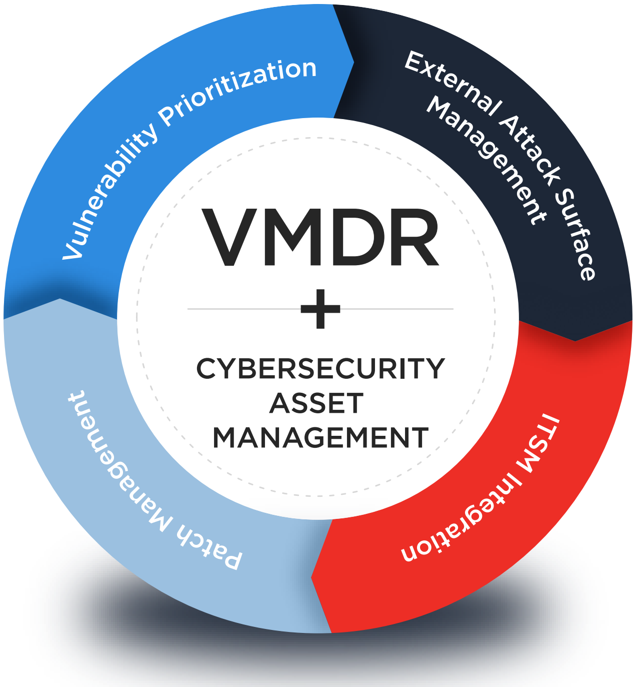
Qualys.

Cyber Asset Attack Surface Management (CAASM)

Reducing Risk Across the Entire Enterprise with Qualys

The attack surface for every organization is expanding rapidly, allowing cybercriminals to leverage unknown external internet-facing assets that conventional Vulnerability Management (VM) programs cannot see to inflict catastrophic disruption to their targets.

Nearly 80% of organizations acknowledge asset visibility gap is the main factor behind their increase in security incidents. These gaps are plagued by a stream of new vulnerabilities, which have grown 8% per year for the last five years according to the National Vulnerability Database (NVD). As a result, cybersecurity practitioners have looked to modernize their VM programs by extending oversight to external, internet-facing assets. Thus, a new category of solutions called Cyber Asset Attack Surface Management (CAASM) has emerged to answer this need by combining inside-out and outside-in views of networks.

