

Cymulate Technology Partners

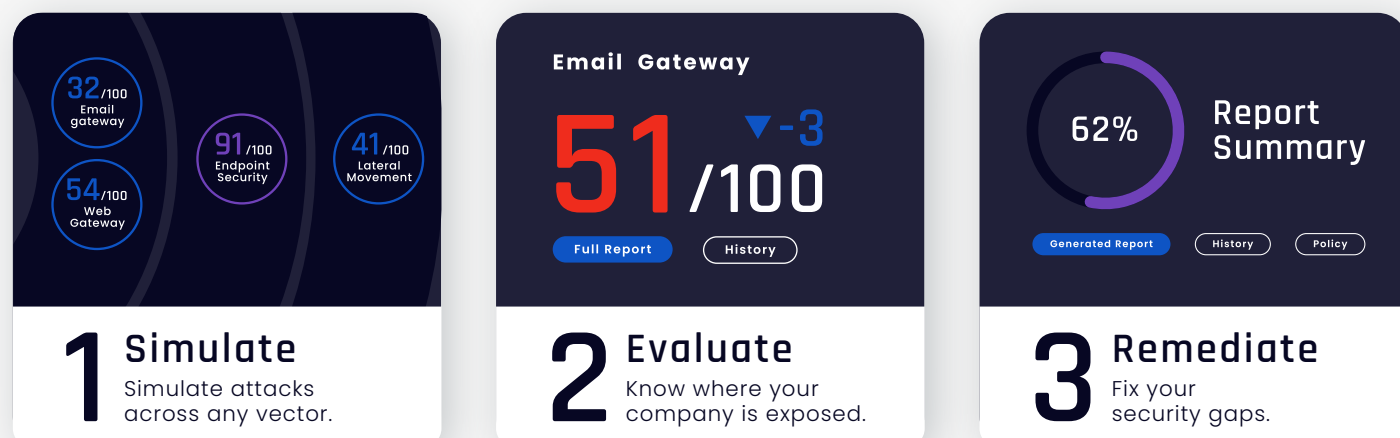
Cymulate SaaS-based continuous security validation makes it simple to measure and improve your security posture across the full attack kill-chain. Cymulate integrates with various technology partners to augment and benefit from existing security programs.

These integrations enable you to:

- Validate and improve EDR and SOC detect and respond capabilities
- Prioritize remediation efforts by correlating attacks to the findings of vulnerability management systems.
- Integrate Cymulate remediation guidance into automated workflows

How it works

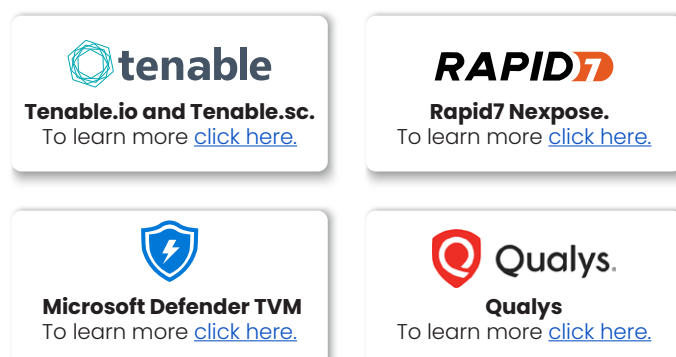
Cymulate facilitates managing your security posture 24X7X365 within minutes and based on facts, in just three simple steps:



Vulnerability management systems

Integration with vulnerability management systems correlates vulnerabilities and vulnerable assets with Cymulate attack results within the platform. This enables security practitioners to assess the asset risk level and prioritize remediation and patching efforts.

Cymulate integrations are available with the following solutions:



Logos for the following solutions:

- tenable**
Tenable.io and Tenable.sc.
To learn more [click here](#).
- RAPID7**
Rapid7 Nexpose.
To learn more [click here](#).
- Microsoft Defender TVM**
To learn more [click here](#).
- Qualys**
Qualys
To learn more [click here](#).

SIEM & EDR Systems

Integration with SIEM & EDR solutions enable the SOC team to validate that these systems detect Cymulate attack simulations by associating the alerts and events they generate with each attack and the specific attack indicators.

Cymulate integrations are available with the following solutions:




Microsoft Defender
Advanced Threat Protection (ATP)



SentinelOne
Autonomous Endpoint Protection



McAfee
Enterprise Security Manager (ESM)



VMware
Carbon Black



Splunk
Log Management & Analytics




IBM QRadar
Security Information & Event Management (SIEM)

SOAR and GRC systems

Integration with SOAR and GRC platforms enable enterprises to import Cymulate BAS security assessment results, risk scores and actionable remediation guidance. From these central management systems, they can access and view simulation results, create customized dashboards and utilize assessment data. This helps security practitioners to plan, manage and automate their remediation efforts.

Cymulate integrations are available with the following solutions:



RSA® Archer®
GRC Platform To learn more [click here.](#)



DEMISTO
A POLO ALTO NETWORKS COMPANY
Palo Alto Cortex XSOAR (Demisto)

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their CyberSecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company—and every company—will be.

Contact us for a live demo, or get started with a free trial

[Start Your Free Trial](#)