

synnovation



Vol. 1 Issue 3

Beating the Odds

Leading an organization through a risk-laden environment is often a game of chance. But enterprise risk management can help your odds.

EDS

Unwelcome Surprises

By Al Decker

Towers Perrin

Coming of Age

By Prakash Shimpi

Microsoft

Defending the Crown Jewels

By Ron Markezich

Oracle

Protect, Detect, Deploy

By Vipin Samar

Dell

Super Power

By Dr. Reza Rooholamini

Sun Microsystems

Tapping Tag Power

By Jim Del Rossi

Xerox

For the Record

By Charles P. Brett

EMC

Reaching Out

By Gregg Therkalsen

Cisco Systems

A Matter of Self Defense

By Bob Gleichauf

EDS

Conversations

With Ron Rittenmeyer

Microsoft

Up Close and Personal

With Ron Markezich

A Matter of



SELF

DEFENSE

By Bob Gleichauf, Cisco Systems

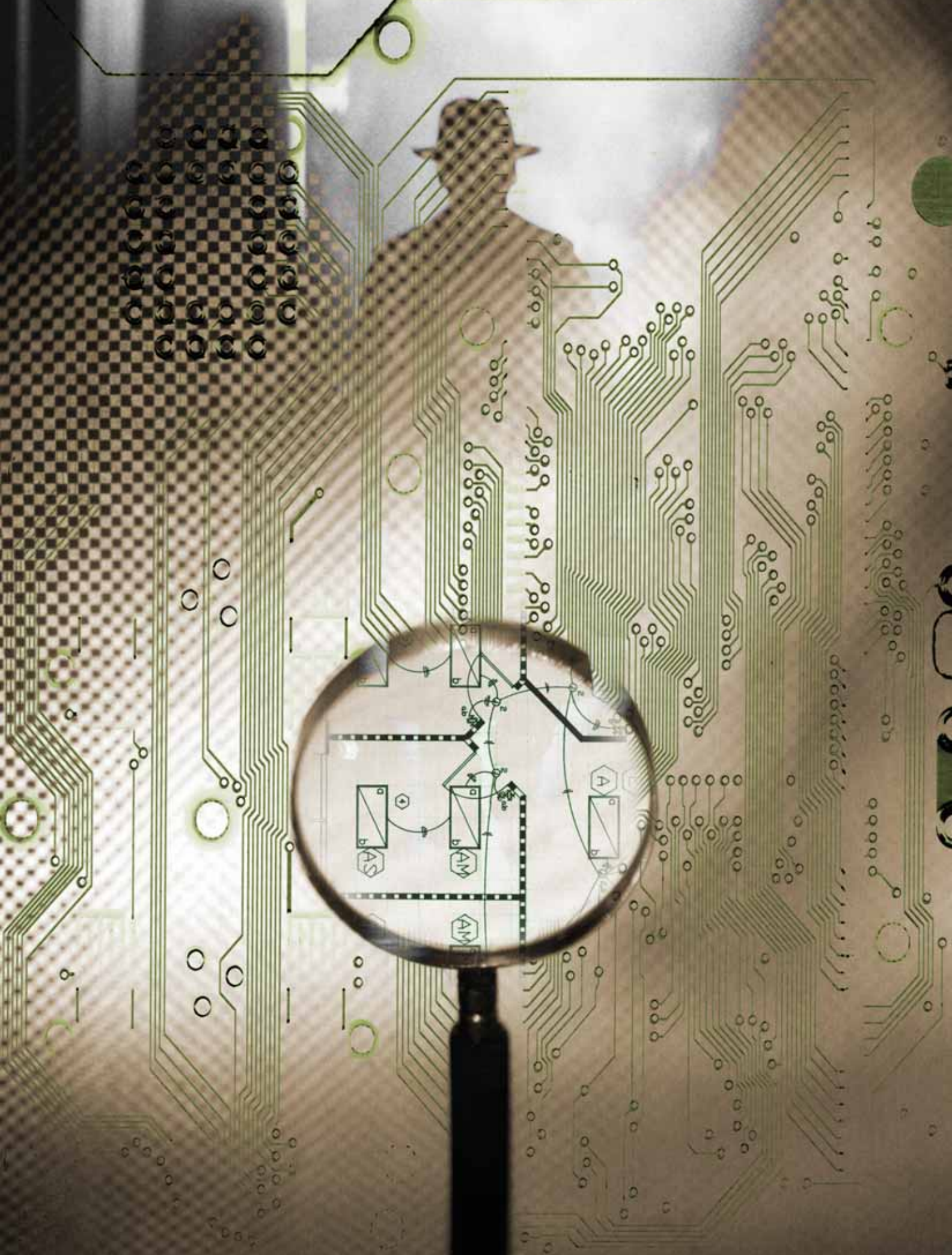
The Business Value of Self-Defending Networks

