IDC OPINION

Endpoint security (EPS) software centrally manages, surrounds, protects, and defends desktop and mobile computing environments (clients). By enforcing security at the endpoint, high-speed broadband users and distributed enterprises are better protected against an ever-increasing number of personal, financial, and technical security threats.

The threat landscape has primarily changed into an organized and profitable vehicle for writing viruses, spyware, and other malicious code. For this reason today's threats are more serious and are increasingly complex to be tackled with a traditional security approach. Clients and desktops are typically the last — and often only — line of defense against the new threat ecosystem. Therefore, IDC believes that a more user-centric approach to protecting digital assets is paramount.

In addition to antivirus and firewalls, properly implemented endpoint security requires additional technologies that also need to be centrally manageable (e.g., antispam, antispyware, and application control) as well as adaptively adjustable to new threats and environments.

To make matters more complicated, the IT ecosystem is changing at a fast pace with increased numbers of uniquely different mobile devices and a widening variety of networking environments only being the tip of the mobility iceberg. Employee productivity, remote access, and centralized access control add to the list of challenges. Managing and ultimately securing the distributed enterprise will be key for organizations small and large in the future. Endpoint security will be a crucial component in the future security mix.
Changing Security Ecosystem

Introduction

Security does not equal insurance. Large organizations increasingly view security as a very positive infrastructure element. This change was driven by the need to expand trusted relationships with customers, partners, suppliers, and channels. The greatest asset belonging to most companies is content (formerly known as data). The ability to use security technologies (e.g., authentication and authorization) to enable greater access to corporate content deepens and stabilizes relationships. These "trusted relationships" can yield numerous benefits, such as higher transaction rates with greater scalability, lower cost per transaction, and transference of personnel from low-value interactions to high-value personalized service. Overall, customers increasingly use security products and services to help them dramatically scale revenue, transactions, and/or customers at high double-digit rates while confining cost increases to single-digit or low-double-digit rates. If implemented successfully, this ensures profitable growth.

IT security for corporate environments has changed considerably in the past three years. The increased number of laptops connecting to broadband access points outside corporate premises combined with a broader use of networking applications exposes the IT infrastructure to new vulnerabilities while increasing the complexity of system management. The latest viruses and worms, such as Sasser, spread incredibly quickly and, in bypassing conventional antivirus software, automatically infect corporate workstations. Adding to this danger, the number of spyware and adware incidents in corporations has rapidly increased during the last 12 months. Together, the viruses, worms, spyware, and network intrusions now represent a more complex threat than has ever been conceived. The clear trend in the added complexity of Internet threats indicates that a conventional antivirus solution is no longer enough.
When looking back at the history of the IT industry, there have been at least three different, clearly identifiable phases within it. In the PC-centric era, the majority of PCs did not have network connectivity and viruses were limited to the simple bootdisk variety. The rise of the Internet and networking started the next phase. In the network-centric era, PCs were networked and the use of the Internet introduced new ways of working, for example remote access VPNs. This accelerated networking also boosted the speed of virus outbreaks. As networking evolved, the range of different types of networks and access devices grew. At the same time, in this integration-centric industry phase, viruses were more often called "blended threats" as they combined different types of hacking techniques to spread even more effectively around the world. Accordingly, businesses were forced to build different protective layers on top of traditional antivirus, such as desktop firewalls, application controls, and antispyware. At this stage, it raises the question whether end users can enjoy the freedom and creativity of modern technology at a time when the IT administrator has increasing control.
The scope of security is expanding and coalescing to present an additional degree of complexity. On the technical side, security is no longer about antivirus protection and firewalls alone; it has now evolved into a holistic approach to prevention and detection of security breaches. From a business perspective, there is a negative impact for every new security breach the organization has to endure. Attacks not only impair technical operations: they also affect business performance, with consequent financial and commercial detriment. But security technology is more than just insurance against attacks. It can add value to the business, allowing it to operate with predictability and resilience.

This increased business impact means that security has become a concern to business managers and is no longer simply an IT issue. As a business imperative, security must be pervasive throughout the organization. This will have a huge impact on the way in which security is managed within organizations and creates a dilemma for security technology — how do organizations implement an enterprisewide security solution that enhances and enables the business, rather than inhibiting it?

**Current Threats**

**Spies among us.** Spyware is no longer just a consumer nuisance: it is quickly becoming a major concern in the corporate environment. The fact that spyware can gather information about an employee or organization without their knowledge is causing corporate security departments to take notice. Spyware is often installed without the user's consent, as a drive-by download, or as the result of clicking some option in a deceptive pop-up window. What concerns corporate security departments is that spyware can also be used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email and other applications. Some of the more sophisticated spyware can even capture screenshots or turn on Webcams.

