SOLUTION BRIEF

Endpoint Security Validation

Maintain Protection against Evolving Threats

Email may be the most frequently used delivery method for cyber attacks, but it is the endpoints that threat actors covet the most. Afterall, endpoints contain the systems and data that threat actors hold for ransom or provide the initial foothold for privilege escalation, lateral movement, and more.

And, with a 93% increase in ransomware attacks on endpoint devices costing an average of $4.45M per breach, endpoint protection platforms are an essential security controls that must be tuned and updated regularly to stop advanced attacks.

Continuous Validation of Endpoint Protection Platforms

Cybersecurity leaders need to continuously test the efficacy of their endpoint security solutions to protect their systems and servers from cyber attacks.

Cymulate enables your security team to conduct a comprehensive assessment of your endpoint security controls to test and validate the efficacy of those controls against the latest attack scenarios and active threats. The full range of test executions applies thousands of known malicious file samples and malicious behaviors to fully challenge your controls and policies and highlight where you have gaps that could be used to compromise your environment.

The endpoint security assessment is fully automated and production-safe, with no harmful execution of malicious payloads during testing. The results of the assessment highlight the gaps and weaknesses in your endpoint security controls that could be used by a threat actor to gain unauthorized access to your systems, exfiltrate your data, and ransom your devices.

Mitigation Guidance to Fortify Your Security Controls

Test scenarios validate both prevention and detection, and every **not prevented** or **not detected** finding includes mitigation guidance that can be used to further fortify your controls to stop more breach scenarios. The Cymulate platform provides you with EDR mitigation rules for your specific endpoint detection and response solution to assist with configuring prevention and detection rules to fine-tune your controls and stop more attacks.

Integration with Leading EDR Solutions

Cymulate integrates with the leading endpoint security solutions, enabling you to query those solutions and validate detections within your endpoint security controls.

Solution Benefits

CONTINUOUS VALIDATION

Automate continuous testing and validation of your endpoint security controls.

IDENTIFY GAPS

Find gaps and weaknesses in your endpoint security controls and policies that could lead to a system compromise.

OPTIMIZE SECURITY CONTROLS

Configure and tune your endpoint security controls with mitigation guidance to prevent and detect the latest threat activity.

REDUCE RISK & EXPOSURE

Continuously measure and improve your endpoint security posture to reduce the risk of a cyber attack.

Comprehensive Testing of Attack Types and Execution Methods

Cymulate tests and validates endpoint security to optimize your endpoint security posture. This assessment challenges your endpoint security controls against a comprehensive set of attacks and, together with the results, provides actionable remediation guidance.

The best practice assessment validates the effectiveness of your endpoint security controls and policies by testing different types of known malicious file samples and malicious behaviors that simulate advanced attacks with full kill-chain scenarios on your endpoint devices. These attack types and execution methods include:

- **Known Malicious Files**
- **Malicious Behaviors**
- **Ransomware, Worms, Trojans**
- **Rootkits**
- **Code Injection**
- **DLL Side-Loading**

Comprehensive Testing of Attack Types and Execution Methods

The assessment results highlight your level of risk and exposure across different attack types and include a complete breakdown by **MITRE ATT&CK** technique to map specific control gaps and weaknesses. The assessment produces a detailed report and findings that include:

- **Risk Score** to measure the overall performance and risk level of your endpoint security exposure.
- **Penetration Ratio** highlighting the number of simulated attacks that were not stopped by your endpoint protection platform.
- **Ratio by Attack Type** to focus efforts on least protected areas of your endpoint security controls.
- **High Risk Files** to prioritize areas of risk and to focus mitigation efforts.
- **Scenario Summaries** with step-by-step test execution results and guidance.
- **Mitigation Guidance** to help optimize controls and enhance policies.
- **EDR Mitigation Rules** to fine-tune prevention and detection rules in your EDR solution.
- **Sigma Rules** to enhance the detection of malicious endpoint behavior in your SIEM solution.

Why choose Cymulate?

DEPTH OF ATTACK SIMULATIONS
Over 490 test scenarios using thousands of known malicious file samples and behaviors to simulate real-world attacks.

PRODUCTION SAFE
The full suite of test cases is completely production-safe and will not harm your endpoint environment.

AUTOMATED VALIDATION
The assessments are fully automated, enabling continuous validation and improvement of your endpoint security controls.

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.

Get a Demo