

WHITE PAPER

Security — Embedded in to the Heart of Your Business

Sponsored by: Cisco Systems

Thomas Raschke

Duncan Brown

April 2004

IN THIS WHITE PAPER

2003 was characterized by a tidal wave of viruses and worms, security breaches, productivity concerns, and legal liability issues affecting businesses across the globe, as those without the essential means of defense will be most painfully aware. With continued attacks, such as the recent Witty Worm, it is hardly surprising that businesses worldwide continue to dedicate valuable IT budgets to securing their networks, with IDC predicting spending to exceed \$48 billion in 2004.

It is in this context that IDC addresses the current nature of the security market in this White Paper, sponsored by Cisco Systems. IDC's research highlights the following key findings, which should be at the forefront of business leaders' thinking worldwide:

- ☒ Attacks on security solutions no longer occur in isolation but as a sophisticated multilayered collaboration designed to confuse today's point security solutions. A holistic approach to security is therefore required.
- ☒ Embedding security into networks greatly decreases the threat of breaches and resulting business impact.
- ☒ Automated solutions decrease the time and effort required to maintain up-to-date protection from attacks, as well as reducing the scope for human error.
- ☒ The security market is growing at almost three times the rate of overall IT spend, and is estimated by IDC to increase from 4.8% to 7% of overall IT budgets by 2007.
- ☒ Overall the mobile security software market, driven primarily by the demand for remote access, will grow at a faster rate than the whole security market, representing \$1.27 billion worldwide by 2007 and attaining a CAGR of 71% between 2002 and 2007.

INTRODUCTION

Businesses of all sizes worldwide have seen wave after wave of security attacks continue to increasingly affect business productivity, a trend likely to continue throughout 2004. These "waves" have been ongoing since commercial use of the Internet began. Viruses and worms, denials of services, and the compromise of sensitive data have led to productivity problems, customer service issues, and legal liability debates among businesses worldwide. This unabated pressure on organizations means that security software spending continues to be a top priority, evidenced by the fact that the worldwide market achieved a spending level of \$42 billion in 2003. Concerns with regulatory compliance, spam, worms/viruses, and identity management are combining to drive the security software market to reach a spending level of more than \$77 billion worldwide in 2007, according to IDC.

The domain of security is expanding in two directions. Firstly, the technical scope of security is enlarging and coalescing to present an additional degree of complexity. 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 in any and every sense.

The second dimension to the growth of security concerns is the business perspective. For every security breach there is a business impact. Attacks not only impair technical operations — they 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?

As a business imperative, security must be pervasive throughout the organization.

The Role of the Network in Security

The network is more than just strands of copper and fiber. We have moved from simple PSTNs and LANs to a network of networks, adding wireless dimensions and building on the growing dominance of IP. The network consolidates components in a technology infrastructure into an integrated whole. As such, the network now underpins entire business operations across all forms of organization worldwide.

The impact of security on the network is, consequently, profound: infect the network and you infect the business. Every application, device, wireless connection, switch, and router is a point of attack. Networks have evolved to respond to the increased business dependence, and the commensurate security threat. Today's intelligent networks embed security features, offering high resilience to attack, adaptive systems functionality, and an integrated approach to design and management. IDC believes that it is imperative for organizations seeking to minimize security breaches, and the resulting business impact, to adopt a holistic approach to secure their networks.

Infect the network and you infect the business.

The Evolution of the Security Ecosystem

The sources of security attacks are ever increasing. There will be no let-up in the ingenuity of the criminal, in the carelessness of some staff, in the impact of incoming regulation, or in the threat from those who would cause economic and political instability. As criminals adapt to barriers implemented by businesses, the effect of a security breach on an organization increasingly impacts the profitability of the attacked entity. Whatever the cause, breaches of security impact businesses at a number of different levels:

- ☒ *Lost productivity.* Downtime leads to decreases in operating efficiency, incurring increased costs and falling margins. The time and effort in administering security solutions is growing with the increase in complexity of threats, and the associated rise in business risk.
- ☒ *Financial losses.* Security breaches can lead to financial consequences, either direct (due to theft, for example), or indirect (such as downtime leading to lost business).
- ☒ *Regulatory compliance.* A series of regulatory changes, such as data protection and risk management, are introducing strict controls on many businesses' operations. Penalties for non-compliance can range from fines and lawsuits to loss of trading licenses.
- ☒ *Shareholder value.* A firm's reputation can add substantial value to its market value. Bad publicity from security breaches affects brand perception and market confidence.

