

Integrierte API-Sicherheit und -Governance für IBM API Connect und DataPower

Das Potenzial und die Herausforderungen von APIs

APIs sind die treibende Kraft für die digitale Transformation und ermöglichen es Unternehmen in allen Branchen, neue Services und Geschäftsmodelle zu entwickeln, um das Wachstum zu beschleunigen. Mit der zunehmenden Verbreitung von APIs nehmen jedoch auch die mit ihnen verbundenen Risiken zu.

- Auch wenn die Nutzung und Integration von APIs von führenden Unternehmen rasant gesteigert wurde, bleibt die effektive Verwaltung von APIs eine Herausforderung.
- Um schnell neue Anwendungen und KI-gestützte Services zu entwickeln und bereitzustellen, enthalten die zugrunde liegenden APIs allzu oft Fehlkonfigurationen, Codierungsfehler und Probleme mit der Geschäftslogik.
- Jedes Mal, wenn ein Kunde, ein Partner oder ein Lieferant digital mit einem Unternehmen in Kontakt tritt, arbeitet eine API hinter den Kulissen, um einen nahtlosen Austausch von (oft sensiblen) Daten zu ermöglichen – und Angreifer wissen das.

Daher haben sich APIs zu einem der größten Angriffsvektoren entwickelt. Und es steht viel auf dem Spiel: Angriffe auf APIs können den Umsatz, die Ausfallsicherheit und die Einhaltung gesetzlicher Vorschriften im Unternehmen gefährden.

Um dieser Herausforderung gerecht zu werden, müssen Unternehmen sowohl bei der Governance als auch bei der Sicherheit einen ganzheitlichen Ansatz verfolgen – einschließlich Design, Entwicklung, Tests, Bereitstellung, Betrieb und Wiederherstellung. Gemeinsam ermöglichen Akamai API Security und IBM es Unternehmen, APIs schnell und zuverlässig zu entwickeln, bereitzustellen und zu verwalten, sodass sie vorhersehbar reagieren und mit dem Unternehmen skalieren können.

Herausforderungen

-  Verwaltung eines API-Bestands über die gesamte Umgebung hinweg und Erkennung unbekannter APIs
-  Identifizierung nicht konformer, falsch konfigurierter oder anfälliger APIs
-  Erkennung und Abwehr von API-Missbrauch, einschließlich Angriffe auf die Geschäftslogik
-  Entwicklung sicherer und konsistenter APIs ohne Abstriche bei Geschwindigkeit oder Agilität
-  Anpassung und Überwachung von API-Sicherheits- und -Governance-Programmen

So unterstützen Akamai und IBM Kunden

Vollständiger Überblick über Ihren API-Bestand

Was Sie nicht sehen können, können Sie nicht schützen. Mit Akamai API Security können Sie APIs, Domains und Probleme automatisch erkennen, um eine robuste API-Bestandsaufnahme zu erstellen, die einen Einblick in Ihre gesamte API-Umgebung bietet. Unternehmen finden in der Regel deutlich mehr APIs, als sie erwartet hätten. Sie können auch leicht ausnutzbare Informationen finden, z. B. Informationslecks, um die Angriffspfade zu verstehen, die Cyberkriminellen zur Verfügung stehen. Außerdem profitieren Sie von der nahtlosen Integration mit den gängigsten Infrastrukturelementen, die mit Ihren API-Gateways und Verwaltungsplattformen in Verbindung stehen, um eine konsistente gemeinsame Nutzung von Sicherheitsdaten im gesamten Unternehmen sicherzustellen.

Stärkere Sicherheit und Governance

Skalieren Sie Ihre Abläufe und setzen Sie Best Practices durch, wenn Sie Akamai API Security für API-Governance verwenden:

- Verstehen Sie jede API in Ihrem Ökosystem mit vollständigem Geschäftskontext und setzen Sie Best Practices für die API-Verwaltung um.
- Optimieren Sie die Kommunikation zwischen Entwicklungs- und Sicherheitsteams.
- Finden Sie Sicherheitsanfälligkeiten von Fehlkonfigurationen bis hin zu nicht richtlinienkonformen APIs.
- Schützen Sie sensible Daten und überwachen Sie Änderungen proaktiv, um Risiken in Ihren APIs zu reduzieren.



