

Globale Skalierung liefert Informationen für effektive Sicherheit

Von Skalierung über Transparenz hin zur Informationsgewinnung

Von komplizierten Algorithmen in KI-Tools bis hin zu den geschäftskritischen Daten im CRM-System Ihres Unternehmens gibt es einen unbestreitbaren Zusammenhang zwischen der Menge an genauen Daten, die in diese Systeme fließen, und der Qualität der Ergebnisse. Die Zusammenstellung dieser qualitativ hochwertigen Daten ist für die Cybersicherheit besonders wichtig geworden. Die Plattform von Akamai bietet hierfür eine beispiellose Skalierbarkeit, die für die Bereitstellung effektiver und marktführender Sicherheitslösungen für unsere Kunden entscheidend ist. Die Skalierung von Akamai bietet wertvolle Einblicke in globale Aktivitäten. Damit werden Daten in verwertbare Informationen umgewandelt, die Unternehmen dabei unterstützen, sich vor immer komplexeren Bedrohungen zu schützen.

Globale Reichweite und Verteilung

Die Plattform von Akamai umfasst 2.000 Standorte weltweit und bietet 10- bis 100-mal mehr Abdeckung als andere Anbieter. Dieses umfangreiche Netzwerk gewährleistet die Nähe zu Ihnen und Ihren Kunden und verbessert so die Performance und Verfügbarkeit Ihres Unternehmens. Bei volumetrischen Angriffen wie Distributed Denial of Service (DDoS) wird unsere Skalierung zu einem leistungsstarken Abwehrmechanismus. Da die Plattform den Traffic auf mehrere Standorte verteilen kann, werden Auswirkungen verringert, Lags reduziert und ein unterbrechungsfreier Betrieb ermöglicht. Außerdem reichen die Vorteile der Plattform über die Sicherheitsaspekte hinaus: Sie verbessern das Nutzererlebnis durch Billionen von Routenkombinationen und intelligentes Traffic-Routing.

Beispiellose Dateneinblicke

Kürzlich analysierte Akamai täglich im Durchschnitt 788 TB Daten aus erster Hand. Aufgrund dieser umfangreichen Datensätze sowie unserer fortschrittlichen Heuristik und Modellen für maschinelles Lernen wurde Akamai von mehreren Analysten als führender Anbieter von Analysen von globalen Traffic-Mustern, Ereignisverfolgung und Bedrohungserkennung positioniert. Die Echtzeitinformationen, die sich aus dieser Skalierung ergibt, verbessert unsere Sicherheitsservices und -produkte noch weiter. Unternehmen, die sich dauerhaft vor CVEs und globalen Bedrohungen schützen möchten, können sich auf die 9 PB große Datenbank verlassen, die Akamai kontinuierlich mit maschinellem Lernen aktualisiert und analysiert, um automatische und adaptive Schutzmaßnahmen schnell und präzise bereitzustellen.

Zuverlässiger Schutz gegen DDoS-Angriffe

In Szenarien wie DDoS-Angriffen, deren Ziel eine Überlastung der Ressourcen ist, ist die Größe der Plattform entscheidend für die Aufrechterhaltung des Betriebs. Da die Anzahl der Angriffe im Jahresvergleich um 45 % gestiegen ist, sind die Skalierbarkeit und Verteilung von Akamai von entscheidender Bedeutung. Wird ein Standort angegriffen, kann der Traffic auf andere Orte in der Nähe umgeleitet werden, wodurch die Effektivität des Angriffs beeinträchtigt wird. Die Plattform verzeichnete kürzlich eine maximale Angriffsgröße von 900 GB, was ihre Fähigkeit unter Beweis stellte, auch großangelegten Angriffen standzuhalten und diese abzuwehren. Akamai löst das DDoS-Problem, indem volumetrische Angriffe auf Layer 3, Layer 4, Layer 7 und auf DNS abgewehrt werden.

