SOLUTION BRIEF

Security Control Validation

Are Your Security Controls Operating as Intended?

Despite years of investment, security leaders struggle to answer the basic questions of “Are we exposed?” and “Where are my biggest gaps?”. The answers become more uncertain when faced with the daily evolution of threats and digital transformation projects that adopt new technologies, migrate applications to the cloud, and integrate internal systems with supply chain partners.

Testing and proving cyber resilience are especially challenging for smaller teams that outsource security operations or rely on managed service providers. With or without a managed service, security leaders struggle to:

- **Test controls against the latest emerging threats**
- **Know the current state of their cyber program – both strengths and weaknesses**
- **Prioritize resources and investments to optimize existing controls or implement new technologies**

Continuously Validate and Optimize Security Controls

Security operations leaders must constantly validate the effectiveness of their security controls against the latest emergent threats facing their organization.

The Cymulate Exposure Management Platform automates production-safe breach and attack simulations for offensive testing that continuously validates security controls using the latest threat tactics and real-world attack techniques.

Automated Security Control Validation Assessments

- Immediate threats
- Endpoint security
- Cloud security
- Email gateway
- Web gateway
- Web application firewall
- Network security
- Data loss prevention
- SIEM detections

The results of these assessments highlight the gaps and weaknesses in your security defenses and provide you with remediation guidance to tune and optimize your controls. As a SaaS solution designed for simple and fast deployments, the Cymulate security control validation solution enables organizations to fortify their cyber defenses, reduce their exposure to cyber threats and prove their state of cyber resilience.

> **You can configure your security solutions to the best of your ability, but you can’t just trust that they will protect you from all the threats out there. Cymulate allows us to validate that our solutions are tuned correctly and that we can do this continuously in different environments.**
>
> – Kevin Roberts, Information Security Analyst, NedBank

Solution Benefits

Continuous control validation

Continuously assess your security control effectiveness.

Fortify security defenses

Find gaps and weaknesses in your cyber defenses.

Increase cyber resilience

Optimize your controls to be more resilient to cyber attacks.

Reduce exposure risk

Reduce your exposure to immediate threats.

Backed by the Industry

FROST & SULLIVAN

FROST RADAR LEADER

cymulate

Frost Radar™ :Automated Security Validation, 2024

Gartner Peer Insights Customers’ Choice 2023

Automated Security Control Validation

The Cymulate Exposure Management Platform provides automated security control validation using breach and attack simulations to assess the effectiveness of critical security controls and identify weaknesses that could expose you to the latest threats facing your industry.

Automate continuous testing

Cymulate includes pre-packaged templates and advanced attack scenarios to both validate individual security controls and test the security stack against full kill-chain attacks and malicious behaviors used by well-known threat actor APT groups.

- Comprehensive testing across critical security controls
- Daily updates to test controls against the latest threats
- AI-powered custom assessment generation using community threat intelligence articles
- Integrations with leading security vendor solutions for SIEM, SOAR, GRC, EDR, firewall and ticketing systems
- Create custom attack scenarios with chained test executions to simulate sophisticated threats to your environment

Optimize controls before the next cyber attack

For every identified control weakness, Cymulate provides the insights, guidance and automation to harden defenses.

- Actionable reporting and findings provide proof of breach feasibility and guidance for risk prioritization
- Mitigation guidance with specific policy tuning and customized detection rules that can be directly applied to controls
- Push control updates including the latest indicators of compromise (IOCs)
- Rerun assessments to validate updated controls are now operating as intended

Detect drift and baseline security posture

With ongoing automated testing, Cymulate identifies changes to the environment and provides proof of the current state of cyber resilience.

- Security control dashboards and MITRE ATT&CK heatmaps highlighting strengths, weaknesses and exposure levels
- Technical and executive level reports provide proof and evidence of security posture
- Achieve cyber resilience compliance for industry standards like PCI-DSS and DORA
- Identify drift in security control configurations and changes to environment that impact security posture
- Industry benchmarking to compare security effectiveness to peers

Why choose Cymulate?

Depth of attack simulations

Over 120,000 attack simulation resources from real-world attack scenarios for comprehensive testing of your security defenses.

Production safe

The full suite of attack simulations and test scenarios are completely production-safe and will not cause harm to your production systems.

Automated validation

The attack simulations are fully automated, enabling continuous validation of security controls and emerging threats.

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.

Get a Demo