QUALYS™
ON DEMAND
VULNERABILITY MANAGEMENT

CASE STUDY: Florida Department of Health–Automating Network Security to Protect E-Gov Health Services and Data

Overview

Scope: Statewide

Business: Government health services

Size: 17,000 employees in the department serve Florida's population of 17 million people

Web site: www.doh.state.fl.us

The State of Florida is renowned for sun-based fun and relaxation, but inside, IT workers serving Florida's population of 17 million have been hard at work transforming manual government operations into e-government. The governor and state legislature set three goals for e-gov: ease information access to improve services; assure the safety of citizens and the security of sensitive information; and cut the cost of government through consolidation and sharing of resources. Through the pursuit of these goals, Florida has become a national leader in e-government. Florida began paving the way for e-government when it launched its e-gov initiative in 1999, three years before the U.S. passed similar legislation for federal agencies.

Florida's IT strategic vision for e-gov includes elements such as outsourcing and data center consolidation to cut costs while providing more efficient services, coordinated efforts to ensure state compliance with the Health Insurance Portability and Accountability Act (HIPAA), and improving cyber security of confidential information for all Floridians. The state's second largest agency, the Department of Health, is playing a key role in this transformation. Secure information technology is crucial for accomplishing the department's mission: "To promote and protect the health and safety of all people in Florida through the delivery of quality public health services and the promotion of health care standards."

IT security policy is devised and implemented by the department's Division of Information Technology. The realignment of IT security policies and procedures for e-gov included aggressive new measures, including the automation of vulnerability management for the Department of Health's enterprise network.

New IT Policies for E-Gov Raised the Profile of Network Security

The first step was upgrading the Department of Health's security framework to conform policies and standards to new legislative and regulatory requirements. Security received new emphasis in Florida's e-gov strategy because of a higher dependency of services and data using a single, converged IP network.

According to David Taylor, chief information officer in the department's Division of Information Technology, prior policies and standards were not linked to law. "We rewrote them to be agency-specific, referencing authority for each policy," Taylor said. "Now it's easier to get compliance."

A big legislative requirement was HIPAA, which has triggered industry-wide upgrades to security of networks and data

The Florida Department of Health Story

Business Problem
Cost-efficiently improve network security of public health services and personal health data.

Operational Hurdle
Department of Health required automation due to limited staff resources and distributed operations.

Solution
QualysGuard on demand vulnerability management and Scanner Appliances.

containing or transmitting confidential personal health information. “Our highest priority is safeguarding the data entrusted to us by the public,” says Taylor.

Issues of efficiency and cost control also affected new security policies and procedures. Florida had to provide secure e-gov while reducing the overall cost of IT. Cost-reduction strategies mandated by the state included reducing complexity of services and redundancy of agency resources; using lower-cost commodity-based components and open source software; using Government-Off-The-Shelf (GOTS) technology solutions; and reducing government investment for infrastructure and upgrades by outsourcing services.

Automation also was to play a key role in providing lower-cost security services. CIO Taylor notes the Department of Health’s IT organization is distributed, and has only 400 staff serving the department’s 17,000 employees. “Only two dozen staffers are devoted to security, which requires us to rely on standardized configurations served by automated security and management processes,” says Taylor. “Very few people actually touch the boxes.”

Automation Backs Network Event Monitoring System for Stronger Security

The heart of automating the Department of Health’s IT security is a new network event monitoring system developed in-house by the Division of Information Technology. A combination of open source tools and commercial security products underpin the system. The DOH automates as many processes as possible, such as software updates and patching. Normalization and correlation capabilities of the network event monitoring system help provide security managers with a holistic view of vulnerabilities and the state of security protection.

“One of our biggest challenges was making sure the automated processes were actually configuring and securing all devices in accordance with new policies and procedures,” said Taylor.

For example, network vulnerability scans were done with open source tools and one commercial product. Conducting scans, however, was still an inefficient, manual process—especially for time-intensive analysis of device logs and other security data.

“There was no easy, automatic way to scan everything we own or do on demand spot checking,” said Huber. “It was a manual, ad hoc process.”

To augment its security automation, the Department of Health conducted a three-month analysis of market alternatives for vulnerability management. The rigorous internal evaluation included working with solution providers to eliminate as many false positives as possible. The department chose the on demand QualysGuard service as its lead

Florida DOH Mandates

- Revamp security policies and procedures to match legal requirements
- Create automated security event monitoring system
- Automate vulnerability management

Why Florida DOH Chose Qualys

- Automates vulnerability management
- Identifies vulnerabilities
- Verifies correct patching
- Provides documentation for security auditors
- Helps comply with HIPAA

system component for finding vulnerabilities, managing the remediation process, and verifying execution of other automated security processes such as patching.

"With Qualys, we gained the ability to automatically scan everything we own for vulnerabilities," said Huber.

QualysGuard Helps the DOH Cut Vulnerabilities and Verifies Automated Security Processes

Use of the web-based on demand vulnerability management solution from Qualys has replaced inefficient, labor-intensive efforts to improve network security. The Department of Health now scans its entire network once a month and does daily scans on critical systems. "Automation is a very important piece of the Qualys solution," says Huber.

Confidence in the accuracy of vulnerability scanning and remediation has improved with Qualys, according to Taylor. "We used patching tools prior to Qualys but had to have a certain faith that they were correctly done," Taylor says. "Qualys taught us that our faith was misguided, which was disconcerting." On demand scans with QualysGuard probe network assets against the industry's largest vulnerability database of 4,000+ signatures.

Since it began to use QualysGuard, the Department of Health has nearly eliminated false positives and vulnerabilities. "Qualys has helped us reduce vulnerabilities, especially by identifying where automated patch processes are not working," says Taylor.

The department also uses QualysGuard for documenting network security efforts. "Qualys provides us with a documentation path for all servers including best security practices, vulnerability ranking and patches," says Huber. Upon request, vulnerability management reports from Qualys are also provided to auditors for verification of Department of Health compliance with HIPAA and other privacy regulations.

> "Qualys has helped us reduce vulnerabilities, especially by identifying where automated patch processes are not working."
>
> **David Taylor**
> CIO, Florida DOH

> "With Qualys, we gained the ability to automatically scan everything we own for vulnerabilities."
>
> **James Huber**
> Bureau Chief, Strategic IT
> Florida DOH

And because QualysGuard is a web-based service delivered over the Internet, the Department of Health has received its benefits without having to invest in additional infrastructure or staffing. QualysGuard's service-based model allows the department to save up to 90% of the cost of doing vulnerability management with manual, software-based processes.

The biggest measure of QualysGuard's benefits is documented assurance that the Department of Health is providing the strongest security for protection of networked data and IT systems.

"We take our responsibility as custodians of data very seriously," says Taylor. "We feel we now have the staff and tools in place to safeguard that data." Taylor says even the occasional internal virus is quickly isolated and eliminated. "They don't have a good footprint to expand because we're well patched and secured."

The department's record bears that out: "We have never had a security incident where data was at risk," Taylor says. He attributes the record to aggressive vulnerability management and use of a layered defense system, including automated solutions such as QualysGuard.

www.qualys.com