**The convergence of spam and virus.** In the past, spammers traditionally sent spam from their own ISP account. When corporate IT departments and antispam solutions first started to block messages from certain domains and ISP accounts, spammers turned to new methods to conceal their identity. We believe spammers are starting to resort to outright criminality in their efforts to conceal the sources of their spam messages, using Trojans to turn the computers of innocent consumers and corporate users into secret spam engines. The explosive growth of cable modems and broadband connections has left consumers and remote employees open to attack. In many cases, their computers are being used as a relay for sending spam to thousands of other people There is also very little chance that the PC's owner will have any idea his system is being used by a third party. The SoBig virus is a good example of the convergence of spam and viruses. Ultimately, since spammers are using viruses as a tool to send spam, writing viruses does have commercial benefits. Hence, whenever there are commercial benefits involved, viruses are getting more sophisticated, they have better quality, and are harder to catch.
**The need for speed.** Viruses remain constant; however, worms and malicious code are now the more significant threat to organizations. With a constant stream of new threats, antivirus companies are producing and distributing signature files faster than ever. However, the speed with which new worms and malicious code are spreading has caused the effectiveness of traditional signature-based antivirus solutions to suffer. Recent malicious code incidents have achieved widespread propagation at rates significantly faster than many previous viruses. Worm propagation times have dropped from hours to minutes. One of the most destructive viruses of all time, the Melissa virus, took several days to spread all over the world. Today, viruses and worms need just hours or, in some cases, minutes to spread across the world.

**The need for greed.** In addition to it being a big year for viruses, worms, and malicious code, the motives and intentions of virus writers have changed. In the past, worms and viruses were typically created to destroy data by amateurs seeking notoriety. Today, more sophisticated attackers, often organized crime, are increasingly using worms and viruses to obtain credit card numbers, bank account information, and other personal information to perpetrate identity theft. The sophistication and scale of online fraud and identity theft are increasing at a rapid pace. The recent incidents of "phishing attacks" on banks and their online customers have opened both consumer and corporate eyes to the increasing dangers of corporate identity theft. Phishing is clearly motivated by financial fraud and gain; thus, hackers are most often behind these attacks, rather than teenagers just trying to cause havoc.

In addition to the dizzying array of security threats organizations are facing today, "pharming" is taking phishing to the next level by applying large-scale identity theft. Pharming is the exploitation of a vulnerability in the DNS server software that allows a criminal to acquire the domain name for a site and to redirect that Web site's traffic to another Web site. If the Web site that receives the traffic is a bogus Web site (e.g., a copy of a bank's Web site) it can be used to steal passwords, PIN numbers, or account numbers of hundreds or thousands of customers. Pharming becomes possible when the original Internet site is not SSL protected and when users ignore warnings about invalid server certificates.

**Transition From Product to Service**

Every major security software vendor plans to migrate to a service model. This evolution takes many forms:

- Acquiring or building a professional service practice.
- Transforming either fully or partially (via a spin-off) into an application service provider (ASP) or managed service provider (MSP) that either rents software directly or indirectly to the customer.

Both vendors and customers want a service based on a fixed monthly charge per seat. Vendors want deferred revenue streams based on long-term contracts. This lowers their customer acquisition costs and enables a vendor to increase an individual customer's annualized contract value by offering the customer additional services. Additionally, offering software as a service opens new channels to the market.
Customers want to avoid the burdensome and unpredictable costs of acquiring security hardware, software, and personnel. They realize they must become more security proficient, but they are experiencing huge problems with increasing complexity, scarcity, and high cost of trained security personnel, and inability to retain this personnel. Customers increasingly want to outsource the management of security tasks such as firewall management (central and remote), antivirus scanning, vulnerability assessment, intrusion detection, email scanning, and Web filtering. The goal is to outsource these increasingly costly activities to a vendor that can perform them in a scalable manner at a fixed cost.

Changing Security Market

The battle against viruses and worms, security breaches, productivity concerns, and legal liability issues continues. Security software spending remains a top priority in many organizations, and the security software market achieved $2.7 billion in revenue in 2004, representing 18.6% growth over 2003.

IDC believes that the continuing focus on security bodes well for opportunities within the security software market. Corporate concerns with regulatory compliance, spam, worms/viruses, and identity management help to drive the security software market to achieve more than $5.2 billion in 2009, representing a CAGR of 14.8%. Secure content management (SCM) solutions and security and vulnerability management (SVM) solutions represent the best growth opportunities. Key security highlights are as follows:

- IDC believes that efficient security is about speed and precaution. Past attacks have shown that the time to proactively protect and patch corporate systems is declining rapidly. Therefore, the importance of keeping security solutions up to date and systems patched must not be underestimated. However, an individual risk analysis leading to a realizable, corporatewide security policy should always form the basis for a holistic security strategy.

