

Enterprise Antivirus 2Q02 MQ: Room for Improvement

Antivirus product and service quality, as well as management functionality, remain the most important criteria for enterprise antivirus protection.

Core Topic

Security and Privacy: Security Tools, Technologies and Tactics

Key Issue

Which vendors will dominate the auditing, assessment and integrity management markets during the next five years?

The enterprise antivirus market is composed of vendors that sell enterprise products for detecting, and sometimes cleaning, viruses and other malicious code on a number of platforms. When evaluating vendors that provide enterprise antivirus products, Gartner weighs the Magic Quadrant evaluation criteria according to the technology challenges and business climate that enterprises face in the short-term 18-month planning period (see "Expect Turmoil in the Enterprise Antivirus Market," M-16-7359).

Magic Quadrant Evaluation Criteria

The Magic Quadrant is a graphical framework that places a particular set of vendors from a specific technology industry sector into a strategic matrix. Gartner assesses a vendor's capabilities according to the requirements of Gartner's midsize to large enterprise clients. We use a combination of objective and subjective criteria to evaluate individual vendors in four areas:

- Viability
- Products and technology
- Features and functionality
- Service and support

These four areas are evaluated along two dimensions:

Completeness of vision (x-axis): Rates the vendor's strategic plan for its antivirus products, and its industry and technology knowledge. Vision is primarily assessed by the current breadth, depth and quality of the vendor's products and services, and its vision and capabilities to create and sustain appropriate technology partnerships. A vendor's vision track record, such as anticipating new customer requirements, is evaluated in this category.

Gartner

Entire contents © 2002 Gartner, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

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 antivirus software, and better support of remote or mobile workers, including integration with virtual private network (VPN) and personal firewalls. Plans for management console tie-in to firewall and intrusion detection systems (IDSs) where necessary.
- *Service and support*: Commitment to quality through service levels, as well as incident response that is tied to policy "signatures."

Ability to execute (y-axis): Rates the fiscal and physical ability of the vendor to execute against its vision. In addition to business performance and financial resources, we also evaluate the vendor's install base; strength of channel; technology partnerships; quality and timeliness of research; service and support; quality and breadth of product offerings; ease of installation; and management of the product line. Access to complementary security products, such as personal firewall, VPN, vulnerability assessments and IDSs, are also evaluated.

Criteria for ability to execute include:

- *Viability*: Strong business and financial base. Antivirus vendors must support a plethora of products, desktop, file servers, enterprise e-mail servers and HTTP scanning, on an increasing number of platforms. In addition, although some antivirus research has become more automated, new malicious-code threats are continually emerging that will affect peer-to-peer, active content, Microsoft .NET and Web services, and will require continual, sustained investment in research. In addition, antivirus vendors with access to complementary research on application, server and network vulnerabilities will be at an advantage when these become more-frequently exploited by malicious-code programs. Enterprises can't ignore the important network effects of a large install base, especially on the desktop, for research purposes. However, a large install base and extensive

research capabilities can't make up for poor quality or unstable products on a particular platform.

