UNIVERSITY OF UTAH WRITES NEW THESIS ON RISK MANAGEMENT

The University of Utah transformed its vulnerability management from ad hoc assessments to a repeatable and comprehensive vulnerability and compliance management program keeping its systems secure and within HIPAA compliance.

> **" Our security program is getting to the point we wanted to reach all along: where the vulnerability scans are transparent. It's as if there was this angst when the security team showed up before, and, 'oh no, we are going to get scanned again.' That's all gone now. "**

David Feyler, Manager of Information Security Operations
The University of Utah

The University of Utah is ranked as one of the top public research universities in the nation. It's also the oldest and largest institution of higher education in the state. "The U", as it is known locally, provides more than 100 undergraduate and 90 graduate degree programs to more than 28,000 students. The U also is well known for the health education, research, and clinical care provided by its University Health Care medical center.

The IT infrastructure necessary to support the university is significant. The network consists of thousands of servers and tens of thousands of endpoints and networked devices that tally roughly 30,000 individual IP addresses. While securing student and employee records is critical in its own right, as a fully operational research and clinical hospital, the university also must contend with compliance to the Health Information Portability and Accountability Act, known as HIPAA. Essentially, HIPAA requires the privacy and security of patient medical information to be maintained at all times.

To keep that infrastructure secure, and within HIPAA compliance, David Feyler, manager of information security operations at the university, explains how the security team used to run periodic network vulnerability assessments using open source tools. "We really didn't have an operationalized program in place," says Feyler. "It wasn't that vulnerability scans were not getting done. The process just wasn't as streamlined as it should have been," he says.

There was good reason why the program ran into a few snags. Not only was the open source scanner the university had been relying inaccurate, but it was very difficult to establish an automated scan cycle. Worse yet: it also would bring down many of the systems it evaluated. "We'd simply run a scan, and it very easily would knock down the boxes, even if we had the settings set very low," he says.

Additionally, the most damaging aspect of the ineffective scans wasn't the lack of accuracy or false positives, or the fact that systems would get knocked offline; it was the loss of trust and the barrier these results created between IT security and other business managers and IT team members at the university.

"It was damaging to our efforts," says Feyler. "Other areas of the university were afraid that scans would knock their systems offline, or we'd ask them to fix flaws that didn't exist," he says. That's an unsustainable condition for any organization, and Feyler set out to automate the vulnerability assessments, increase accuracy, and do it transparently so that the rest of the university was hardly aware of the process.

Insightful Reporting, Simplified Management

A team in the research hospital had already started using QualysGuard® Vulnerability Management, from Qualys, Inc. QualysGuard automates the lifecycle of network auditing and vulnerability management, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Driven by the most comprehensive vulnerability KnowledgeBase in the industry, QualysGuard delivers continuous protection against the latest security threats. And, because it is delivered as on-demand Software-as-a-Service (SaaS), there is no infrastructure to deploy and manage. This reduces costs substantially, as well as the resources needed to manage traditional on-premise software.

After a close look at QualysGuard and its simplified management, Feyler decided to expand QualysGuard's use throughout the university. "We immediately appreciated the more thorough reporting accuracy, and QualysGuard did not incapacitate the systems we scanned," he says.

QualysGuard enables organizations small or large to manage their vulnerabilities effectively and maintain control over network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates, and impact on business, plus trend analysis on security issues.

Transparent, Accurate, Automated Vulnerability Management

Bottom line: QualysGuard has enabled the University of Utah to achieve what it needed with its vulnerability management and compliance program: automation, accuracy, and transparency. "Now, with QualysGuard, vulnerability management has become tremendously easier," says Feyler. "The fact that it is centrally managed by Qualys, and that it can be used remotely from anywhere means that we can run and manage scans at any time, and from anywhere," he says.

Like most regulated organizations, the university's IT security and compliance teams are always under pressure to ensure that the business is running both secure and within compliance. Using QualysGuard, the University of Utah is now able to reduce IT risks associated with system misconfigurations and vulnerabilities, and the security group can provide the detailed reports necessary to prove systems are being maintained within HIPAA compliance.

While those security and compliance successes are more than welcome, perhaps the biggest change, as a result of the QualysGuard deployment, has been how other business managers and IT operations groups view the security team. "We're now noticing that after we dispatch the reports to the points-of-contact, they'll come back within a day or two and ask us to run a verification scan. That didn't happen before," says Feyler. "We're now getting great turnaround in terms of other business units working with us."

"Our security program is getting to the point we wanted to reach all along: where the vulnerability scans are transparent. It's as if there was this angst when the security team showed up before, and, 'oh no, we are going to get scanned again.' That's all gone now."

BUSINESS

The oldest and largest institution of higher education in the state of Utah. The university provides more than 100 undergraduate and 90 graduate degree programs to more than 28,000 students. The university is also well known for the health education, research, and clinical care provided by its University Health Care medical center.

BUSINESS PROBLEM

The University of Utah needs to keep its systems secure, and within HIPAA compliance.

OPERATIONAL HURDLE

The network assessment tools the university had relied on were not only inaccurate, but wouldn't enable functional automated scan cycles. They'd also, often times, crash the systems being evaluated.

SOLUTION

QualysGuard

WHY THE UNIVERSITY OF UTAH CHOSE QUALYS

- QualysGuard provides control of the entire vulnerability management life cycle: asset discovery, vulnerability assessments, and tracking of security fixes.
- Qualys' SaaS delivery model reduces management overhead.
- Greater accuracy and comprehensive reporting for operations and managers.
- Actionable vulnerability remediation information.
- Comprehensive HIPAA compliance reporting.

WEBSITE

www.utah.edu