



ASTELIT DIALS INTO A NEW, POWERFUL VULNERABILITY MANAGEMENT SERVICE

For improved security and regulatory compliance, this leading telecommunications provider knew it had to move away from unreliable, decentralized vulnerability scanners.

“Though QualysGuard, we now have a centrally managed vulnerability management program.”



Andriy Zhelo,
Manager of information security
management unit
Life:)

With the increase of complex attacks on business IT systems, and the necessity for sustainable approaches to regulatory compliance, it's never been more important for organizations to ensure that they have effective vulnerability management programs in place. Also, as a way to make certain that attackers can't penetrate out-of-date networks or Web site configurations to steal corporate data, plant malware, or snag customer account information, effective vulnerability management is one of the best defenses organizations can have in place.

However, it's not easy. Not without the right tools. Such a vulnerability management program requires putting into place a continuous system management lifecycle, including asset discovery, asset prioritization, vulnerability assessment, analysis, remediation, fix verification, and powerful risk and compliance reporting. This is how all organizations can quantify their security progress and proactively maintain the confidentiality, integrity, and availability of their IT systems and sensitive customer information – and keep auditors content.

Consider the efforts of Astelit, the Ukrainian GSM operator, widely known for its life:) brand, that serves 8.7 million contract and prepaid subscribers. The company's network covers 96,4% of Ukraine's population. life:) provides roaming opportunities in 172 countries via 468 roaming partners. 488 life:) customer care centers and exclusive sales points operate in 185 cities of the country. In addition to that, life:) subscribers can order life:) services through 34,600 non-exclusive shops.

Keeping its vast IT system secure, which consists of 140 servers and 32 network connected devices, had proven to be a steep, but surmountable, challenge. Two years ago the company was relying on open source vulnerability scanners to conduct periodic assessments. While the systems were maintained securely, there was no repeatable vulnerability management process. “We needed a more effective, repeatable, measurable vulnerability management program in place, especially for systems that manage critical data,” says Andriy Zhelo, manager of the information security management unit. “Not only would this help us to maintain adequate levels of security, but also would help us remain compliant with a number of government and industry regulations.”

The move away from ad-hoc assessment processes

To get there, Zhelo and the security team knew they would have to improve the tools they used to find and remedy system vulnerabilities. For that, Astelit chose QualysGuard Vulnerability Management (VM), from Qualys Inc. Zhelo explains that Astelit selected QualysGuard because of its comprehensive vulnerability management capabilities, the ease with which it enables assessments to be performed, and its ability for remote management. Initially, Astelit used QualysGuard to harden its Internet-facing Web applications and external perimeter. As those systems were completed, the security team turned its attention to its internal network. “We covered our internal critical hosts, those that are a subject for Sarbanes-Oxley compliance review, in order to enhance our existing patch management process,” Zhelo says.

Astelit Dials into a New, Powerful Vulnerability Management Service

Through its Software-as-a-Service (SaaS) delivery model, QualysGuard provides Astelit with the detailed network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking it needed. Powered by the most comprehensive vulnerability knowledge base in the industry, QualysGuard VM spots and helps to remedy the software flaws and system misconfigurations that make many attacks possible. Also, as an on demand service, there is no additional infrastructure for Astelit to deploy.

“We are planning to use the QualysGuard Policy Compliance (PC) module soon to assess those platforms for security controls with respect to Sarbanes-Oxley requirements and security best practices,” Zhelo says. QualysGuard PC extends the capabilities of QualysGuard VM to collect operating system configuration and access control setting from hosts and other IT assets within the enterprise. QualysGuard PC then maps this information to user-defined policies in order to accurately document compliance with security regulations and business mandates. QualysGuard PC also provides an efficient and automated workflow that allows IT security and compliance professionals to help define system security compliance, validate that systems are operating within policy, and provide proof of compliance to audit teams.

Because QualysGuard VM and PC are delivered as an on demand Web service, QualysGuard assesses and helps to remedy network security at a fraction of the cost associated with traditional software. “Our current vulnerability management scope with QualysGuard covers all critical corporate IT assets and Web applications. Also, our corporate network edge is part of our vulnerability management program to defend possible external risks, including such important network components as routing devices and firewalls,” he says.

Insightful, easy-to-grasp reports for both business and technical managers mean that the entire organization knows the security and compliance status at any moment. At the same time, pre-built and fully customizable reporting capabilities provide a straightforward substantiation of security and compliance levels to internal auditing teams and external regulators. “If we didn’t use QualysGuard and used another dedicated vulnerability scanner, we definitely would need more labor resources to manage our current program,” he says.

OVERVIEW

Business: Third largest Ukrainian mobile telephone network operator.

Scope: Ukraine

Size: \$339,3 mil revenue in 2010 (life.) is one of the largest employers in the country, employing around 1,100 people

BUSINESS PROBLEM

Astelit was relying on open source vulnerability scanners to conduct periodic assessments. While the systems were maintained securely, there was no repeatable vulnerability management process. Astelit needed a more effective, repeatable, measurable vulnerability management program in place.

SOLUTION

QualysGuard Vulnerability Management

WHY ASTELIT CHOSE QUALYSGUARD?

- Ease of use: very simple user interface that doesn’t require extensive training
- Streamlined vulnerability management workflow.
- Qualys’ network infrastructure scans are highly accurate and reliable.
- Comprehensive reports provide the insight needed to mitigate most pressing risks first.

WEBSITE

www.life.com.ua



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

