

iQ

SMALL
MEDIUM
BUSINESS

Your Business Just Got Smarter
SECOND QUARTER 2005

A Better Way

DISCOVER THE POWER
OF IP COMMUNICATIONS

PAGE 24

IAN SMITH, NEW YORK CITY
ECONOMIC DEVELOPMENT
CORPORATION

CISCO SYSTEMS



CISCO.COM/GO/IQMAGAZINE



Self-Defending

Adaptive security solutions emerge to help you manage evolving network threats.

Ron Roth knows about the challenges of operating a small business. The president of Premier Realty in Toluca Lake, California, he must take care of clients, manage employees, oversee technology, and supervise finances. But these days Roth finds himself devoting an increasing amount of time to another pressing issue: network security.

“All it takes is a virus, spyware, or another problem to wreak havoc,” says Roth, who has become all too familiar with downloading the latest patches and virus definitions to ensure that the applications on his network remain secure and continue to function properly.

“As a small business, security is crucial,” he explains. “A huge amount of time, expertise, and resources go into creating the necessary level of protection.”

A growing number of businesses find

by SAMUEL GREENGARD

Networks

Illustrations by
RICCARDO STAMPATORI

themselves in a similar situation. Although 24-hour network connectivity has fueled enormous growth and profitability for small and medium-sized businesses (SMBs), for many, protecting company resources from an ever-increasing number of potential threats has proven to be a formidable challenge.

“While some SMBs are adopting stringent solutions and strategies, too many are approaching the issue in a haphazard manner,” says Anil Miglani, senior vice president at AMI-Partners, a research and consulting firm.

Nearly half of all SMBs have yet to take even the most basic precautions—such as installing antivirus and antispyware programs, firewalls, and updated operating-system patches, according to experts at AMI-Partners. More sophisticated security solutions—such as intrusion prevention and authentication systems—are virtually nonexistent among SMBs.

The consequences of inadequate security measures can be catastrophic; the total economic damage from *malware*—viruses, worms, and Trojan-horse attacks—totaled somewhere between \$169 billion and \$204 billion in 2004, according to U.K.-based security consulting firm mi2g.

While the cost of maintaining security is a huge concern for most SMBs, the alternative is even worse: An SMB that has been affected by a security breach or attack can find

solutions are finally catching up with needs of users,” Miglani explains.

This emerging adaptive security model is based on the premise that a higher level of network intelligence can pay dividends. A self-defending network—one that can constantly adapt to threats as they evolve—can provide a secure infrastructure that identifies and manages internal and external threats, both known and unknown. This type of network provides a flexible design that speeds the deployment of services and applications, creates administrative controls that match solutions with business needs, and simplifies the integration of new solutions and technology.

Security Threats Evolve


While early computer viruses could eradicate applications and data, they offered nowhere near the payload of today’s malware. Now, new viruses stream in through e-mail attachments, instant messaging applications, and the Web, providing entrée to systems. Eventually, these security breaches can result in distributed denial of service attacks (DDoS), spamming, and theft of data directly from PCs on the network. Spyware applications can steal passwords and log keystrokes.

So-called *blended threats*, which combine different methods and assume multiple forms to attack systems in numerous ways, are raising the stakes even higher. They can unleash a variety of attacks and enable the propagation of malicious code. In a worst-case scenario, the malware might modify the system registry within PCs, erase files, change access privileges, and add destructive scripts to HTML files on a server. Often, blended threats proliferate without human intervention.

Although external threats garner much of the attention, internal threats—both intentional and unintentional—can be equally problematic. Too often, employees wreak havoc on systems by downloading games, file-sharing and instant-messaging applications, music files, pornography, and more. In some cases, these programs or files infect a PC with destructive viruses or worms that may enable a hacker to gain full control of the device.

While it might seem that attackers are more likely to focus on large enterprises, Miglani says that it’s unwise for SMBs to adopt a relaxed approach toward network security. “Small and medium-sized businesses are attractive targets for hackers and crooked employees,” says Miglani. “In most cases, people with ill intent will take the easiest path available to achieve their goals.”

A comprehensive approach to security is essential. Rapidly evolving threats—along with the sheer number of technical and practical challenges—can overpower your limited resources. The lack of integration between devices and systems often leads to breakdowns; in many cases,



IN BRIEF

GOALS: As threats evolve, SMBs must find ways to effectively manage network security while tightly controlling the costs and resources necessary to do so.

STRATEGIES: New adaptive security solutions are emerging that combine several formerly standalone tools into a single, integrated security device.

