

AKAMAI-KUNDENREFERENZ

Eine große europäische Bank wählt Akamai, um mit einem innovativen Segmentierungsansatz die Sicherheits- und Compliance-Kosten zu reduzieren



Umfassende Netzwerktransparenz

10x

schnellere Segmentierung



Automatisierte Richtlinienerstellung

Der Kunde

Eine große europäische Bank

Ein multinationales Unternehmen für Investment und Finanzdienstleistungen, das Kunden in über 50 Ländern in Europa, Nordamerika und Asien Dienstleistungen anbietet, musste seine Compliance-Strategie verbessern. In Anbetracht der Regulierungen für Cybersicherheit von verschiedenen Behörden in Europa, Großbritannien, Singapur und den USA war es das Hauptziel des Unternehmens, seine Workloads zu segmentieren und die Umgebungen des Rechenzentrums zu trennen.

Die Herausforderung

Sicherheits- und Compliance-Anforderungen durch Segmentierung erfüllen

Der stärkere Fokus der regulierenden Behörden auf eine erhöhte Sicherheit der Rechenzentren und das Sicherstellen der Marktstabilität für Finanzdienstleistungen führte zu neuen Regulierungen, die es erforderlich machten, dass die Bank technische Anforderungen durch Segmentierung erfüllte.

Interne Prüfer hatten das Unternehmen außerdem auf die Sicherheitsrisiken flacher Netzwerke aufmerksam gemacht, durch die sich die Auswirkungen von Sicherheitsvorfällen zusätzlich verstärken. Eine vorrangige Sorge war, dass menschliches Versagen oder nicht genehmigte Aktivitäten zu einem Informationsleck oder einem Produktionsfehler führen und die gesamte Umgebung der Bank destabilisieren könnten.

Um diese Herausforderungen anzugehen, begann die Bank mit der Implementierung einer internen Netzwerksegmentierung im Rechenzentrum.

Auswahl der richtigen Lösung

Der Kampf mit der Komplexität herkömmlicher Firewalls

Der erste Segmentierungsversuch erfolgte mit herkömmlichen Tools wie Firewall-Regeln und VLANs. Dieses Projekt nahm viel Zeit in Anspruch und erforderte die Aufmerksamkeit von vielen Verantwortlichen und Teams, was Produktionsausfallzeiten und unklare Richtlinien mit sich brachte. Neben den hohen Implementierungskosten hatte die Bank aufgrund von mangelnder Compliance erhebliche Bußgelder zu zahlen.



Große europäische Bank

Branche

Finanzdienstleistungen

Lösung

[Akamai Guardicore Segmentation](#)

Die wichtigsten Vorteile

- Reduzierung der Compliance-Kosten
- Schutz von IT-Umgebungen
- Sichere Cloud- und Container-Umgebungen
- Automatisierung der Sicherheitsprozesse



Aufgrund der Ineffizienz der herkömmlichen Ansätze suchte das IT-Team der Bank nach einer alternativen und kosteneffektiveren Segmentierungslösung, um die Compliance-Anforderungen zu erfüllen. Zusätzlich zu der lokalen Segmentierung wollte die Bank eine cloud- und containerfertige Lösung.

Als das Bewertungsteam auf Akamai Guardicore Segmentation stieß, war es von der hohen Transparenz und der flexiblen Richtliniengestaltung begeistert. Auch die DevOps-Integration und die Automatisierung waren überzeugend. Diese Fähigkeiten vereinfachten die Erstellung und Durchsetzung von Richtlinien auf eine einheitliche Weise über verschiedene Infrastrukturen hinweg. Das Wichtigste war jedoch das enorme Engagement des Akamai-Teams sowohl während der Machbarkeitsstudie als auch danach. Diese partnerschaftliche Zusammenarbeit mit Akamai bot einen zusätzlichen Mehrwert.

Nach einem tiefgreifenden Bewertungsprozess, der verschiedene Anbieter umfasste, einigten sich die Entscheidungsträger in den Infrastruktur- und IT-Sicherheits-Teams der Bank auf folgenden Konsens: Die Technologie von Akamai ermöglichte die schnellste und unkomplizierteste Mikrosegmentierung. Die Lösung von Akamai entsprach zudem der Zukunftsstrategie der Bank. Die Bank erhielt damit umfassenden Einblick in den East-West-Traffic und konnte Segmentierungsrichtlinien in ihren neuen Multi-Cloud- und Container-Umgebungen durchsetzen.

Akamai Guardicore Segmentation

Vereinfachte und beschleunigte Mikrosegmentierung

Die Bank implementierte Akamai Guardicore Segmentation in verschiedenen Bereichen und Infrastrukturtypen, einschließlich Containertechnologie. Da alle Anwendungen beibehalten werden konnten, gab es keine Ausfallzeiten in der Produktionsumgebung. Die Bank gewann zudem schnell einen zentralisierten, transparenten Überblick über die Workloads des Rechenzentrums und konnte die Produktions-, Test- und Entwicklungsumgebungen isolieren. Mit Akamai Guardicore Segmentation gelang es dem Kunden außerdem, den Zugriff von Druckern, anderen IoT-Geräten und nicht autorisierten Nutzern auf seine Server zu unterbinden.

In weniger als drei Monaten war das Projekt abgeschlossen. Es ging zehnmal so schnell wie ursprünglich mit herkömmlichen Segmentierungsmethoden geschätzt. Durch das schnelle Abbilden der Umgebung und das Erstellen neuer Richtlinien anhand der erfassten Informationen konnte die Bank ihre Sicherheit erhöhen und die Compliance-Anforderungen von mehr als 10.000 bisher nicht konformen Assets erfüllen. Diese zügige Implementierung führte zur Risikoreduzierung sowie zu erheblichen Kosten- und Ressourceneinsparungen.

Das Professional Services-Team von Akamai half der Bank, ihren Segmentierungsprozess vollständig zu transformieren. Die heutigen Richtlinien für das Kennzeichnen und Segmentieren von Assets sind voll automatisiert und in Anwendungsentwicklungs- und Implementierungsrichtlinien eingebettet. Label-Erstellung, Änderungsmanagement, Sicherheitsvorfälle und Serviceanforderungen sind vollständig in die ServiceNow-Workflows integriert. Der Kunde war mit den Ergebnissen der Plattform und deren Mehrwert extrem zufrieden. Auch überzeugte ihn die partnerschaftliche Zusammenarbeit mit Akamai und dessen kompetenten und engagierten technischen Serviceteam.

Weitere Informationen finden Sie unter akamai.com/guardicore.



[Akamai] hat uns bei der Implementierung einer engen Netzwerksegmentierung in lokale und Cloudumgebungen geholfen. Dadurch können wir unsere kritischen Assets und Anwendungen effizient schützen.

Vice President Information Security
einer großen europäischen Bank