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 App & API Protector von Akamai 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 einfacher zu implementieren und zu verwenden, bietet ganzheitliche Transparenz und implementiert automatisch aktuelle, nutzerdefinierte Schutzmaßnahmen über die Akamai Adaptive Security Engine.

Leistungsstarke adaptive Sicherheit

Mit dem App & API Protector werden Sicherheitsmaßnahmen kontinuierlich und automatisch aktualisiert. Individuelle Richtlinienempfehlungen werden zudem mit einem einzigen Klick implementiert. Die Adaptive Security Engine, die Technologie im Kern des App & API Protector, bietet modernen Schutz durch eine Kombination aus maschinellem Lernen, Echtzeit-Sicherheitsinformationen, fortschrittlicher Automatisierung und den Erkenntnissen von mehr als 400 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 zeitaufwändiger manueller Feinabstimmungen mithilfe von Zero-Touch-Updates für ein nahezu vollständig automatisiertes Erlebnis. Dies verdoppelt die Erkennungshäufigkeit und reduziert False Positives auf ein Fünftel. 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-Kontrollen, 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.

Akamai

Kontinuierliche Innovation für die Anwendungssicherheit

Akamai arbeitet kontinuierlich an Innovationen und bietet neue Funktionen und erweiterte Schutzfunktionen, die Kunden begeistern. Zu den verbesserten DDoS-Abwehrfunktionen auf Anwendungsebene gehören konfigurierbare Fenster zur Ratenberechnung zum Schutz vor kurzen, intensiven DDoS-Angriffen sowie erweiterte Übereinstimmungsbedingungen bei der Ratenbeschränkung (wie z. B. Client-Reputationsbewertungen und TLS-Fingerabdrücke). Im Gegensatz zu den heute gängigen Methoden zur Ratenbeschränkung kann unser innovativer neuer Ansatz – URL-Schutz mit intelligentem Load Shedding – DDoS-Angriffe auf Anwendungsebene mit ursprungsbasierter Ratendrosselung erkennen und abwehren. Die Adaptive Security Engine wurde verbessert, um eine schnelle Bereitstellung von Schutz vor neuen Bedrohungen und hochkarätigen CVEs zu ermöglichen. Zur Verbesserung der Bot-Kontrollen ist in Bot Visibility & Mitigation jetzt eine neue und innovative Bot-Erkennungsmethode zur Erkennung von Browser-Imitation enthalten, die ein dynamisches Bewertungsmodell und maschinelles Lernen verwendet.

Nicht nur Anwendungssicherheit, sondern auch API-Schutz

Die branchenführende API-Sicherheit von Akamai bietet transparente Einblicke in den Traffic aller digitalen Ressourcen, proaktives Aufdecken von Schwachstellen, Erkennen von Umgebungsänderungen und Schutz vor versteckten Angriffen.

Die Funktion für API-Erkennung warnt Sicherheitsteams vor neuen, häufig ungeschützten APIs, die mit verschiedenen Geschäftsbereichen verknüpft sind. Akamai App & API Protector erkennt automatisch alle 24 Stunden APIs basierend auf einem Bewertungsmechanismus, der den Content-Typ der Antwort, die Pfadeigenschaften und Traffic-Muster berücksichtigt. Mit API-Erkennung 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 (PII) von App & API Protector kontrollieren, um Compliance zu gewährleisten

Und das Beste ist: Um ab der Installation von App & API Protector eine starke API-Sicherheit zu gewährleisten, werden alle API-Anfragen automatisch auf schädlichen Code überprüft – unabhängig davon, ob Sie sie registrieren oder nicht. Der Akamai App & API Protector vereinfacht die Komplexität von Sicherheitsabläufen für alle Ressourcen und versetzt Sicherheitsteams in die Lage, die Abstimmung mit Entwicklungsteams, Geschäftsbereichsleitern und Führungskräften zu verbessern.

