# Qualys Launches Context XDR to Prioritize Threat Detection and Reduce Alert Fatigue

February 8, 2022

New XDR solution built on the highly scalable Qualys Cloud Platform combines native asset and vulnerability risk context with endpoint telemetry and third-party logs for effective threat detection and response

FOSTER CITY, Calif., Feb. 8, 2022 /PRNewswire/ -- [Qualys, Inc](). (NASDAQ: QLYS), a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, today unveiled Qualys Context XDR the industry's first context-aware XDR. Powered by the highly scalable Qualys Cloud Platform, the solution combines rich asset inventory and vulnerability context, network and endpoint telemetry from Qualys sensors, along with high-quality threat intelligence and third-party log data to identify threats quickly and reduce alert fatigue.
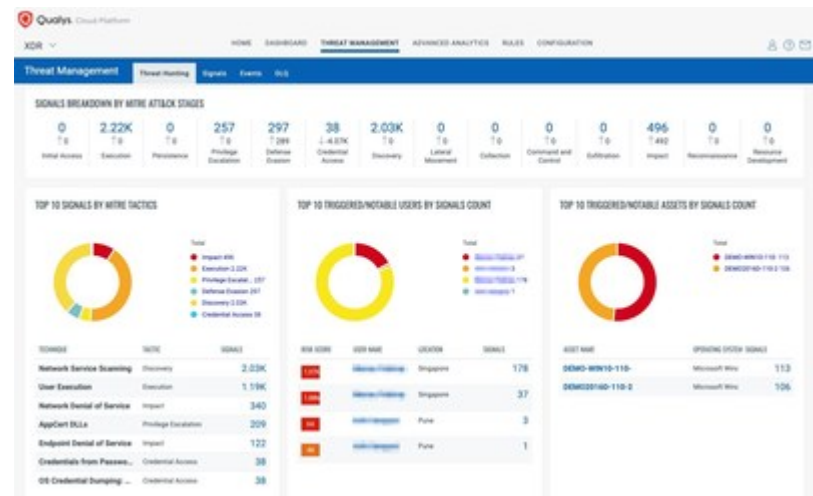
Protecting environments against an overwhelming and constantly evolving threat landscape is frustrating when detecting and responding to cybersecurity threats using siloed products that provide a narrow view of the attack. Current SIEM and XDR solutions passively and reactively collect disparate, unrelated logs creating an avalanche of notifications that place the burden of correlation and prioritization on the analyst. Incident response and threat hunting teams need an accurate, comprehensive picture of their attack surface to maintain an effective security, risk, and compliance program.

"Attack surface complexity and diversity requires security teams to implement risk assessment strategies that help focus their limited resources on the critical assets most vulnerable to attack," said Dave Gruber, principal analyst for Enterprise Security Group. "Leveraging a single agent, the Qualys platform combines security risk posture data with native endpoint telemetry, and threat intelligence to align threat investigation and response activities with the most critical assets."

"Cybersecurity operators need risk awareness to prioritize the alerts, incidents and threats bombarding our teams. Far too often, SIEM and XDR solutions deliver the data and expect us to make sense of it. True telemetry is so much more than just data. Integrating, correlating and transforming the data to provide meaningful context and actionable insights is the ultimate goal. Combining next-gen technology, such as Qualys, with our people and processes helps us proactively keep our clients resilient in the face of ever-evolving threats," said John Ayers, vice president of Advanced Detection at Optiv.

Qualys Context XDR provides the security context that operations teams need to eliminate false positives and noise by triangulating risk posture, asset criticality, and threat intelligence. Together, this provides visibility, contextual priority, and meaningful insights about the assets that allow teams to quickly make the most impactful decisions for enhanced protection. For example, a vulnerability that is being actively exploited by malware on an executive's computer or a highly sensitive server introduces a higher level of risk to the business than a system in a test environment and requires an immediate response.

The Qualys Cloud Platform, which processes more than 10 trillion data points, seamlessly collects IT, security and compliance telemetry using its multiple native sensors along with third-party logs to provide a broader view across organizations' global networks. Qualys Context XDR leverages this intelligence and the platform's cloud agent response capabilities - like patching, fixing misconfigurations, killing processes and network connections, and quarantining hosts – to comprehensively remediate the threats identified, and increase the productivity of time-starved security analysts.

Qualys Context XDR uses more than just logs to provide clarity through context by bringing together:

- **Risk Posture** – The solution leverages comprehensive vulnerability, threat and exploit insights to natively correlate OS and third-party apps, including misconfiguration/end-of-life (EOL) awareness for continuous vulnerability mapping.
- **Asset Criticality** – Leveraging the Qualys Cloud Platform, active asset discovery is coupled with dynamic, policy-driven criticality assignments to deliver the security and business context needed to prioritize high-value assets in real time.
- **Threat Intelligence** – A deep understanding of exploits, attacker techniques mapped against the MITRE ATT$CK

framework, and vulnerabilities used for defense penetration delivers preventative and reactive response capabilities to stop active attacks, remediate root-cause, and patch to prevent future attacks.

- **Third-Party Data** – Using Qualys' cloud-based agent and on premises sensors, Context XDR gathers up-to-the-second log and telemetry data from your enterprises' third-party solutions and triangulates it with asset risk posture, criticality, and threat intelligence to detect threats and create high fidelity alerts.

"Cybersecurity is getting increasingly complex - with software supply chain attacks such as Kaseya, ransomware attacks like Colonial Pipeline and widespread severe vulnerabilities like Apache Log4j - providing threat actors with multiple pathways into organizations IT infrastructure," said Sumedh Thakar, president and CEO of Qualys. "Qualys Context XDR is built to simplify this complexity by detecting threats, prioritizing alerts with comprehensive context and responding swiftly with multiple response actions."

Qualys Context XDR Live

Please join Qualys President and CEO Sumedh Thakar as he unveils Qualys Context XDR Live on February 22 at 10 am PT. Attendees will see Context XDR in action as we show how context is the crucial differentiator that adds clarity to incident response. The session will include a live Q&A. To attend this virtual live event, visit http://www.qualys.com/context-xdr-live.

Availability

Qualys Context XDR is currently available; request a demo at https://www.qualys.com/context-xdr-trial/. To learn more, read the Qualys Context XDR Blog.

Additional Resources

- Read the Context XDR Blog
- Learn about Qualys Context XDR
- 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 19,000 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 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 across on premises, endpoints, cloud, containers, and mobile environments. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and 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.

Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

Media Contact:
Jackie Dutton
Qualys
media@qualys.com

C View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-launches-context-xdr-to-prioritize-threat-detection-and-reduce-alert-fatigue-301477331.html

SOURCE Qualys, Inc.