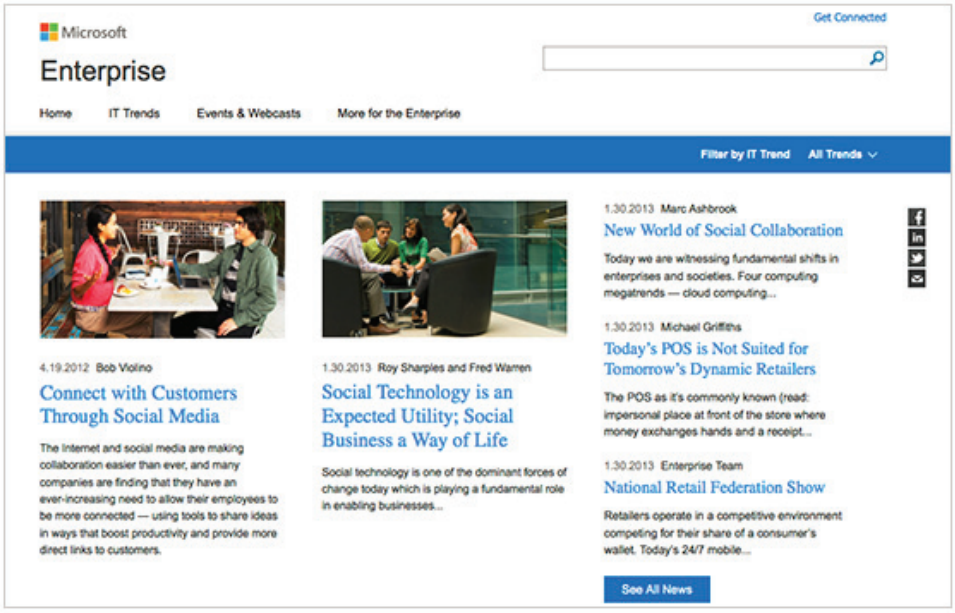
Reigning in Global Web Application Security Risk

The Microsoft Information Security & Risk Management (ISRM) Team needed a way to efficiently evaluate the security of hundreds of web applications that come online every year through its subsidiaries around the world. QualysGuard Web Application Scanning solved their problem.



Microsoft

www.microsoft.com

INDUSTRY: Technology

BUSINESS: Part of Microsoft Information Technology organization, the Microsoft ISRM Team performs application and IT infrastructure security consulting and assessments.

SCOPE: Global

SIZE: 90,000 employees

BUSINESS CHALLENGE: Assess the security of thousands of web applications put into use annually by Microsoft's subsidiaries around the world.

SOLUTION:
QualysGuard Web Application Scanning (WAS)

WHY THEY CHOSE QUALYSGUARD:

- QualysGuard WAS proven more accurate than other web application scanners.
- Comprehensive reports provide the actionable information needed to remedy software flaws.
- A highly accurate, extensive database of security checks that is constantly updated.
- QualysGuard WAS was the easiest web application scanner to use.

Application development moves quickly today, and it's easy to make mistakes. So, while many programming mistakes lead to a poor user experience, or perhaps latency and availability issues – which are serious enough – many other types of mistakes, such as unchecked inputs, allowing for poorly structured queries, and other common programming errors, can lead to serious security vulnerabilities that, if not caught and remedied, can lead to significant data loss.

Consider the findings of the Verizon 2012 Data Breach Investigations Report, which found that a staggering 54% of all attacks on large organizations come through web applications. Unfortunately, finding web application flaws is as challenging as it is difficult – especially if development, quality assurance, security or audit teams lack the right toolsets.

Of course, none of this is new to the Microsoft ISRM Team, which plays an important role within the Microsoft Information Technology department at the $70 billion software maker. As part of its duties, ISRM performs application and IT infrastructure security consulting and assessments, which includes assessing the security of thousands of web applications that help to drive their many subsidiaries around the world. While these web applications do not support an IT line of business, their security is vital.

Challenges Faced

There are a number of challenges that ISRM faces when it comes to keeping these applications secure. First, some are developed by third-party organizations, and they often are in service only for very short timespans, perhaps 30 or 60 days, to support a special event or other transient need. “Our application assessment processes were designed to be implemented and conducted against ongoing line of business applications. The assumption was that these applications would be available for significant periods,” explains Ahmad Mahdi, ISRM Manager at Microsoft.