Die Funktionen zur Verhinderung von API-Datenverlust von App & API Protector bieten einen besseren Schutz von personenbezogenen Daten und anderen sensiblen Daten. Sie erkennen, wo personenbezogene Daten durch APIs offengelegt oder verwendet werden können, und gewährleisten leistungsstarke Transparenz und Kontrolle über sensible Daten, um die Sicherheit Ihres Unternehmens und Ihrer Kunden zu gewährleisten.

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.

DDoS-Schutz: Der App & API Protector ist als marktführende DDoS-Lösung bekannt, wehrt DDoS-Angriffe auf Netzwerkebene direkt an der Edge ab und bietet ganzheitliche Verteidigungsstrategien gegen DDoS-Angriffe auf Anwendungsebene. Sie sind nicht nur vor DDoS-Angriffen geschützt, sondern auch vor den Trafficspitzen eines Angriffs – der DDoS-Gebührenschutz von Akamai gleicht durch einen DDoS-Angriff entstandene Kosten aus.

Top 10 der OWASP-Sicherheitsrisiken

Akamai wehrt die OWASP Top 10- sowie 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.

Transparenz bei der Bot-Abwehr: Über das umfangreiche 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. Die Erkennung von Browser-Imitation, die auf maschinellem Lernen basiert, ist jetzt im App & API Protector enthalten.

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

Site Shield: Dieses beliebte Produkt ist jetzt im App & API Protector enthalten und hindert Angreifer daran, cloudbasierte Schutzmaßnahmen zu umgehen und gegen Ihre Ursprungsinfrastruktur gerichtete Angriffe auszuführen. Weitere Produkte aus dem Sicherheitsportfolio von Akamai wie Client-Side Protection & Compliance und der Account Protector können Ihre Browser-Sicherheitsfunktionen noch erweitern.

Nutzerfreundliches, umfassendes Sicherheitstool: 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 Reporting-Tools für die Websicherheit nutzen, um kontinuierlich die Effektivität Ihrer Schutzmaßnahmen zu überwachen und zu bewerten.

DevOps-Integrationen: Beschleunigen Sie das Onboarding, verwalten Sie Ihre Sicherheitsrichtlinien durchgängig, setzen Sie sie zentral über Cloudinfrastrukturen hinweg um und verbessern Sie die Zusammenarbeit zwischen DevOps- und Sicherheitsteams in einem GitOps-Workflow. So stellen Sie sicher, dass Ihre Sicherheit immer mit dem aktuellen Tempo der Entwicklungen Schritt hält. Da die Akamai-APIs auch in Form eines Wrappers mit einem Akamai-CLI-Paket oder Terraform verfügbar sind, können Sie den App & API Protector über Code verwalten. Auf jede in der Nutzeroberfläche verfügbare Aktion kann über programmierbare APIs zugegriffen werden. Sicherheitsteams können auch Warnungen bei der Freigabe von WAF-Regeln oder der Aktivierung von Konfigurationen in IT-Service-Management-Tools wie Slack integrieren.

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 Produkte, die bei Akamai-Kunden am beliebtesten sind, wie:

- **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 logische Ausführung 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.

Doppelte Erkennungshäufigkeit und Reduzierung von False Positives auf ein Fünftel

Erweitertes Sicherheitsmanagement

Das optionale Advanced Security Management-Modul bietet flexible Automatisierungen und Konfigurationen für Kunden mit komplexeren Anwendungsumgebungen und besonderen Sicherheitsanforderungen. Wir empfehlen die Verwendung automatischer Updates. Diese Option bietet jedoch auch einen manuellen Betriebsmodus für granulare Aktionen und die Möglichkeit, einzelne Updates bei Bedarf zu aktivieren. Sie können mit dem Auswertungsmodus auch neue Updates zusammen mit aktuellen Schutzfunktionen testen, um Verbesserungen vor der Implementierung genau zu verstehen. Außerdem umfasst die Advanced Security Management-Option 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 zwei Stufen an: vollständig verwalteter WAAP-Service und verwaltete Angriffsabwehr.

Weitere Informationen erhalten Sie auf der App & API Protector-Website oder kontaktieren Sie das Vertriebsteam von Akamai.