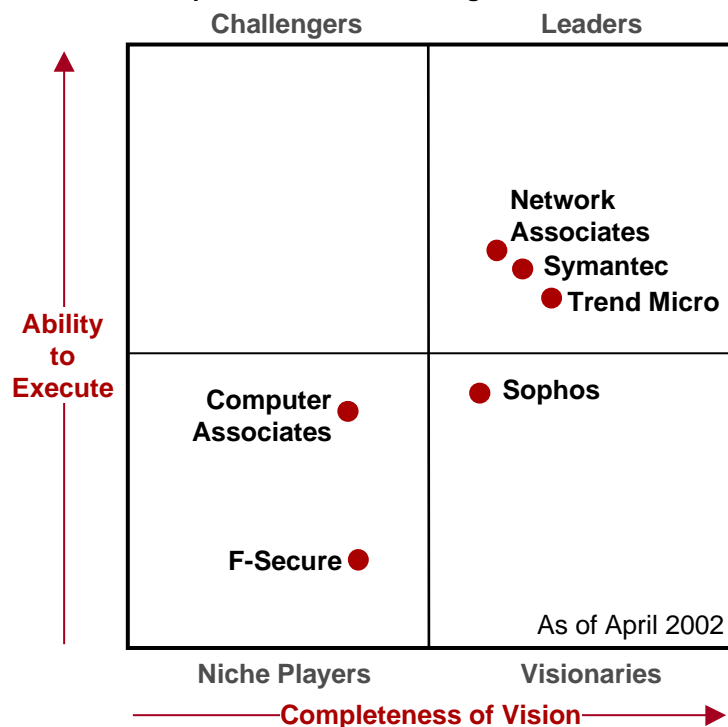
- *Products and technology:* The quality and stability of the antivirus vendor's current product offerings, especially for Lotus Notes and Exchange.
- *Features and functionality:* A good Web-based management console that enables easy installation, the central management of antivirus products, support for remote users, automated updating of signatures from enterprise servers and comprehensive reporting. The inherent management capabilities within the vendor's solutions are weighted heavily. Complementary features, such as content blocking at the SMTP gateway and firewall, are also evaluated.
- *Service and support:* Timeliness and quality of updates, especially in emergency outbreak situations, and overall service and support.

The Enterprise Antivirus 2Q02 Magic Quadrant

To be placed on the enterprise antivirus 2Q02 Magic Quadrant (see Figure 1), the vendor must:

- Own its antivirus engine
- Provide products for the desktop, file servers, the SMTP gateway, and FTP and HTTP traffic
- Provide inherent management and distribution capabilities
- Sell and support its products to midsize and large enterprises worldwide

Figure 1
Enterprise Antivirus 2Q02 Magic Quadrant



Source: Gartner Research

Leaders

Trend Micro was responsible for shaking up the traditional rivalry between Symantec and McAfee. Since Trend entered the North American market more than five years ago, it has been the product leader for enterprise e-mail servers and for Internet gateways and firewalls. Trend also was the first major antivirus vendor to offer a more-automated, centralized approach to desktop antivirus protection. Gartner believes that Trend's suite of antivirus products and management, especially with its products for Lotus Notes and Exchange, is the strongest in the market.

Trend has reacted adeptly to changing security trends and customer expectations, and it delivers timely, quality products. Despite these strengths, Trend still has not managed to significantly penetrate the enterprise desktop antivirus market in North America and Europe. Rapid growth also has led to some product quality and customer support problems.

Gartner believes that Trend will continue to have a strong vision in this space. However, as a stand-alone antivirus vendor, Trend must rely on strong partnerships with key technology vendors (that is, appliances, VPN and intrusion detection) and must work hard to ensure its survival. To date, Trend has faltered in executing on initial announcements with partners. Trend must increase its desktop presence in North American and European

enterprises, and it must continue to deliver leading HTTP solutions for large enterprises. Most importantly, Trend must ensure consistent, high-quality products and services to have a chance of unseating its larger rivals.

Network Associates has achieved a significant comeback since the company's near-fatal problems came to a head in 2000. However, recent revelations of accounting irregularities from that period continue to haunt the company. Network Associates' strengths with its McAfee antivirus product line are in its global install base and "mind share."

McAfee also has significantly improved its antivirus product offerings with the introduction of ePolicy Orchestrator (EPO) in 2001. EPO — in addition to the new antivirus desktop product line, Active Virus Defense — provides the type of light-client, centrally managed architecture that Trend Micro introduced with Trend Virus Control System in 1998, and which EPO now surpasses in terms of features and functionality. McAfee introduced the E500 appliance for SMTP and HTTP virus scanning, which has been popular with midsize enterprises. McAfee is also the only vendor to provide managed antivirus services for the desktop and file servers. In 2003 and 2004, Gartner believes managed antivirus services will be more heavily adopted by midsize enterprises, and by all enterprises for remote users and partners.

McAfee's product suite is weakened by its patchy products for Lotus Notes and Exchange, and by ongoing customer concerns with service and support. McAfee should strengthen its technology partnerships, especially since the cutting of Gauntlet and its network intrusion detection system (IDS) products. McAfee recently announced a partnership with ISS (see "Security Vendors Will Reap Marketing Gain from Partnership," FT-16-5290) that offers a new channel for the antivirus gateway products and managed antivirus services.