RESULTS: By combining disparate solutions into one device, adaptive security products simplify security management, helping SMBs to proactively detect security threats and minimize the damage they cause.

itself facing customer-satisfaction issues resulting from lost or misplaced data, struggling to conduct business, or—even worse—going out of business altogether.

“There’s no simple panacea. Today, defending a network requires layers of security, and it requires having systems in place that can create redundancies,” states Victoria Fodale, a research analyst for market research and consulting firm In-Stat. “Highly integrated solutions that reduce complexity and cost are essential.”

Fortunately, more sophisticated solutions are now available. Network-based antivirus solutions, desktop-based firewalls, and effective antispyware applications are helping to fortify computing environments. In addition, the emergence of software suites and security appliances that consolidate an array of functions are making it easier to approach security in a reliable and cost-effective way. “The

business leaders believe that the network is secure, when in reality the network is susceptible to security threats.

Vignette, an enterprise content-management firm in Austin, Texas, has approximately 750 employees and powers the Web applications for customers such as the 2004 Olympic Games in Athens. For Vignette, protecting the network is a top priority. "Security is a big concern—not only for our customers but for our internal employees as well," says Selim Nart, a senior network engineer at the company. "Security brings a peace of mind and trust in Vignette, and we have to provide this to our customers."

Vignette is a technology-savvy, network-centric company—one with a comprehensive security policy in place—but it faces many of the same issues as other companies: maintaining, updating, and managing multiple disparate security solutions. "It is a challenge to manage many appliances such as firewalls, intrusion prevention, wire scanning, and monitoring," explains Nart.

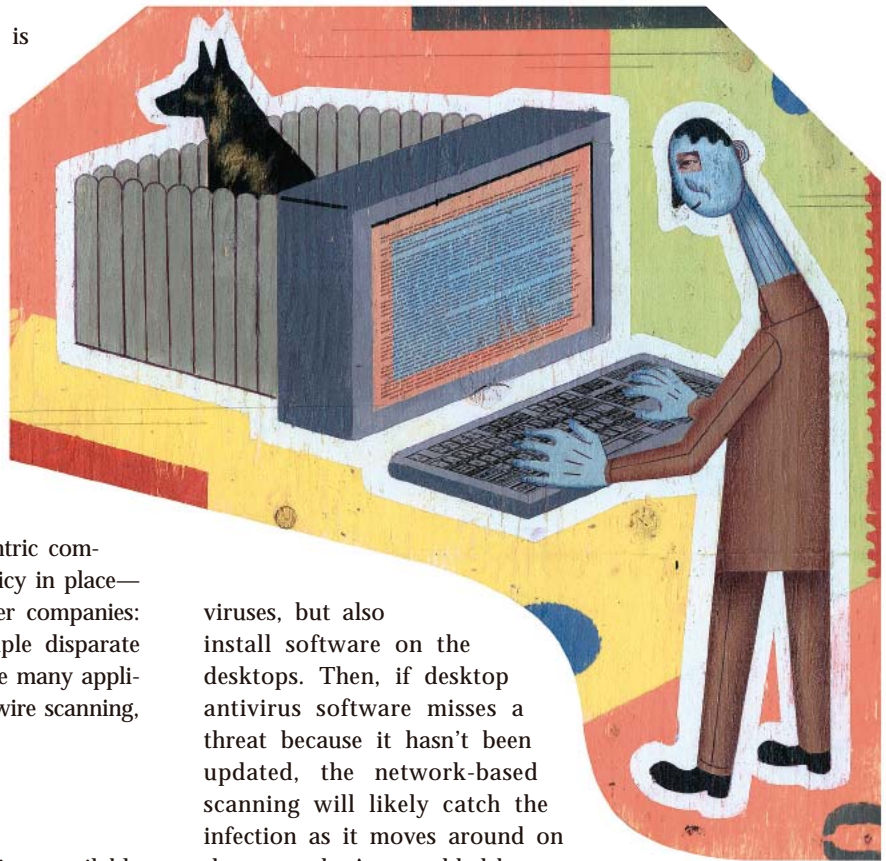
Playing it Safe

Fortunately, the technologies and applications available to thwart security breaches are also evolving. Leading technology vendors are now introducing integrated solutions that offer all the major security capabilities in a single device with turnkey integrated management.

These systems offer network-based antivirus protection, spyware controls, intrusion prevention, firewall, virtual private network (VPN) support, and other functions in a single network appliance with unified management. One example is the Cisco ASA 5500 Series Adaptive Security Appliance, which the company just introduced as part of the Cisco Adaptive Threat Defense initiative. (To learn more, read "The Cisco Adaptive Security Appliance," on page 45.)

