



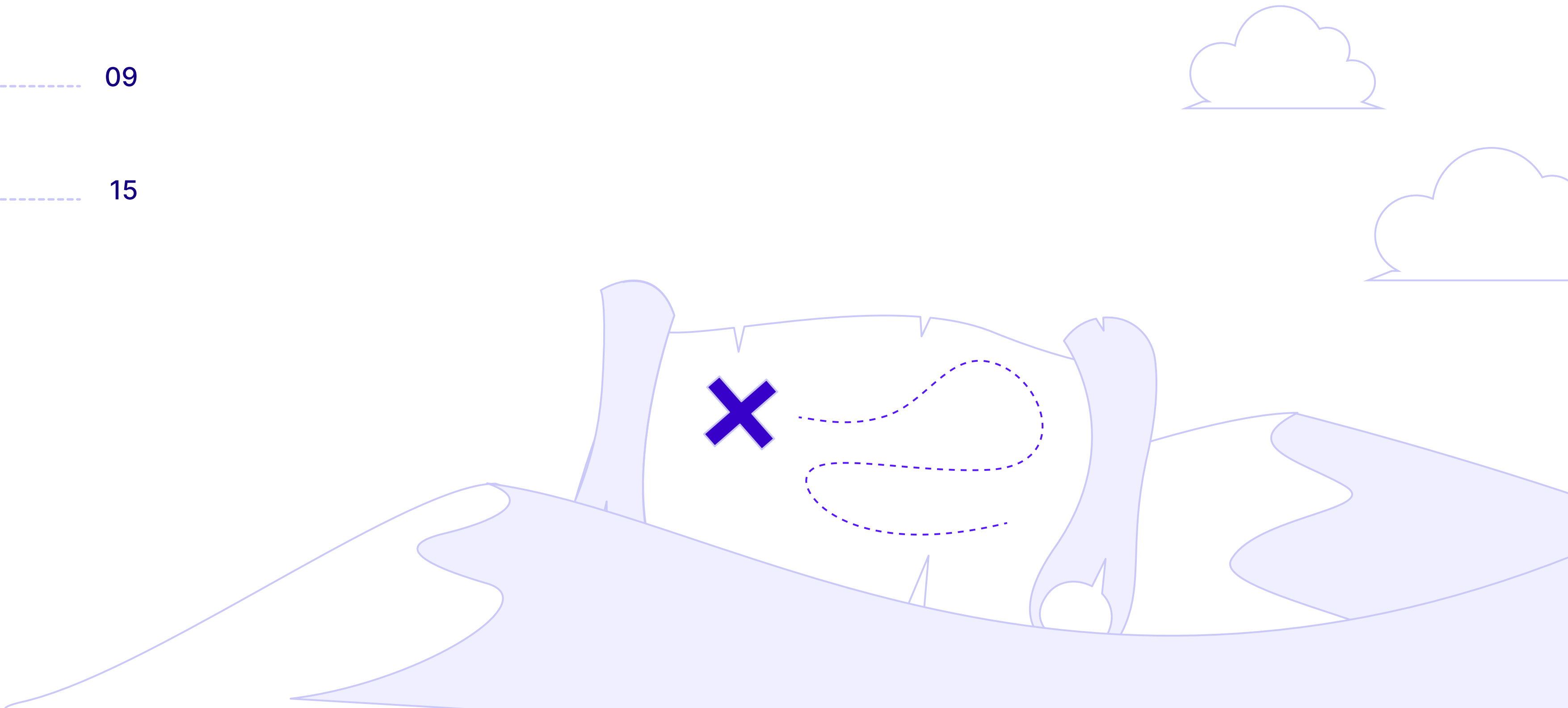
Cymulate Exposure Validation Platform

Product White Paper



Table of Contents

Introduction	03
Adversarial Exposure Validation Mandatory Features	04
Adversarial Exposure Validation Common Features	09
Embracing the Future of Exposure Validation with Cymulate	15



