February 25, 2014

Qualys Introduces Groundbreaking Continuous Monitoring Cloud Service for Global Perimeters

New Paradigm for Vulnerability Management Alerts Companies About Threats Before They Turn Into Breaches

SAN FRANCISCO, CA -- (Marketwired) -- 02/25/14 -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud security and compliance solutions, today introduced Continuous Monitoring, the most recent addition to its QualysGuard Cloud Platform. This new offering gives organizations the ability to proactively identify threats and unexpected changes in Internet-facing devices within their DMZ, cloud-based environments, and web applications, before they are breached by attackers. It brings a new paradigm to vulnerability management, empowering customers to continuously monitor mission-critical assets throughout their perimeter and immediately get alerted to anomalies that could expose them to cyber attacks.

"At Ancestry.com, we have millions of visitors per month and many perimeter devices that we operate to secure against possible attacks," said Deal Daly, VP of information technology for Ancestry.com. "The Qualys Continuous Monitoring service delivers real-time alerts of security and network configuration issues that we can proactively remediate."

Built on the QualysGuard Cloud Platform used by the majority of the Fortune 1000 and thousands of companies around the world, this new service allows companies to continuously monitor:

- ***Hosts and devices exposed to the Internet*** - to see whenever systems appear, disappear, or are running unexpected operating systems.
- ***Digital certificates*** - to track SSL certificates used on systems to know if they are weak or self-signed, and when they're due to expire.
- ***Ports and services open on each system*** - to keep tabs on which network ports are open, which protocols are used, and whether they change over time.
- ***Vulnerabilities on hosts or applications*** - to know when vulnerabilities appear (or reappear), whether they can be exploited, and if patches are available.
- ***Applications installed on perimeter systems*** - to find out when application software gets installed or removed from these systems.

When Continuous Monitoring detects changes in the perimeter that could lead to exploitation, it alerts the responsible IT staff assigned to these assets to take the appropriate mitigation measures. The immediate notification provided by Continuous Monitoring frees security teams from the delays and burdens of waiting for scheduled scanning windows and sifting through reports.

"The Cloud is expanding the boundaries of the corporate perimeter to include every browser, device or application that touches the Internet, leaving us more exposed to cyber attacks than ever," said Philippe Courtot, chairman and CEO for Qualys. "With our groundbreaking Continuous Monitoring service, companies can see their perimeter the way today's hackers do, so that threats can be identified and addressed before they turn into breaches."

In the MarketScope for Vulnerability Assessments, Gartner Analyst Kelly Kavanagh noted "Gartner's vulnerability management life cycle activities include the secure configuration of IT assets, regular assessment of vulnerabilities and compliance with security configuration policies, remediation of vulnerabilities or security configuration issues, and ongoing monitoring to detect malicious events or activities. The use of VA products or services as a best practice has been incorporated into a number of prescriptive compliance regimes, including the PCI DSS, the U.S. Federal Information Security Management Act (FISMA) and desktop configuration requirements. In particular, the National Institute of Standards and Technology (NIST) 800-53 requirements for 'continuous monitoring' serve as an accelerator for the frequency of VA use."(1)

Availability
QualysGuard Continuous Monitoring is available immediately in Beta for all customers. General availability is scheduled for March 27, 2014. It is sold as annual subscriptions based on the numbers of perimeter IP addresses being monitored, starting at $295 for small businesses and $1,995 for larger enterprises. The first version of the service encompasses continuous

monitoring of networked devices and the next releases will include monitoring of web applications.

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, 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.

(1) Gartner: MarketScope for Vulnerability Assessment, published September 9, 2013.

Source: Qualys

News Provided by Acquire Media