

---

## **Waarom één virusengine niet genoeg is**

---

Om de tijd tussen virusuitbraak en signature update terug te brengen, heeft u meer dan één virusengine nodig

Geen enkele antivirusengine is altijd het snelst en het meest effectief als het gaat om het identificeren van virussen, trojans en andere dreigingen. Dit white paper legt uit hoe de installatie van twee of meer virusscanners op mailserverniveau de kans op infectie substantieel reduceert en vertelt u hoe u het best te werk kunt gaan.

---

## Inleiding

Het is bekend dat virussen, trojans, wormen, spam en andere soorten malware een dreiging vormen voor alle organisaties en een negatieve invloed hebben op de productiviteit en de bedrijfsvoering. Volgens de FBI Crime and Security Survey uit 2006 heeft 97% van de ondervraagde organisaties antivirussoftware geïnstalleerd. Daarvan zegt 65% in de afgelopen 12 maanden besmet te zijn geraakt met minstens één virus. Volgens in Network World geciteerde onderzoeken zijn bedrijven in de VS in totaal \$3,5 miljard kwijt aan de bestrijding van Blaster, SoBig.F, Sober en andere e-mailvirussen. Uit een onderzoek van de Britse overheid uit 2006 is gebleken dat 43% van de bedrijven in het Verenigd Koninkrijk in 2005 met virussen besmet is geraakt.

Organisaties met verantwoordelijkheidsgevoel zijn zich ervan bewust dat ze hun netwerk tegen virusaanvallen moeten beschermen door een product voor e-mailbeveiliging te installeren. Schadelijke codes worden echter met de dag geavanceerder doordat virusschrijvers steeds beter worden en hun codes zo schrijven dat ze virusscanners en firewalls kunnen omzeilen. Het succes van deze virussen heeft vooral te maken met de inherente zwakte van beveiligingsstrategieën die gebaseerd zijn op een enkele virusscanner om het risico van binnenkomende bestanden te beoordelen.

Is één virusengine genoeg om het interne netwerk te beschermen tegen mass-mailing virussen, wormen en andere gevaren? In dit white paper kunt u lezen dat het antwoord "NEE!" luidt. Ook wordt uitgelegd waarom u meer dan één virusengine nodig heeft om sneller op virusuitbraken te kunnen reageren en dus minder kans te lopen op infectie. Netwerkbeheerders die verschillende virusengines gebruiken zijn voor hun virusscans niet afhankelijk van één bedrijf. Op deze manier kunnen ze de beste virusengines gebruiken die er verkrijgbaar zijn.

Inleiding .....	2
Het belang van snelle reacties .....	2
Case study: Reactie op het Worm/Sobervirus .....	3
Het belang van het combineren van technologieën .....	4
Argumenten voor de inzet van verschillende virusengines .....	5
Een nieuw paradigma en een nieuwe strategie .....	6
About GFI MailSecurity for Exchange/SMTP .....	6
Over GFI .....	8

---

## Het belang van snelle reacties

Een van de belangrijkste factoren in de bescherming van uw netwerk tegen virussen is de snelheid waarmee u tijdens een virusuitbraak aan nieuwe signature files (bestanden die virussen kunnen identificeren) voor de virusengine kunt komen. Door middel van e-mail kunnen

virussen met grote snelheid worden verspreid. Een enkel e-mailvirus is genoeg om uw gehele netwerk te infecteren. De snelheid waarmee bij de uitbraak van een nieuw virus de signature files worden geactualiseerd is dus van groot belang. Bij iedere virusaanval verloopt er tijd tussen de uitbraak van het nieuwe virus en de uitgave van signatures die het virus moeten elimineren. Hoe sneller er een signature file wordt gecreëerd, des te kleiner is de kans op infectie. Hoewel 100% van de grote bedrijven in Groot-Brittannië antivirusproducten gebruikt, is 43% in 2006 besmet met virussen, grotendeels doordat men niet op tijd signature updates had geïnstalleerd. Dit is gebleken uit een onderzoek van de Britse regering uit 2005.

Iedere fabrikant van antivirusproducten beweert snel op virussen te reageren. De realiteit is echter niet zo ideaal. Antiviruslabs produceren met verschillende intervals updates voor uitbraken van wormen en virussen. Een lab kan bijvoorbeeld voor het ene virus binnen 6 uur een update produceren en maar liefst 18 uur nodig hebben voor een ander virus. Wat het nog ingewikkelder maakt is het feit dat hoewel sommige bedrijven gemiddeld beter presteren dan andere bedrijven, geen enkel bedrijf altijd het eerst en het snelst is. Sommige bedrijven zijn vaker sneller, maar de snelste bescherming wordt nooit steeds door hetzelfde bedrijf geboden. De ene keer is het Kaspersky, de volgende keer McAfee, een andere keer BitDefender of Norman, enzovoort.