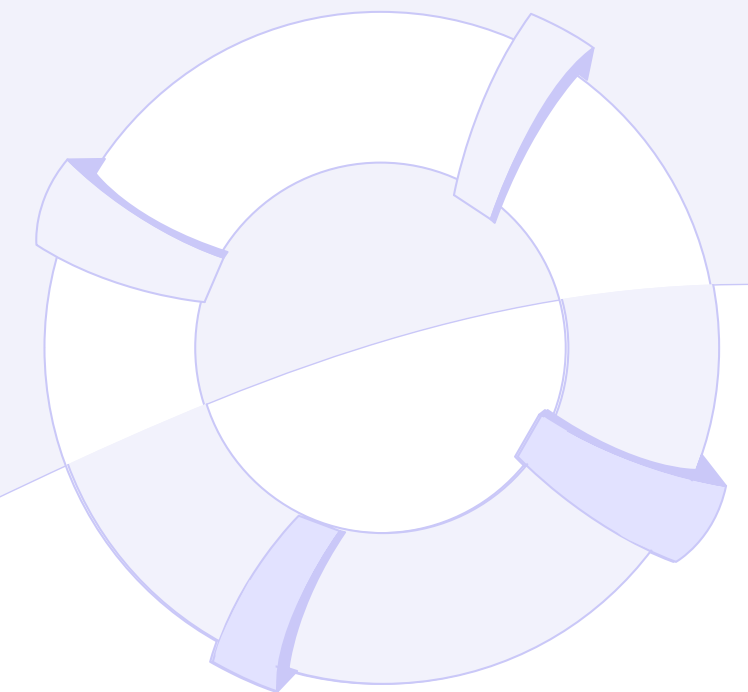
Introduction

The 2025 Gartner® Market Guide for Adversarial Exposure Validation¹ (AEV) provides essential insights for security and risk management leaders considering AEV solutions. The [Gartner report](#) highlights key use cases, defines critical capabilities and helps organizations evaluate the right solutions for their needs. We're proud that Cymulate has been recognized as a Representative Vendor in this guide.

With a growing number of solutions for breach and attack simulation (BAS), automated red teaming and automated penetration testing, security leaders face increasing complexity when assessing their options. The challenge lies in understanding which capabilities are essential, how they align with specific security objectives and how to maximize value from their security investments.

Gartner® outlines four mandatory features that every AEV solution must include and 11 common features. While different security validation solutions may address some or most of these areas, the Cymulate Exposure Validation Platform is designed to deliver on all 15 capabilities.

In this whitepaper, we will break down how Gartner® defines the required and common features of AEV and explore how the Cymulate Exposure Validation Platform aligns with them.



¹Gartner, Market Guide for Adversarial Exposure Validation, Eric Ahlm, Dhivya Poole, Angela Zhao, Mitchell Schneider, 11 March 2025

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

AEV Required Features

Mandatory Feature #1 – Part 1

Comprehensive Attack Simulations Across Multiple Threat Vectors

Gartner: *Performing attack scenarios for multiple threat vectors, including but not limited to: malware, email, application infrastructure, and application and identity abuses.*

The Cymulate Advantage

Cymulate combines technology for breach and attack simulation and automated red teaming to create real-world attack scenarios executed in a production-safe mode to test and validate security controls against the latest emergent threats and threat actors. The platform validates multiple security controls and numerous threat vectors and executes post-breach attacks to map attack paths to critical assets.



Cymulate's scale and variety of automated assessments enhance the team's productivity and provide the most comprehensive picture a CISO can expect to address his concerns and perform optimally.

