Qualys Unveils Multi-Vector EDR, a New Approach to Endpoint Detection and Response

July 29, 2020

Groundbreaking app natively built on the Cloud Platform provides context beyond the endpoints that reduces false positives and streamlines threat hunting

FOSTER CITY, Calif., July 29, 2020 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, today announced Qualys Multi-Vector EDR. Taking a new multi-vector approach to Endpoint Detection and Response (EDR), Qualys now brings the unifying power of its highly scalable cloud platform to EDR.

Traditional EDR solutions singularly focus on endpoints' malicious activities to hunt and investigate cyberattacks. Qualys' multi-vector approach provides critical context and full visibility into the entire attack chain to provide a comprehensive, more automated and faster response to protect against attacks.

Multi-Vector EDR enables security teams to unify multiple context vectors like asset and software inventory, end-of-life visibility, vulnerabilities and exploits, misconfigurations, network traffic summary, MITRE ATT&CK tactics and techniques, malware, endpoint telemetry, and network reachability by leveraging the Qualys backend to correlate with threat intelligence for accurate detection, investigation and response – ALL, in a single, cloud-based app with a single lightweight agent.

"Qualys Multi-Vector EDR gives a broader view beyond the endpoint, which is necessary to eliminate false positives and more effectively prevent lateral movement. This is possible because Qualys Multi-Vector EDR is native to the cloud platform and collects vast amounts of telemetry from multiple sensors while capturing network information. The Qualys Cloud Agent, combined with the highly scalable Cloud Platform and forthcoming Incident Response capabilities, offers a unique opportunity for MSSPs to consolidate their managed services technology stack and orchestrate the appropriate response for faster and effective protection," said Vishal Salvi, Chief Information Security Officer at Infosys.

"Qualys Multi-Vector EDR represents a major extension to both the Qualys Cloud Platform and our agent technology," said Philippe Courtot, chairman and CEO of Qualys. "Adding context and correlating billions of global events with threat intelligence, analytics and machine learning results in a truly groundbreaking approach to EDR that not only stops sophisticated multi-vector attacks, but also automatically orchestrates the appropriate response all from a single solution, thus greatly reducing the time to respond while drastically reducing cost."

Spell Security Asset Acquisition

Qualys also announced that it has acquired the software assets of startup Spell Security. This acquisition will further strengthen Qualys' security and threat research, advance endpoint behavior detection and bring rich telemetry to the Qualys Cloud Platform. For Multi-Vector EDR, Spell Security's knowledge of threat hunting and adversary techniques will deliver additional capabilities to the app and additional analysis on the specific threats customers detect in their organizations. To read the press release visit, www.qualys.com/spellsecurity_pr.

Qualys Multi-Vector EDR Overview
Qualys Multi-Vector EDR helps security teams stay on top throughout the attack lifecycle from preventative protection, pre- and post-breach detection, automated investigation, and multi-layered response capabilities across the environment via a powerful cloud-based platform.

Cloud Agent Telemetry Collection – Widely deployed Qualys cloud agents have been enhanced to collect large amounts of telemetry that is sent to the Qualys Cloud Platform on a real-time basis allowing deep analysis in the shortest timeframe. This approach helps customers eliminate an additional EDR agent on their endpoints.

Multi-Vector Detection – Leveraging the highly scalable data lake as part of the Qualys Cloud Platform, security analysts can quickly correlate additional vectors like software inventory, patch levels, vulnerability threat intelligence, and misconfigurations with endpoint telemetry like file, process, registry, network and mutex data. This approach eliminates the need for threat hunters to access multiple security solutions for context.

Investigate and Prioritize – By augmenting in-house MITRE ATT&CK-based detections with other context vectors enriched with third-party threat feeds, security teams can receive real-time alerts, investigate and prioritize security incidents, and threat hunt via intuitive workflows that take into account asset criticality and network attack paths.

Respond and Prevent – Qualys Multi-Vector EDR uses multi-layered response strategies to remediate threats and mitigate the risk in real time. In addition to traditional EDR response actions, Qualys Multi-Vector EDR orchestrates workflows for patching exploitable vulnerabilities and remediating misconfigurations across the environment to prevent attacks on other endpoints. To augment Multi-Vector EDR, endpoint protection capabilities like anti-malware/anti-virus are being added to the agent in Q4 2020.

Availability
Qualys Multi-Vector EDR is currently in beta for Windows endpoints and will be released for GA in late Q3 2020. If you would like to join the beta program, please sign up at https://www.qualys.com/beta-signup/. Linux support is targeted for Q1 2021.

Additional Resources

- More information on Multi-Vector EDR
- Details on the Qualys Cloud Platform
- Follow Qualys on LinkedIn and Twitter

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions with over 15,700 active customers in more than 130 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 native Qualys Cloud Platform and its integrated Cloud Apps deliver 360-degree visibility across on premises, endpoints, cloud, containers, and mobile environments. The platform delivers the visibility businesses need to assess critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance, and protection for IT systems and web applications. Founded in 1999 as one of the first SaaS security companies, Qualys has built a large, impressive customer base and established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, as well as preeminent managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, 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 Contacts:
Tami Casey, Qualys
(650) 801-6196
tcasey@qualys.com

View original content to download multimedia:http://www.prnewswire.com/news-releases/qualys-unveils-multi-vector-edr-a-new-approach-to-endpoint-detection-and-response-301101812.html

SOURCE Qualys, Inc.