Customer Case Study

Simpler-Webb Uses Cisco Security Solutions to Provide Enterprise-Class Protection for Small Business Customers

Managed services firm Simpler-Webb uses Cisco security solutions as the foundation of its managed security services offering. The solutions bring sophisticated intrusion prevention and mitigation tools to the firm's small- and medium-sized business customers.

EXECUTIVE SUMMARY

Simpler-Webb

- Technology/Professional Services

BUSINESS CHALLENGE

- Deliver strong protection against worms, viruses, and both internal and external attacks, without blocking legitimate traffic
- Provide a cost-effective, highly manageable platform for remotely monitoring and mitigating attacks on customer networks
- Enhance efficiency and effectiveness of security technicians

NETWORK SOLUTION

- Cisco security solutions, including Cisco IPS 4200 Series sensors with Cisco IPS 5.0 Software and Cisco Security Agent

BUSINESS RESULTS

- Provides stronger, more comprehensive protection of customer networks
- Reduces risk of mistakenly blocking legitimate network traffic and disrupting service
- Provides cost-effective, manageable solutions to support continued growth of managed services business

BUSINESS CHALLENGE

Protecting just one business against the constant barrage of worms, viruses, and Internet attacks that plague today's open networks is hard enough. Imagine trying to protect hundreds. That's the challenge that Austin, Texas-based Simpler-Webb, a managed security services firm specializing in small and medium-sized financial institutions, faces every day.

"A lot of our clients are becoming much more aware of the need for ongoing network security and information privacy, but they don't have the staff or expertise to use modern security technologies themselves," says Chris Cobb, chief financial officer for Simpler-Webb. "Today, a local bank in Midland, Texas is just as vulnerable as a national conglomerate. So they look to us to provide that security."

To provide an effective defense, Simpler-Webb must monitor all client network activity—both traffic coming from outside the network and traffic behind the firewall—to sniff out any potential threats. But a key challenge for Simpler-Webb isn't just separating the bad traffic from the good—it's recognizing the difference.

"Our customers often introduce new systems that we don't know about, so 'false positives' can be a big problem," says Sean Martin, director of Security for Simpler-Webb. "At the rate new threat alarms are published, there's a real possibility that legitimate traffic will be mistaken for something malicious and trigger an alarm. If one of our sensors blocks traffic that shouldn't be blocked, that's a service interruption for our customers."

Historically, Simpler-Webb addressed this issue by maintaining an extremely knowledgeable staff and using an internally developed software engine to detect patterns of malicious behavior among multiple systems and alarms. But as the propagation speed of network attacks increased, this system was strained.

"If we saw one alarm fire along with two other alarms that we knew were associated with a specific attack, then detecting what was genuinely bad was easy," says Martin. "But when hundreds of alarms were coming in at once, it was much more difficult."

Simpler-Webb's managed services business is growing rapidly, so the firm needs remote security solutions that are scalable, cost-effective, and highly manageable. The need to manage multiple separate network appliances (intrusion prevention system sensors, routers, firewalls, etc.) at each client site has historically been a substantial burden on the firm's 35-member staff.

In addition, many of the firm's financial industry clients must meet strict state and federal regulatory guidelines, such as the Sarbanes-Oxley Act of 2002. Any security solution must include detailed auditing and reporting of all network activity.

“We’ve preached for a long time that most bad traffic comes from inside the network. The Cisco IPS 5.0 system gives us the ability to look inside our customers’ networks in a way that wasn’t really possible before. It allows us to identify problems that might have been hidden in the past, while also providing the detailed compliance reporting our customers require.”
—Sean Martin, Director of Security, Simpler-Webb

NETWORK SOLUTION

To provide the most robust, scalable, and manageable security solutions for its customers, Simpler-Webb provisions its entire service portfolio with security solutions from Cisco Systems®. Depending on the client and the scope of the network, the firm uses Cisco® Intrusion Prevention System (IPS) sensors, Cisco Security Agent software, and Cisco PIX® security appliances, as well as the security features embedded within the Cisco IOS® Software in Cisco routers and switches.

State-of-the-Art Threat Detection and Mitigation

At the core of most Simpler-Webb security solutions is a Cisco IPS 4200 Series sensor, equipped with Cisco IPS Sensor Software Version 5.0. Cisco IPS 5.0-based solutions provide multi-vector threat identification, multiple interfaces to protect several networks and subnets, and simultaneous operation in both promiscuous and inline modes. Cisco IPS 5.0 software also includes a suite of sophisticated threat evaluation and mitigation tools that allow organizations to respond to a broad range of threats with confidence. Additionally, Cisco responds quickly to late-breaking threats by furnishing the sensors with new updates in an automated manner. This considerably reduces the operational overhead expended on IPS deployments.

“With Cisco IPS Software 5.0, we can now have a single inline IPS sensor monitoring incoming traffic from the Internet, as well as performing promiscuous monitoring of the network,” says Martin. “We have the same packet-dropping reaction capabilities for both internal and external traffic. But one of the critical value propositions of the Cisco IPS solutions is their ability to reach across the network and dynamically reconfigure switches and routers. The result is that the user has unprecedented attack mitigation capabilities to stop malicious traffic not only at the IPS sensor but also at critical ingress and egress points through the automated management of networking devices.”