– Gil Shua, Director of Information Security, TASE

Validate Security Controls	Validate Threats
Secure Email Gateway (SEG)	APT Groups
Secure Web Gateway (SWG)	Vulnerabilities (CVEs)
Web App Firewalls (WAF)	ATT&CK Tactics & Techniques
Endpoint Security (AV/EDR)	Ransomware Threats
Network Security (IDS/IPS)	Malware, Worms and Trojans
Data Loss Prevention (DLP)	Targeted Platforms (OS, Cloud, Containers, SaaS, Databases, Active Directory)
Cloud Security (CWPP)	
Kubernetes/Containers (K8S)	
SIEM/SOAR Detections	


Mandatory Feature #1 – Part 2


Framework-Aligned Attack Scoring


Gartner: *Delivered outputs include: security-framework-aligned reporting, attack scoring and prioritized lists of attack scenario findings with estimated impact and suggested remediation actions.*


The Cymulate Advantage


Cymulate maps security validation to common cybersecurity frameworks, such as NIST 800-53, MITRE ATT&CK® and CIS (Center for Internet Security), with heatmaps of strengths and weaknesses based on proof and evidence of security effectiveness. The Cymulate dashboard provides a comprehensive, at-a-glance overview of your organization’s security posture, highlighting the performance of individual security controls and presenting an overall Cymulate score. You can filter Cymulate dashboards and reporting by environment, controls and threats for straight-forward metrics and trending of:

 Prevention rates

 Detection rates

 MITRE Techniques and techniques not prevented

 CVEs not protected

 APT groups not prevented

Cymulate offers an extensive, full-scale view of all findings from all assessments performed on the platform. To focus on what’s truly exploitable in your environment, you can filter assessments that were not prevented and/or not detected, each providing easy-to-digest remediation guidance on how to strengthen your defenses. Additionally, the platform’s integration with ticketing systems lets you streamline security ticket management directly from Cymulate to prioritize, collaborate and manage critical security-related tasks.

To optimize controls and improve resilience to missed attacks, Cymulate provides actionable and automated remediation. For many missed attacks, Cymulate will suggest an IoC that can be immediately applied to a security control with the option to automatically push that IoC to the control. Cymulate also suggests detection rules that are customized for specific EDR, SIEM and XDR controls.



The Cymulate MITRE ATT&CK Heatmap helps us easily visualize our gaps and coverage of the MITRE framework. We quickly understand if there are specific MITRE techniques or sub-techniques that we haven’t been able to detect, so we know exactly where we need to allocate our resources for better protection.

– Markus Flatscher, Senior Security Manager, RBI

Mandatory Feature #2

Evidence-Based Security Posture Insights

Gartner: *Providing empirical results about an organization's defensive posture as it relates to various attack techniques and scenarios. The validation results data should greatly improve upon other more theoretical data (such as vulnerability data) and give insights into urgently needed changes.*

The Cymulate Advantage

Cymulate scenarios imitate the tactics and techniques outlined by the MITRE ATT&CK® framework. From credential harvesting to privilege escalation or data exfiltration, the simulations provide an authentic feel of how real-world adversaries operate. In the platform, you can search for and run assessments, including scenarios that test specific MITRE tactics or techniques.

Cymulate also maps its attack library to CVEs, so your security team can test its controls and security infrastructure against specific CVE exploits. This proves a vulnerability's exploitability, allowing your team to prioritize the urgency of remediation and patching.



Cymulate helps us evaluate whether a vulnerability is exploitable in our environment and enables us to prioritize remediation efforts. If there are compensating controls in place, we can prioritize remediating other high-risk vulnerabilities that are more likely to be exploited.

– Adam Champion, Head of Information Security, Saffron Building Society



Using the Cymulate integrations, we launch assessments to see if our tools detect them. If they don't, Cymulate provides mitigation guidance and Sigma rules, and we easily rerun the assessments to validate remediation.

– Karl Ward, Head of Cybersecurity, LV=

Mandatory Feature #3

Scalable Defensive Testing with Pre-Built Scenarios

Gartner: *Ability to scale defensive testing with vendor-supplied attack scenarios that require little to no hacking knowledge to execute and obtain results data.*

The Cymulate Advantage

Cymulate makes it easy to automate offensive security by providing quick access to hundreds of out-of-the-box templates. Leveraging templates streamlines the assessment process, allowing you to efficiently launch targeted assessments based on best practices and use cases, such as cloud security, APT groups and MITRE techniques.

