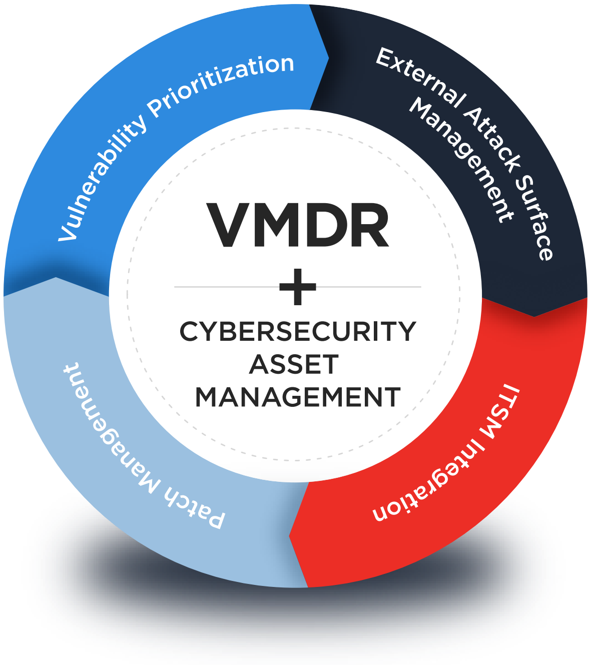
Qualys.

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

Secure your entire attack surface

The modern attack surface is evolving faster than ever, threats are becoming more sophisticated, and vulnerabilities are getting weaponized faster than ever before. Choose a unified approach to defending your ever-changing attack surface.

Only 9% of organizations believe they monitor 100% of their attack surface. It's no surprise, as the modern attack surface includes IT, OT, IoT assets, cloud and on-prem assets, legacy external assets exposed to the internet… the list goes on. While this diversity of technology 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. 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).


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

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 view of risk across the attack surface. Qualys VMDR and CSAM with EASM are complimented by Qualys TruRisk™, which streamlines prioritization through a single measurement that goes beyond vulnerabilities and CVEs to account for risk factors such as asset criticality, EoL/EoS, risky ports, expired certs, and more.

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 (CASM) with External Attack Surface Management (EASM) Capabilities and Benefits:

External Attack Surface Management

Find all your assets from mergers, acquisitions, and subsidiaries, attributing them to a specific area of the business. Leverage industry leading vulnerability scanning immediately upon discovery, for accurate and continuous assessment of external risk.

Go Beyond Vulnerabilities to Identify All Risk Factors

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.

Keep Your CMDB Up to Date

Continuously update your CMDB to improve a complete inventory of internal and external assets, including cyber risk context such as EoL/EoS, expired SSL certs, and missing security agents. Auto-assign tickets with 96% accuracy based on Qualys tags.

Reduce Blind Spots and Add Business Context with 3rd-Party Connectors

Discover assets from ServiceNow, BMC Helix, Active Directory, Webhook, and more to add coverage and business context to your security program. Extract data such as asset criticality, device ownership, and assigned support group to drive risk prioritization.

Measure and Drive Compliance

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

Steamline SecOps and ITOps Workflows

With a single click, add previously unknown assets to your VM, web app scanning, and patch jobs. Leverage out-of-the-box integrations with IT and SecOps tools and produce executive level risk reports.

