



EPO STREAMLINES VULNERABILITY MANAGEMENT TO ENSURE THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF PATENT INFORMATION

As the European Patent Office grew increasingly reliant on its IT infrastructure to transform how it accepts and manages patent applications, the security risks of its infrastructure grew, too. So the EPO sought a more effective way to automate its vulnerability management processes.

“Through the use of QualysGuard, we’ve managed to hold down the number of full-time employees dedicated to security that would have been required to be.”



David Allin, Director of Planning, Security, and Inventory
European Patent Office

The patent system plays a vital role in manufacturing and knowledge-based economies. And with the accelerated rise of international trade, organizations seeking to protect their intellectual property find that they need to increasingly weave through a complex matrix of patent laws that vary from nation to nation. Founded in 1977, The European Patent Office (EPO), which now comprises 32 countries, including every member of the European Union, aims to remove much of the complexity involved in filing for, and attaining, patent protection in Europe.

The EPO has proven a tremendous success. In 2006, the organization received more than 200,000 patent applications, and granted just over 60,000. The processes and labor required to determine whether the information within an application actually describes a novel invention is both complex and information-intensive. Of the 6,500 employed by the EPO, nearly 4,000 are engineers dedicated to the very detailed technical analysis of each application in search of true novelty.

To build greater efficiency, and enhance and streamline application submission and analysis, the EPO has undertaken a huge effort to move toward digitizing the largely paper-driven application process. “When we saw the number of applications submitted each year continuing to increase, we recognized the clear benefits of digitizing as much of the process as possible,” says David Allin, director of planning, security and inventory for the EPO. Today, nearly 40 percent of all applications the EPO processes are received electronically. In addition, the EPO’s patent search portal, Esp@cenet, makes more than 400 million pages of information, and 100 different databases, freely available for search. “We serve about 200 gigabytes of data a day over the Internet, and all of the supporting systems are internally hosted and maintained,” says Allin.

Effective IT Security Is Crucial

While these efforts have dramatically streamlined the EPO’s patent application acceptance processes and associated workflow, they also have required the deployment of hundreds of additional servers within its infrastructure. These deployments, and the exposure of more of its internal IT systems to the Internet, have significantly increased the organization’s IT security risks. “While we have excellent and technically competent people, these systems were all set up for various projects within the organization at varying times. Without centralized management, properly operating and maintaining these systems and the associated risk grew difficult to sustain,” says Allin.

EPO Streamlines Vulnerability Management to Ensure the Confidentiality, Integrity, and Availability of Patent Information

The stakes here are high. It's vital that EPO not only keep those systems secure, but it must ensure the security of the very confidential patent information it receives, and make certain the availability of its databases and the integrity of the information they hold remain intact. "If we were to suddenly discover that our databases, against which we validate the legal position of a patent, have been compromised, we would have the very uncomfortable problem of determining whether the patent we granted was valid," says Allin.

The most effective ways to maintain the highest levels of security and system availability possible is to put into place a continuous process of assessing and remedying software vulnerabilities and system misconfigurations that could place those systems at risk to viruses and worm infestations, or allow attackers to exploit weaknesses by infiltrating servers and desktops that aren't properly locked down.

Manual vulnerability management and patching couldn't keep up

Allin and his team first wanted to streamline the heavy manual processes, and lack of centralized control, associated with having each server assessed and patched by hand. "It was our recognition that the scale of our environment had grown beyond the point where our labor-intensive and informal approaches were going to work," says Allin. For instance, with each group of servers and end-points, Allin and his security team had little visibility into patch-level status remediation efforts, let alone be able to automatically validate that administrators had updated each system properly. "From our point of view, computer systems are as critical as the lights around here on a winter's day. If you walk into the office and the computer doesn't work, you might as well walk back out and go home," he says.

When the EPO evaluated different approaches and vendor tools that could be used to automate its vulnerability management processes, only one seemed to provide every capability that EPO sought. "We tried a number of approaches to vulnerability scanning. But when we piloted QualysGuard, it just worked. And, because of Qualys' service model, it works with no overhead efforts from us. We don't have to manage a server, vulnerability updates, or any other hassles," says Allin. "From our perspective, this was the most accurate, easiest way to manage vulnerabilities."