Additionally, the Cymulate Research team actively monitors emerging threats and adds the most relevant ones to the platform so that you can easily run assessments within 24 hours of discovery.

To help your security team scope and plan its validation strategy, Cymulate provides AI-guided customization to tailor assessments based on industry, compliance requirements, relevant threat actors, primary security controls and more.

To help you quickly find specific results, Cymulate includes an AI chatbot that analyzes your security findings based on natural language prompts. The chatbot provides a concise breakdown of critical security insights and reports, including overall security posture, scenarios prevention overview, scenario detection overview, drift detection and more.



We no longer have to wait for a periodic pen test every six months. With the same small security team, Cymulate allows us to optimize our resources and use automation to run more assessments continuously.

– Renaldo Jack, Group Cybersecurity Head, Globeleq



I love that Cymulate can replicate a real-world attack in a safe and repeatable way. I no longer need to engage with third-party sources because Cymulate is my reliable, vetted source.

– Head of Cybersecurity Operations, Credit Union

Mandatory Feature #4

Automated Scheduled Testing for Continuous Validation

Gartner: *Automated scheduling for increased testing frequency without the need for human intervention, helping to reduce errors and improve trending measurability data for exposure management and defensive operations.*

The Cymulate Advantage

For regular security monitoring, you can schedule Cymulate assessments to run at predetermined times, ensuring consistent security evaluations. Additionally, you can schedule certain assessments to recur at specified intervals.

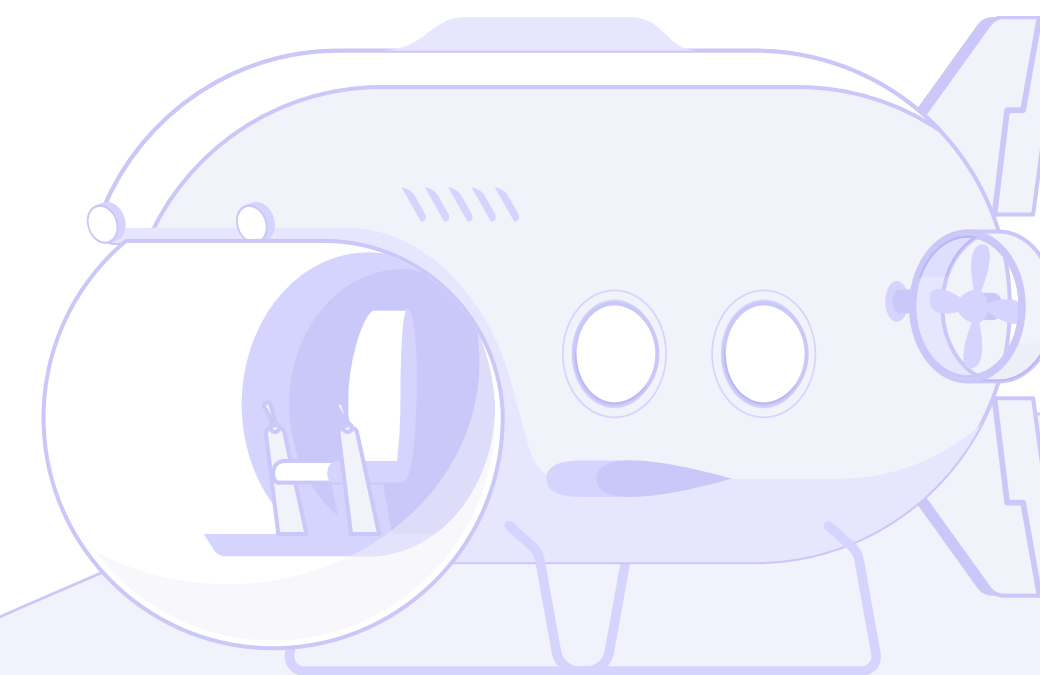
To ensure that assessments remain up-to-date and reflect the latest threat landscape, Cymulate smart templates continuously evolve by automatically pulling the latest scenarios that match predefined filter criteria at the time of assessment execution.

