WHITE PAPER

symantec™

Integrated Security: Creating the Secure Enterprise

INSIDE

INSIDE

- Evolving IT and business environments
- The impact of network attacks on business
- The logical solution

Contents

Executive summary

As organizations become more dependent on their networks for business transactions, external data sharing, and simple day-to-day communications, the need increases for these networks to be more accessible and operational. But as accessibility to the network becomes easier, so does gaining access to the critical data they are storing. The challenge is to ensure that the right people gain access and the wrong people do not, making the role of information security even more critical to enabling today's businesses. Yet, current security solutions are typically comprised of multiple point products, resulting in a lack of interoperability, manageability, and a higher cost of ownership.

The concept of integrated security is emerging as an effective approach to address the new challenges facing e-businesses. This method combines multiple security technologies with policy compliance, customer management, service and support, and advanced research for complete protection. By adopting a comprehensive strategy that holistically addresses security at each tier of the network (i.e., client, server, and gateway), organizations are able to reduce costs, improve manageability, enhance performance, tighten security, and reduce risk of exposure. An integrated security approach offers the most effective security posture at the optimal cost-benefit ratio, compared to multiple point product security implementations. This paper provides an overview of the key drivers behind this shift toward integrated security, including the growing sophistication of network attacks; summarizes the business impact of attacks on networks that are not employing integrated security; and describes the key elements and benefits of an integrated security solution.

Evolving IT and business environments

The ability to have open communications and collaborations among company stakeholders, including customers, employees, suppliers, partners, contractors, and telecommuters is required in an enterprise network environment.

The gateway, server, and client layers of the network are interconnected to meet the needs of the hyper-connected firm. This means that business-critical information resides at multiple levels in the internal network, each of which requires its own protection. While IT personnel have traditionally focused on centralized security at the data-center level, they now have to address the ever-expanding definition of the network reach and corresponding security requirements.

At the same time, threats to the network have become increasingly sophisticated. Advanced attacks employ multiple methods to propagate, as well as discover and exploit, network vulnerabilities.

Although information security is not a core competency of most organizations, it is clearly a requirement for transacting online business. Security thus becomes a key business enabler, not simply an IT option. For this reason, information security is receiving a growing amount of scrutiny from higher-level executives, such as CIOs, who are interested in how security will assist the enterprise in achieving business goals, not necessarily how the technology works. From a security standpoint, executive goals include the following:

- Implementing solutions that ensure openly robust, yet secure network infrastructures to protect information assets and to ensure business continuity
- Keeping pace with the changing requirements of e-business (e.g., high network availability, data integrity, and privacy) and the corresponding security threats
- Meeting logging, reporting, auditing, and compliance requirements
- Facing these challenges with limited resources at lower cost
- Selecting solutions that maximize employee productivity, including that of the IT department (e.g., ease of security solution administration and management)

Types of network attacks

Many types of network attacks exist, each with its own varying degree of impact. Common types of threats include:

- MALICIOUS CODE ATTACKS These types of attacks, capable of damaging or compromising the security of individual computers as well as entire networks, are usually viruses, worms, and Trojan horses that hide within files or programming code only to self-replicate, self-propagate, or be spread by unknowing computer users
- DENIAL-OF-SERVICE (DoS) ATTACKS Capable of disabling a single computer or entire networks, DoS attacks are explicit hacker attempts with the sole intention of keeping legitimate users of a network from using that service and/or to disrupt normal business operations. Examples include attempts to "flood" a network, thereby blocking legitimate network traffic, and attempts to disrupt connections between two machines, thus preventing access to a service.

