DATA SHEET

Cymulate

Cymulate Attack Surface Management (ASM)

Close the Gap Between Traditional ASM & Vulnerability Management

Cymulate Attack Surface Management (ASM) discovers vulnerabilities and misconfigurations to identify assets exposed to unapproved access, exploits, and other attacks. It scans domains, subdomains, IPs, ports, cloud platforms, configurations, devices, and privileges and maps potential attack paths that could be used by threat actors to access sensitive systems and data.

Cymulate ASM includes unified attack path mapping and analysis to demonstrate how an attacker can traverse the network from on-premises to the cloud and back. Visualizing the combination of gaps and weaknesses from start to finish provides a more complete and detailed picture, so organizations can accurately assess asset risk.

Cymulate ASM Capabilities

Minimize External Threat Exposure

Cymulate ASM includes external ASM capabilities to map the external attack surface by emulating reconnaissance and probing methods of threat actors to identify digital assets (such as web domains, IP addresses, applications, and more) and assess their exploitability. With findings mapped to the MITRE ATT&CK® framework's tactics, techniques, and procedures (TTPs), businesses can take the necessary mitigation steps. Customers only need to install one lightweight agent per environment to run assessments. The agent facilitates seamless communication between customer devices and the Cymulate platform, ensuring timely updates and efficient transfer of operational data.

How it Works

- Scan for internet-facing (external) assets
- Tag important assets to highlight their significance
- Run vulnerability and misconfiguration scans against all of the found external assets
- Prioritize discovered vulnerabilities and misconfigurations according to the probability of exploitation and the importance of the asset
- Remediate prioritized and exploitable security gaps

Cymulate ASM Benefits

COMPREHENSIVE VISIBILITY

Identify misconfigurations, vulnerabilities, externally accessible systems & the security gaps they can cause, on-prem & in the cloud

UNIFIED ATTACK PATH MAPPING AND ANALYSIS

Put information into context for a better view of viable attack potential

ENHANCED PRIORITIZATION

Target remediation to close gaps to critical systems, resources & data

RISK SCORING

Track & trend risk scores for continuous improvement & benchmark against peers

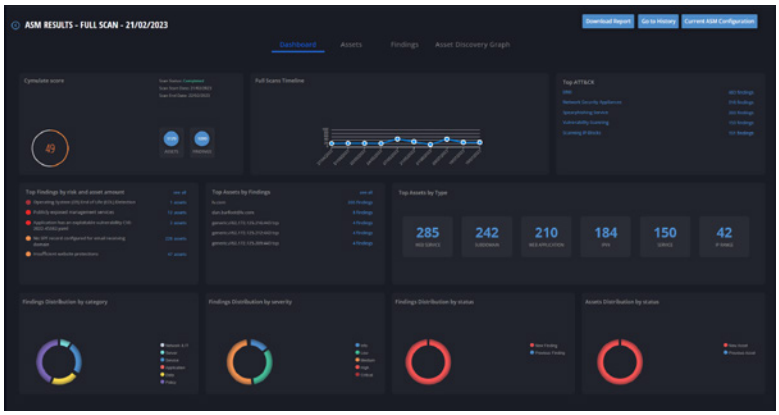
Discover High-Risk Internal Assets

Cymulate ASM includes internal ASM capabilities to map the internal attack surface with authenticated scans using user credentials to identify exploitable assets that an adversary can leverage to propagate from a foothold to crown jewels. A single light-weight agent facilitates seamless communication between customer devices and the Cymulate platform, ensuring timely updates and efficient transfer of operational data.

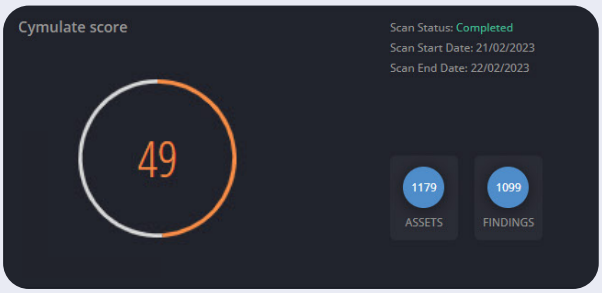
How it Works

- Scan for internal assets
- Run vulnerability and misconfiguration scans (on-premise and in the cloud) against the identified internal assets
- Perform deep analysis of the security issues and relationship between assets
- Identify vulnerabilities and security gaps with detailed recommended mitigations