- Providing excellent quality while continuously staying at the forefront of technology innovation is a must for successful security vendors. Additionally, they need to customize their go-to-market strategy (by industry, company size, and country), gain the mindshare of executive decision makers through non-technical and business-benefit focused marketing language, and use an overall consultative approach to customer problems such as complexity, inconsistency, and non-quantifiability.

- IDC believes that regulations (like Basel II) are forcing companies to meet minimum levels of security for their systems and the information in their databases. This puts additional demands on both the vendors that provide security solutions as well as the CIOs responsible for the implementation of government regulations and standards. The newly established European Network and Information Security Agency (ENISA) will further enhance this process.
Due to convenience and cost advantages, hardware security appliances are proving extremely popular in Western Europe and over recent years have become the preferred solution form factor for delivering security for vendors, channel partners, and customers. During 2004, the Western European security appliance market grew by 51.2% in revenue. IDC is forecasting a 26.7% CAGR for 2004 to 2009. Ultimately, this means that more and more software vendors are losing share to an increasing range of multifunctional security appliances.

**FIGURE 2**

*Western Europe Security Software Revenue and Growth by Segment, 2004–2009 ($M, %)*

![Graph showing Western Europe Security Software Revenue and Growth by Segment, 2004–2009 ($M, %)](image)

Source: IDC, 2005

**Key Security Market Trends**

**Identity and access management.** In the past, the mix of in-house, open source, and partner software was presented to customers as 3A, but these disparate products had little affinity to one another. As a result, system integration costs were very high. Customers soon began to demand a more comprehensive set of solutions to not just reduce costs, but also increase security and productivity. IDC expects to see more and more hardware in the identity management area. Tokens, smart cards, and, to a lesser extent, biometrics, will become parts of comprehensive identity and access management solutions.
**Threat management.** The threat management security market incorporates firewall/VPN software and intrusion detection and prevention. Software firewall/VPN products face considerable challenges brought on by the popularity of appliances and new infrastructures and technologies. This is already happening in that all enterprise-level firewalls are incorporating more sophisticated intrusion and worm protection capabilities. Desktop products are becoming complete endpoint security solutions that incorporate intrusion prevention and worm protection and are tied to antivirus and other content security capabilities.

The intrusion detection and prevention market is making a transition from pure detection to prevention. However, IDC research estimates that about 80% of those purchasing intrusion prevention-capable products are using some of the blocking features in the product. Only a fraction (about a third) of the total prevention features are being used at this time, but as confidence levels grow, so should the level of prevention enabled. Additionally, to increase ID&P performance and manageability, vendors and customers are turning to appliance-based network ID&P products.

**Secure content management.** The challenge of controlling electronic communications as they flow into and out of an organization is becoming increasingly critical. Government and industry regulations (e.g., Basel II) are expected to place additional pressure on corporations to secure the use of their electronic communications.

Spyware is the newest pest wreaking havoc on corporate and consumer users alike. What concerns corporate security departments is that spyware can also be used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email and other applications.

The convenience and efficiency of electronic mail has been dramatically reduced by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Spam has become more than just a nuisance; it is quickly becoming both a major productivity drain and potential legal liability in organizations across the globe. The volume of spam sent worldwide every day will jump from 7 billion in 2002 to 23 billion in 2004, according to IDC estimates.

**Security and vulnerability management.** The problem of coordinating and managing multiple security technologies across the enterprise is a major obstacle facing organizations today. A growing number of security products across the enterprise require frequent upgrades and reconfigurations as new threats and vulnerabilities are detected. Integration of security with current system and network management systems, assurance of high uptime for network and applications, administrative cost reduction (help desk), and a singular view of the IT environment were all key factors in the convergence of security and vulnerability management solutions. Today's ebusiness world requires fully integrated and more comprehensive security management solutions to deal with the multiple security products implemented across the enterprise. Consolidated consoles for managing various security solutions along with aggregated reporting, analysis, and control functions can reduce IT administration chores and costs as well as personnel costs.
**Why Are Conventional Antivirus Solutions Not Enough?**

In the mid-1990s, viruses used network shares to spread through the corporate network. Pure worms that spread using network shares or email did not exist at the time. In the late 1990s, virus writers started to use email as a spreading mechanism. In the early 2000s, writers of malicious code began expanding the capabilities of the viruses and worms they created. These so-called hybrid worms or blended threats used multiple mechanisms to spread, combining traditional hacker techniques to find operating systems or software vulnerabilities and adding malicious virus-like behavior to do damage and replicate. Some of the latest network worms, such as the Slammer, do not write anything onto the computer’s hard drive. Since workstation-level antivirus products are designed to detect worms that write onto the hard drive, these new types of worms are not detected by any vendor’s antivirus solution. Some of the modern worms are also capable of downloading upgrades from the Internet.

