cymulate

DATA SHEET

Technology Integrations

Cymulate Exposure Management automates threat validation by turning theoretical risks into proven, actionable insights — enabling security teams to prioritize truly exploitable exposures and efficiently close the most critical security gaps to strengthen threat resilience.

The Cymulate Exposure Management Platform seamlessly integrates with a wide range of security controls, IT infrastructure, cloud platforms and configuration management tools. By integrating with security controls, Cymulate validates detection capabilities by assessing how effectively threats are prevented and identified, attributing detection outcomes to the relevant integrated security technologies. After aggregating data across all integrations, Cymulate calculates true exposure scores that factor in validated existing security control mitigations, threat intelligence and business context. This enables security teams to focus on their riskiest exposures.

Focus on true exposure

Correlate control effectiveness, threat intel and business context to prioritize validated threat exposure.

Validate security controls

Automate continuous testing of threats techniques and attack paths with real-world attack simulation.

Optimize security controls

Tune security controls and policies to close prioritized threat exposures with automated mitigations.

Improve threat resilience

Monitor security posture with the evidence of automated security validation, MITRE ATT&CK® coverage and lateral movement assessments.

EDR and Anti-Malware

Cymulate analyzes logs and alerts from endpoint detection and response (EDR) and anti-malware solutions to correlate attack simulations and validate endpoint security policies. Cymulate prioritizes exposure gaps and provides remediation guidance for configuration updates and custom mitigation rules that can be easily implemented into most endpoint security controls. Cymulate can also automatically push new IoCs to endpoint controls for immediate control updates.

CROWDSTRIKE	Microsoft	SentinelOne	CORTEX BY PALO ALTO NETWORKS	Trellix
cybereason	FORTINET	kaspersky	Taegis™ XDR	TANIUM.
Harmony Endpoint	CISCO SECURE	BlackBerry	Carbon Black.	SOPHOS

Vulnerability Management

Cymulate integrates with vulnerability management systems to provide a complete picture of the risk associated with known exposures. By correlating threat prevention and detection findings to data from vulnerability management systems, Cymulate calculates true risk scores to prioritize exposures and mitigations that deliver the most significant risk reduction.

tenable
RAPID7 insightVM
Qualys.
CROWDSTRIKE
Windows Defender

Cloud Security

Cymulate integrates with cloud native application protection (CNAP) and other cloud security tools to aggregate and analyze assets and exposure findings for a more comprehensive view of your organization's security posture. Cymulate maintains an extensive library of attack tests to validate cloud environments including AWS, Azure and Goole Cloud.

WIZ
CloudGuard

Network

Cymulate integrates with firewalls and other network security solutions to validate policies governing both inbound and outbound traffic by executing attack techniques used across the lifecycle from initial access and data exfiltration. Cymulate integrates with Zero Trust architectures to assess exposures related to credential access, privilege escalation, and lateral movement—uncovering exposures in access controls, identity management, and network segmentation across the internal attack surface.

paloalto NETWORKS
Guardicore
Now part of Akamai

Active Directory

Cymulate integrates with Microsoft Active Directory and Microsoft Entra ID (formerly Azure Active Directory) to validate access control policies and configurations delivering a more comprehensive view of identity and access security posture.

Microsoft Active Directory
Microsoft Entra ID

SIEM

Cymulate verifies and optimizes the effectiveness of security information and event management (SIEM) solutions in complex threat landscapes. Cymulate correlates logging and incident generation with assessments to produce a more complete picture of the efficacy of SIEM operations. By integrating with security controls, Cymulate validates detection capabilities by assessing how effectively threats are prevented and identified, attributing detection outcomes to the relevant integrated security technologies. For some SIEMs, Cymulate applies AI to map the SIEM rules to the Cymulate attack library for customized testing of each rule.

Azure Sentinel, splunk >, Chronicle part of Google Cloud, CROWDSTRIKE, Trellix, snowflake

McAfee, elastic, exabeam, IBM Radar, LogRhythm, aws

MICRO FOCUS ArcSight, NETWITNESS An RSA Business, RAPID7 insightIDR, SECURONIX, sumo logic, DEVO

SOAR

By integrating Cymulate with SOAR systems, organizations can leverage assessment data across other platforms and workflows, enabling greater automation and more streamlined compliance operations.

CORTEX XSOAR BY PALO ALTO NETWORKS

Resilient an IBM Company

Web Gateway

Cymulate integrates with secure web gateway (SWG) solutions to validate the effectiveness of their threat mitigation capabilities. For identified exposure gaps, Cymulate delivers clear, actionable guidance for fast and effective mitigation.

zscaler™

Ticketing

Integration with ticketing systems enables security teams to manage security tasks from within the Cymulate platform. This integration streamlines security ticket management so security and IT teams respond to threats faster, more efficiently and stay focused on what is most critical to the organization.

servicenow

Jira

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. For more information, visit www.cymulate.com.