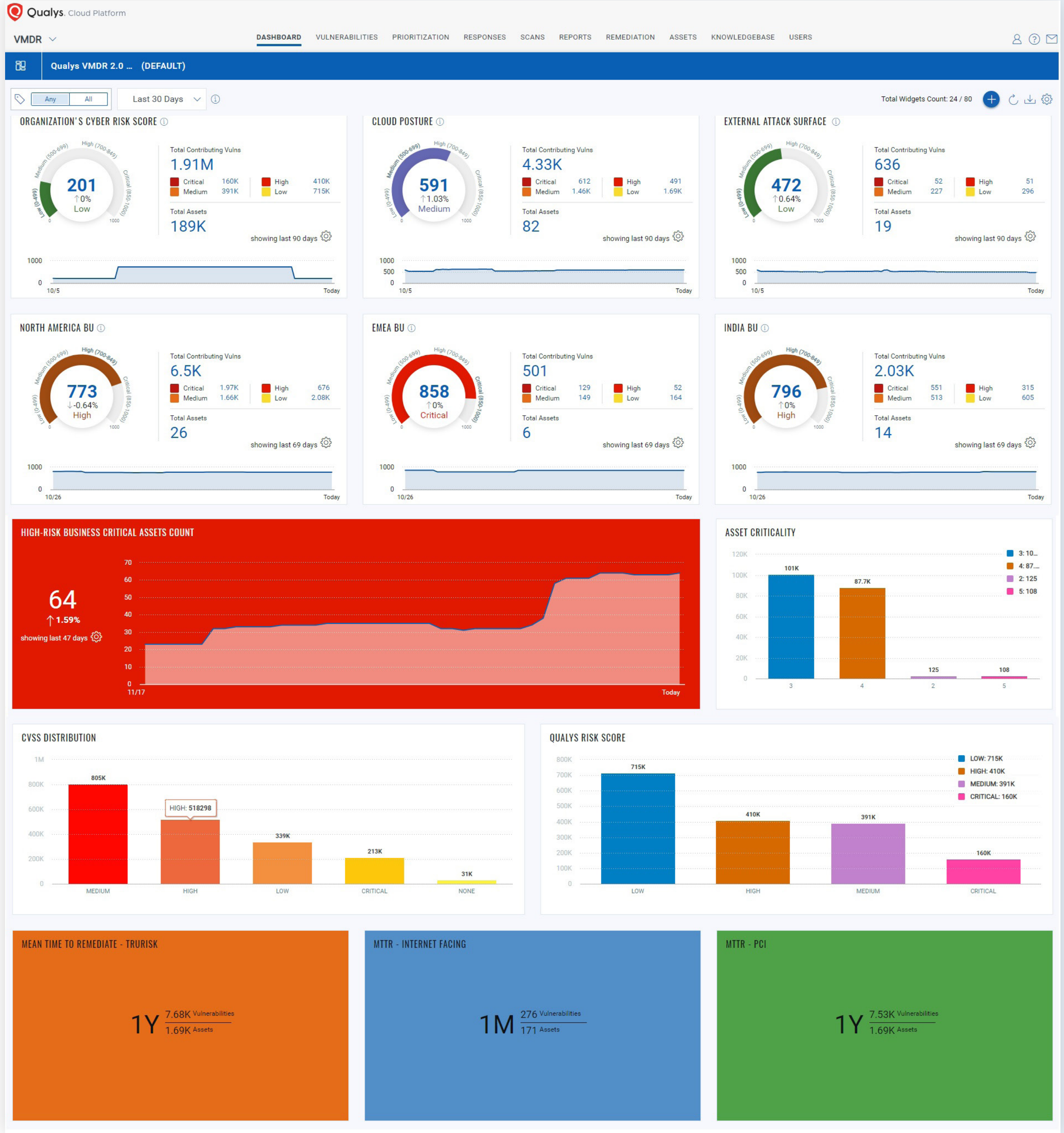

Vulnerability Prioritization
External Attack Surface Management
ITSM Integration
Patch Management
VMDR
+
CYBERSECURITY ASSET MANAGEMENT

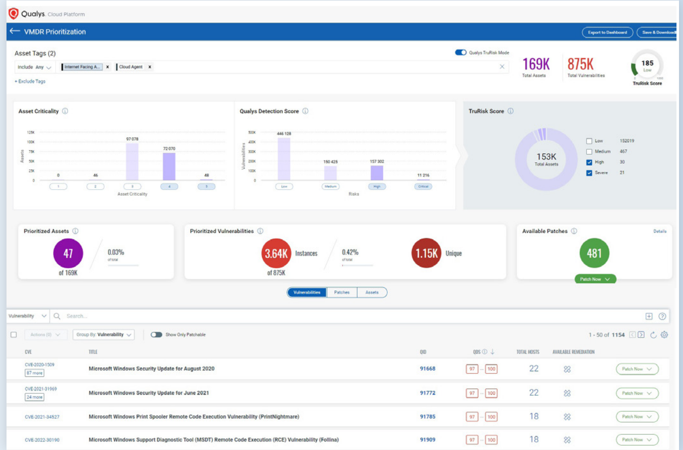
The Qualys Approach to CAASM is VMDR + CSAM with External Attack Surface Management (EASM).

With Qualys, organizations gain access to a scalable CAASM program that is delivered with the seamlessly integrated VMDR and CyberSecurity Asset Management solution on one powerful dashboard. With this approach, security practitioners and IT stakeholders alike improve the coverage of VMDR with extended oversight over previously unknown, external internet-facing assets, asset groups, domains, subdomains, and more.

