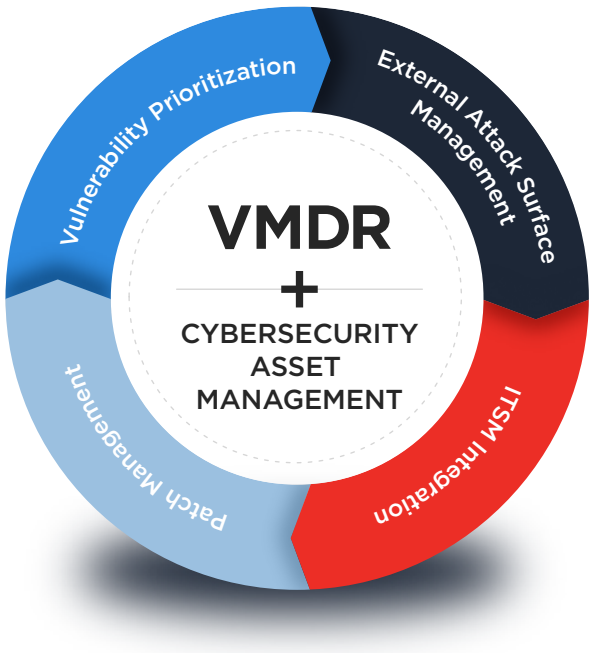
Qualys.

VMDR and CyberSecurity Asset Management with External Attack Surface Management (EASM)

Reducing Cyber Risk Across the Entire Enterprise

In recent years the fragmented IT infrastructure across IT, IoT, OT, cloud, mobile has continued to expand in turn resulting in exponential rise in the attack surface of an organization, threats are becoming more sophisticated, and vulnerabilities are getting weaponized faster than ever before. Reducing this risk can seem like a never-ending battle.

Add to that remote-work culture is forcing the security perimeter of the conventional enterprise to expand beyond the data center to each device within its evolving and elastic infrastructure. While this change has made businesses and work more agile, it has increased cyber risk exposure of organizations with legacy Vulnerability Management (VM) and Attack Surface Management (ASM) solutions that are ill-equipped to navigate a fluid cyber asset attack surface. In fact, nearly 80% of organizations identify asset visibility gaps as the main factor behind a 300% increase in security incidents, according to a study conducted by Enterprise Strategy Group (ESG).



With Qualys Vulnerability Management, Detection and Response (VMDR) and CyberSecurity Asset Management (CSAM) together, customers gain world-class Risk Based vulnerability management solution, combined with External Attack Surface Management (EASM) delivered via a single, unified dashboard. In addition to achieving a consolidated means of managing and remediating vulnerabilities wherever they may be, Qualys VMDR and CSAM with EASM are complimented by Qualys TruRisk™, which help security practitioners to manage cyber security risk by quantifying cyber risk so that they can measure risk and take prioritized set of actions to reduce risk. This transparent and powerful approach to cyber risk improves the operationalization of Vulnerability Management (VM) and Attack Surface Management (ASM) programs with actionable insights that go far beyond basic capabilities of legacy VM solutions.

With one platform, one universal agent, and one data model, Qualys VMDR and CSAM with EASM bring both IT and SecOps teams enhanced decision-making tools for more productivity and more comprehensive security and compliance programs. No more spreadsheets are required!

VMDR and CyberSecurity Asset Management (CSAM) with External Attack Surface Management (EASM) Capabilities and Benefits:

External Attack Surface Management

See and secure your entire enterprise from the vantage-point of an attacker with outside-in data coverage over previously unknown, external internet-facing assets on-premises and in the cloud.

Risk-Based Prioritization

Tag and assign criticality scores to assets and asset groups according to industry, compliance, or operational need using TruRisk™, saving analysis time, reducing the MTTR, and improving cyber risk exposure and reporting.

CMDB Integration

Accurately and continuously update CMDB to improve the relevance of vulnerability risk assessments by mapping business criticality data to assets for better cyber hygiene.

Security and IT Team Alignment

Achieve a single source of truth for assets and vulnerabilities with ITSM integrations. No more complex handoff processes, non-correlated data, inconsistent data, or disagreements between security and IT teams on what needs to be tackled first for remediation.

