SafeBreach

zscaler™

JOINT SOLUTION BRIEF

# Continuously Measure & Optimize Your Hybrid, Multi-Cloud Security Posture

Empower your security team against constantly evolving network and cloud threats with a joint solution that combines continuous security validation—powered by the SafeBreach breach and attack simulation (BAS) platform—with Zscaler Internet Access™ (ZIA).

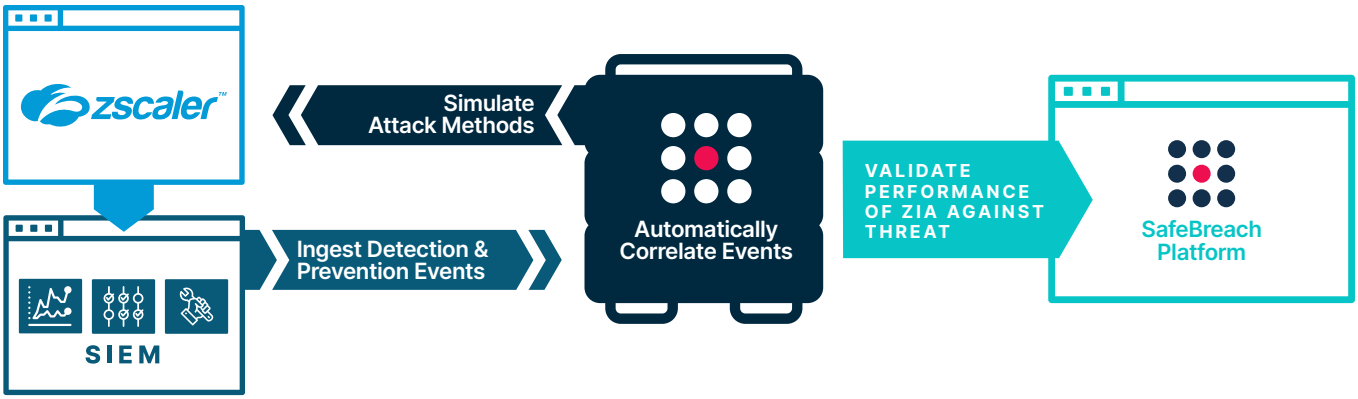
SAFEBREACH.COM


Security operations teams are finding it increasingly difficult to maintain a hardened posture against evolving network and cloud threats. Threat actors continually adapt their methods to evade traditional perimeter security solutions, and the rapid adoption of cloud platforms and SaaS tools has dramatically expanded the attack surface. One small control misconfiguration can create a security gap that attackers can easily exploit.

The SafeBreach and Zscaler joint solution helps security organizations combat these challenges by effectively validating and optimizing their deployed network and cloud security controls. The offering combines continuous security validation—powered by the SafeBreach breach and attack simulation (BAS) platform—with Zscaler Internet Access™ (ZIA), a comprehensive suite of AI-powered security and data protection services designed to stop cyberattacks and data loss. Together, SafeBreach and ZIA empower security teams to proactively test their defenses to prevent network and cloud attacks that use malicious domains, URLs, connections with malicious servers and blacklisted IP addresses.

SafeBreach

FOR MORE INFORMATION OR TO REQUEST A DEMO, VISIT: **SAFEBREACH.COM**




## How the Integration Works

SafeBreach safely executes various web attacks that trigger ZIA's detection and prevention capabilities to validate that potential attacks are visible and appropriate alerts are configured. ZIA security events and alerts are forwarded to a SIEM and continuously fetched and correlated by SafeBreach to provide visibility per simulated attack. This allows SafeBreach to accurately determine if ZIA was able to detect or prevent network/cloud threats or if the threat was missed. This additional context (including results of simulated attacks and associated remediation information) is available to security analysts via SafeBreach Insights to appropriately update ZIA to detect and prevent such attacks in the future.

