Publication date:
09 Apr 2025
Author(s):
Andrew Braunberg, Principal Analyst

On the Radar - Exposure Management Solutions: Cymulate Exposure Validation Platform

Summary

Cymulate's entrance into the exposure management market demonstrates the rapid consolidation of proactive security capabilities into comprehensive platforms.

Catalyst

Cymulate's value proposition is framed around the ability to better prioritize remediation recommendations by providing a single source of truth for threat exposure and determining the appropriate actions required to proactively close security gaps.

This capability is built on the company's core competency of security control validation. Omdia agrees that a dynamic understanding of security posture, supported by deployed security controls, is a critical capability for exposure management solutions. Traditionally, security control validation has delivered the most accurate understanding of the real risk associated with exposures.

Omdia view

Estimating the risk associated with exposures is the primary problem that exposure management solutions are designed to address. Real-world exploitability is arguably the best predictor of risk associated with software vulnerabilities, which are often seen as the most critical exposures to remediation.

Traditionally, the most sophisticated security control validation has been achieved with red teams and breach and attack simulation tools. In practice, however, these teams and techniques are used relatively sparingly, given their cost and complexity.

To better enable security, as opposed to compliance, use cases for these solutions, Cymulate has invested heavily in automating security control validation. For example, in 2024, it released a new AI Copilot that is designed to automate many of the routine tasks associated with validation. The goal is to allow customers to move past point-in-time assessments and closer to a real-time view of their security posture, which is a requirement for applying security control validation to exposure management.

Why is Cymulate Platform notable?

Cymulate has positioned itself as a leading provider of exposure validation, which it views as foundational for broader exposure management solutions. Omdia agrees that an understanding of the actual protection provided by existing security controls is a requirement for delivering true operational cyber risk management with exposure management solutions. However, validation of security controls, or even posture management of security controls, is often lacking, even in leading exposure management solutions.

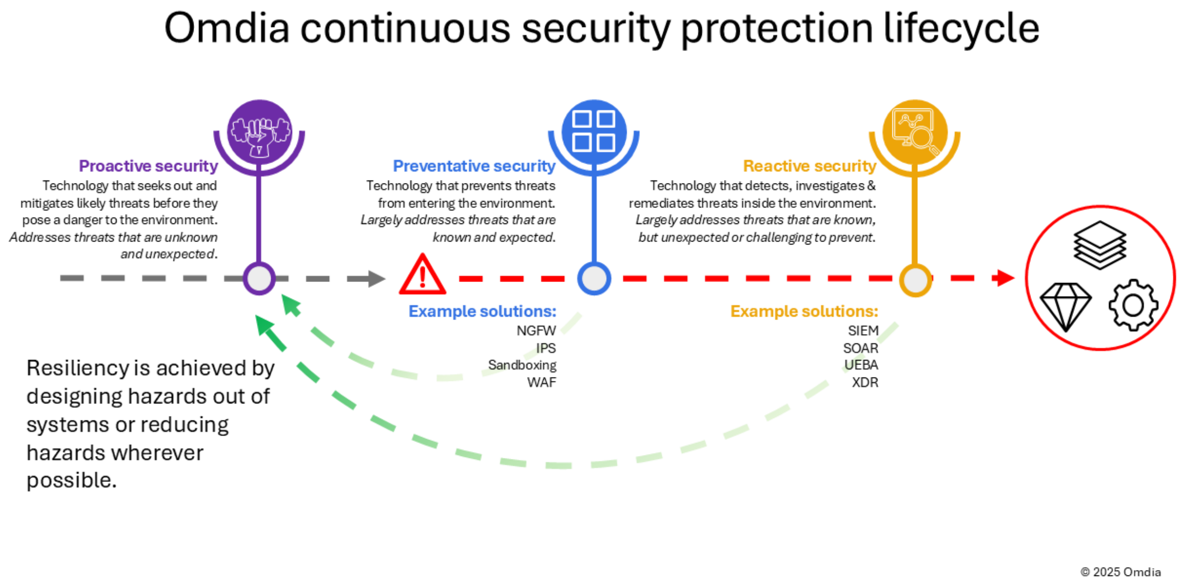
Market context

It is important to understand that proactive security controls are not a replacement for an organization’s existing security stack. Preventative and reactive tools are not going away. However, Omdia does see a shift in spend from more traditional security tool categories toward proactive capabilities. This shift is driven in part by the commoditization and consolidation of some preventative and reactive technologies but also by the sheer size and rate of expansion of the threat landscape, mandating a “left-of-boom” approach as the only way to keep pace.

