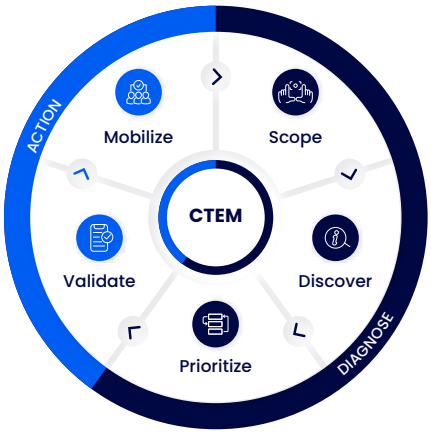
DATA SHEET

Cymulate

Cymulate Exposure Management & Security Validation Platform

Cybersecurity risk and resiliency concern both technical and business leaders as they strive to find a common language to understand and communicate the impact of threats and business operation changes.
It is difficult to define the security risk related to business initiatives while achieving a balance between over-protection and negatively impacting a company's risk tolerance levels.

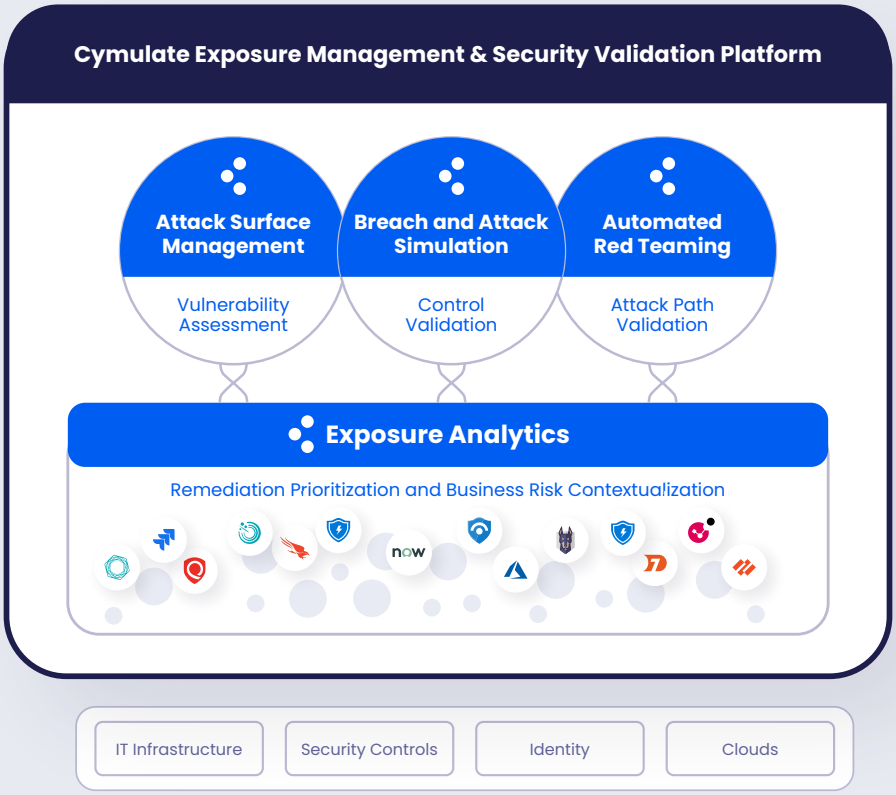
Proactive security defense requires both security validation and threat exposure management to create a consistent, actionable security posture remediation and improvement plan that connects to business risks and initiatives. To accomplish this, Gartner identifies continuous threat exposure management (CTEM) as a programmatic approach to managing exposure risk, optimizing cyber programs, and improving cyber resilience.



Gain an attackers view of attack surfaces, vulnerabilities, and security efficacy to support continuous threat exposure management programs

The Cymulate Exposure Management and Security Validation Platform provides the technology for exposure discovery, validation, and prioritization with business insights and intelligence. This simplifies security leaders' risk and resilience to emergent threats and a rapidly changing attack surface. With a complete view of the security posture and business risks, the Cymulate platform gives security leaders the data they need to define the scope for cyber initiatives, successfully mobilize mitigations, and continuously assess security operations performance.

The Cymulate platform consolidates exposure management and control validation. Customers can deploy modular offerings based on their specific needs and add additional offerings as their needs change.



