SOLUTION BRIEF

Cymulate

Exposure Management

Challenges

Security leaders recognize that legacy approaches to security operations cannot answer the critical question, "How exposed is the organization?" To this end, exposure management, or continuous threat exposure management (CTEM), provides a framework for cybersecurity programs to view their cyber assets and support processes from the attacker's view of the organization. With this approach, organizations can identify the biggest gaps and prioritize appropriate remediation.

When applying exposure management into practice, cyber programs face the challenge of integrating programs like vulnerability management and threat detection and response. When bringing these practices together, security programs often struggle to:

- Understand their biggest weaknesses and gaps because domain-specific tools have a limited scope, such as endpoint, cloud, vulnerabilities, etc.
- Prioritize remediation and bigger initiatives because each domain has dozens of issues with vendor-specific scoring for each issue.
- Measure the true state of their security posture, prove resilience to new threats, and baseline improvements as the program matures.

Discover & Aggregate Weaknesses, Validate Exposure Risk

Security teams rely on Cymulate as the single source of truth for threat exposure risk and the actions required to minimize that risk. The Cymulate Exposure Management and Security Validation Platform provides the essential technologies, workflows, and metrics to drive exposure management programs. Cymulate combines full visibility of the attack surface with business context and the most advanced security validation to focus remediation and prove cyber resilience.

Through the automation of exposure discovery, security validation, and actionable remediation plans, Cymulate provides continuous assessments that transform one-off exercises into a repeatable program to strengthen security posture before the next attack.

Solution Benefits

MAXIMIZE EXISTING RESOURCES

"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

OPTIMIZE SECOPS & INCIDENT RESPONSE

"Cymulate enables us to test our defenses against the latest cyber threats as they emerge, prioritize remediation efforts, and improve our security team's incident response skills."

- CISO, Healthcare Organization

RATIONALIZE INVESTMENTS

"With Cymulate, we can present quantifiable data to the board and show a direct correlation between investments and the reduction in risk."

- Avinash Dharmadhikari, CISO, Persistent Systems

BENCHMARK SECURITY RESILIENCE

"Cymulate improved our risk management process and decision-making."

- Yoav Gefen, CISO, Maman Group

Cymulate

Scoping with Business Context to Baseline Security Posture

To deliver measurable results, exposure management must start with an understanding of where you are today and the related risks for the business. Cymulate baselines security posture for the entire attack surface across environments and adds business context to every asset across endpoints, systems, applications, clouds, and more.

Discovery with Native Assessments & Integrations for Risk-Profiled Asset Inventory

Cymulate provides native discovery of the attack surface and an open platform that integrates with security controls and IT infrastructure. By aggregating the findings from vulnerability scanners, security controls, configuration management, and more, Cymulate provides a consolidated view of all potential exposures while creating a risk-profiled asset inventory.

Prioritization based on Validated Threats & Potential Business Impact

To highlight the biggest weaknesses, Cymulate correlates all assets with their exposure risk and business context. This prioritization also considers the results from validated attack paths, the effectiveness of compensating controls to mitigate the threat, and the various options for remediation or mitigation.

Validation with Breach and Attack Simulation & Automated Red Teaming

Cymulate automates offensive security testing to validate controls, threats, and attack paths. Offering the most trusted security validation, Cymulate combines breach and attack simulation with automated red teaming to safely test how controls respond to threats and assess the potential for threats to move laterally to reach the crown jewels.

Mobilization with Comprehensive Remediation Guidance

To effectively address exposure risk and strengthen security posture, Cymulate provides detailed remediation plans backed by the proof and evidence provided through validation. Cymulate delivers actionable remediation guidance that includes all options for remediation (patching and configuration updates), mitigation through security controls, and potential business impact of the risk.

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.

Contact us for a private demo

Start Your Demo

info@cymulate.com | www.cymulate.com