# OLYMPUS

## OLYMPUS USES QUALYS' SOLUTION TO ASSURE THAT ITS IT INFRASTRUCTURE REMAINS SECURE AND IN CONFORMITY WITH REGULATIONS

*A business such as Olympus Europa Holding GmbH can only efficiently monitor the security guidelines of its IT infrastructure if the testing mechanisms are highly automated and fully integrated into the business's workflow. With the QualysGuard Suite, Olympus has established a central monitoring process that also serves as the data basis for communicating with its executives.*

> **" QualysGuard is the central basis for communication with our executives. "**

Matthias-Marc Gsuck
IT Audit Manager IT Security,
**Olympus Europa**

Founded as "Takachiho Seisakusho" in Japan in 1919 and renamed "Olympus Optical Co, Ltd" in 1949, Olympus ranks among the world's leading manufacturers of optical products. In addition to digital cameras for the consumer market, the company's spectrum of products primarily includes microscopes and endoscopes for medical and industrial applications.

Olympus's forty-seven European subsidiaries are conjoined in the Olympus Europa Holding GmbH, which is headquartered in Hamburg, Germany. The holding company offers its subsidiaries comprehensive services in the fields of finances, human resource management, IT, logistics, marketing and business communication. In addition to the Corporate Division, Olympus Europa Holding also includes the Product Division and the Medical Systems and Micro-Imaging Solutions Group.

The Olympus Europa Holding GmbH employs a staff of 4,700. Revenues in the 2009-2010 fiscal year totaled 1,383.712 million euros.

Olympus' IT infrastructure is based on Windows servers and clients, plus a variety of host systems (databases and Citrix terminal systems). Olympus Europa relies on Cisco in the network area. The business orients itself along the guidelines specified in Standard 27001 for Information Security Management (ISMS) and it is certified according to the standard.

### Automating the Scans Was Unavoidable

Particularly sensitive IT areas in the intranet and extranet, e-commerce and CRM had already been regularly scrutinized to search for weak points. "Here at our Hamburg location, we had established a testing scheme that satisfies the Sarbanes-Oxley (SOX) requirements and/or JSOX (its Japanese equivalent) and also complies with the COSO- and CObIT frameworks," says Matthias-Marc Gsuck, IT Audit Manager IT Security at Olympus Europa.

These tests had originally been manually conducted and had used, for example, Nessus and other open-source systems. The results had been quite good, but because of the extensive size of the IT infrastructure, manual handling had soon reached the limits of its capability. Independent systems for conducting such tests existed, but they required continual updating. "The test schemata were oriented according to the business sequences, so it was also necessary to include the corresponding specialized divisions whenever these updates were conducted. This involved a tremendous amount of labor, so automating the scans was unavoidable," Matthias-Marc Gsuck explains.

### In the Future, Clients Too Will be Tested to Assure They Conform to Regulations

The people responsible for IT at Olympus Europa therefore sought a scan solution that could unify the analyses of weak points throughout IT areas and that could be centrally guided. No local installations should be needed on the individual computers and other devices.

**Olympus uses Qualys' solution to assure that its IT infrastructure remains secure and in conformity with regulations**

With its software-as-a-service (SaaS) approach, the QualysGuard Suite was therefore precisely what Olympus Europa had been seeking. After a lengthy test phase, the QualysGuard Vulnerability Management (VM) module has now been implemented in productive operations. The Policy Compliance module and the Web Application Scanning module, both from Qualys, are currently running in pilot operations.

Thanks to the SaaS concept, analyses of weak points in Olympus Europa's various business divisions can be used uniformly. The scan parameters can be individually adjusted to match the requirements of each particular task, and these adjustments can be accomplished without the need for onsite installation of software or hardware.

QualysGuard has helped to automate the entire workflow at Olympus Europa. "Patch processes in firefighter style [i.e. as retroactive responses to emergencies] simply aren't suitable for the high degree of security that we need," explains Matthias-Marc Gsuck. In the future, he says, modules such as Policy Compliance will automatically scan not only the abovementioned exposed systems, but also the clients.

### Regulatory Requirements Are Well Covered by QualysGuard

According to Gsuck, the QualysGuard Scan Engine thus acquires an important added value because it can also be used to cover the regulatory requirements. The necessary guidelines are integrated into the workflow and the ticketing system. "We began with a test account from Qualys, which we still have, but in the meantime we also have a license for QualysGuard based on IP addresses," Matthias-Marc Gsuck recounts from the history of the collaboration. Olympus Europa presently scans approximately 2,000 IP addresses, and it intends ultimately to implement this solution on all core systems. Circa 6,000 systems (servers, clients and network components) could be added in coming years, Gsuck says. "As far as the processes and the assignation of the systems is concerned, Qualys fits as perfectly as a lid fits its pot," the IT audit expert enthuses. Gsuck further explains: "One system proprietor is defined for each host, and this information is automatically transferred into the ticketing system so everything is transparent, comprehensibly traceable and correctly assigned to its responsible authority. This assures compliance with the rules stipulated by SOX and with the internal control systems that are valid at Olympus."

Another factor which was important in persuading Olympus to decide in favor of QualysGuard is that Qualys delivers an application programming interface (API) which can be easily handled. This assures that the results of the analyses of weak points can be readily integrated into the system-management and helpdesk systems. "Our systems for these purposes will be consolidated in coming years, but scanning for weak points shouldn't necessitate a prior decision for or against a particular management system – we wanted to remain completely free in this choice," Gsuck explains.

### The SaaS Approach Offers Tremendous Advantages

Some businesses are still rather hesitant to implement SaaS solutions in the security field because internal data are entrusted to an external service provider. Matthias-Marc Gsuck understands their reluctance, but he doesn't share it in this instance. After all, data from weak-point analyses are stored in QualysGuard's database in an enciphered form that's accessible only to the client to whom these data belong. Above all, Gsuck sees tremendous advantages: for example, QualysGuard VM can use matured correlative mechanisms to assign weightings to recognized weak points.

The SaaS approach brings inestimable benefits because, on the one hand, the requirements of individual parts of the business can be quickly implemented and, on the other hand, the scan process can be centrally guided, which also facilitates centralized reporting. "For me, the QualysGuard platform is simultaneously also the central data basis for communicating with the management. The reports contain all of the essential points and are readily comprehensible, so they strengthen our executives' commitment to IT-security-related issues," says the specialist responsible for IT auditing at Olympus Europa.

**OVERVIEW**
**Business:** Olympus Europa Holding GmbH
**Branch of industry:** Optical industry (digital cameras, endoscopes and microscopes)
**Business' headquarters:** Hamburg, Germany
**Business' size:** Revenues in the 2009-2010 fiscal year totaled 1,383.712 million euros; 4,700 employees.

**GOALS FOR IT SECURITY**
Automation and centralized guidance of weak-point analyses

**SOLUTIONS**
- QualysGuard Vulnerability Management (in productive operation)
- QualysGuard Policy Compliance Management (in pilot operation)
- QualysGuard Web Application Scanning (in pilot operation)

**WHY DID OLYMPUS EUROPA HOLDING GMBH CHOOSE THE QUALYSGUARD SUITE ?**

- QualysGuard enables Olympus to automate existing test schemata and to integrate them into the workflow.

- The API from QualysGuard leaves the user all freedoms with regard to inclusion in other software solutions.

- Without requiring onsite installation of software or hardware, the SaaS concept makes it simple to use the solution's scanner in Olympus Europa's various business units.

- QualysGuard serves as an ideal basis for communication between the specialists responsible for IT security and the business' executives.

- The licensing model, which is based on scanned IP addresses, is equitable and readily comprehensible.