



EURO BANK OPTIMIZES VULNERABILITY MANAGEMENT

This leading retail bank automated key processes for vulnerability management, slashing the amount of time it spent every week remediating system vulnerabilities and streamlining security throughout its 30 networks.

“QualysGuard makes it possible for us to get so much more done with such less effort. With our previous scanner, it took 20 hours a week for us to conduct our work. With QualysGuard, that time is reduced to three hours a week. Most everything is accomplished automatically now with an 85 percent time savings.”

Andrzej Piotr Klesnicki
IT security manager,
Euro Bank

Euro Bank S.A. is a growing retail bank headquartered in Wroclaw, Poland, and its 3,100 employees serve its customers from more than 500 bank branches across the country. As Euro Bank’s business prospered, and its locations and number of customers grew, so did the challenges associated with maintaining the business-technology systems the bank depends upon so heavily. “We needed to expand our vulnerability management processes to make certain our same security posture is in place throughout all of our systems,” explains Andrzej Piotr Klesnicki, IT security manager at Euro Bank.

Manual Vulnerability Processes Overly Time Consuming

One of the most important initiatives for any organization to have in place to ensure that its systems are properly maintained and secure is a continuous vulnerability management program. That entails periodic assessments of servers, endpoints, and network devices designed to identify systems that are in need of patch or system updates. Euro Bank had an ongoing vulnerability management program in place: the IT security team would conduct monthly vulnerability assessments of its critical systems to ensure that its system patch levels were kept up to date, and firewall and intrusion prevention systems were tuned properly. However, the processes primarily were manual, and it was proving increasingly time consuming to evaluate the security of the bank’s complex array of storage systems, web servers, online banking services, databases, and various business-to-business applications.

It was becoming clear that a better way was needed. Unfortunately, the commercial assessment tool the IT team relied upon also failed to provide a way to automate many of the processes associated with vulnerability management. “We had to do everything manually, from getting information about vulnerabilities, to selecting the teams for remediation, to managing the remediation process,” says Klesnicki. “That was extremely time consuming.”

To make matters worse, the bank’s commercial vulnerability scanner was limited to assessing a single network. “To expand our capabilities to work with all of our locations, we would have had to purchase many more scanners,” Klesnicki says. “That would make it too expensive.”

To optimize the vulnerability management program, Klesnicki and his team wanted to find a way to conduct vulnerability assessments centrally throughout all of its 30 networks and to bring a much higher degree of automation to the processes. That’s when Klesnicki and the security team at Euro Bank began evaluating other possible ways to conduct its security assessments.

Increased Automation and System Transparency

After a careful evaluation, aided with the help of a local consultancy IMNS Polska, the security team selected QualysGuard Vulnerability Management (VM) from Qualys Inc. QualysGuard VM automates the vulnerability management lifecycle for organizations of all sizes. Through its Software-as-a-Service (SaaS) delivery model, QualysGuard provides Euro Bank with detailed network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Powered by the most comprehensive vulnerability KnowledgeBase in the industry, QualysGuard VM spots and helps to remedy the software flaws and system misconfigurations that make

Euro Bank Optimizes Vulnerability Management

many exploits and attacks successful. As an on-demand solution, there is no additional infrastructure to deploy or manage.

The security team at Euro Bank knew immediately that its decision to move to QualysGuard VM was the wise choice. “The implementation went effortlessly and administration is very easy,” says Klesnicki. Today, a single QualysGuard VM appliance enables Euro Bank to evaluate the security of all of its 30 individual networks. “QualysGuard’s assessments provide us the full visibility we needed. In fact, within a day we had full visibility into our networks and all of the information we needed to identify and remedy our system risks,” he adds.

And, because QualysGuard VM automatically identifies and maps all networked devices; finds vulnerabilities and provides actionable remediation advice; and delivers easy-to-understand reports to IT asset owners, Klesnicki reports phenomenal time savings and results. “QualysGuard makes it possible for us to get so much more done with so much less effort,” he says. In fact, Klesnicki calculates that QualysGuard VM has slashed the amount of time the security team had to dedicate to vulnerability management by 85 percent. “With our previous scanner, it took 20 hours a week for us to conduct our work. With QualysGuard, that time is reduced to three hours a week, or less. Most everything is accomplished automatically now,” he says.

Building on Success

With the success it has reaped by optimizing its vulnerability management program, the security team now is considering new ways to improve how they manage risk even further. “Our goal was to find a vulnerability assessment tool that would help us streamline vulnerability management throughout the organization with improved accuracy and automation. And that’s exactly what QualysGuard has helped us to achieve,” he says. To obtain even further benefits, Euro Bank is considering how the company can manage the configuration and access policies of its systems, databases, and applications more effectively.

For these efforts, Euro Bank will evaluate QualysGuard Policy Compliance to help automate the assessments of the organization’s operating system and application policies and controls – and then compare policy assessment results to the policies that should be in place. This will help the security team validate their level of compliance and repair any discrepancies. “We are now looking at QualysGuard Policy Compliance to bring the same level of success we’ve experience with QualysGuard Vulnerability Management.”

ORGANIZATIONAL OVERVIEW

Organization: Euro Bank S.A.
Location: Headquarters: Wroclaw, Poland
Scope: Growing retail bank with 3,100 employees and more than 500 bank branches across Poland.

BUSINESS CHALLENGE

The bank wanted to find a way to automate many aspects of its vulnerability management lifecycle.

SOLUTIONS

QualysGuard Vulnerability Management

WHY EURO BANK CHOSE QUALYSGUARD ?

- A single QualysGuard appliance can assess 30 of the bank’s internal networks centrally.
- Automated, on-demand security and vulnerability audits.
- Highly accurate vulnerability and configuration scans.
- Detailed, comprehensive, actionable reporting.
- Easy to manage and operate.



QUALYS
www.qualys.com

USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • Beechwood House, 10 Windsor Road, Slough, Berkshire, SL1 2EJ • 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
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • P.O Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495



ON DEMAND SECURITY