Ownership of security and its implications by senior management is therefore mandatory, otherwise the consequences of ignoring its importance can have a strong negative impact on organizations.

Ownership of security and its implications by senior management is therefore mandatory.

As if these pressures were not enough, further challenges for organizations are a continued focus in 2004:

- ☒ Complexity of solutions
- ☒ Poor business justification
- ☒ Interoperability of solutions
- ☒ Government regulations
- ☒ Market consolidation
- ☒ Test implementations
- ☒ Hybrid threats
- ☒ Physical and IT security convergence
- ☒ Mobile and wireless

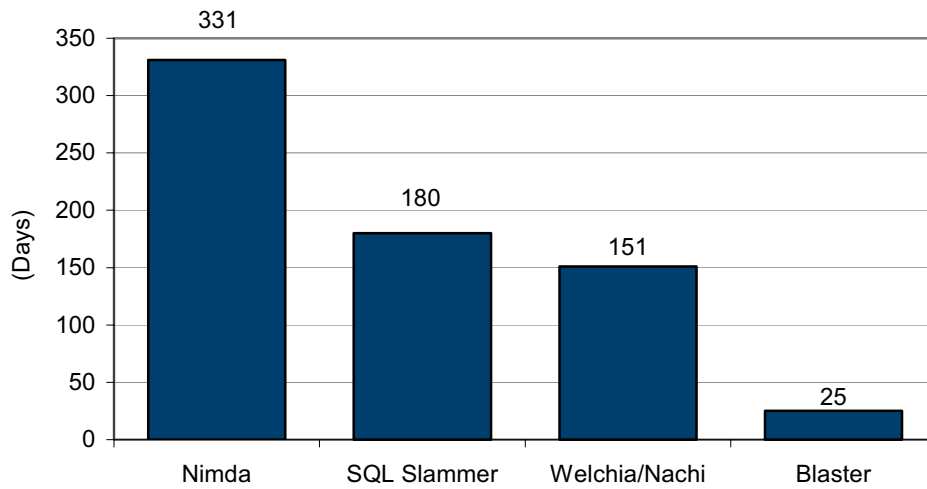
Threats: Increasing in Speed and Complexity

Businesses are subject to changing conditions at 21st century speed, and security demands are no exception. For example, the time between the release of a security patch for a security defect and the active exploitation of that defect is measurable in days (see Figure 1).

The time between infiltration of an attack and its propagation throughout the business can be measured in minutes. This is because many security solutions guard at the perimeter of the network, rather than throughout the infrastructure.

FIGURE 1

Days Between Patch Release and Exploitation



Source: IDC, 2004

The reduction in time allowed to defend against security attacks is compounded by the increased complexity of the threat. Worms, Trojans, and viruses no longer act in isolation but as sophisticated multilayered collaborations designed to confuse today's point security solutions.

Defense against these blended threats demands a holistic, multilayered approach to security.

Defense against these blended threats demands a holistic, multilayered approach to security.

Secure Content Management

In the words of Sir Francis Bacon, the 17th century English philosopher and statesman, "knowledge is power," and seen in the 21st century sense knowledge also equates to electronic information held by companies that gives them competitive advantage. This information and electronic content are business assets that need to be protected, as much as any other commercial asset or property. Secure content management has, therefore, become a core area of interest for IT and business managers alike. However, this is just part of the solution to providing as secure a network to your business as possible.

