ATTACKIQ®

zscaler™

Solution Brief

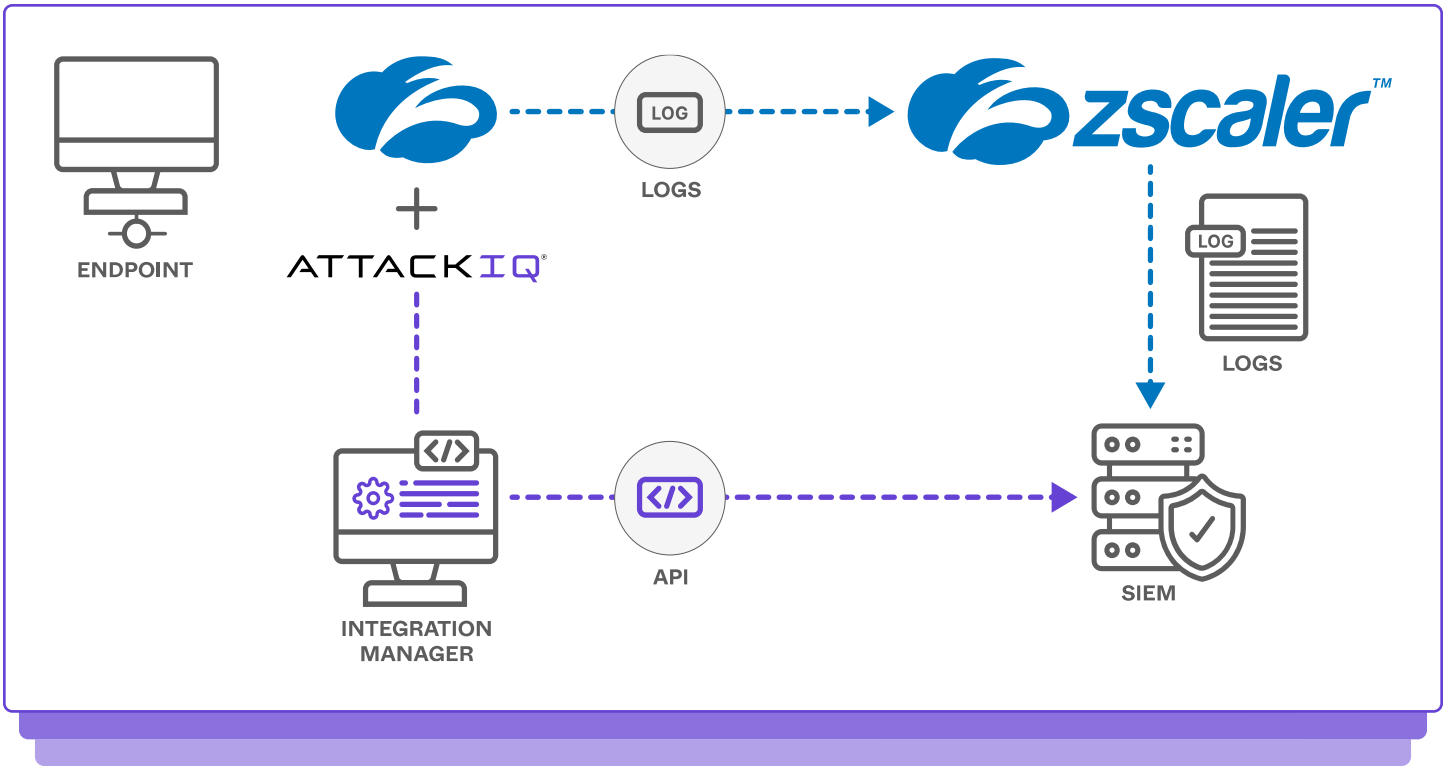
AttackIQ and Zscaler

The AttackIQ's Security Optimization Platform and Zscaler ZIA Integration

Continuously Validate Your Security Efficacy

Ensuring a security stack is configured correctly can be challenging. Traditional security stacks leveraging different point solutions creates complexity and potential gaps. Zscaler's Zero Trust Exchange delivers a complete security stack through a Secure Services Edge (SSE) architecture, delivered as a service from the cloud.

The AttackIQ Platform integrates with Zscaler by continuously examining activity logs to conduct ongoing assessments, confirm, and provide feedback on security effectiveness. It safely conducts simulations of attacks, including advanced threats and data exfiltration, and evaluates them against Zscaler's detection and prevention capabilities.



Integration Benefits

- Validate the effectiveness of ZIA policies by simulating real-world attack scenarios. Ensure that your ZIA deployment is configured to provide maximum security while minimizing false positives.
- The integration of Zscaler ZIA with AttackIQ helps identify which attacks are detected, prevented, or missed on the endpoint.
- Validate defenses against real-world threats aligned to MITRE ATT&CK, informed by AttackIQ's founding research partnership with the Center for Threat-Informed Defense
- Generate significant savings across the organization by improving your technology and team performance.

