SOLUTION BRIEF

Cloud Security Validation and Exposure Management

Challenges

As organizations increasingly rely on the cloud for critical operations, security teams frequently struggle to manage their threat exposure risk and measure the cyber resilience of their cloud environments.

The core concepts of identity, privileged access, segmentation, vulnerability assessments, and essential security controls are neither new nor unique to the cloud. Still, cloud security presents new challenges in the areas of:

- Visibility of the cloud environment attack surface (VMs, containers, shadow IT, and more)
- Misconfiguration and drift due to the dynamic nature of cloud deployments and their frequent updates
- Identity and access management that enables flexibility and rapid change but often leads to over-privileged users and the potential for abuse and privilege escalation

To manage cloud security risk posture, security teams need visibility, control validation, and focused mitigation for their cloud environments – just as they do for traditional IT. While each can be accomplished with a specialized cloud-focused tool, best practices for threat exposure management require a consolidated approach to cloud, on-prem, and hybrid environments.

Cymulate Cloud Security Validation and Exposure Management

The Cymulate platform provides security validation and exposure management for both cloud and on-premise environments with critical capabilities for the cloud across its entire product suite.

Add Business Context

Exposure management starts with scope, and cloud environments are no different. Cymulate enables organizations to scope their cloud exposures by including the business context to cloud resources. This provides an understanding of business impact related to cloud availability, sensitive data in cloud storage, and business processes supported by the cloud. Organizations use **Cymulate Exposure Analytics** to aggregate assets from cloud infrastructure and third-party tools (cloud security posture management, configuration management databases, etc.) and assign each asset one or more business contexts (business unit, programs, sensitivity to downtime, or other factors).

Identify Assets and Misconfigurations

Organizations must identify assets and misconfigurations across cloud, on-prem, and hybrid environments to discover the entire cloud environment and understand its cybersecurity posture. **Cymulate Attack Surface Management** allows companies to scan and identify assets and cloud misconfigurations around the cloud attack surface. Additionally, **Cymulate Exposure Analytics** pulls misconfigurations from CSPM, vulnerabilities from vulnerability scanners, and network security policies from the cloud infrastructure. With this centralized intelligence, Cymulate Exposure Analytics creates a risk-profiled asset inventory.

Solution Highlights

- Scope cloud exposure risk with context to business and impact on operations
- Identify assets and misconfigurations across clouds, on-prem, and hybrid environments
- Validate cloud controls, policies, and defensive capabilities
- Prioritize mitigation activity based on the context of business impact, compensating controls, and breach feasibility
- Mobilize cloud security teams with mitigation guidance based on risk reduction
- Measure cloud cybersecurity posture and baseline exposure risk

Validate Cloud Controls and Policies

Validating cloud controls, policies, and defensive capabilities allows organizations to evaluate their detection and response strategy regarding attackers who gain access to cloud environments. With **Cymulate Breach and Attack Simulation**, organizations test and validate controls and policies against attack scenarios that target identity and misconfiguration across the cloud infrastructure, VMs, and Kubernetes. Companies use **Cymulate Continuous Automated Red Teaming** to test and validate attack paths across cloud infrastructure, cloud-to-ground, and ground-to-cloud.

Prioritize Mitigation Activity

When security teams understand the context of business impact, compensating controls, and breach feasibility, they can prioritize mitigation activity. **Cymulate Exposure Analytics** enables organizations to correlate and prioritize cloud weaknesses and all IT gaps based on breach feasibility, business context, and risk reduction.