"The goal is to centralize administration capabilities and avoid time-consuming and relatively expensive [specialty] solutions," Miglani explains. More broadly, the primary aim of today's security solutions is to preempt attacks by preventing perpetrators from reaching their targets in the first place. Simply put, the closer to the network's entry point that the organization stops an attack, the greater the odds that the virus or worm won't proliferate. Sophisticated preventive capabilities are therefore increasingly important, since attacks can now spread across an entire network and begin wreaking havoc in a matter of minutes.

Integrated security appliances add an extra layer of protection, according to Fodale. For example, you can use a device at the perimeter of your network to scan for



viruses, but also install software on the desktops. Then, if desktop antivirus software misses a threat because it hasn't been updated, the network-based scanning will likely catch the infection as it moves around on the network. As an added bonus to this dual-pronged approach, a business can catch so-called "polymorphic viruses," which change with each infection. "The goal is to eliminate a single point of failure," Fodale explains.

Self-Defending Networks Emerge

The quest to develop a secure infrastructure has created a heightened interest in so-called "self-defending networks," which provide holistic protection and adapt to changing conditions quickly and effectively.

"The end goal is to fortify a network so that it is protected from the [network] jack in the wall to the back-end server. It's all about creating a more proactive and automated environment," says Scott Pope, a manager of VPN and security product marketing for Cisco Systems.

Self-defending networks also integrate and connect network and security technologies, making them even more powerful. As a result, networks like these can function across different operating systems, hardware platforms, and security devices, including dedicated security appliances, routers, and switches. They can support converged data, voice, and video applications such as IP telephony and authentication solutions. Finally, they can work across multiple user environments, including local-area, wide-area, and wireless networks. This flexibility extends network

protection beyond the main office: With a self-defending network, branch offices and mobile workers are also protected from security threats.

For SMBs, these improvements in network-security applications mean far more advanced functionality, including role-based and rules-based logic. For example, a system not only looks at files or e-mail messages for specific signatures or patterns associated with virus definitions but it is also able to detect unusual system behavior, such as attempts to modify files. In addition, the system can readily identify unusual log-on patterns or data streaming inexplicably across a network. And if someone attempts to install a program or software component, the system generates a pop-up message requesting confirmation from the system's administrator; without approval, the system automatically prevents the installation from occurring.

Adaptive Security

Today, the most sophisticated devices combine multiple functions and advance the concept of a self-defending network to a higher level of sophistication and effectiveness.

These devices provide adaptive threat defense, which employs core security enforcement technologies such as firewalls, intrusion-prevention system (IPS), network antivirus and anomaly detection to deliver *Anti-X* defenses, application security, and network containment and control solutions. *Anti-X* defenses respond to attempted security

network is able to evolve in order to react to changing conditions," explains Cisco Program Manager Chad Reese. "It greatly reduces the need to monitor systems and evaluate their effectiveness. It can help a business function more strategically."

Miglani agrees. "The idea of adaptive security represents the future of network protection," she says. "The need to

"The need to adapt and evolve in response to threats will only continue to grow."

—Anil Miglani, AMI-Partners

adapt and evolve in response to threats will only continue to grow."

For Vignette, an adaptive security approach simplifies the job of providing the safe network environment it requires to develop and deliver products to its own customers. Vignette was among the first companies to pilot the Cisco ASA 5500 Series. "With the Adaptive Security Appliance, you can pull all the tools together in a single box, a single management console," says Nart. "It's easy to use, easy to manage, and easy to deploy. And it saves us on the cost of real estate, electricity, data-center spacing, shipping, and management."

With an adaptive security approach, intelligent networking technology bears more of the burden of protecting your network, requiring fewer employees and resources but resulting in more effective network security.

"Having many people does not solve the issue, but having a smart, manageable environment brings us the greatest flexibility with our customers and employees. Adaptive security helps us manage our environment in the most flexible, simple, and deployable way," says Nart.

All Systems Go

An effective security strategy involves more than the sum of its technological parts. It also requires that you develop rules for how systems should respond to security threats, guidelines for IT and other departments, and policies that establish the kind of software and access privileges that employees should have. Without a solid foundation to address corporate-culture issues, even the best security systems can fail. Employees must know which types of applications and content they can load onto their PCs, what level of access they have to applications and files, and how they can manage content and

TALK TO A CISCO EXPERT

Call **1-800-745-8308, ext. 4603** to get more information about Cisco Self-Defending Networks.

breaches—and ultimately prevent them—through a combination of traffic- and content-oriented security services such as network antivirus, antispymware, antispam, *antiphishing*, and DDoS mitigation. This approach contains malicious traffic before it can spread across the network.