## Benefits of the Integration – Together SafeBreach & Zscaler Internet Access:

- Provides unparalleled visibility into network and cloud readiness and enterprise security posture
- Enables continuous improvement of alerting accuracy and prevents drift in detection rules
- Optimizes prevention and detection abilities of ZIA against advanced cloud and network threats
- Automatically correlates simulation results and SIEM event logs to simplify and expedite threat investigation, analysis, and remediation.

**USE CASE 1**

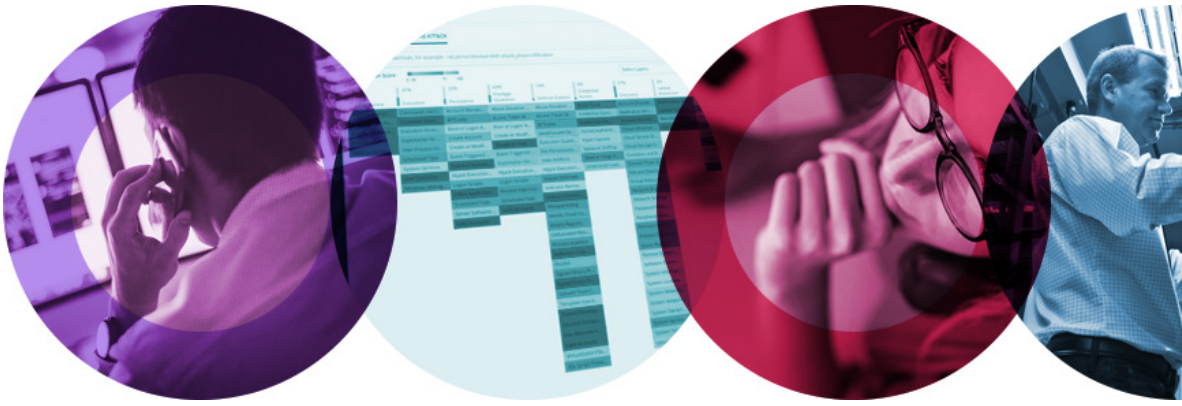
# Validate Internet & Cloud-Access Configurations & Policies

## Challenge

Security teams have traditionally focused on securing network gateways against advanced threats. However, as traffic patterns shifted to the internet and applications moved to the cloud, user traffic began bypassing traditional network gateways and going straight to the cloud. This led to the addition of several new security controls, increasing the chances of security control misconfiguration that can create exploitable security gaps.

## Solution

SafeBreach validates the security posture by executing attacks from known threat groups, safely and continuously, to bring visibility into which network and cloud controls prevented an attack and which attacks sailed past them. The dedicated SafeBreach Labs team monitors the threat landscape 24/7 to ensure the SafeBreach Hacker's Playbook includes coverage for the latest indications of compromise (IOCs) and tactics, techniques, and procedures (TTPs). The integration with Zscaler tests advanced attacks against ZIA to validate which threats and associated IOCs were blocked. In the case of any IOCs and threats being missed, SafeBreach Insights provides security teams with raw IOC data that can be used to optimize Zscaler threat detection.



**USE CASE 2**

# Improve Efficacy of Security Operations Against Network & Cloud Threats

## Challenge

Security teams analyze and process network and cloud alerts collected in a security information and event management (SIEM) system. This data is often correlated using user-defined rules to discover trends, detect threats, and investigate alerts across network and cloud deployments. However, data reported back to the SIEM by misconfigured security controls may not accurately indicate the severity of the network/cloud threat or provide enough contextual information to make accurate remedial decisions. This can lead to incorrect correlation of threat data, reducing the efficacy of the security operations center (SOC) team, causing them to miss critical threats and delay remedial threat response.

