

Benefits and Considerations for a Single-Vendor Antivirus Strategy

An IDC Executive Brief, June 2002

Analysts: Natasha David and Jane Chesher



The world is a much smaller place than it was ten, five, even two years ago. The virus outbreaks that occurred in 2001 which spread so quickly and caused such damage to organisations around the globe are an indication of things to come. The lowered technical barriers needed to script such viruses and malicious mobile code is ensuring these types of outbreaks are likely to keep recurring. Additionally, increased globalisation coupled with the use of email as a key communication tool makes understanding your security options a vital concern.

The Virus Landscape

Melissa and the Lovebug were only the start of new viruses aimed at servers and mail gateways. On the desktop, IDC predicts a whole new range of viruses and malicious applets. These applets will creep into many enterprises and unfortunately, a high percentage of mobile code attacks will go undetected.

The following graph from the Computer Emergency Response Team (CERT) demonstrates the exponential rate with which virus incidents are growing. In the past five years, there has been a compound annual growth rate of 83%.

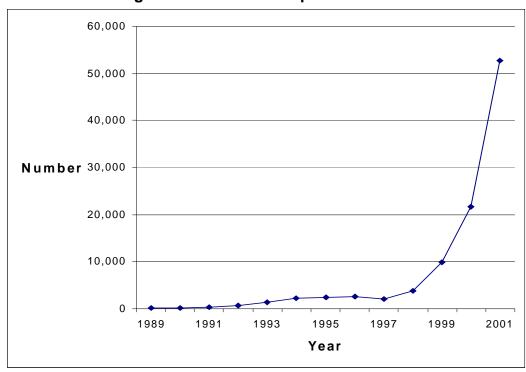


Figure 1: Increase in Reported Incidents

Source: CERT, 2002

Figure 1 does not show the number of viruses that are released to the wild each year, but rather illustrates the number of organisations who report a breach by a virus. While there are only about 200 viruses circulating at any one time, the frequency of each virus incident is increasing, particularly those attached to mass-mailers.

There has also been an increased threat over the past year from new forms of viruses that are "hybrids", or "blended threats". These blended threats differ from traditional viruses and worms. These so-called polymorphic viruses have multiple points of infection and propagation and are capable of doing damage in many ways. Examples are Nimda, Code Red and Sadmind. As these hybrids are designed to get past point solution security systems, they will require multi-layered protection on gateways, server and clients.

Unlike traditional viruses, which rely on the user to spread the infected files, hybrid threats are automated and are always scanning the Internet and local networks for vulnerabilities and other computers to infect. In this way, they spread without user interaction.

Finding the Right Solutions

1. Antivirus Software

Antivirus (AV) software prevents and cures attacks from viruses and malicious mobile code (e.g. rogue ActiveX and Java applications).

Because the Internet now delivers most viruses, AV software is increasingly sold as a networked, rather than a desktop, application. Corporate environments are migrating to serverbased and gateway implementations because most viruses are network and/or mail based. Mail gateways are a major new platform because of Melissa's rapid infection of Exchange servers.

Some AV vendors have developed platform independent management consoles to manage AV implementations across the entire network. This is an especially important development because enterprises with multiple sites are demanding a console for managing hundreds to thousands of AV applications on distributed servers.

As illustrated in Figure 2, there are three points where AV products can be implemented to protect corporate networks from outbreaks:

- Gateway an IP server that interfaces between the external network (outside the firewall) and the internal network. It is at this point that firewalls, proxy servers and messaging servers can be candidates for an AV strategy
- Server the platform on which all applications, network devices and databases are deployed
- Desktop all organisations now have many users that are all able to access email and Internet applications. These are still vulnerable from viruses via floppy disks and wireless devices

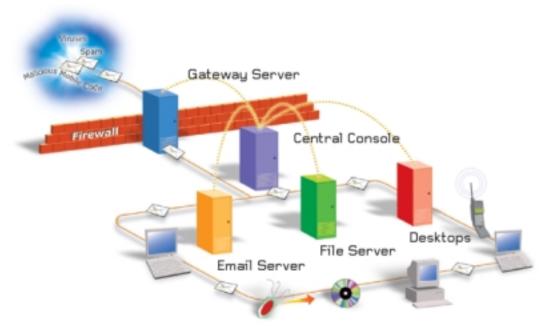


Figure 2: Points of Infection/Protection

Source: Trend Micro, 2002

2. Single-Vendor Strategy

Single-Vendor Strategy describes the practice of implementing one vendor's products on all three points into the network (gateway, server and desktop).

3. Multi-Vendor Strategy

Multi-Vendor Strategy describes the practice of implementing products from two or more vendors' products on all three points into the network (gateway, server and desktop).

4. Virus Signature

A virus signature is a unique bit string that is common to each copy of a particular virus and that may be used by a scanning program to detect the presence of the virus.

Evolution of the Antivirus Strategy

Historically, AV vendors were advising users to load more than one AV product on their systems. Around 1992 to 1994, this was the acceptable practice for organisations. This was because most viruses spread via floppy disks, so it was highly likely any outbreak would be localised. Additionally, these outbreaks were typically written by local virus writers. For example, a virus in the wild of Slovakia had little chance of making it to Australia, England or the United States. Organisations would run one international AV product and one good local product. The locally derived product would cover local outbreaks much quicker than those created by international vendors.

