

SOLUTION BRIEF

Continuous Wiz Validation and Optimization

Easy, automated threat validation to optimize cloud security

Cloud environments can change by the minute, and traditional validation methods can't keep pace. Security teams require continuous assurance that their cloud threat detections work as intended, not just during a point-in-time test.

The Wiz–Cymulate integration bridges this gap by continuously validating Wiz Defend's threat detection and providing actionable insights to optimize coverage, accelerate detection engineering and strengthen threat resilience.

Test, validate and strengthen cloud threat detections

Wiz and Cymulate combine to deliver validated cloud security against the latest threats. Cymulate simulates advanced cloud and runtime attack scenarios to test and validate how cyber defenses prevent, detect and respond. By integrating Cymulate with Wiz, organizations can automate threat validation, security control testing and the development of new detection logic. The integration enables Cymulate to correlate Wiz detections and threat alerts with simulated attack activity, proving visibility and detection of advanced threats.

With easy, automated validation of cloud security, Cymulate provides:

- Metrics on validated threat detection to measure effectiveness
- Drift detection to identify decreases in Wiz Defend coverage
- Heatmaps and reporting mapped to MITRE ATT&CK, CIS and NIST 800-53
- Detection logic formatted for Wiz Defend, accelerating detection engineering and rule tuning

Build, tune and validate custom detection logic

Cloud detection engineering is a constant race against change. Even the best-configured cloud security solutions can lose effectiveness as threats, infrastructure and policies evolve. Misconfigurations, custom or incomplete rules can leave critical gaps, yet security teams often lack proof that their detections actually trigger when threats occur.

The Wiz Defend–Cymulate integration closes this gap by validating that Wiz detections, sensors and policies correctly identify simulated cloud threats. Cymulate safely runs offensive scenarios that create and modify cloud resources, while Wiz monitors and flags the resulting activity. Detection coverage is automatically correlated in Cymulate, helping teams see exactly what was detected and what was missed.

When a gap is identified, security teams can fine-tune Wiz-specific detection logic and immediately retest with Cymulate, accelerating detection engineering, enhancing rule quality and validating fixes in real-time. The result is measurable detection confidence, reduced exposure and continuously optimized cloud resilience across AWS, Azure and Google Cloud.

Solution Benefits



Validate Threats

Confirm Wiz sensors, policies and detections by running Cymulate automated attack simulations.



Optimize detection

Continuously test and tune Wiz Defend detection logic to maximize threat coverage and accuracy.



Identify drift

Immediately recognize when configuration changes cause a decrease in threat coverage.



Baseline threat coverage

Validate security across AWS, Azure and Google Cloud with alignment to MITRE and NIST.

Spot security drift early with posture baselines and trend reports

Cymulate continuously validates Wiz Defend against emerging threats, exploits and techniques, giving security teams clear, evidence-based metrics for detection performance. Trending dashboards and executive-ready reports enable easy baselining of security posture over time, demonstrating improvement and communicating results to leadership and auditors. Cymulate also maps Wiz Defend detection coverage to frameworks such as MITRE ATT&CK and NIST 800-53, providing heatmaps that clearly identify strengths and weaknesses.

As cloud environments and control configurations change, security posture can erode. Cymulate detects this security drift by comparing current validation results against historical baselines and highlighting decreases in Wiz Defend threat coverage. When gaps appear, Cymulate provides a clear mitigation path, including newly generated detection rules, to restore and strengthen protection.

Why choose Cymulate for validating and optimizing Wiz?

 <p>Automated Validation</p> <p>Pre- and post-exploitation assessments to test controls and policies for different layers of cloud architecture.</p>	 <p>Production safe</p> <p>The full suite of test cases is completely production-safe and will not harm cloud environments.</p>	 <p>Adapt to New Threats</p> <p>Actionable and automated findings to maximize threat detection for the most effective threat coverage.</p>
--	---	--

Cymulate-Wiz Integrations

 **Exposure Validation**

Attack Scenarios		
Daily Threat Feed	Assessment Templates	Custom Attacks
⌵		⌵
Assessment Results		
Security Gaps	MITRE Heatmap	Alerts & Logs
⌵		⌵
Mitigations		
Threat Updates	Guided Configuration	Detection Logic

Production-safe attack simulation targeted at cloud deployments

Integrations send Wiz alerts, logs and attack actions of Cymulate attack simulations

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.