Omdia believes that the emergence of proactive security platforms marks a generational shift in enterprises’ approach to cybersecurity. We define proactive security as technology that seeks out and mitigates likely threats and threat conditions before they pose a danger to the extended IT environment, enabling enterprises to identify and eliminate areas of opportunity for adversaries before they can be exploited.

Omdia sees proactive security as the third major type or category of security solution, joining preventative security solutions like firewalls, intrusion prevention, and agent- or workload-based protections and reactive solutions like SIEM/next-generation (NG) SIEM, SOAR, behavioral analytics, and various detection and response solutions.

Figure 1: Understanding the role of proactive security



Omdia continuous security protection lifecycle

Proactive security
Technology that seeks out and mitigates likely threats before they pose a danger to the environment.
Addresses threats that are unknown and unexpected.

Preventative security
Technology that prevents threats from entering the environment.
Largely addresses threats that are known and expected.

Example solutions:
NGFW
IPS
Sandboxing
WAF

Reactive security
Technology that detects, investigates & remediates threats inside the environment.
Largely addresses threats that are known, but unexpected or challenging to prevent.

Example solutions:
SIEM
SOAR
UEBA
XDR

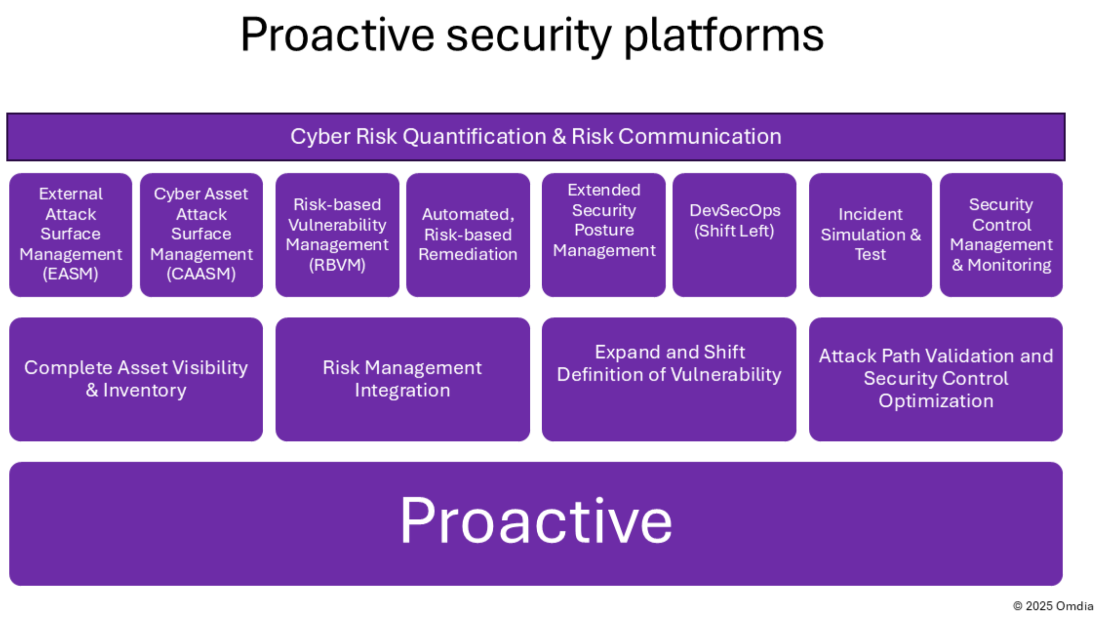
Resiliency is achieved by designing hazards out of systems or reducing hazards wherever possible.

