



April 21, 2015

Qualys Introduces End-to-End Web Application Security Cloud Service

Qualys Web Application Firewall Version 2.0 Includes Virtual Patching and Event Response Capabilities, Along with Tight Integration of Qualys WAS; Enables Organizations to Efficiently Address Web Application Security

SAN FRANCISCO, CA -- (Marketwired) -- 04/21/15 -- **RSA Conference USA 2015, Booth #N3421** -- [Qualys, Inc.](#) (NASDAQ: QLYS), a pioneer and leading provider of cloud security and compliance solutions, today announced the availability of [Qualys Web Application Firewall](#) (WAF) version 2.0 that comes fully integrated with the [Qualys Web Application Scanning solution](#) (WAS). The new release includes virtual patching capabilities to enable organizations to fine-tune security policies, remove false positives and customize rules leveraging vulnerability data from the Qualys WAS. Qualys WAF also includes customizable event response, helping customers evaluate and create exceptions to web events to better prioritize and mitigate vulnerabilities, making it one of the first end-to-end web application security services to combine WAF security rules and policies with WAS data to address web application security threats.

"While web application firewall solutions have long been deemed too complex to set up and manage, today's vendors have made significant investments in product development to simplify and automate WAF functionality," said Chris Rodriguez, senior industry analyst, Frost & Sullivan. "Qualys' ability to provide an end-to-end solution that combines web application scanning and web application firewall to effectively to detect and mitigate vulnerabilities is a strong value proposition and is in alignment with where we believe the WAF market is heading."

As hackers continue to find new ways to penetrate web applications, WAFs can detect, alert and block known attacks. With the latest version of Qualys WAF, users can now create "virtual patch" rules in direct response to their Qualys WAS findings, to enable rapid false positive resolution, as well as customization of security rules tailored for the organization's environment. This helps customers better tune security policies, quickly remove false positives, and easily customize WAF security rules for web applications.

Qualys Web Application Firewall is a next-generation cloud service that brings an unparalleled combination of scalability and simplicity to web app security. Its automated, adaptive approach provides organizations with the following:

- **Easy, set-up.** Qualys WAF is deployed as a virtual image alongside web applications. It can be set up and configured in minutes, requiring no equipment or admin resources or dedicated security staff to get set up and running.
- **Real-time application defense and hardening.** Qualys WAF blocks attacks against websites in real time. The service provides a shield around coding defects, application framework flaws, web server bugs, and improper configurations.
- **Seamless, automatic updates, increasing security over time.** Running on the Qualys Cloud Platform, the WAF service is updated automatically with new defenses from the Qualys research team, and the defense is activated intelligently according to specified policies -- all without disrupting the websites or site visitors.
- **Centralized Cloud Management.** Delivered via the Qualys Cloud Platform, WAF can be centrally managed from anywhere in the world via the Qualys console. It provides a clear dashboard showing timelines and geo-location graphs of events. The cloud platform also provides maximum efficiency by security events from all customers, with immediate rules deployment to all WAFs connected to it.

Tight Integration with Qualys Web Application Scanning

Qualys WAS provides customers the ability to continuously discover, catalog and scan web applications on a global scale with a high degree of accuracy. It provides the industry's first continuous progressive scanning capability to scan and monitor thousands of web apps. Qualys WAS crawls and tests web applications for OWASP top 10 risks, SQL injection, Cross-Site Scripting, and web site misconfigurations. By tightly integrating the scan and the firewall, when Qualys WAS identifies a threat or a risk, it can automatically deploy the relevant virtual patch to the Qualys WAF to mitigate associated risks.

Additionally, Qualys WAF monitors all web pages visited by users and automatically shares this information back to the web application scanner, ensuring these pages are not missed during the next scan. Such an approach helps block attacks on web app vulnerabilities, prevent disclosure of sensitive information and control where and when applications are accessed.

"Many organizations are struggling to find a balance between identifying and effectively addressing vulnerabilities fast enough to avoid falling victim to large-scale breaches," said Philippe Courtot, chairman and CEO of Qualys, Inc. "By integrating security rules and policies from our WAF solution with Qualys WAS data, we are providing significant value to our customers with the flexibility and automation needed to tackle web application security threats. It's a giant step towards complete automation of web application security."

Availability

Qualys Web Application Firewall is now available and sold as an annual subscription starting at \$1,995 for small businesses and \$9,995 for larger enterprises based on the number of web applications and virtual appliances. Visit <https://www.qualys.com/WAF> for more pricing and additional information.

Additional Resources

- Register for a [free trial](#) of Qualys Web Application Firewall
- Stop by [Qualys' RSA booth](#) (#3421) for more information
- Product video: <http://youtu.be/7CQ4TAKHB2E>
- Follow Qualys on [LinkedIn](#) and [Twitter](#)

About Qualys, Inc.

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 7,700 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, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA) and Council on CyberSecurity. For more information, please visit 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.

MEDIA CONTACTS

Melissa Liton
Qualys, Inc.
[Email Contact](#)
(650) 801-6242

Michelle Kincaid
LEWIS PR on behalf of Qualys
[Email Contact](#)
(415) 432-2467

Source: Qualys

News Provided by Acquire Media