Cymulate ASM Dashboard

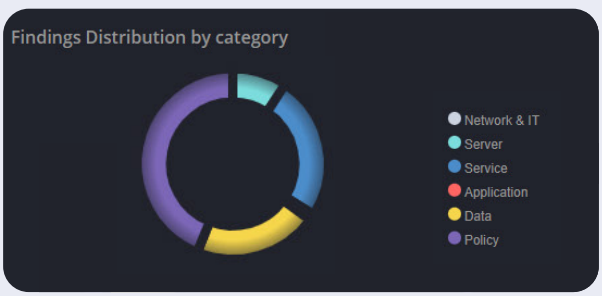


Overall Score
Security score based on simulated attack success rate correlated with industry standards.

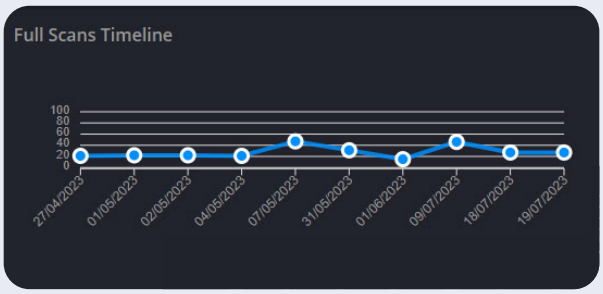


Top Findings
At a glance, expandable, view of top attacks, top assets and top findings.

Findings Distribution
Immediate understanding of findings distributions by category, severity or status, and asset status.



Trending
Easily follow the evolution of the attack surface security with a timeline reflecting the ASM module score at selected time intervals.



Map Attack Paths Across the Entire Organization

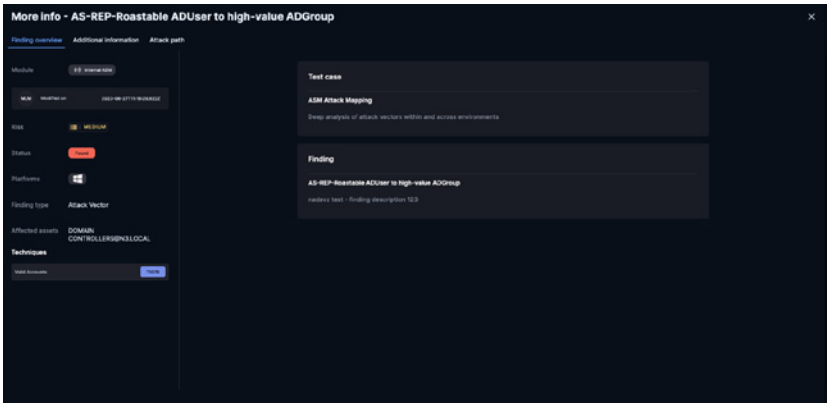
With findings from the internal attack surface, the **Cymulate ASM unified attack path mapping and analysis** capability maps attack paths across networks, cloud platforms (AWS, Azure, and GCP), and identity systems, including Active Directory services. Interconnections, trusts, permissions, and other factors can change the path of an attacker in unexpected ways, and having the ability to clearly identify and see these paths allows the organization to quickly identify and close gaps without disrupting business operations.

How it Works

- Map attack paths across networks, cloud platforms, identity systems, and Active Directory services
- Assess most crucial attack paths by degree of exploitability
- Identify which changes to process and technology would have the most impact on reducing risk

Findings Overview

View the related findings per scan. In each finding, view the risk, status, platform, and affected asset to identify areas of potential risk.



