Akamai

WHITE PAPER

Hürden der Cybersicherheit mit softwarebasierter Segmentierung überwinden

Akamai Guardicore Segmentation trägt zur Verbesserung der Zugriffssicherheit und zur Senkung der Kosten für Cyberrisiken im europäischen Finanzsektor bei

Übersicht

Der Finanzsektor ist ein wesentlicher Bestandteil der Wirtschaft der Europäischen Union, und einige europäische Regierungen und Regulierungsbehörden betrachten die Finanzsysteme als kritische Infrastruktur. Die von Finanzdienstleistern angebotenen Produkte und Dienstleistungen sind in hohem Maße von hochverfügbaren IT-Systemen und zeitnahem Zugriff auf Informationen abhängig, die über mehrere Kanäle und Parteien bereitgestellt werden.

Ransomware- und Kryptomining-Angriffe haben jedoch gezeigt, wie schnell Cyberkriminelle diese kritische Infrastruktur für Tage oder sogar Wochen lahmlegen und unter Umständen auf verbundene Dritte und Partner ausweiten können.

Es ist von entscheidender Bedeutung, dass die europäischen Finanzinstitute unter der Prämisse Wettbewerbsfähigkeit, Kundengewinnung und Kundenbindung auf innovative digitale Möglichkeiten zurückgreifen können. Doch die zunehmenden gesetzlichen Auflagen für Sicherheitskontrollen und Reporting verlangsamen die Cloud-Einführung erheblich. Die DSGVO (Datenschutz-Grundverordnung) der Europäischen Union beispielsweise kann Geldstrafen von bis zu 4 % des weltweiten Umsatzes gegen Unternehmen verhängen, die ihre Kunden nicht schützen.[1]

Darüber hinaus erfordern jüngste Verordnungen wie SWIFT CSP (Society for Worldwide Interbank Financial Telecommunication Customer Security Programme) und ECB CROE (European Central Bank Cyber Resilience Oversight Expectations) insbesondere eine differenziertere Netzwerksegmentierung.

Herkömmliche Segmentierungskonzepte und die damit verbundenen manuellen Verfahren sind kein praktikabler Ansatz, um mit dem Tempo der technologischen Innovation, den zunehmenden Sicherheitsrisiken und den immer strengeren Vorschriften Schritt zu halten.

Unternehmen müssen nicht nur neue Tools einführen, sondern auch ihre Sicherheits- und Segmentierungsprozesse grundlegend ändern, um Einfachheit, Transparenz und Automatisierung zu erreichen.

In diesem Dokument werden folgende Themen behandelt:

- Die wichtigsten Herausforderungen für die Cybersicherheit, denen sich der europäische Finanzsektor heute gegenübersieht
- Wie Banken und Finanzinstitute diesen Risiken mit einem kosteneffizienten und unkomplizierten Segmentierungsansatz begegnen können
- Wie der Ansatz von Akamai Guardicore Segmentation Unternehmen dabei unterstützt, ihre Sicherheitsprozesse zu vereinfachen, Kosten zu senken und Compliance zu beschleunigen

Die Cybersicherheit von heute ist komplex und kostspielig

Obwohl die europäischen Banken und Finanzinstitute sich verpflichtet haben, die organisatorische Sicherheit zu gewährleisten und die Daten ihrer Kunden zu schützen, ist es angesichts der sich ständig ändernden Risiken, der Zugriffsanforderungen Dritter und der Compliance-Anforderungen nicht einfach, den Weg zu einer stärkeren Sicherheitsstrategie zu beschreiten.

Ein erhöhtes Cyberrisiko erhöht die finanziellen Verluste

Die Risiken im Zusammenhang mit Cyberkriminalität sind für Finanzinstitute besonders schwerwiegend. Die Finanzbranche gibt bereits den zweithöchsten Betrag aller Branchen für die Abwehr von Angriffen aus, mit durchschnittlichen Kosten von 5,72 Millionen US-Dollar pro Datenschutzvorfall.[2]

Aber auch eine Verbesserung der Sicherheitsmaßnahmen zu erreichen, ist teuer. Die Durchsetzung von Sicherheitskontrollen zum Schutz nicht nur mehrerer Plattformen, sondern auch des Zugriffs von Drittanbietern, der für die Bereitstellung von Bankdienstleistungen entscheidend ist, ist eine komplexe Aufgabe. Sie geht einher mit einem erheblichen Anstieg der Infrastruktur- und Arbeitskosten.