N

Not long ago, the most serious threat to an enterprise was a 15-year-old who spammed web sites on a double-dare from his friends. Those were the good old days. Now, we read the following headlines:

- "Attack Knocks Out Buy.com"
- "Hackers Reverse-Engineer Vegas Slots, 'Win' a Million Dollars"
- "Trojan Exploits Zero-Day Vulnerability in Microsoft Word"

As these headlines attest, today's cyber thieves are a much more serious threat. They go after customer information, intellectual property, bank account numbers, and anything else of value. Organized crime syndicates, drug cartels, and ex-employees with a grudge are >>





To keep the bad guys out and let the good guys in, security on open networks must be pervasive—it must deliver end-to-end protection.

spending a lot of time and effort creating focused attacks that will reap millions, take down businesses, or achieve other nefarious goals. Ironically, today's online business models make their jobs even easier. Organizations are opening their networks to customers, vendors, and partners to sell products, verify credit, speed purchase orders—in short, to cut costs and increase sales and customer satisfaction. But those benefits are offset by increased risks.

Until the mid-'90s, companies primarily used the Internet to send e-mails, conduct research, and provide limited file and print sharing. Their biggest security concern was preventing virus attacks, which were more of a nuisance than a danger to the bottom line. When organizations started doing more business online, however, it didn't take many security breaches to get their attention, as when a worm burrowed into **Air Canada's** logistics network and grounded its worldwide fleet for 16 hours. Or when a denial of service (DoS) attack forced a start-up hosting company to burn through \$150 million in venture capital in two weeks and eventually go out of business.

Self-Defending Networks Close Security Gaps

The industry's initial response to these attacks was to add "point" solutions to the network—firewalls, virtual private networks (VPNs), encrypted communications, antivirus servers, and so on—rather than taking a comprehensive approach to

security. Those point solutions are no longer enough to counter the latest forms of misuse, an issue compounded by the fact that the point products rarely work well with one another. The tendency to mix products from a wide range of vendors in pursuit of a "best-of-breed" strategy also increases costs and slows response to the latest threats because administrators must deal with a variety of vendors for support.

To keep the bad guys out and let the good guys in, security on open networks must be pervasive—it must deliver end-to-end protection. Cisco calls these "self-defending networks" (SDNs). SDNs have defensive features designed into such infrastructure products as switches, routers, and endpoints, which are fully integrated and can communicate with each other. SDNs also provide interfaces to security applications that reside on customers' servers and client infrastructures. This approach weaves security into the network fabric so that intelligent networking features work with security applications to provide a coordinated response, without the gaps inherent in classic perimeter-based security architectures. Within an SDN, networks and endpoints can benefit from the unique information the other possesses, creating an environment where one plus one equals three.

Security Requirements Evolve with the Business

The days of defining best practices for a firewall or VPN without a proper appreciation for the business are over. Also, it's insufficient to focus only on protecting your data—because that data frequently changes as it passes from one area to another within an organization. To truly secure your business infrastructure, you need to understand the transactions that make up the business: the applications, the users, the data, as well as the underlying infrastructure. >>



REUTERS/SHAUN BEST

Securing Montréal's Transit Network

The city of Montréal's transit system, the **Société de Transport de Montréal (STM)**, relies on Cisco Systems to keep its network up and running and its operations secure 24x7.

STM operates four subway lines, a fleet of 759 cars serving 65 metro stations, 1,567 buses, and 94 paratransit minibuses that, combined, make more than 1.3 million trips each weekday. The transit system's IT department acts as the nerve center to maintain the availability and confidentiality of its 120 information systems on this extremely complex network, which includes a routing and switching infrastructure that supports 165 servers, 6,000 hosts, and more than 7,400 employees.

Payroll data and employee records traverse STM's network each week. With its online recruiting applications and planned credit card-based ticket-sales system that stores personal information, the transit system's web site presents a highly visible target for hackers. STM is also a public company, regulated by several municipal, provincial, and federal agencies, which require compliance to standards for data and network security and extensive reporting.

