JOINT SOLUTION BRIEF

zscaler™ +

Cymulate

Test and optimize your cyber security defenses using real-world attack simulations.

cymulate

INTEGRATION HIGHLIGHTS

- Production-safe, automated security validation
- Threat detection and response optimization
- Baseline security posture and security drift identification

The Market Challenge

Organizations frequently encounter gaps in their defenses caused by hidden vulnerabilities, unvalidated security controls, misconfigurations, and inefficient threat response processes. For security programs to remain effective, it is essential to promptly identify weaknesses, assess the effectiveness of security measures, and prioritize risks. With the rapid evolution of cloud applications and remote work environments, new threat vectors emerge that can bypass traditional defences. It is imperative that security controls are continuously tested and validated.

Breach Attack Simulation (BAS) platforms address this critical challenge of ensuring cybersecurity measures are both effective and comprehensive by

- proactively enhancing organizational cyber defences
- improving incident readiness
- meeting compliance requirements

while minimizing operational complexity and reducing the likelihood of breaches.

The Solution

The Cymulate Exposure Validation Platform integrates with ZIA to continuously test and validate security effectiveness with actionable and automated mitigations that boost detection for any identified gap. With breach and attack simulation and automated red teaming, the Cymulate platform tests different types of web-based threats and malicious content to fully challenge ZIA's effectiveness.

Through this integration, Cymulate provides ZIA users with:

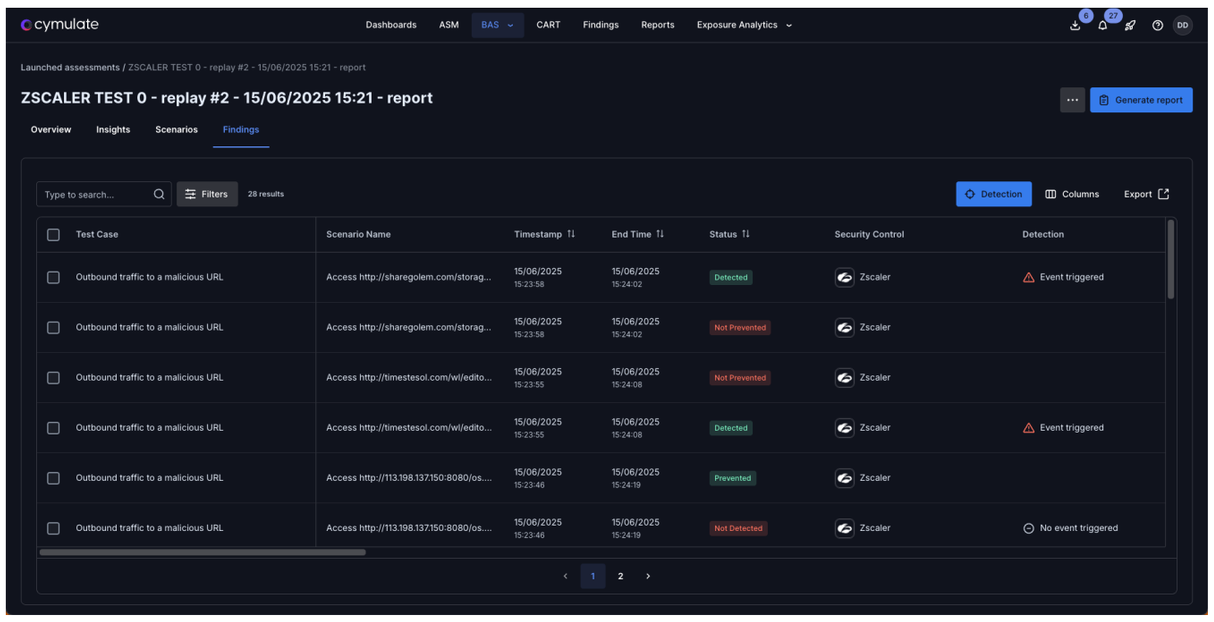
- Automated updates of IoCs for immediate prevention
- Mitigation recommendations for modifying gaps
- Drift detection to identify decreases in threat detection
- Executive, technical and compliance reports backed by evidence of security effectiveness

