

Why one virus engine is not enough

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

There is no single anti-virus engine on the market today that is always the fastest and most effective at identifying viruses, trojans and other threats. This white paper examines why having multiple anti-virus scanners at mail server level substantially reduces the chance of virus infection and explores ways in which this can be achieved.

Introduction

It is a well known fact that viruses, trojan horses, worms, spam, and other forms of malware present a real threat to all modern-day organizations and affect productivity and business operations negatively. According to the 2006 FBI Crime and Security Survey, 97% of organizations have anti-virus software installed, yet 65% have been affected by a virus attack at least once during the previous 12 months. Network World cited studies that placed the cost of fighting Blaster, SoBig.F, Sober and other email viruses at \$3.5 billion for US companies alone. Similarly a 2006 study by the British government found that 43% of companies in the United Kingdom were infected by viruses during 2005.

Responsible organizations agree that they need to protect their network from virus attacks by installing an email security product. Yet malicious code is becoming more sophisticated and is advanced everyday as virus writers hone their skills and sharpen their code to stay one-step ahead of virus detection methods, penetrating anti-virus and firewall solutions with alarming regularity. The success of these viruses is, to a large part, linked to the flawed logic and inherent weakness of protection strategies that are based on a single scanning engine to assess the threat of incoming files.

This white paper explains why the answer to the question: “Is one anti-virus engine enough to protect the internal network from mass-mailing viruses, worms and other email-borne threats?” - is an emphatic “NO!” It also examines the need for multiple anti-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 study: Response to the Worm/Sober virus	3
The need for blending technologies	4
The case for multiple anti-virus engines.....	5
A new paradigm and strategy.....	6
About GFI MailSecurity for Exchange/SMTP	6
About GFI	7

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 – those files released by anti-virus labs that help to identify a virus 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. In every virus attack there is a time differential between the outbreak of the new virus and the release of signatures to defeat and eliminate it. The faster a signature file is created, the less likely the chance of an infection. A 2006 study by the UK government found, for example, that although 100% of large British companies use anti-virus products, 43% of them were infected by viruses during 2005, largely because virus signature updates had not been deployed fast enough.

Every anti-virus vendor in the market claims to have a fast response time. However the reality is not quite so sanguine. Anti-virus labs produce updates for virus and worm outbreaks at different intervals. For example, the same lab may produce an update for one virus within six hours, yet take 18 hours for the next one. Complicating the matter further is that 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 the same company that delivers protection the first. One time it is Kaspersky, the next it is McAfee, another time BitDefender or Norman and so on.

Time differences may also occur that are not the result of the quality of the work or the competency of the lab, but reflect their geographic location and time zone related factors.

Case study: Response to the Worm/Sober virus

The tables below illustrate the response time of anti-virus companies to two separate threats.

Table 1 – Response times of anti-virus companies to the outbreak of w32.Sober.C

Company	Time to respond in hours (closest half hour)
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

Range: 10.5 hours - 56.5 hours, Median: 17.5 hours, Mean: 24.53h

Data taken from the February 2004 VirusBTN issue

Table 2 – Response times of anti-virus companies to the outbreak of w32.Sober.Y

Company	Time to respond in hours (closest half hour)
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

Range: 11.5 hours - 170.0 hours, Median: 115.75 hours, Mean: 105.6

Data taken from av-Test.de for November 2005

Clearly, the differences range from hours to even days – more than enough time for your network to get infected!

The need for blending technologies

Every virus lab and scan engine is different. When it comes to protection there is no single best engine, each has its own strengths and weaknesses. Anti-virus products often use a mix of technologies to detect and defeat viruses. The three most common approaches are:

- **Signature files** which are prepared and released by anti-virus labs on a regular basis and contain details that help identify a virus. Signature files are the usual way anti-virus engines are updated.
- **Heuristics** are used to detect viruses and other threats that have not yet had signature files developed for them. Essentially they look at different characteristics of a file, assess the characteristics and flag those that appear to be viruses. This method can also detect and catch metamorphic viruses (viruses that can mutate) which are notoriously resistant to signature files.
- **Sandboxing** isolates and executes suspicious code in a virtual machine isolated from the

rest of the IT infrastructure to determine if it's malicious or not.