Secure content management protects Web content and downloadable applications execution. It incorporates three specific product areas:

- ☒ **Antivirus software** identifies and/or eliminates harmful software and macros. Antivirus software scans hard drives, email attachments, floppy disks, Web pages, and other types of electronic traffic (e.g., instant messages and short messaging service [SMS]) for any known or potential viruses. Typically, antivirus software has to be updated manually, leaving organizations vulnerable to attack if they are not up to date.
- ☒ **Web filtering software** is used to screen and exclude Web pages from access or availability that are deemed objectionable or unrelated to business. Web filtering is used by corporations to enforce corporate policy, as well as by schools and universities and home computer owners (for parental controls).
- ☒ **Messaging security software** is used to screen messaging applications such as email, instant messaging, SMS, and peer-to-peer for spam or other objectionable content. The software is also used to enforce corporate policy by screening for company confidential information and to enforce compliance with privacy regulations (e.g., Basel II). Messaging security also includes secure email.

Security of content extends beyond inbound media from external sources. It also includes the security of outbound information, the validity and accuracy of which is critical to business operations.

The "Rogue" Element in Security Solutions — People

Securing businesses would be more straightforward if people were not involved. Unfortunately, this is rarely the case, and the context of any security solution must account for the actions and attitudes of a variety of individuals, for example:

- ☒ *End users* generally find security inconvenient. Passwords are forgotten, or written down. Manuals are unread. Processes are ignored. Lack of awareness and ignorance of threats are standard.
- ☒ *Senior management* often minimizes the threat of security. This tends to lower the perception of threat, which means that security solutions are then viewed as expensive. Return on investment (ROI) is often only belatedly evident when spectacular failure indicates insufficient investment.

Securing businesses would be more straightforward if people were not involved.

☒ *Hackers* and other sources of malice actively track security solutions. Vendors of such solutions are well understood and predictable, often publishing their strategies and activities to a broad community. This visibility naturally also extends to the hackers, who are then better prepared when creating the next security threat.

☒ Vendors of security solutions often sell security as a panacea. No such thing exists and high expectations are no substitute for vigilance.

Therefore, security solutions must be simple, requiring little or no training. The more automated and hidden the technology, the better, and any measures that prove the value of security (such as system availability) should be publicized. This helps to underline the business benefits to decision makers who have traditionally viewed security as an IT-specific issue.

The more automated and hidden the technology is, the better.

Security solutions also need to be able to adapt to emerging threats as they happen to better protect organizations today. This means more than vendors being up to date with the latest threats — it requires the security solution itself to recognize an attack, even if it has no prior knowledge of the threat.

Ultimately, responsibility for security resides not in technology but in the attitudes and actions of people. Security policies can make a difference, where people and technology processes combine to assure the integrity of the business, and these have been increasingly employed across a number of organizations worldwide.

The Changing Security Market

IDC sees four key security trends in the next five years which organizations should be aware of when reviewing their networks and security policies. These are:

- ☒ Appliances will become the standard deployment medium.
- ☒ Identity management will be the preferred user interface for security.
- ☒ Messaging security moves from point products to holistic solutions.
- ☒ Wireless and mobile security become mainstream.

Appliances: A Standard Deployment Medium for Security

IDC predicts that by 2007, 80% of all security solutions will be delivered via a dedicated security appliance. Security appliances are defined as a combination of hardware, software, and networking technologies whose primary function is to perform specific or multiple security functions.

Typically, a security appliance consists of hardware with a secure operating system (OS), a limited applications set, and no user software installation. Security appliances may also include other features such as security management, policy management, quality of service, network switching and routing, load balancing, high availability, and bandwidth management.

The original security appliances were based on firewall/VPN functions, but the threats have evolved to infiltrate organizations in a number of different ways. Now, there are appliances available for almost all security functions, including intrusion detection and prevention, antivirus, secure content management, authentication, vulnerability assessment, and security event management.

The attraction of appliances is obvious as their out-of-the-box or “plug and play” nature confers ease of installation with minimal maintenance overhead, lowering the cost of ownership. Performance is tuned at manufacture, and components are specifically selected due to their “hardened” security specification.

However, there is a danger in viewing a collection of appliances as a preventative cure as threats to organizations' networks have evolved to become more complex. To address this, state-of-the-art appliances incorporate multilayered security features to manage blended attacks.

