



AMERICAN SPECIALTY HEALTH'S IT RISK IMMUNIZATION PLAN

Weekly vulnerability assessments ensure that American Specialty Health's IT infrastructure stays in shape, is secure, and is compliant to numerous regulations, including HIPAA and the PCI Data Security Standard.

“I've never found any other vulnerability management tool that is as comprehensive as QualysGuard. We have never encountered a situation where a third-party audit found something QualysGuard didn't.”



Tina Mitchell, Senior Director of IT Operations and Information Security Officer
American Specialty Health

American Specialty Health Incorporated (ASH) makes it easier for people to stay fit and healthy. The San Diego, Calif.-based company provides health benefits, fitness, and health improvement programs for health plans, insurance carriers, plan sponsors, employer groups, and trust funds across the country. The privately-held company covers more than 13 million members in its benefits, coaching, and fitness programs. Its e-Commerce site, Healthyroads.com®, offers award-winning weight management, tobacco cessation, and healthy living programs. While it's the mission of its 600-plus employees to make sure that a healthy and fit lifestyle is within reach of its members, it's the goal of Tina Mitchell, senior director of IT operations and information security officer at ASH, to maintain the health and well-being of the company's IT infrastructure.

The Need for Demonstrable Security and Regulatory Compliance

It's a job that certainly keeps her and her IT team of five administrators quite busy. That's why ASH sought an effective and automated way to manage the software vulnerabilities and system misconfigurations that place its IT systems at risk to attack and falling out of regulatory compliance. In fact, with CERT Coordination Center estimating that roughly 99 percent of all successful attacks are made possible by exploiting known software vulnerabilities and misconfigurations, efficient vulnerability risk management is one of the most important aspects of any security effort.

While that's true for almost every organization, it's especially so for ASH. Because the company provides health care benefit programs and works so closely with health plans and insurance carriers, it must operate in compliance with the Health Information Portability and Accountability Act (HIPAA), which includes security and privacy rules that require administrative, technical, and physical security procedures be in place to assure the confidentiality, integrity, and availability of health information.

Continuous, Accurate, and On-Demand Vulnerability and Regulatory Compliance Management

When Mitchell began her search for a vulnerability auditing solution, she noticed the free two-week trial offer from Qualys Inc., for its QualysGuard on-demand vulnerability management and policy compliance appliance. Mitchell immediately put QualysGuard to work. The fact that QualysGuard proved flexible, required minimal maintenance, and provided a way for automated scans was especially useful to ASH. “I was immediately impressed, especially with its ease of use and the quality of QualysGuard's reporting,” says Mitchell. “That's what initially sold me.” Today, ASH scans its internal and externally-facing Internet sites each week, including Healthyroads.com. Its internal infrastructure consists of 110 servers and more than 600 desktops.

American Specialty Health's IT Risk Immunization Plan

QualysGuard provides ASH's system administrators with a proactive way to protect the company's network throughout the entire vulnerability management life cycle, including asset discovery, asset prioritization, vulnerability assessment and analysis, remediation planning, and fix verification. And its highly flexible, on-demand architecture makes it easy for ASH's systems administrators to successfully perform their individual security responsibilities. "The members of the IT Operations team have dual roles, including the management of our IT infrastructure and security," explains Mitchell.

As a direct result of QualysGuard's innovative on-demand architecture, there are no additional operational or administrative burdens for ASH. Once the appliance is deployed, all system maintenance, vulnerability signature updates, and software enhancements are controlled directly from Qualys' Secure Operations Center. That means that ASH and every one of Qualys' 2,500-plus customers automatically run the latest version of QualysGuard—the most-up-to-date, comprehensive database of security checks in the industry. "Because QualysGuard is always up to date, we know exactly what patches we are missing," she says.

QualysGuard Streamlines IT Security Auditing Efforts

To make certain that its systems are maintained securely, and within HIPAA and PCI compliance rules, ASH undergoes an extensive IT security assessment and auditing process. This includes the weekly QualysGuard scans, quarterly third-party security audits, and an annual full-scale internal risk assessment. "We take our security very seriously, and QualysGuard makes certain that we have an adequate level of checks and balances in place," she says.

Those efforts are great news for ASH's most demanding constituency: its clients. "It is important that our clients know that they can trust us with their information," says Mitchell. To help ease its customers' security concerns, and substantiate the company's high-levels of security, since 2003, ASH has been fully accredited by the independent, non-profit organization URAC for HIPAA Privacy and Security, among other health care-specific accreditations. URAC establishes meaningful quality measures for the health care industry and is a well-known leader in promoting health care quality through its accreditation and certification programs. "QualysGuard plays a key role in our internal security program, regulatory compliance, and URAC accreditation efforts," she says.

QualysGuard Simplifies ASH's PCI Compliance Efforts

The Payment Card Industry Data Security Standard (PCI DSS) aims to help merchants make certain that their customers' credit card information doesn't end up in the wrong hands. PCI DSS requires merchants to put into place standard security practices, including the use of firewalls, anti-virus programs, the encryption of cardholder data in transit and at rest, and conducting vulnerability scans to keep systems secure.

American Specialty Health relies on QualysGuard to help it remain compliant. The QualysGuard service, a PCI DSS-approved scanning vendor, makes it simple for merchants to conduct their annual self-assessments and quarterly network scans. "QualysGuard plays a central role in our PCI compliance," says Tina Mitchell, senior director of IT operations and information security officer at ASH. "It increases our level of compliance and helps us to continuously stay secure," she says.

ASH SCOPE & SIZE

National
13 million members
Privately held

BUSINESS

ASH provides complementary health benefits, fitness, and health improvement programs.

BUSINESS PROBLEM

Cost-effectively achieve ongoing IT security and regulatory compliance risk mitigation for its own network and new company acquisitions.

OPERATIONAL CHALLENGE

ASH doesn't have a staff dedicated to IT security; as a result, its IT director and system administration team need the most automated way to keep its systems secure and compliant.

SOLUTION

QualysGuard

WEBSITE

www.ashcompanies.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