© 2025 Omdia

Source: Omdia

As seen in Figure 2, proactive security encompasses a large set of traditionally disparate products and services. Exposure management solutions are currently consolidating many of these capabilities.

Figure 2: Proactive security categories & capabilities



Proactive security platforms

Cyber Risk Quantification & Risk Communication

External Attack Surface Management (EASM)

Cyber Asset Attack Surface Management (CAASM)

Risk-based Vulnerability Management (RBVM)

Automated, Risk-based Remediation

Extended Security Posture Management

DevSecOps (Shift Left)

Incident Simulation & Test

Security Control Management & Monitoring

Complete Asset Visibility & Inventory

Risk Management Integration

Expand and Shift Definition of Vulnerability

Attack Path Validation and Security Control Optimization

Proactive

© 2025 Omdia

Source: Omdia

Proactive security vendors are pivoting into exposure management from several different directions and core competencies, and therefore, vary widely, as do product roadmap priorities. The number of vendors that currently claim to participate in this market easily runs into the dozens, and the diversity of vendors moving into the exposure management market has resulted in a variety of approaches. Omdia believes it is too early to suggest a common set of standard functionalities that customers should expect in exposure management products. We expect market activity (i.e., M&A) to accelerate in 2025 as a broad set of vendors act to fill perceived gaps in their capabilities.

Vendors in this market are making remarkably different bets on where the long-term value lies with these tools. These areas include:

- Delivering a data fabric that can ingest any security-related asset or exposure information.
- Understanding and communicating risk.
- Orchestration and automation of workflows to enable exposure remediation.
- Native integration with reactive and preventive security suites.

Omdia has long been expecting better integration between exposure management and vendors that have specialized in security control validation and attack path optimization. What we are seeing in 2025 is a blurring of the lines between these camps as exposure management becomes the preferred platform for almost all proactive security vendors.

Product/service overview

The Cymulate portfolio of SaaS offerings is based on the combination of 1) breach and attack simulation (BAS) to test and validate controls, and 2) continuous automated red teaming (CART) to target specific environments and assets. Additionally, the company has a strong threat intelligence capability, and Cymulate’s exposure validation capabilities are supported by a deep understanding of the active threat landscape. The company monitors active threats and tailors simulations to specific campaigns targeting verticals or geographies. The effectiveness of these tactics, techniques, and procedures (TTPs) can be validated against any customer environment through attack simulation.

Cymulate also supports internal context related to business risk. For example, Cymulate can group assets into pre-defined “business context” categories that present similar risks to the organization. Assets can be grouped according to business units, product lines, regions, and other relevant groupings.

CYNC’s contribution to the Cymulate portfolio

The CYNC Secure acquisition brings foundational data management capabilities to Cymulate. Using API-based tools, CYNC ingests, de-duplicates, and normalizes security findings related to assets and exposures to create an asset inventory.

CYNC’s risk prioritization engine can leverage external threat intelligence, and business impact evaluation, to create risk scores and prioritize exposures. The solution integrates with leading ticketing systems and supports the orchestration and automation of remediation recommendations. SLAs can be created and monitored with automated reminders and notifications, while analysts can monitor real-time analytics with role-specific dashboards.

Cymulate's AI Copilot

In August 2024, Cymulate released an AI Copilot based on large language models (LLM), allowing analysts to automatically create attacks using unstructured data inputs such as articles and social media posts. This Attack Planner determines potential steps to be executed in a proposed attack and then creates a logical flow between these steps to outline potential attack paths. These potential paths are mapped in a graph database to determine the shortest effective route of attack.

The generative AI solution allows analysts to deploy, test, and tune security controls to evaluate their effectiveness against these real-time threats. The company's goal is to enable a more continuous testing cadence in support of security posture drift detection.

Cymulate can also provide mitigation guidance with specific policy tuning and customized detection rules that can be pushed to controls. For example, a vulnerability present in a specific web infrastructure component can be tested to determine if it is effectively protected by a Web Application Firewall (WAF). Cymulate can also create and push new detection rules directly to SIEM, EDR, and XDR solutions.