Cymulate Exposure Management and Security Validation Benefits

- Scope cybersecurity risk with business context
- Take the attacker's view of exposures and security control weaknesses that can be exploited
- Intelligently model tactical and strategic outcomes
- Mobilize new security programs with benchmarks and baselines

The Cymulate Platform Drives Continuous Threat Exposure Management Programs

Step	Cymulate Offering	CTEM Value
Scoping	Cymulate Exposure Analytics	Provide insights for security and non-technical leaders to define the scope for initiatives based on a clear view of security posture that considers business context and risk quantification calculated from data aggregated across IT infrastructure and security stack.
Discovery	Cymulate ASM	Discover new assets, identify vulnerabilities and misconfigurations, and map attack paths.
	Cymulate Exposure Analytics	Aggregates discovered assets from multiple sources including Cymulate ASM, endpoint security, cloud scanners, and many others. Profiles the risk of each asset based on the security findings reported across security controls. Extracts data about the coverage of security controls for each asset, including the specific policies applied for each asset by each control.
Prioritization	Cymulate ASM, BAS, CART	Vulnerability prioritization, security control optimization, and remediation planning are based on individual ASM, BAS, or CART findings and remediation recommendations.
	Cymulate Exposure Analytics	Contextualized vulnerability prioritization correlates vulnerability findings (of multi-vendor aggregated data) with business context and security control effectiveness.
Validation	Cymulate BAS	Validate control effectiveness and security posture to determine the likelihood of attack success, estimate potential impact, and measure response capabilities.
	Cymulate CART	Automate testing for vulnerability validation, what-if scenario, targeted, and custom-testing within a flexible framework for repeatable and scalable testing.
Mobilization	Cymulate Exposure Analytics	Analyze data to understand various program or response outcome options and establish baselines that track performance and risk profiles.

Cymulate

Cymulate Breach and Attack Simulation

Cymulate Breach and Attack Simulation (BAS) validates cybersecurity controls by safely conducting threat activities, tactics, techniques, and procedures in production environments. With automation and a library of real-world and production-safe attack scenarios and simulations, Cymulate BAS gives security teams an easy-to-use interface to test security architecture, people, and processes for continuous assessment of cyber resilience.

Cymulate BAS applies the latest threat intel from multiple sources and primary research from the Cymulate Threat Research Group with daily updates on emergent threats and new simulations – all mapped to the MITRE ATT&CK Framework. On-demand and scheduling systems allow for both one-off checks and automated testing to validate security controls against emergent threat activity, confirm remediation, or prepare for audits and penetration tests.

Cymulate BAS Scenarios

- Email Gateway
- Web Gateway
- Web Application Firewall
- Endpoint Security
- Data Exfiltration
- Immediate Threat Intelligence
- Full Kill-Chain Scenarios

Cymulate BAS Advanced Scenarios

- Custom Attack Simulations

BAS Scenarios

Email Gateway, Web Gateway, Web Application Firewall, Endpoint Security & Data Exfiltration

Cymulate BAS Scenarios includes production-safe control validation capabilities for email gateways, web gateways, web application firewalls, endpoint security, and data exfiltration to test for detection, control, and alerting on threats. Cymulate BAS confirms that security controls are functioning correctly and identifies threats that evade them. Each vector is scored independently and aggregated for an overall risk score based on industry-standard frameworks.

Immediate Threat Intelligence

The immediate threat intelligence capability tests security controls against new and emergent threats observed in the wild. The Cymulate Threat Research Group updates Cymulate BAS daily with attack simulations of these latest threats that require urgent attention and action. Threat and simulation updates include insights into threat actors, attack vectors, techniques mapped to MITRE ATT&CK, and indicators of compromise.

Full Kill-Chain Scenarios

The full kill-chain scenarios capability simulates end-to-end attack scenarios of known advanced persistent threat (APT) groups and potential campaigns. These attack simulations deliver and execute production-safe ransomware, trojan, worm, or custom payloads via web or email attack vectors. Instead of challenging each attack vector separately, Cymulate BAS tests the effectiveness of various security controls across the entire cyber kill-chain – from attack delivery to exploitation and post-exploitation.