The network registers about 5 million suspicious events every 24 hours—and 2,000 incidents per day. After filtering out false alarms, IT technicians must manually investigate about 200 events

daily, which requires looking through 30-megabyte system logs with hundreds of thousands of lines of data. Faced with these challenges, STM employed state-of-the-art defenses from Cisco, including Catalyst switch-based firewall and intrusion-prevention system (IPS) services, the Cisco VPN 3000 Concentrator for secure remote access, and the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS).

Today, the STM IT department can identify and respond to security threats more quickly and efficiently than ever before. Those advantages translate into substantial productivity increases for the staff. In addition, by providing a real-time picture of activity across the network, Cisco Security MARS offers management capabilities that go beyond network security. The solution has also greatly helped the STM IT department with regulatory compliance by decreasing the time spent doing audits as well as increasing the accuracy.

Shortly after the systems were installed, a worm attacked a PC in one of STM's garages. The network detected it immediately and shut down the PC's switch port within minutes. Without the solution, the PC would've likely infected the 75 other PCs in the building within an hour. And from that point, the situation could have gotten even worse.



If, for example, a retail company that relies on Internet-enabled cash registers wants to add online bridal registries at every retail outlet, it must deal with a number of issues to implement an end-to-end SDN. At a minimum, the retail store needs firewall protection and secure VPN connectivity from the bridal site to the corporate site, and from the corporate site to the warehouse. The store also needs to protect against potential DoS threats to the bridal registry and cash registers by putting in place the right systems to maintain minimal quality of service (QoS) for each application. This means that having the firewall close ports in the face of DoS is no longer appropriate, as that would shut down legitimate transactions along with the offending traffic. The goal is to keep the business running—not to shut it down. Instead of closing down ports or locking

out traffic from offending service providers, an SDN uses advanced anomaly-based services to scrub offending traffic from the legitimate traffic.

The machines that run applications—in this example, the bridal registry and cash registers—frequently have a general-purpose operating system such as Microsoft Windows. Protecting these machines can be a challenge because they can't be treated the same as a desktop computer. In an SDN, these systems are guarded by special software agents that monitor the operating system for activ-

ities that deviate from established norms and stop those activities before they can compromise the system. This approach allows the cash register and bridal registry systems to be protected without needing to track and install operating system patches or deal with ongoing anti-virus updates. And this frees the retailer from needing to hire an operating system expert for each of the retail store's outlets.

An SDN also needs to compensate for the realities of ever-changing business environments. It's not uncommon for application developers to deploy upgrades that disrupt existing security. For example, providing end-to-end security for the cash register application via Secure Socket Layer (SSL) hides the traffic content from the firewall and intrusion prevention services deployed at the network edge and can actually make it easier for malware to travel from one domain to another. In

an SDN, the endpoints can share information with the network services to re-establish comprehensive visibility into business transactions.

Lifecycle Approach to Security

No matter how well a company secures the business environment, it's a good idea to bring in a trusted third party to perform regular security assessments of the entire business. Organizations must know where they're at the greatest risk so they can make wise security investments and not inadvertently spend money in the wrong places.

Regular external security posture assessments are recommended because security is most effective when viewed from a lifecycle perspective—it's not a one-time fix. Partners, applications, and business goals change on a regular basis at the same time that hackers are looking for new ways to wreak havoc. SDNs compensate for this problem in two ways:

- SDNs are designed to stay up-and-running and conduct commerce even if they're infected or have other security issues.
- SDNs are based on a defense-in-depth model, which has intelligent layered security features to detect and compensate for threats that slip past classic perimeter defenses.

A Healthy Network

An SDN is like the human body's immune system. A healthy immune system allows us to function even if our allergies kick in or we catch a cold. A sophisticated SDN provides the same protection for an organization. When it discovers a threat, it triggers a variety of services that eradicate or neutralize the danger and keep the network running. Having an infection is not the same as being compromised.

For example, one SDN feature is an early-warning service. As soon as a virus application identifies a signature for a new threat, a warning is propagated through all security mechanisms. This service is specifically designed to minimize the impact a zero-day virus (one for which no patch is yet available) can have on a company's infrastructure. The early-warning service creates a dampening effect: It reduces the number of systems and the number of entry points where the virus can spread so IT technicians have more time to identify the root cause and take appropriate action. Shutting down the network is not an option. >>

No matter how well a company secures the business environment, it's a good idea to bring in a trusted third party to perform regular security assessments of the entire business.



