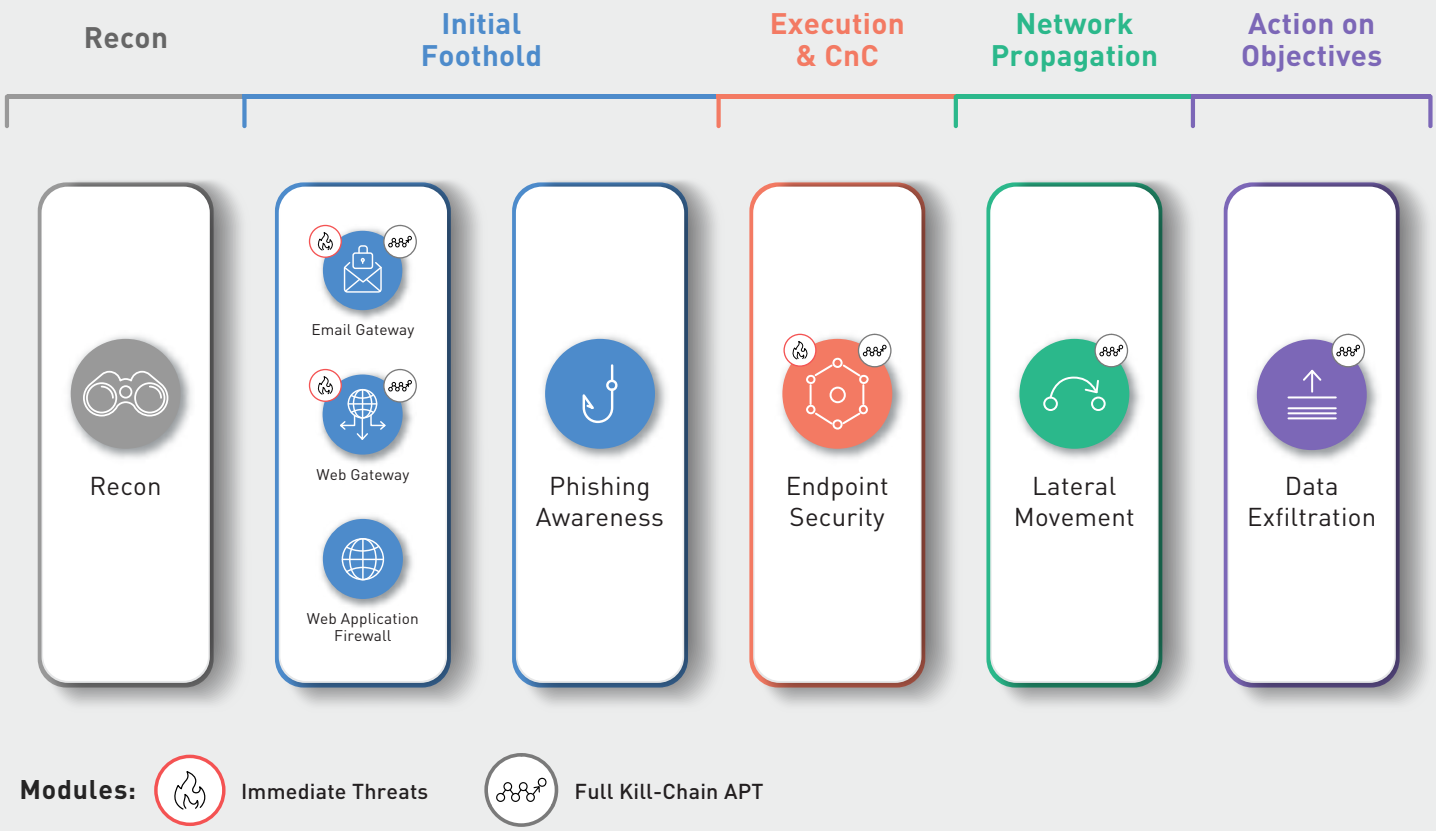
#1 In Continuous Security Validation

Ranked #1 in innovation by Frost & Sullivan in the 2021 BAS Radar™ Cymulate SaaS-based Breach and Attack Simulation (BAS) enables companies to continuously test and optimize the effectiveness of their security controls in light of the changing attack surface and evolving security threats.
The platform proactively challenges security controls and infrastructure by mimicking the tactics and techniques of an adversary via attack simulations. It enables security testing anytime, anywhere on the production environment without interruption to the business.
Simple to use, Cymulate is based on the expertise of professional and seasoned security practitioners. Out-of-the-box, best-practice templates provide extensive testing scenarios to discover misconfigurations and security gaps across the entire kill chain.
In addition, the platform provides high levels of customization for red-teams to create attack scenarios using hundreds of commands mapped to the MITRE ATT&CK framework.
Integrations with security systems, such as SIEM, EDR and vulnerability management systems augment existing security programs and improve SOC and blue-team performance.
Technical and executive reports show you exactly where you are exposed and provide you actionable remediation guidance. Please find hereunder a brief description of the currently available security assessments that enable end-to-end security testing.



