

Why one virus engine is not enough

Multiple virus engines are needed to reduce time lag between virus outbreak and signature update

This white paper explains the importance of response time, shows the response time differences between virus engines, and explains why having multiple scanners at mail server level decreases the average response time and therefore the chance of virus infection.

Introduction

Responsible organizations agree that they need to protect their networks from virus attacks by installing an email security product. Yet, how does one choose the right solution out of the wide variety of virus scanning engines available? And is one anti-virus engine enough to protect the internal network from mass-mailing viruses, worms and other email-borne threats?

This whitepaper explains the need for multiple virus engines to reduce the average response time to a virus outbreak, and thus reduce the chance of having your network infected. The use of multiple virus engines also enables security administrators to be vendor independent when it comes to virus scanning, thereby able to use the best of breed virus engines available on the market.

Introduction.....	2
The need to have a fast response time.....	2
Case in point: Response to Sober virus.....	2
The case for multiple virus engines.....	3
About GFI MailSecurity for Exchange/SMTP.....	4
About GFI.....	4

The need to have a fast response time

One of the most important factors in the successful protection of your network against viruses is how fast you get new virus engine signature files when there is a virus outbreak. Email allows viruses to be spread at lightning speed in a matter of hours, and a single email virus is enough to infect your whole network. Obviously then, a critical factor is how fast the signature files of your anti-virus solution are updated when a new virus emerges.

A 2004 study by the UK government found, for example, that although 99% of large British companies use anti-virus products, 68% of them were infected by viruses during 2003, largely because virus signature updates had not been deployed fast enough.

Every anti-virus vendor in the market will claim to have a fast virus response. However, reality clearly demonstrates otherwise. While, on average, some companies perform better than others, there is no one company that will always be the first and fastest to respond to a virus outbreak. Granted, some companies may be faster on more occasions, but it is never always the same company that delivers virus protection the first. One time it is Kaspersky, the next it is McAfee, another time BitDefender or Norman, and so on.

Case in point: Response to Sober virus

The table below illustrates the response times of anti-virus companies (CET) to the outbreak of

W32/Sober.C (worm discovered on 20 December 2003 at 03:00 h, CET).

Company	Response time
BitDefender	2003-12-20 at 13:20 h
Kaspersky	2003-12-20 at 14:45 h
F-Prot (Frisk)	2003-12-20 at 15:25 h
F-Secure	2003-12-20 at 15:45 h
Norman	2003-12-20 at 18:25 h
eSafe (Alladin)	2003-12-20 at 18:35 h
Trend Micro	2003-12-20 at 19:50 h
AVG (Grisoft)	2003-12-20 at 20:15 h
AntiVir (H+BEDV)	2003-12-20 at 22:20 h
Symantec	2003-12-21 at 04:05 h
Avast! (Alwil)	2003-12-21 at 09:55 h
Sophos	2003-12-21 at 14:35 h
Panda AV	2003-12-21 at 17:05 h
McAfee/NAI	2003-12-22 at 04:10 h
Ikarus	2003-12-22 at 10:35 h

Data taken from the February 2004 VirusBTN issue

Clearly the differences range from hours to even days. Symantec, for example, took more than a day to deploy new signature files - more than enough time to allow your network to get infected!

The case for multiple virus engines

Unfortunately having an engine with the fastest *average* response time will not help you if that engine was not the fastest for a particular virus, resulting in your network being infected that one time. Given the inability of any individual anti-virus engine to always be the first to release a signature update for a new virus, logic dictates that combining multiple engines will greatly increase your chance of at least one of those virus engines being updated on time, and therefore increases the chances of your network being protected.

In simple terms, having say three or four virus engines increases your chances of getting network protection on time threefold! This way, you do not have to rely on one vendor to be one of the fastest each and every time, but can instead hedge your bets on three or four anti-virus vendors.

About GFI MailSecurity for Exchange/SMTP

GFI MailSecurity for Exchange/SMTP is an email content checking, exploit detection, threats analysis and anti-virus solution that removes all types of email-borne threats before they can affect your email users. GFI MailSecurity's key features include multiple virus engines, to guarantee higher detection rate and faster response to new viruses; email content and attachment checking, to quarantine dangerous attachments and content; an exploit shield, to protect against present and future viruses based on exploits (e.g., Nimda, Bugbear); an HTML threats engine, to disable HTML scripts; a Trojan & Executable Scanner, to detect malicious executables; and more. For further information and to download a full trial, please visit <http://www.gfi.com/mailsecurity/>.

About GFI

GFI is a leading provider of network security, content security and messaging software. Key products include the GFI FAXmaker fax connector for Exchange and fax server for networks; GFI MailSecurity email content/exploit checking and anti-virus software; GFI MailEssentials server-based anti-spam software; GFI LANguard Network Security Scanner (N.S.S.) security scanning and patch management software; GFI Network Server Monitor that automatically sends alerts, and corrects network and server issues; GFI LANguard Security Event Log Monitor (S.E.L.M.) that performs event log based intrusion detection and network-wide event log management; and GFI LANguard Portable Storage Control that enables network-wide control of removable media. Clients include Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, the US IRS, and the USAF. GFI has offices in the US, the UK, Germany, Cyprus, Romania, Australia and Malta, and operates through a worldwide network of distributors. GFI is a Microsoft Gold Certified Partner and has won the Microsoft Fusion (GEM) Packaged Application Partner of the Year award. For more information about GFI, visit <http://www.gfi.com>.

© 2005 GFI Software Ltd. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.

