# Essential Must-Haves: Attack Surface Management

Ransomware attacks, data breaches and phishing scams continue to grow in volume and complexity. Meanwhile, the enterprise attack surface continues to expand, further exposing organizations to threat actors looking to exploit legacy cybersecurity defenses and vulnerability management (VM) programs that have fallen behind the demands of today's threat landscape.

Research from ESG found that **69% of organizations have experienced an attack targeting an "unknown, unmanaged or poorly managed internet-facing asset."** As a result, Attack Surface Management (ASM) has grown in popularity, helping security practitioners bolster their existing VM program with greater cybersecurity. But with so many options available, what ASM requirements are key?

---

## Build the right ASM strategy with these five essential must-haves:



### 1 External Attack Surface Management (EASM)

Although External Attack Surface Management, or EASM, is becoming a vogue term among security vendors, many ASM solutions today still do not provide a comprehensive "external" view of your network. This leaves security practitioners at a disadvantage against malicious actors leveraging dormant, external devices to

penetrate defenses. When assessing ASM capabilities from any vendor, put their EASM capability to the test. Make sure that external scans are not cost-prohibitive and that the advertised EASM capabilities are in fact able to cover domains and subdomains. With comprehensive EASM, security practitioners gain insight and asset intelligence from the vantage point of an external malicious actor, offering greater threat context and proactive threat hunting that complement VM.

**How we do it**

Qualys CSAM offers a truly powerful natively integrated EASM capability, providing continuous discovery, risk assessment, prioritization and remediation of the entire attack surface. With Qualys CSAM, achieve coverage for both internal known and external unknown internet-facing assets (on-prem, multi-cloud, subsidiary) from a single platform that includes unlimited network scans for all asset types, including domains and subdomains. Qualys CSAM is 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. In addition, Qualys CSAM is natively integrated and deployed with Qualys Vulnerability Management, Detection and Response (VMDR), combining the best in VM, asset visibility and risk-based attack surface management.

## 2 Asset Inventory and Discovery

ASM will always be part of a comprehensive security stack. Therefore, testing how well your selected ASM solution integrates and leverages adjacent tools within your existing security stack is not to be overlooked. For example, if an ASM solution does not integrate seamlessly with your VM program, your ASM will not be able to leverage key asset analytics necessary for targeted policy enforcement and remediation pathways. To get the most out of your ASM investment and to assure that your ASM complements your VM program, make sure to test that your ASM works well with your asset inventory and discovery platform.

**How we do it**

Qualys CSAM provides coverage for the entire attack surface with unified asset inventory and visibility alongside risk-based threat prioritization, covering container, datacenter and multi-cloud assets. As part of the Qualys Cloud Platform, Qualys CSAM has a natively integrated workflow across VMDR, ITSM, Patch Management and SecOps products that helps operationalize the asset metadata with ease. The result is one orchestrated and seamlessly integrated cybersecurity tool stack.

## 3 Advanced Analytics

In most hybrid networks, finding devices without endpoint agents is not uncommon. However, finding agentless endpoints and remediating them with ease is important because devices without endpoint agents represent serious security implications for your environment. Without amicable endpoint visibility and analytics down to the asset level, security practitioners are left guessing regarding endpoint policy adherence and threat context across their expansive network. Strive to avoid this constant game of whack-a-mole and guesswork when it comes to endpoint security and advanced analytics. When building an ASM strategy, make sure that your ASM supports a risk-based approach to cybersecurity analytics and that all endpoints are accounted for.

**How we do it** Built from one of the industry's most comprehensive asset inventory and VM solutions, Qualys CSAM provides unparalleled asset visibility and risk-based threat analysis down to the asset and endpoint level. Also, with the ever-expanding Qualys Threat DB that is armed with over 180k sourced vulnerabilities from 25+ threat sources, security practitioners can be sure that Qualys CSAM will always provide the very best and up-to-date threat intelligence to guide your ASM strategy.

## 4 Vulnerability, Patching and ITSM Support

With a growing network of diverse physical and virtual assets, many traditional asset management solutions fall short in their ability to identify zero-day threats. Facilitate patching and—most of all—faster remediation action between both IT and Security teams. When a vulnerability is identified, the industry average to remediate that threat is often over eight days—much too slow to thwart an attack and respond to an exploit that takes less than 48 hours. To reduce the mean time to respond (MTTR), both IT and Security stakeholders need a new approach to asset management that can help make threat detection and response faster and more targeted.

**How we do it** How we do it With a focus on ITSM tool integration such as ServiceNow, Qualys CSAM brings not only a risk-based approach to asset management, but also facilitates better IT and Security coordination. With Qualys CSAM, threats are prioritized based on asset criticality ratings and are natively integrated with Qualys VMDR and Patch Management. This allows organizations to immediately pivot from an alert to an active incident investigation to identify all assets susceptible to the same exploit and patch them using Qualys Patch Management.

# Essential Must-Haves: Attack Surface Management

## 5 Cloud Misconfiguration Identification

The enterprise has moved workloads from the datacenter to the cloud, contributing to a more productive and elastic working model. However, this "multi-cloud" environment has also amplified cybersecurity risk with an extended attack surface. Security practitioners are now challenged with maintaining an accurate asset inventory that is capable of tracking cloud assets and their configuration status, as well. Without this capability, cloud misconfigurations can result in security breaches, or indicate that a breach has already happened. Real-time cloud misconfiguration identification is critical for maintaining a proper ASM strategy fit for today's multi-cloud working environment.

**How we do it**

Qualys CSAM instantly identifies misconfigurations across the entire multi-cloud environment, applying risk context to indicators of compromise thanks to Qualys VMDR with TruRisk. With Qualys CSAM, security practitioners can be confident that cloud instances and misconfigurations do not go unnoticed and unaddressed.

---

**CyberSecurity Asset Management (CSAM) is a cloud service that allows customers to continuously discover, classify and remediate threats.** It measurably improves cybersecurity posture for both internal and external IT assets before attackers can find vulnerabilities—leveraging the same actionable intelligence that attackers use. It discovers all known and previously unknown internet-facing assets for 100% visibility and tracking of risks.

To learn more about Qualys CSAM with External Attack Surface Management go to:
**www.qualys.com/csam**



v240228