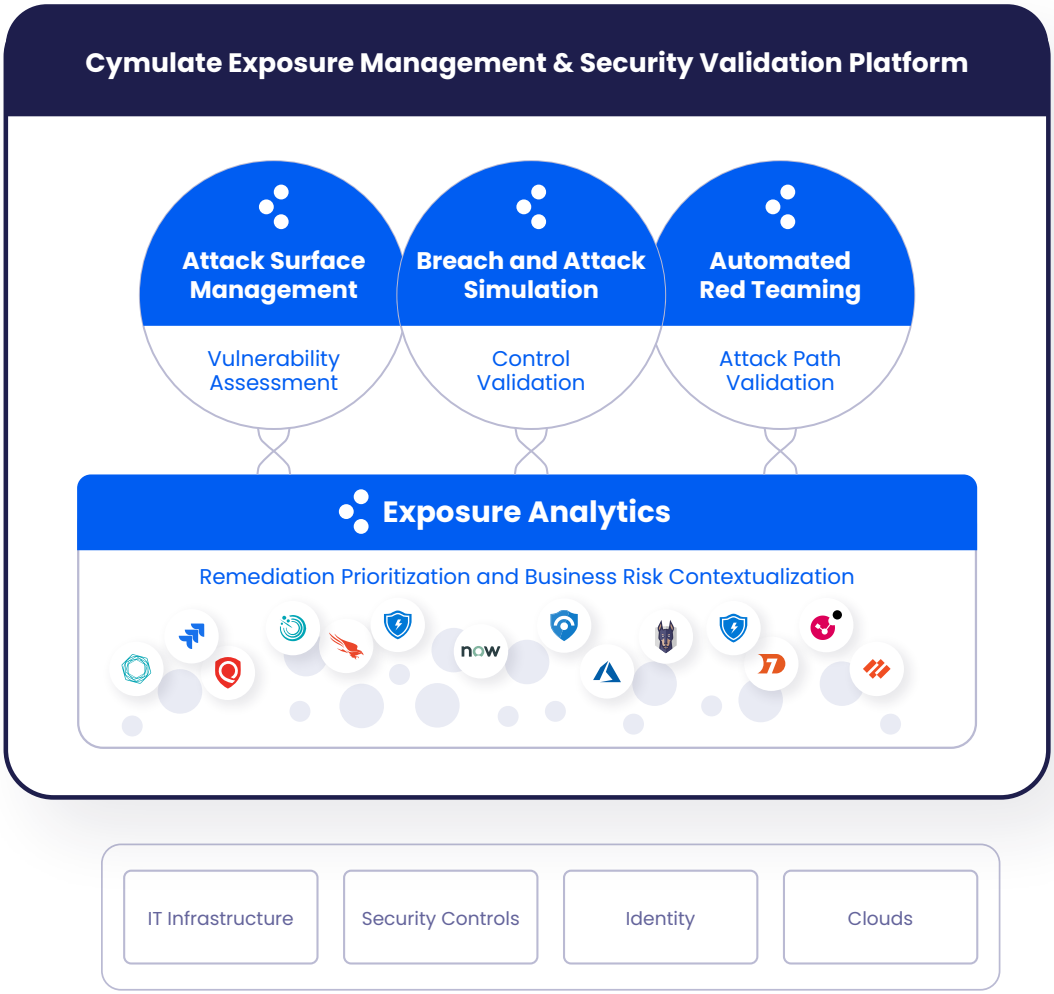
Attack Path Mapping

Visualize the interconnections between discovered assets, considering both legitimate relationships and relationships resulting from vulnerabilities and misconfigurations. The score of each relationship shown in the attack path corresponds to its level of risk and probability of exploitation—the higher the score, the higher the risk. Gain a clear and actionable understanding of an organization's internal security posture, enabling prompt prioritization and resolution of vulnerabilities.

Cymulate

The Cymulate Platform

Cymulate ASM is available both as a standalone SaaS offering and as an integrated offering within the Cymulate Exposure Management and Security Validation Platform. The Cymulate platform provides a comprehensive and scalable solution for security leaders, regardless of their security posture maturity, to drive their continuous threat exposure management program and support both the technical and business requirements of scoping, discovery, prioritization, validation, and mobilization.



About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience — before an attack occurs. More than 500 customers worldwide rely on the Cymulate platform to drive their threat exposure management programs from scoping through discovery, prioritization, validation, and mobilization. The Cymulate platform automates the attacker's perspective to help organizations of all sizes understand threat exposure, how controls and processes respond to threats, and the improvements they can make to mitigate exposure risk. For more information, visit www.cymulate.com.

Contact us for a private demo

Start Your Demo

info@cymulate.com | www.cymulate.com