Compliance wird teurer

Finanzdienstleister in Europa haben einen dramatischen Anstieg der Kosten, des Zeitaufwands und der Gesamtressourcen erlebt, die für die Vorbereitung und Validierung von Compliance-Initiativen erforderlich sind. Während die Vorschriften dazu beitragen, die Stabilität des Finanzsektors zu gewährleisten, wirkt sich die kontinuierliche Einführung neuer Cybersicherheitsvorschriften jedoch auf Rentabilität und Wachstum aus, da sie die digitale Transformation verlangsamt und erhebliche Investitionen erfordert.

Der erhöhte Druck zur Verschärfung von Richtlinien begann mit der DSGVO, danach folgte die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS), die CROE-Leitlinie der EZB und zuletzt das EU-Cybersicherheitsgesetz. Wenn man die Anbietervorgaben wie SWIFT CSP hinzunimmt, bedeutet die Einhaltung gesetzlicher Vorschriften heute, dass eine Vielzahl von Reporting- und technischen Anforderungen erfüllt werden müssen.

Daher müssen Banken und Finanzinstitute bei der Aktualisierung ihrer Technologie auch Wege finden, die Verwaltung zu vereinfachen und die Betriebskosten in Bezug auf Cybersicherheit und Compliance zu senken.

Sicherheitslücken durch Interaktionen mit Dritten und Finanzmärkten

Die überarbeitete EU-Zahlungsdiensterichtlinie (Payment Services Directive, PSD2), die auf eine Verbesserung der Nutzerfreundlichkeit und Transparenz abzielte, erhöhte die Risiken des Zugriffs Dritter und der Gefährdung personenbezogener Daten. Auch der Druck von Finanzdienstleistungspartnern und Regulierungsbehörden auf Effizienz und Transparenz in Bezug auf Geschäfts- und Technologieprozesse nimmt zu.

Zusätzliche Anforderungen von Kunden in Bezug auf Sicherheit, Mobilität und neue Dienste haben zu einer erhöhten Abhängigkeit der Infrastrukturen für Informations- und Kommunikationstechnologie Dritter, Outsourcing-Anbietern und deren Lieferketten geführt.

Da Umgebungen stärker vernetzt sind als je zuvor, ist der Schutz aller Arten von Kommunikation, wie etwa automatisierter Transaktionen zwischen und innerhalb von Banken, ressourcenintensiv geworden.

Jetzt könnte ein einziger Einbruch in das Rechenzentrum einer Partei einen Dominoeffekt auslösen, da Angreifer nur ein einziges Asset ausnutzen müssten, um sich lateral zwischen miteinander verbundenen Parteien zu bewegen, einschließlich gleichrangiger Finanzinstitute und Finanzmärkte, wodurch die Sicherheit und Geschäftskontinuität des gesamten europäischen Finanzdienstleistungsökosystems gefährdet würde.

Die Hybrid Cloud erfordert einen neuen Sicherheitsansatz

Compliance-Vorschriften und die Leitlinien der Europäischen Bankenaufsichtsbehörde[3] prägen die Trends bei der Cloudeinführung im Finanzsektor. Während die Einführung der Cloud in Europa auf dem Vormarsch ist, ist die Migration von On-Premise-Systemen in die Cloud aufgrund der gesetzlichen Vorgaben noch komplexer geworden.

Aus diesem Grund neigen europäische Unternehmen eher dazu, Kernfunktionen vor Ort zu belassen und hybride Cloudumgebungen statt reiner Cloudumgebungen zu nutzen. Viele Banken haben sich auch für mehrere Cloudservice-Anbieter entschieden, was zu einer Multicloud-Infrastruktur geführt hat.

Unternehmen streben jedoch in der Regel mehr als nur mehr Sicherheit an. Sie möchten auch Kosteneinsparungen und eine Verbesserung der Betriebseffizienz durch veränderte Prozesse durchsetzen. Automatisierung und Prozessmodernisierung werden dabei der Schlüssel zum Erfolg.

Wichtige Herausforderungen im Bereich Cybersicherheit mit Netzwerktransparenz und -segmentierung bewältigen

Ein roter Faden, der sich durch diese Herausforderungen zieht, ist die Notwendigkeit, kritische Anwendungen und Workloads sicher zu isolieren – allgemein als Segmentierung bezeichnet. So können Finanzinstitute skalierbare Sicherheit erreichen, die den Geschäftsanforderungen entspricht, und einen risikobasierten Ansatz verfolgen, der mit den gesetzlichen Anforderungen in Einklang steht.