BAS Advanced Scenarios

Cymulate BAS Advanced Scenarios enables red teams to create and automate custom attack simulations. Applying the MITRE ATT&CK® framework, security teams use BAS Advanced Scenarios to create complex scenarios from both pre-built resources and custom binaries and executions. This open framework reduces time to remediation with the ability to re-run assessments whenever and wherever needed.

Cymulate Attack Surface Management

Cymulate Attack Surface Management (ASM) automates the ongoing process of identifying internal and external assets, showing where security gaps exist, where they can be used to perform an attack, and where defenses are strong enough to repel an attack. Cymulate ASM looks at on-prem and cloud platforms, public-facing and internal systems, users, entitlements, and other components. Organizations can then identify security gaps efficiently and prioritize remediation.

External ASM

Cymulate ASM maps the external attack surface by emulating reconnaissance and probing methods of threat actors to identify digital assets (such as web domains, IP addresses, applications, and more) and assess their exploitability.

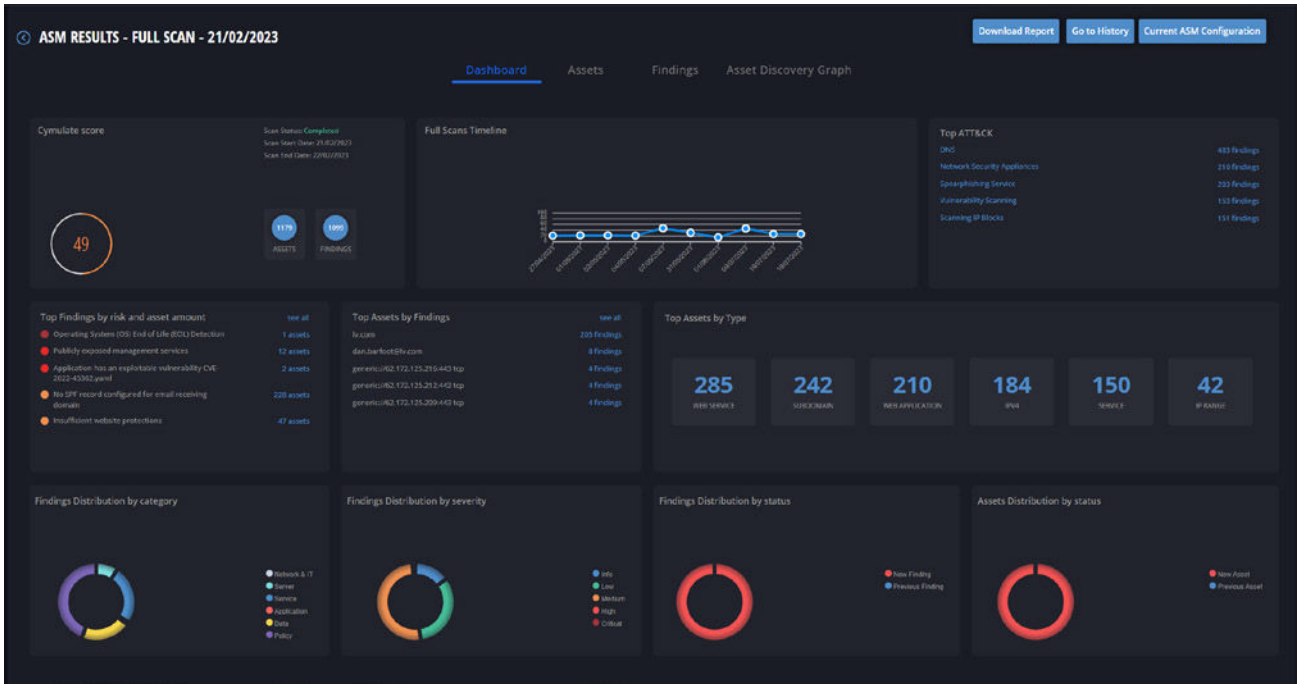
Internal ASM

Cymulate ASM maps the internal attack surface with authenticated scans using user credentials to identify exploitable assets that an adversary can leverage to propagate from a foothold to crown jewels.

Attack Path Mapping

With findings from the internal attack surface, Cymulate ASM maps attack paths across networks, cloud (AWS, Azure, and GCP), and identity systems, including Active Directory services, so organizations can quickly identify and close gaps without disrupting business operations.