With QualysGuard Enterprise's wide-ranging reporting, EPO's security managers now can automatically monitor the organization's vulnerability management process, track remediation, and ensure the highest levels of security. With its comprehensive vulnerability KnowledgeBase, which consists of thousands of unique checks, and a Six-Sigma accuracy rate, QualysGuard provided the exacting precision EPO required. Now, EPO has attained streamlined control of its vulnerability management life cycle: asset discovery, vulnerability assessments, and tracking of security fixes. "Through QualysGuard we were able to rapidly identify where we had patch deficiencies, and identify where we had configuration issues. We even saw where we had firewall issues—and that we should lock a few things tighter. Our introduction to Qualys proved it to be very effective."

“We tried a number of approaches to vulnerability scanning. But when we piloted QualysGuard, it just worked. And, because of Qualys' service model, it works with no overhead efforts from us. We don't have to manage a server, vulnerability updates, or any other hassles.”

David Allin, Director of Planning,
Security, and Inventory
European Patent Office

Centralized Management Total Visibility: Vulnerability and Security Event Correlation

Today, utilizing QualysGuard, EPO conducts a full vulnerability assessment every evening to analyze the security status of both its internal and Internet facing systems. QualysGuard's distributed architecture enables Allin and his security team to centrally manage all of the organization's vulnerability assessments, as well as facilitate administrators from each of its business units to assess the systems they manage. "QualysGuard has made it possible for us to establish an efficient scanning regime in collaboration with our various business units. In this way, we're able to regularly scan and quickly identify any trouble spots, and analyze security trends across our entire enterprise," he says.

Not only has QualysGuard streamlined and dramatically improved EPO's ability to identify and remedy any at-risk systems, the deep insight QualysGuard provides into EPO's infrastructure is now being integrated within its security event management system from ArcSight. While ArcSight provides EPO security information from within its routers, firewall and system logs, password stores, and network traffic, QualysGuard is giving the system the intelligence it needs regarding the current configuration and patch status of EPO's entire infrastructure. Now, on any given day, Allin and his security team know whether or not fast-moving Internet threats actually pose a risk to their systems based on security configurations, the defenses they have in place, and overall organization risk posture. "By enhancing the information within our security event manager with the configuration and vulnerability status provided by QualysGuard, we get transparency into our security posture that wouldn't otherwise be possible," he says.

Through daily automated vulnerability assessments, centralized management, and the correlation of real-time security events with the accurate vulnerability information provided by QualysGuard, EPO is now well positioned to rapidly identify any risks posed against its systems—and quickly remedy any security concerns. "Our target is to get critical patches on our systems within days. We're just not prepared to run any unnecessary risks," says Allin. "Now, with much credit to QualysGuard, we don't have to."

EPO SCOPE & SIZE

32 European nations, including every member state of the European Union. 6,500 employees

BUSINESS

Grants European patents for the contracting states to the European Patent Convention.

BUSINESS PROBLEM

As the EPO expanded the use of IT systems to digitize the patent application acceptance process, as well as open more than one hundred databases to public search, security managers found that manual, time-consuming vulnerability assessment processes failed to provide the high levels of security the EPO demanded.

OPERATIONAL HURDLE

Manual vulnerability scans lacked visibility into CIGNA's infrastructure, and failed to easily identify servers and vulnerabilities that jeopardized security and compliance efforts.

SOLUTION

QualysGuard Enterprise

WHY EPO CHOSE QUALYS

- **Low Total Cost of Ownership:** On-demand technology offers significant economic advantages with no capital expenditures, extra human resources, or infrastructure to deploy and manage.
- **Extremely accurate and up-to-date:** With more than 5,000 unique security checks, QualysGuard has the largest KnowledgeBase of vulnerability signatures in the industry, and performs more than 150 million IP audits per year with 99.999% accuracy.
- **Scalable:** Can deploy and expand rapidly, using QualysGuard's distributed scanning and on-demand architecture.



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