Identity Management: A Preferred User Interface to Security

One of the imperatives of business delivery is to provide a single point for multidevice, personalized, seamless access to enterprise systems and information over the Web. Consolidating the management of user preferences and privileges while mitigating the need to key and re-key authentication credentials like usernames and passwords improves user experience and drives operational efficiencies.

IDC estimates that expired user accounts may be upwards of 60% of all accounts in corporate systems. This opens the enterprise to serious security vulnerabilities. Moreover, providing self-administration for the updating/reset of passwords and other identity information reduces administrative and help desk costs.

Identity management automates and simplifies the workflow of activating and deactivating (known as provisioning) of accounts, access rights policies, cards, and other privileges from across the enterprise. Whether accounts reside with HR, IS/IT, or another department, managing the churn of employees and contractors is less costly from a systems and personnel perspective. Furthermore, automated provisioning of accounts can help ensure a higher and more consistent level of security uniformly across enterprise resources, while reducing administrative costs.

Messaging Security Moves From Point Products to Holistic Solutions

Email remains the dominant form of electronic communication and collaboration for both business and consumer users. But growth is being restrained by spam due to its high volume. IDC believes spam can account for up to 80% of all inbound Internet email — plus the effort required to scan it for viruses, worms, and offensive content.

IDC believes spam can account for up to 80% of all inbound Internet email.

Spam has become the primary driver for messaging security implementations, overtaking antivirus technologies. Spam is no longer just a nuisance; it is quickly becoming both a potential legal liability and a major productivity drain for corporate IT departments and corporate users alike. Other threats to the dominance of email come from regulatory requirements to retain documentation and the rise of instant messaging, which is itself now becoming a target for spam.

Managing the security threat, whether from spam, complying with regulations, or coping with new vulnerabilities introduced by instant messaging, means that organizations must deploy multiple layers of security throughout the enterprise.

Managing the security threat means that organizations must deploy multiple layers of security throughout the enterprise.

Security solutions must therefore cater for these situations in an integrated, holistic manner. IDC believes that due to the previously mentioned developments, point products lack the comprehensive approach required to avoid inadvertent gaps in the level of prevention and detection.

Wireless and Mobile Security Become Mainstream

As if securing a business is not hard enough, the introduction of wireless devices and applications adds another layer of complexity, and another threat of exposure to security breach. Mobile phones and smart handheld devices will become an increasingly tempting target for virus writers.

The proliferation of untethered devices will increase demand for greater security, especially in the enterprise IT market. Specifically, Wi-Fi security features and products will drive organizations toward Wi-Fi-based solutions and away from cellular-based devices for sensitive corporate data.

Overall, the mobile security market will grow at a faster rate than the whole security market, attaining an overall 2002–2007 CAGR of 71.2%. Security software solutions, designed for mobile and wireless environments, are forecast by IDC to represent \$1.27 billion in revenue worldwide by 2007, up from \$127.7 million in 2003.