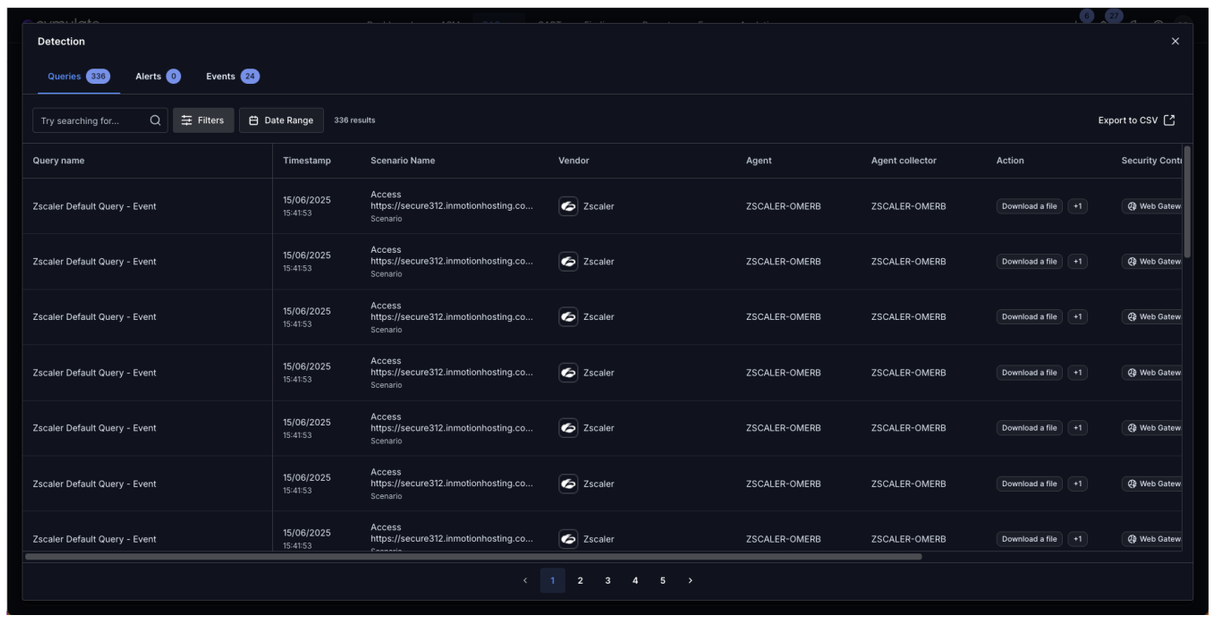
Together, Zscaler and Cymulate deliver a cloud-based, end-to-end zero trust solution that provides users continuous validation and optimization of security controls to ensure organizations are always a step ahead of the evolving threats.

Solution Components Deep Dive

Cymulate validates detection in ZIA by correlating events from the Zscaler API with Cymulate assessment findings. During assessments, the Cymulate agent actively simulates threat scenarios by leveraging IOCs of URLs and file paths. It does so by attempting to access URLs categorized as malicious and by downloading files identified as threats.

After the assessment, Cymulate queries the Zscaler API to determine whether Zscaler's Zero Trust Exchange has logged any events, ensuring a comprehensive evaluation of your detection capabilities.





KEY USE CASES

Optimize Threat Detection and Response

With a daily update of the latest threats, Cymulate continuously tests and proves the effectiveness of ZIA in detecting advanced cyber attacks. Cymulate also provides mitigation guidance to help optimize control and enhance policies. Furthermore, for threats not detected, Cymulate includes automated mitigation that can push new IoCs directly to ZIA for immediate threat prevention. For speed and ease of use, Cymulate aggregates the recommended IoC updates and allows security teams to push the new IoCs in a single update.

Baseline Security Posture and Identify Security Drift

By continuously validating ZIA against new threats, exploits and the latest techniques, Cymulate provides security teams and leaders with evidence-based metrics for threat detection, with trending and baselined results over time. Dashboards and reports make this trending data easily accessible for security leaders to present in executive meetings, create board reports and share with auditors. Because updates to control configurations and changes in IT infrastructure can impact security posture, security teams rely on Cymulate to identify security drift.

Today's security challenges require defence in depth. Zscaler + Cymulate are key components in the security stack that help advance overall security posture. Together, Zscaler + Cymulate automate the threat protection, validation and optimization required to continuously prove and improve threat resilience.

Nir Krumer

VP of Product Management, Cymulate

Zscaler + Cymulate Benefits

ACTION	DESCRIPTION
Validate ZIA continuously	Proactively validate ZIA policies with automated, continuous testing, ensuring real-time visibility into security effectiveness and risk exposure.
Maintain prevention	Stay ahead of emerging threats with automated validation of Zscaler's threat prevention capabilities, confirming defenses are up to date and functioning as intended.
Optimize detection	Configure, test and tune detection rules to minimize false positives and optimize threat coverage.
Identify security drift	Quickly identify and address unintended gaps in Zscaler protection caused by policy changes, infrastructure updates or misconfigurations before attackers exploit them.

Conclusion

Deliver better business results with Zscaler and Cymulate

By simulating real-world attack techniques and testing ZIA in production, Cymulate ensures that security policies are aligned with business intent and optimized against evolving threats. This proactive approach eliminates blind spots and ensures threat prevention, detection and response are always tuned and effective. The outcome: stronger cyber resilience, faster incident response and a continuously hardened Zero Trust posture, without increasing operational complexity.

Learn more at **www.zscaler.com/partners/technology**

zscaler™ | Experience your world, secured.™

About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.