AKAMAI-PRODUKTBESCHREIBUNG

App & API Protector

In der vernetzten Welt von heute ist es für den Geschäftserfolg von entscheidender Bedeutung, Webanwendungen und APIs vor einer Vielzahl von neuen und sich verändernden Bedrohungen zu schützen. Der Schutz von digitalen Interaktionen im Rahmen von Cloud-Transformationen, modernen DevOps-Prozessen und sich stetig verändernden Anwendungen bringt jedoch neue Schwierigkeiten und Herausforderungen mit sich.

Eine umfassende WAAP-Lösung (Web Application and API Protection) stärkt die Sicherheit Ihres Unternehmens durch adaptive Aktualisierung von Schutzfunktionen und proaktive Bereitstellung von Erkenntnissen zu angegriffenen Schwachstellen.

Der **Akamai App & API Protector** ist eine Lösung, die viele Sicherheitstechnologien wie Web Application Firewall (WAF), Bot-Abwehr, API-Sicherheit und DDoS-Schutz (Distributed Denial of Service) vereint. Der App & API Protector ist eine führende WAAP-Lösung zur schnellen Erkennung und Abwehr von Bedrohungen, die die Funktionalität herkömmlicher Firewalls übersteigen, um digitale Ressourcen vor mehrdimensionalen Angriffen zu schützen. Die Plattform ist einfach zu implementieren und zu verwenden, bietet ganzheitliche Transparenz und implementiert automatisch aktuelle, nutzerdefinierte Schutzmaßnahmen über die Akamai Adaptive Security Engine.

Leistungsstarke adaptive Sicherheit

App & API Protector vollzieht mit der Adaptive Security Engine den Schritt über bloße Regelsätze hinaus. Mit dieser innovativen Technologie werden Sicherheitsmaßnahmen kontinuierlich und automatisch aktualisiert. Individuelle Richtlinienempfehlungen werden zudem mit einem einzigen Klick implementiert. Die Adaptive Security Engine bietet modernen Schutz durch die Kombination von maschinellem Lernen, Echtzeit-Sicherheitsinformationen, fortschrittlicher Automatisierung und Erkenntnissen von mehr als 400 Sicherheitsexperten und Bedrohungsforschern. Die Adaptive Security Engine ist aus folgenden Gründen einzigartig:

- Analysiert die Eigenschaften jeder Anfrage in Echtzeit an der Edge für eine schnellere Erkennung
- Lernt Angriffsmuster, indem lokale und globale Daten genutzt werden, um kundenspezifische Sicherheitsanpassungen vorzunehmen
- Passt sich zukünftigen Bedrohungen an und sorgt so für aktuellen Schutz, selbst wenn sich Angriffe weiterentwickeln

Die Adaptive Security Engine reduziert die Last zeitaufwendiger manueller Feinabstimmungen mithilfe von Zero-Touch-Updates für ein nahezu vollständig automatisiertes Erlebnis. Bei der Einführung dieser Technologie wurde nachgewiesen, dass sie die Erkennungshäufigkeit verdoppelt und die Anzahl der False Positives auf ein Fünftel verringert. Durch neue Aktualisierungen unserer Algorithmen auf der Grundlage von maschinellem Lernen ließen sich die False Positives zusätzlich um den Faktor 4 verringern. So haben Sicherheitsexperten wieder mehr Zeit, sichere und kundenfreundliche digitale Geschäftsabläufe bereitzustellen.

Vorteile für Ihr Unternehmen

Zuverlässige Angriffserkennung
Entwickeln Sie sich mit der wachsenden Bedrohungslandschaft und schützen Sie sich vor bekannten und aufkommenden Bedrohungen wie DDoS, Botnets, Injections, Anwendungs- und API-Angriffen und mehr.

Ein Produkt, umfassender Schutz
Maximieren Sie Ihre Investitionen in die Sicherheit mit einer Lösung, die WAAP, Bot-Transparenz und -Abwehr, DDoS-Schutz, SIEM-Connectors (Security Information and Event Management), Weboptimierung, Cloud Computing, API-Beschleunigung und mehr umfasst.

Automatisierter Schutz
Vermeiden Sie zeitaufwändige manuelle Wartungsaufgaben mit automatischen Updates und proaktiven Empfehlungen zur Selbstoptimierung von der Akamai Adaptive Security Engine.