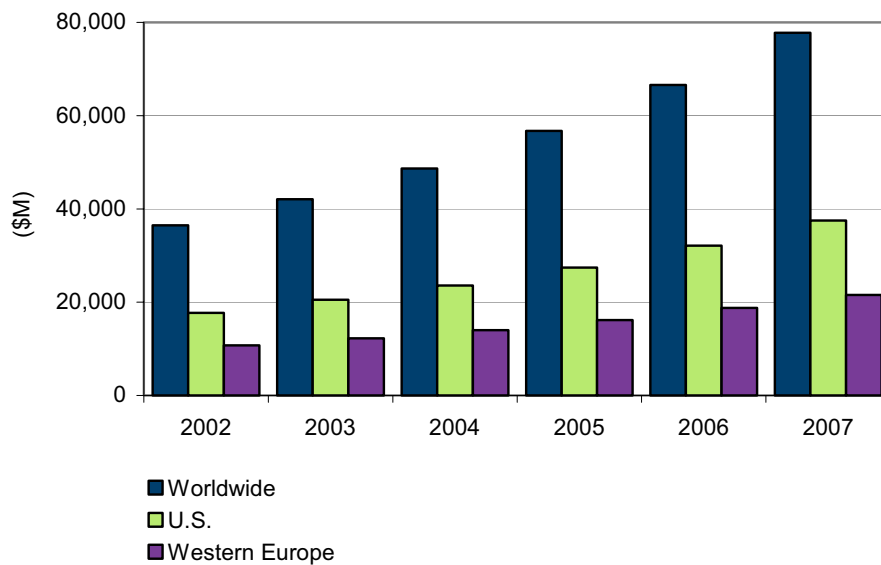
The Security Paradox

Security is a key issue for both IT and business managers. But if security is such an important agenda item, why does it currently represent just \$42 billion, or 4.8%, of overall IT spend among organizations worldwide? Compare this with the \$43 billion spent worldwide on printers and multifunctional peripherals in 2003.

IDC concludes that there is a legacy of a lack of awareness among business leaders of the increasing security threat to company infrastructure, and that this will inevitably impact on business performance.

FIGURE 2

Security Spending Comparison



Source: IDC, 2004

Increasing awareness of the importance of securing company infrastructure leads IDC to predict that the current 4.8% of IT spend dedicated to security will grow to over 7% by 2007. The security market is, therefore, growing at almost three times the rate of the IT market as a whole, which demonstrates the growing acceptance of security as a strategic issue for organizations of all sizes today.

The security market is growing at almost three times the rate of the IT market as a whole.

SECURITY IN 2004 AND BEYOND

So what does the future of security look like and where should organizations be looking to keep abreast of changes in the market? IDC believes that there are three core areas of best practice in a state-of-the-art security solution, that deal with:

- Connectivity
- Threats
- Trust

Connectivity

Security best practice starts and ends at the network. The starting assumption for defining the network boundary is that everything connects to everything. Whether planned or inadvertent, all manner of devices, Web sites, applications, switches, and routers can be endpoints in the network. With the emergence of high-availability wireless connectivity there is often no cable to alert managers or users to the existence of a connection.

Security best practice starts and ends at the network.

This places unprecedented demands on the vigilance of the security solution, to prevent and detect threats. An underlying secure transport layer is essential to any connectivity regime. IPSec and SSL-based VPNs can enable access from any location in a secure way.

Threats

The nature of security threats continues to evolve. The sophistication of methods of attack increases and the blending of multiple types of threat (virus+worm+Trojan, etc.) combine to pose a severe threat to all but the most resilient system.

The blending of multiple types of threat combine to pose a severe threat to all but the most resilient system.

In response, security solutions must also exhibit multiple layers of defense — simple antivirus and firewall protection are no longer enough. Modern security tools merge intrusion detection and prevention, vulnerability assessment, and 3A (administration, authorization, and authentication) capabilities to provide a much more robust defense against attack.

The 3A market will continue to undergo significant changes over the next few years. IDC believes that point products and utilities will find less and less acceptance among users, because of the systems integration costs. Increasingly, IDC believes that identity management will become a superset of 3A. Identity management will embrace all 3A software technologies and extend into directory services and hardware authentication devices as well.

Trust

Each component that touches an enterprise's infrastructure must be trusted, in order for it to interact securely with other components. The network, as the mechanism for connecting components, must also be trusted, but in addition it can perform validation on users and devices that attempt to access resources via the network. Thus the network can be an integral part of identity management, verifying users and devices, as well as performing centralized configuration, monitoring, and analysis.

Each component that touches an enterprise's infrastructure must be trusted, in order for it to interact securely with other components.

Trust is not a static entity. It erodes over time (sometimes overnight) as new threats emerge. Trusted status must be continually verified and updated. Security solutions will therefore check the credentials of endpoints connected to the network, and deny or restrict access if suspicions are raised. Periodic checks are insufficient, as day-zero attacks become more commonplace. Continuous, adaptive trust validation that is close to, or preferably part of, the network is mandatory to ensure as secure a network as possible.

An Industry Example — Cisco Network Admission Control

Cisco Network Admission Control is a comprehensive security solution that enforces an organization's vulnerability patch policies and to manage distrusted systems in a secure manner. It combines information regarding endpoints' trusted status with network admission policies to increase the resilience to security attacks.

