



February 29, 2016

Qualys Unveils ThreatPROTECT to Empower Organizations With Actionable Threat Intelligence

New Service Correlates Active Threat Information With Vulnerability Data to Help Customers Identify, Prioritize and Remediate Security Threats

SAN FRANCISCO, CA -- (Marketwired) -- 02/29/16 -- **RSA Conference USA 2016, Booth #N3421** -- [Qualys, Inc.](http://Qualys.Inc) (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced the Qualys ThreatPROTECT solution.

Built on the Qualys Cloud Platform, ThreatPROTECT correlates data from vulnerability scans and active threat data from multiple sources into a single dynamic dashboard to provide a holistic and contextual view of an organization's threat exposure. With ThreatPROTECT, customers can visualize, prioritize and take action to minimize exposure from vulnerabilities related to the threats that matter most.

Not all Common Vulnerabilities and Exposures (CVEs) are created equal. According to the 2015 Verizon Data Breach Investigations Report, about half of the CVEs, which were exploited, went from publish to pwn in less than a month, compromising organizational assets. 10 CVEs account for almost 97 percent of exploits, per the report.

Dealing with huge numbers of vulnerabilities remains an issue for most organizations, as fixing every issue can take a considerable amount of time. Chasing the deployment of fixes to every vulnerability results in more critical issues being left unaddressed for longer periods.

Organizations must prioritize remediation efforts to have an immediate and measurable impact on risk reduction. This requires not only accurately identifying vulnerabilities, but also understanding a variety of point-in-time factors that contribute significantly to the overall risk exposure. For example, certain vulnerabilities with publicly available exploits that are actively being leveraged by attackers present greater threat exposure compared to less well-known and automated vulnerabilities. Providing actionable security intelligence with organizational context leads to better countermeasures against the threats that matter most, protecting IT assets against compromises and protecting the organizational brand.

Leveraging vulnerability data collected via Qualys scanners or in real time via the Qualys Cloud Agents, Qualys ThreatPROTECT correlates this data with Real-time Threat Indicators (RTI) from multiple industry sources, providing customers with an easy-to-understand dashboard that provides clear insight into which vulnerabilities to fix first. The dynamic ThreatPROTECT dashboard, with powerful ElasticSearch capabilities, helps customers to rapidly find and prioritize responses to vulnerabilities based on these RTIs according to the level of threat seen in the wild.

RTIs are external data points that enrich and provide context when correlated with vulnerability scan data collected by Qualys. RTIs can be used on a standalone basis or cascaded with each other to prioritize efforts for patching, or to select compensating controls to reduce exposure when patches are not available. The interactive, dynamic dashboards in Qualys ThreatPROTECT help customers visualize the threat level, which can be combined with additional information about the environment from other modules such as [AssetView™](#). This allows customers to further mine asset information to prioritize remediation to the most important assets with the greatest threat exposure.

"In today's rapidly changing threat landscape, the most effective way for companies to protect themselves is to accurately identify assets, prioritize threats and take action to prevent a compromise," said Philippe Courtot, chairman and CEO for Qualys. "We continue to innovate and leverage our extensible Cloud Architecture to bring solutions like ThreatPROTECT to our customers."

Source of Qualys' Real-time Threat Indicators (RTI)

Qualys gathers RTI information from its own research and from multiple external sources. In its Research Labs, Qualys has a worldwide team of researchers who constantly monitor and track RTI data points. This includes information on attacks, exploits and exploits kits. Qualys researchers also analyze this information to determine additional RTI attributes like Lateral Movement. In addition, Qualys has partnerships with trusted industry sources like Core Security, Exploit Database, Immunity, TrendMicro, VeriSign iDefense and others from which intelligence information is obtained and correlated. Current RTIs provided by the new service include:

<i>RTI</i>	<i>Description</i>
Zero Day	Active attack has been observed in the wild but there is no patch from the vendor.
Exploit Public	Exploit Knowledge is well known and a working exploitation code is publically available. Potential of active attacks is very high.
Actively Attacked	Active attacks have been observed in the wild. If there are no patches, Qualys will mark it as zero day in addition to actively attacked.
High Lateral Movement	After a successful compromise, attacker has high potential to compromise other machines in the network.
Easy Exploit	The attack can be carried out easily and requires little skills or does not require additional information.
High Data Loss	Successful exploitation will result in massive data loss on the host.
Denial of Service	Successful exploitation will result in denial of service.
No Patch	Vendor has not provides an official fix.
Malware	Malware has been associated with this vulnerability.
Exploit Pack	Exploit Pack has been associated with this vulnerability.

Additional Resources

- | Stop by [Qualys' RSA booth](#) (#N3421) for more information
- | Follow Qualys on [LinkedIn](#) and [Twitter](#)

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,800 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, Dell SecureWorks, Fujitsu, HCL Comnet, Infosys, NTT, Optiv, 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.

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 CONTACT

Jennifer McManus-Goode
 LEWIS for Qualys
qualys@teamlewis.com
 (781) 418-2406

Source: Qualys

News Provided by Acquire Media