Nutzerfreundlichkeit
Die verbesserte Nutzeroberfläche vereinfacht das Onboarding und umfassende Sicherheitsabläufe, für die außerdem Anleitungen zur Einrichtung und Fehlerbehebung zur Verfügung stehen.

Vereinheitlichte Transparenz
Analysieren Sie über die gemeinsame Telemetrie der Sicherheitslösungen von Akamai Ihre gesamte Bandbreite an Sicherheitskennzahlen mit einem einzigen Dashboard oder proaktiven Erkennungsbericht.

Neu: Verhaltensbasierte DDoS-Engine

Die neue verhaltensbasierte DDoS-Engine stärkt und vereinfacht die DDoS-Abwehr auf Anwendungsebene und basiert auf maschinellem Lernen. Die verhaltens- und anomaliebasierten Erkennungsalgorithmen der verhaltensbasierten DDoS-Engine untersuchen verschiedene Trafficdimensionen wie Ursprungland, Netzwerkfingerabdruck und andere HTTPS-Abfrageattribute, um einen individuellen Schutz zu schaffen und einen praktischen Ansatz gegen DDoS-Angriffe auf Anwendungsebene zu bieten.

Die Nutzung von maschinellem Lernen durch die verhaltensbasierte DDoS-Engine verbessert die Wirksamkeit und Entscheidungsfindung in Bezug auf Trafficdimensionen für die Erstellung von Trafficprofilen oder -baselines. Der Bewertungsmechanismus für verschiedene Empfindlichkeitsstufen berücksichtigt die Risikobereitschaft Ihres Unternehmens bei der Erkennung von Angriffen und der Minimierung von False Positives.

Akamai App & API Protector wird von der Adaptive Security Engine unterstützt und geht über Regelsätze hinaus.

Führende Angriffserkennung – Wenn Ihre digitale Umgebung wächst, erhöht sich auch der Umfang Ihres Schutzes als Kunde von Akamai. Zusätzlich zu den automatischen Updates und der adaptiven Selbstoptimierung, die die Adaptive Security Engine bietet, liefert der App & API Protector auch von Analysten als führend anerkannte Erkennungsfunktionen für DDoS, Bot-Angriffe, Malware und andere Angriffsvektoren. Bestärken Sie Ihren Akamai-Schutz vor neuen und fortschrittlichen CVEs mit unserem Tool zur Bedrohungsanalyse.

Anwendungssicherheit – App & API Protector bietet eine umfassende Suite von Abwehrmaßnahmen und Anpassungen, damit die Sicherheit an die Anforderungen Ihres Unternehmens angepasst werden kann. Effektive Funktionen wie Client Reputation, Netzwerklisten, neuartige Angriffserkennung und vieles mehr bieten Ihnen den Vorteil, dass Sie Angreifer abwehren können, während gleichzeitig die Sicherheitsabläufe vereinfacht werden. Die erweiterten Schutzmechanismen der WAAP-Lösung von Akamai wehren DDoS, SQL-Injections, Cross-Site Scripting, Local File Inclusion, Server-Side Request Forgery (serverseitige Fälschung von Anfragen) und andere Angriffsvektoren auf Anwendungsebene ab.

