April 22, 2014

Qualys Releases New SSL Dashboard to Help Customers Globally Audit the Health of Their Certificates

The New QualysGuard SSL Dashboard Provides Comprehensive Checks Including for "Heartbleed"

REDWOOD SHORES, CA -- (Marketwired) -- 04/22/14 -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud security and compliance solutions, today introduced a new SSL Dashboard to its award-winning QualysGuard Vulnerability Management (VM) solution. This new console provides organizations with global discovery of SSL certificates, including issue date, signature, fingerprint information and new Heartbleed filters that identify SSL certificates from vulnerable hosts.

This month's Heartbleed bug awakened the world to the importance of a healthy SSL public key infrastructure to the proper functioning of the Internet. Yet, despite the continued high growth in SSL traffic, organizations often leave life-cycle management of SSL certificates to spreadsheets, which are labor intensive and error prone, or standalone software solutions, which must be deployed and managed. This creates the risk of a security breach or of a poor customer experience when invalid, expired or otherwise faulty certificates remain in use.

"As our web presence grew organically, we risked losing visibility into the health of our SSL certificate base," said Jonathan Trull, CISO, State of Colorado. "Qualys' ability to bring all SSL data into a single place makes it easy for us to take control and efficiently manage the certificate lifecycle."

"It is time for companies to mature the management of their SSL assets," said Pete Lindstrom, Research Director, IDC. "At a minimum, problems with certificates create a corporate reputation issue as customers encounter security warnings, but poor certificate management can also lead to real security exposure as we have seen in the ongoing response to Heartbleed."

Because Qualys stores and indexes a customer's scan results in its cloud platform, there is no need to re-scan networks specifically to collect SSL data. The dashboard provides the following capabilities:

- Drill-down charts that summarize statistics about expired or soon-to-expire certificates, top 10 certificate authorities (CA), certificate by key size and self-signed certificates;
- Detailed reports that can be filtered on multiple criteria including issue and expiration dates, key size, host name, validity, self-signed certificates and certificates at risk due to Heartbleed;
- The ability to create charts and reports specific to customer-defined asset groups;
- Access to specific information about each certificate including validity dates, IP address and host, issuer and certificate path, key size, fingerprint, raw certificate data and associated vulnerabilities, including their severity;
- Ability to export data in CSV, XML and other formats.

In addition, customers subscribing to the QualysGuard Continuous Monitoring (CM) service can set up alerts based on SSL certificate information, such as expired/days until expiration, self-signed certificates, name of Certificate Authority, weak key size and other validity measures.

"The SSL public key infrastructure underpins the security of internet traffic and e-commerce," said Wolfgang Kandek, CTO of Qualys. "We developed the SSL Dashboard to help our customers scale and automate the security management of this core component of their growing web infrastructure."

Please visit www.qualys.com/heartbleed/ for more information on how to use the new dashboard to help identify certificates that should be revoked because of Heartbleed.

Upcoming Webinar on Heartbleed Recovery

On Thursday, April 24, 2014 at 10 AM PDT, Qualys will host a webcast entitled "A Post-Mortem on Heartbleed -- What Worked and What Didn't," featuring Qualys CTO Wolfgang Kandek and State of Colorado CISO Jonathan Trull, and will cover the Heartbleed bug, recovery strategies and how the State of Colorado responded to this critical vulnerability. Those interested can register at www.qualys.com/heartbleedwebcast/.

About QualysGuard Cloud Platform

The QualysGuard Cloud Platform and its integrated suite of security and compliance solutions help provide organizations of all sizes with a global view of their security and compliance posture, while reducing their total cost of ownership. The QualysGuard Cloud Suite, which includes Vulnerability Management, Continuous Monitoring, Web Application Scanning, Malware Detection Service, Web Application Firewall, Policy Compliance, PCI Compliance, Questionnaire and Qualys SECURE Seal, enables customers to automatically identify their IT assets, collect and analyze large amounts of IT security data, discover and prioritize vulnerabilities and malware, recommend remediation actions and verify the implementation of such actions.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 6,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The QualysGuard 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 Accuvant, BT, Dell SecureWorks, Fujitsu, NTT, Symantec, Verizon, and Wipro. The company is also a founding member of the CloudSecurityAlliance (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.

Source: Qualys

News Provided by Acquire Media