CUSTOMER SUCCESS STORY

NETWORKGUYS SAFEGUARDS VITAL INSURANCE ASSETS FOR LEGACY MARKETING GROUP WITH CISCO DEFENSE IN-DEPTH SECURITY SOLUTION

EXECUTIVE SUMMARY

CUSTOMER NAME

- Legacy Marketing Group

INDUSTRY

- Financial Services

BUSINESS CHALLENGE

- Safeguard the Legacy network from internal and external threats
- Improve network availability and performance
- Enhance network management

NETWORK SOLUTION

- Cisco® Catalyst® 6500 with security modules and Cisco Security Agent endpoint security software deliver multilayer security
- Dual chassis for Legacy's Cisco Catalyst 6500 switches reduce potential points of failure
- CiscoWorks VPN/Security Management Solution supports network administration

BUSINESS VALUE

- Cisco Systems® security solution enables Legacy to protect its most important business assets
- Increased network availability and performance reduces risk of lost revenue associated with network outages
- Reduced need for security patches and updates

Using the SAFE Blueprint for security from Cisco, The NetworkGuys and Legacy's Network Engineers staff upgraded Legacy Marketing network to safeguard Legacy's insurance business.

A leader in the financial services industry, Legacy Marketing Group needed to enhance its network to deliver better security, availability, and performance. This success story describes how NetworkGuys enabled Legacy to:

- Protect its most important business assets with a defense-in-depth Cisco security solution
- Increase network availability and performance to reduce the risk of lost revenue

CHANNEL PARTNER BACKGROUND

NetworkGuys, Inc. is a leading network security integrator whose focus is to provide customers with the most up-to-date technology to secure their networks and their connections to the Internet. Founded in 1996, NetworkGuys offers a full range of implementation and support options to meet its customer requirements.

Headquartered in Fremont, California, NetworkGuys works with leading network security vendors of firewall, VPN, content filtering, antivirus and antivandal, and reporting solutions. The company also offers robust authentication solutions, intrusion detection systems, high availability and load-balancing solutions, e-mail security, application security, and security assessments.

CUSTOMER BACKGROUND

Legacy is an industry-leading provider of insurance and financial products nationwide. The company develops and maintains strategic alliances with multiple insurance carriers to provide a "one-stop shop" for a broad range of products. The company is based in Petaluma, CA, and has an office in Rome, GA. Driven and owned by a network of independent agents, Legacy has generated over $8.5 billion in fixed annuity premiums in the last five years.

BUSINESS CHALLENGE

With a staff of more than 400 employees and numerous business partners throughout the world, Legacy depends on its network to keep its distributed business operations running smoothly. The company is based in Petaluma, California, and connects to a remote site in Rome, Georgia via an ATM WAN. Legacy also uses the Internet to communicate with insurance producers. With key financial packages, data warehouse applications, payroll, and other core business processes running over its infrastructure, network security and reliability are paramount. As its business matured, the Legacy IT staff became aware that the company's previous network could no longer deliver the security and availability required to support mission-critical applications.

“As we evaluated the Legacy infrastructure, we used a defense-in-depth strategy based on the SAFE Blueprint from Cisco. Then the Cisco team came in, and they did a tremendous job in fitting a specific solution to the framework that we had laid down.”

— Brian Emery, Corporate Account Manager, NetworkGuys

“By implementing Cisco’s multi-tiered network and security infrastructure, Legacy could reinforce its commitment to providing unparalleled performance, reliability, and security to clients,” explains Kelvin Si, IT Operations network engineer at Legacy.

Recent regulatory changes have imposed new pressures on Legacy. Legislation such as the Sarbanes-Oxley Act of 2002 requires financial firms to improve transparency and documentation in their reporting, which requires a high-performance, extremely reliable network infrastructure. The Legacy network also must meet strict security and confidentiality requirements from its business partners.

“As regulatory compliance becomes more of a focal point for IT, Legacy is uniquely positioning itself to meet customer needs into the foreseeable future,” says Si.

To perform a detailed evaluation of its network security and reliability and recommend specific solutions, Legacy contacted NetworkGuys. Specializing in network security, NetworkGuys was strongly recommended by Cisco Systems representative Britt Norwood.

“We’ve had a relationship with Cisco for several years now, and they believed we fit the bill in our ability to provide Legacy a cost-effective yet thorough security assessment and solution,” explains Brian Emery, corporate account manager at NetworkGuys.

THE SOLUTION

NetworkGuys performed a Security Posture Assessment (SPA), analyzing the network and potential security breaches in great detail, and recommended that Legacy update its network based on the SAFE Blueprint from Cisco for enterprise network security. The SAFE Blueprint from Cisco provides best practices information on designing and implementing secure networks. The SAFE Blueprint takes a defense-in-depth approach to network security design and incorporates layers of security so that the failure of one security system is not likely to lead to the compromise of the rest of the network.

“Since we started our company eight years ago we’ve concentrated solely on network security,” says Tim Carney, CEO at NetworkGuys. “We work only with best-of-breed security providers, so Cisco is obviously one of our preferred vendors.”

