Automating Security and IT Risk Management

When the City of Miami Beach needed to streamline PCI DSS compliance as well as secure its internal networks and web-facing applications, the vacation capital of the Southeastern US found success through QualysGuard.

MIAMIBEACH

www.miamibeachfl.gov

INDUSTRY: Government

LOCATION: Miami, FL

SIZE: Pop. 89,000, 7.1 square miles

BUSINESS CHALLENGE: Automate many regulatory compliance and vulnerability management efforts

SOLUTION:
QualysGuard Vulnerability Management (VM)
QualysGuard Web Application Scanning (WAS)

WHY THEY CHOSE QUALYSGUARD:

- Hassle-free deployment and Software-as-a-Service delivery.
- QualysGuard automates network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking.
- QualysGuard WAS proved more accurate than other web application scanners.
- Comprehensive reports provide the actionable information needed to remedy software flaws.
- A highly-accurate, extensive database of security checks that is constantly updated.

IT departments are forced to stretch their budgets further every year. And as end-users and business executives ask more of them, the budgets earmarked to support those demands have remained relatively flat. The 2013 Budget Benchmarking Survey, published by the Corporate Executive Board, found that CIOs only expect their IT budgets to rise by 1.8% this year. This forces IT teams to be smart and strategic with how they put to use the budget and resources they're allocated.

Nelson Martinez, systems support manager for the City of Miami Beach, Florida, is always looking for ways to be smarter and improve how he manages and protects the IT systems the city depends upon to run. When it comes to the city's IT infrastructure, there are about 5,000 unique IP addresses that consist of endpoints, servers, routers, and other devices that must be managed and always kept reasonably secured.

Toward continuous risk management

About a year ago, Martinez started looking for ways to improve the efficiency of the city's IT security and risk management efforts. He decided to outsource the vulnerability assessments, as managing a fully-staffed, in-house security team was not a viable option. "It made sense for our internal security team to leverage a cloud-based service with expertise in vulnerability management," Martinez says.

The search didn't take long. One of the City of Miami Beach's service providers had been using QualysGuard, from Qualys Inc., to perform its mandatory PCI DSS (Payment Card Industry Data Security Standard) vulnerability scans. "We had been using this service provider for a number of years, and Qualys had already proven itself to be a reputable service to us," says Martinez. He decided that the city would continue to have the services provider perform the PCI DSS scans for regulatory compliance purposes, but it would also conduct automated, regular scans across their network in addition to its own PCI DSS scans.

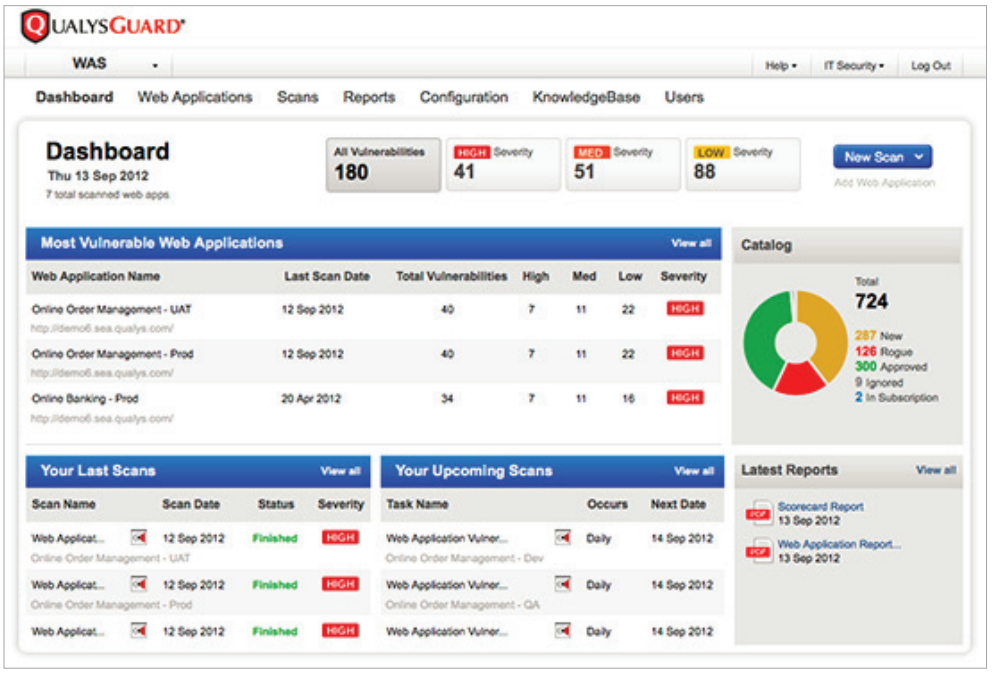
"This way, we would be maintaining the overall infrastructure as tightly as possible, but also preparing ourselves so that there weren't any surprises come time for our PCI DSS assessments," he says. To do so, Martinez and his team would use QualysGuard Vulnerability Management (VM), leveraging the Qualys Cloud Platform. QualysGuard VM automates the life cycle of network auditing and vulnerability management across the enterprise, 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 protects systems against the latest security threats without substantial cost, resource, and deployment burdens.