The Cymulate Research team diligently tracks new threats, incorporating the latest and most pertinent ones into the platform, typically within 24 hours of their discovery. You can schedule these new assessments to run as soon as a new threat is detected or to run weekly at a specific time.



Instead of chasing after the latest threat, the Cymulate research team keeps us up to date with emerging threat assessments so we can immediately evaluate our security and know if we are protected. We automatically run the immediate threats assessments daily.

– Kevin Roberts, Information Security Analyst, Nedbank



AEV Common Features

Common Feature #1

Continuously Updated Scenario Library

Gartner: *A continuously updated marketplace of pre-built attack scenarios for validation usage.*

The Cymulate Advantage

Cymulate provides over 120,000 attack simulation resources from real-world attack scenarios designed to test and validate your security controls. The Cymulate Research team diligently tracks new threats, incorporating the latest and most pertinent ones into the platform, typically within 24 hours of their discovery.



The Cymulate Research Group is always quick to create new emerging threat assessments. With minimal effort, we understand our exposure and how to mitigate it.

– Adam Boden, Lead Cybersecurity Operations Specialist, LV=

Common Feature #2

Customizable Dashboards

Gartner: *Customizable dashboards that allow for better workflow through common use cases.*

The Cymulate Advantage

Cymulate custom dashboards allow you to gather insights based on findings from across the platform and create customized dashboards tailored to meet your specific needs and goals. With the ability to create multiple widgets, you have complete control over the information displayed. The widgets can be configured to show data based on the selected type, dimensions and filters and are updated in real-time with the latest assessment metrics.



Cymulate is easy to implement and use – all you need to do is click a few buttons, and you receive a lot of practical insights into how you can improve your security posture.

– Raphael Ferreira, Cybersecurity Manager, Banco PAN

Common Feature #3

Contextualized Threat Validation

Gartner: Ability, either natively or through third-party integrations with tools like external attack surface management (EASM), to leverage estate information such as asset discovery, attack surface management or vulnerability management data.

The Cymulate Advantage

Cymulate includes an option for external attack surface scanning to conduct comprehensive scans across domains, subdomains, IP addresses, ports and other sources for internet-facing vulnerabilities and open-source intelligence. With an attacker's view of your organization's cyber assets, you can proactively identify potential entry points and vulnerabilities within their external infrastructure. These scans enable you to detect weaknesses that could be exploited by threat actors seeking unauthorized access to sensitive systems and data.



I chose to implement Cymulate attack surface management because I wanted intelligence on my assets, not just a long list of vulnerabilities that a vulnerability management tool would give me.

– Shaun Curtis, Head of Cybersecurity, GUD Holdings

Common Feature #4

SaaS-Hosted Point of Attack

Gartner: Providing, through a SaaS model, the ability to use an externally hosted point of attack system (POA) hosted by the provider.

The Cymulate Advantage

Cymulate operates as a SaaS (software-as-a-service) platform to enable efficient and secure attack simulations. The platform is deployed in the cloud to eliminate the need for complex on-prem installations and enable fast and easy setup. Cymulate leverages POA systems hosted externally to simulate production-safe real-world attack scenarios across multiple vectors.

To safely run advanced testing, the external point of attack targets the Cymulate agent—a lightweight software installed on target systems within your organization's network. The agent executes attack simulations, collects relevant data and securely communicates with the Cymulate Platform. Attacks are launched using predefined or custom scenarios that mimic tactics, techniques and procedures (TTPs) used by adversaries. These simulations target various layers of your organization's security infrastructure to test defenses and identify vulnerabilities. The success of an attack is determined by analyzing whether the simulated threat was prevented, detected or executed successfully.