Cymulate Attack Surface Management Dashboard



The Cymulate CART dashboard includes an overall security score based on simulated attack success rate correlated with industry standards and other details such as top findings, trending, and distribution of findings across categories.

Cymulate Continuous Automated Red Teaming

Cymulate Continuous Automated Red Teaming (CART) provides cybersecurity teams a platform to increase operational efficiency and optimize their adversarial activities with production-safe methodologies. The implementation is easy, and the assessments can test any technique at any stage of the attack kill-chain independently – start with a well-crafted phishing email or begin from inside the network and move laterally in stealth, using a variety of exploits. The Cymulate CART solution supports automated testing for vulnerability validation, what-if scenario, targeted-, and custom-testing within a flexible framework for repeatable and scalable testing.

Full Kill-Chain Campaign

Cymulate CART includes full kill-chain campaign capabilities to validate an organization's security framework against real-world cyber attacks attempting to bypass security controls across the cyber kill-chain, from attack delivery to exploitation and post-exploitation. The full kill-chain capability begins with one or more production users interacting with targeted attack emails that pose no real risk to the organization. Once the recipient clicks and executes the payload, follows a link to download and run a payload, or performs other user actions to initiate the attack, production-safe code execution and defense evasion techniques challenge endpoint security resilience with ransomware, trojans, worms, advanced scenarios, or lateral movement. Each step of the attack and each technique used is controlled by the cybersecurity team and uses Cymulate code components to ensure safety.

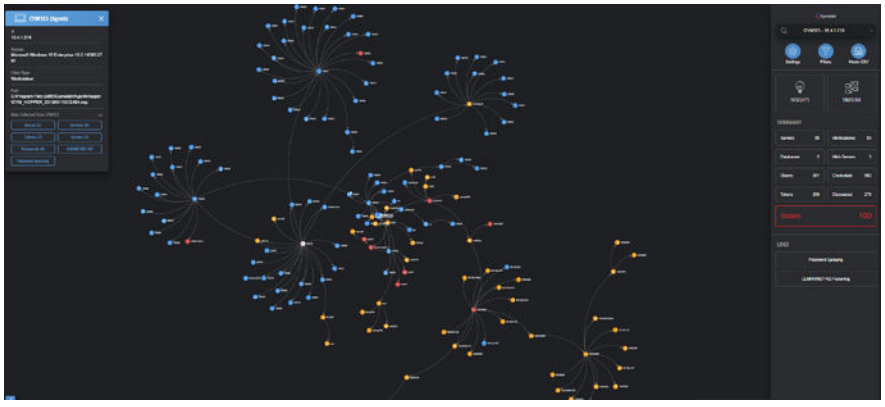
Network Pen Testing

The network penetration testing capability simulates an attacker that has gained an initial foothold in a company's network and moves laterally in search of any additional assets that can be compromised. It safely applies threat tactics and techniques to uncover infrastructure misconfigurations and security weaknesses. Providing this functionality as an independent capability allows the organization to segregate network-level defenses from endpoint-level defenses for a more accurate analysis of both layers of controls. At the end of the assessment, the system also cleans up after itself to remove any components that were distributed to other machines.

Phishing Awareness

Cymulate CART includes the phishing awareness capability to provide all the resources to create an internal phishing campaign and measure employee resilience against phishing attacks. Creating a customized assessment with Cymulate CART is quick and easy. Employee interactions with the mock phishing emails are automatically recorded, logging hazardous behaviors such as clicking links or entering credentials. This identifies employees needing additional phishing awareness training and highlights users who are not following proper policies and procedures.

Network Pen Testing: Validated Attack Paths



Each network penetration testing assessment produces a visualization of the attack path, including all the endpoints reached and the methods used, providing insight into the weaknesses in the network infrastructure.

Cymulate Exposure Analytics

Cymulate Exposure Analytics is a data aggregation and exposure intelligence solution that collects data from across enterprise IT, clouds, and the security stack to support exposure management programs to measure and baseline cyber resilience, focus on the biggest risks, and accelerate mitigations. Cymulate Exposure Analytics pulls data from vulnerability management platforms, asset inventories, clouds, security controls, and the IT infrastructure. Data feeds are aggregated to normalize and contextualize the information with business relevance, prioritize remediation, and measure and optimize cyber resilience.

