SOPHOS

Assessing endpoint security solutions:
why detection rates aren't enough

Evaluating the performance of competing endpoint security products is a time-consuming and daunting task. Enterprise decision-makers have to rely on independent competitive comparisons, performance benchmarks, and detection certifications, all covering different solutions and criteria, providing conflicting results. This paper highlights the pitfalls of simply looking at virus detection rates and investigates the effect of the rapidly developing IT environment and fast-moving threat landscape on assessment criteria. It gives the six critical questions businesses need to ask to ensure the most successful outcome to their evaluations.

A Sophos white paper

March 2008

Assessing endpoint security solutions: why detection rates aren't enough

The primary reason for an organization to buy an endpoint security solution is to protect its network, systems and data from malware. It is tempting, therefore, to base an assessment of potential solutions largely on malware detection rates.

In reality, however, detection tests – no matter how thorough – provide only a snapshot of a security vendor's ability to provide ongoing manageable protection. There are several other equally important criteria that should be taken into account. It is in the vendors' approach to these extended security factors that the clearest difference between competing products emerges, allowing a viable shortlist to be created for further evaluation.

First, however, it is important to have an understanding of the changing security environment, in which increasingly open networks and a rapidly evolving threat landscape are presenting IT with new and significant challenges.

> *Detection tests provide only a snapshot of a security vendor's ability to provide ongoing manageable protection.*

The dissolving IT perimeter

It used to be relatively easy to secure the corporate network. It was a physically connected entity used only by internal users. Web browsing was not generally available at the desktop, and data was transferred only by removable media or email.

Today, networks as we once understood them are disappearing as the network perimeter has become blurred by the prevalence of new technologies and business practices. Instant Messaging (IM), Voice Over IP (VoIP), peer-to-peer (P2P) file-sharing software, and wireless and mobile devices all offer new ways of transferring data. Network access is given to remote workers, business partners and contractors.

These changes fulfil the real business need to remain competitive, but they also increase the risk of malware and other threats infecting the network via unsecured hardware and unmonitored communication channels.

The changing nature of security threats

Malware is now big business and large criminal gangs, with considerable IT resources, have replaced fame-seeking teenagers as the primary source. The threats they create are low-profile, silent and targeted to avoid the attention of their victims and security vendors alike. These threats do not crash computers or delete files; they steal passwords and financial information.

In addition, today's threats change with increasing frequency, looking to avoid detection. Over the course of 2007, around 50,000 variants of the Storm (aka Dorf or Dref) worm were seen.[1]

There has also been a significant change in the routes used by malware for attack. A move away from infected email attachments – in 2005, 1 in 44 emails had an infected attachment, compared with 2007's 1 in 909 – has been matched by an increase in the use of blended threats, which use several different technologies to spread their malicious payload.

The challenge for IT

The changes in network environment and the speed and complexity of threats raise major new security challenges for IT. Solutions are needed that go far beyond simply installing up-to-date anti-virus software at regular intervals. They need to address the much wider issues that now exist:

- More infection routes and more types of endpoint device need securing
- All endpoint computers need assessing and controlling
- Compliance with security policy needs monitoring
- Fast-moving, zero-day threats demand effective proactive protection.

One answer to the problem is to buy numerous point solutions but, on the whole, IT budgets are not increasing to meet the new requirements. Another drawback is that point solutions increase the total cost of ownership since more security solutions mean:

- More initial purchase and set-up costs
- Slower networks
- More management effort
- Increased support issues (especially when the solutions conflict).

How blended threats work – an example

An email is spammed out containing a link to an infected webpage.

When the link is clicked on by the recipient, a script on the webpage triggers the download of a Trojan onto the user's computer. The Trojan being downloaded might change several times a day to avoid detection.

Once downloaded, the Trojan might download more files and malware to the infected computer – which might in turn download more malware before delivering the actual payload.

For these reasons, there is an increasing trend away from point solutions towards more consolidated products. Yet despite getting "total protection" from "integrated solutions" businesses are still getting infected.

So how does an organization ensure best protection?

6 critical questions to ask vendors

To ensure that a vendor not only provides best protection now, but is also best placed to address the IT challenges an organization will face going forward, there are a number of important questions that should be asked.

QUESTION 1
How good is your malware detection?

Totally reliable malware detection remains the primary driver behind any decision to buy an endpoint security solution.

Since the risks involved make testing possible solutions against real malware infeasible, organizations have to rely on word-of-mouth, reviews, and results from independent testing organizations.

Malware detection tests can regularly be found in the media and they can be very useful in comparing the performance of rival security vendors. However, care should be taken to understand what is, and is not being tested – what malware collection methodologies have been used, has the product been used with its default settings or specifically configured, and so on. In drawing up a shortlist of potential vendors, it is also important to look at several tests and not to rely on one test alone.

