zich verder te verspreiden en schade aan te richten.
- **Worm** – zoekt zelfstandig computers om te besmetten, hoeft in tegenstelling tot een virus niet mee te liften op een ander programma.

## KWETSBAAR

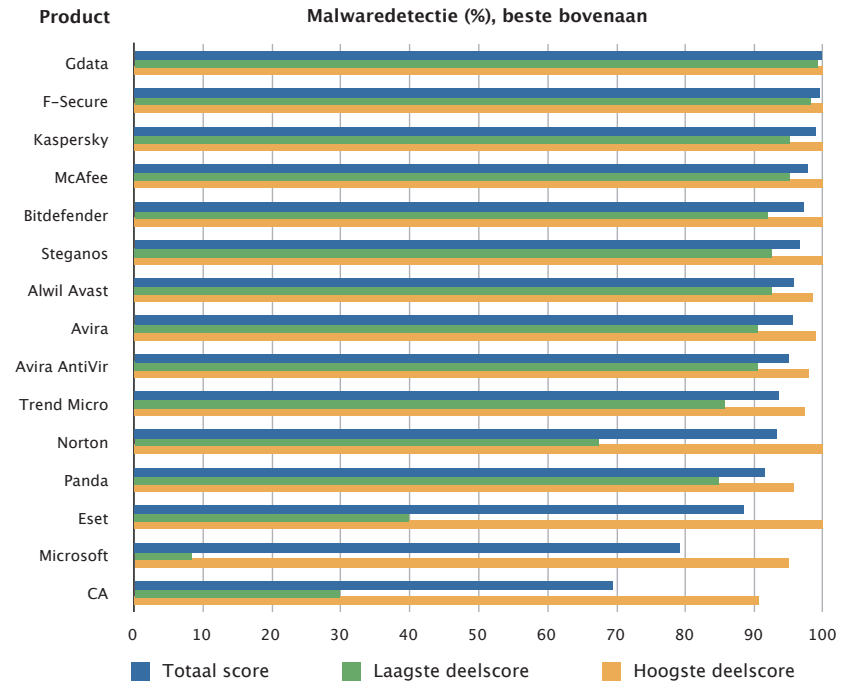
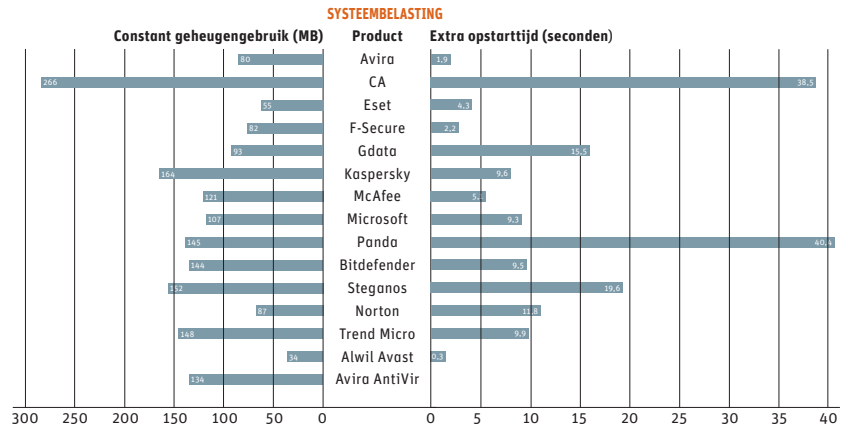
Microsoft heeft lering getrokken uit de kritiek op Windows XP, waar geen volwaardige firewall in zit, en heeft Vista standaard voorzien van een betere en gebruiksvriendelijkere firewall, die in de tabel het oordeel redelijk zou krijgen. Maar als het om veiligheid gaat, kunt u daar beter geen genoeg mee nemen.

Trend Micro valt negatief op, want het laat een poort open staan, en zet er op verzoek van buiten nog twee open. Vier pakketten (Avira, Eset, Microsoft en Bitdefender) tonen zich kwetsbaar voor een zogeheten Denial of Service (DoS)-aanval, een truc om een systeem plat te krijgen door deze te overspoelen met datapakketjes.