Using the software’s integrated meta event generator (MEG) and risk-rating tools, Simpler-Webb can assign specific confidence levels to every potential alarm, correlate multiple alarms to detect “meta” events, and better craft strategies for when to block—and not block—traffic. And, since the MEG provides detailed reporting of all network activity and events, Simpler-Webb can use the tool to provide documentation to meet customers’ auditing requirements.

Strong Endpoint Protection

To protect customer PCs, servers, and other network endpoints, Simpler-Webb uses Cisco Security Agent. Unlike traditional antivirus systems, which detect only known virus signatures, Cisco Security Agent monitors actual operating system (OS) behavior, allowing it to block even unknown, or “day zero” threats. Simpler-Webb has even been able to extend Cisco Security Agent beyond traditional network endpoints.

“We’ve had a lot of success using Cisco Security Agent for some of our credit union customers,” says Cobb. “A lot of ATM machines these days are actually IP-based. So we’ve been able to install Cisco Security Agent directly on the ATMs and protect them against anything jumping the network into their operations.”

The enhanced protection provided by Cisco Security Agent also allows Simpler-Webb to better manage the deployment of new OS patches—an otherwise extremely challenging effort for an organization remotely monitoring thousands of endpoints for hundreds of customers.

"In some cases, Cisco Security Agent allows us to take a more measured approach to patch management, because we don't have to install every single patch that comes out immediately," says Martin. "But more importantly, it gives us the opportunity to test patches before we have to deploy them, and make sure there are no adverse effects on our customers' systems."

Simplified Management and Integration

Cisco security solutions are designed from the ground up for scalability, using open standards and protocols, so Simpler-Webb has been able to develop proprietary tools for remotely managing hundreds of network sensors and Cisco Security Agents simultaneously, and providing rich reporting to customers.

Since most of the firm's customers already use Cisco network routers and switches, Simpler-Webb is also able to easily integrate Cisco security solutions into customer architectures, and design security strategies that take full advantage of network protection tools already embedded within Cisco network technologies.

Additionally, Cisco management solutions aggregate and correlate events from Cisco IPS 5.0 sensors and Cisco Security Agents. This allow users to take advantage of IPS services on both the network and endpoints to make critical attack mitigation decisions.

BUSINESS RESULTS

By outfitting its expert technical staff with state-of-the-art Cisco security solutions, Simpler-Webb is able to provide more robust protection for its customers than ever before. As a result, the firm's clients can harness the full potential of network- and Internet-enabled financial services, confident that critical business applications and sensitive customer data are protected.

"We've had clients who, before they joined us, had their servers hacked, had frequent spyware and malware outbreaks, and even had Web sites defaced," says Martin. "Since they began using our services, they haven't had any of those issues."

Using intelligent Cisco IPS 5.0 Software and Cisco Security Agent, Simpler Webb can bring a level of sophistication to the defense of its clients that would otherwise be extremely difficult for these small businesses to achieve. The dual inline/promiscuous capabilities of Cisco IPS 4200 Series sensors, for example, provide a much more detailed, comprehensive view of client network activity.

"We've preached for a long time that most bad traffic comes from inside the network," says Martin. "The Cisco IPS 5.0 system gives us the ability to look inside our customers' networks in a way that wasn't really possible before. It allows us to identify problems that might have been hidden in the past, while also providing the detailed compliance reporting our customers require."

The Cisco IPS 5.0 Software MEG and risk-rating tools also allow Simpler-Webb to mount a much more effective, intelligent response to any network threats.

"The event correlation features built into the Cisco IPS sensors are a huge advantage," says Martin. "Since we began using Cisco IPS Software 5.0, we've seen a substantial reduction in the number of alarms generated that we have to actively respond to. We are also much more confident about dropping malicious data, without worrying about blocking legitimate traffic."

A More Efficient, Scalable Solution

The ability to more intelligently identify and respond to network threats has significantly reduced Simpler-Webb's administrative requirements, and positioned the firm to take on new business without major staffing increases.

"We don't have the staff to look at every single emerging threat that's present on the Internet," says Martin. "With tools like the MEG, we don't have to have a technician review every single alarm. Instead, the system can automatically identify the issues that actually pose a serious threat. That reduces the total number of alarms we have to react to, which definitely eases staffing."

"One of the metrics we look at in our business is how many sensors each of our security technicians can effectively support," says Cobb. "We're always looking for ways to increase that. Using Cisco IPS 5.0, we're seeing a very large jump in that number."

The Cisco security technologies also provide for more cost-effective solutions for Simpler-Webb's small and medium-size business customers.

"If we can use one sensor to monitor both the inside and the outside of a network, and perform both monitoring and packet dropping functions, that means we no longer have to sell our customers multiple devices," says Martin. "That provides a definite cost savings."

FOR MORE INFORMATION

Cisco Systems has already helped organizations worldwide deploy the robust, intelligent security solutions necessary to protect against constantly evolving threats.

To find out how Cisco can help your organization, contact your local account representative, or visit http://www.cisco.com/go/ips.

This customer story is based on information provided by Simpler-Webb and describes how that particular organization benefits from the deployment of Cisco products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

Cisco provides this publication as is without warranty of any kind, either express or implied, including the implied warranties of merchantability or fitness for a particular purpose. Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA 36-359353-00 08/06