DATA SHEET

Cymulate Exposure Validation

Validate Threats, Optimize Resilience

Cybersecurity can no longer rely only on reactive defenses. Security teams need a proactive, continuous approach that validates their ability to withstand real-world threats before attackers strike. This is the essence of threat resilience.

Cymulate Exposure Validation empowers you to take control by continuously testing your defenses across the full kill chain using the latest adversarial techniques. With automated testing and actionable insights, you can:

- Prove resilience against advanced cyber attacks
- Optimize security controls to close gaps and reduce risk
- Accelerate detection engineering
- Measure and baseline your security posture

Validate Made Easy with Automation and AI

Powered by breach and attack simulation (BAS) with easy AI-guided workflows, Cymulate Exposure Validation delivers empirical proof of threat resilience through live, offensive testing. This threat-first approach exposes strengths and weaknesses across your prevention and detection, providing a clear, measurable view of your ability to withstand real-world attacks.

With the deepest collection of attack actions that cover the complete kill chain and MITRE ATT&CK framework, Cymulate combines templates for best practices with threat intelligence that automatically incorporate emerging attack scenarios. Paired with a daily-updated threat intelligence feed from the Cymulate Research Labs, your validation efforts stay in sync with the latest real-world threats and TTPs.

With Cymulate, you can validate 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

Create Custom Attacks in Minutes with AI

Cymulate AI-powered workflows create realistic, multi-stage attack chains without requiring deep scripting knowledge. Cymulate streamlines this process by removing the technical and complexity barriers when creating advanced attacks.

Through plain language prompts or URLs of threat advisories, users can type in plain text, such as “Simulate lateral movement in a cloud environment” or paste the URLs of threat intel to map relevant tactics and techniques from the library of real-world attack scenarios.

Benefits

Test new threats in <1 hour

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

30% ↑ in threat prevention

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

3x ↑ in threat detection

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

60% ↑ in team efficiency

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

Backed by the Industry

Optimize Threat Resilience

Cymulate simplifies control optimization by integrating with your security ecosystem — SIEM, SOAR, EDR, XDR, firewalls and more — through robust API connectivity. By embedding into existing workflows, Cymulate ensures that every assessment leads to tangible, continuous improvement, transforming exposure validation from a static report into a dynamic driver of threat resilience.

For identified security weaknesses, Cymulate provides actionable guidance to immediately improve threat resilience in the form of: control-ready threat updates for immediate prevention, custom detection rules formatted for specific SIEM, EDR and XDR platforms and tuning guidance to improve prevention and minimize false positives. Once updates are in place, your team can re-run assessments to validate that threats are blocked or quarantined and that alerts trigger as expected, ensuring a fast, accurate response to evolving threats.

Measure and Benchmark Cyber 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. AI accelerates analysis by delivering concise breakdowns of key findings, giving both technical teams and leadership fast, actionable intelligence to validate readiness, identify gaps, and guide remediation efforts.

Mapped to frameworks like MITRE ATT&CK and NIST 800-53, Cymulate generates scorecards, heatmaps and control coverage insights to help validate threat readiness, demonstrate progress and drive informed decision-making across technical and executive stakeholders.

Expand your Validation Capabilities into Exposure Management

Upgrade from Cymulate Exposure Validation to the complete **Cymulate Exposure Management** to consolidate validation, prioritization and mobilization. By integrating with vulnerability scanners and other exposure discovery tools, **Cymulate Exposure Management** stack ranks exposures with analysis that includes proof of threat prevention and/or threat detection. This focuses your security team on the exposures that pose real risk and drives measurable reduction.

The Cymulate Platform also includes options for:

- **Automated Mitigation** — Push threat updates directly to security controls for immediate threat prevention
- **Cloud Security Validation** — Validate cloud infrastructure, web apps, databases and identity policies using templates aligned with best practices and advanced attack campaigns targeting AWS, Azure, Google Cloud and Kubernetes
- **WAF Validation** — Test and optimize web application firewalls with attack simulation of OWASP and other threats specific to web applications
- **Attack Creator** — Customize multi-stage attacks across the entire adversary lifecycle with a user-friendly workbench to add custom attack actions and fully validate your security across the architecture
- **Attack Path Discovery** — Test for privilege escalation and lateral movement, uncover hidden attack paths, assess real-world exposures and reveal how far an attacker can go in your network to reach critical data and act maliciously

Why choose Cymulate?

Continuous Threat Validation

Best-in-class exposure validation with a single platform to optimize controls, scale offensive testing and provide essential exposure insights.

Simple Automation

Advanced testing for any blue or red teamer to run and customize with templates, best practices and AI assistant to scale offensive testing.

Trusted Results

Remove skepticism with evidence of exploitability and confidence to integrate automated testing in exposure management.