Companies today have acknowledged the need for virus protection in email servers and Web traffic, as the majority of the viruses spread via email or the Web. Virus writers have noted this as well and have started to write worms that use other channels to bypass email and Web traffic protection. An example is a worm called Fizzer that spreads using Instant Messaging, peer-to-peer file-sharing networks (e.g., Kazaa), and Internet Relay Chat (IRC). These channels can be blocked at the gateway-level firewall, but for an IT administrator there is no means to prevent employees from using these kinds of applications in corporate laptops outside office premises. In most cases, file-sharing applications are forbidden under corporate security policies, but again, IT administrators lack the means to prevent their use. Spyware in peer-to-peer software increases the risk of spreading companies’ confidential documents to the Internet and opens ports to hackers and worms.

One of the recent characteristics of worms has been the increasing speed of infection. So far, the fastest spreading virus was Slammer, which infected a major part of its targeted hosts globally in 15 minutes and caused the entire Internet to slow down. Even if F-Secure has been the fastest antivirus vendor to provide a cure for virus outbreaks, this kind of virus outbreak cannot be stopped using traditional signature-based virus detection.
FUTURE OUTLOOK

Changing Security Needs: Endpoint Security

Definition of Endpoint Security (EPS)

Client, host, or endpoint security is a difficult thing to both describe and obtain. The endpoint challenge is obvious: While organizations are constantly been attacked by malicious code, a sea of different mobile devices transmits highly sensitive data via a variety of networking environments. Organizations, however, seem to disagree on what encompasses endpoint security. Many feel that they are protected as long as they have both firewalls and antivirus in place.

Historically, the term "endpoint security" has been connected to personal firewalls that are centrally managed. However, IDC believes that due to the dynamics of the security market endpoint security needs to incorporate antivirus, content security, authorization and authentication mechanisms, and emerging security technologies — simply because customers demand their inclusion.

EPS as defined by IDC refers to the centrally managed enforcement of security policy at the client level (such as remote desktops, laptops, PDAs, or cell phones) and network access points (such as remote servers, internal desktops, Internet kiosks, or Web browsers). This activity can be performed by the enterprise's IT organization or an external service provider by using security management software on servers or gateways.

Typical Installation Scenarios

Every corporate network is different, especially when comparing companies with 10 computers or 15,000 computers. Let's take a look at some simplified installation scenarios for both small and large enterprises for endpoint security software.

A Small Business Without a Full-Time IT Administrator

It's clear that for small businesses that do not have a full-time IT administrator the security software needs to be very easy to use. Just install and forget. The installation starts by pushing the software remotely to desktops and laptops. The automatic updates take care that the virus definitions are updated so that the software does not need any operational actions after installation.

The installation covers the following basic steps:

1. Install the management server from a CD or through some other media to a company file server or dedicated server.
2. Start the management console.
3. "Push" install endpoint software to the computers.
4. Make final configurations and check that virus definition updates work.
A Company With an IT Administrator and Remote Office

In the second example, we have a larger enterprise with one remote office. A company of this size typically has designated IT staff in-house, with the company’s IT fleet, including file servers, email servers, and firewalls, as their responsibility. Many employees work remotely, carrying laptops out of the office. By connecting laptops to the Internet through hotel networks, cable/xDSL connections etc., these “road warriors” can expose their laptop computers to viruses, hackers, and networking software that is forbidden in the company. This means that the protection must be always on and properly updated even when the road warrior is connecting to the Internet outside the corporate network. The network administrator should lock down the endpoint security software settings on desktops and laptops, thereby leaving no room to bypass the protection.
In a typical remote office, the Internet or WAN connections to the headquarters are limited. Daily virus definition updates from each workstation at the remote office can consume precious network capacity. Using proxy mechanisms, the Internet traffic can be significantly reduced, as the virus definition updates can be downloaded to the workstations from a local proxy server rather than each workstation downloading the update from the Internet. With the proxy, remote office workstations are updated faster against the latest threats and network bandwidth can be used more efficiently for business purposes.