Company/product information

Background

Cymulate was founded in 2016 with the goal of automating the process of pen testing. The company has built out a platform that delivers BAS, CART, and attack surface management (ASM). To help accelerate the jump into exposure management, Cymulate acquired CYNC Secure in early 2025.

Founded in 2022, CYNC Secure developed a platform designed to streamline the collection and normalization of data from a wide range of security solutions. The CYNC Secure technology enables security teams to prioritize vulnerabilities based on risk and impact, and to create actionable remediation recommendations.

Current position

Omdia expects exposure management solutions to become hubs for operational cyber risk management and, therefore, these solutions need to aspire to real-time monitoring of the security posture of an organization's entire digital domain.

This requires both internal and external context from which to asset risk. Some of this context can be acquired relatively painlessly. For example, checking which vulnerabilities are currently listed in CISA's Known Exploited Vulnerabilities (KEV). Other contexts, such as security control validation, require more effort and expertise. Vendors such as Cymulate, with core competencies in validation, need to demonstrate to exposure management customers that validation significantly improves risk assessment and prioritization.

Future plans

It is still relatively early in Cymulate's evolution within the exposure management market. The company has a planned release of an Exposure Management module for its Exposure Validation platform scheduled for the summer of 2025. The release will leverage the technology acquired from CYNC Secure and deliver exposure prioritization based on the correlation of 1) proven effectiveness of mitigating controls to prevent or detect an exploit, 2) asset criticality, and 3) threat intel.

As Cymulate continues to evolve, it will add visibility into more domains. The company supports external attack surface scanning but recognizes the need for broader domain expertise to offer full discovery. Currently, Cymulate can consume security findings from vulnerability scanners and Active Directory. Visibility into cloud security posture is in development and the company has road-mapped additional integrations for identity posture, CMDBs, OT scanners, and other attack surface management solutions. With the acquisition of CYNC Secure, Cymulate can now consume and analyze this additional data for other factors in addition to control effectiveness.

Key facts

Table 1: Data sheet: Cymulate

Product/Service name	Cymulate Platform	**Product classification**	Exposure validation Exposure management
Version number	NA (SaaS updated weekly)	**Version release date**	NA (SaaS updated weekly)
Industries covered	Banking & financial services IT & high-tech Healthcare Manufacturing & consumer goods Energy & utilities Transportation & logistics Retail Education	**Geographies covered**	Global: North America, Latin America, Europe, Middle East, South Africa, Asia Pacific (India, Australia, Japan, Singapore, etc.)
Relevant company sizes	Mid-to-large enterprise	**Licensing options**	SaaS subscription based on assets
URL	www.cymulate.com	**Routes to market**	Direct Value Added Resellers MSSPs

Source: Omdia

Analyst comment

As discussed, exposure validation is not the same as exposure management and, oddly, it is not even a standard component of many exposure management solutions. But that is only because it is difficult to achieve. Vendors focused on security control validation have been working for years to make their solutions easier to use and to operate on a cadence that can support the exposure management use case.

Exposure validation has the potential to significantly improve the risk assessment capabilities of exposure management solutions. Exposure management risk calculations should be informed by the continuous evaluation of compensating controls and determinations should be made regarding available mitigations supported with these controls. Even temporary mitigations can have a material impact on how exposures are prioritized.

The task for vendors taking this approach is to demonstrate superior risk reduction and quantify how much validation improves risk prioritization.

These vendors also need to position against a host of security control management and continuous control monitoring solutions that can deliver a level of security posture management with respect to existing security controls. These tools cannot test whether exposures are exploitable, but they can, at least, confirm that deployed security controls are turned on, properly configured, and up to date. Might that information supply enough context to achieve a “good enough” risk assessment for actionable prioritization?

Appendix

The On the Radar – Exposure Management Solutions reports are a series of profiles on leading services and/or solutions within a particularly dynamic market segment poised for growth and/or change. Omdia profiles solutions based on their potential impact on markets, as their capabilities, innovation, strategy, and growth could prove disruptive and of interest to tech buyers and users.

Further reading

Understanding the rapid emergence ofexposuremanagement (July 2024)

Fundamentals of Proactive Security (September 2023)

Author

Andrew Braunberg, Principal Analyst, SecOps

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com