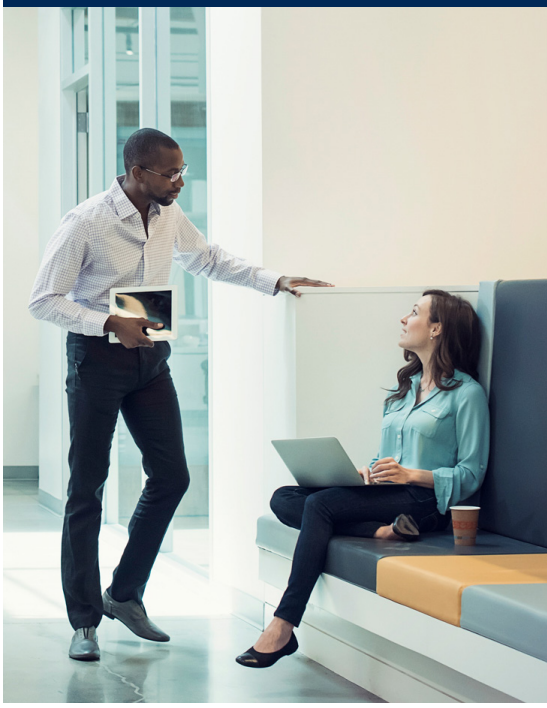
DDoS-Schutz und granulare Ratensteuerung – Als marktführende DDoS-Lösung bietet der App & API Protector Schutz vor DDoS-Angriffen auf mehreren Ebenen. Das beginnt damit, dass DDoS-Angriffe auf Netzwerkebene sofort an der Edge abgewehrt werden, um Risiken zu mindern und Ressourcen einzusparen. Darüber hinaus erkennt sie ausgeklügelte Layer-7-DDoS-Angriffe und wehrt diese an der Edge selbsttätig ab. Dadurch haben Sie automatisierten Schutz in Echtzeit vor der sich ständig weiterentwickelnden DDoS-Bedrohungen. Die detaillierte Ratensteuerung passt Ihre DDoS-Abwehr speziell an Ihren Traffic- und Ihre Angriffsprofile an.

Bot-Transparenz und -Abwehr – Über das Akamai-Verzeichnis mit mehr als 1.750 bekannten Bots erhalten Sie Echtzeiteinblicke in Ihren Bot-Traffic. Sie können verfälschte Web-Analysen untersuchen, eine Überlastung des Ursprungs verhindern und eigene Bot-Definitionen erstellen, um den reibungslosen Zugriff auf Bots von Drittanbietern und Partnern zu ermöglichen. Im App & API Protector sind jetzt erweiterte Bot-Kontrollmechanismen enthalten, darunter Erkennung von Browser-Imitation, bedingte Aktionen und Krypto-Challenges.

OWASP Top10

Akamai wehrt sowohl die OWASP Top 10- als auch die OWASP API Top 10-Schwachstellen ab. Erfahren Sie mehr darüber, wie App & API Protector und Sicherheitslösungen von Akamai Kunden vor großen, bekannten oder aufkommenden Bedrohungen schützen.

Laden Sie das Whitepaper herunter, um mehr darüber zu erfahren, wie Akamai Sie vor den OWASP Top 10-Schwachstellen schützt.



API-Sicherheit – Die branchenführende API-Sicherheit von Akamai verbessert Ihren Schutz durch transparente Einblicke in den Traffic aller digitalen Ressourcen, proaktives Aufdecken von Schwachstellen, Erkennen von Umgebungsänderungen und Schutz vor versteckten Angriffen. Mit den API-Funktionen von App & API Protector können Sie:

- automatisch eine ganze Reihe neuer, unbekannter und sich verändernder APIs in Ihrem gesamten Webtraffic aufdecken, einschließlich ihrer Endpoints, Definitionen und Traffic-Profile
- neu erkannte APIs schnell und einfach registrieren
- APIs vor DDoS-Angriffen, Injection von Schadcode, Missbrauch von Anmeldedaten und Verstößen gegen API-Spezifikationen schützen
- den Umgang mit sensiblen Daten mit der Berichtsfunktion für persönlich identifizierbare Informationen von App & API Protector kontrollieren, um Compliance zu gewährleisten

Performance und mehr aus dem größten globalen Netzwerk – De Akamai-Plattform bietet Kunden dank ihrer unübertroffenen globalen Skalierbarkeit einen Wettbewerbsvorteil und bietet Echtzeiteinblick in einen beträchtlichen Anteil des globalen Internettraffics. Dank dieser umfangreichen Daten kann Akamai verwertbare Bedrohungsinformationen bereitstellen. Damit sind Unternehmen den sich entwickelnden Sicherheitsbedrohungen immer einen Schritt voraus und können Angriffe in verschiedenen Umgebungen schneller erkennen und abwehren. Die Plattform bietet außerdem eine bewährte Performancesteigerung und ein SLA für 100 % Verfügbarkeit.

Malware Protector – Dieses Add-on-Modul scannt Dateien an der Edge, bevor sie hochgeladen werden. So wird Malware erkannt und verhindert, dass sie als schädlicher Datei-Upload in Unternehmenssysteme gelangt. Es ist keine zusätzliche Anwendungs- oder API-Konfiguration erforderlich, daher sparen Sie sich die Zeit, die Sie für die individuelle Einrichtung des Schutzes in jedem einzelnen System aufwenden müssten.