Cisco's offering continually monitors the status of each endpoint, based on its degree of antivirus protection and operating system patch level. There are four main components:

- ☒ Cisco Trust agent — software that resides on an endpoint system and that collects information from various security software elements. The company has integrated trust agent technology from leading vendors.
- ☒ Network Access Devices — routers, switches, wireless access points, and appliances that store security credentials and pass this information on to policy servers.
- ☒ Policy Server — based on the Cisco Secure Access Control Server, this gathers information sent from network access devices and decides on the appropriate policy to apply.
- ☒ Management System — a collective of Cisco management solutions that provides provisions and monitors Cisco Network Admission Control elements.

Cisco's solution ensures that all elements connected to the network are validated according to the latest antivirus and operating systems patches available. Non-compliant or suspect elements are isolated until secured remedially. Existing antivirus technologies can also be integrated with Cisco network infrastructure.

Cisco's current offering is the first phase of the company's Self-Defending Network concept. This multiphased initiative incorporates all the elements of a state-of-the-art security solution, to provide "built-in" security that dynamically identifies, prevents, and responds to security threats.

The applications of Cisco's solution are numerous. Remote access security is a key area in which a layered security regime is recommended, and Cisco's technology assists in the automated management of remote clients. It can also keep host servers updated with the latest versions of AV defense, ensuring that protection remains current.

CHALLENGES FOR CISCO

Although security as a broad issue affects the business of an organization, security solutions are seen largely as technical implementations. Responsibility is handed to the CIO, IT manager, or office manager, who often must fund security infrastructure from a diminishing IT budget. This tends to support the procurement of point products, rather than holistic solutions. Improving visibility of security at the business level must remain an ongoing campaign.

However, failure of security regimes is visible, but success is invisible. Proving the value of a robust security system remains like asking for a leap of faith — reporting numbers of rebuffed attacks and high levels of system availability do not reflect accurately the costs sustained had a security breach occurred. IDC therefore believes that Cisco will need to support decision makers in user organizations with proof points of return on security investment in order to support the change to a holistic approach to security.

Cisco has already established partnerships with leading providers of trust solutions, as part of its Network Admission Control program. Players in the security market need to collaborate in order to ensure compatibility between certification processes, and to offer flexibility to customers. Cisco must therefore continue to add partners to its NAC program to ensure its leadership in the broad security solutions market.

Cisco should also partner with managed security service providers. The use of outsourced services, especially for firewall management and intrusion detection, is growing. Typically, the customer does not purchase the security solution but instead leases it as part of the service. In these cases, the service provider can provide a revenue stream back to Cisco. This could be very significant with small and medium-sized vendors, where price is more important.

CONCLUSION

Customers of security solutions, from large enterprises to small businesses, need security policies that are embedded into their technology infrastructures. Because the scale and complexity of infrastructures vary enormously, flexibility of deployment mechanisms is a must. A full range of security appliances, software, and services will be on offer, with the common objective of providing a holistic, integrated security environment.

However, businesses should demand more from their security solutions in the future. Security should incorporate a considered approach to risk mitigation, and this planned strategy brings implications for security systems. It means that security solutions must be automated and proactive to threats rather than reactive — in other words, security must be preventative rather than remedial.

Above all, organizations today tell IDC that they regard their security as an integral part of their IT infrastructure. Thus security solutions must be embedded within multiple layers of the core infrastructure, rather than veneers of protection.

As continued attacks drive the adoption of security solutions, IDC believes that companies of all sizes need to be more aware of the threat to their operations and take necessary steps to secure their businesses. To aid business leaders from diverse organizational types in this endeavor, IDC has put together a list of issues company management should have at the forefront when assessing their security policies and infrastructures:

- Think holistically. Are you relying on point solutions and ignoring potential cracks in your protection?
- Multilayered protection is a must. Does your company have solutions in place to combat today's blended threats?
- The rate of change of security threats demands continuous management of upgrades to security solutions. How up to date is your security infrastructure?
- The economics of managed security services make sense. Should you consider procuring security as a service?
- Automate security in order to manage it. Do you know how much you spend on security administration?

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 2004 IDC. Reproduction without written permission is completely forbidden.