QUALYS™
ON DEMAND
VULNERABILITY MANAGEMENT

CASE STUDY: Bank of the West — Major Financial Institution Protects Information Assets Through Regular Network Vulnerability Audits

At a Glance

Company: Personal and business banking

Location:
Headquarters in San Francisco, California; 300 branches throughout the West

Systems Scanned:
Internet-facing servers, termination routers for Internet access, Check Point firewalls

Chief Benefits:

- Defense of valuable information assets
- Protection of customer confidence and bank reputation
- Access to comprehensive KnowledgeBase of vulnerabilities and remedies, reducing IT staffing requirements
- Scalability to handle network growth
- Compliance with FDIC audit requirements

BANK OF THE WEST

Bank of the West provides personal and business banking services for customers in Northern California, Oregon, New Mexico, Nevada, Washington, and Idaho. Protecting customer information ranks as a top priority for the bank's IT group.

"For financial institutions, information is an asset that translates directly into revenue," says Lenard East, VP Network Engineering and Operations. "By protecting our information, we not only protect our revenues, we also maintain the public image and customer confidence at the heart of the bank's reputation." As part of its security efforts, Bank of the West regularly identifies and resolves network vulnerabilities with the QualysGuard on demand vulnerability management solution.

Internet Applications Demand Proactive Measures

Bank of the West adopted QualysGuard in early 2000. Before that time, the bank's information assets were stored in mainframes with no external access, so risk was small. Then the bank increasingly began taking advantage of the Internet—for example, to obtain credit scores for customers applying for loans, and to offer a popular online banking service called eTimeBanker. The bank's expanding use of the Internet drove the decision to take proactive security measures.

After evaluating numerous vulnerability assessment solutions, Bank of the West selected QualysGuard. "The QualysGuard solution is easiest to deploy, requires the least maintenance in terms of day-to-day care and feeding, has the least potential for conflicts with our existing platforms and production environment, and is economical," states East. The economic advantages of QualysGuard pertain both to subscription costs and reduced staffing requirements. "With its huge KnowledgeBase of known vulnerabilities and fixes, QualysGuard eliminates the need to hire experts on each of our operating systems and applications," says East. This benefit is particularly compelling given the bank's heterogeneous network, which includes Check Point firewalls; Microsoft Internet Information Server (IIS), Windows NT, and Windows 2000 operating systems; Nokia and Sun platforms; and many other hardware and software components.

Detects and Prioritizes Vulnerabilities

Bank of the West ran its first QualysGuard scan the day after signing an agreement, scanning all Internet facing devices, including termination routers for Internet access and Check Point firewalls. As soon as the bank provided the IP addresses and network names of the components it wanted to scan,

QualysGuard Platform: Automated Network Vulnerability Identification, Remediation and Verification

QualysGuard is the only scalable, affordable on demand solution designed for companies of every size to audit network vulnerabilities. Delivered over the Internet, QualysGuard employs advanced vulnerability detection techniques, with its proprietary Inference-Based Engine, to assess a network's security exposures and suggest remedies before intruders can take advantage of them.

Qualys provided a sign-on and password. From that point on, the bank could conduct unlimited scans. In fact, Bank of the West conducted daily scans until it had identified and resolved nearly all of the several hundred vulnerabilities discovered during the first scan. After following Qualys' recommendations to fix the vulnerabilities, only a very few vulnerabilities remain—none of which are serious. Now the bank runs pre-scheduled scans at regular intervals, supplementing them with manual scans whenever a device is updated or reconfigured.

Provides Recommendations for Fixes

After each QualysGuard scan, the bank receives a report identifying vulnerabilities and prioritizing them by severity level: 1 to 5. Each reported vulnerability is accompanied by links providing more information, vendor-provided patches, or other recommendations. "The recommendations are among the most valuable QualysGuard features," says East.

Recently, for example, a QualysGuard report noted that the bank's Check Point firewall had a vulnerability related to the operating system version, and recommended upgrading to the next release. The bank made the recommended fix, re-scanned, and determined that the vulnerability had been eliminated. East notes that the bank has had similar recommendations pertaining to Microsoft Internet Information Server. "With limited staff, the type of knowledge and recommendations that Qualys offers is invaluable," he says.

> "By showing the FDIC our QualysGuard reports, we prove that we regularly identify risks, rank them by priority, adjust our actions to eliminate those risks, and then verify that we're no longer vulnerable."
>
> "With its huge Knowledge-Base of known vulnerabilities and fixes, QualysGuard eliminates the need to hire experts on each of our operating systems and applications."
>
> **Lenard East**
> VP Network Engineering and Operations

The QualysGuard reports are especially helpful during the FDIC's yearly audit of risk management, when the bank is asked which tools it uses to control risk, and how often. Verbal assurances are not enough. "By showing the FDIC our QualysGuard reports, we prove that we regularly identify risks, rank them by priority, adjust our actions to eliminate those risks, and then verify that we're no longer vulnerable," says East.

Augments Bank's IT Staff

East has come to regard QualysGuard as an augmentation to his staff: "QualysGuard is almost like having an additional staff member to do R&D on our numerous hardware and software platforms," he says. "It's another pair of eyes that will never get tired of seeing what the brightest hacker is up to, documenting it, and developing a remedy that will help protect our business. QualysGuard helps me sleep at night."

If QualysGuard is like another staff member, it's an extremely productive one. Since subscribing to QualysGuard, Bank of the West has grown from 102 branches and one Internet access point to 300 branches and six Internet access points. The QualysGuard service scaled to scan more devices without a hitch. "As the network continues to grow in terms of size and services, our risks will increase," says Jim Jennerson, Enterprise Information Security Officer. "Tools like QualysGuard will enable us to continue to identify risks and take proactive action, protecting our assets, our customers, and our business."

www.qualys.com