CIGNA
A Business of Caring.

CIGNA Finds Good Therapy: Builds A More Efficient Risk Management, Streamlined Compliance, and System Security Program

"QualysGuard gives us the ability to detect our vulnerabilities across our network and really ensure that we have the level of security and compliance we need."

Craig Shumard, Chief Information Protection Officer
CIGNA Corporation

CIGNA Corporation and its subsidiaries constitute one of the largest publicly owned employee benefits organizations in the United States and throughout the world. In 2005, its revenues totaled $16.7 billion, and as of June 30, 2006, it held shareholder equity of $4.7 billion. Its subsidiaries are major providers of employee benefits offered through the workplace, with products and services including health care, group life, accident and disability insurance, dental, vision, behavioral health, and pharmacy. CIGNA appreciates healthy outcomes, and its ongoing commitment is to ensure that the 42 million people it serves receive the highest levels of care and well-being.

As a provider of employee benefits, as well as a public company, CIGNA must observe a bevy of regulatory compliance mandates, from state laws to federal laws such as Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act (HIPAA). "We deal with probably every regulation you can imagine. We focus a lot of our efforts on regulatory compliance," says Craig Shumard, chief information protection officer at CIGNA.

CIGNA has embraced technology, and is constantly rolling out new products and services to help employers better manage their benefits offerings, and give their employees access to round-the-clock information regarding their employee benefits. An example is the company's myCIGNA.com portal that gives consumers the ability to conduct side-by-side comparisons of the costs and quality of health care providers, and even the cost of prescriptions at various pharmacies. These efforts, among others, helped CIGNA to rank number 17 on the 2006 InformationWeek 500 (an annual listing of the top 500 technology innovators published by InformationWeek magazine). Also, Shumard recently was honored with Information Security magazine's Security 7 Award, an award bestowed on the world's top seven security professionals each year.

It should come as no surprise that a sizable portion of Shumard's efforts, and those of his security team, focus on ensuring that all of their systems are adequately secured, and that compliance controls—designed to maintain the confidentiality, integrity, and availability of regulated and other forms of sensitive information—remain in place. A crucial part of those efforts includes the ability to quickly identify systems that have configuration errors, lack the latest security patches, or are not being maintained to internal security governance standards.

Lack of Visibility. Increasing Complexity.

Some time ago, CIGNA relied heavily on a vulnerability scanner that proved difficult to manage, and couldn't identify—let alone properly scan—all of the servers in CIGNA's environment. "We managed to get the job done, but it required too many ad-hoc and manual scans, and it was difficult to prioritize the vulnerabilities that really mattered," says Sridhar Srinivasan, information protection manager at CIGNA.

To bolster the vulnerability management portion of its overall risk management program, Shumard and his team knew that they needed a vulnerability scanner that could be easily deployed, was capable of scaling throughout its vast geographically distributed network, didn't require an expensive infrastructure to maintain and secure, was highly accurate at spotting misconfigurations and vulnerabilities, and could identify potential rogue systems and devices that crept onto the network. "The complexity of our environment continued to grow, and so did the security threats. We needed something that would help us to really hone in on the vulnerabilities across our network, regardless of the operating system or platform," Srinivasan adds.

Automated Vulnerability Management

CIGNA selected QualysGuard® from Qualys® Inc., thus enabling the company to streamline control of its entire vulnerability management lifecycle: asset discovery, vulnerability assessments, track security fixes, and meet federal, state, and internal policy regulations. "We were looking for a true black box solution that required only an IP address and would run from there," says James Lemieux, CIGNA's information protection director. That's what CIGNA found in QualysGuard. The on-demand solution delivered as a Web solution requires no software or costly infrastructure to deploy, and is fully managed by Qualys. "We don't have to keep the devices up to date. Qualys takes care of all of the care and feeding of the device," says Lemieux.

QualysGuard provides CIGNA what it needs to help keep systems secure and compliant—even from fast-moving threats and zero-day vulnerabilities, giving CIGNA a way to quickly assess its complex infrastructure to make certain that the security and mitigating controls are in place. "It's especially helpful when zero-day exploits come out. We can very quickly go to QualysGuard, and more often than not, they'll have a signature before anything even hits," says Lemieux.