API-Missbrauch und Angriffe mit Laufzeitschutz verhindern

Erkennen und blockieren Sie API-Angriffe von der Edge bis zum Kern – einschließlich Datenlecks, Datenmanipulation, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und mehr – mit Echtzeitanalyse des Traffics, Out-of-Band-Überwachung, Inline-Wiederherstellungsoptionen und Workflow-Integrationen, die die Effektivität des Security Operations Center (SOC) erhöhen.

Schnellere Bereitstellung von sicheren APIs mit Active Testing

Integrieren Sie API-Sicherheitstests nahtlos in jede Phase der API-Entwicklung und decken Sie Schwachstellen, Fehlkonfigurationen und Compliance-Probleme auf, bevor APIs in die Produktion gehen. Mit Active Testing können DevSecOps-Mitarbeiter eine umfassende Suite von mehr als 200 API-basierten Sicherheitstests nach Bedarf oder im Rahmen der CI/CD-Prozesse des Unternehmens durchführen. Active Testing findet und testet jede API basierend auf der zugrunde liegenden Geschäftslogik der Anwendung, sodass Entwickler komplexe Schwachstellen aufdecken können, die anderen Testtools entgehen.

Wie Akamai IBM-Nutzern durch eine effizientere Integration mehr Transparenz und Schutz bietet

Akamai API Security lässt sich über mehrere Cloudplattformen und Bereitstellungsoptionen hinweg in API Connect und DataPower integrieren. Wenn API Connect DataPower verwaltet, werden außerdem einseitige Konfigurationsänderungen systemübergreifend vorgenommen, was die betriebliche Effizienz steigert und gleichzeitig das Risiko unbefugter und nicht konformer Entwicklungsaktivitäten verringert.

Nahtlose Angriffserkennung und -reaktion

Darüber hinaus können Kunden von IBM DataPower durch die Integration mit Akamai API Security Bedrohungen nahezu in Echtzeit erkennen und blockieren, ohne dass dadurch die Performance oder Latenz beeinträchtigt werden und ohne dass zusätzliche Plug-ins auf DataPower-Gateways installiert werden müssen.

IBM API Connect kann Zugriffsanfragen für Ressourcen anhand der Autorisierungsrichtlinien von Akamai API Security bewerten und Blockierregeln in IBM DataPower-Clustern durchsetzen, wodurch die Behebungszeit von Tagen auf Minuten oder Sekunden verkürzt wird.

