SOFTPROM cymulate

DATA SHEET

Cymulate Attack Surface Management (ASM)

Discover Threat Exposures and Prioritize Remediation

Cymulate Attack Surface Management (ASM) identifies assets exposed to unapproved access, exploits and other attacks. Cymulate ASM automates the attacker's view of your on-prem, cloud and hybrid environments by scanning autonomous system numbers (ASN), domains (email and web), subdomains, IPs, ports, services, applications and cloud platforms to identify all assets within your organization's IT infrastructure. The platform also scans the dark web for sensitive information and indicators of data leaks and cyber attacks.

These scans provide a comprehensive assessment of vulnerabilities, misconfigurations and over-provisioning, enabling organizations to prioritize and address potential risks to strengthen their security posture. Cymulate ASM empowers organizations to manage their attack surface proactively, combining advanced scanning, detailed insights and strategic mitigation to enhance their security posture effectively.

See Every Asset from the Attacker's View

After providing one or more primary assets (such as a web domain), Cymulate ASM maps the external attack surface by emulating reconnaissance and probing methods of threat actors to identify all 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.

How it works

1. Automatically scan for internet-facing (external) assets
2. Tag important assets to highlight their significance
3. Automatically run vulnerability and misconfiguration scans against all found external assets
4. Prioritize discovered vulnerabilities and misconfigurations according to the probability of exploitation and the importance of the asset
5. Remediate prioritized and exploitable security gaps

> Cymulate Attack Surface Management provides another pair of eyes for us to understand what an attacker sees when looking at our organization from the outside.
> - Karl Ward, Head of Cybersecurity, LV=

Backed by the Industry

GIGAOM RADAR REPORT LEADER 2024 OPERATIONAL TECHNOLOGY (OT) SECURITY

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENCE MAGAZINE 2024

Cymulate ASM Benefits

Comprehensive visibility

Identify externally accessible systems and the security gaps they can cause – on-prem and in the cloud.

Enhanced prioritization

Close gaps in critical systems, resources and data with targeted remediation.

Risk scoring

Track and trend risk scores for continuous improvement and benchmark against peers.

Minimal operational overhead

Quickly deploy the agentless solution to identify, diagnose and validate your attack surface.

Cymulate ASM dashboard

The Cymulate ASM dashboard summarizes campaign results information. Clickable elements within the dashboard open the relevant assets or findings results. Dashboard highlights include:

- **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 the findings distributed by category, severity or status and asset status.
- **Trending** – Easily follow the evolution of the attack surface security with a timeline reflecting the Cymulate ASM score at selected time intervals.

Asset Discovery Graph

Cymulate ASM displays a graph of all found assets and how they link to one another, showing the hierarchy of the discovery. Each asset icon is color-coded according to type (domain, subdomain, IPv4, etc.). Clicking on an asset icon will open a window displaying more information about that asset.

The ASM dashboard displays information on general campaign results, while the asset discovery graph shows how each found asset is linked to one another.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

Get a Demo