



COMMERCIAL BANK OF DUBAI AUTOMATES VULNERABILITY MANAGEMENT

By moving away from inaccurate open source vulnerability scanners, the Commercial Bank of Dubai is able to rapidly remedy the software flaws that could threaten the security of its IT network.

“We no longer have to spend so much time checking the accuracy of scanner reports, or maintaining the software. We simply assess our network regularly and can trust Qualys’ results.”



Rinaldo Ribeiro, Senior Manager and
Head of IT Security
Commercial Bank of Dubai

The emirate of Dubai, part of the United Arab Emirates (UAE), is growing. While Dubai’s economy once relied heavily on oil revenue, today Dubai is an important tourist destination and its port, Jebel Ali, constructed in the 1970s, is home to the largest man-made harbor in the world. Dubai is also developing as a hub for such service industries as IT and finance. Some of the IT companies with offices in Dubai include Oracle Corporation, Microsoft, and IBM.

Founded in 1969, the Commercial Bank of Dubai (CBD) is in the thick of the region’s economic growth. Begun as a public shareholding company, the bank last year reported record net profit of AED 601 million, and assets totaling AED 18.7 billion. Now, the Commercial Bank of Dubai offers a wide range of retail and commercial banking services with a network of 21 branches (14 in Dubai).

For years, the CBD and Rinaldo Ribeiro, senior manager and head of IT Security at the bank, had relied on open source tools to scan its systems for vulnerabilities, but as the bank’s network grew more complex, they simply couldn’t provide the accuracy or reporting the bank required. Today, with more than 200 servers, security administrators had to dedicate unacceptable blocks of time to vet the number of false positives generated. Additionally, the lack of comprehensive and business-context reporting meant IT teams couldn’t present reports to business departments without manually writing reports that managers could understand.

The Rising Vulnerability Threat

Today’s IT security threats such as worms, Trojans, keystroke loggers, and Web-based spyware designed to steal financial information are becoming more frequent and invasive as they grow in sophistication. All of these threats are fueled by software vulnerabilities—an average of 155 new vulnerabilities are announced each week. Mitigating these risks is one of the greatest challenges to any size organization today, let alone a financial institution. And the fact is that while defenses such as network firewalls, anti-malware, and intrusion detection/prevention systems provide necessary layers of security, they’re not designed to proactively detect network vulnerabilities and can’t reliably prevent attacks, especially quick moving zero-day threats.

To keep systems persistently at a high level of security, more companies are turning to vulnerability risk management tools. Vulnerability management—the processes associated with finding, remedying, and then validating that software vulnerabilities and system misconfigurations have been fixed—has become the central component of security programs built on best practices.

Commercial Bank of Dubai Automates Vulnerability Management

In fact, security professionals who use vulnerability management tools are able to correct weaknesses before they are exploited, and no longer rely solely on defensive security measures to protect their infrastructure and sensitive information.

The challenge is putting into place an automated, repeatable, verifiable way to manage software vulnerabilities. As the CBD experienced, many open source and commercial vulnerability scanners fall short because they don't offer the level of reporting, accuracy, or thoroughness needed to stay ahead of today's fast-moving threats. The bank needed a more efficient way to ensure that its systems always were kept up to date, and that it could demonstrate its high level of security for upcoming UAE regulations that require banks to maintain security best practices. "We turned to a number of our trusted security service providers to find a solution. The company that looked the very best from the beginning was Qualys," says Ribeiro. "From the first presentation, QualysGuard looked like it would give us the accuracy and reporting we sought."

Automated, Verifiable Vulnerability Risk Management

CBD selected QualysGuard from Qualys Inc., thus enabling the bank to streamline control of its entire vulnerability management lifecycle: asset discovery, vulnerability assessments, and track security fixes. "We wanted a tool that was easier to use, and more accurate than our open source scanners," says Ribeiro. "We found that with QualysGuard," he adds. The on-demand solution delivered as a Web service required no software or costly infrastructure for CBD to deploy, and it is fully managed by Qualys. "We don't have to keep the devices up to date. Qualys manages everything for us. We can focus on keeping secure," says Ribeiro.

The thorough QualysGuard scans not only provide the ability to identify and mitigate vulnerabilities and misconfigurations; its comprehensive reporting can be tailored for security teams, IT operations, and the bank's business executives. "We no longer have to waste time making reports manually. The administrators get what they need, and the business executives can see how well we're managing our network vulnerabilities," he says. Perhaps the greatest saving comes from QualysGuard's accuracy and the fact that security team members no longer have to waste extraordinary amounts of time chasing false positives. CBD benefits from Qualys' largest KnowledgeBase of vulnerability signatures in the industry (5,500+) and having more than 150 million IP audits per year with a Six-Sigma accuracy rate. And since QualysGuard is centrally managed, all vulnerability updates are provided in real time.

Today, CBD conducts QualysGuard scans of its internal network every week, and of its external, Internet-facing networks every day. "We no longer have to spend so much time checking the accuracy of scanner reports, or maintaining the software. We simply assess our network regularly and can trust Qualys' results."

COMMERCIAL BANK OF DUBAI SCOPE & SIZE

United Arab Emirates
AED 18+ billion (total assets)
AED 600+ million (annual revenue)
20+ branches

BUSINESS PROBLEM

Needed effective and efficient way to keep its network and IT infrastructure secure and updated with the latest software patches.

OPERATIONAL CHALLENGE

Open source vulnerability scanners lacked accuracy, and IT security team-members had to spend inordinate amounts of time sorting the false positives from actual vulnerabilities.

SOLUTION

QualysGuard Express

WEBSITE

www.cbd.ae



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

