

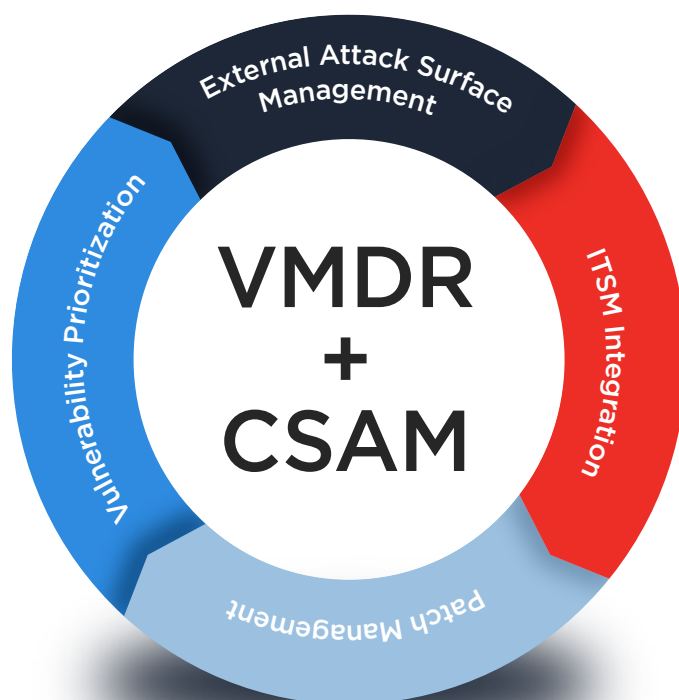


CyberSecurity Asset Management

with External Attack Surface Management

The attack surface of an enterprise can now change minute-to-minute. Every time an employee spins up a cloud instance, abandons a domain, configures a certificate or installs a virtual machine, they create another internet-facing asset that holds the potential for security vulnerabilities your team needs to track. Hybrid environments have seen a proliferation

of these external risks, but they fall outside the reach of many attack surface management solutions. Security practitioners need a technology that provides the same intelligence that attackers use – and one that can integrate seamlessly with their solutions for vulnerability management, prioritization, patch deployment and IT service management.



Your VM solution can now discover both internal known – and external unknown – assets for a 360-degree inventory of the IT ecosystem and rapid vulnerability remediation.

Discover the full extent of your attack surface – before bad actors find it for you.

CyberSecurity Asset Management (CSAM) is a cloud service that allows enterprises to continuously discover, classify and remediate vulnerabilities to measurably improve their cybersecurity posture. It includes External Attack Surface Management (EASM) for 100% visibility of internet-facing risks.

CyberSecurity Asset Management is Part of the VMDR Ecosystem



Environment Risks

Qualys CyberSecurity Asset Management Provides:



External Attack Surface Management leveraging continuous credentialed and non-credential scanning technologies to quickly discover and classify internet-facing assets, including assets in connected subsidiaries and business partners.



A Remedy for “Shadow IT” that finds policy violations and unauthorized software that spin up faster than IT can track with legacy tools, including baseline discrepancies in containers, functions-as-a-service, IoT devices, repositories, certificates, VMs, domains and subdomains.



CISA-compliant Tracking for End-of-life Software that reduces tech debt by uncovering outdated or unsupported applications, missing required software and unauthorized or missing titles.



A Solution to the IT-security Gap thanks to integration with Qualys CMDB – which tracks 80k vulnerabilities sourced from over 25+ threat sources – plus support for ITSM ticketing that results in a faster MTTR across teams.



Integrated Patch Management that automatically quarantines suspicious devices until they can be investigated and quickly deploys the most relevant and superseding patches across any size environment.



Risk Scoring giving CSAM the power to analyze vulnerabilities and misconfigurations in real time with six-sigma accuracy using Qualys TruRisk to prioritize remediation based on criticality and potential business impact.



Context-relevant Prioritization that allows security teams to assign risk profiles that prioritize security efforts by tagging assets according to function, environment, service and business relevance.

Key Use Cases for Qualys CyberSecurity Asset Management

CHALLENGE	SOLUTION	OUTCOMES
Visibility of unknown devices More than 30% of all on-premises and cloud assets are not inventoried by security teams. Even with a vulnerability management solution, many enterprises cannot see or remediate vulnerabilities across cloud services, domains, unauthorized software and other internet-facing assets.	CSAM with EASM works in conjunction with the Qualys Cloud Platform and Qualys sensors (scanners, cloud connectors, container sensors, cloud agents, passive sensors and APIs) to continuously discover all assets. It continuously tracks IT assets for 100% real-time visibility of a global hybrid IT environment.	Security teams can easily inventory the entire attack surface – internal and external – for remotely exploitable vulnerabilities. They can also expose “shadow IT” by automatically tracking baseline discrepancies in containers, functions-as-a-service, non-compliant software, VMs, IoT and other potential endpoint blind spots.
Prioritizing vulnerability response An asset management program needs the ability to identify the most consequential vulnerabilities and act on them immediately. Resources are limited, and enterprises must quantify the risks they face and prioritize remediation actions accordingly.	Leveraging its integration with VMDR 2.0 and Qualys TruRisk, CSAM analyses vulnerabilities to identify those with the easiest path to compromise business processes or steal valuable data. As a result, cybersecurity teams know exactly which vulnerabilities to address first based on actual risk, and which can be de-prioritized or ignored due to low or no impact on the business.	CSAM and the Qualys platform allow cybersecurity teams to efficiently prioritize risks across the entire IT ecosystem. CSAM is also the only ASM solution that can offer external asset data mapping, combined with internal asset data, to help identify the blast radius of externally exposed devices.
Customizing risk profiles to the enterprise Every organization contends with a unique IT ecosystem and threat landscape. Security leaders often need a way to customize a vulnerability management solution to match the specific risks they face.	CSAM allows users to easily correlate key business and technical context with assets and asset groups for accurate threat and remediation response prioritization according to “Asset Criticality.” Asset Criticality is a user-defined measure of asset function, environment and service.	Users can easily assign scores to tags that are applied to assets to ensure the most sensitive services and endpoints are prioritized for remediation when needed. If integrated with CMDB, the Asset Criticality score is automatically assigned to a tag and the corresponding asset.
Reducing the IT-Security gap for threat response and compliance Coordinating vulnerability data and remediation actions across IT and security is essential to reduce MTTR. These teams need to work more closely together to not only discover risks, but successfully orchestrate their response.	VMDR with CSAM is fully integrated with ticketing systems, ServiceNow, Patch Management and other Qualys services. The platform enables orchestration across teams for efficient vulnerability response, from alerts through automated device quarantine and instant patch deployment or manual remediation with a shared view of the threat.	A security team's response tasks are continually synched with IT and benefit from shared context as both teams work to address risks. Additionally, Qualys solutions can auto-document compliance for PCI DSS, FedRAMP, NIST, ISO, SOC 2 Type II and other policies as IT and security work to reduce asset vulnerabilities.