cymulate

DATA SHEET

Cymulate Exposure Validation

Prove the Threat. Build Exposure-Informed Defenses.

The security era of detect and respond is over. Security teams need a proactive, continuous approach that validates their defenses against real-world threats and adapts controls before attackers strike.

Powered by agentic AI and the industry’s deepest attack library, Cymulate Exposure Validation delivers autonomous threat validation and cyber defense engineering that proves the state of your security and updates security controls based on your real-world exposure.

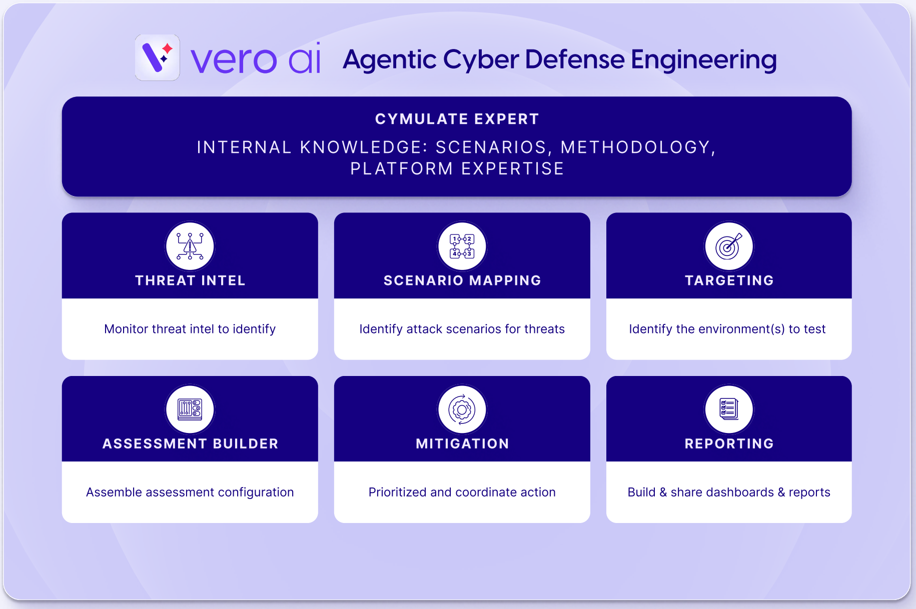
With a daily feed of new threats and the most complete attack library, Cymulate continuously tests your security controls against advanced threats and MITRE ATT&CK techniques. Cymulate integrates with security controls to understand response and build vendor-specific mitigations in the form of detection rules, IoCs and recommended updates.

Vero AI Tailors Validation to Your Threats and Environment

Cymulate Exposure Validation includes Vero AI to design, build and execute offensive testing specific to your environment and threats. With Vero AI, Cymulate provides near autonomous workflows for continuous threat validation that prove the state of your security and update your security controls based on your real-world exposure.

Vero AI provides an agentic system to:

- Analyze the latest threat intel for what is relevant to you
- Recommend custom assessment templates
- Create new assessments based on user-supplied threat intel
- Prioritize threat mitigation based on findings
- Generate custom reports that summarize threats and actions



Benefits

<1 Hour to Test New Threats & Update Controls

Automate continuous validation with daily updates of new attacks and recommended mitigations.

>90% Threat Prevention

Optimize threat prevention by finding gaps and updating security controls.

50% ↑ Threat Detection

Build, test and tune new threat detections in hours, not weeks.

60% ↑ Team Efficiency

Automate and streamline the most critical and resource-heavy tasks in modern SecOps.

Gartner Peer Insights Customers’ Choice 2025

>300 5-star reviews

Test with the Most Complete Attack Library

Cymulate Exposure Validation automates continuous testing with the industry's most comprehensive library of attack scenarios, spanning the full kill chain and aligned with the MITRE ATT&CK framework. The daily threat provides updates for the latest attacks and campaigns.

Ready-to-use templates configure and chain together the attack scenarios for best practices, threat categories, known APTs and specific campaigns. The attack scenario workbench allows users to build and modify testing.

Cymulate Exposure Validation tests defenses against:

- APT groups
- Vulnerability exploits
- ATT&CK tactics and techniques
- Ransomware threats
- Malware, worms and trojans
- Production platform risks
- Software exploits
- Emerging threats from daily feeds

Virtual Patch and Build Detections with Cyber Defense Control Plane

Unlike automated penetration testing and red teaming, Cymulate Exposure Validation includes a cyber defense control plane that integrates with more than 50 security controls. This cyber engineering control plane creates the connections to understand how controls respond to threats, build new detection logic and deploy updates to block and detect what was missed.

As part of an engineering-native platform, Cymulate attack simulations include unique identifiers for accurate tracking and results of security control telemetry, logging and alerting. This allows for confident analysis of detection without affecting security logs and events in production.

With clear insight into control performance, Cymulate highlights missed attacks and provides actionable mitigation guidance, including virtual patching and behavioral detection rules. These vendor-specific updates can be applied directly to security controls or automatically pushed to controls with Cymulate Auto Mitigation.

Measure and Benchmark Threat Resilience

Cymulate provides a unified view of your security posture, backed by continuous exposure validation, real-world testing data and AI-powered insights. The platform delivers operational metrics, board-ready reports and benchmarking against industry peers, giving you a clear picture of how resilient your organization truly is. Mapped to frameworks like MITRE ATT&CK, CIS and NIST 800-53, Cymulate generates scorecards, heatmaps and control coverage insights to validate threat readiness, demonstrate progress and drive informed decision-making across technical and executive stakeholders.

Why Choose Cymulate?

Complete threat coverage

The most comprehensive threat library that enables validation across the full attack lifecycle – plus daily updates for the latest threats.

AI-powered environment and context mapping

AI personalizes what to test, what matters and what to do next based on your assets, industry, controls, and exposures.

Defense engineering control plane

A closed-loop system that turns validation into continuous improvement across controls and threat detection.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.

Get a Demo