Veraltete Firewalls sind keine Lösung

Es gibt mehrere Gründe dafür, dass die Segmentierung von europäischen Banken und Finanzinstituten nicht stärker angenommen und umgesetzt wurde.

Wartungs- und Ressourcenintensität: Viele Sicherheits- und IT-Experten zögern, Segmentierungsinitiativen umzusetzen, da sie zu lange dauern und personal- sowie ressourcenintensiv sind. Diese Zögerlichkeit ist verständlich, da traditionelle Methoden häufig sowohl kompliziert als auch zeitaufwändig sind. So ist beispielsweise die standort- und umgebungsübergreifende Konfiguration von VLANs, ACLs und Firewalls sehr häufig ein mühsamer, langsamer und fehleranfälliger Prozess. Darüber hinaus basieren herkömmliche Methoden in hohem Maße auf unzuverlässigen Identitätsdaten wie IPs, die wenig Bedeutung haben und sich häufig ändern können.

Mangelnde Transparenz: Ein weiteres Hindernis für Unternehmen ist der fehlende Einblick in den Ost-West-Traffic, wodurch es schwierig wird, Abhängigkeiten zwischen den Segmenten zu erkennen und Segmentierungsrichtlinien zu erstellen, ohne Schaden anzurichten. Selbst bei Verwendung von Traffic Taps oder ähnlichen Technologien fehlt der daraus resultierenden Ansicht häufig der Kontext und die komplexen Übersetzungen, die zwischen IPs und Ports erforderlich sind. In dynamischen Umgebungen wie Platform-as-a-Service (PaaS) ist dies so gut wie unmöglich.

Infrastrukturabhängigkeit: Wenn Workloads auch in der Cloud abgewickelt werden, was immer häufiger vorkommt, wird der Prozess noch komplizierter. Die Installation einer Hardware-Firewall an jedem Datenausgangspunkt ist kostspielig. Weitere Verwaltungsherausforderungen ergeben sich aus den komplexen Netzwerkkonfigurationen. Diese Konfigurationen sind erforderlich, um die Anforderungen verschiedener Umgebungen mit virtualisierten oder älteren Assets sowie Cloud und Containern zu erfüllen.

> **„In einigen Bereichen hat das Regulierungssystem Mühe, mit technologischen Innovationen Schritt zu halten, aber dies gilt auch für das Risikomanagement und die Kontrollframeworks der Unternehmen."**
>
> **– Financial Markets Regulatory Outlook 2023, Deloitte EMEA Centre for Regulatory Strategy**

Einführung grundlegender Prozessänderungen

Selbst mittelständische Finanzdienstleister mit nur einigen hundert Servern können Tausende von Segmentierungsrichtlinien generieren. Die manuelle Verwaltung ist ineffektiv, insbesondere in Umgebungen mit automatisierter Anwendungsbereitstellung, in denen Tools wie Jenkins und CI/CD-Zyklen verwendet werden, bei denen der Kontext entscheidend ist.

Aus diesem Grund geht Akamai Guardicore Segmentation noch einen Schritt weiter und unterstützt Unternehmen dabei, die Erstellung und Aktualisierung von Richtlinien von einem grundlegend manuellen Prozess in einen automatisierten umzuwandeln.

Mit Akamai Guardicore Segmentation können Regelerstellung und -Updates in einen wiederholbaren Prozess überführt werden, bei dem Stakeholder und Anwendungseigentümer lediglich automatisch generierte Richtlinien genehmigen müssen, sobald die Profilerstellung einer Anwendung automatisiert ist und alle Abhängigkeiten zugeordnet sind. Dadurch entfällt die Notwendigkeit manueller Eingriffe, die Projekte erheblich verlangsamen können, und das Risiko von Fehlkonfigurationen und menschlichem Versagen wird verringert.

Die automatisierte Regelerstellung gewährleistet die strukturelle Konsistenz der Regeln und die Skalierbarkeit der Richtlinie selbst, was eine Optimierung der Firewall zur Folge hat.

Beschleunigen der IT-Transformation zum Aufbau einer echten Zero-Trust-Umgebung

Finanzinstitute sollten sich nicht von manuellen Prozessen und begrenzten Ressourcen davon abhalten lassen, eine skalierbare Segmentierung zu erreichen. Echtes Zero Trust erfordert nicht nur die richtige Technologie, sondern auch die Modernisierung der Prozesse zur Erstellung, Änderung und Wartung von Sicherheitsrichtlinien.