Test with Intelligence

The Cymulate **Recon vector** discovers what a hacker can find out about your company during the initial information gathering phase of an attack. The module identifies and fingerprints your domains and sub domains to discover internet facing weaknesses and vulnerabilities. It also looks for Open Source Intelligence (OSINT) to uncover leaked credentials and organizational information that can be used in an attack.

Testing Your WAF Security

The **Web Application Firewall (WAF) vector** enables you to test and optimize your web security controls. This vector first identifies all the forms and other means of data import available on the target domain and then challenges the WAF against thousands of attacks, including OWASP top payloads, command injection and file inclusion attacks to assess the integrity of the WAF configuration and its blocking capabilities.

Email Security Testing

The **Email Gateway vector** enables you to test and optimize your email security posture. This vector challenges your email security controls against a comprehensive set of attacks by sending emails with attachments containing ransomware, worms, trojans, or links to malicious websites. The simulation reveals which malicious emails, file types and embedded files that could potentially reach your employees' inbox.

Securing Your Web Gateway

The **Web Gateway vector** validates your organization's web security controls. This vector challenges the controls that protect employees from both accessing and downloading malware from malicious and compromised websites. The vector tests inbound protection against thousands of different simulated malicious files and exploits, and outbound protection against a feed comprised of thousands of URLs, which are updated daily

Full Kill-Chain APT Simulation

Full Kill-Chain APT module enables you to test, measure and improve the effectiveness of your security controls against real-world advanced persistent threats. The module provides pre-defined templates for testing against well-known APT groups and enables red-teams to create their own APT attacks from tens of thousands of attack simulations across the entire kill chain, including Email, Web, Phishing, Endpoint, Lateral Movement and Data Exfiltration.

Endpoint Security Testing

The **Endpoint Security Assessment vector** enables you to test and optimize the effectiveness of your endpoint security. The vector challenges your endpoint security controls against a comprehensive set of attacks that simulate malicious behavior of ransomware, worms, trojans and other types of malware. Red-team testing enables the creation of custom attack scenarios using hundreds of commands across the cyber-attack kill chain, mapped to the MITRE ATT&CK Framework.

Cymulate

Safeguarding Your Internal Network

The **Lateral Movement (Hopper) vector** challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems. The vector simulates an adversary that has control over a single workstation and attempts to move laterally within the organization. The result of the assessment is a visualization of all the endpoints that the assessment was able to reach with a detailed description of the methods used for every hop. The assessment identifies infrastructure weaknesses, network misconfigurations and weak passwords, and provides guidance to remediate them.

Challenging Your DLP Controls

The **Data Exfiltration vector** enables you to test the effectiveness of your Data Loss Prevention (DLP) security controls and optimize them. This vector challenges your DLP controls with a broad range of synthetic regulatory, company confidential and custom data sets. The vector packages the data into different file types including images and office files and attempts to exfiltrate them using multiple exfiltration methods. The attack simulation results are presented in a comprehensive and easy-to-use format, allowing organizations to understand their DLP-related security gaps and take the appropriate measures to remediate.

Defending Against the Latest Attacks

The **Immediate Threats Intelligence module** enables you to safely test and optimize your organization's security posture against specific, real and emerging cyber threats.
The module is updated daily by Cymulate security analysts that monitor the web for new threats.
The Immediate Threats Intelligence module tests email, web gateway, and endpoint security controls.

Improving Security Awareness

The **Phishing Awareness vector** enables you to evaluate employee security awareness. It provides all the resources required to create, customize, launch and measure phishing campaigns.
Each campaign is tracked for 5 different actions (opening, clicking, entering credentials, reporting and completing a quiz) providing the full picture of employee security awareness levels, enabling the organization to focus on those that require more education and monitoring than others.

Who We Are

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security controls against the full attack kill chain, enabling organizations to avert damage and stay safe.
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 easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company - and every company - will be.

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

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: 31W 34th Street, 8th floor New York, 10001 | +1 212 6522632