A good test should include the following:

- **On-access testing**. Tests that simply scan a set number of malware samples in on-demand mode, do not accurately reflect the real world threat from malware or the real detection capabilities of solutions that incorporate runtime analysis or HIPS (Host Intrusion Prevention System) functionality.
- **Several thousand malware samples.** With over 5 million unique malware samples seen in 2007[2], any test with fewer than 1000 samples cannot be considered to be statistically significant.
- **All types of malware**. Tests that analyze single types of malware, such as looking only at traditional viruses, give no indication of the products' ability to detect the wide variety of other malware. Some tests, for example, do not include Trojan horses even though they account for the vast majority of malware seen today.
- **False-positive testing**. Most endpoint security solutions can score 100% detection in particular tests. The important issue is that they do not at the same time quarantine clean files.
- **Proactive/zero-day detection tests**. The changing nature of threats makes proactive detection the first line of defense against today's malware, ensuring protection from threats before they have been seen and analyzed by experts in the vendor's labs.
- **Response times**. Signatures to protect against specific viruses and other malware remain a significant part of successful protection, and the speed with which the vendor creates and deploys them is important. A combination of response times and proactive detection gives a comprehensive indication of the real protection a particular solution will provide.

Although no one test organization is perfect, organizations that provide more comprehensive and representative testing include AV-Test.org[3], AV-Comparatives.org[4], Virus Bulletin[5], ICSA Labs[6], Cascadia Labs[7], and West Coast Labs[8].

QUESTION 2
Do you have integrated visibility of all threat sources?

The increased use of blended threats shows how important it is for vendors to have integrated visibility of spam, virus and web-based threats in order to ensure a rapid response to new malware as it is released. For example, vendors without anti-spam capabilities will not see the email that is used to propagate the link to an infected website. Similarly, without a web-monitoring capability, a vendor cannot tell when an infected website is established or get early insight into new malware made available through that website – and with one infected webpage every 14 seconds[2] this lack of visibility is critical.

Even if the vendor does have this cross-threat capability, it needs to be supported by integrated research laboratories with information being rapidly and automatically passed between them to ensure a quick response to all new threats.

QUESTION 3
How good is your proactive, zero-day protection?

Today's criminally motivated, targeted, fast-moving threats have decreased the time available for security vendors to react to new threats before they have their malicious impact. This problem is exacerbated by the sheer volume of threats, with vendors' research labs having to protect against hundreds of thousands of new threats every year. Such large volumes of rapidly mutating malware require proactive, zero-day protection, against malware that the vendor has not yet seen or analyzed.

Vendors need to offer both:

- Pre-execution analysis – examines the behavior and characteristics of files before the file is run to find traits commonly found in malware.
- Runtime protection – analyzes the behavior of files and processes as they are running, checking for suspicious activity.

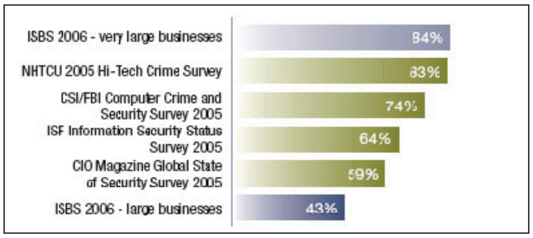
Strong proactive protection reduces the number of individual threats that a research lab needs to analyze, enabling the rapid creation of new signatures and protection where necessary.

> *Point products for antivirus, antispyware, personal firewalls, and Host Based Intrusion Prevention (HIPS) are rapidly being replaced by suites with a centralized and extensible management framework. The management and reporting capability of EPP (Endpoint Protection Platforms) suites is a substantial differentiator especially in large enterprise. A modular architecture that allows selective configuration based on security requirements and device location is also critical.*
>
> *Gartner, Magic Quadrant for Endpoint Protection Platforms 2007*[9]

QUESTION 4
Is your solution easy to manage across my network?

A security solution will only protect the network if it is correctly configured, deployed and updated across the whole network. So its ease of use and ease of management should be given almost as much weight as its detection capabilities in the evaluation process.

The vulnerabilities created by security solutions that are difficult to manage are highlighted by surveys variously indicating that between 43 percent and 84 percent of large businesses suffered from a malicious code infection in 2005/6, even though 100 percent had implemented an anti-virus solution.[10]



Businesses infected by malicious code 2005/6[10]

Similarly, on replacing one solution with another vendor's solution, it is common for an organisation to find a large amount of malware on the network – not because the earlier solution could not detect the malware but because it had not been kept up to date or managed properly.