## VEDERLICHT

Gebruikers van oudere Norton-versies kunnen erover meepraten: een beveiligingspakket dat de pc zo traag als stroop maakt. Computers worden nog steeds sneller en hebben minder last van 'zware' software. De gratis virusscanners zijn vederlicht. Ze vertragen het opstarten amper, nemen weinig intern geheugen in en belasten de processor minimaal. De meeste – ja, ook Norton – draaien ook nog goed op een doorsneecomputer. Gdata en Bitdefender eisen zoveel systeembronnen op, dat je een snel systeem nodig hebt om er geen last van te hebben.

Ter illustratie een paar negatieve uitschieters: Panda vertraagde de opstarttijd op onze testpc met 40 seconden. Van de vrije hardeschijfruimte is na installatie van Norton, F-Secure en Microsoft een halve gigabyte minder over. Kaspersky heeft tijdens een scan maar liefst 700 MB (!) aan werkgeheugen nodig. En Gdata en Bitdefender doen zo'n zwaar beroep op de processor (80% be-



## Beveiligingstips

- Laat zo veel mogelijk automatisch de laatste updates ophalen van het besturingssysteem en andere veelgebruikte software.
- Wees op uw hoede bij het downloaden via ruilnetwerken. Daar zit nog weleens een besmet bestand tussen.
- Blijf niet te lang met oude beveiligingssoftware werken (2006 of ouder). De nieuwste versie is het best ingesteld op de laatste bedreigingen (zoals nu phishingsites).
- Zet ook de firewall in de router aan, meestal is dit standaard het geval. Ga liever niet zonder tussenkomst van een router het internet op. Een router vormt een extra barrière tussen de computers erachter en het internet.
- Open geen mailtjes van onbekenden met een bijlage, of scan in elk geval de bijlage.
- Beveilig uw Windows-account altijd met een wachtwoord.
- Zet mappen delen in Windows uit.
- Kies een draadloos netwerk met WPA-beveiliging (en zet die aan!).
- Gebruik wachtwoorden die niet makkelijk te raden zijn.
- Neem een virusscanner bij uw internetabonnement; die vormt een eerste verdedigingslinie en is meestal gratis.
- Neem ook een virusscanner als u Windows Vista heeft. Onderdeel van Vista is weliswaar Windows Defender, maar dat scant vooral op spyware en niet specifiek op virussen.
- Wees altijd alert!

lastig) tijdens het scannen van bijvoorbeeld een bestandsbijlage bij een mail, dat ons testsysteem even op slot ging.

### SCHOOLVOORBEELD

Installeren is eenvoudig. Vier pakketten (F-Secure, Panda, Steganos en Norton) bieden vóór installatie aan om het systeem te scannen. Een goede gewoonte, want aanwezige malware kan de installatie proberen te verhinderen. Alle pakketten schakelen terecht de Windows-firewall uit, twee kapiteins op één schip werkt niet. Alleen Gdata, Kaspersky, Microsoft, Steganos en Bitdefender laten bij de installatie nauwelijks sporen achter.

Een schoolvoorbeeld van een goede handleiding is die van Gdata. Minder goed leesbaar, met name voor beginners, zijn de handleidingen van Kaspersky, McAfee en Bitdefender. Veel fabrikanten leveren uit kostenoopt punt alleen nog een pdf-handleiding op cd, let daar dus op als u daar waarde aan hecht.



Voorbeeld van een onduidelijke vraag van Kaspersky's firewall

### IRRITANT

Dan het gebruiksgemak. Want wat heb je aan een auto als je niet weet hoe je hem moet besturen? Elk pakket heeft een bedieningsscherm waarin je onder meer scans kunt starten en instellingen kunt aanpassen.

Helaas staat de helft van die schermen vol onoverzichtelijke menu's. Gdata, Steganos en Norton hebben hier wel goed over nagedacht.

Prettig is dat de gebruiker bij F-Secure, Kaspersky, Alwil en Bitdefender zelf op eenvoudige wijze kan instellen wat belangrijker is: betere bescherming of een sneller systeem.

