SafeBreach

Akamai

JOINT SOLUTION BRIEF

Transform Zero Trust Segmentation with Continuous Attack-Based Validation

Extend your security strategy by unifying SafeBreach's Exposure Validation Platform with Akamai Guardicore's microsegmentation platform to deliver continuous exposure visibility, validated Zero Trust enforcement, and measurable risk reduction.

SAFEBREACH.COM

Organizations invest heavily in Zero Trust strategies and microsegmentation to limit attacker movement and reduce business risk. Yet even with these controls deployed, segmentation policies can drift, misconfigurations can open unintended pathways, and attackers can still exploit lateral movement opportunities undetected.

With SafeBreach and Akamai Guardicore, enterprises can continuously validate the effectiveness of segmentation policies, uncover lateral movement risks before attackers do, and ensure Zero Trust controls operate as intended—every day, against the latest attacker techniques.

THE CHALLENGE

Enterprise environments rarely sit still. Teams spin up new apps, migrate workloads, and adjust infrastructure faster than security teams can document it. In this constant motion across hybrid and multi-cloud architectures, segmentation rules can quietly drift, becoming outdated or overly permissive.

This creates:

- Unintended lateral movement paths
- Policy drift and misaligned enforcement
- Blind spots across east–west traffic
- Difficulty proving segmentation effectiveness to auditors, insurers, and CISOs
- A lack of continuous validation that Zero Trust controls are working

Attackers rely on this complexity. One compromised endpoint becomes a foothold for privilege escalation, ransomware propagation, or access to crown-jewel systems.

THE SOLUTION

SafeBreach Tests; Akamai Guardicore Defends

SafeBreach serves as the validation layer for Zero Trust, continuously emulating attacker behavior inside segmented environments. Akamai Guardicore acts as the enforcement layer, applying and managing microsegmentation policies to contain threats and limit east–west traffic.

Together, they provide continuous assurance that segmentation isn't just configured, but truly effective.

The integration enables organizations to:

- Test Akamai Guardicore segmentation policies with real-world attack simulations
- Detect misconfigurations or overly permissive traffic rules before attackers exploit them
- Quantify the impact of segmentation on stopping attacker movement
- Validate Zero Trust architectures across ransomware, privilege escalation, and lateral movement scenarios
- Produce evidence-based compliance artifacts demonstrating control effectiveness for frameworks such as DORA, PCI DSS, and NIST 800-207

How the Integration Works

SafeBreach simulates attacker behavior across the environment—including credential theft, reconnaissance, SMB/RDP-based movement, privilege escalation, and ransomware propagation. These simulations reveal which lateral movement attempts would succeed or fail based on the existing segmentation rules.

Akamai Guardicore then provides deep visibility into which policies blocked the attack, which flows remained open, and where segmentation must be hardened.

Integration outputs include:

- SafeBreach simulation findings mapped to Akamai Guardicore segmentation policies
- Reports showing segmentation gaps, overly permissive rules, and recommended remediation steps
- Metrics demonstrating exactly where Akamai Guardicore stopped attacks and where risks remain
- Dashboards enabling continuous tracking of Zero Trust posture over time

Benefits of the Integration

1. Validate Zero Trust Controls

Confirm that segmentation policies actually prevent real attacker behaviors—not just on paper, but in practice.

2. Quantify Risk Reduction

SafeBreach provides measurable outcomes showing which attacks Akamai Guardicore blocked and which require remediation.

3. Optimize Segmentation Configurations

Continuous testing identifies misconfigurations, unused rules, and unintended open pathways.

4. Improve Resilience Across the Kill Chain

Organizations can validate detection, response, recovery, and governance processes end-to-end.

5. Strengthen Compliance & Auditability

Demonstrate segmentation effectiveness for DORA, PCI DSS, NIST 800-207, and cyber insurance requirements.

USE CASE 1

Validate & Optimize Microsegmentation Policies

CHALLENGE

Segmentation rules often drift from intended design due to environmental change. Without continuous validation, it's difficult to know whether policies truly block lateral movement, privilege escalation, or ransomware propagation attempts.

SOLUTION

SafeBreach simulates attacker techniques across segmented zones, revealing every possible path an attacker would attempt. Akamai Guardicore shows whether those paths are blocked, misconfigured, or overly permissive. Together, they provide actionable insights to optimize policies and close gaps proactively.

USE CASE 2

Stop Lateral Movement & Reduce Blast Radius

CHALLENGE

Even with strong perimeter defenses, lateral movement remains one of the most common breach escalation techniques. Attackers exploit east–west traffic to reach high-value assets, expand privileges, and deploy ransomware.

