Management Update: What You Should Know About the Antivirus Market

As hacking and virus cyber-incidents soar, enterprises are fighting back. Firewalls and gateway antivirus systems are examples of first-generation, network-based intrusion prevention systems. Gartner discusses the antivirus market and personal firewalls, and presents its Enterprise Antivirus Magic Quadrant.

As hacking and virus cyber-incidents soar, enterprises are trying to fight back. Firewalls and gateway antivirus systems are examples of first-generation, network-based intrusion prevention systems. Gartner discusses the antivirus market, personal firewalls and antivirus vendors, including Gartner’s Enterprise Antivirus Magic Quadrant.

Information Security: A Growing Problem

The purchase and support of traditional, signature-based antivirus (AV) solutions take up the largest portion of IT budgets allocated to information security. (An AV signature file is used to detect the presence of known viruses.) Indeed, during the past five years, the emergence of macros and e-mail and Internet worms have transformed malicious code management for enterprises. Enterprises are spending increasing amounts on product licenses, signature and product update testing and distribution, and clean-up and incident response.

Despite spending more, many enterprises actually experience more downtime and costs because of malicious code infections. Internet worms such as Nimda and Slammer exploit server-based vulnerabilities and simply bypass installed AV products. Peer-to-peer (P2P) and Web services also bypass gateway controls and thus require new desktop controls. Moreover, despite more regular signature updates, many viruses spread so rapidly that enterprises are infected before the AV vendor can produce the signature, let alone provide time for enterprises to test and deploy signatures to the desktops.

Signature-based AV products are now relegated to the routine detection of variants and other “routine noise” viruses. Enterprises must look beyond traditional AV for controlling their risk of malicious code infection. That will require enterprises not only to look at new tools, but also to choose vendors and platforms based on their histories of vulnerabilities, patch management and end-user lockdown strategies.
The Antivirus Market Evolution

Key Issue: How will the antivirus market evolve?

The market for AV is changing rapidly for those that supply and purchase AV technologies. Historically, AV has held a position outside the mainstream security market. Those that manage and implement IT are desktop, LAN, e-mail or network groups, rarely the security organization. AV tools, because they are implemented on a large number of machines and platforms, also resemble network and systems management (NSM) products.

Indeed, the manageability of AV remains a huge product selection criterion. However, as the weaknesses in signature-based AV becomes apparent, AV product selection and implementation must become more integrated into core security areas. At the same time it must be even more widely dispersed into platform or NSM requirements.

AV products, except for e-mail, are typically bought on a stand-alone basis. However, AV product considerations should now include consideration of other relevant products. Behavior blockers, lockdown products and personal firewalls require significant technology usage changes and executive buy-in. Enterprises must consider the role of the network as well as host intrusion detection system or even emerging security management systems. In addition, third-party products for instant messaging, mobile code scanning, anti-spam and URL blocking and content filtering are also increasingly necessary, because AV vendors have failed to integrate best-of-breed technology in those areas with their AV solutions.

Turmoil in the AV Market

Tactical Guideline: Regard traditional signature-based AV as a tactical, legacy solution for virus management.

Until recently, the enterprise AV market was frequently dismissed as a saturated and increasingly commodity market. However, viruses continue to be the biggest security challenge for enterprises, and they account for a large portion of enterprise spending on security. Moreover, the emergence of macros and e-mail as the predominant vector for virus infections during the past five years has resulted in continued strong growth for the largest AV vendors, especially from products for e-mail servers.

A number of factors are driving the evolution of the AV market.

- Virus management remains the No. 1 security “pain point” for enterprises.
- Customers make AV decisions primarily based on management functionality and quality of platforms.
- E-mail AV is only one component of wider e-mail security products.
- Signature-based AV on the desktop will be supplemented and replaced by other functionality.

During the past five years, the virus risk has changed substantially. Viruses are created more frequently and can infect enterprises at a rapid-fire rate, often before a software update is available from the AV vendor, and before the enterprise can distribute the update to relevant platforms. The need for continual updating already has enterprises buckling under the costs and effort involved.
Current AV approaches simply will not be enough to counter emerging malicious-code threats, such as those posed by the vectors of instant messaging and P2P applications, active content and Web applications for malicious-code infection.