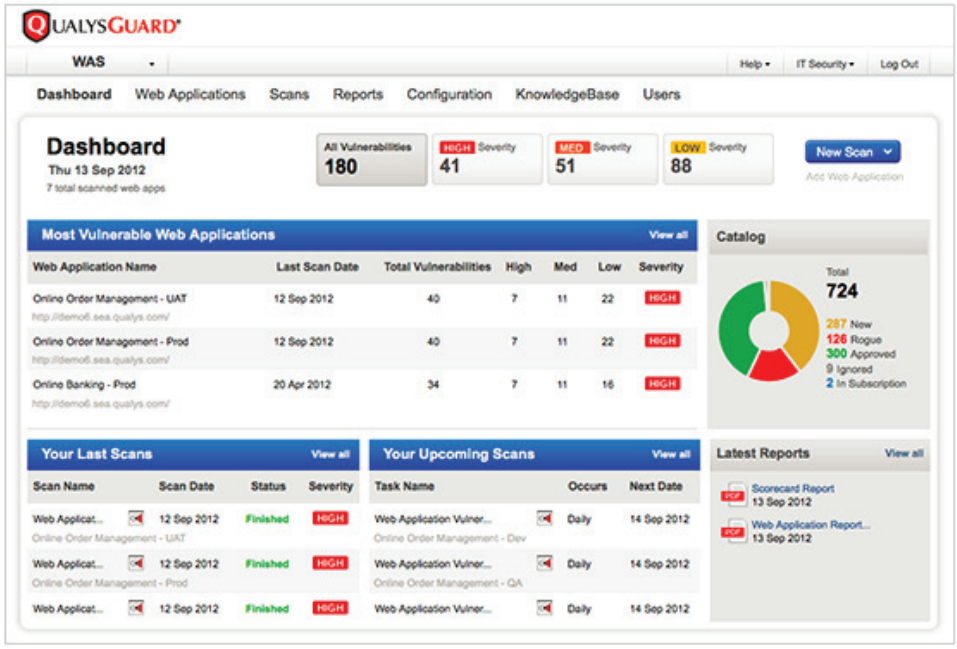
Additionally, the software security evaluation tools in place to assess these applications couldn’t be automated or scaled to meet the sheer number of applications in such short periods. “We needed a comprehensive way to evaluate the security of these applications with speed and accuracy,” says Mahdi.

ISRM began evaluating the leading web application security tools in the market. The solution they would eventually choose needed to be able to assess thousands of applications annually and strong enough to handle significant demands for assessments as needs spike during busier periods. Also, the web application vulnerability assessment results needed to be accurate, with low rates of false positives and false negatives. “We also required it to be easy to configure and use, so that our efforts could be streamlined. Comprehensive reporting was also essential,” Mahdi says.

> “We found QualysGuard WAS ideal for our need to assess thousands of web sites with limited resources.”
>
> **Ahmad Mahdi**,
> infrastructure security team manager at Microsoft

High Volume Scanning with Automated Workflow and Low False-Positive Rate

The team evaluated the web application assessment tools by scanning roughly 200 separate applications over a period of 90 days. Following completion of the tests, the ideal choice turned out to be QualysGuard Web Application Scanning (WAS) from Qualys Inc. “We concluded this for a number of reasons. First, QualysGuard WAS best met our criteria to perform the high volume of scans without a requirement to purchase additional licenses,” he says.



Built on Qualys’ powerful Cloud Platform, QualysGuard WAS provides unsurpassed web application security by leveraging the power and scalability of cloud computing to drive accurate web application security assessments and improve application security and resiliency. QualysGuard WAS identifies web application vulnerabilities in the OWASP Top Ten such

as SQL injection, cross-site scripting, URL redirection, and many other vulnerabilities. It also simplifies and reduces the costs associated with web application scanning with its intuitive, easy-to-use automated workflow, an extremely low false-positive rate, and a rich dynamic user interface.

“The quality of QualysGuard WAS is maintained across many different types of applications. It proves to be very thorough and accurate as well as easy to configure and use,” Mahdi says. Finally, Mahdi appreciated the comprehensive, detailed reports provided by QualysGuard WAS. These would be the reports his team would provide to the web application developers to address the vulnerabilities discovered.

Today, hundreds of web applications deployed by subsidiaries every year are assessed with QualysGuard WAS, identifying common web software vulnerabilities and significantly improving the security posture for Microsoft. “Thanks largely to QualysGuard WAS, we now have a process that ensures applications meet a specific and very important security threshold.” Mahdi says.

In the near future, Microsoft would like to be able to make QualysGuard WAS broadly available to more of its business users, so that many necessary assessments are performed using a streamlined standard process. “We plan to accomplish this goal with a simple web-based application using the very flexible QualysGuard WAS application programming interface, and providing configuration options for the businesses to check the security of their own applications,” says Mahdi. “We found QualysGuard WAS well-suited for our need to assess thousands of web sites using limited resources.”