February 13, 2017

Qualys Introduces Two New Disruptive Services at RSA Conference USA 2017

New File Integrity Monitoring (FIM) service based on Qualys Cloud Agent enables organizations to increase visibility and security while removing point-product agents from their endpoints; New Indicators of Compromise (IOC) service provides continuous detection of compromised IT assets across endpoints, on-premise or elastic cloud environments

SAN FRANCISCO, CA -- (Marketwired) -- 02/13/17 -- ***RSA Conference USA 2017, Booth #N3817*** -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced a major expansion of its Qualys Cloud Platform which helps organizations continue to reduce the complexity and cost of security and compliance. New services include File Integrity Monitoring (FIM) and Indicators of Compromise (IOC) detection solutions that enable customers to consolidate even more critical security and compliance functions into a single cloud-based dashboard, and remove the point-solution sprawl that proliferates across their endpoints.

Qualys will showcase these new services during RSA Conference USA 2017 at booth #N3817.

Qualys now combines a comprehensive set of both prevention and detection solutions in the same lightweight Qualys Cloud Agent already deployed for an organization's global asset inventory, vulnerability management, and policy compliance programs. With Qualys FIM and IOC, customers can instantly add continuous visibility of breaches and system changes to their single-pane view of security and compliance posture already powered by the Cloud Agent.

"With FIM and IOC, Qualys has grown its platform capabilities to provide a comprehensive Security and Vulnerability Management offering that now provides breach detection, policy and compliance context, vulnerability information, and ultimately, a comprehensive view of enterprise risk management," said Robert Ayoub, Research Director, Security Products, IDC. "The Qualys Cloud Platform can simplify the complexity associated with managing multiple security solutions, while at the same time increasing the automation, effectiveness and proactive nature of security."

Qualys File Integrity Monitoring (FIM) - Qualys FIM logs and centrally tracks file change events across global IT systems, delivering users a single-view dashboard from which to detect and identify critical changes, incidents, and audit risks resulting from normal patching and administrative tasks, change control exceptions or violations, or malicious activity. As a cloud-based solution, Qualys FIM scales visibility and control to a variety of enterprise operating systems without the need to deploy and maintain complex security infrastructure. This allows teams to improve compliance, reduce downtime and limit damage resulting from compromise without the expense of a software-based solution. File Integrity Monitoring offers:

- ***Preconfigured content:*** Deciding what to monitor is a challenge for most security teams, so FIM comes with out-of-the-box profiles based on industry best practices and vendor-recommended guidelines for common compliance and audit requirements, including PCI mandates.
- ***Real-time change engine:*** The Qualys Cloud Agent continuously monitors the files and directories specified in the monitoring profile and captures critical data to identify what changed along with environment details such as which user and process was involved.
- ***Automated change review:*** Qualys FIM provides review workflows and points for external integration to reduce the data users have to look at so they can focus on critical changes and violations first.

Qualys Indicators of Compromise (IOC) - Qualys IOC continuously monitors endpoint activity to detect suspicious activity that may indicate the presence of known malware, unknown variants, and threat actor activity on devices both on and off the network. Qualys IOC integrates endpoint detection, behavioral malware analysis, and threat hunting techniques that incorporate a continuous view of an asset's vulnerability posture along with suspicious activity monitoring. Indicators of Compromise offers:

- ***Continuous event collection:*** Qualys IOC uses the Cloud Agent's non-intrusive data collection and delta processing techniques to transparently capture endpoint activity information from assets on and off the network in a way that is more performant than other solutions' query-based approaches or distributed data collectors.
- ***Highly scalable detection processing:*** Analysis, hunting, and threat indicator processing is performed in the cloud on billions of active and past endpoint events. Those results are then coupled with threat intelligence data from Qualys Malware Labs and third-party threat intelligence sources to identify malware infections (indicators of compromise) and threat actor actions (indicators of activity).

- ***Actionable intelligence for security analysts:*** Confidence-scored alerts are displayed in the Qualys platform's web-based user interface with contextual asset tags to help security teams prioritize responses for critical business systems.

"Breaches continue to rise despite the investments in traditional mechanisms that organizations have deployed to support their businesses in the new era of digital transformation," said Philippe Courtot, chairman and CEO, Qualys, Inc. "Our new disruptive services for FIM and IOC extend the capabilities of our Cloud Agent platform, allowing companies to get the visibility and prevention they need against cyber threats from one single platform, drastically reducing their security costs."

Qualys FIM and IOC provide significant benefits to security administrators -- as delivered by the Qualys Cloud Agent and cloud-based processing platform -- over traditional on-premise point security solutions:

- ***Easy setup and no maintenance:*** FIM and IOC modules operate on endpoints via the lightweight Qualys Cloud Agent. Modules can be instantly activated across any or all assets without reinstalling the agent or rebooting the endpoint.
- ***Minimal performance impact:*** The Cloud Agent minimizes performance impact on the endpoint by simply monitoring for file changes and system activity locally, sending all data to the Qualys Cloud Platform for storage, correlation, analysis, and reporting.
- ***Unified security posture:*** Qualys presents FIM and IOC alert data for on-premise assets, cloud server instances, and off-net remote endpoints in a single view that is integrated with the asset's inventory, vulnerability posture, and policy compliance controls, even for assets that are currently offline -- thus significantly reducing the time required to effectively detect and respond to threats before breach or compromise can occur.
- ***Integration with AssetView:*** Security analysts can make use of dynamic dashboards, interactive and saved searches, and visual widgets in Qualys AssetView to monitor changes within the context of asset groups.

Availability

Qualys FIM and IOC will both be available in limited beta starting in March.

Additional Resources:

- Follow Qualys on LinkedIn and Twitter
- Read more about the Qualys Cloud Agent
- Visit Qualys at RSA Conference USA Booth N3817

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 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, Deutsche Telekom, Fujitsu, HCL Technologies, HP Enterprise, Infosys, NTT, Optiv, SecureWorks, 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 MEDIA CONTACT

David Conner
Qualys, Inc.
dconner@qualys.com
650-801-6196

Source: Qualys

News Provided by Acquire Media