SOLUTION

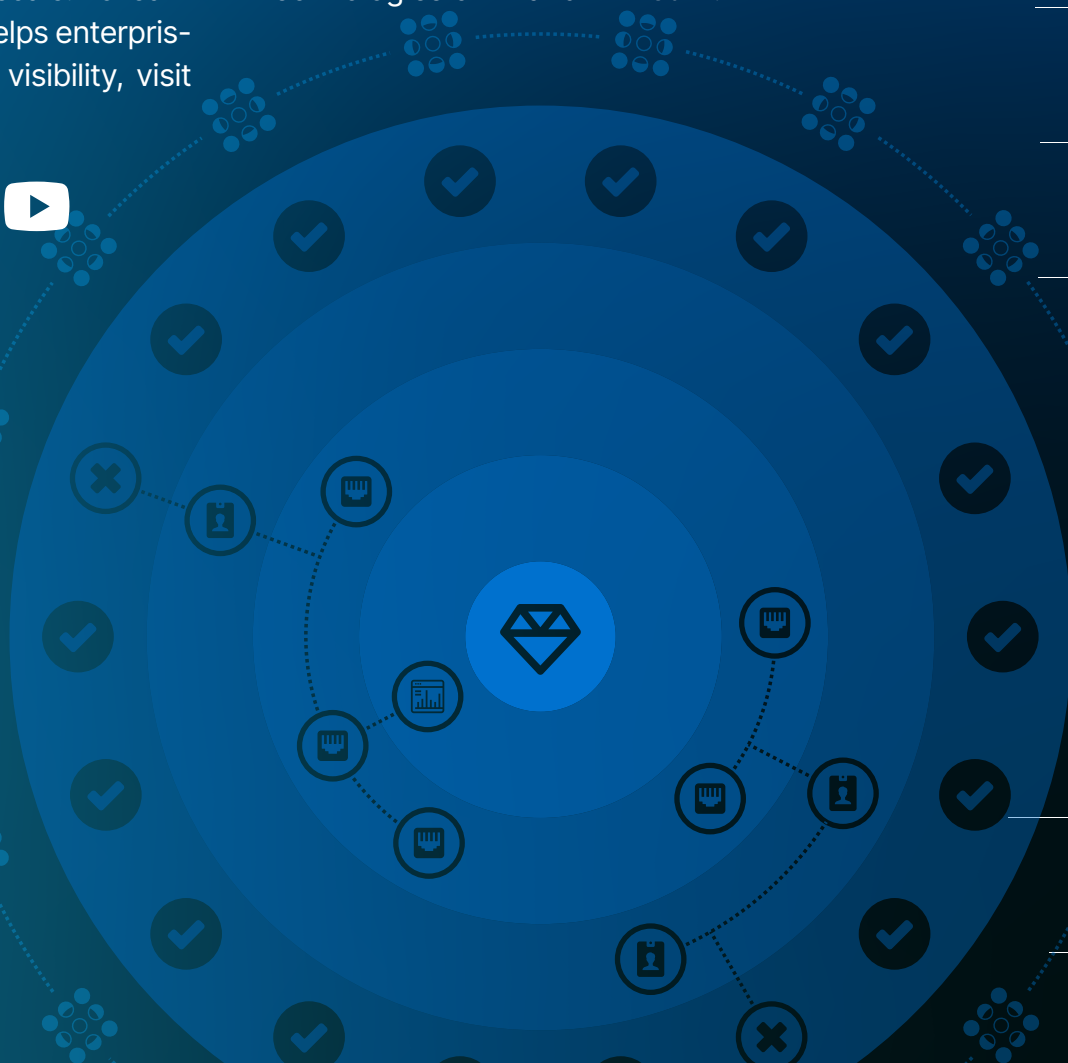
SafeBreach Propagate identifies all lateral movement opportunities inside the environment, from credential misuse to service exploitation. Akamai Guardicore enforces microsegmentation to prevent those movements, effectively reducing blast radius and stopping ransomware spread before it begins.

About SafeBreach

SafeBreach is the leader in enterprise-grade exposure validation, providing the world's largest brands with safe and scalable capabilities to understand, measure and remediate threat exposure and associated cyber risk. The award-winning SafeBreach exposure validation platform combines pioneering breach and attack simulation and innovative attack path validation capabilities to help enterprise security teams measure and address security gaps at the perimeter and beyond. Backed by a world-renowned original threat research team and world-class support, SafeBreach helps enterprises transform their security strategy from reactive to proactive safely and at scale. To learn more about how SafeBreach helps enterprises with end-to-end exposure visibility, visit **www.safebreach.com**.

About Akamai

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence. Learn more at **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X** and **LinkedIn**.



SafeBreach