Gartner believes that McAfee should improve its personal firewall and better integrate it with antivirus protection, as well as develop partnerships with VPN vendors. The company must include policy enforcement and protection from P2P malicious-code threats at the desktop to maintain its presence in this area.

Symantec has garnered a strong presence in the enterprise market compared to its corporate base five years ago. The acquisition of Intel's and IBM's antivirus businesses in 1998 helped to improve Symantec's penetration of the enterprise market.

Symantec continues to be a leader in the antivirus market. Symantec's portfolio of enterprise security products (gained via the acquisition of Axent Technologies) will help to retain its strengths in malicious-code research and in developing automated policy enforcement using these products. Symantec has a strong vision for the changing nature of the malicious-code threat. The recent introduction of Symantec's Gateway Security appliance for antivirus scanning, firewall and network IDS is a first for the antivirus market.

However, apart from the appliance, Symantec has not had a strong track record over the past five years in delivering timely products and features to meet emerging customer requirements. For example, Symantec was slow to deliver products for Lotus Notes and Exchange, and we continue to hear stability complaints from customers. Also, Symantec has not integrated these products or the SMTP gateway products into its central management system. Symantec's management system currently offers limited automation and reporting capabilities compared to Trend's and McAfee's management functionality.

Visionaries

Sophos has a long and strong history in offering antivirus protection to corporate enterprises. Sophos has a particularly strong reputation for the quality of its products, updates and customer service. Its traditional strength has been at the desktop and its broad support of server platforms. Sophos' recent introduction of products for Exchange, Lotus Notes and the SMTP gateway gives the company a full enterprise suite of products.

Sophos has been active and successful in extending its presence and reputation via relationships with technology partners and service providers such as Sybari Software, CipherTrust and Mirapoint. Partnerships are integral to the company's continued growth in the antivirus market. Sophos should be wary of channel conflict as it builds its own products instead of partnering for new platforms. It also should focus on creating strong partnerships with VPN, personal firewall and security management vendors.

Niche Players

Computer Associates (CA) has a broad range of security technologies that were gained by acquisitions, which have been branded under the eTrust umbrella. CA is focusing its security strategy on building more-sophisticated security management capabilities that will leverage Unicenter's event management and correlation functionality. However, CA's antivirus product line is not directly related to these efforts.

CA has improved its inherent management and distribution functionality within the antivirus products. Also, CA has mobile code management technology through its acquisition of Security 7.

Client dissatisfaction with CA antivirus products is common. CA's products for Lotus Notes and Exchange have been unstable and lack management capabilities. Its timeliness of updates, as well as its quality of service and support, also have been criticized by customers. CA must improve its SMTP gateway and HTTP offerings, and must develop more partnerships with security and messaging service providers and technology vendors.

F-Secure (formerly Datafellows) is a Finnish antivirus vendor that has a long history in the antivirus space, and has expanded into the wider security market in the past five years. However, the consolidation that has marked the antivirus market over that same time period, and F-Secure's tardiness in developing products for e-mail servers and the Internet gateway, have eroded its mind share and market share in the enterprise market. However, F-Secure remains well-regarded in the Western European market and has strong desktop, file server and personal digital assistant antivirus products, which are bolstered by central management functionality.

Vendors Not on the Magic Quadrant

Aladdin Knowledge Systems (eSafe) and Panda Software meet most of the basic inclusion criteria and have references from large-scale enterprise deployments. They are not included on the Magic Quadrant because they have not generated sufficient user demand through Gartner client-driven inquiries to enable accurate quadrant placement.

Acronym Key

EPO	ePolicy Orchestrator
IDS	Intrusion detection system
MQ	Magic Quadrant
P2P	Peer-to-peer
VPN	Virtual private network

Bottom Line: New malicious-code threats will create upheaval in the mature enterprise antivirus market. However, enterprises should continue to evaluate antivirus vendors on the basis of product and service fundamentals: quality, management functionality, and research and support.