Entwicklungsplattformen



Netzwerk und Cloud



Workflow-Integrationen



Ökosystem



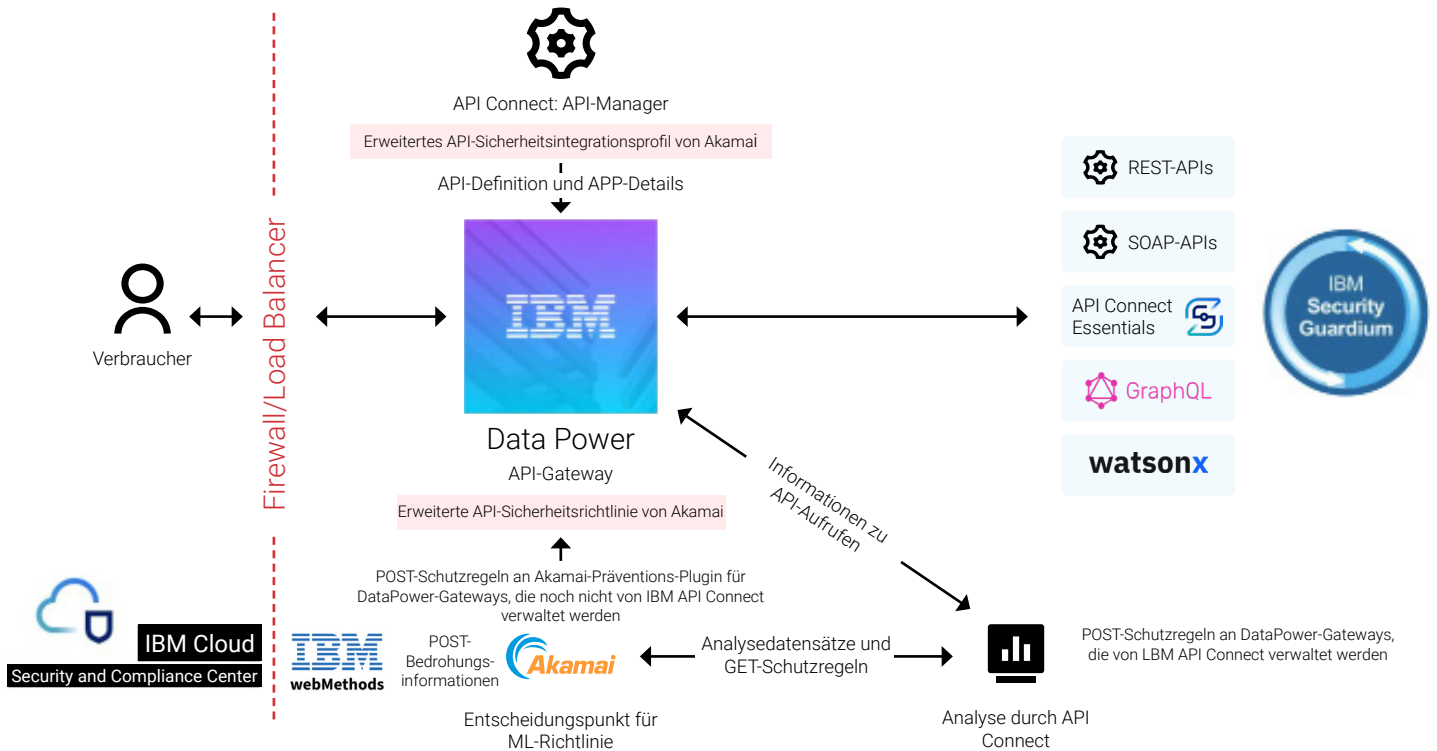
IBM API Connect

API-Gateway



Kombinieren Sie die Leistungsfähigkeit von IBM webMethods und Akamai API Security für beispiellose API-Verwaltung und -Sicherheit. Diese Partnerschaft bietet eine Komplettlösung, die die fortschrittliche API-Erkennung von Akamai mit der robusten Governance und Echtzeit-Datenintegration von IBM webMethods verbindet. So erhalten Sie vollständige Transparenz und Kontrolle über Ihre APIs, um Sicherheit und Compliance zu gewährleisten. Diese Integration stärkt nicht nur die Verteidigung, sondern verbessert auch die Effizienz, sodass Ihr Unternehmen schnell und sicher auf dynamische Marktanforderungen reagieren kann.

Und schließlich können IBM DataPower-Kunden die eBPF Red Hat OpenShift-Integration von Akamai nutzen, um APIs zu erkennen, die noch nicht von API Connect verwaltet oder von DataPower Proxy-Services bereitgestellt werden, sodass sie APIs finden und schützen können, die risikobehaftete Transaktionen und vertrauliche Daten verarbeiten. Diese Funktionen reichen über On-Premise-Abdeckung hinaus bis hin zu Cloud- und Hybridkonfigurationen und unterstützen Amazon Web Services (AWS), Microsoft Azure und die Google Cloud Platform (GCP).



Nächste Schritte

APIs sind eine treibende Kraft für die Fähigkeit von Unternehmen, Kundenbedürfnisse zu erfüllen, Umsätze zu generieren und in einer sich schnell entwickelnden digitalen Wirtschaft wettbewerbsfähig zu bleiben. Das kontinuierliche Wachstum, die Nähe zu Daten und zahlreiche Schwachstellen machen APIs jedoch auch zu einem attraktiven Ziel für Angreifer. Da API-Sicherheitsvorfälle stetig zunehmen, ist es unerlässlich, über Funktionen zum Erkennen, Schützen und Testen jeder API im gesamten Unternehmen zu verfügen. Durch die Partnerschaft von IBM und Akamai können Unternehmen darauf vertrauen, dass APIs sicher und skalierbar entwickelt, verwaltet und verwendet werden.

Erfahren Sie, wie wir Sie unterstützen können, und vereinbaren Sie eine individuelle **Demo zu Akamai API Security**. Sie können sich auch an Ihren IBM-Ansprechpartner wenden, um mehr zu erfahren.