Bovendien kan er vertraging optreden die niet veroorzaakt wordt door de kwaliteit van het werk of de competentie van het lab, maar de tijdzone waarin het lab zich bevindt.

## Case study: Reactie op het Worm/Sobervirus

In de onderstaande tabellen kunt u zien hoe snel diverse antivirusbedrijven op twee verschillende dreigingen hebben gereageerd.

**Tabel 1 – Reactietijden van antivirusbedrijven na de uitbraak van w32.Sober.C**

Bedrijf	Reactietijd in uren (afgerond op een half uur)
BitDefender	10.5
Kaspersky	12.0
F-Prot (Frisk)	12.5
F-Secure	13.0
Norman	15.5
eSafe (Alladin)	15.5
TrendMicro	17.0
AVG (Grisoft)	17.5
AntiVir (H+BEDV)	19.5
Symantec	25.0

Avast! (Alwil)	31.0
Sophos	35.5
Panda AV	38.0
McAfee/NAI	49.0
Ikarus	56.5

Spreiding: 10,5 uur – 56,5 uur, mediaan: 17,5 uur, gemiddelde: 24,53 uur. Bron: VirusBTN, februari 2004

**Tabel 2 – Reactietijden van antivirusbedrijven na de uitbraak van w32.Sober.Y**

Bedrijf	Reactietijd in uren (afgerond op een half uur)
AntiVir	11.5
McAfee/NAI	40.5
Kaspersky	43.0
Norman	60.0
BitDefender	114.5
Symantec	116.0
ClamAV	164.5
TrendMicro	168.0
Panda	168.0
Sophos	170.0

Spreiding: Spreiding: 11,5 uur – 170,0 uur, mediaan: 115,75 uur, gemiddelde: 105,6 uur. Bron: av-Test.de, november 2005

Zoals u ziet bedragen de verschillen uren of zelfs dagen – dit is meer dan genoeg tijd om geïnfecteerd te raken!

## Het belang van het combineren van technologieën

Ieder viruslab en iedere scanengine is anders. Er is geen engine die de beste is. Iedere engine heeft zijn sterke en zwakke punten. Antivirusproducten gebruiken vaak een combinatie van technologieën om virussen te detecteren en te bestrijden. De drie meest gebruikte benaderingen zijn:

- **Signature files** die regelmatig door antiviruslabs worden geproduceerd en uitgegeven en die informatie bevatten aan de hand waarvan een virus geïdentificeerd kan worden. Antivirusengines worden meestal geactualiseerd door middel van signature files.
- **Heuristieken** worden gebruikt voor de detectie van virussen en andere dreigingen waarvoor nog geen signature files zijn ontwikkeld. Ze kijken naar diverse kenmerken van een bestand, beoordelen deze kenmerken en geven aan welke waarschijnlijk virussen zijn. Deze methode

kan ook metamorphische virussen (virussen die kunnen muteren) detecteren. Deze zijn hardnekkig bestand tegen signature files.

- **Sandboxing** isoleert verdachte code en voert deze uit op een virtuele machine die los staat van de rest van de IT-infrastructuur om te bepalen of het om schadelijke code gaat.

Elk van deze technologieën kan zeer effectief zijn, maar geen enkele is 100% succesvol. Hoewel sommige antivirusproducten twee of meer van deze technologieën combineren, is geen enkele oplossing de beste. U kunt uw netwerk het best beveiligen met een beveiligingssysteem dat uit verschillende lagen bestaat. Dit kunt u bereiken door verschillende antivirusengines te gebruiken.

---

## **Argumenten voor de inzet van verschillende virusengines**

PC SecurityShield schat dat er elke dag meer dan 40 nieuwe virussen worden gevonden. Microsoft heeft in juni 2006 bericht dat 1 op de 300 PC's geïnfecteerd was met malware. Het is ook belangrijk om te onthouden dat de huidige omgeving van malware die zich continu verder ontwikkelt het werk is van een enorm aantal onafhankelijke ontwerpers van malware die elk een individualistische benadering hebben en ieder een eigen aanvalsstrategie hanteren.

