cymulate

SOLUTION BRIEF

Control Validation and Optimization

Security teams should not assume controls are working just because they are deployed, enabled or configured. Control drift, rule regressions, telemetry gaps and environment changes can quietly weaken prevention, detection and response coverage over time.

Cymulate control validation continuously proves whether prevention, detection and response controls perform as intended and then helps teams tune, improve and retest them over time. By measuring effectiveness, identifying gaps and retesting after improvements, Cymulate helps security teams improve detection quality and prove security control performance over time.

Prove your controls. Optimize security effectiveness.

Cymulate continuously validates prevention, detection and response security controls with production-safe testing. The results expose control gaps and drift, then guide prioritized tuning, automated remediation where possible and closed-loop retesting to optimize performance.

With Cymulate, organizations can:

- Validate prevention, detection and response controls against realistic attack behavior
- Measure gaps in rules, telemetry, configurations and coverage based on validated outcomes
- Optimize controls through prioritized tuning, Mitigation Hub workflows, automated updates and closed-loop retesting

Validate controls continuously

Cymulate safely tests controls in production environments to validate performance against realistic attack behavior. Security teams can confirm whether preventive controls block expected activity, whether detections are triggered correctly and whether response workflows operate as intended.

Key capabilities include:

- Full attack lifecycle validation with the most comprehensive threat library
- Verification that preventive controls and response workflows perform as intended under realistic conditions
- Integrations with more than 70 controls to validate telemetry and alerting of attack simulations
- Integrations with SIEM to map existing rules to attack library with Cymulate Detection Studio
- AI-powered, environment-tailored validation across assets, telemetry sources and the control stack

Solution Benefits

90% threat prevention with existing controls

40 hours saved each quarter testing controls

81% improvement in security risk score in 4 months

Cymulate validates and optimizes:

- EDR
- AntiVirus
- SIEM
- Email
- SWG
- DLP
- CWPP
- K8s
- IPS/IDS
- WAF
- SOAR
- CDR

> Cymulate ensures we get the most out of our security controls. It gives us accurate and timely assurance regarding the posture of our security program.
>
> – Head of Cybersecurity, Financial Services

Measure effectiveness, drift and coverage gaps

Cymulate gives security teams measurable evidence of control performance. Instead of relying on configuration status or vendor coverage claims, teams can see what was prevented, what was detected, what failed and where confidence is low.

Operational teams can use these insights to find gaps in telemetry, parsing, policies and detection logic. Security leaders can use outcome reporting to demonstrate validated improvements, reduced false confidence and a stronger security control posture over time.

Key capabilities include:

- Control effectiveness metrics
- Prevention, detection and response measurement
- Coverage and gap analysis
- Drift monitoring
- MITRE ATT&CK, CIS and NIST mapping
- Executive and operational reporting

Optimize and improve controls

Validation only creates value when it leads to action. Cymulate turns failed validations into prioritized tuning guidance so teams know what to adjust, which controls to harden, where to improve logging and how to reduce operational risk.

After changes are made, Cymulate supports closed-loop retesting to confirm that improvements worked and did not introduce regressions. With Mitigation Hub and Auto Mitigation, teams can operationalize remediation, route work to the right owners and automate control updates where appropriate.

Key capabilities include:

- Guided tuning recommendations
- Prioritized optimization based on validated risk
- Mitigation Hub workflows to accelerate remediation and control improvements
- Auto Mitigation for quick control updates and mitigation actions
- Closed-loop retesting
- Measurable proof of improvement

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 detection engineering for your environment.

Cyber defense engineering control plane

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. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.