Host- oder softwarebasierte Firewalls haben sich als unkomplizierter und kostengünstiger Ansatz für die Sicherheit auf Anwendungsebene etabliert. Dieser Ansatz beschleunigt die Implementierung erheblich, vereinfacht die fortlaufende Wartung und wehrt letztendlich Bedrohungen effektiver ab. Akamai Guardicore Segmentation wurde von Grund auf so konzipiert, dass die Segmentierung für Unternehmen jeder Größe einfach, kostengünstig und schnell umgesetzt werden kann.

Die Lösung bietet eine visuelle Übersicht aller Anwendungen im Rechenzentrum und ihrer Abhängigkeiten. Sicherheitsbetreiber können dann Sicherheitsrichtlinien auf Netzwerk- und Prozessebene erstellen und durchsetzen, um kritische Anwendungen und Assets zu isolieren und zu segmentieren. Der softwaredefinierte Overlay-Ansatz ist unabhängig von der zugrunde liegenden Infrastruktur und schützt Workloads, die lokale Legacy-Systeme, VMs, Container, Clouds und mehr nutzen. Richtlinien können für einzelne oder logisch gruppierte Anwendungen erstellt werden, unabhängig davon, wo sie sich befinden. Diese Richtlinien bestimmen, welche Komponenten miteinander kommunizieren können und welche nicht, und bilden die Grundlage für einen Zero-Trust-Ansatz in Sachen Sicherheit.

Effiziente Reduzierung von Cyberrisiken und -kosten

Finanzinstitute, die Akamai Guardicore Segmentation einsetzen, haben festgestellt, dass sie in kurzer Zeit, einige ihrer dringendsten Sicherheitsbedenken lösen und gleichzeitig die Kosten senken konnten:

Kosten durch Cyberrisiken senken durch die Durchsetzung von IT-Hygiene und Best Practices im Rahmen der Netzwerksicherheit in immer komplexeren und vernetzten Umgebungen.

Compliance-Management vereinfachen durch detaillierte kontextbezogene Transparenz- und Segmentierungsrichtlinien, sodass Compliance-bezogene Assets und geschäftskritische Anwendungen schnell zugeordnet und isoliert werden können. Durch die Verwendung einer zentralen Managementübersicht kann ein Finanzinstitut angemessen nachweisen, dass es Maßnahmen ergreift, um kritische Assets zu sichern, Betrugsrisiken zu minimieren und die Privatsphäre des Kunden zu schützen.

Zugriffswege von Drittanbietern schützen durch die Durchsetzung von Routen für Drittanbieter-Traffic mit identitätsbasierter Segmentierung werden Nutzer isoliert und an einer weiteren Bewegung durch das Netzwerk gehindert. Die Sicherheit in Bezug auf Interaktionen von Drittanbietern und Finanzmärkten wird dadurch erhöht und verhindert, dass Angreifer über das kompromittierte System eines Dritten „landen und sich ausbreiten".

Geldtransfer- und Zahlungssystemen von der allgemeinen IT isolieren, um die Anforderungen für Systeme des elektronischen Zahlungsverkehrs, insbesondere SWIFT, zu erfüllen, die eine strikte Trennung der SWIFT-Dienste von der allgemeinen IT-Umgebung eines Instituts verlangen. Eine granulare Segmentierung ermöglicht es den IT-Teams von Banken, kontextbezogene Grenzen (Nutzer, Domain) um die „Zone" eines Service-Anbieters festzulegen, um den unberechtigten Zugang weiter einzuschränken.

Sichere und schnelle Migration in die Cloud durch Mapping von Workloads und Inventarisierung aller kritischen Anwendungen und deren Abhängigkeiten vor der Migration. Ringfencing-Richtlinien können diese Zuordnungen als Grundlage für eine konsistente Sicherheit nutzen, die die Workloads während des gesamten Migrationsprozesses begleitet. Dieser Ansatz ermöglicht eine schnellere und sicherere Migration in die Cloud, wobei unabhängig von Anwendungs- oder Infrastrukturänderungen dieselben Sicherheitskontrollen beibehalten werden können.

Effiziente Abwehr von Sicherheitsverstößen zur Gewährleistung der Geschäftskontinuität durch detaillierte Transparenz des Ost-West-Traffics und Indikatoren für Sicherheitsverstöße, um bei ungewöhnlichen Bewegungen zu warnen und die Akteure zu stoppen, bevor sie vertrauliche Finanz- und Kundendaten stehlen.