The installation follows basically the same steps as with the smaller company, with some exceptions. The configurations may have greater granularity and more attention is paid to deployment, reporting, and monitoring the status of the endpoint software.
Security Best Practices and How They Relate to Endpoint Security

Any enterprise regardless of size that intends to ensure its business continuity and protect itself should consider several issues when evaluating security products in general and endpoint security solutions in particular. Common for both is that the chosen solutions must meet enterprise security, manageability, and business requirements.

What Kind of Protection is Needed?

To ensure continuous protection, security software needs to be turned on and operate in real-time mode. In order to maintain the highest level of protection antivirus and spyware scanning should be applied to all applications accessing file systems, and also directly from email and HTTP traffic, which are the most likely ways that viruses and other malicious code are spread. Therefore an effective endpoint security approach includes preventing violations in real time, rather than noting attacks or system changes after they have occurred.

As many network worms exploit vulnerabilities in operating systems and software the security software must integrate a firewall component for desktop computers in order to block worm infections from the network. The desktop firewall protection is mandatory for remote laptop users who cannot be protected by the gateway-level firewall at the office network.

The networking applications, such as peer-to-peer software, are not malicious as such but can be dangerous for the company by distributing confidential documents to the Internet. Another risk for the company is employees downloading or distributing copyrighted materials with company-owned workstations or laptops. The network administrator should be able to configure which applications are used at the endpoint (workstations, laptops, etc.) regardless of time and place.

How Must Protection be Configured?

In order to continuously maintain the highest level of protection the security software should be turned on with automatic virus and spyware definition updates by default. Despite the heuristics and other proactive security features, most endpoint security software nowadays has virus definitions that offer precise detection of malicious code and should be updated frequently.

Seamless protection of the whole company network requires policies that cannot be altered or bypassed locally at endpoints. As the end users usually do not have the required security expertise the security solution should have enforceable policies set by the network administrator.

Each company network is different in terms of security requirements. As company laptops typically connect to different networks (office network, home network, branch office network, public WLANs, etc.), security policies should be able to adapt to different environments and situations. When the antivirus software, for example, does not have the most recent updates the desktop firewall automatically limits the networking access in order to minimize the risk of being infected by new viruses until the software has been updated. Another example is to automatically tighten the security settings when the laptop is connected to the Internet outside the corporate office network.
Viruses and other malicious code arriving in emails typically use certain file types in attachments, such as .com, .exe, .vbs, .shs, or .pif. Some viruses try to fool end users by using more than one file extension. In order to limit the number of viruses spreading through emails these file extension and file types with more than one extension should be dropped at the gateway level.

Another important piece in the endpoint security puzzle is to ensure that all data coming into the company is checked from viruses and spyware. The best way to achieve this is to implement defense mechanisms at gateway, server, and endpoint levels. For remote laptops the defense should have the same protective components as the hosts inside the corporate LAN — real-time antivirus and spyware scanning, scanning of emails, firewall and intrusion prevention, and application control.

To reduce the time spent on updating and installing security software, and to monitor the status of the security in the company network, centralized management of the security software is needed. Having the control of security software settings in one central location makes sure employees do not have to be trained for the new software as well.

**What Processes Must be in Place?**

Software vendors such as Microsoft issue security advisories through a mailing list on software patches available for protection. Many antivirus vendors have mailing lists or more advanced methods to give instant notification of serious security events, such as new virus outbreaks. The company IT personnel should join both of these informative channels to be able to react before the company security is compromised. Naturally, the IT personnel should also have the means to patch the software in company desktops, laptops, servers, and gateways if needed.
CONCLUSION

Like a digitized watchdog, properly implemented endpoint security is often the last line of defense between a destructive threat ecosystem and the security of organizations. However, confusion surrounding endpoint security — defined by IDC as centrally managed client security — is leaving some organizations vulnerable to the malware, malicious code, and destructive spam that criminals are bent on pushing.

Exposed through increased numbers of uniquely different mobile devices and a widening variety of networking environments, IT organizations must be prepared to embrace EPS. The complexity of the EPS problem will have profound and far reaching effects throughout an organization. Therefore, senior management, as well as IT and business unit leaders, must see the big picture to address concerns about security, mobile device use and employee productivity, remote access, and centralized access control. F-Secure's Anti-Virus Client Security 6 is an example of a good endpoint security solution that fulfills the needs of enterprises that want to protect their business from modern threats.

Copyright Notice

External Publication of IDC Information and Data — 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.

For further information regarding this document please contact:

Marketing Department

Tel: +44 (0) 20 8987 7100

Copyright 2005 IDC. Reproduction without written permission is completely forbidden.