Individually each of these technologies can be very effective, but none are 100% successful. While some anti-virus products combine two or more of these technologies, there is no single best solution. The only effective way to assure the highest level of safety and security is by a multi-layered in depth defense which can be achieved by using multiple anti-virus engines.

The case for multiple anti-virus engines

PC SecurityShield estimates that over 40 new viruses are found every day. In June 2006, Microsoft reported that 1 out every 300 PCs were infected with malware. It is also important to remember that today's environment of constantly evolving malware is the product a legion of independent malware designers, each with an individualistic approach and attack strategy.

The argument in favor of using multiple anti-virus engines is simple and is predicated on the simple reality that there is no single anti-virus engine that does everything. There is no single anti-virus engine that is fastest, most effective and "the best" all the time. If you have an engine with the fastest average response time then that is all you have. It doesn't mean it will be the fastest for the next virus outbreak. It doesn't mean much if that engine was not the fastest for that particular virus or wasn't equipped with the right mix of technologies and heuristics, what matters is that your network was infected that one time – with potentially disastrous consequences. The results of the infection and effective "crash" of the system can include lost productivity, lost business, downtime and increased business costs.

Furthermore, from time to time, erroneous anti-virus engine updates might seep through since anti-virus vendors are constantly trying to release updates as quickly as possible to combat an outbreak. Relying on one single anti-virus engine will fail in such an event as viruses might bypass the erroneous single anti-virus protection, whilst multiple anti-virus engines will provide a backup.

A small caution

While using multiple anti-virus engines is a superior solution, it is important to remember precisely what you are getting. Having five anti-virus engines does NOT provide you with five times the protection. It provides you with five opportunities to have the correct answer, each of which are, statistically speaking, independent events. It can be thought of as passing through five security check-in points at an airport where each security check is more or less the same though each does something slightly different, and thus increases your chances of catching a negative event before it happens.

Constant attacks attrite defenses

Referring back to the previously cited 2006 FBI/CSI study where it was reported that 65% had been affected by a virus attack at least once in the immediately preceding 12 months costing

US organizations almost 16 million dollars. Yet virtually all of the respondents were users of industry-recognized anti-virus software. The failure to protect could almost certainly be tracked back to reliance on a single anti-virus engine.

Multiple layers are used in all other forms of security

It is unlikely that you will find an organization that relies on a single security guard or alarm system to protect its most valuable physical assets from a variety of different threats such as theft, vandalism, fire and natural disaster. Instead, there is a multi-layered defense that might consist of security guards, surveillance cameras, sprinkler systems and vaults – all of which have back-up systems in the event of failure.

An organization's data, the most valuable asset of all, requires the same multi-faceted defense system, and that can only be provided by multiple anti-virus engines. You can't afford to trust to any other method.

A new paradigm and strategy

Since it is obvious that single scanning engine defenses are insufficient for the protection of your network then logic dictates a different strategy. Organizations need to implement a layered scanning solution that combines multiple engines to greatly increase chances of having at least one of those virus engines updated on time. Multiple virus engines might also result in the right mix of technological capabilities for any particular threat, thus increasing the chances of your network being protected.

While nothing is perfect, having four or five anti-virus engines running simultaneously through a multiple engine manager such as GFI MailSecurity for Exchange/SMTP immeasurably increases your chances of getting effective on-time network protection. It also frees you from reliance on the ability of a single vendor to respond promptly and appropriately.

About GFI MailSecurity for Exchange/SMTP

GFI MailSecurity for Exchange/SMTP is an email security solution that provides exploit detection, threats analysis and anti-virus, effectively removing all types of email-borne threats before they can affect an organization's email users. GFI MailSecurity uses multiple virus scanners to scan all email, which include Kaspersky, McAfee, BitDefender, Norman and AVG Anti-Virus. Other key features include an email content and attachment checking module, 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; and a Trojan & Executable Scanner, to detect malicious executables. For further information and to download a full trial, please visit <http://www.gfi.com/mailsecurity/>.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, Adelaide, Hamburg and Cyprus which support more than 160,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at <http://www.gfi.com>.

© 2006 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 EndPointSecurity, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor 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.