I really like the product. Super-fast deployment and visibility on your network and major attack vectors.

– Team Leader, Healthcare and Biotech Organization

Common Feature #5

Attack Scenario Workbench

Gartner: *A custom attack creation workbench for advanced users that allows for the creation of validation tests, useful for purple and red teams.*

The Cymulate Advantage

Cymulate includes an attack scenario workbench to build tailored assessments and apply custom threat actions, providing a highly customized approach to adversarial exposure validation. When creating the scenario, you can configure various actions and resources, define success indicators, edit execution code, manage clean-up processes and review pre-requirements. By building scenarios that align perfectly with your security objectives, you can comprehensively assess your organization's defenses.



With Cymulate, we have many tests that we can run out of the box, like immediate threats assessments, endpoint security assessments and APT-focused advanced scenarios. But we also can highly customize chained assessments – we decide what we want to run, how we want to run it and where we want to run it.

– Markus Flatscher, Senior Security Manager, RBI

Common Feature #6

Integrations for Mobilized Remediation

Gartner: *Ability to assist in the mobilization of findings through integration with workflow, ticketing or actual defensive systems.*

The Cymulate Advantage

Cymulate integrates with ticketing systems, enabling you to streamline security ticket management directly from Cymulate to prioritize, collaborate and manage critical security-related tasks. Additionally, Cymulate provides actionable and sometimes automated remediation. For many missed attacks, Cymulate will suggest an IoC that can be immediately applied to a security control with the option to automatically push that IoC to the control. Cymulate also suggests detection rules that are customized for specific EDR, SIEM and XDR controls.



We've completely integrated the Cymulate platform into our SecOps processes. Once the scheduled assessments automatically test our controls, we review the results. The team has procedures to quickly implement remediation guidance and optimize our security.

– SOC Manager, Utility Organization

Common Feature #7

Integrated Threat Intelligence

Gartner: Access to threat intelligence from various sources, either through native or third-party integrations that is available for use while creating custom attack scenarios.

The Cymulate Advantage

The Cymulate Research team diligently tracks new threats, incorporating the latest and most pertinent ones into the platform, typically within 24 hours of their discovery. This prompt update mechanism ensures that your organization has the intelligence to respond quickly to new threats, which may be delivered through email attachments or downloadable links on legitimate or compromised websites. Cymulate also has an AI attack planner to help you automatically generate an attack simulation for specific threats based on threat advisories and other threat intel. Simply input a URL or free text about the threat, and Cymulate will create a ready-to-run, production-safe assessment.



I love that Cymulate can replicate a real-world attack in a way that is safe and repeatable. I no longer need to engage with third-party sources because Cymulate is my reliable, vetted source.

– Head of Cybersecurity Operations, Credit Union

Common Feature #8

Security Control Integrations

Gartner: Ability to integrate with security controls via APIs or native interfaces to enhance the alignment of attack data with the defensive posture through contextualized content suggestions.

The Cymulate Advantage

Cymulate integrates with various technology partners to augment and benefit existing security solutions. You can integrate your endpoint detection and response (EDR), security information and event management (SIEM), vulnerability management (VM), firewalls, web gateway and other solutions with Cymulate to validate security control detection performance, prioritize remediation plans, manage security tasks and more.



Using the Cymulate integrations, we launch assessments to see if our tools detect them. If they don't, Cymulate provides mitigation guidance and Sigma rules and we easily rerun the assessments to validate remediation.