CIGNA's initial deployment consisted of multiple QualysGuard Enterprise scanner appliances. That quickly grew to 18, so every facet of CIGNA's distributed network can be scanned whenever needed. "We use QualysGuard to examine all of our vulnerability issues; we look at risk configurations, default installations of applications; we look at the whole gambit of Qualys' strong knowledge base when we do any type of scanning," says Srinivasan.

Added Efficiencies Strengthen Security, Operations and Regulatory Compliance

The thorough QualysGuard scans not only provide the ability to identify and mitigate vulnerabilities and misconfigurations; its comprehensive reporting can be tailored for security teams, operations, business executives and auditors to show security readiness and compliance. "One reason we selected Qualys is the quality of its reporting capabilities. We are able to customize the reports for our specific business purposes, and we don't have to rely on trying to explain the risk, based on what the security industry and software vendors are saying about the vulnerability," adds Srinivasan.

> *"Before QualysGuard we had an ad hoc process; Qualys brought much stronger control and visibility into our processes."*

James Lemieux, Information Protection Director
CIGNA Corporation

The use of QualysGuard also has helped to build greater unity between CIGNA's IT operations and security teams. In the past, Shumard and his team sometimes were viewed as a source of business friction. "It was often, 'Oh, here comes security again, doing scans. They're going to give us some big report,'" says Lemieux. "Now we're really viewed as a partner. And the other business and IT operation units look at us and understand that we can really facilitate system remediation, cleanup, and help them to identify servers that no one knew were out there."

The ease of QualysGuard's deployment and manageability, along with a powerful application programming interface, has enabled CIGNA to embed QualysGuard as an integral part of its risk management program. CIGNA has integrated QualysGuard with various security tools and processes throughout its organization. For example, QualysGuard is tightly integrated with Symantec's Enterprise Security Manager, or ESM. This integration enables CIGNA to automatically coalesce ESM's detailed system configuration information with QualysGuard's extensive vulnerability report to provide a holistic status of the system's health. CIGNA is also investigating ways to more closely integrate QualysGuard with its patch management and intrusion detection systems.

"In the past, all of this information was fragmented. Now, when we give the reports to operations or our patch management group, we're able to pull our security information together and provide a complete picture," says Lemieux.

Ongoing, On-Demand, Security Checkups

To remain competitive, CIGNA is constantly releasing new products, applications, and Internet-based services. It is steadily forging new relationships, and integrating with customers and suppliers. "Every product or application that you can see over the Internet has to go through QualysGuard before it's allowed to go live," says Lemieux.

The same is true for any customer or vendor where there's a network connection. Since installing the QualysGuard solution, CIGNA not only has found its compliance efforts to be more efficient, but it has garnered greater insight into its security posture. "It's allowed us to be very focused on the risks that matter, as soon as they surface. We're able to really focus our energies on the true vulnerabilities that need our attention. QualysGuard has really helped us to raise our level of compliance across our entire environment," says Shumard—and that's a healthy outcome for everyone.

CIGNA SCOPE & SIZE

United States & worldwide
26,500 employees.
Total assets $44 billion.

BUSINESS

One of the largest publicly-owned employee benefits organizations in the United States and throughout the world. Its subsidiaries are major providers of employee benefits offered through the workplace, with products and services including health care, group life, accident and disability insurance, dental, vision, behavioral health, and pharmacy.

BUSINESS PROBLEM

Provide effective IT security and regulatory compliance risk mitigation for global network.

OPERATIONAL HURDLE

Manual vulnerability scans lacked visibility into CIGNA's infrastructure, and failed to easily identify servers and vulnerabilities that jeopardized security and compliance efforts.

SOLUTION

CIGNA turned to QualysGuard's on demand Web service appliance to automatically identify and more effectively mitigate system vulnerabilities and misconfigurations.

WHY CIGNA CHOSE QUALYS

- Automated on-demand security and vulnerability audits
- Highly accurate vulnerability and configuration scans
- Easy to deploy, manage and operate
- Scalable enough to secure CIGNA's global network
- Comprehensive reporting capability for technical teams, business managers and auditors
- Integrates with other areas of CIGNA's risk management program, including patch and change management, and compliance tools

QUALYS®
www.qualys.com

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

ON DEMAND SECURITY