Diagnosing Risk

The University of Chicago Medical Center needed to consolidate the tools it used for to reduce vulnerability and improve risk management to meet expanding HIPAA and PCI requirements.

> *"QualysGuard enables us to automate our risk management and compliance functions, and we will continue to leverage QualysGuard to automate manual processes wherever possible. This is how QualysGuard improves our security and gives us more time to focus on other strategic things."*

Plamen Martinov,
Lead Security Engineer
The University of Chicago Medical Center

Since 1927 the University of Chicago Medical Center (UCMC) has provided medical care to the residents of the Chicago metropolitan area and beyond. Today, this nonprofit corporation includes four campus-based centers of care: the Bernard A. Mitchell Hospital; the Comer Children's Hospital; the Chicago Lying-in Hospital, a facility for women and maternity; and the Duchossois Center for Advanced Medicine, a state-of-the-art ambulatory-care facility that boasts a full spectrum of preventive, diagnostic, and medical treatment. University of Chicago revenues for patient care total more than $1 billion annually.

UCMC's IT infrastructure, which supports four separate units, is considerable. It consists of a couple thousand servers and about 11,000 individual networked devices. Special attention is paid to the security of financial records, as well as the protection of Personal Health Information (PHI), which is growing in importance as sensitive patient data is stored and shared electronically. The Health Insurance Portability and Accountability Act (HIPAA) mandates that health care organizations ensure the privacy of patients' PHI. The unauthorized disclosure of this information can result in fines and penalties.

The Challenge: Manual Vulnerability Assessments, Lack of Reporting Clarity

In order to keep its systems secure, the UCMC IT security team had relied on a number of separate tools to conduct network vulnerability assessments, validate proper patch deployment to at-risk systems, and then generate the reports necessary for both technical teams and business managers. Unfortunately, the applications it relied on didn't provide a way to manage workflow centrally among the various hospitals and business units, nor was there a convenient way to generate the reports that security managers, operation teams, and business managers needed to perform their jobs. "Our challenge was not only to conduct vulnerability management, but also to provide appropriate reports that detail what executive management needs to know and understand about our compliance with internal security policies," explains Plamen Martinov, lead security engineer at UCMC.

"It took tremendous effort just to get reports that provided the quantifiable data they needed to make decisions. We would have to run three or four different reports and then pull them all together manually for each audience," explains Martinov.

Toward Insightful, Structured Vulnerability and Risk Management

After an evaluation of the available vulnerability management solutions, it Martinov and his team selected the QualysGuard Security and Compliance Suite, from Qualys, Inc., because they felt it could provide the structured, consolidated vulnerability and risk management that UCMC sought, as well as the comprehensive reporting it needed. Through its Software as a Service (SaaS) delivery, the QualysGuard Security and Compliance Suite combines Qualys' vulnerability management service with a comprehensive IT compliance solution. For UCMC, the QualysGuard Security and Compliance Suite eliminated network auditing and compliance inefficiencies by leveraging the organization's own IT security information. In one consolidated suite, groups with different responsibilities can now utilize the detailed information they need for their specific job functions.

Today, instead of relying on multiple vulnerability assessment applications, UCMC relies on the QualysGuard Security and Compliance Suite to automate and unite the process of vulnerability management and policy compliance across the organization: network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking, according to business risk. Policy compliance features also enable security managers to audit, enforce, and document compliance with internal security policies and external regulations.

Within three months of deploying QualysGuard, UCMC security and IT managers were able to establish a continuous vulnerability management program. Now they can track remediation efforts and ensure that internal policy compliance is maintained through comprehensive reporting. With its broad vulnerability KnowledgeBase, consisting of thousands of unique checks and a high accuracy rate, QualysGuard supplies UCMC precise security checks.

“The switch from our previous vulnerability management programs to QualysGuard went smoothly,” says Martinov. “We ran a short proof-of-concept trial, which went without a hitch,” he explains. “Now that we have QualysGuard in place, we can use it to provide all of the different audiences (business managers, IT security, and operations groups) with the exact information they need from a centralized location,” he adds. In addition to the more comprehensive, targeted reporting capabilities, UCMC was able to streamline its vulnerability management workflow with QualysGuard’s integrated remediation ticketing system.

A built-in feature of QualysGuard generates tickets based on internal policy rules and tracks each vulnerability from its identification to verified remediation. To help security managers work as effectively as possible, each remediation ticket is assigned a unique number and includes vulnerability details, remediation history, and all actions taken. During the subsequent scan, QualysGuard automatically verifies which vulnerabilities were fixed and then retires the related tickets. “When a vulnerability is identified, QualysGuard automatically opens an internal remediation ticket. “That ticket gets delegated to the appropriate group within Qualys, and it is closed automatically when the system is verified to be patched,” Martinov says, adding that at some point, they plan to integrate Qualys’ internal ticket policy engine with their own enterprise service request system.”

That type of workflow not only ensures that systems are remedied in time, but also helps to improve overall security and HIPAA compliance. Recently, when a rapidly-spreading Internet threat surfaced, UCMC quickly was able to establish a custom scan that detected any systems that could have been susceptible to infection. “We used QualysGuard to detect all systems that could have been vulnerable, and we efficiently worked with each group to make certain that those systems were hardened against the threat,” Martinov says. “This is how QualysGuard enables us to understand the security of our systems better, and to respond more quickly to all of the rapidly changing threats.”

QualysGuard Security and Compliance Suite enables organizations to:

Define policies to establish a secure IT infrastructure in accordance with good governance and best practices frameworks.

Automate ongoing security assessments, and manage vulnerability risk effectively.

Mitigate risk and eliminate threats utilizing the most trusted vulnerability management application in the industry.

Monitor and measure network compliance in one unified console—saving time, assuring reliability, and reducing costs.

Distribute security and compliance reports customized to meet the unique needs of business executives, auditors, and security professionals.

THE UNIVERSITY OF CHICAGO MEDICAL CENTER SCOPE & SIZE
Greater Chicago Metropolitan Area
Total Employees: 9,500+
Annual Revenue: $1+ billion

BUSINESS Health Care

BUSINESS PROBLEM
Consolidate multiple vulnerability management applications, across multiple locations, and provide security and IT operation teams, as well as business managers, with the risk and regulatory compliance reports they need for their specific job functions.

SOLUTION
QualysGuard Security & Compliance Suite

WEBSITE www.uchospitals.edu

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. • Beechwood House, 10 Windsor Road , Slough, Berkshire, SL1 2EJ • T: +44 (0) 1753 872100
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
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • P.O Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

ON DEMAND SECURITY