Qualys Releases Highly Scalable IOC Cloud App Providing 2-Second Visibility of Compromised Assets and Threat Hunting Capabilities

New extension to Qualys Cloud Platform delivers customers a continuous view of suspicious activity on IT assets, including presence of known malware and other threat actors

REDWOOD CITY, Calif., – October 2, 2017 – Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced the availability of its Indication of Compromise (IOC) Cloud App, a new major expansion to the Qualys Cloud Platform.

Qualys IOC expands the capabilities of the Qualys Cloud Platform to deliver threat hunting, detect suspicious activity, and confirm the presence of known and unknown malware for devices both on and off the network. Leveraging the same Qualys Cloud Agent already deployed for an organization's asset inventory, vulnerability management, and policy compliance programs, Qualys now consolidates even more security functions into a single lightweight agent. This approach allows enterprises to eliminate the challenges with point-solution agent sprawl that proliferates across their endpoints which impacts end-user experience, adds IT management complexity, and is cost prohibitive to operate.

“Threat hunting relies on both advanced threat knowledge and deep knowledge of the organization's IT environment, which will also benefit the organization itself in learning more about its IT environment and finding the places where attackers can hide,” said Anton Chuvakin, VP, Distinguished Analyst, Gartner.[1]

“In the new era of digital business where everything is interconnected, having the continuous visibility to know where and which IT assets have been compromised is essential,” said Philippe Courtot, chairman and CEO, Qualys, Inc. “Our new IOC Cloud App delivers enterprises the 2-second visibility they need to help detect compromised assets across their global IT environments. In addition, with our Cloud Platform they also get the continuous view of their

[1] *Gartner, How to Hunt for Security Threats, Anton Chuvakin, April 2017*

security and compliance posture in a single user interface, significantly reducing the time to respond to threats before any compromise occurs."

Traditional approaches for detecting breach activity, including signature detection, can often allow both known and unknown variants of malware to go undiscovered and unmitigated for months, and are blind to non-malware attacks, leading to costly and damaging breaches. Qualys IOC integrates endpoint detection, behavioral malware analysis, and pre-defined threat hunting techniques that incorporate a continuous view of an asset's vulnerability posture along with suspicious activity monitoring. With Qualys IOC, security analysts and incident responders can correlate endpoint activity with threat intelligence, network alerts, and sandbox analysis to quickly determine exactly when and where a compromise took place.

Qualys IOC provides unique benefits, as delivered by the Qualys Cloud Agent and Qualys Cloud Platform, over traditional enterprise security solutions:

- **Unified agent 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 that is more performant than query-based approaches or log collectors.
- **Highly scalable detection processing:** Threat hunting, suspicious activity detection, and OpenIOC processing is performed in the Qualys Cloud Platform on billions of active and past system events, and coupled with threat intelligence data from Qualys Malware Labs to identify malware infections (indicators of compromise) and threat actor actions (indicators of activity).
- **Actionable intelligence for security analysts:** Customers can use pre-defined threat hunting rules and easily import indicators of compromise artifacts into widgets, dashboards, and saved searches to quickly verify threat intelligence, scale of infections, first-infected asset ("Patient Zero"), and timeline of compromises — even for assets that are currently offline or have been re-imaged by IT.
- **Streamline investigations with a Single View of Asset:** Qualys IOC creates a Single View of the Asset, showing threat hunting details unified with other Qualys Cloud Apps for hardware and software inventory, vulnerability posture, policy compliance controls, and file integrity monitoring change alerts for on-premise servers, cloud instances, and off-net remote endpoints. A single user interface significantly reduces the time required for incident responders and security analysts to hunt, investigate, detect, and respond to threats before breach or compromise can occur.

Availability and Pricing

Qualys IOC Cloud App is generally available to customers today. Pricing is based on the number of assets where the Qualys Cloud Agent is installed, and annual subscriptions start at $2,995.

Planned capabilities in future releases include support for integration of external threat intelligence in open formats (STIX/TAXII, OpenIOC, CybOX); pre-built integrations and apps with leading SIEM, threat intelligence platforms, and security orchestration platforms to automate incident response investigations; a partner and community-developed library of shareable threat hunting rules; and, expanded detection techniques for more malware families, credential stealing, and lateral movements.

Additional Resources:

- Follow Qualys on LinkedIn and Twitter
- Read more about the Qualys IOC Cloud App
- Read more about the Qualys Cloud Agent

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 120 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. Founded in 1999 as one of the first SaaS security companies, 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, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance. For more information, please visit www.qualys.com.

###

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