cymulate

DATA SHEET

Cymulate Platform

Agentic Cyber Defense Engineering

Security leaders know they'll never patch fast enough to stay ahead of the next attack – and they can't rely on vendors to tune defenses to their unique apps, exposures and business priorities.

Cymulate helps you close the gap between identifying and mitigating risk, faster and with less effort. Driven by agentic AI and the industry's deepest attack library, Cymulate delivers autonomous threat validation and cyber defense engineering that proves the state of your security and updates your security controls based on your real-world exposure.

Prove the Threat. Build Exposure-Informed Defenses.

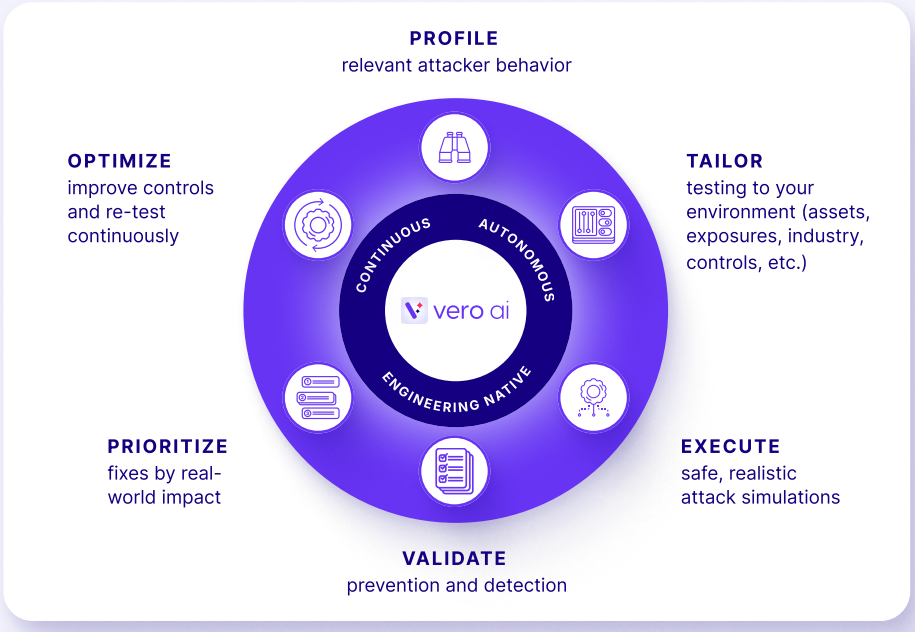
Cymulate delivers industry-leading adversarial exposure validation to continuously test your security against the largest, most complete attack library and daily updates for the latest threats.

Beyond validation, Cymulate includes a cyber defense control plane that integrates with your security stack to understand control response and automate a closed-loop system for cyber defense engineering. Cymulate turns validation into a continuous, adaptive process for proactive security that includes:

- Insights to control response to attack simulation
- Threat updates pushed directly to security controls
- Exposure mitigation for vulnerabilities
- New and modified detection logic

Automation and Intelligence Powered by Vero AI

To make validation and cyber defense engineering easy and autonomous, Cymulate includes Vero AI, an agentic system to tailor testing, mitigation and workflows to your environment, threats, security controls and business objectives.



Benefits

>90% Threat prevention

Optimize threat prevention by finding your weaknesses and updating security controls.

50% ↑ Threat detection

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

Save 60 hours per month

Continuous threat validation and adaptive security control updates.

Test new threats in <1 hour

Automate continuous validation of threats with daily updates of new attacks and campaigns.

