CSO Custom Solutions Group

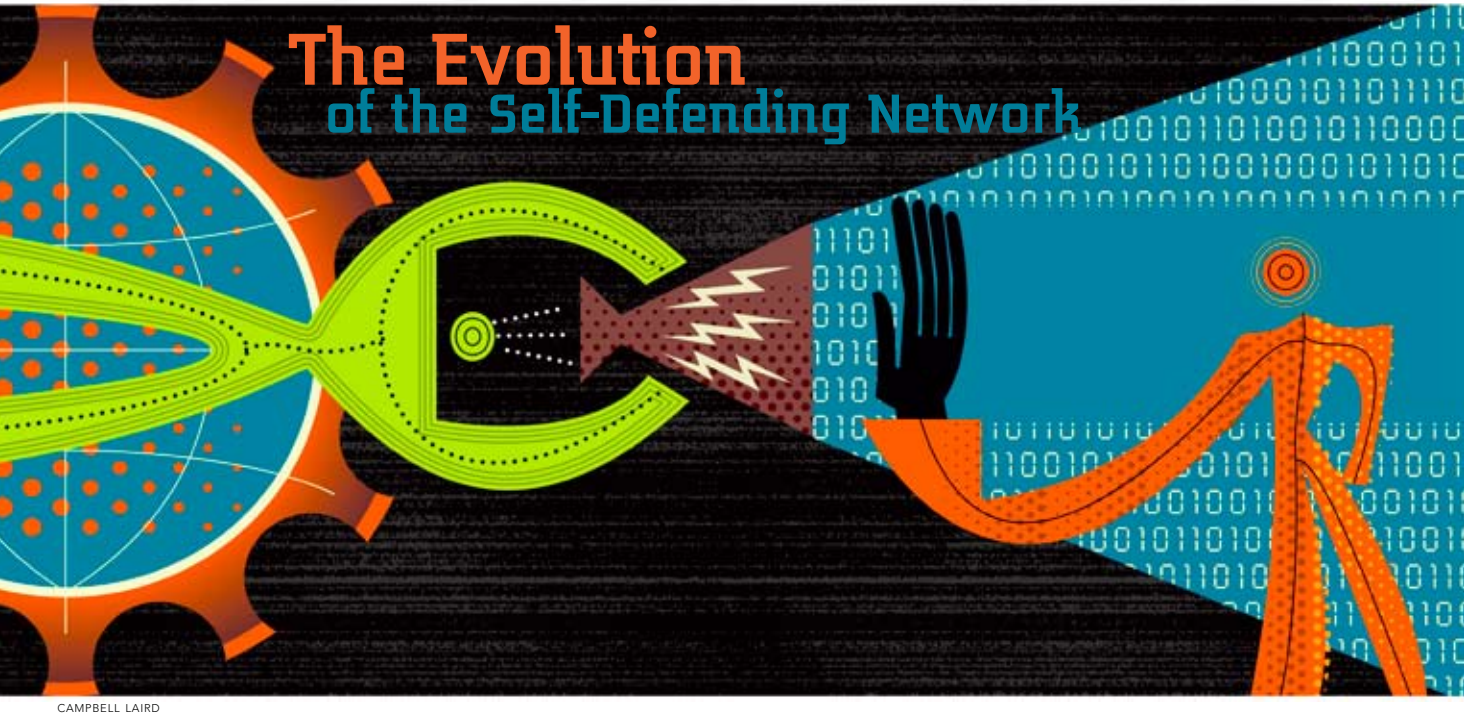
cisco

Executive Summary

The constantly-changing landscape of cyber threats and increasing automation of business processes underscores the necessity of the self-defending network. Many CSOs are successfully throttling attacks with adaptive security strategies that leverage deep integration and collaboration between components. This report explores how these strategies are quickly evolving and expanding to address the next generation of threats.

The Best Defense

The Evolution of the Self-Defending Network



CAMPBELL LAIRD

The global Internet continues to change how we work, live, play and learn. For the better, it's connecting people, information and business processes in ways we could never have imagined. For the worse, it's creating greater opportunities for a sophisticated new breed of criminals whose imaginations are now hard at work.

"As we've gained control over many aspects of security, the bad guys have gone deep underground and stealthily refocused on the doors that traditional security solutions have left open—namely web, email, and instant messaging traffic," says Scott Weiss, former CEO of IronPort and now general manager of the IronPort Business Unit at San Jose, CA-based Cisco Systems, Inc.

