

Tenable Integration

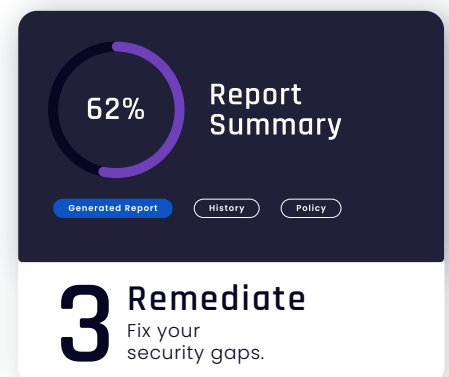
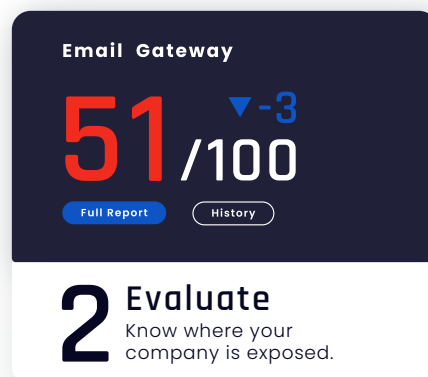
Solution Brief



Cymulate overview

Cymulate Breach and Attack Simulation (BAS) addresses the needs of companies to continuously test and optimize the operational effectiveness of their security controls in light of the changing attack surface and evolving security threats. For both cloud and on-premise environments,

our SaaS based platform proactively challenges security controls against the full attack kill chain by mimicking the tactics and techniques of an adversary. It enables continuous testing of your security controls anytime and from anywhere on the production environment.



Product Highlights

- With a few clicks, Cymulate challenges your security controls across the entire kill chain by initiating thousands of attack simulations.
- Reports are generated immediately to show you exactly where you're exposed and providing you actionable remediation guidance.
- With a Research Lab that keeps abreast of the very latest threats, Cymulate BAS is updated daily for you to verify that your security controls are operating at optimal effectiveness.
- Best practice templates provide extensive testing scenarios to discover misconfigurations and security gaps. In addition, we also provide high levels of customization.
- Cymulate is simple to deploy requiring one agent per environment for full testing capabilities.

Integration with Tenable

Cymulate integrates with various technology partners to augment a company's security testing program and to improve their detection and response capabilities.

Cymulate - Tenable integration correlates vulnerabilities and vulnerable machines to attack and threat simulations and ultimately to risk. The correlation helps you to:

- 01** Identify high risk, vulnerable machines that are susceptible to attacks.
- 02** Identify machines that can be exploited along a simulated lateral movement attack route.
- 03** Identify machines that are vulnerable to the latest threats found in the wild.

How it Works

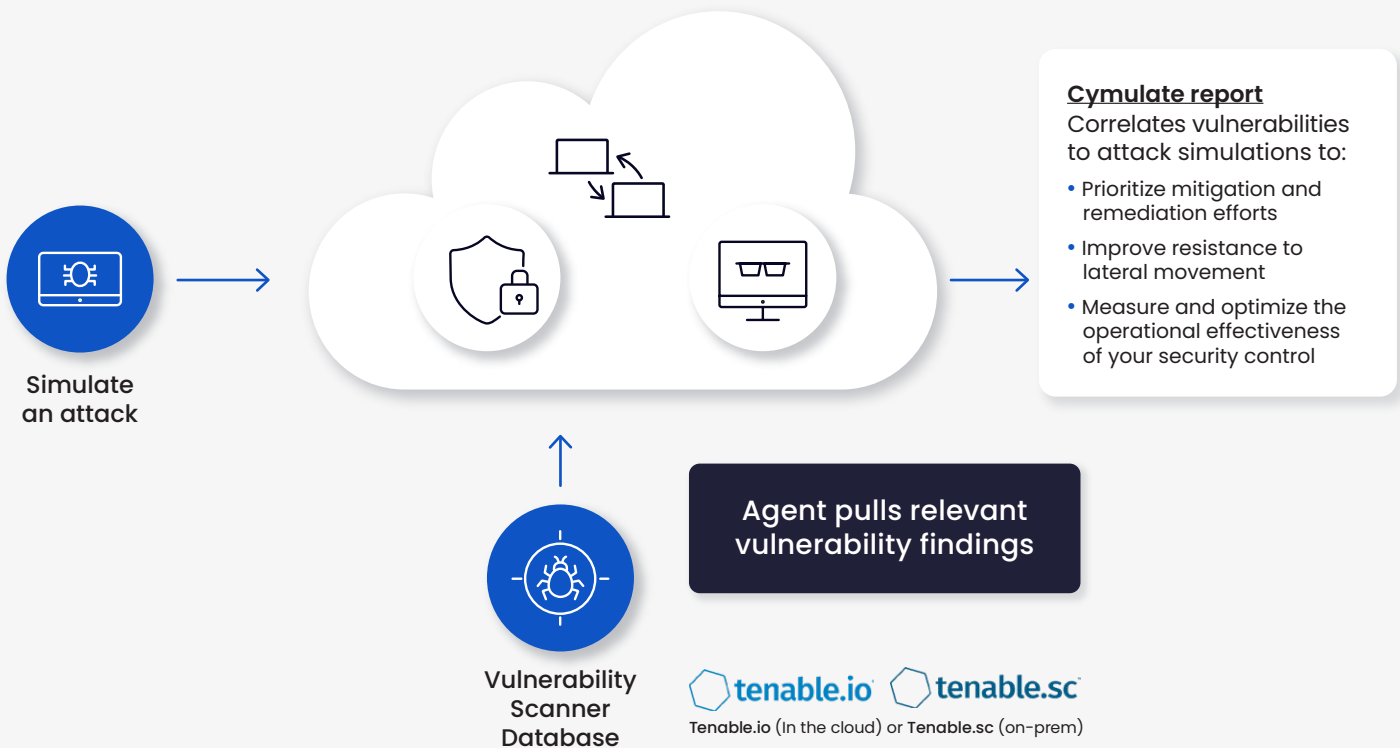
- 01** Vulnerability assessments are performed regularly using Tenable.
- 02** The Cymulate agent extracts relevant vulnerability findings for every applicable security assessment via the API.
- 03** The Cymulate agent combines the vulnerability findings with the security assessment findings and correlates them to create a comprehensive report.
- 04** Actionable insights help security teams to improve security controls and prioritize vulnerability remediation efforts.

The Benefits

- 01** Prioritize vulnerability remediation efforts.
- 02** Validate that security controls are safeguarding vulnerable machines.
- 03** Improve network configurations to increase resistance to lateral movement.

This is what EuroNext - The leading pan-European marketplace, had to say about Cymulate:

“ I would recommend Cymulate because of its ease of use, it can quickly provide you a window into how vulnerable or how protected your organization is against external threats ”



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](#)