Einfaches Onboarding – Großartige Sicherheitstools funktionieren nur, wenn sie auch verwendet werden. Akamai hat sich dem Aufbau einer nutzerfreundlichen Plattform verschrieben, die Produktivität und starken Schutz ermöglicht. Mit Simple Start können Sie die Lösung schnell bereitstellen oder Schutzfunktionen mit nur wenigen Klicks auf neue Anwendungen erweitern.

Dashboards, Warnungs- und Reporting-Tools – Web Security Analytics ist das Dashboard für detaillierte Angriffstelemetrie von Akamai. Hier können Sie Sicherheitsereignisse analysieren, E-Mail-Warnungen in Echtzeit mit statischen Filtern und Schwellenwerten erstellen und individualisierbare Reporting-Tools nutzen, um kontinuierlich die Effektivität Ihrer Schutzmaßnahmen auf der gesamten Akamai-Plattform zu überwachen und zu bewerten.

DevOps-Integrationen – Integrieren Sie mit GitOps die Sicherheit nahtlos in DevOps-Workflows, um zu gewährleisten, dass die Sicherheit im schnellen Entwicklungsprozess nicht ins Hintertreffen gerät. Die APIs von Akamai, die über CLI oder Terraform verfügbar sind, ermöglichen die vollständige Verwaltung von App & API Protector über Code und passen jede Aktion an, die in der Nutzeroberfläche verfügbar ist.

SIEM-Integrationen – Darüber hinaus sind auch SIEM-APIs verfügbar, und vorgefertigte Konnektoren für Splunk, QRadar, ArcSight und mehr sind automatisch im App & API Protector enthalten.

Integrierte Funktionen – Um Transparenz und Performance zu verbessern, enthält der App & API Protector jetzt bereits viele der beliebtesten Produkte von Akamai-Kunden, darunter:

- Site Shield: Hindern Sie Angreifer daran, cloudbasierte Schutzmaßnahmen zu umgehen und gegen Ihre Ursprungsinfrastruktur gerichtete Angriffe auszuführen.
- mPulse Lite: Erhalten Sie detaillierte Einblicke in das Nutzerverhalten, beheben Sie Performanceprobleme in Echtzeit und messen Sie die Auswirkungen digitaler Veränderungen auf den Umsatz.
- EdgeWorkers: Entdecken Sie die Vorteile von serverlosem Computing, darunter verbesserte Markteinführungszeiten und Logikausführung in der Nähe Ihrer Endnutzer.
- Image & Video Manager: Optimieren Sie intelligent Bilder und Videos durch die ideale Kombination von Qualität, Format und Größe.
- API Acceleration: Erhöhen Sie Ihre API-Performance mit einfacher Zugriffsverwaltung, Skalierung für Trafficspitzen bei hoher Nachfrage und verbesserter API-Sicherheit.

Für kostenlose Angebote gelten möglicherweise Nutzungsbeschränkungen. Wenden Sie sich an Akamai, wenn Sie mehr darüber erfahren möchten.

Erweitertes Sicherheitsmanagement

Das optionale Advanced Security Management-Modul bietet flexible Automatisierungen und Konfigurationen für Kunden mit komplexeren Anwendungsumgebungen und besonderen Sicherheitsanforderungen. Die Advanced Security Management-Option umfasst sofort einsatzbereite zusätzliche Sicherheitskonfigurationen, Raten- und Sicherheitsrichtlinien, DDoS-Kontrollen auf Anwendungsebene, nutzerdefinierte WAF-Regeln und positive API-Sicherheit sowie Zugriff auf Bedrohungsinformationen auf Basis von IP-Reputation (Client Reputation).

Managed Security Service

Der Standard Support steht allen Kunden von Akamai rund um die Uhr zur Verfügung. Zusätzlich zu den On-Demand-Professional-Services für Beratung oder Einzelprojekte bietet Akamai Managed Services auf verschiedenen Stufen an: vollständig verwalteter WAAP-Service, verwaltete Angriffsabwehr und spezialisierter Support im Security Operations Center.

Mehr Informationen zu App & API Protector und eine kostenlose Testversion finden Sie unter akamai.com/aap.