PHOTOS COURTESY OF CISCO SYSTEMS

August 10, 2005, marked the first time in 34 years that the NASDAQ Stock Market conducted opening and closing ceremonies from outside New York. Three thousand miles away at Cisco Systems' San Jose, Calif., headquarters, Cisco and NASDAQ recreated the Market-Site, including a replica blue video wall and electronic podium to mirror the NASDAQ opening and closing bell ceremonies. Cisco president and CEO, John Chambers, along with 2,250 Cisco employees, rang the bell to signal the start of trading from a "virtual" control center, complete with NASDAQ's famous video wall that provides trading updates throughout the day.

Stock trading information is among the many kinds of critical data transmitted over networks, and it demands the security of self-defending networks. This historic event was made possible thanks to a dual path, secure, private IP network. Cisco's Internet protocol (IP) networking equipment and software transmitted NASDAQ trading information from New York to San Jose, highlighting the benefits of IP technology, network-based security, and virtualization for business and society.



Defense-In-Depth Protects Against Emerging Threats

A defense-in-depth approach recognizes that every defense has limitations that must be dealt with by other services. The goal is to implement a comprehensive solution for securing the infrastructure, because you may never discover all of the places someone can pry into your network. Some weaknesses are side effects of well-intentioned security policies. These adverse effects must be anticipated and addressed or they can cause more trouble than the initial problem.

For example, in an effort to comply with privacy regulations, some banks encrypt every bit of customer data. In one instance, however, worms entered the network of a global bank through encrypted links and moved through the system undetected. The resulting infection took longer to discover, cost more to eliminate, and caused greater damage. This was a case of good intentions going awry because all potential side effects were not considered and compensated for.

Plugging Data Leaks

Another area of security where SDNs are making advances is controlling where data can and can't go. The unauthorized release of files affects businesses in every industry. Newspapers are filled with stories about the theft of personal identity information, trade secrets ending up in a competitor's hands, and confidential reports published online. One solution is to carefully assess the role of every employee in the enterprise, assign employee access to the network at a level appropriate to the job description, and strongly enforce the policy. This would go a long way toward stanching data leakage, but it would not eliminate leaks completely, because as business processes change, new security leaks appear that are nearly impossible to predict or prevent with point solutions.

For example, in certain countries, there may be regulatory or legal requirements that constrain the movement or transmission of customer data from one country to another. But consider this common scenario: A banking executive, located in one country, plugs her laptop into the company network and downloads customer records, and then catches a flight to another country. The moment she and her laptop enter customs, she could be violating the privacy regulations or laws of her originating country. If the executive remotely logs onto the corporate network from another country and downloads more customer data to her PC, she may again be violating certain regulations and laws of the country where the information origi-

nated. This violation and potential data leak aren't detected by point technology.

So how do you enforce access based not just on rules but also on variables such as geographic location? Security applications alone are not the answer. Classic AAA services—authorization, authentication, and audit—are no longer sufficient to deal with the complexity of the business environment we live in. Cisco is currently exploring how SDNs can work with applications to address such subtle scenarios by looking at role-based information in a broader context. IT departments need more tools to help them determine how data is moving around their networks and crossing unacceptable boundaries.

This is a very tough security challenge, and significant investments still need to be made by both industry and customers to properly address this problem. Any solution must ultimately tie back to an organization's needs and processes. These determine where data can and can't go.

Security Represents Business Value, Not Overhead

The advantages of a self-defending network include:

- The integration of security throughout all aspects of the network
- Collaborative processes between various security and network elements to quickly contain and eliminate threats
- The ability of the network to adapt to new threats as they arise

Taken together, those advantages provide a more robust business infrastructure and markedly better security against today's high volume of attacks, as well as a higher return on security investments.

An SDN, however, is not just technology. It's also the people, processes, and, these days, regulations that shape the business. An SDN is only as good as the policies that drive the security infrastructure.

Even with the best defenses, security is not an all-or-nothing proposition. Policies must strike a balance between acceptable risk and protection of the infrastructure. The result is an agile defense that makes security devices aware of network-wide activity so that they can develop a coordinated response based on business priorities. |s|

About the Author: **Bob Gleichauf** is vice president and chief technology officer, Security Technologies Group, Cisco Systems, Inc.