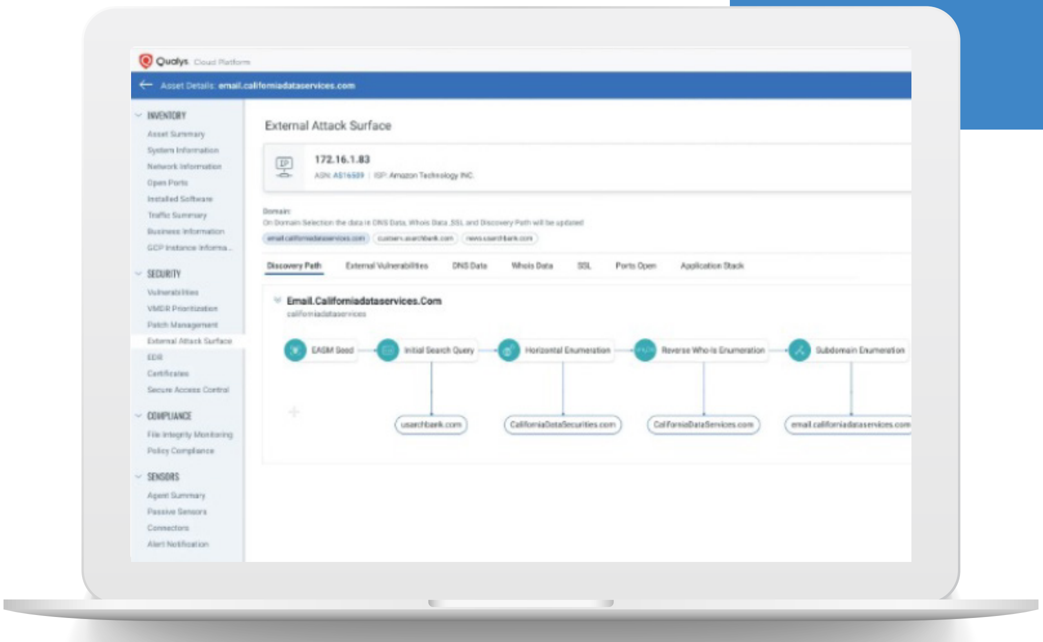
Manage Tech Debt (EoL/EoS) Proactively

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

Transform Cloud Agents Into Passive Sensors

Identify unmanaged devices connected to your network in real time, including IoT and rogue devices. Quickly add them to your VM program for risk assessment.

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



On Domain Selection the data in DNS Data, Whois Data ,SSL and Discovery Path will be updated

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

USE CASE CHALLENGE	SOLUTION	OUTCOMES
Secure your External Attack Surface Unknown internet-facing assets make up over 30% of the average enterprise attack surface, resulting in blind spots and elevated cyber risk. While VM is the cornerstone of any security stack, it can only scan the assets under management. Organizations need a continuous discovery method for internet-facing devices and systems, especially when it comes to mergers, acquisitions, and subsidiaries.	VMDR and CSAM with External Attack Surface Management (EASM) consolidates asset and vulnerability insights for a unified view over the entire attack surface. Continuously monitor the external attack surface for unknown assets, and conduct automated lightweight vulnerability scans with industry-leading accuracy. Attribute assets to your organization with confidence, and instantly see the TruRisk of previously-unknown assets.	Improve coverage of the external attack surface by discovering an average of 38% more unknown assets on the internet. Track and remediate cyber risk across mergers, acquisitions, and subsidiaries. Eliminate false positives and accuracy gaps that result from banner grabbing and other popular EASM tactics. Consolidate external asset discovery and risk assessment with VMDR and CSAM with EASM to lower TCO, drive compliance, and reduce MTTR with a unified platform.
Manage Risk From Tech Debt (EoL/EoS) Most organizations have no singular view of current and upcoming End-of-Life (EoL) and End-of-Service (EoS) technology that includes cyber risk assessment. CISOs and CIOs need a unified view of of upcoming EoL/EoS to prioritize based on cyber risk, budget for upgrades, and mitigate before unpatchable vulnerabilities introduce critical business risk.	Qualys VMDR and CSAM with EASM comes with EoL/EoS software tracking compliant with CISA guidelines. By proactively tracking upcoming EoL/EoS up to 12 months in advance, CISOs and CIOs have a shared view of the scope and risk to determine budget and resources required to upgrade or mitigate. While it may not be realistic to eliminate EoL/EoS from the environment entirely, organizations can focus resources on reducing risk.	Track, manage, and mitigate tech debt from EoL/EoS up to 12 months in advance, reducing cyber risk and expenses associated with a reactive approach. Align IT and Security leadership with a risk-based view of EoL/EoS, streamlining prioritization and resource deployment. Pinpoint categories, publishers and manufacturers, and products that require mitigation to proactively eliminate risk, improve compliance, and limit disruption to the business.
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 and BMC Helix, 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. Map tickets to your ITSM solution with 96% accuracy, and reduce MTTR up to 60% with streamlined IT-Security workflows.
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 CSAM with External Attack Surface Management. Try it for 30 days. **qualys.com/forms/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**