The second category of network protection includes application security, which operates through application-level access controls, application inspection, and the enforcement of application-use policies, Web-application control, and transaction privacy.

Finally, self-defending networks enable network control and containment. With greater network intelligence in place, it's possible to use sophisticated auditing and correlation capabilities to protect networked applications from attacks.


Ultimately, the ability of these systems to adapt to evolving threats and respond to them in a flexible, dynamic way is what makes them so compelling. "A self-defending

exchange files using various security tools and features.

Education and training play a vital role in this process. It's important that employees understand the importance of logging out of the system or locking their screens when they leave their desks, creating effective passwords and changing them regularly, encrypting sensitive files on their laptops, and maintaining adequate security on home PCs or devices that connect to the company network. According to Fodale, it's also important for employees to understand how systems become infected in the first place, and how they can play a role in preventing damage.

When all the pieces come together, it's possible to transform network security from an overwhelming proposition into a highly manageable process. Instead of constantly reacting to threats and scrambling to keep up with the dizzying array of risks, you can instead devote more time and attention to the core issues of running your business

in the most efficient and effective way possible.

"A business is finally in a position to reap the potential of the Information Age rather than becoming a slave to it," concludes Miglani. 

SAMUEL GREENGARD IS A BURBANK, CALIFORNIA-BASED BUSINESS AND TECHNOLOGY WRITER. HE CONTRIBUTES REGULARLY TO *IQ* MAGAZINE.

NEXT STEPS

Go to cisco.com/go/iq-adt to learn more about the Adaptive Threat Defense initiative.

Visit cisco.com/go/iq-asa5500 for more information about the Cisco ASA 5500 Series Adaptive Security Appliance.

Read "Addressing Network Security" on page 71 for strategies to help you create a comprehensive approach to network security.

Use the free Cisco Security Policy Builder tool (cisco.com/go/iq-spb) to help you start developing a sound network-security policy.

FROM CISCO

THE CISCO ADAPTIVE SECURITY APPLIANCE

In the past, developing a self-defending network was seemingly *Mission: Impossible*. However, the introduction of Cisco's self-defending network has changed the security landscape—and introduced a new era of network protection and cost efficiency.

The self-defending network dramatically improves an organization's ability to identify, prevent, and adapt to threats by harnessing a comprehensive suite of leading security technologies. The technology core of the self-defending network is Adaptive Threat Defense, which intelligently combines multiple security technologies to deliver a more proactive and effective network defense and streamlined security operations.

Cisco's newest innovation in Adaptive Threat Defense is the Cisco ASA 5500 Series Adaptive Security Appliance (pictured at right). The Cisco ASA 5500 architecture combines the latest innovations in security technologies, integrating Cisco's market-proven firewall, intrusion prevention, network antivirus, and virtual private network (VPN) services. Offering a unified management package, the ASA 5500 delivers strong performance for concurrently running services, and provides simplified management for enterprise and

SMB applications.

The Cisco ASA 5500 delivers a tighter, more proactive threat defense that stops attacks before they spread across the network. It also controls network activity and application traffic while reducing operational complexity. Diverse enforcement capabilities, resilient firewall technology, and traffic inspection for intrusion prevention enable it to preempt a broad range of threats, including worm and application layer attacks. Add network antivirus services to the mix, and the result is a set of threat-mitigation services capable of detecting and thwarting today's most damaging network attacks.

Perhaps more important, this approach virtually eliminates the need to make difficult—and often risky—choices about which security technologies to deploy in specific locations.

While improving network security, the Cisco ASA 5500 also decreases the cost and time associated with operating and managing systems. Because of its broad VPN and security services capabilities, it is a multifunction device. An organization can monitor threats from a central site,



using access-control, application-inspection, and threat-mitigation technologies simultaneously. This adaptive approach of integrating multiple applications onto a single device minimizes the number of platforms that an organization must manage, while offering a common operating and management environment.

In addition, standardizing on a common platform with unified management increases staff knowledge and expertise on a single platform, which can simplify configuration, monitoring, troubleshooting, and staff training.

Scott Pope, a manager of VPN and security product marketing for Cisco, says the ASA 5500 can lower costs by reducing the number of single-purpose security devices that an organization uses across a network. Furthermore, it can minimize costly and time-consuming upgrades by enabling the deployment of new security technologies without installing new hardware.—S.G.