## Solution

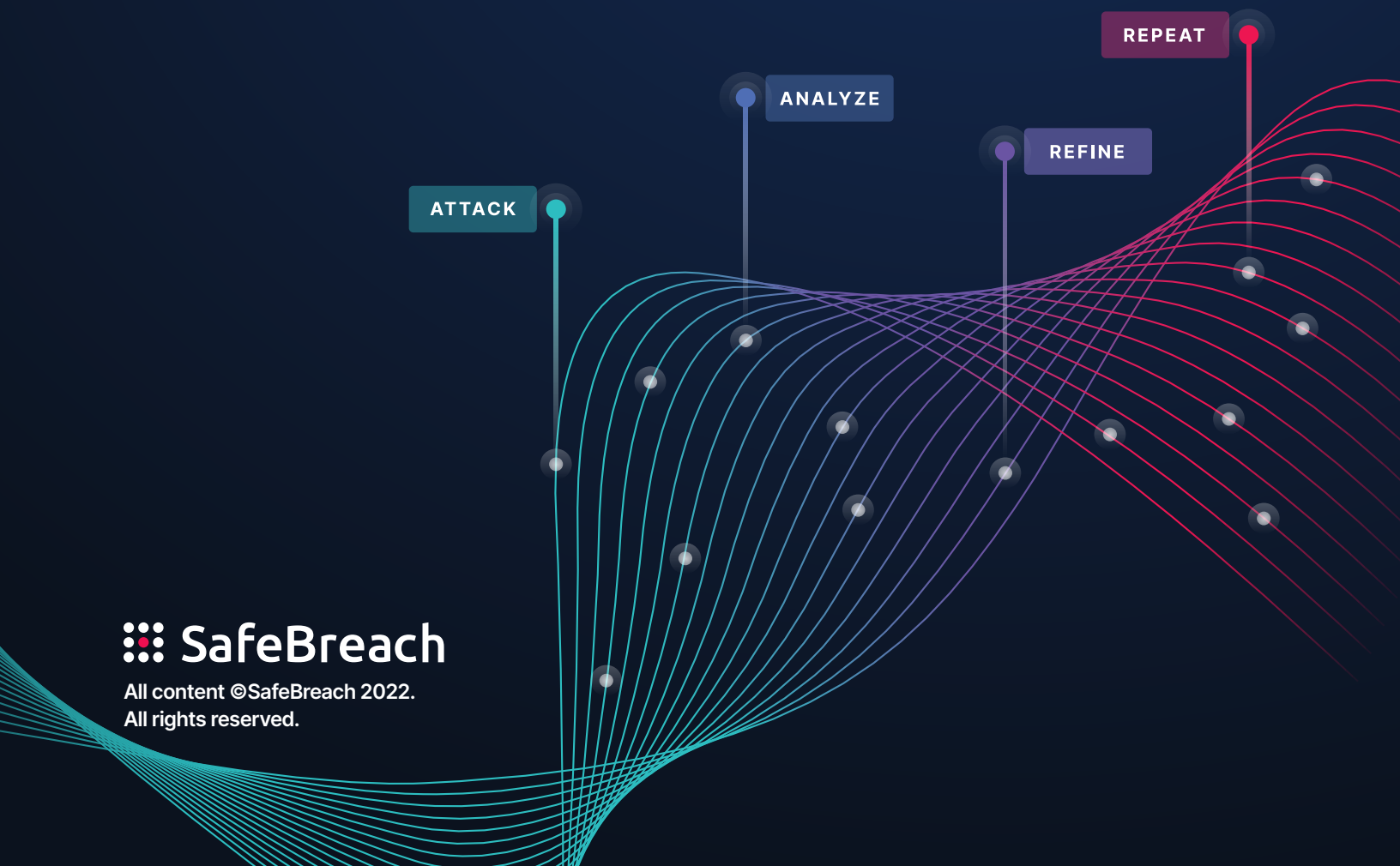
SafeBreach continually validates ZIA to ensure its efficacy against evolving cloud and network threats. Insights from this validation can be correlated with corresponding SIEM alerts/events to ensure they are accurate tracking in your SIEM, thereby measuring the efficacy of your Zscaler security control. SafeBreach Insights also provide security teams with the necessary contextual data required to build new alerts for previously missed network/cloud threats, thereby improving the detection accuracy of ZIA while reducing the mean time to detect and respond.

## About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

## About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital trans-formation so 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 SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.




SafeBreach