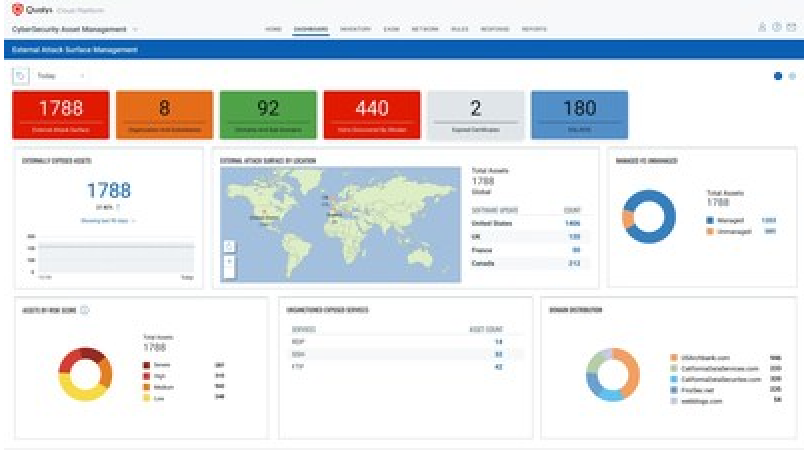
Qualys Brings External Attack Surface Management (EASM) to the Qualys Cloud Platform

August 3, 2022

New capabilities in CyberSecurity Asset Management 2.0 enable security and IT teams to continuously discover unknown internet-facing assets and automatically assess their risk posture

FOSTER CITY, Calif., Aug. 3, 2022 /PRNewswire/ -- **Qualys, Inc**. (NASDAQ: QLYS), a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, today announced it is adding External Attack Surface Management (EASM) capabilities to the Qualys Cloud Platform. Integrated into CyberSecurity Asset Management 2.0, the new component adds the external attacker view to identify previously unknown internet-facing assets for a complete and accurate picture of the enterprise attack surface.



Digital transformation, increased adoption of cloud and Internet of Things (IoT), a growing remote workforce, and a technology talent shortage have led to an exponential rise in organizations' attack surface. This expansion makes it harder for security teams to correlate externally visible and internally managed assets and govern compromises that occur because of undiscovered, unmanaged, or poorly managed IT assets. Organizations need a new approach to view vulnerable assets from the outside in and execute like an attacker to quickly identify areas of risk.

"Organizations must proactively manage their cyber defenses, which includes finding and addressing vulnerabilities to reduce cyber risk," said Michelle Abraham, research director, Security and Trust at IDC. "Qualys' unique approach to EASM is integrating the internal and external asset data from CyberSecurity Attack Management with its Vulnerability Management, Detection and Response (VMDR) solution into a single view. As a result, organizations can better identify undiscovered assets and immediately access and mitigate the cyber risk within the same workflow."

"Qualys CyberSecurity Asset Management provides invaluable attack surface insights from an external attacker's point of view," said Mike Orosz, vice president information and product security at Vertiv. "This view allows us to proactively augment our vulnerability management program by discovering risks presented by previously unknown internet-facing devices. Additionally, the automated workflows enable us to prioritize security engineering actions that will reduce cyber risk and rapidly improve our company's security."

Qualys CyberSecurity Asset Management 2.0 with EASM enables organizations to continuously monitor and reduce the entire enterprise attack surface including internal and internet-facing assets and discover previously unidentified exposures. It also helps synchronize with CMDBs, detect security gaps like unauthorized or end-of-support software, open ports, remotely exploitable vulnerabilities, digital certificate issues, unsanctioned apps and domains, and mitigate risk by taking appropriate actions.

Qualys CyberSecurity Asset Management with EASM allows Security and IT teams to:

Uncover Gaps Across the Entire Attack Surface - From a single cloud platform, the solution continuously discovers and accurately classifies internal and external internet-facing assets. It automatically finds your subsidiaries, performs horizontal and vertical domain and subdomain enumeration, correlates WHOIS and DNS records and attributes assets to your organization.

Get a Reliable, Accurate View Aligning Security and IT Ops - Augment uncertain, outdated data in your CMDB with CyberSecurity Asset Management. Teams can capture unmanaged assets and gain a single source of truth for internet-facing assets, along with location and context, through automatic synchronization with enterprise CMDBs and vulnerability management to streamline ongoing attack surface monitoring and response.

Rapidly Remediate Risk with Native VMDR 2.0 Integration - CyberSecurity Asset Management 2.0 and Qualys VMDR 2.0 improve the cybersecurity program posture with TruRisk scoring and automated and one-click orchestration of vulnerability and remediation workflows to convert internet-facing assets into fully managed and patched assets.

"Achieving full asset visibility remains one of cybersecurity's most elusive goals," said Sumedh Thakar, president and CEO of Qualys. "CyberSecurity Asset Management 2.0 solves this by providing both the holistic, external attacker-level and internal view of the attack surface to comprehensively address the increased threat landscape. Taking protection a step further, we've natively integrated the solution with Qualys VMDR so organizations can prioritize vulnerabilities and asset groups based on risk and proactively remediate to quickly reduce exposure."

Availability
Qualys CyberSecurity Asset Management 2.0 with EASM is currently in preview and available to existing customers. It will be generally available in mid-September. To request a free trial, visit qualys.com/csam-trial. Learn more by reading our blog, or attending our webinar on September 14.

Additional Resources

- Learn about CyberSecurity Asset Management 2.0
- Watch the video on CyberSecurity Asset Management 2.0 with EASM
- Read the CyberSecurity Asset Management product blog
- 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 security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Cloud Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit http://www.qualys.com.

Qualys, Qualys VMDR® 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

View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-brings-external-attack-surface-management-easm-to-the-qualys-cloud-platform-301598646.html

SOURCE Qualys, Inc.