Organizations can then define business contexts (by business unit, sensitivity to downtime, or other factors) and assign assets to one or more contexts. By correlating exposure potential with business information, Cymulate Exposure Analytics quantifies risk and resilience so security teams can make informed data-based decisions and provide better insights to strategic leadership and company boards.

Contextualized Vulnerability Management

Cymulate Exposure Analytics provides context-based vulnerability prioritization that correlates vulnerability findings with business context and security control effectiveness. By integrating with tools for breach and attack simulation and continuous automated red teaming, Cymulate Exposure Analytics creates a risk score that considers the exploitability and effectiveness of compensating security controls.

Cymulate Exposure Analytics – CVM

Full-featured option with the contextualized vulnerability management (CVM) capability, including integrations to vulnerability management solutions and other Cymulate products.

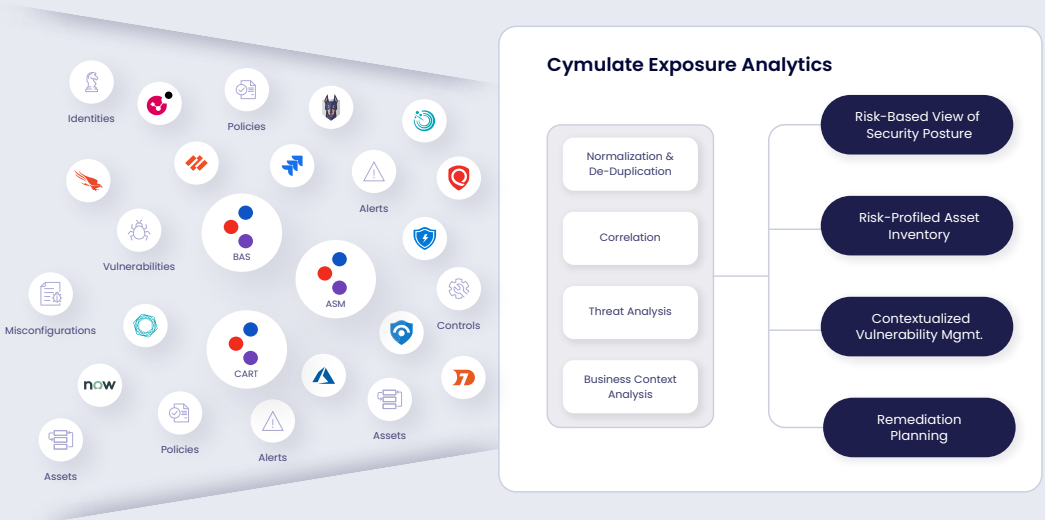
Cymulate Exposure Analytics – Enterprise

Full-featured option with correlated analysis of any third-party data (including vulnerability management solutions) and other Cymulate products.

Core Capabilities:

- Correlates exposure potential with business context
- Reports on issues to be addressed, in context, by risk and area of responsibility
- Creates remediation plans to reduce exposure and close gaps
- Baselines risk and security posture with improvement tracking
- Builds risk metrics and performance tracking for CTEM program scoping and mobilization

Fuse Technical Data with Business Context



Cymulate

Customer Quotes

> *With Cymulate, we can measure our infrastructure and our security controls automatically against the latest and most pervasive threats from one platform and get a metric which is consumable by leadership.*
>
> **Shaun Curtis, Head of Cybersecurity, GUD**

> *Cymulate provides us with the insights to close gaps and optimize the controls we already have in our security stack—we don't need to waste time or money looking for new tools to improve our security.*
>
> **Liad Pichon, Director of Cybersecurity, BlueSnap**

Awards and Accolades

About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience against emergent threats, evolving environments, and digital transformations. The solution has a quantifiable impact across all five continuous threat exposure management (CTEM) program pillars and on a business's ability to reduce risk by understanding, tracking, and improving its security posture. Customers can choose from its Attack Surface Management (ASM) product for risk-based asset profiling and attack path validation, Breach and Attack Simulation (BAS) for simulated threat testing and security control validation, Continuous Automate Red Teaming (CART) for vulnerability assessment, scenario-based and custom testing, and Exposure Analytics for ingesting Cymulate and 3rd-party data to understand and prioritize exposures in the context of business initiatives and cyber resilience communications to executives, boards, and stakeholders. For more information, visit www.cymulate.com.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com