Risikominderung durch Begrenzung lateraler Bewegungen. Heute verläuft der Großteil des Traffics im Rechenzentrum lateral zwischen Anwendungen (East-West) und nicht von außen (North-South) in das Rechenzentrum. Das Festlegen interner Grenzen durch die Abschirmung geschäftskritischer Anwendungen und Systeme reduziert die Angriffsfläche effektiv, schützt vor der lateralen Ausbreitung von Angriffen und begrenzt den Schaden im Falle eines Einbruchs.

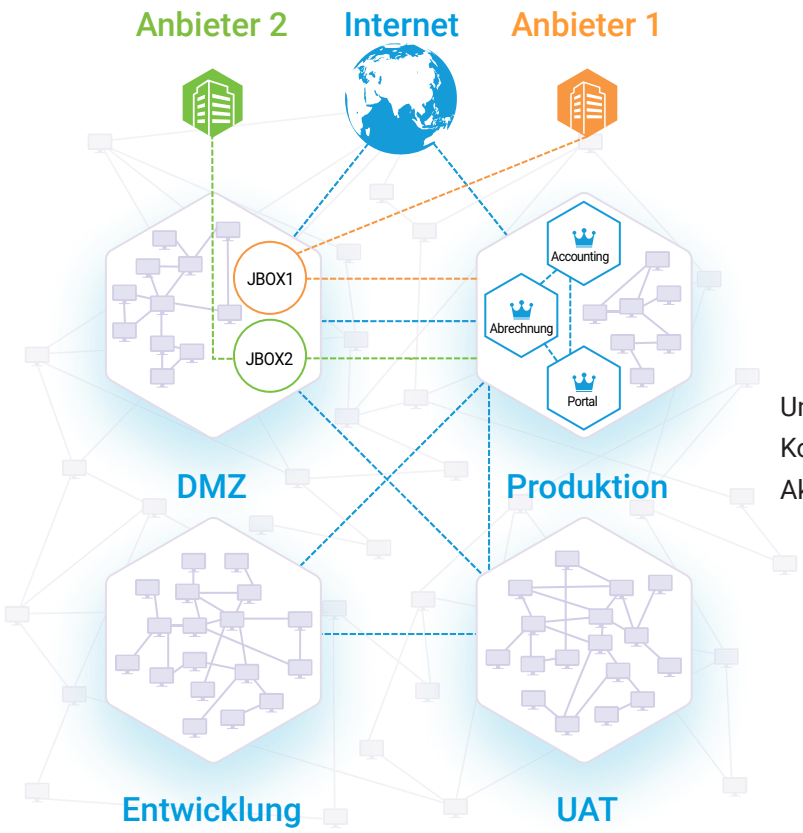
Fallstudie: Reduzierung der Compliance-Kosten bei einer großen europäischen multinationalen Bank

Eine große europäische Bank suchte nach einem neuen, effizienten Ansatz für die Netzwerksegmentierung, um die technischen Anforderungen mehrerer Regulierungsbehörden zu erfüllen, darunter die Federal Reserve Bank of NY (FRBNY), die Monetary Authority of Singapore (MAS) und die EZB.

Der Einsatz traditioneller Segmentierungsansätze, Firewallregeln und VLANs erwies sich als ineffektiv und verursachte hohe jährliche Kosten für die Nichteinhaltung der Vorschriften. Außerdem beeinträchtigte dies den IT-Betrieb durch erhebliche Produktionsausfälle und die für die Erstellung und Aktualisierung von Richtlinien erforderlichen Ressourcen.

Um die Segmentierungsziele der Bank zu erreichen, war ein kosteneffizienterer und einfach umzusetzender Ansatz erforderlich. Die wichtigste Anforderung an eine neue Lösung bestand darin, die Auswirkungen auf die Infrastruktur und die Ressourcen der Bank so gering wie möglich zu halten und gleichzeitig die Einhaltung der relevanten Vorschriften zu gewährleisten.

Nach einem tiefgreifenden Bewertungsprozess, der verschiedene Anbieter umfasste, einigten sich die Entscheidungsträger in den Infrastruktur- und IT-Sicherheits-Teams der Bank auf folgenden Konsens: Akamai Guardicore Segmentation bietet den schnellsten und einfachsten Weg zur Mikrosegmentierung.



