Akamai-Lösungsüberblick

Transformation der Zero-Trust-Segmentierung mit kontinuierlicher angriffsbasierter Validierung

Unternehmen investieren stark in Zero-Trust-Strategien und Mikrosegmentierung, um Angreifer in ihrer Beweglichkeit zu begrenzen und Geschäftsrisiken zu reduzieren. Doch selbst mit diesen Kontrollmaßnahmen können Segmentierungsrichtlinien abweichen, Fehlkonfigurationen können unbeabsichtigte Pfade öffnen und Angreifer können weiterhin Möglichkeiten zur lateralen Netzwerkbewegung unentdeckt ausnutzen.

Erweitern Sie Ihre Sicherheitsstrategie, indem Sie die Exposure Validation Platform von SafeBreach mit der Mikrosegmentierungsplattform von Akamai Guardicore vereinheitlichen, um eine kontinuierliche Expositionstransparenz, eine validierte Zero-Trust-Durchsetzung und eine messbare Risikominderung zu gewährleisten. Mit Akamai und SafeBreach können Unternehmen das Risiko lateraler Netzwerkbewegungen erkennen, bevor Angreifer dazu in der Lage sind. So lässt sich sicherstellen, dass Zero-Trust-Kontrollen wie vorgesehen funktionieren – jeden Tag und auch gegen die neuesten Angreifertechniken.

Die Herausforderung

Unternehmensumgebungen stehen selten still. Teams entwickeln neue Anwendungen ein, migrieren Workloads und passen die Infrastruktur schneller an, als Sicherheitsteams sie dokumentieren können. Bei dieser konstanten Bewegung über Hybrid- und Multicloud-Architekturen hinweg können Segmentierungsregeln unbemerkt abweichen, veraltet werden oder zu viele Freigaben erteilen.

Die Folgen:

- unbeabsichtigte Pfade für laterale Netzwerkbewegung
- Richtlinienabweichung und falsch ausgerichtete Durchsetzung
- blinde Flecken im East-West-Traffic
- Schwierigkeiten beim Nachweis der Segmentierungseffektivität gegenüber Auditoren, Versicherern und CISOs
- fehlende kontinuierliche Validierung, ob die Zero-Trust-Kontrollmaßnahmen funktionieren

Angreifer setzen auf genau diese Komplexität. Ein kompromittierter Endpunkt kann Angreifern genügen, um Privilegien zu eskalieren und Ransomware zu verbreiten oder den Zugriff auf wichtige Ressourcen zu erlangen.

Die Lösung: SafeBreach testet und Akamai Guardicore schützt

SafeBreach dient als Validierungsebene für Zero Trust und emuliert kontinuierlich das Angreiferverhalten in segmentierten Umgebungen. Akamai Guardicore fungiert als Durchsetzungsebene und wendet Mikroregmentierungsrichtlinien an, um Bedrohungen einzudämmen und den East-West-Traffic zu begrenzen.

Gemeinsam können beide Tools kontinuierlich sicherstellen, dass die Segmentierung nicht nur korrekt konfiguriert ist, sondern auch tatsächlich effektiv wirkt.

Vorteile für Ihr Unternehmen

Zero-Trust-Kontrollen validieren
Stellen Sie sicher, dass Segmentierungsrichtlinien echtes Angreiferverhalten verhindern – nicht nur auf dem Papier, sondern in der Praxis.

Risikominderung quantifizieren
SafeBreach liefert messbare Ergebnisse und zeigt an, welche Angriffe von Akamai blockiert wurden und wo Maßnahmen getroffen werden müssen.

Segmentierungskonfigurationen optimieren
Durch kontinuierliche Tests werden Fehlkonfigurationen, ungenutzte Regeln und unbeabsichtigt geöffnete Pfade identifiziert.

Über die gesamte Kill Chain hinweg die Resilienz erhöhen
Unternehmen können Prozesse für Erkennung, Reaktion, Wiederherstellung und Governance von Anfang bis Ende validieren.

Compliance und Auditfähigkeit verbessern
Demonstrieren Sie die Segmentierungseffektivität für DORA, PCI DSS, NIST 800-207 und Anforderungen für Cyberversicherungen.