– Karl Ward, Head of Cybersecurity, LV=

Common Feature #9

Detection Engineering Guidance

Gartner: *Recommend vendor-specific detection engineering content on systems – such as security information and event management (SIEM), extended detection and response (XDR) and endpoint detection and response (EDR) – based on actual test results that will improve defensive posture.*

The Cymulate Advantage

Cymulate validates detection across SIEM, EDR and XDR systems and provides everything needed to refine and fine-tune detection rules for maximum accuracy. By integrating and testing these security systems against thousands of real-world attack scenarios, Cymulate identifies undetected threats and weaknesses, ensuring no gaps are left unaddressed. Beyond validation, it enhances detection accuracy by supplying IoCs, indicators of behavior, sigma rules and vendor-specific translations to streamline rule tuning.



When we create a new detection rule in our SIEM that we can't validate with historical logs, we use Cymulate assessments to generate the appropriate events and see if the rule was successful in its detection. The immediate feedback is useful when fine-tuning our SIEM and practicing detection engineering.

– Markus Flatscher, Senior Security Manager, RBI Bank

Common Feature #10

Detailed Reporting Based on Role

Gartner: *Detailed reports based on roles such as executives, asset owners, blue team owners, content engineers and testing teams. These reports should include necessary context for each role, such as industry peer baselining, vendor scorecards or attack path graphics.*

The Cymulate Advantage

Cymulate custom dashboards allow you to gather insights based on findings from across the platform and create customized dashboards tailored to the different roles in your organization. With the ability to create multiple widgets, you have complete control over the information displayed. The widgets can be configured to show data based on the selected type, dimensions and filters and are updated in real-time with the latest assessment metrics.

The platform also quantifies your organization's cyber resilience and control effectiveness relative to industry benchmarks. This comparison provides insights into how your organization's security measures align with industry norms and helps identify potential gaps or areas for improvement.



Cymulate provides us with the visibility and standardization we were missing. The platform's analytics and reporting make providing a holistic view of our cyber security posture to management and the board easier.

– Renaldo Jack, Group Cybersecurity Head, Globeleq

Common Feature #11

Framework-Based Prioritization

Gartner: *Intelligent posture prioritization suggestions based on the use of frameworks such as MITRE's Threat-Informed Defense.*