- UNAUTHORIZED ACCESS: INTERNAL AND EXTERNAL HACKING A hacker is someone who is able to gain access and control over computers, information, and technology without proper authority. By exploiting security vulnerabilities in an organization's network, a hacker can gain access to important network or data resources for purposes of removal, duplication, or even destruction of proprietary assets. Whether the culprit is a disgruntled employee, contractor, or anonymous outsider, the invasion can lead to company downtime, cleanup costs, and/or the often unrecoverable cost of stolen proprietary data.
- BLENDED THREATS These threats combine the characteristics of viruses, worms, Trojan horses, and/or malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By utilizing multiple methods of attack and self-propagation, blended threats can spread rapidly and cause widespread damage. Blended threats, such as Nimda and CodeRed, are designed to exploit the vulnerabilities of security technologies working independently from one another.

The impact of network attacks on business

Network attacks range from easy-to-quantify consequences such as interrupted business operations, to losses that are difficult to calculate (e.g. damaged brand equity). Other consequences of network attacks may include:

- INTERRUPTION OF BUSINESS OPERATIONS Downtime due to an attack results in lost productivity and revenues, and the costs associated with restoring a hacked network can increase the overall financial impact of an attack. Once attacked, an organization typically deploys a cleanup team to enable customers, employees, and partners to resume business as soon as possible. Not only is business brought to a halt until a fix is implemented, but the cleanup team is pulled away from its daily duties, compounding productivity loss.
- LEGAL LIABILITY AND POTENTIAL LITIGATION Organizations that have been hacked may find themselves in court as a defendant or key witness. Companies required to comply with privacy and security regulations, such as health care organizations and financial institutions, may need to demonstrate their due diligence in minimizing their exposure to network attacks. This process is a drain on both employee productivity and company cash flow.
- REDUCED ABILITY TO COMPETE Information is often considered a company's most valuable asset (70% or more of a company's value resides in its intellectual property assets)[1], the loss or theft of that data can pose serious consequences, even rendering the company's market position untenable. According to the 2002 CSI/FBI Computer Crime and Security Survey, the most serious financial losses due to security breaches included theft of proprietary information (26 respondents reported losses over $170,000,000)[2].
- DAMAGE TO BRAND EQUITY Damage to a company's brand may assume various forms, each of them capable of degrading a company's position in the marketplace. For example, companies who have had customer data (such as credit card information) stolen and publicly displayed on other web sites have a hard time restoring customer confidence in their brand.

[1] "Trends in Proprietary Information Loss" survey report, American Society for Industrial Security and PricewaterhouseCoopers, 1999.
[2] Richard Power, Computer Security Institute, "Computer Security Issues and Trends," 2002 CSI/FBI Computer Crime and Security Survey.

Current security solutions

Current security solutions typically consist of multiple point products. These are products that must be purchased, installed, deployed, managed, and updated separately. With this approach, IT managers need to address problems related to the lack of interoperability between each of the products. Protection is usually not comprehensive because cross-vendor interoperability issues often allow threats to slip through the cracks, compromising security. What's more, when an outbreak occurs, the "fixes" that each vendor provides must be tested and verified across the various technologies. This can slow response to attacks, potentially increasing the costs that are incurred. Independent point products can also degrade network performance; since the products were not designed to work together, they present more of a performance hit. More generally, multiple point products that are not integrated cannot be effectively managed, which helps raise IT administration and support costs.

The implications of current security solutions include inefficiencies, disappointing results (e.g., lower than anticipated risk mitigation and loss of customer and market trust), and a higher cost of ownership. In addition to providing inadequate protection against blended threats, current products require labor intensive implementation and configuration. These products are part of an enterprise security posture that may be difficult to understand and which provide little insight into security planning and performance.

The logical solution: integrated security

Integrated security provides a comprehensive, holistic security system that addresses the challenges and opportunities of today's networked enterprises. This security method combines multiple security technologies with policy compliance, management, customer service and support, and advanced research, for complete protection. It uses the principles of defense in depth and employs complementary security functions at multiple levels within the IT infrastructure.