The nature of the today's attacks is simply "more"—more complex, more frequent, more vicious and especially more targeted than ever before. Hackers have graduated from annoying pranksters to full-fledged criminals spurred more by financial gain than the underworld notoriety that comes with unleashing a particularly nasty virus or worm.

The fact is, today's attacks translate into big business. Online drug sales grossing millions from illegal activity. Trusted websites infected with silent

Getting Started

Advice from the Experts

When it comes to getting started, our experts from Cisco offer some learned advice to put you on the right path to building a winning self-defending network:

- Start the journey by proactively piloting new capabilities, learn from deployments and then scale as required.
- Accept that security technologies are more systematic, touching more components of the infrastructure; approach your strategy from that perspective.
- Integration and cooperation among security services are the underpinning of success.
- Do a thorough X-ray of your network, so you know exactly what's going on and what isn't.
- Users can be a weak link—especially with desktop tools like i-Phones and PDAs—but creating the right security culture is a great way to get them involved.
- Security is essentially risk management, so it always boils down to a tradeoff discussion and making some tough calls.
- Remember, the great unknown problem is the next area to clean up. Make sure you're ready when it hits.

spyware designed to steal valuable corporate data. Large-scale credit card fraud and identity theft scams. What's more, these criminals are looking to cash in big—usually at significant expense to enterprises.

Network, Defend Thyself

With integrated, proactive security technology or "self-defending networks," many CSOs are beating these stealthy evil-doers at their own games.

"A self-defending network is essentially a strategy and vision oriented around linking security services so they are able to collaborate and act adaptively to proactively protect against evolving threats and security situations," says Richard Palmer, senior vice president and general manager of Cisco's Security Technology Group. "It enables CSOs to simplify policy and management so the network components can enforce security policy with minimal manual intervention."

The underlying concept is simple: Instead of approaching enterprise security as a mishmash of stand-alone components, a self-defending network considers security as the sum of its parts. Thus, security services are deeply integrated into the network, sharing information for higher levels of protection and ever-evolving to address constantly changing security requirements.

"Better Together" Approach to the New Threat Landscape

It is the self-defending network's demonstrated ability to adapt and expand with the changing threat landscape that makes it so appealing to CSOs.

"Over time, increasingly complex threats have been the key driver in the evolution of the self-defending network," says Weiss. "The original focus was on locking basic access and keeping hackers out by using firewalls and VPN systems. Then, deep packet analysis was introduced, including the integration of intrusion prevention systems with firewalls, switches and routers."

"These tactics proved to be extremely effective against timely threats—namely, viruses and worms—and such activity has fallen off significantly," adds Palmer. "But CSOs are not getting complacent; instead they are moving up the stack for wider protection."

Protection, that is, against a sophisticated new breed of threats, he says. Some blend email and web technology and are launched as increasingly targeted and stealthy attacks. Others are polymorphic attacks that evolve very rapidly, exploiting different vulnerabilities in succession in an effort to outsmart enterprises toward a very specific end. Examples:

fraudulent email messages that seem to come from the IRS, messages from friends that contain links to corrupted web servers, or even trusted entertainment web sites being used to silently serve up spyware intent on hijacking unsuspecting devices.

Such malicious ingenuity has lead to a major shift in the industry, forcing the convergence of traditionally separate network, content and application security markets. Meaning, there's a newly evolved self-defending network that combines tried and true network-level security with next-generation capabilities for inspecting email, web and instant messaging traffic. Such wide traffic inspection techniques essentially aggregate worldwide threat intelligence from sources inside and outside the network—for improved protection against a wider array of threats.

The "new and improved" self-defending network is all about broader component collaboration. This includes a comprehensive approach that extends beyond the perimeter and spans all networking levels—from the packet to the content. So, for instance, content can be flagged for examination when suspicious traffic patterns are identified. Perhaps most compelling, wide traffic inspection brings cooperation to a worldwide level by sharing intelligence beyond the corporate network to envelop threat data for email and web servers throughout the global Internet.

Wide traffic inspection is supported by reputation scores provided by services like SenderBase. Every IP address from every email server that makes a connection is assigned an aggregated spam probability; the lowest being near certain spam and the highest being most likely legitimate. Reputation scores consider positive attributes like whether the IP

Inside SenderBase

The World's Largest Email and Web Traffic Monitoring Service

The SenderBase Reputation Score (SBRS) is a wide traffic inspection service that enables security appliances to weed out suspicious email and web content—before it hits the network.