This scenario has now changed with the shift in the way viruses spread, in that the Internet and email have become primary carriers. In this way, a virus in the wild in China can spread throughout the world in less than 24 hours, as we have seen with Melissa and CodeRed. Access to virus signatures and incorporating these in AV product quickly has become less of a competitive difference amongst AV vendors. Most commercially available AV products now detect the same viruses; in fact, most leading AV vendors are all members of CARO (Computer Antivirus Research Organisation), where virus samples can be shared amongst the vendor community within one hour.

Today organisations are more likely to use two vendors' products due to legacy issues. For example, organisations running on platforms such as DOS, 3X as well as Linux or varieties of Unix may find it difficult to run only one AV product across all these platforms.

Key Benefits for a Single-Vendor Approach

There are a series of important benefits for an organisation to reflect upon when developing their AV strategy.

1. Lower Total Cost of Ownership

AV Product Suite

Using the one vendor to protect gateway, server and desktops will lower the total cost of ownership, as products are typically bundled into suites. By bundling a suite of products, AV vendors typically offer a lower total price than the sum of list prices for

each component. There are also hidden costs to consider such as the need to manage and renew multiple licences, often at different times of year. While renewals may not be an issue if organisations choose to purchase the products at the same time, the management of multiple AV products could be costing an organisation in administration overheads as well as the IT administration staff's time.

Lowering Internal Support

Additionally, using one vendor's products will result in lowered internal support and training costs, as staff only need to be trained on one product.

Cost of Protection

Choosing the right security strategy ultimately comes down to cost of protection. Organisations should calculate the value of the assets it is trying to protect. If these assets are worth \$10,000, for example, it makes no sense spending more than this amount in protection.

2. Simplifying Administration

Central Console

Leading vendors provide central consoles to manage multiple AV products across a network, as described in Figure 2. By using two or more vendors' products, an organisation eliminates the central control functionality and introduces the issue of consolidating logs for reporting. Under a multi-vendor strategy, administrators may need to use four or more consoles to manage and update their AV products.

Standardise Interface

AV vendors also typically standardise their interface layouts for all AV products. A single-vendor strategy ensures management is consistent across all AV products, which again simplifies administration.

Virus signatures

While it is certainly true that AV vendors collaborate in providing new virus signatures that have been detected in the wild, these vendors also use different name formats for these viruses when updating their products. This can cause confusion when an organisation goes to update its AV products in a multivendor scenario, and can sometimes hinder effective virus response and management.

3. Ease of Updates

Update Schedule Management

Some vendors provide one universal virus signature for all AV products. Organisations with a single-vendor AV policy are therefore only required to download one file per update, rather than one or more files per vendor. Vendors also release program version upgrades at different times of the year. A single-vendor policy allows an organisation's administrator to keep a straightforward schedule in terms of updates. New signature updates are currently available every few days, and this trend is increasing rather than decreasing. To manage and download these files across multiple systems could become very confusing and time consuming.

Reduced Bandwidth Disruption

By using a single vendor that offers a universal update for gateway, server and desktop installs, deployment of the update across a network will ensure that disruption to network resources is minimalised. This is important considering signature updates can exceed 5 megabytes, with the size and frequency only set to increase.

4. Response to virus outbreaks

ISO Certification

Because management and speed of updates is faster with a single-vendor policy, deployment of updates in virus outbreak scenarios is faster provided a vendor's pattern development process is ISO-certified. If an infection does occur, the infection can be more easily traced and rectified in a single-vendor scenario rather than having to use multiple consoles and deal with different virus name formats.

5. Support

Local Technical Assurance

When an organisation purchases a licence, it is not simply buying product, but also access to updates and technical support. Whether a single user or large corporation, a large outbreak will give rise to the need to contact someone for assurance. With increasing complexity of new viruses, it is becoming harder to protect and clean all possible viruses and variances of viruses. Access to local support in the same time zone is critical to managing outbreaks.

One Support Team

Organisations with a single-AV vendor policy also gain benefits from using one vendor support team. This is important in terms of consistent technical support as well as escalation processes.

Additional Points for Consideration

While there are obvious benefits in considering a single vendor strategy, there are also issues for an organisation to consider:

- There is a potential risk of price increase out of step with AV industry. However, this can work either way, as the AV software market has become more mature and, as such, more price sensitive and competitive
- There is also the risk of lock-in to one vendor as staff members become familiar with one particular product. The ability to switch vendors is more difficult to overcome in the face of internal resistance
- This also leads to the risk of an inability to take advantage of any new product development if the current AV vendor does not continue to invest in AV development

Call To Action

The decision to choose either a single or multi-vendor strategy should be made by considering all issues. The most important issue obviously centres on quality of protection. However, this should be considered alongside the overall cost of that protection.

While a multi-vendor policy can increase the chance of getting virus updates, this is less of an advantage as it historically was. In fact, in light of the speed of infection, having multiple vendors' AV products to administer and update may actually be a hindrance to quality of protection.

This document was adapted from research published as part of an information service also available by subscription from IDC, providing written research, analyst-on-call, e-flashes, telebriefings and conferences. Visit www.IDC.com to learn more about IDC's subscription and consulting services. Please contact Jane Chesher at ichesher@idc.com or 61-2-9925 2238 for additional copies or Web rights for this document or for related documents.

Quoting IDC Information and Data: Internal Documents and Presentations — Quoting individual sentences and paragraphs for use in your company's internal communications does not require permission from IDC. The use of large portions or the reproduction of any IDC document in its entirety does require prior written approval and may involve some financial consideration. External Publication — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2002 IDC. Reproduction is forbidden unless authorized.