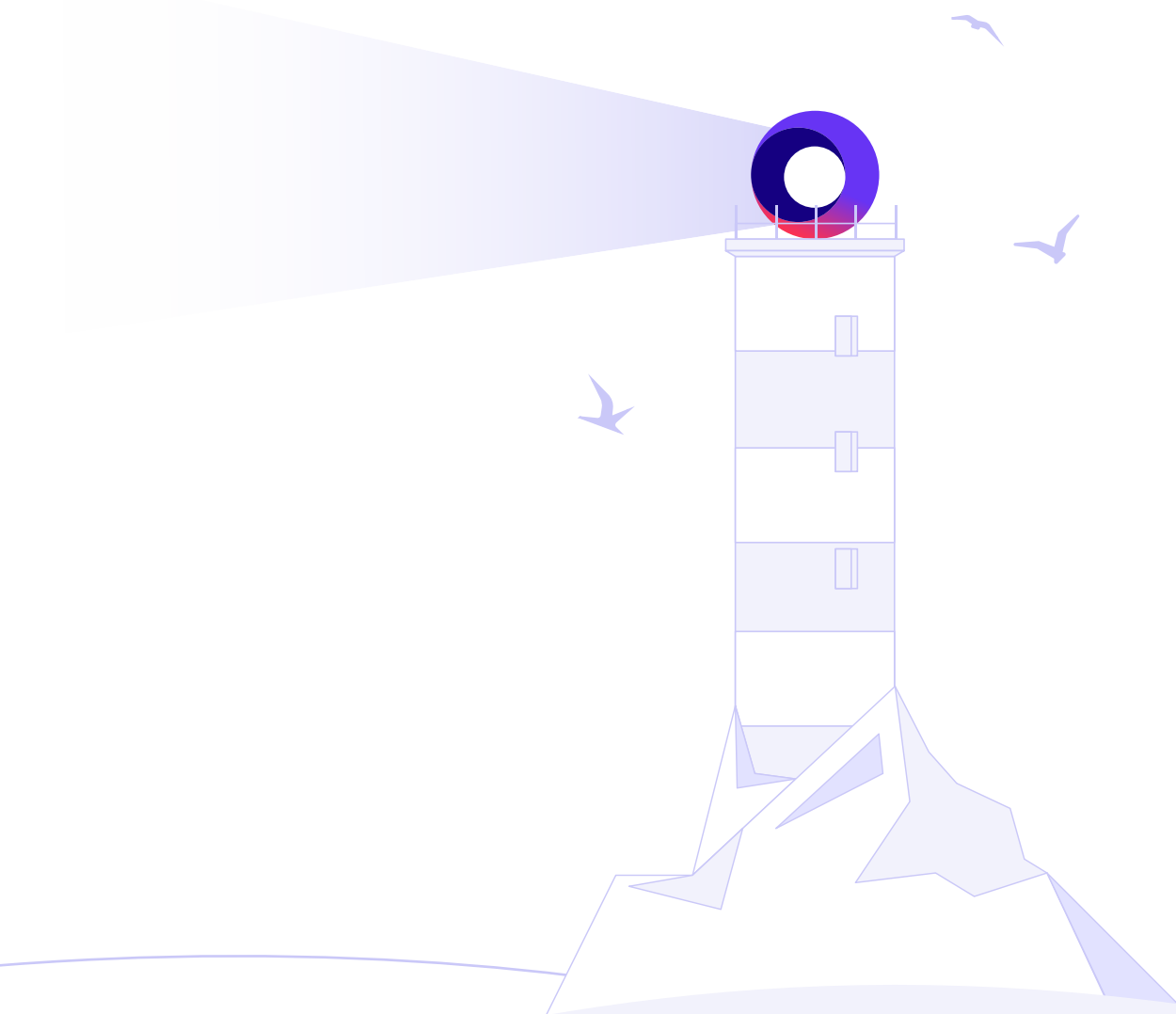
The Cymulate Advantage

Cymulate aligns security validation with widely used cybersecurity frameworks, such as NIST 800-53, MITRE ATT&CK® and CIS, with heatmaps that highlight strengths and weaknesses backed by concrete evidence of security effectiveness. You can easily filter Cymulate assessment findings by critical and high-risk security gaps found in these frameworks and prioritize their mitigation.



The Cymulate MITRE ATT&CK Heatmap helps us easily visualize our gaps and coverage of the MITRE framework. We quickly understand if there are specific MITRE techniques or sub-techniques that we haven't been able to detect, so we know exactly where we need to allocate our resources for better protection.

– Markus Flatscher, Senior Security Manager, RBI



Embracing the Future of Exposure Validation with Cymulate

Gartner® predicts that by 2027, **40% of organizations will have formal exposure validation initiatives**. As security teams strive to keep up with evolving threats, it's clear that exposure validation is no longer optional, it's essential.

For mature security teams, AEV is a critical component of the shift toward Continuous Threat Exposure Management (CTEM). Unlike traditional vulnerability management, which struggles to keep up with hundreds or thousands of new exposures weekly, CTEM prioritizes the threats that are actually exploitable.

Gartner® strongly advocates for AEV as a mandatory capability in CTEM, emphasizing its role in proving the effectiveness of security controls. By emulating real-world attack techniques, Cymulate helps your organization confirm whether its security measures can detect or prevent a threat. This evidence-based validation allows you to avoid unnecessary emergency patching and disruptions, focusing only on exposures that pose a real risk.

Cymulate is committed to evolving exposure validation into a continuous, proactive security practice. Our platform enables you to test against the latest threats daily, automate attack scenarios and gain deep insights into attack paths and root causes. As threats grow more sophisticated, you need more than just visibility, you need a dynamic, adaptive defense.

The future of security lies in continuous exposure validation and CTEM. We invite you to explore how Cymulate can help your organization strengthen its security posture.

[Request a demo](#)