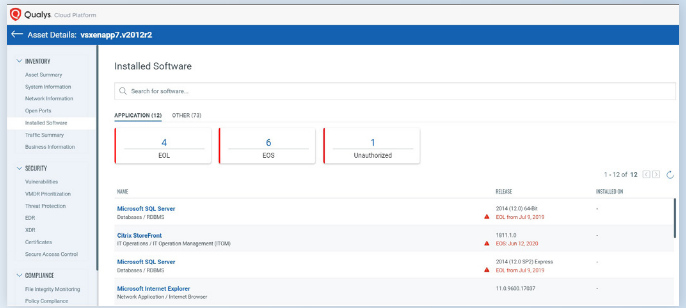
See and secure all assets across your entire attack surface.

Qualys Vulnerability Management, Detection and Response (VMDR) and CyberSecurity Asset Management (CSAM) with External Attack Surface Management (EASM) offers a unified and consolidated view of your organization's entire attack surface. As a natively integrated solution, VMDR users can deploy CSAM with EASM in a single-click, rapidly extending their VM program to external internet-facing assets for a holistic, risk-based approach to cybersecurity across the entire enterprise.

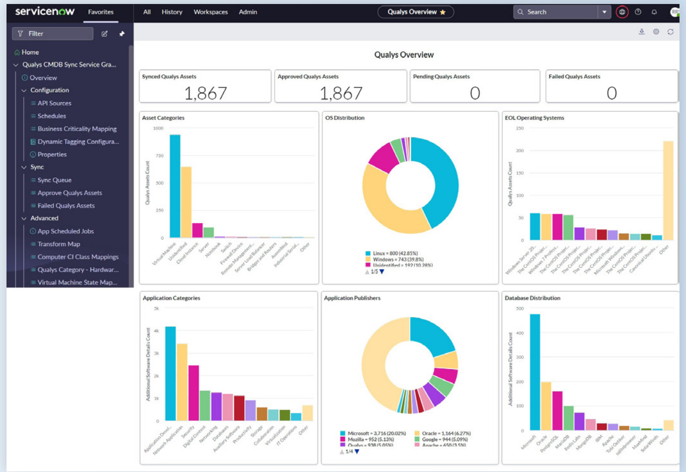




Integrate VM and Cyber Asset Attack Surface Management (CAASM) programs together to track your organization's cyber risk exposure, cloud posture, external attack surface, and more.



Lower the risk of shadow IT by reducing the time-to-inventory for current and upcoming End of Service (EOS) and End of Life (EOL) software instances, complemented with automated alerts for IT and budget planning for up to 1-year into the future.



Bridge the IT-Security gap by optimizing cross-functional threat response with ITSM tool integration, such as ServiceNow.

Qualys CAASM Capabilities and Benefits

(Powered by VMDR and CyberSecurity Attack Surface Management with External Attack Surface Management)

360-DEGREE ASSET DISCOVERY

Continuously discover all internal and external internet-facing assets on-premises, hybrid, IoT and in the cloud. From instances to containers, CSAM uses advanced credentialed and non-credential scanning technologies to discover continuously and quickly classify vulnerabilities for remediation.

UNIFIED VM AND CAASM

Consolidate your security stack with the Qualys Cloud Platform, which brings together all elements of an effective VM and CAASM program delivered with a single unified SaaS platform.

FEWER CRITICAL VULNERABILITIES WITH QUALYS TRURISK™

TruRisk

Reduce cyber risk by focusing on fewer, more important vulnerabilities. With TruRisk™ you can reduce risk by 23% to 50%.

OUTSIDE-IN AND INSIDE-OUT ASSET VIEW

Improve cybersecurity hygiene and better enforce compliance directives with an outside attacker's view of your entire surface leveraging Shodan.io integration.

RISK-BASED VULNERABILITY MANAGEMENT

Go beyond CVSS scores with Qualys TruRisk™, which combines real-time intelligence of malware, historical vulnerability data, threats, and assets to identify the real business impact that threats pose to your organization for targeted alert prioritization.

EOL AND EOS SOFTWARE MANAGEMENT

Make sure inventories are always up to date with automated discovery of unapproved applications, approaching end-of-life policies, missing titles, critical misconfigurations, and more across your entire application ecosystem.

ITSM TOOL INTEGRATION

Improve IT-Security workflows with ITSM integrations for up-to-date, complete, structured, and enriched CMDB bi-directional dataflows.