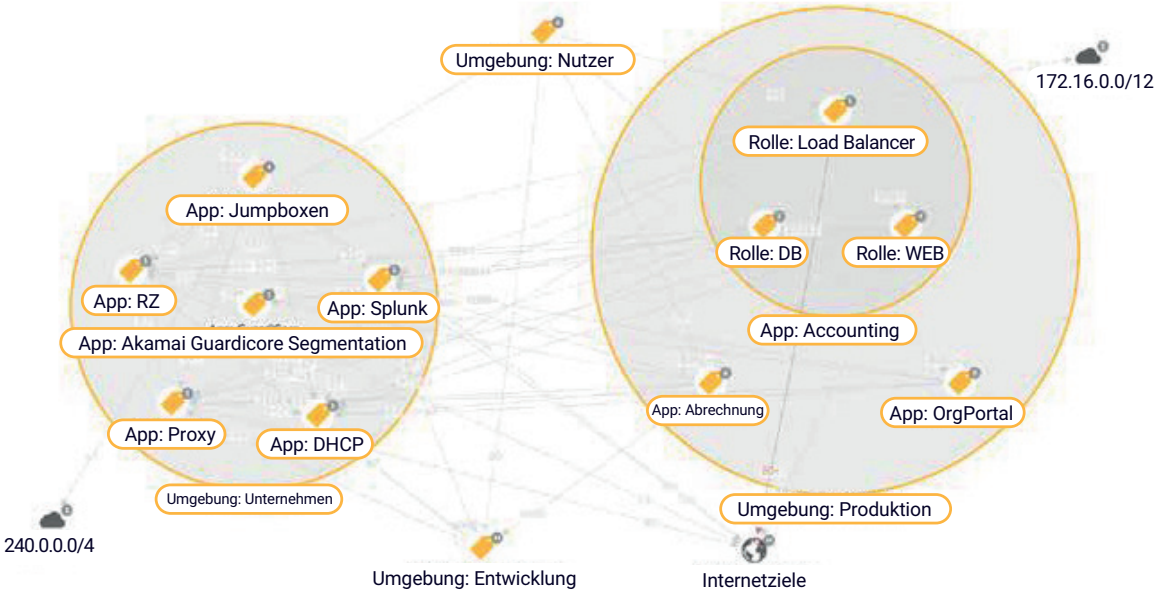
Umgebungssegmentierung und Kontrolle der Zugriffe durch Dritte mit Akamai Guardicore Segmentation

Segmentierung vereinfachen und beschleunigen

Die Bank implementierte Akamai Guardicore Segmentation über verschiedene Regionen und IT-Infrastrukturtypen hinweg, einschließlich Containern. Da keine Anwendungen geändert werden mussten, verursachte dies keine Ausfallzeiten in der Produktionsumgebung. Es ermöglichte der Bank außerdem, schnell eine zentralisierte Transparenz der Workloads des Rechenzentrums zu erreichen und die Produktions-, Test- und Entwicklungsumgebungen zu isolieren. Mit Akamai Guardicore Segmentation konnte der Kunde außerdem den Zugriff auf Server von Druckern, anderen IoT-Geräten und nicht autorisierten Nutzern unterbinden.

In weniger als drei Monaten war das Projekt abgeschlossen. Es ging zehnmal so schnell wie ursprünglich mit herkömmlichen Segmentierungsmethoden geschätzt. Durch das schnelle Ausarbeiten der Umgebung und das Erstellen der Richtlinien basierend auf den gesammelten Informationen verbesserte die Bank ihre Sicherheit und konnte die Compliance-Anforderungen von mehr als 10.000 bisher nicht konformen Assets angehen. Diese zügige Implementierung führte zu Risikoreduzierung sowie zu erheblichen Einsparungen in Bezug auf Kosten und Ressourcen.

Mit dem Team für Professional Services von Akamai konnte die Bank ihren Segmentierungsprozess vollständig 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 sehr zufrieden mit den Ergebnissen der Plattform und dem Mehrwert, den sie bot, sowie mit den kompetenten und engagierten technischen Serviceteams von Akamai.



Weitere Informationen zu Akamai Guardicore Segmentation finden Sie unter akamai.com/guardicore

1 „What are the GDPR Fines?“ DSGVO.eu, 13. Februar 2019.

2 „Cost of a data breach 2022“, IBM.

3 „A Comprehensive Guide to Cloud Adoption in Europe’s Banking sector“, Techerati, 31. Oktober 2019.

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. Möchten Sie mehr über die Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn. Veröffentlicht: 06/23.