Mobilize Cloud Remediation

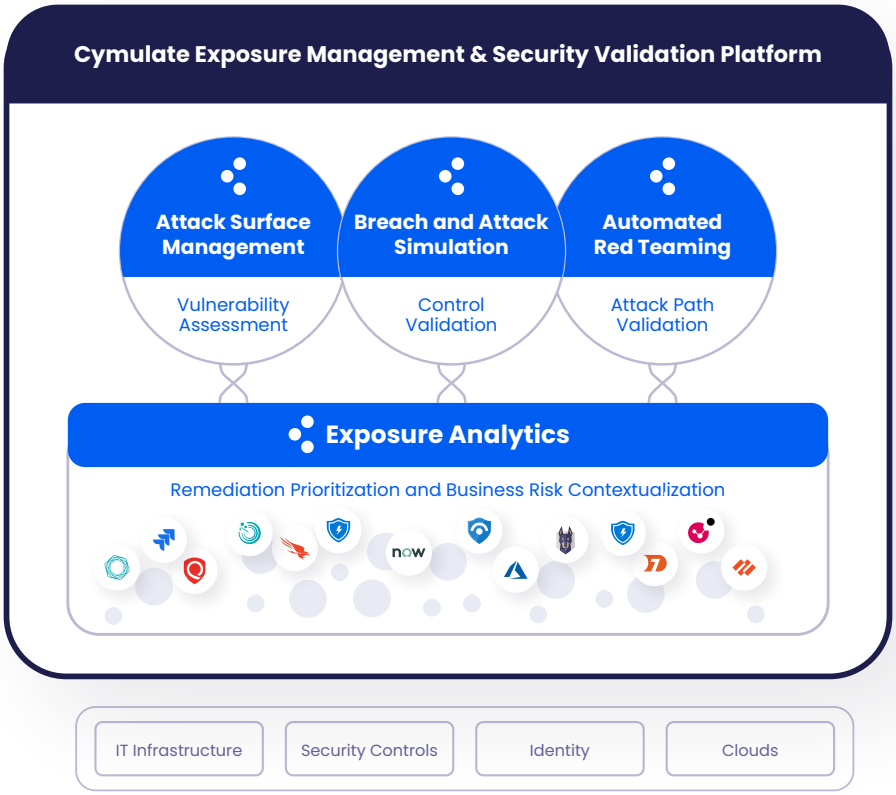
Cloud remediation guidance mobilizes teams to correct cloud misconfigurations or implement new policies or controls, resulting in security teams recognizing the business impact and accepting potential business disruption. With **Cymulate Exposure Analytics**, teams can plan remediation based on risk reduction and business context across all cloud, on-prem, and hybrid environments.

Measure Cybersecurity Posture

Cymulate Exposure Analytics provides organizations with a risk posture view of cloud environments. It also drills down into risk and cyber resilience, enabling teams to measure cybersecurity posture and baseline exposure risk for both cloud deployments and the cloud as part of the collective IT infrastructure.

Cymulate Cloud Exposure Management Capabilities

The Cymulate platform delivers comprehensive exposure management for the cloud and all IT environments with its integrated SaaS offerings across Attack Surface Management, Breach and Attack Simulation, Continuous Automated Red Teaming, and Exposure Analytics.



Cymulate Solution	Cloud Capabilities
Attack Surface Management (ASM)	• Discover cloud assets across AWS, Azure, and GCP to inventory VMs, storage objects, virtual private clouds, entitlements, Kubernetes containers, and more • Identify misconfigurations for both internal (authenticated) & external (un-authenticated) assets and deployments • Unified attack path mapping and analysis across multi-cloud, on-prem, and hybrid environments
Breach and Attack Simulation (BAS)	• Validate core controls (endpoint defenses, WAF, Web Gateways, etc.) for cloud assets against malicious behaviors, including those specific to cloud threats • Validate control detection of emergent threat activity against cloud assets with immediate threats
Breach and Attack Simulation (BAS) Advanced Scenarios	• Validate configuration best practices for cloud and Kubernetes policy configuration • Validate cloud controls against malicious activity targeted at user access, secrets management, data exfiltration, ransomware, container discovery, and more • Create, store, modify, and execute both simple and sophisticated assessments using custom or out-of-the-box resources with the Cymulate open framework
Continuous Automated Red Teaming (CART)	• Validate potential propagation within the cloud and from cloud to on-prem and back with automated network penetration testing
Exposure Analytics	• Collect data directly from cloud infrastructure and other third-party systems and align with business contexts to create risk-profiled asset inventory across clouds and all IT • Fully integrated with Cymulate ASM, BAS, and CART • Prioritize remediation for exposure risk in relation to all validated security gaps across the cloud, on-prem, and hybrid environments • Measure and baseline security resilience for cloud deployments • Map controls and security findings to control frameworks – including MITRE ATT&CK Cloud Matrix

Manage Cloud Exposure Risk as Part of a Continuous Threat Exposure Management Program

The Cymulate platform provides a comprehensive and scalable solution for security leaders, regardless of their security posture maturity, to manage cloud exposure risk as part of their continuous threat exposure management (CTEM) program and support both the technical and business requirements of scoping, discovery, prioritization, validation, and mobilization. With Cymulate cloud security validation and cloud exposure management, organizations can build a threat-informed defense for their cloud assets and environments.

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 5 continuous threat exposure management (CTEM) program pillars and on a business's ability to reduce risk by understanding, tracking, and improving its security posture. For more information, visit www.cymulate.com.

Let's get started

Request a demo

info@cymulate.com | www.cymulate.com