

# Continuous Security Validation Made Simple

## Measuring your cyber posture seems impossible?

Every day brings change to your security posture. Changes in the IT architecture modify the attack surface, configuration changes to security controls introduce unforeseen security gaps and, the evolving threat landscape introduces new threats to avoid. It seems impossible to know how effective your security controls are right now and what requires fixing. You have tried penetration testing and other alternatives. But by the time you get their report, it is already outdated and irrelevant. There must be an effective and simple way to know you are secure, continuously.

## How it works

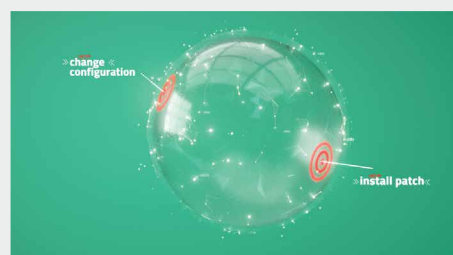
Cymulate lets you improve your security posture 24X7X365 within minutes, in just three simple steps:



**01** Simulate  
Attacks across  
the full kill chain



**02** Evaluate  
Controls to  
identify gaps



**03** Remediate  
With actionable  
guidelines

## Key platform capabilities

**In-depth validation** - By mimicking the myriad of strategies and tools attackers deploy, the platform challenges your company's security controls with thousands of simulated attacks that cover the MITRE ATT&CK framework in-depth. This comprehensive validation assesses your company's true preparedness to handle cybersecurity threats effectively.

**End to end validation** - Cymulate validates your security posture across the full attack kill chain: Reconnaissance, initial foothold, execution, command and control, lateral movement, and action on objective. It combines assessments of outside-in reconnaissance, security awareness, infrastructure resilience and security control validation in one platform.

## Simply know you're secure

Cymulate continuous security validation makes it simple to measure, track, and improve your security posture across the full kill-chain, including your 3rd party ecosystem. The SaaS-based platform deploys and provides results in minutes. Cymulate research labs updates assessments with new threats and TTPs daily. Additionally, red teams can customize attacks and attack flows. Assessments are mapped to the MITRE ATT&CK framework, scored and include actionable remediation guidance to mitigate risk and optimize security control effectiveness. Cymulate enables you to take data-driven decisions and manage your security resources efficiently.

**Third party security rating** - Cymulate Recon provides continuous and quantitative technical analysis and scoring for public-facing digital assets. It also discovers organizational and credential intelligence that a hacker can use in an attack. It enables you to measure, track and manage the external risks of your company and the indirect risks created through its digital business ecosystem.

**Test against the latest threats as they emerge** - Cymulate Research Lab stays abreast of the very latest threats, updating the platform on a daily basis with Immediate Threats Intelligence. This enables organizations to rapidly assess their resilience against the latest threats.

**Outcomes and reports** – An executive report is generated after every assessment. It scores the outcome of the assessment, summarizes the results, and provides high level countermeasure recommendations. The executive report also compares the score to previous assessments and to the score of industry peers. A technical report is also generated. It provides a description of each individual test or finding together with a risk level and actionable remediation guidance.

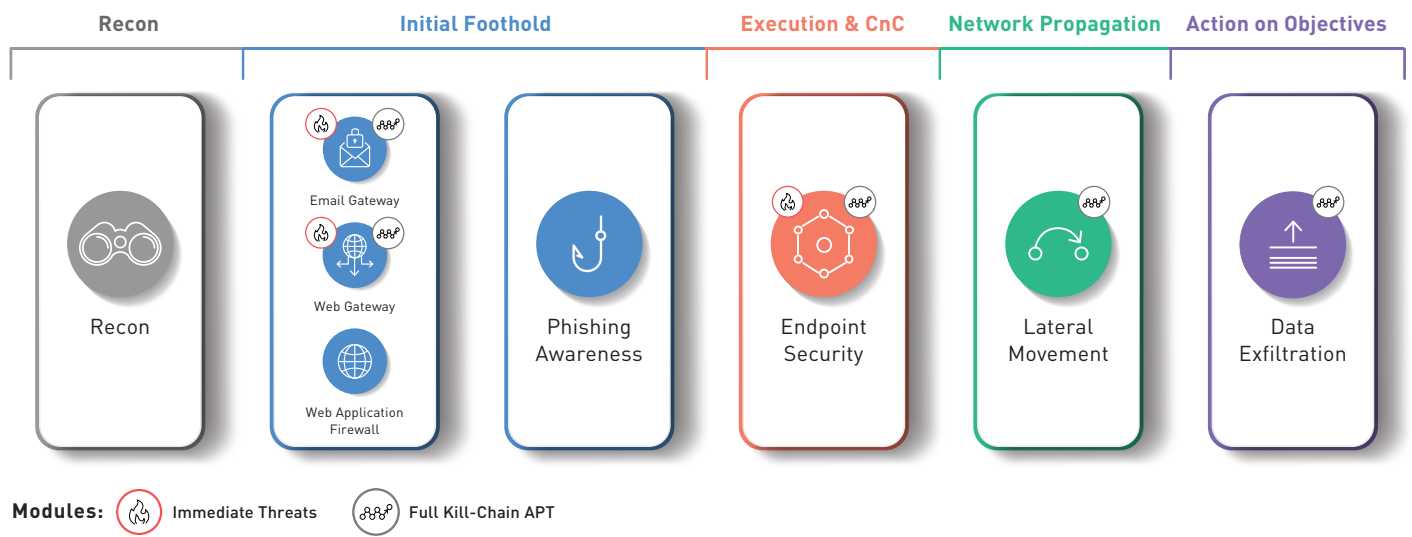
**Security Scoring** - Cymulate security scoring provides a measurement of your company’s security posture and the effectiveness of its security controls. The scoring system enables you to track and improve your security posture in addition to rationalizing security spend and the allocation of resources. The score is calculated using industry-recognized

standards; the NIST Risk Management Framework, CSVSS v3.0 Calculator, Microsoft’s DREAD and the MITRE ATT&CK™ Framework.

**Attack customization** – You can create and launch your own attack scenarios with simple to use templates that leverage the rich library of attack commands, malware and adversarial tactics and techniques, mapped to the MITRE ATT&CK framework.

**Integration partners** - Cymulate integrates with technology partners to augment existing security testing programs by correlating simulated attacks to their findings. These integrations enable you to validate and improve EDR and SOC detect and respond capabilities and prioritize remediation and patching efforts by correlating attacks to vulnerability management system findings

## End to end security validation



## Why Cymulate

- Deploys in minutes
- Simple to use
- Single agent, unlimited attacks
- SaaS-based platform
- Automated or on-demand
- Very latest threats simulated with a few clicks
- Covers the full attack kill chain

## Who we are

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security controls, allowing hyper-connected organizations 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 companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision-to make it 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 our partner for a live demo, or get started with a free trial [www.softprom.com](http://www.softprom.com)