



July 29, 2014

Qualys Bolsters Continuous Monitoring for Proactive Enterprise Incident Response

New Features Provide the Most Comprehensive View of the Perimeter and Seamless Integration of Alerts With Incident Response Systems

REDWOOD CITY, CA -- (Marketwired) -- 07/29/14 -- [Qualys, Inc.](#) (NASDAQ: QLYS), a pioneer and leading provider of cloud security and compliance solutions, today announced it has further bolstered its industry-leading cloud service [Qualys Continuous Monitoring \(CM\)](#). The latest features include automated alerts for changes in perimeter IP addresses, as well as a new API interface that enables integration of alerts into incident response systems and SIEMs such as Splunk and HP ArcSight. The new features and functionality provide organizations with the most comprehensive view of their security perimeters, while empowering them to proactively identify and address potential threats.

Organizations' perimeters today are very distributed, complex and highly dynamic. There are often various operational teams managing firewalls, load balancers, systems, applications and databases, making frequent changes to a network environment independent of one another. Perimeter scanning and response to unintentional security holes created by these changes is often event-driven and only performed at designated times, rather than on a continuous, always-on basis. This presents a significant opportunity for cybercriminals to exploit newly introduced vulnerabilities and infiltrate corporate networks in between scans.

"In an era of continuous compromise, enterprises need to shift from a mindset of 'incident response' -- wherein incidents are thought of as occasional, one-off events -- to a mindset of continuous response -- wherein attacks are relentless, hackers' ability to penetrate systems and information is never fully blocked, and systems must be assumed to be continuously compromised, and this, they must be continuously monitored," said Neil MacDonald, Vice President and Distinguished Analyst for Gartner.

Qualys Continuous Monitoring provides organizations with a comprehensive, always-on view of potential security holes, enabling organizations to immediately identify and proactively address potential threats before they turn into breaches. Built on the [Qualys Cloud Platform](#) used by Fortune 1000 and organizations around the globe, Continuous Monitoring uses its elastic scanning capacity to dynamically scale to continuously scan networks of any size and scope, and instantly provide alerts as soon as an unauthorized change is detected.

"More and more customers are asking us to help them address 'toxic combination' type scenarios that can lead to compromises in their IT environments. An example of this could be a server that exhibits a combination of configurations or vulnerabilities that can make it susceptible to attacks," said Philippe Courtot, Chairman and CEO of Qualys. "Combining a continuous security approach that integrates alerts into the incident response system, enables customers to quickly address potential toxic combinations by alerting them when a critical change suddenly appears in their environment. These alerts help to direct the information to the hands of first responders so they can immediately address and mitigate risk within their global perimeter."

Qualys Continuous Monitoring now includes:

- **Integration with Leading SIEM Providers** - a new extensible API interface incorporates alerts into incident response and monitoring systems via integrations with leading security incident and event management (SIEM) platforms, including Splunk and HP ArcSight
- **Common Event Format (CEF) Support** - use CEF format to send events into all popular SIEM and incident response products and get email alerts delivered directly to the inbox

In addition, Qualys Continuous Monitoring allows businesses to continuously monitor and respond to any of these combinations:

- **New Hosts** - to see whenever systems appear, disappear, or are running unexpected operating systems
- **OS Changes on Existing Hosts** - to see when changes have been made to operating systems on systems
- **Open Ports/Services** - to keep tabs on network ports including newly opened ports, changes to ports, new services on ports, and closing of ports

- **SSL Certificates** - to track SSL certificates used on systems including expired, soon-to-expire, rogue or unknown certificates
- **Vulnerabilities Changes** - to know when there are changes in vulnerabilities including new, re-opened and closed instances
- **Software Changes** - such as installation of new software, upgrades or downgrades of existing software, and removals

Availability

Qualys Continuous Monitoring is available immediately and sold via annual subscription, based on the number of perimeter IPs. To learn more about Continuous Monitoring or see a demo, visit <https://www.qualys.com/enterprises/qualysguard/continuous-monitoring/>. Qualys will also demo Continuous Monitoring at [Black Hat USA 2014](#) in Las Vegas, Nevada from August 5 - 7, 2014.

Additional Resources

- Learn more about [Qualys Continuous Monitoring](#)
- Register for a [demo](#) of Qualys Continuous Monitoring
- Visit the Qualys expo booth (#211) at [Black Hat USA 2014](#)
- Follow Qualys on [Facebook](#) and [Twitter](#)

About Qualys, Inc.

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 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 and the Qualys logo 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