To protect the network from outside threats, NetworkGuys and Legacy’s network engineers installed integrated, modular Cisco Catalyst 6500 Series Switches with intrusion detection system (IDS) services modules in the Legacy Ethernet network that detect and alert network administrators about unauthorized network activity. The Cisco IDS module monitors traffic in real time, around the clock, without jeopardizing the performance of Legacy’s most important networked business applications. Cisco Catalyst 6500 Series firewall services modules running on Legacy switches provide stateful firewall protection for the Demilitarized Zone (DMZ) that separates Internet traffic from internal network resources.

To provide protection deeper in the Legacy network, NetworkGuys deployed the Cisco Security Agent endpoint security software on 50 servers throughout the company. Cisco Security Agent is specifically designed to provide threat protection for server and desktop computing systems. It identifies and prevents known and unknown (“Day Zero”) security risks, including such attack types as port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms.

By permeating every layer of the Legacy network, the Cisco security solution provides maximum protection for sensitive insurance data and transactions.

“The main advantage of the Cisco solution is that it offers defense-in-depth,” says Brian Emery. “Other solutions from multiple vendors can’t be implemented and closely interact with one another. For example, one competitor’s solution could protect Legacy’s servers but did not secure both their servers and their desktops.”

Network availability was another key requirement for Legacy, and NetworkGuys and Legacy’s network engineers deployed dual chassis for the company’s Catalyst switches to reduce potential points of failure. Multiple Cisco Catalyst 6500 Series firewall services modules for each core chassis provide additional fault tolerance.

“We evaluated Legacy’s redundancy and scalability as well, as network availability is an important part of security,” says Emery. “If a company is attacked, and it ends up bringing down a firewall or exposing an internal vulnerability, then having redundancy built in not only adds an extra layer of security but also increases the availability of the asset.”

Legacy manages its secure network using the CiscoWorks VPN/Security Management Solution (VMS). CiscoWorks VMS provides Web-based tools for configuring, monitoring, and troubleshooting firewalls, network IDS, VPNs, and other security systems. It also provides support for network device inventory, change audit, and software distribution features.

RESULTS

Legacy was pleased with the support and input provided by NetworkGuys throughout the upgrade process and confirmed that the organization lived up to its reputation as security experts.

“The NetworkGuys team was knowledgeable, professionally astute, and very much aware of industry best practices,” says Troy Myers, IT Operations network architect/manager at Legacy. “As they evaluated our business, they were willing to give us the answers that we needed to hear to secure our network, rather than the ones we wanted to hear.”

Legacy also had an excellent relationship with the Cisco account team, which delivered corporate-class service to the growing company.

“Cisco was instrumental in working the design with NetworkGuys,” says Myers. “They were very helpful and very much willing to go the extra length for us. We’re a midtier company, not a huge company, and they gave us a lot of support.”

The Cisco security solution enables Legacy to safeguard its most important business assets, as well as meet its obligations to its customers, partners, and government regulators. And increasing network availability and performance helps ensure that Legacy will not suffer from lost revenue associated with network outages.

Legacy also is experiencing substantial improvements in productivity, as a result of its easy-to-manage Cisco security solution. By deploying Cisco Security Agent software throughout its servers, Legacy no longer has to worry about individually updating security components and patches on its business applications.

WINNING THE DEAL WITH BEST PRACTICES

The Cisco account team and NetworkGuys collaborated closely to develop an end-to-end security solution to meet Legacy’s requirements. NetworkGuys initiated the sale with a three-week SPA to evaluate the entire organization, consider the function of every network device, and produce a strategic plan. The Cisco team followed up with a detailed set of product recommendations based on the results of the SPA.

“As we evaluated the Legacy infrastructure, we used a defense-in-depth strategy based on the SAFE Blueprint from Cisco,” says Emery. “Then the Cisco team came in, and they did a tremendous job in fitting a specific solution to the framework that we had laid down.”

Presenting its recommendations to the Legacy IT staff was only part of the sales process. NetworkGuys also needed to communicate the advantages of a comprehensive Cisco security solution to skeptical executives.

"NetworkGuys developed presentations based on our compliance and regulatory requirements, and presented them to our upper management," says Myers.

"We provided a lot of education, and sat down with key executives to pitch the need for a secure environment," adds Emery.

The flexible finance options offered by Cisco also played an important part in closing the deal because they enabled Legacy to upgrade its entire network yet continue to keep expenses under control.

"Cisco leasing played a key role in allowing the deal to happen," says Emery. "Legacy's previous equipment lease was coming up for renewal, and the Cisco Systems Capital Leasing organization showed them that they could fully refresh their product lines and provide additional security and redundancy for only a thousand dollars a month more than the previous lease. It ended up being a no brainer."

NEXT STEPS

The new Cisco network solution was designed with scalability and flexibility in mind, to enable IT operations staff to adapt their infrastructure to meet new business needs or support additional applications and users in the future.

"We intentionally chose more modular products, and the architecture of our network is open-ended," explains Myers.

With its secure Cisco network, together with the expertise and best practices provided by NetworkGuys, Legacy is poised to maintain its position as a leader and innovator in the financial industry.

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 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

204189.u_ETMG_JR_2.05

Printed in the USA