



NO ADMISSION FOR VIRUSES, WORMS, AND MALWARE AT COLBY-SAWYER COLLEGE

By turning to an on-demand vulnerability management solution, Colby-Sawyer was able to effectively and affordably, secure its network and systems from modern, fast-moving threats.

“Qualys provides us the easiest way to prioritize and fix our software vulnerability and configuration issues. You plug it in, and it works.”



Scott Brown, Information
Security Analyst
Colby-Sawyer

Colby-Sawyer College is widely known for its innovative liberal arts and science curriculum that prepares its nearly 1,000 students for successful, well-rounded careers. The college, founded in 1837, spans 29 buildings nestled on 200 acres located within the scenic Dartmouth-Lake Sunapee region of New Hampshire.

Keeping college networks and critical systems secure from viruses, worms and attacks is very different than securing government or corporate systems. “Imagine trying to protect a network where 1,000 systems can suddenly show up with no security installed—where the end users have full control over the configuration of their own systems,” says Scott Brown, information security analyst at Colby-Sawyer. “Working with consultants, or anyone who has never dealt with an academic network before, is always very difficult. This is the most demanding environment out there—hands down,” says Brown.

Corporations and government agencies have near total control over the majority of systems connecting to their network. They have the ability to establish and enforce secure system and application configurations. They can make certain that end users don’t have administrative privileges over their desktops and notebooks, and that all of the required security defenses are in place: personal firewalls, anti-virus programs, and up-to-date patches. Security just doesn’t work that way at most colleges and universities.

“In our environment, the faculty and staff have administrative privileges on their machines. And the students own their own machines,” explains Brown. So when that’s coupled with the curiosity of youth and the dangers of the Internet, it’s easy to see how viruses, worms, and malicious spyware will find their way onto systems and threaten the security and availability of the academic and administrative networks and applications. “I’ve seen 3,000 infections on a single student’s system. If you just put on an anti-virus package that you go buy at an office supply store, the system is just going to blow up,” says Brown.

Lack of Security Control: Heavy Price Paid

As a result of such a decentralized environment, the college endured a number of widespread infections. In 2003, both the Welchia and MS Blaster worm ripped through student systems, grinding availability to a halt. Following a widespread infection of the Sasser worm during finals in 2004, the college knew it had to do more to stop the continuous worm outbreaks. The Sasser worm infected nearly every PC on campus; it was “unbelievably devastating,” says Brown.

No Admission For Viruses, Worms and Malware at Colby-Sawyer College

The school responded the best it could by installing anti-virus software and patching against the vulnerability that made it possible for Sasser to propagate. The process proved time-consuming, as IT administrators had to make in-person appointments with more than 900 students in order to clean infected systems. They found it nearly impossible to keep up with the proliferation of the worm, as it kept spreading as infected systems continuously reinfected those that had already been cleansed. The worm's denial-of-service attack ground the school's network to a halt, and nearly every PC had to be shut down in order for IT administrators to regain control.

"They decided to make sure that none of this ever happens again," says Brown, who was hired shortly after the outbreaks to head-up Colby-Sawyer's security efforts as a consultant at the time.

While trust and brand reputation is crucial for any company, it's especially true for colleges that depend heavily on alumni and community donations and gifts to keep running. "We have generous alumni who want to see the college continue to grow. And the last thing alumni want to see is a college that is under siege from viruses and worms, where sensitive student information is placed at risk," says Brown.

Security-Related Shutdown: Hopefully Never Again

Following the Sasser infection, Colby-Sawyer hired Scott Brown as its first security manager; he went to work immediately to make sure the school wasn't so vulnerable again. "Back then, security was handled by everyone, while no one was responsible for pulling it all together," he says. Brown began to unify Colby-Sawyer's security infrastructure by deploying anti-virus software that could be readily updated, and a Network Access Control system that examines student systems to make sure that their anti-virus and other security configurations are up to date before they're granted full access to the network.

In order to sustain the improved security, Brown needed the ability to scan the school's systems for software and operating system vulnerabilities and misconfigurations. The university had tried a number of scanners that, ultimately, failed to get the job done. "We had one that was just a glorified port scanner; you got a bunch of information that nobody knew what to do with," says Brown.

Security Vulnerabilities: Under Control

While examining various available scanners, largely because of its two-week free trial, Brown decided to try Qualys Inc.'s on-demand vulnerability scanner, QualysGuard. He found that with QualysGuard Colby-Sawyer could control its entire vulnerability management lifecycle: asset discovery, vulnerability assessments, security fix tracking, and comprehensive remediation reporting. Other vulnerability remediation solutions had proven too costly and lacked the on-demand scanning flexibility provided by QualysGuard.

“I can tell you that all of the time and effort we've invested in security has paid off. Our workload has been cut dramatically. We're much more efficient now—and much more secure.”

Scott Brown, Information
Security Analyst
Colby-Sawyer

No Admission For Viruses, Worms and Malware at Colby-Sawyer College

Brown's first course of action with QualysGuard was to scan the college's total administrative systems for all vulnerabilities ranked at levels three, four and five. "We had about 2,000 vulnerabilities. It was a real eye-opener," Brown recalls. While Brown immediately saw the benefits of QualysGuard, the school's budget remained tight considering all of the security technologies Colby-Sawyer had acquired: intrusion prevention systems, bandwidth managers, network access control, and new anti-virus software. "Qualys provides affordable academic pricing," says Brown.

Today, Colby-Sawyer depends daily on QualysGuard to keep the college's servers and PCs safe. All newly-built desktop images are scanned to ensure that they're compliant with security policy; internal systems are scanned three times a week, while externally facing Internet addresses are examined twice each week. "I can tell you that all of the time and effort we've invested in security has paid off. Our workload has been cut dramatically," says Brown. "Now, whenever vulnerabilities are announced, we quickly turn to QualysGuard and identify all of the systems that need to be taken care of right away. Prior to QualysGuard, all we knew was that there was a problem and a patch, and we had to log into each computer to see which needed patches," says Brown. "We're much more efficient now—and much more secure."

COLBY-SAWYER SCOPE & SIZE

New London, New Hampshire
964 undergraduates, representing
26 states and six foreign countries.
Total Employees: 380
Total Faculty: 128

BUSINESS

Colby-Sawyer, founded in 1837, is a comprehensive liberal arts college located in the scenic Lake Sunapee Region of central New Hampshire where students learn in small classes through a select array of programs that integrate the liberal arts and sciences with pre-professional experience.

BUSINESS PROBLEM

Provide effective IT security throughout its network to ensure a secure and highly-available academic environment.

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

As a critical part of its risk management program, Colby-Sawyer deployed QualysGuard to conduct daily scans of its critical servers and externally facing network addresses.

WHY COLBY-SAWYER CHOSE QUALYS

- Automated on-demand security and vulnerability audits
- Attractive academic pricing structure
- Highly accurate vulnerability and configuration scans
- Easy to deploy, manage, and operate
- Comprehensive reporting capability

WEBSITE

www.colby-sawyer.edu



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