Gartner Peer Insights Customers' Choice 2025

>300 5-star reviews

Cyber Defense Engineering

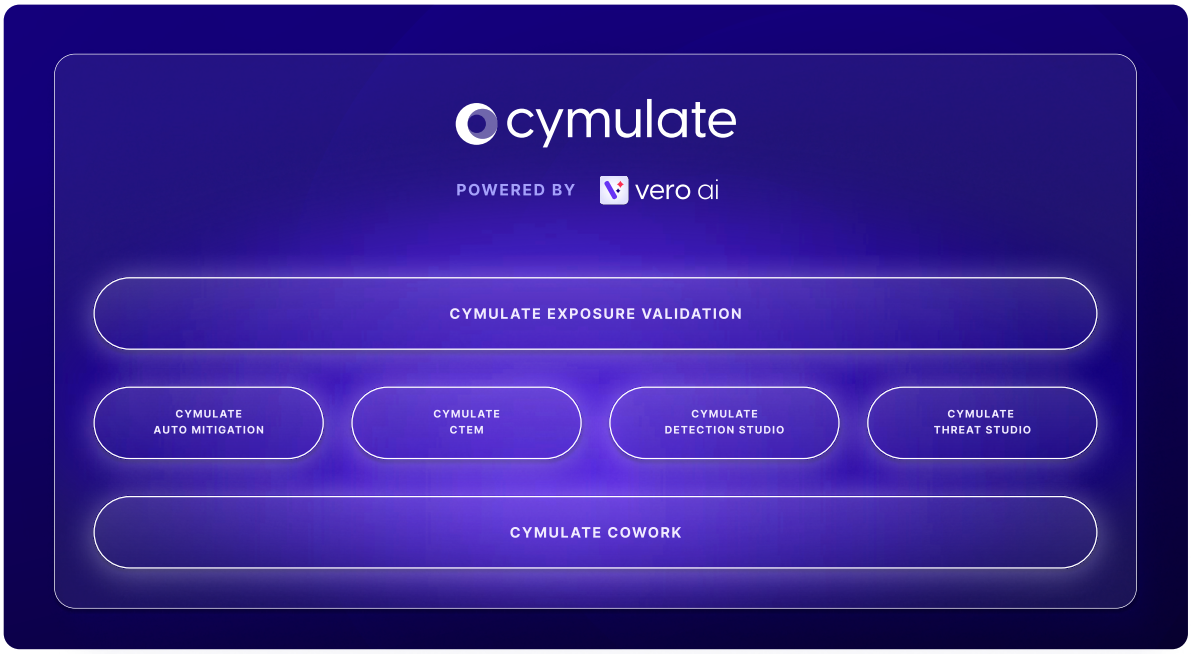
While continuous testing identifies risks and gaps, Cymulate goes beyond validation to deliver agentic cyber defense engineering for an autonomous approach continuous improvement. Security leaders, security operations and red teams rely on Cymulate for:

- **Threat validation** and continuous testing of controls against MITRE ATT&CK techniques and the latest threats
- **Detection engineering** that intelligently maps SIEM rules to attack library, validates telemetry and detection logic and creates new detection rules
- **Exposure prioritization and mitigation** based on validated control effectiveness to prevent or detect exploits and immediate security control updates that mitigate the threat

The Cymulate Platform

With Vero AI integrated throughout the platform, Cymulate delivers an integrated platform that goes beyond validation to engineer cyber defenses for your specific threats and exposures. The Cymulate Platform includes:

- **Cymulate Exposure Validation** for continuous threat validation and security control integrations
- **Cymulate Auto Mitigation** to deploy threat and detection updates directly to security controls
- **Cymulate CTEM** to integrate with vulnerability scanners, validate CVEs and prioritize exposures
- **Cymulate Detection Studio** to build, test and manage detection with AI that maps SIEM rules to attack library
- **Cymulate Threat Studio** to build custom attack chains with attack library and custom attack scenarios
- **Cymulate Cowork** to manage autonomous workflows and create custom routines based on agents, AI skills and trusted integrations



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

Autonomous, AI-driven usability and workflows customize validation for your environment with intent-aware execution of what comes next.

Defense engineering control plane

A closed-loop system that turns validation into continuous improvement (prove → prioritize → improve → re-prove) across controls and threat detection.