Weaknesses in Enterprise Antivirus Offerings

Tactical Guideline: Central management and reporting functionality and remote access support should be considered primary selection criteria for desktop AV and personal firewalls.

Strategic Planning Assumptions:

- Through 2005, third-party products, rather than AV products, will be required to manage instant messaging security, granular active content policies and anti-spam (0.7 probability).

- AV vendors with personal firewalls will capture less than 50 percent of the personal firewall market by 2005 (0.6 probability).

Despite new, ambitious visions, AV vendors have glaring weaknesses in their enterprise AV offerings. For example, the primary complaint is the cost and difficulties associated with keeping signatures up to date at the desktop.

Until recently, however, most AV vendors ignored the need to develop better management functionality that would enable easier updating and managing of AV products and virus outbreaks. Similarly, products for Lotus Notes and Exchange are frequently quite unstable, and HTTP virus scanning solutions for large enterprises create substantial performance problems.

AV products still do not easily support remote users, and partners and customers without up-to-date AV signatures can’t be routinely blocked from entering an enterprise’s networks. In addition, although research capabilities among the AV vendors have significantly improved, the developments have not been passed on to customers.

Most notably, many enterprises have complaints about AV vendors concerning the quality of their products, the necessity of frequent patches, the quality of updates, and less-than-desirable service and support responsiveness.

The basic requirements that enterprises should expect from their AV product vendors are:

- Product stability and compatibility on specific platforms
- Management and reporting functionality
- Quality and timeliness of products and updates
- Remote access and support of machines not owned by the enterprise

However, some requirements may not come from an AV vendor, such as:

- Policy enforcement at the desktop
- Automated responses and security management
- Support of emerging threats, active content, instant messaging and P2P
AV and Anti-Spam Vendors and Evaluation Criteria

Strategic Planning Assumptions:

- By 2005, non-AV vendors will supply the majority of e-mail AV functionality (0.8 probability).
- Consolidation among anti-spam providers will continue through the end of 2003, leaving less than five enterprise anti-spam vendors (0.8 probability).
- Prices for anti-spam will fall by more than 50 percent by 2004 (0.8 probability).

AV products for e-mail, Notes, Exchange and SMTP (Simple Mail Transfer Protocol) were major growth areas for AV vendors during the past five years. Non-AV vendors are now gaining ground. Many enterprises are implementing anti-spam technologies and services, but the technology and market are immature, and enterprises face risks from investing in nascent services. Some of the risks are lack of production implementation references, small vendors that may be acquired or go out of business, high product prices, and unknown ownership and administration costs.

For their technology selections, many enterprises want AV, and they have other e-mail security requirements, such as content filtering or message encryption. Therefore, enterprises must decide whether they want a managed service, appliance, or software for anti-spam, and whether to include AV in their requirements or select products on a piece-by-piece basis.

E-mail AV (either on Exchange/Notes or at the SMTP gateway) is often evaluated separately from the rest of enterprise AV technology decisions, but some enterprises buy AV suites that include licenses for all platforms, or they want to manage all AV from a central console (see Figure 4). The AV vendors are also starting to provide their own anti-spam technologies, but the best-of-breed anti-spam vendors have more implementations and dedicated expertise. Anti-spam pricing is quite high — typically, $4 to $10 per seat per year. Appliances and some products are sold on a software product basis.

Figure 4

Antivirus and Anti-Spam for E-Mail: Technology Choices
Personal Firewalls

Strategic Planning Assumption: By 2004, 75 percent of corporate laptops will be preconfigured with personal firewall software (0.7 probability).

The three segments to the desktop security platform are: virtual private network (VPN), AV and personal firewall. A fourth segment, file encryption, would protect data after theft of the computer.

When enterprises began to use the Internet in the mid-1990s, it became apparent that corporate networks and servers were not secure enough to allow them to be exposed to attacks from the Internet. Firewalls arose as a simple means of putting security at the edge of the network, without having to build security into every server and subnetwork.

In the mobile environment, people carry our computers around with them. In the near future, people will be carrying a networked set of computers, as their cell phones, personal digital assistants and laptops intercommunicate over IrDa (Infrared Data Association), Bluetooth and 802.11b networks. Gartner believes this will require every person to carry a personal firewall to protect those “networks in motion.” Personal firewalls should be deployed on all laptops used for remote access VPNs or wireless LAN access because they are a second line of defense. The critical ingredient will be a lightweight agent for employee-owned PCs.