How It Works

To validate your existing Zscaler ZIA setup, follow these simple steps:

1. Install the AttackIQ agent on an endpoint protected by Zscaler ZIA.
2. Install the AttackIQ integration manager and configure the SIEM integration to validate Zscaler ZIA logs.
3. Create emulations of the threats you wish to evaluate your defense systems against.
4. Analyze the insights about the level of protection and detection provided by Zscaler ZIA.
5. Mitigate the critical gaps based on the findings.

Key Use Cases

Continuous Security Validation for Zscaler ZIA Policies

The AttackIQ Platform empowers organizations to assess and evaluate the effectiveness of their Zscaler ZIA policies in safeguarding against the most recent threats. When vulnerabilities or deficiencies are detected, the platform assists in quantifying their consequences and refining current toolsets to mitigate them.

MITRE ATT&CK Threat Emulation and Detection Engineering

AttackIQ's Platform improves detection capabilities and makes detection engineering easy by automatically emulating adversary behaviors aligned to the MITRE ATT&CK framework, focusing your organization on threats that matter most. AttackIQ runs continuous tests against Zscaler ZIA, emulating adversarial techniques to test detection and prevention, and by identifying gaps that you may need to fill with new capabilities. Together, AttackIQ and Zscaler ZIA emulate and stop breaches before they impact your organization.

Security Posture Management

Through the AttackIQ Platform, security leaders gain greater visibility into their security stance by evaluating and measuring the efficiency of security measures in thwarting, identifying, and responding to threats across the entire cyber kill chain.

AttackIQ Platform

AttackIQ is the industry-leading provider of breach and attack simulation products for security control validation. AttackIQ emulates adversary tactics, techniques, and procedures, aligned to the MITRE ATT&CK framework, and provides visibility into your security program performance with clear data-driven analysis and mitigation guidance. AttackIQ products are built on the company's core emulation platform, which tests adversary tactics, techniques, and procedures with realistic attack scenarios and real-time performance metrics and recommendations

The Value of AttackIQ

Improved Efficiency

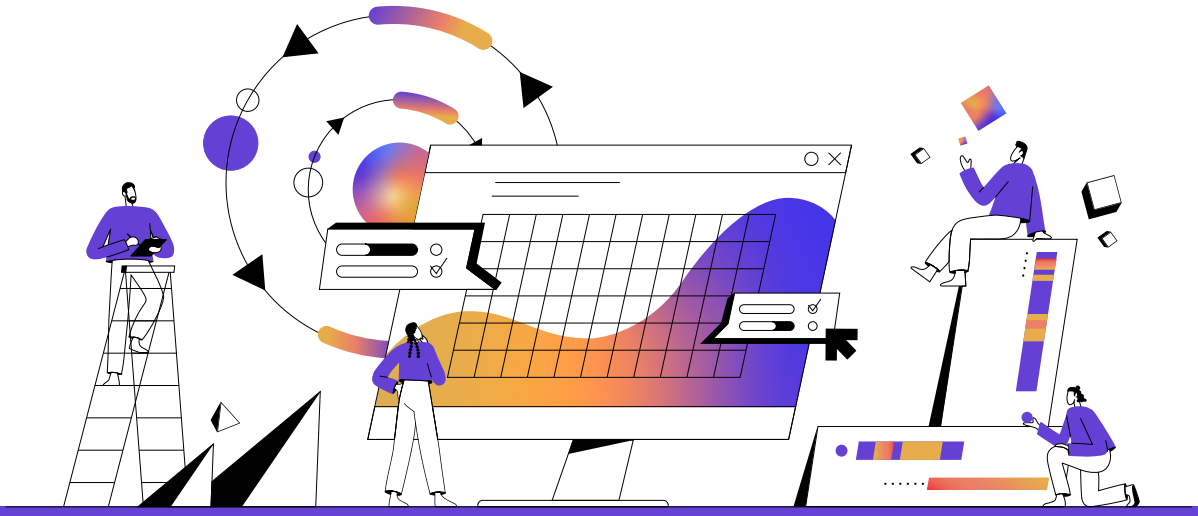
Customers benefit from a 57% efficiency increase in red team staff, roughly $80K per year in testing costs. By quickly identifying and prioritizing risks, security leaders can focus investments, while security teams see a 47% increase in efficacy by prioritizing vulnerabilities and measuring security controls' effectiveness.

Flexible Consumption

Flexible testing options that fits your business needs and maturity, comanaged, self-managed, or testing as a service with the industry's first agentless testing solution.

Faster Time to Value

Proactively identify and remediate risks in hours, not weeks. The AttackIQ platform enables organizations to get answers to security risk questions fast with form factors that fit their business needs.



About AttackIQ, Inc.

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency.

AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework.

The Company is committed to giving back to the cybersecurity community through its free award-winning AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat-Informed Defense.

For more information, visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.

About Zscaler, Inc.

Zscaler (NASDAQ: ZS) accelerates digital transformation 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.

ATTACKIQ
U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ
AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.