Akamai Connected Cloud

Die weltweit am stärksten verteilte Plattform für Cloud Computing, Sicherheit und Inhaltsbereitstellung



Über 4.100

Edge Points of Presence



Über 1.200

Netzwerke



Über 130

Länder



Über 750

Städte



SSD-gestützte

Hardware



Plattformbausteine gewährleisten Verfügbarkeit und reduzieren Risiken

DNS-basierter Vorteil

Die DNS-basierte Architektur der Akamai-Plattform mit unserem proprietären DNS-Netzwerk ist ein grundlegender Baustein. Da DNS praktisch das Gateway zum Internet darstellt, priorisiert unser Netzwerk die Performance und bietet ein außergewöhnliches Nutzererlebnis. Die Redundanz unseres DNS-Netzwerks gewährleistet einen unterbrechungsfreien Service, der durch ein SLA von 100 % Verfügbarkeit unterstützt wird.

Optimiertes Traffic-Management

Das Content Delivery Network von Akamai, der Eckpfeiler unserer Plattform, akzeptiert ausschließlich Port 80- und Port 443-Traffic. Damit wird die Angriffsfläche sofort erheblich reduziert. Indem unnötiger Traffic an der Edge reduziert wird, mindern Unternehmen Risiken und eliminieren die Ressourcen, die zur Unterstützung dieses Traffics erforderlich sind. Dadurch steigert sich die Gesamteffizienz.

Unterstützung eines vielfältigen Portfolios an Sicherheitslösungen

Durch die Skalierung der Plattform von Akamai entsteht ein umfangreicher und einheitlicher Datensatz, mit dem auf maschinellem Lernen basierende Empfehlungen für ein umfassendes Portfolio an Sicherheitslösungen bereitgestellt werden können. Durch die Bereitstellung dieser Informationen über eine einzige Schnittstelle können Unternehmen die Sicherheitsabläufe optimieren, Ressourcen freigeben und ihre gesamte Cybersicherheit verbessern.

Fazit

Die Größe unserer Plattform macht Akamai seit über 25 Jahren zu einem vertrauenswürdigen Marktführer. Von beispielloser Skalierbarkeit und Transparenz bis hin zu modernster Informationsgewinnung ermöglichen wir Unternehmen, eine komplexe Bedrohungsumgebung zuverlässig zu bewältigen. Durch den umfassenden Sicherheitsansatz von Akamai können CISOs ihre Unternehmen mit Effizienz, Ausfallsicherheit und Intelligenz schützen, die in der Branche einzigartig sind.

Möchten Sie erfahren, welchen Unterschied die Plattform von Akamai macht?

Die Sicherheitslösungen von Akamai nutzen die einzigartigen Vorteile unserer Plattform, um Ihr Unternehmen und Ihre Kunden zu schützen. Ihre Anforderungen an die Skalierung ändern sich, und das Portfolio von Akamai erfüllt eben diese. Testen, ändern oder wechseln Sie Ihre Lösung. Sie können alles über unser zentrales Plattform-Portal verwalten, das unter einem Vertrag abgewickelt wird und von demselben engagierten Support-Team unterstützt wird.



Mit Akamai wird die Sicherheit leise und effektiv im Hintergrund gewährleistet.

– Operations and Commercial Manager, British Council

Akamai App & API Protector

Schutz vor DDoS-, Bot-, Anwendungsebenen- und API-Angriffen

Akamai Bot Manager

Fortschrittliches Bot-Management, das raffinierte böartige Bots erkennt und beseitigt, aber gute Bots zulässt

Akamai Account Protector

Erkennt und verhindert die Übernahme von Konten, missbräuchliche Erstellung von Konten und Credential Stuffing

Akamai Brand Protector

Erkennt und verhindert Markenimitationsangriffe, einschließlich Phishing und gefälschten Websites

Akamai Client-Side Protection & Compliance

Unterstützt Ihre PCI-Compliance und schützt Ihre Website vor JavaScript-Angriffen

Akamai Edge DNS

Verstärkt Ihre DNS-Infrastruktur mit einem externen autoritativen DNS-Service

Akamai Prolexic

Schützt Ihre Infrastruktur vor DDoS-Angriffen

Akamai API Security

Erkennt, überwacht und bewertet API-Aktivitäten mithilfe von Echtzeitanalysen, um auf Bedrohungen und Missbrauch zu reagieren



Die Bedrohungserkennung ist für jede WAF entscheidend. Akamai ermöglicht effektive Erkennung selbst in einer komplexen Umgebung.

– Principal IT Consultant,
Panasonic Business
Support Europa

Weitere Informationen finden Sie auf unserer [Seite zur Anwendungs- und API-Sicherheit](#).