By combining multiple security functions, integrated security can more efficiently protect against a variety of threats at each tier to minimize the effects of network attacks. Key security technologies that can be integrated include:

- FIREWALLS Control all network traffic by screening the information entering and leaving a network (or portion of a network) to help ensure that no unauthorized access to computers and/or the network occurs
- INTRUSION DETECTION Detects unauthorized access and provides alerts and reports that can be analyzed for patterns and planning
- CONTENT FILTERING Identifies and eliminates unwanted traffic
- VIRTUAL PRIVATE NETWORKS (VPN) Secure connections beyond the perimeter, enabling organizations to safely communicate with other networks across the Internet
- VULNERABILITY MANAGEMENT Enables assessments of a network's security position by uncovering security gaps and suggesting improvements
- VIRUS PROTECTION Protects against viruses, worms, and Trojan horses

Individually, these security technologies can be cumbersome to install and generally are difficult and expensive to manage and update. When integrated into a single solution, however, they offer more comprehensive protection while reducing complexity and cost.

[3] "From Trojan Horses to Worms: Understanding Various Malicious Threats," Symantec feature article, June 13, 2000.

In most enterprises, a variety of individual security products from different vendors have probably been implemented as network security has evolved. Enterprises are thus likely to gradually migrate to an integrated security solution, to ensure the interoperability and integration of competing security products at each network tier. Such a phased approach will initially involve the integration of a subset of security functions.

Benefits of integrated security

OPERATIONAL EFFICIENCY OF SECURITY FUNCTIONS

Integrated security reduces the need to purchase, install, update, and manage multiple security products from multiple vendors or address interoperability issues between various vendors' products at each network tier. Such a solution enables reallocation of IT personnel to other strategic projects while maximizing the productivity of the often overburdened IT department, improving security manageability overall.

MINIMIZED IMPACT OF ATTACKS ON BUSINESS

Since an integrated security solution can be implemented at all network tiers, it offers greater protection of proprietary assets. Integrated security allows for uninterrupted business operations, promotes employee productivity, maximizes revenues, and minimizes the possibility of litigation.

Features of integrated security

Due to the rapid evolution of threats, security is a constant moving target. As a result, security is only as effective as the most recent update of virus and other software. By applying a uniform approach to systems and devices that contain business-critical and sensitive information assets, organizations can ensure the integrated updating of virus pattern files, intrusion detection signatures, firewall configurations, and the other critical aspects of a security system.

Technology alone does not address security issues. An integrated security solution works best when built upon strong policies and procedures and supplemented by appropriate personnel and physical security measures. Solid security policy and standards define what needs to be protected, who is granted access, and the reason access is required. High-level support in the organization for the security policy, as well as employee awareness, helps ensure successful policy adoption.

An integrated security strategy improves the overall security posture of the network in a way not possible via implementation of individual products from many different of vendors. Whether security is handled in-house or outsourced, ensuring that all of these features are in place is vital to maintaining a secure critical infrastructure.

The future of integrated security

Organizations can now benefit from integrated security in a variety of ways, including improved efficiency of security functions, minimized business impact of attacks, and an improved overall security posture. In fact, companies that adopt an integrated security strategy today will be in the best position to take advantage of the next stage of integrated security, whereby all network tiers will be integrated and centrally managed. Through this enterprise-wide integration of security, administrator resources will be optimized, as installation, reporting, and updates will be possible from a single console. This management capability will further improve protection, while reducing the administrative, support, and ownership costs typically associated with enterprise security.

References

1. "From Trojan horses to worms: understanding various malicious threats," Symantec feature article, June 13, 2000.
2. "Trends in proprietary information loss," American Society for Industrial Security and PricewaterhouseCoopers, http://www.asisonline.org/spi.pdf, 1999.
3. Richard Power, Computer Security Institute, "Computer Security Issues and Trends," 2002 CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com/forms/fbi/pdf.html.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT HTTP://ENTERPRISESECURITY.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
408.517.8000
800.721.3934

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.