In addition to offering visibility of the network, some security solutions support the management task further by automatically identifying endpoint computers that are out of date with security software or policy, or by automatically deploying anti-malware software to new endpoint computers logging on to the network.

Other solutions also ease the administrative burden by making management actions that cannot be automated easier and quicker to perform. By reducing the need for administrators to understand and write complex rules for determining suspicious behavior, these products help make the network more secure and free up more time to be spent on other IT matters.

QUESTION 5
What added value does your solution offer?

Higher volumes and increasing complexity of threats are not mirrored by a similar trend in the IT budgets set out to counter them. Adding ever more point products and IT staff to combat these additional risks and protect increasingly open networks is not realistic.

So an important question to ask is, "How will this vendor's security solution allow me to get more out of my existing budget?" The answer lies in how successfully the solution will defend against the new set of threats posed by user behavior and poorly configured or non-compliant computers, in particular how far it lets organizations control who and what is on the network.

Capabilities to look for beyond straightforward protection against malware include:

- Restricting use of legitimate but non-business-critical software applications – like VoIP, IM and P2P software – that can cause productivity, support and security issues.

- Reducing the risk of infection by ensuring security policy is being complied with by all computers – not just those owned and managed routinely by the company but also those unmanaged guest computers connecting to the network.

- Assessing and certifying systems before and after they connect to the network, ensuring, for example, that security software is in place and properly configured, and operating system and application patches are up to date.

Comprehensive endpoint security

» Anti-virus
» Anti-spyware/adware
» HIPS (Host Intrusion Prevention System)
» Firewall
» Network access control
» Application control
» Device and data control

In addition to protection from malware and control of applications and network access, an endpoint security solution might offer device control and data leakage prevention. By offering some, if not all, of these capabilities a good endpoint security solution will reduce the financial, network performance and management costs, and increase efficiency through being one product to understand, deploy and manage.

QUESTION 6
What level of support can I expect?

Vendor support is an important aspect of the successful implementation of endpoint protection. Although hard to test it needs to be taken into account during the evaluation process.

Help might be needed from the vendor at various times over the lifetime of the license, either to do with the product itself, for example to do with deployment, configuration, or updating, or over a related issue, such as the discovery of a suspicious file on the network that needs analyzing. Given that security may be at risk until the matter is resolved, it is important to understand the vendor's policy towards support – is 24/7 support standard or is this something that requires extra payment?

Some vendors will limit the number of contacts that are allowed to call with technical queries, which is not helpful where a quick resolution is required. Some – especially those with large consumer customers to support – will use off-shore support centers to provide economies of scale, but these often prove unpopular with businesses.

One further area that should be investigated is how integrated product support is. Will a single support analyst be able to address issues across the vendor's entire product range or will different products require separate, time-consuming conversations?

Conclusion

Detection of malware is at the heart of any endpoint security solution and comprehensive published detection rates are a valid source of information. However, good malware detection rates alone will not guarantee the best protection. The most successful solutions are easy to manage, provide proactive protection against zero-day threats, and offer other security capabilities, such as HIPS, application control, firewall, and network access control. Underlying these should be 24-hour threat analysis from integrated global research labs, and technical support from cross-product experts. By assessing potential products against all these criteria, organizations will go a long way to ensuring they choose the right endpoint security solution to protect them against today's rapidly evolving threats and increasingly open network environment.

Sophos solution

Sophos Endpoint Security and Control provides proactive malware detection and preventive protection. A single integrated scan detects viruses, spyware, adware, potentially unwanted applications (PUAs), suspicious files, suspicious behavior and unauthorized applications such as VoIP, IM, P2P and games. New and unknown threats are proactively stopped by Sophos HIPS technology along with rapid signature updates. Simplified management functionality reduces administration burden by enabling centralized and automated deployment, updating, alerting and reporting across Windows, Mac and Linux platforms, safeguarding the integrity of the entire network. SophosLabs™ – our global network of threat research centers – analyzes web and email traffic 24 hours a day to secure and protect against any new virus, spyware, spam, or web-based threat anywhere in the world, irrespective of origin. Web, email and telephone support is included in all licenses.

Sources

1 Sophos Security Threat Report 2008
www.sophos.com/security/whitepapers/sophos-security-report-2008

2 news.bbc.co.uk/1/hi/technology/7232752.stm

3 av-test.org

4 www.av-comparatives.org

5 www.virusbtn.com

6 www.icsalabs.com

7 cascadialabs.com

8 www.westcoast.com

9 Gartner Research, "Magic Quadrant for Endpoint Protection Platforms, 2007", P Firstbrook, A Hallawell, J Girard and N MacDonald. December 21, 2007.

10 Information Security Breaches Survey 2006 – DTI
www.infosec.co.uk/files/Survey_DTI_ISBS_2006.pdf

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.COM