SenderBase collects and correlates data on the behavior of a large and wide spectrum of active email and web servers throughout the Internet, measuring parameters such as how long the server has been delivering content, its country of origin and whether any content has proven to be spam or malware. In addition, threat insight comes from industry "blacklists" and participants in the SenderBase Network can "opt in" to sharing data. All told, SenderBase aggregates threat intelligence from more than 100,000 sources, including ISPs, universities and enterprises from around the world.

Over 150 attributes in all are used to determine a sender's reputation score. Each factor is assigned a weight, based on the historical probabilities that messages from an IP address with that characteristic were spam. Individual probabilities are aggregated using an advanced algorithm—which produces an overall probability that the content coming from a given IP address is spam or malware. Then the aggregate reputation probability is mapped to a score between -10 and +10.

In the case of spam, this score ultimately allows security appliances to automatically apply appropriate mail flow policies for blocking suspicious senders or allowing trusted senders to bypass spam filters. Not only does this prevent widespread infection, but rejecting known suspicious mail at the beginning of a transaction can significantly improve system performance due to reduced filtering volumes.

"This reputation data is what connects content and network security across protocols to support wide traffic inspection and deliver holistic protection for the enterprise,' says Weiss. When an email arrives and is determined to be a phishing attack, any URLs the email contains are passed to a web security device to ensure that other end users aren't getting hit with a variant of the attack. Similarly, when the web security appliance detects malicious content coming from a web server, any emails that contain URLs that point to that server are carefully examined or blocked.

Such cooperation increases overall network defense exponentially.

Cisco Self-Defending Network

Better Together

Integrated security systems that can collaborate and share threat data across protocols, network boundaries and the global Internet offer a very strong and adaptive defense against the efforts of even the most creative cyber criminals. Bringing IronPort into the Cisco fold is helping CSOs make major strides toward this goal. The combined company integrates IronPort's industry-leading content security appliances, SenderBase, the worlds first and largest email and web traffic monitoring service, and Cisco's broad array of network infrastructure and security products. The result is a highly-evolved, self-defending network that will prepare enterprises for whatever new threats should arise in the future.

address is controlled by a Fortune 1,000 company, and more important, negative attributes such as its inclusion on an industry "black list," the number of messages sent to "spam traps," and the validity of message recipients.

In the end, policies are automatically applied to block known bad senders. This stops suspicious senders in their tracks, while allowing trusted senders to bypass spam filters altogether—resulting in greater outer-layer defense for the network and less stress on the system.

CSOs are not getting complacent; instead they are moving up the stack for wider protection.

"Wide traffic inspection exemplifies the guiding principles behind effective self-defending networks," says Palmer. "Not only does it leverage integrated security capabilities in network, but it's collaborative in nature and adaptive to emerging threats."

Bringing It All Together in the Real World

"This 'better together' effect is at the heart of wide traffic inspection technology," says Weiss. "Meaning, the promise of the solution grows as cooperation extends beyond the perimeter, starts to span all networking levels and pushes past the individual corporate network."

He explains how that cooperation might work in the real world: When a desktop client detects a new "zero day" attack, the signature of that exploit can be captured and sent to perimeter equipment to block further spread of the attack. If packet level analysis identifies suspicious traffic patterns, the content from that transaction can be examined more carefully with content-aware devices. And these analyses can be shared across individual corporate networks to provide a global view. "Taken further, as Network Admission Control [NAC] systems begin to be incorporated into wide traffic inspection, the illicit activity detected at the firewall can be shared with the NAC systems to ensure that infected clients are automatically quarantined and remediation measures launched," Weiss says.

Scenarios like these translate into real world rewards. This converged approach to security leverages traditional capabilities in new ways with more intelligence and more effective policy controls, so CSOs can simplify the operational environment and reduce manual intervention. In addition, CSOs can dramatically improve the overall security health of their enterprises with big-picture, global views of security threats, and by casting wider nets for identifying vulnerabilities inside and outside their networks. Of course, that level of visibility can net real results in helping organizations to achieve higher levels of compliance. The "better together" approach, combining network and content security, is the only sure-fire way to do all of that.

In the end, concludes Palmer, "a self-defending network strategy enables CSOs to more effectively and cost-efficiently deal with security threat environments."

To learn more about the Cisco Self-Defending Network, visit www.cisco.com/go/sdn