



February 13, 2017

## Qualys Brings Web Application Security Automation to a New Level by Offering Unprecedented Scalability and One-Click Patching Capabilities

**Seamless integration of Web Application Scanning (WAS) 5.0 with Web Application Firewall (WAF) 2.0 uniquely brings scalable scanning, reduction of false-positives and one-click patching to web apps, including mobile apps and IoT services**

SAN FRANCISCO, CA -- (Marketwired) -- 02/13/17 -- **RSA Conference USA 2017, Booth #N3817** -- [Qualys, Inc.](http://Qualys.Inc) (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced new functionality in its web application security offerings, including scalable fast scanning, detection and patching of websites, mobile applications and Application Programming Interfaces (APIs) in one unified platform. New features in Qualys Web Application Scanning (WAS) 5.0 and Web Application Firewall (WAF) 2.0 allow customers to scan thousands of web applications and APIs using WAS 5.0, deploy one-click virtual patches for detected vulnerabilities using WAF 2.0 and manage it all from a centralized self-updating cloud platform.

**Qualys will showcase this enhanced functionality during RSA Conference USA 2017 at booth #N3817.**

Web application security is complex due to the continuously evolving threat landscape, the diverse nature of web, mobile and Internet of Things (IoT) applications and the broad range of systems needed to manage security across them. Qualys is addressing this complexity by extending automated web application vulnerability scanning to APIs, and adding increased WAF customization capabilities, simplified controls and stronger security rules.

Customers can now use one cloud platform to programmatically scale rapid scanning and patching of web application vulnerabilities across browser-based, mobile and IoT services, then simulate attacks to verify protection. This agile solution will also empower DevOps teams to make web application security an integral part of their processes, so they can detect and patch vulnerabilities early on in the development cycle, avoiding costly security issues in production.

"We use Qualys WAS to scan and secure all our web applications on a continuous basis, and we are pleased with the speed and accuracy of the service," said David Cook, Chief Security Officer at Jive Software. "We are excited about the Qualys WAF that will allow us to act quickly and respond to threats by using the one-click virtual patching feature to remediate active vulnerabilities."

"Digital transformation is driving global enterprises to retool and expand the reach of their web applications to power the mobile and IoT revolution, hence introducing more challenges to identify and secure them on a global scale," said Philippe Courtot, chairman and CEO, Qualys, Inc. "Qualys' seamless integration of WAS 5.0 and WAF 2.0 gives security teams a powerful, scalable and cost-effective solution to detect, scan and secure thousands of web apps and IoT services continuously."

WAS 5.0 offers:

- | **Programmatic scanning of SOAP and REST-based APIs** - In addition to scanning Simple Object Access Protocol (SOAP) APIs, Qualys WAS architecture now allows testing of REpresentational State Transfer (REST) API services. Users need only provide the service locations in the Qualys WAS user interface and the scanner will test for common application security flaws.
- | **IoT and mobile app backend scanning** - With SOAP and REST API scanning capabilities, WAS can now test IOT services and mobile apps as well as API-based business-to-business connectors for security flaws with the precision and scale of the Qualys Cloud Platform.
- | **Unprecedented scalability with parallelization of scanning resources** - WAS now automatically load-balances scanning of multiple applications across a pool of scanner appliances to complete the scan efficiently. This means less idle time for the scanning appliances, with greater coverage.
- | **Increased coverage** - Improvements to Progressive Scanning to allow for customers to scan very large sites, one slice at a time, in order to cover large applications that are problematic to scan in a short window.

WAF 2.0 offers:

- | **One-click Virtual Patching** - Integrated into Qualys' WAF and WAS solutions, the one-click virtual patching feature addresses both false-positives and the inability to quickly patch vulnerabilities. First, Qualys WAS identifies critical vulnerabilities in web apps, then Qualys WAF allows security teams to virtually patch these vulnerabilities with one-click, and block targeted attacks. This integrated process empowers security teams to quickly protect web apps and minimizes false-positives.
- | **Out-of-the-box security templates for popular platforms** - Included Wordpress, Joomla, Drupal and Outlook Web Application templates are based on the latest Qualys security intelligence, offer fully customizable security policies and make it easy to continuously monitor business-critical web applications.
- | **Ease of Use and flexible deployment** - WAF is available on VMWare, Hyper-V and Amazon Web Services, and includes load-balancing of web servers, health checks for business-critical web applications, custom security rules based on HTTP request attributes, reusable Secure Socket Layer profiles, detailed event log information and centralized WAF management.

### **Availability**

Qualys WAS 5.0 and WAF 2.0 are available now as annual subscriptions. Pricing is as follows, based on the number of web applications and virtual appliances:

#### Web Application Scanning

- | Starting at \$1,695 for small businesses
- | Starting at \$2,495 for larger enterprises

#### Web Application Firewall

- | Starting at \$1,995 for small businesses
- | Starting at \$9,995 for larger enterprises

### **Additional Resources:**

- | Follow Qualys on [LinkedIn](#) and [Twitter](#)  
Read more about [Qualys Web Application Scanning](#)  
Read more about the [Qualys Web Application Firewall](#)
- | Register for a [free trial](#)

### **About Qualys**

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL Technologies, HP Enterprise, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit [www.qualys.com](http://www.qualys.com).

Qualys, the Qualys logo and QualysGuard are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

### **QUALYS MEDIA CONTACT**

David Conner  
Qualys, Inc.  
[dconner@qualys.com](mailto:dconner@qualys.com)  
650-801-6196

Source: Qualys

News Provided by Acquire Media