SOLUTION BRIEF

Security Control Validation

Are Your Security Controls Operating as Intended?

Despite the investments in cybersecurity, security leaders still lack the confidence that their security defenses could withstand and attack from a sophisticated threat actor.

Security teams struggle to test their controls on a routine basis and understand their security posture (both strengths and weaknesses). This makes it difficult to know where to prioritize resources to remediate vulnerabilities and optimize defenses.

Continuously validating that security controls are operating as intended and capable of blocking attacks trying to exploit the vulnerabilities that exist in your IT environment, is one of the most critical steps in managing your exposure to cyber risks.

Continuously Validate and Optimize Security Controls

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

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

Automated Security Control Validation Assessments

- Endpoint Security (AV / EDR)
- Secure Email Gateway (SEG)
- Network Security (IDS/IPS)
- Cloud Security (CWPP, Cloud IDS)
- Secure Web Gateway (SWG)
- Data Loss Prevention (DLP)
- Kubernetes / Containers (K8S)
- Web App Firewalls (WAF)
- SIEM Detections / SOAR Playbooks

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, Cymulate 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

Know your exposure and reduce risk by tuning controls for today's threats.

Backed by the Industry

FROST & SULLIVAN
FROST RADAR LEADER
cymulate
Frost Radar™ Automated Security Validation, 2024

Gartner
Peer Insights
Customers' Choice 2024

Automated Security Control Validation

The Cymulate Exposure Validation Platform provides automated security control validation using breach and attack simulation and automated red teaming to test 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 kill-chain attacks and malicious behaviors used by well-known threat actor APT groups. Cymulate automates security control testing with:

- Comprehensive testing across critical security controls
- Daily updates to test controls against the latest threats
- AI-powered custom assessments created from community threat intelligence articles and plain text queries
- Integration with leading security vendors 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. Cymulate optimizes security controls with:

- 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
- Control updates and automation that includes the latest indicators of compromise (IOCs)
- Easy management to 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. Cymulate detects and benchmarks cyber resilience with:

- Security control dashboards and MITRE ATT&CK heatmaps highlighting strengths, weaknesses and exposure levels
- Technical and executive level reports that provide proof and evidence of security posture
- Automation that continuously validates security to meet the cyber resilience compliance for industry standards like PCI-DSS and DORA
- Drift detection that tracks security control performance and changes to the environment that impact security posture
- Industry benchmarking to compare security effectiveness to peers

Why choose Cymulate?

Depth of attack scenarios

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

Production-safe execution

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

Fully automated testing

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