Continuous Visibility

Maintain complete visibility of assets, software, and vulnerabilities across distributed hybrid environments.

Improved Compliance

Manage and build asset inventories required by security standards, including CISA, PCI DSS, FedRAMP, NIST, and SOC 2.

Automated Workflows

Auto-remediate specific issues and even quarantine assets using Qualys Flow (QFlow) with flexible, no-code rules.

Improved EOL and EOS Software Management

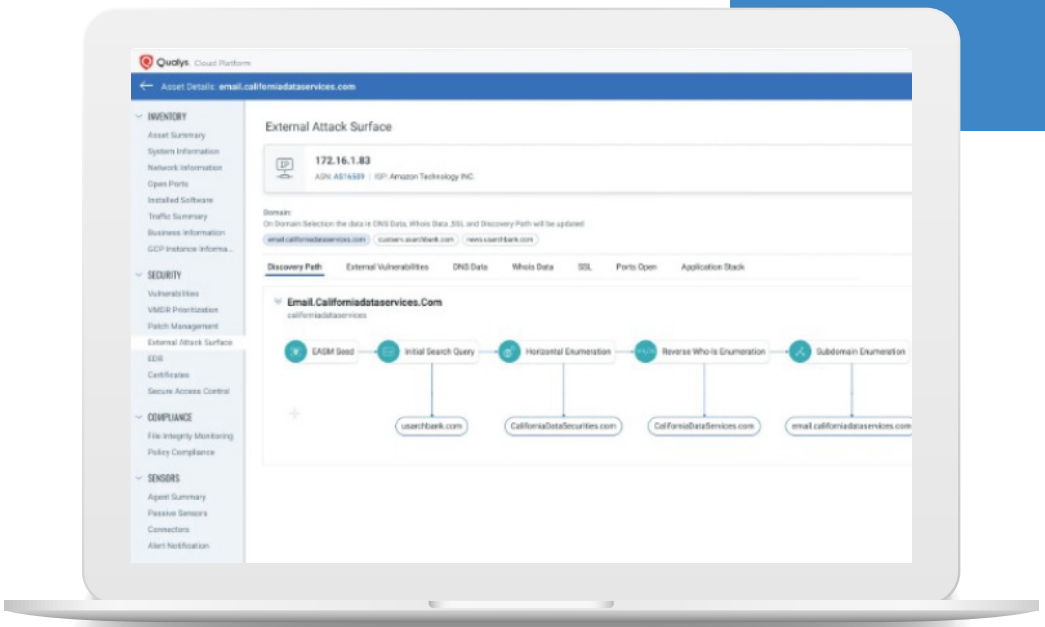
Decrease the attack surface by uncovering outdated or unsupported applications, missing required software, and unauthorized software.

Single Cloud Agent

Consolidate security stack. Reduce cost, complexity, and risk of managing cloud, server, desktop, laptop, and other endpoints — with Qualys.

"On average, Attack Surface Management tools will find 30% more surface area assets than IT was aware of."

Forrester Research



Key Use Cases for Qualys VMDR and CyberSecurity Attack Surface Management (CSAM) with External Attack Surface Management (EASM)

USE CASE CHALLENGE	SOLUTION	OUTCOMES
Integrating VM and Cyber Asset Attack Surface Management (CAASM) Unknown internet-facing assets make up about 30% of any organization's application infrastructure, resulting in blind spots and elevated cyber risk. While VM is the cornerstone of any 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) consolidate 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 improved asset visibility with the ability to measure cyber risk improvements over time with a single, consolidated platform. Using 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 enterprise conventional security perimeter extends from the datacenter to remote endpoints. This has led to new challenges for VM and security practitioners, including securing their environment for unapproved or exploited assets. Still, as much as 60% of organizations today still 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 integrates 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.	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 reduce the risk of lateral movement of malware.	Qualys VMDR and CSAM with EASM provides 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

Learn more about VMDR and CyberSecurity Attack Surface Management, the Qualys CAASM Solution. Try it for 30 days.
qualys.com/try/vmdr/

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**