Endpoint Security Assessment

Solution Brief

Endpoint Security Testing

Cymulate Endpoint Security Assessment Vector enables you to test and optimize your endpoint security posture. This vector challenges your endpoint security controls against a comprehensive set of attacks and together with the results, provides actionable remediation guidelines.

Securing the Endpoint

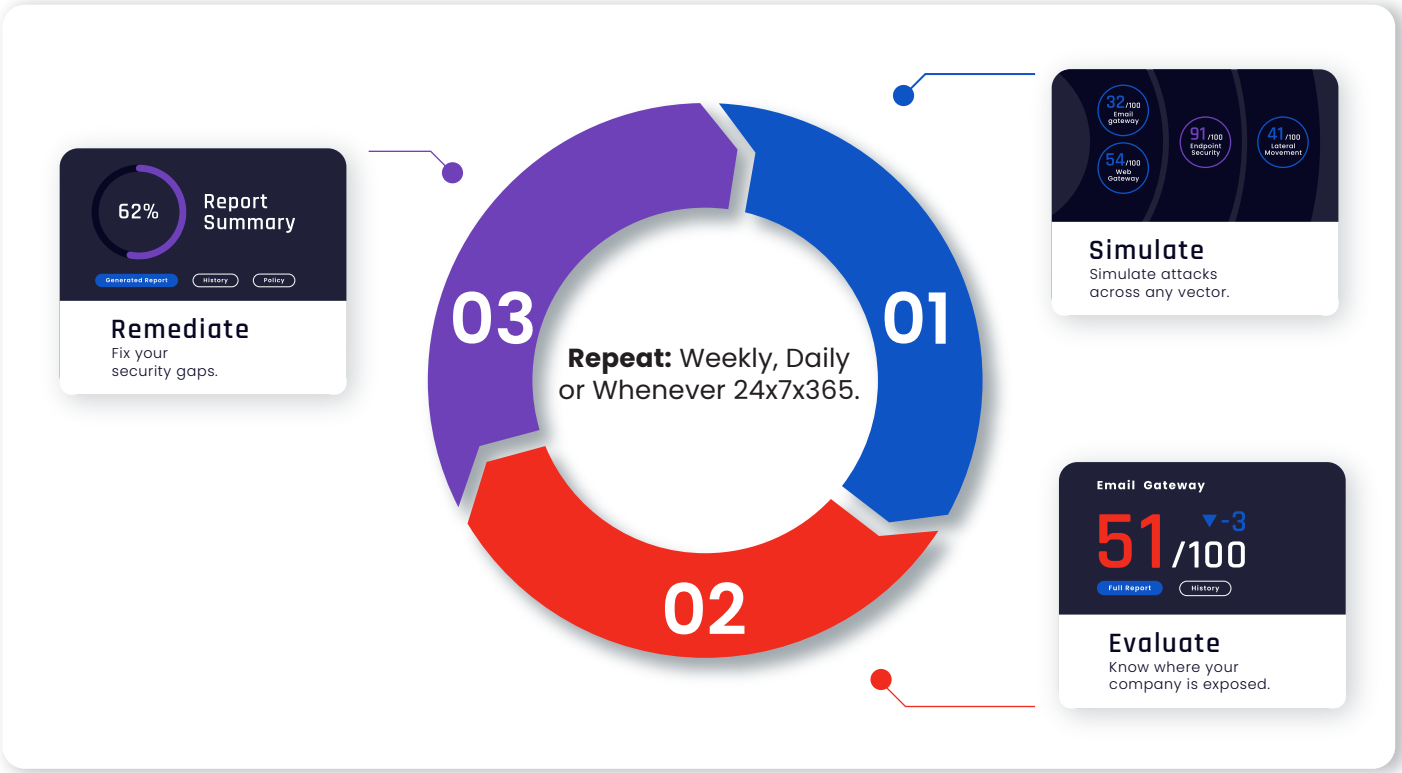
User workstations and endpoints are the most common target for initial foothold of a cyber attack, and a base for lateral movement within a compromised network.

That's why organizations invest heavily in endpoint protection platforms (EPP) and endpoint detection and response solutions (EDR). However, as repeatedly witnessed in the headlines and based on the Cymulate Research Lab's findings, endpoint security measures often fall short through lack of optimization and misconfiguration.

The best implementation will not be optimal within a few months or even weeks and will miss out on evolving variants of worms, ransomware and trojans, and fail to detect new hacker tools and tecniques.

Continuous testing

Testing of the endpoint against behavior and signature-based attacks, lateral movement and MITRE ATT&CK methods and commands will expose gaps. The Cymulate platform simulates scenarios that mimic the behavior of an adversary.
Based on the results, it identifies the security gaps and provides guidance to remediate them.
Continuous testing enables you to verify remediation efforts and maintain endpoint ecurity at optimal efficacy.



How It Works

Test setup - Endpoint security assessments are based on a library of templates available in the platform. Templates can be custom made by the end user or out-of-the-box. Each of the templates contain a library of malware types and attack methods and commands. Templates include:

Behavior based attacks - including ransomware, worm and trojan attacks.

Signature based attacks – updated daily, dropped to disk.

MITRE ATT&CK Execution methods and commands

- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Exfiltration

Customers can create their own templates based on combinations of malware and commands to build their own attack scenario to test their endpoint security against specific requirements and to validate that “blue-team” EDR and analytics solutions are identifying attacks accurately and taking appropriate responsive action.

Test Execution - Assessments can be executed on demand or scheduled. The testing is performed on a dedicated machine, where the Cymulate agent is installed to execute and report the results of the test. Tests can be initiated anytime from anywhere with one click.

Test Results and Remediation – After each test a technical and an executive security assessment reports is generated. The reports provide test results and guidance to remediate the gaps found by the test. Integration with SIEM and EDR vendor solutions provide the logs and alerts generated by these systems in the Cymulate platform.
The events and alerts are synchronized to the actions performed during the test, to help security teams validate accurate detection.

Key Features

Test using one dedicated machine which does not affect users or servers in the organization's network

Leverage Cymulate extensive library of commands mapped to the MITRE ATT&CK framework.

Run Cymulate best practice, out-of-the-box endpoint security assessments and your own custom attack scenarios.

Test continuously from anywhere, anytime

Execute from a collection of pre compiled behavior-based malware simulations, executed using different methods, without risk of business disruption.

Actionable Insights

The simulation results are presented in an easy-to-understand comprehensive report. Mitigation recommendations are offered for each security gap discovered, enabling IT and security teams to take the appropriate countermeasures.

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

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632