Akamai

Die Integration ermöglicht es Unternehmen:

- die Segmentierungsrichtlinien von Akamai Guardicore mit realen Angriffssimulationen zu testen
- Fehlkonfigurationen oder übermäßig zulässige Trafficregeln zu erkennen, bevor Angreifer sie ausnutzen können
- die Effizienz der Segmentierung beim Eingrenzen von Angreiferbewegungen zu quantifizieren
- Zero-Trust-Architekturen in Bezug auf Ransomware, Berechtigungseskalation und laterale Netzwerkbewegungsszenarien zu validieren
- evidenzbasierte Compliance-Artefakte zu erstellen, die die Effektivität der Kontrolle für Frameworks wie DORA, PCI DSS und NIST 800-207 belegen

So funktioniert die Integration

SafeBreach simuliert das Verhalten von Angreifern in der gesamten Umgebung – dies schließt Methoden wie den Diebstahl von Anmeldedaten, Aufklärung, SMB/RDP-basierte Bewegung, Privilegieneskalation und Ransomware-Verbreitung ein. Diese Simulationen zeigen auf, welche lateralen Bewegungsversuche die bestehenden Segmentierungsregeln verhindern würden und welche Erfolg hätten.

Akamai Guardicore bietet dann umfassende Transparenz in die Richtlinien, die den Angriff blockiert haben, welche Flüsse offen blieben und wo die Segmentierung verstärkt werden muss.

Die Integration gibt unter anderem diese Informationen aus:

- Ergebnisse der SafeBreach-Simulation, die den Segmentierungsrichtlinien von Akamai Guardicore zugeordnet sind
- Berichte über Segmentierungslücken, übermäßig zulässige Regeln und empfohlene Abhilfemaßnahmen
- Kennzahlen, die genau darstellen, wo Akamai Guardicore Angriffe gestoppt hat und wo Risiken bestehen bleiben
- Dashboards zur kontinuierlichen Verfolgung der Zero-Trust-Haltung im Zeitverlauf

Anwendungsfall 1: **Validierung und Optimierung von Richtlinien zur Mikrosegmentierung**

Herausforderung

Segmentierungsregeln können aufgrund von Veränderungen an der Umgebung häufig vom beabsichtigten Design abweichen. Ohne kontinuierliche Validierung ist es schwierig zu wissen, ob Richtlinien die laterale Netzwerkbewegung, die Eskalation von Privilegien oder die Verbreitung von Ransomware tatsächlich blockieren.

Lösung

SafeBreach simuliert Angriffstechniken über segmentierte Zonen hinweg und zeigt so jeden möglichen Pfad auf, den ein Angreifer versuchen würde. Akamai Guardicore analysiert, ob diese Pfade blockiert, falsch konfiguriert oder übermäßig zulässig sind. In Kombination bieten die Produkte umsetzbare Erkenntnisse, um Richtlinien zu optimieren und Lücken proaktiv zu schließen.

Anwendungsfall 2: **Laterale Netzwerkbewegungen stoppen und den Auswirkungsradius verringern**

Herausforderung

Selbst bei starken Abwehrmechanismen am Netzwerkperimeter ist die laterale Bewegung nach wie vor eine der häufigsten Methoden zur Eskalation von Verstößen. Angreifer nutzen den East-West-Traffic aus, um hochwertige Assets zu erreichen, ihre Privilegien zu eskalieren und Ransomware bereitzustellen.

Lösung

SafeBreach Propagate identifiziert alle Möglichkeiten zur lateralen Netzwerkbewegung innerhalb der Umgebung – vom Missbrauch von Anmeldedaten bis hin zur Ausnutzung von Diensten. Akamai Guardicore setzt Mikrosegmentierung durch, um diese Bewegungen zu verhindern. So wird der Auswirkungsradius effektiv reduziert und die Verbreitung von Ransomware gestoppt, bevor sie beginnt.

Wenn Sie mehr erfahren oder eine gemeinsame Demo anfordern möchten, besuchen Sie akamai.com/guardicore oder www.safebreach.com

© 2026 Akamai Technologies | Support |
| Veröffentlicht: Februar 2026