The Enterprise AV Magic Quadrant

Gartner’s Enterprise Antivirus Magic Quadrant plots the market position of enterprise AV vendors along Ability to Execute and Completeness of Vision axes (see Figure 5).
The criteria for vision include:

- **Viability.** Strong and proven track record for successful technology partnerships and the acquisition of relevant technologies. Gartner believes that best-of-breed technologies and products will continue to dominate enterprise selection of security products.

- **Products and technology.** Plans for the support of desktop policy enforcement and automated lockdown, as well as hardware-based solutions for HTTP scanning.

- **Features and functionality.** Plans for functionality that enables the blocking of network access to partners without up-to-date AV software, and better support of remote or mobile workers, including integration with VPN and personal firewalls. Plans for management console tie-in to firewall and intrusion detection systems where necessary.

- **Service and support.** Commitment to quality through service levels, as well as incident response that is tied to policy “signatures.”

**Microsoft’s AV Management Role**

*Strategic Planning Assumptions:*

- **By 2008,** 80 percent of enterprises will use the Microsoft Longhorn operating system’s embedded policy controls, rather than third-party desktop software for behavior blocking and malicious code detection (0.6 probability).

- **By 2008,** behavior policies, malicious code, anti-spam and security incident updates will be purchased as research services and delivered via application programming interfaces, or APIs (0.8 probability).
Microsoft’s role in enterprise virus management has long been debated. For the past four years, it has offered APIs for AV scanning for Exchange, but until recently, enterprises and AV vendors preferred workarounds for performance and stability reasons. The virus-scanning API has become more pervasive, and Microsoft continues to add new rules functionality in Office and with Titanium. The XP personal firewall is less successful. Gartner does not believe it is appropriate for enterprise requirements, and third-party products are needed.

Microsoft has ambitious visions for the next desktop operating system, Longhorn, which will embed greater policy lockdown capabilities. Longhorn and Trusted Computing represent a grand vision of identity and security management put forth by Microsoft: a set of operating system capabilities and new applications tied to new hardware-resident functions that purport to offer identity, system integrity, enhanced security and rights management functionality.

The Trusted Computing design is able to authenticate and run trusted code that cannot be observed or modified, as well as being able to uniquely identify the machine in various ways. This ambitious project will also require an immense change in corporate technology usage culture. If successful, third-party AV and personal firewall products will seldom be necessary, although Microsoft will not provide update services.

**Bottom Line**

- Enterprises should regard signature-based AV at the desktop as legacy technology and conduct negotiations with AV vendors under that assumption.
- Plan to replace purely signature-based detection at the desktop by 2006.
- Effective virus management will require integration with patch management and other security technologies; executive support of a more restrictive technology usage culture will be necessary.
- Start evaluating personal firewall and desktop lockdown requirements and implementation strategy. Begin the budget allocation process. Some enterprises will start with remote users first, and others should implement on a group-by-group basis.
- E-mail AV is incorporated into wider e-mail security and productivity products and services.
- Effective virus management will require enterprises to redefine their technology usage and adoption culture, incorporate patch management, and wider security strategy.

Written by Edward Younker, Research Products

Analytical sources: Arabella Hallawell and Richard Stiennon, Gartner Research

*This article is an excerpt of a chapter from a new Gartner report, “Securing the Enterprise: The Latest Strategies and Technologies for Building a Safe Architecture.” The report is an offering of the Gartner Executive Report Series, a new business venture of Gartner Press that provides buyers with comprehensive guides to today’s hottest IT topics. For information about buying the report or others in the Executive Report Series, go to www.gartnerpress.com/executivereports.*

For related Inside Gartner articles, see:

- “CIO Update: Enterprise Security Moves Toward Intrusion Prevention,” (IGG-06042003-03)
• "Management Update: Security Strategies for Enterprises Using Web Services," (IGG-05282003-02)

• "CIO Update: Gartner’s IT Security Management Magic Quadrant Lacks a Leader," (IGG-04092003-04)

• "CIO Alert: Follow Gartner’s Guidelines for Updating Security on Internet Servers, Reduce Risks," (IGG-02122003-02)