Nog belangrijker zijn de vragen die je op het scherm krijgt, zoals 'wat moet er met virus X gebeuren?' of 'mag programma Y het internet op?'. Als die vragen niet te begrijpen zijn, is dat niet alleen irritant, maar loopt u ook meteen een beveiligingsrisico. De beste pakketten nemen zo veel mogelijk beslissingen zelf en vallen de ge-

## Virusschappen

Een relatief nieuwe ontwikkeling is malware die constant nieuwe instructies krijgt, de 'payload'. Die instructie kan bijvoorbeeld zijn dat ze zich zoveel mogelijk moeten verspreiden vóór exact 12 uur, om daarna met zijn allen één specifieke computer te overspoelen met verzoekjes. Na de missie zoeken de virussen en wormen zelf weer contact met de 'herder' of 'zombiemaster' om nieuwe opdrachten te ontvangen.

bruiker zo min mogelijk lastig. De firewalls van Kaspersky en Panda doen dat wel, en blijven maar berichten afvuren op de gebruiker. De meeste anderen houden zich meer in, en als ze het doen, is het meestal ook in klare taal.

### REDDINGSBOEI

Een nuttige extra is de mogelijkheid om de installatie-cd ook als 'reddingsboei' in te zetten, mocht u toch slachtoffer zijn geworden van een virusaanval en de schade zo groot is dat Windows niet meer start. Met die cd kunt u dan toch de laatste updates van internet halen en het virus opsporen. Bij Gdata en F-Secure werkt dit het prettigst.

Tot slot is het een kleine moeite voor de fabrikant om het programma standaard voldoende veilig in te stellen. Onbegrijpelijk is dat Kaspersky de firewallbescherming standaard op 'laag' heeft gezet, en (net als Norton) geen periodieke malwarescan heeft ingepland. Avira scant standaard geen virussen die ingepakt zijn. Het virus in een zipbestand stoppen, is dan voldoende om de beveiliging te foppen. Al deze zaken zijn aan te passen, maar daar moet je als gebruiker dan maar wel opkomen. ●

## De wereld buiten Windows

Mac OS X en Linux Ubuntu hebben een firewall die minder bescherming en gebruiksgemak biedt dan die van Windows Vista. Hackers richten zich liever op de vetste vis, Windows, en er is dan ook (nog!) veel minder malware voor Mac OS X en Linux Ubuntu. Voor Mac en Linux is er op dit moment slechts een enkele (open source-)malwarescanner, de bekendste is ClamAV. Ook mobieltjes kunnen in theorie worden aangevallen, maar er zijn nog geen concrete aanwijzingen dat dit ook echt gebeurt.

## CONCLUSIE ●

GDATA IS HET BESTE PAKKET EN EEN VAN DE GOEDKOOPSTE BOVENDIEN. F-SECURE DOET HET OOK GOED EN IS EEN OPTIE VOOR WIE EEN SNELLER SYSTEEM BELANGRIJKER VINDT DAN GEBRUIKSGEMAK. BEIDE GRATIS SCANNERS PRESTEREN ONVOLDOENDE. CA EN MICROSOFT BIEDEN SLECHTS SCHIJNVEILIGHEID.

## Consumentengids Online, actueel en overzichtelijk!



Op de website van de Consumentenbond staan actuele en onafhankelijke tests! De pagina's zijn overzichtelijk weergegeven waardoor u sneller vindt wat u zoekt.

Consumentengids Online betekent:

- ▶ Actuele testinformatie op het gebied van geld en verzekeringen, elektronica en communicatie, gezondheid en voeding, vervoer en reizen.
- ▶ Handige rekenmodules en vele (aankoop)tips.
- ▶ Persoonlijk advies op maat.
- ▶ Gegarandeerd onafhankelijk en betrouwbaar.

Leden met de Consumentengids hebben al toegang. Leden met alleen een abonnement op de Digitaalguids betalen slechts €21 per jaar.

## Abonneren?

 [www.consumentenbond.nl/digitaalguidsleden](http://www.consumentenbond.nl/digitaalguidsleden)

 (070) 445 45 45

Consumentenbond

Dan weet je het.