Het argument voor het gebruik van meer dan één virusengine is eenvoudig: de realiteit leert dat geen enkele antivirusengine alles doet. Er is geen enkele antivirusengine die altijd de snelste, de effectiefste en “de beste” is. Als u een engine met de snelste gemiddelde reactietijd heeft, dan is dat ook alles. Het houdt niet in dat deze engine bij de volgende virusuitbraak de snelste zal zijn. Dan heeft u niet veel aan het feit dat deze engine de snelste gemiddelde reactietijd heeft. Wat belangrijk is, is dat uw netwerk geïnfecteerd is geraakt – met mogelijk rampzalige gevolgen. De infectie en de “crash” van het systeem kunnen leiden tot productiviteitsverlies, verlies van klanten, downtime en verhoogde bedrijfskosten.

Bovendien kan af en toe een onjuiste antivirusupdate voorkomen doordat antivirusbedrijven constant proberen om bij virusuitbraken zo snel mogelijk updates uit te brengen. Als u maar één antivirusengine heeft, heeft u in zo'n geval dus geen bescherming.

### **Een woord van waarschuwing**

Hoewel het gebruik van verschillende virusengines een superieure oplossing is, is het belangrijk om te onthouden wat u precies krijgt. Met vijf antivirusengines beschikt u NIET over vijf keer zoveel bescherming. U heeft vijf kansen op het goede antwoord en statistisch gezien is elk van de vijf onafhankelijk. U kunt het vergelijken met vijf controlepunten op een vliegveld. De vijf controles zijn min of meer hetzelfde maar iedere controle is een beetje anders. Zo is de kans groter dat een dreiging op tijd wordt gevonden.

### **Constante aanvallen verzwakken de beveiliging**

Zoals we eerder hebben gezien is uit onderzoek van FBI/CSI gebleken dat 65% in de

afgelopen 12 maanden het slachtoffer is geweest van één of meer virusaanvallen. De schade bedroeg bijna 16 miljoen dollar. Vrijwel alle respondenten gebruikten echter antivirussoftware. Dat ze er niet in slaagden hun netwerk adequaat te beschermen is vrijwel zeker te wijten aan het feit dat ze slechts één antivirusengine hadden.

### **In alle andere vormen van beveiliging worden verschillende lagen gebruikt**

U zult waarschijnlijk moeite hebben om een organisatie te vinden die slechts één beveiligingsmedewerker of alarmsysteem heeft om haar meest waardevolle fysieke activa te beschermen tegen verschillende soorten dreigingen zoals diefstal, vandalisme, brand en natuurrampen. In plaats daarvan bestaat de verdediging uit verschillende lagen, bijvoorbeeld beveiligingsmedewerkers, bewakingscamera's, sprinklers en kluisen, die allemaal beschikken over back-ups systemen voor het geval dat er iets mis gaat.

Uw informatie (uw meest waardevolle bezit!) verdient een even veelzijdige bescherming. Deze kan alleen worden geboden door verschillende antivirusengines. U kunt het zich niet veroorloven om op andere methodes te vertrouwen.

---

### **Een nieuw paradigma en een nieuwe strategie**

Aangezien het overduidelijk is dat één virusengine onvoldoende is om uw netwerk te beschermen, is het logisch dat u een andere strategie dient aan te wenden. Organisaties moeten een gelaagde scanoplossing implementeren die verscheidene engines combineert en zo meer kans biedt dat in ieder geval één van die virusengines op tijd wordt bijgewerkt. Met meer dan één virusengine heeft u tevens meer kans dat u over de juiste combinatie van technische mogelijkheden beschikt om bepaalde dreigingen af te weren en is de kans dus groter dat uw netwerk beschermd is.

Hoewel er geen perfecte oplossing bestaat, vergroot het gebruik van vier of vijf antivirusengines met een multiple engine manager zoals GFI MailSecurity for Exchange/SMTP uw kansen op effectieve, tijdige bescherming van uw netwerk. Bovendien hoeft u niet meer op één fabrikant te vertrouwen.

---

### **About GFI MailSecurity for Exchange/SMTP**

GFI MailSecurity voor Exchange/SMTP is een e-mailbeveiligingsoplossing met exploitdetectie, dreigingsanalyse en virusbestrijding die alle soorten dreigingen verwijdert voordat ze uw gebruikers kunnen bereiken. GFI MailSecurity scant alle e-mail met verschillende virusscanners, waaronder Kaspersky, McAfee, BitDefender, Norman en AVG Anti-Virus. Andere belangrijke functies zijn een module voor het checken van de inhoud van e-mails en attachments om gevaarlijke inhoud en attachments in quarantaine te kunnen plaatsen; een exploit shield voor bescherming tegen huidige en toekomstige exploits (bijvoorbeeld Nimda en

Bugbear); een HTML threats engine voor de uitschakeling van HTML-scripts; en een Trojan & Executable Scanner voor de detectie van schadelijke executables. Kijk voor meer informatie en een trialversie op <http://www.gfi.nl/nl/mailsecurity/>.

---

## Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