Learn more about VMDR and CyberSecurity Attack Surface Management with External Attack Surface Management (EASM), the Qualys CAASM Solution. Try it for 30 days. qualys.com/forms/vmdr/

Key Use Cases for Qualys CAASM

(Powered by VMDR and CyberSecurity Attack Surface Management with External Attack Surface Management)

USE CASE CHALLENGE	SOLUTION	OUTCOMES
Integrating VM and Cyber Asset Attack Surface Management (CAASM) Unknown internet-facing assets are about 30% of any organization's application infrastructure, resulting in blind spots and elevated cyber risk. While VM is the cornerstone of a security stack, CAASM is increasingly necessary for organizations to improve security coverage and reduce their exposure to cyber risk.	VMDR and CSAM with External Attack Surface Management (EASM) provides consolidated asset and vulnerability insights for a unified view over the entire attack surface. Deployed with the Qualys lightweight agent or via the comprehensive Qualys sensor ecosystem, you achieve improved threat detection, automated remediation workflows, and a risk-based approach to cybersecurity that works across the entire enterprise.	Reduced MTTR and better asset visibility lets you measure cyber risk improvements over time with a single, consolidated platform. With VMDR and CSAM with EASM, you get the best in VM and CAASM while driving a consolidation strategy that improves TCO at no degradation to your risk posture.
Managing and Securing Organization from Shadow IT The hybrid conventional security perimeter is from the datacenter to remote, external internet-facing assets. This creates new challenges for VM and security practitioners, including securing their environment for unapproved or exploited applications. Still, as much as 60% of organizations today do not include shadow IT in their internal threat assessments.	Qualys VMDR and CSAM with EASM comes with EOL/EOS software tracking compliant with CISA guidelines to help expose baseline discrepancies, including VMs, containers, and functions-as-a-service. By identifying deviations from established baselines, VMDR and CSAM with EASM discovers and supports remediation of untracked, new externally facing software instances and services.	Continuous enumeration of unknown assets and services automatically baselines asset inventories across the entire ecosystem, improving security hygiene, optimizing IT-security coordination, and reducing exposure to cyber risk. Shadow-IT risk is inherently and automatically mitigated as a result.
Bridge the IT-Security Gap Processes of vulnerability discovery, patch management, and remediation span several steps of action that require multiple tools and include various stakeholders from both IT and security teams. As a result, security and IT stakeholders are challenged with cyber risk becoming an overarching concern and shared KPI between both departments.	Qualys VMDR and CSAM with EASM integrate with ITSM tools, including ServiceNow, for accurate and up-to-date ticketing between all security and IT stakeholders. With complete, structured, and enriched CMDB bi-directional dataflows, users of Qualys VMDR and CSAM with EASM can easily track and trace vulnerabilities from detection to close out with ease.	More time spent in high-value tasks and less time spent on vulnerability analysis and reporting due reduced ticketing complexity, automated reporting and improved coordination between security operations, IT operations and respective cyber risk leaders and C-level executives.
Risk Based Vulnerability Management Assets and applications are exposed to a rising number of vulnerabilities and targeted malware that can infect various areas of the network due to increased connectivity between IoT and IT networks. 70% of vulnerabilities can be exploited without needing special privileges. Security practitioners must identify and isolate vulnerabilities faster than ever before to minimize the risk of lateral movement of malware.	Qualys VMDR and CSAM with EASM provide continuous and robust vulnerability assessments on all assets. Hardware, software, and firmware-based vulnerabilities impacting all applications are covered with the Qualys lightweight agent, numerous sensors, and the Qualys optional cloud agent, enabling security practitioners to formulate zero-trust network access policies and enforce them across the entire enterprise without affecting network performance.	Security partitioners can identify and manage vulnerabilities at all endpoints, enabling zero-trust segmentation, targeted remediation, and compliance programs to reduce lateral movement of cyber threats between industrial applications and IT and IoT network environments. With EASM, security coverage and policy enforcement are extended to external, internet-facing assets, all with one unified solution.

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. 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.

For more information, please visit **qualys.com**