By continuously and proactively monitoring network access points with QualysGuard VM, Martinez and his team no longer need to depend on third party service providers to assess their infrastructure. They have largely automated the process for themselves, and have dramatically reduced the time it takes to research, scan, and fix network exposures, and proactively remediate network vulnerabilities before they can be exploited.

> "To succeed in IT today, you have to wear more than one hat. And QualysGuard makes it so you don't have to worry about your vulnerability assessments. The scans are set up, and we know that they'll run. If something is found that needs attention, we will know immediately. That's how QualysGuard enables us to be proactive."
>
> **Nelson Martinez**,
> Systems support manager at City of Miami Beach

Automated compliance and security risk management

They've also been able to maintain PCI DSS compliant systems on their own. "Our ongoing assessments make it straightforward for us to remedy any issues that may arise before our scheduled quarterly assessment. So once we actually perform the real third-party assessment, we know it's going to pass, thanks to QualysGuard," Martinez says.



Martinez explains how easy it was to deploy QualysGuard, with most of the effort involving the automated mapping of the city's network and configuring the scope of the scans. "The QualysGuard appliance is a snap

to install, and once running, it doesn't require much in the way of maintenance, and the scans run automatically," he says.

That maintenance-free service and automation is something that Martinez greatly appreciates about QualysGuard. "Because QualysGuard is an outsourced service, we don't have to worry about anything when it comes to maintaining the device or the vulnerability Knowledgebase," he says. The result is that the city's security group can focus on other initiatives.

In addition to its network and PCI DSS scans, the City of Miami Beach's IT team has also established regular assessments of the external facing network assets and web servers with QualysGuard Web Application Scanning (WAS). Also built on the QualysGuard Cloud Platform, QualysGuard WAS provides accurate and swift web application security assessments and identifies web application vulnerabilities in the OWASP (Open Web Application Security Project) Top Ten, such as SQL injection, cross-site scripting, URL redirection, and many other pressing vulnerabilities.

"We scan all of our web applications for potential vulnerabilities. It's about being proactive and finding flaws as quickly and rapidly as possible," says Martinez. It's also about succeeding with tightly run operational teams. "The reality is everyone in an IT department, unless you're talking about a very big IT shop, is focused on the day to day operations. They are launching new products, they are conducting system maintenance on the weekends, and they're dealing with production issues during the week. QualysGuard WAS enables our team to also stay ahead of security issues while managing everything else," he says.

Martinez explains how QualysGuard VM and WAS all work together to help his team to improve its ability to secure the infrastructure, maintain regulatory compliance, and effectively achieve more with the same resources. "To succeed in IT today, you have to wear more than one hat. And QualysGuard makes it so you don't have to worry about your vulnerability assessments. The scans are set up, and we know that they'll run. If something is found that needs attention, we will know immediately. That's how QualysGuard enables us to be proactive," Martinez says.