Cloudflare API Shield

Verwalten und sichern Sie die APIs, die Ihr Geschäft beflügeln

Moderne API-Herausforderungen

Im Fadenkreuz der Angreifer

APIs regieren die (digitale) Welt. 58 % des dynamischen HTTP-Traffics im Cloudflare-Netzwerk sind API-bezogen.

APIs bieten spannende Geschäftsmöglichkeiten, um Produkte schneller bereitzustellen und das Kundenerlebnis zu verbessern. Sicherheitsverantwortliche müssen einen Mittelweg finden, um ihre APIs zusätzlich zu ihren Web-Apps zu sichern, ohne die Innovation zu bremsen.

Sicherheits- und IT-Teams müssen die sensiblen Daten ihrer Kunden schützen und gleichzeitig Geschäftsabläufe über Web-Apps und API-Objekte hinweg ermöglichen.

Schließlich steht das Vertrauen der Kunden auf dem Spiel.

Cloudflare API Shield

Kunden können ihre öffentliche API-Sicherheit und -Verwaltung entdecken, absichern und vereinfachen, indem sie den Schutz für Webanwendungen und APIs am Cloudflare-Edge konsolidieren.

API Shield gehört zu den Lösungen für Anwendungssicherheit von Cloudflare, mit denen außerdem Bots gestoppt, DDoS-Attacken vereitelt, Anwendungsangriffe verhindert und nach Supply Chain-Attacken Ausschau gehalten wird.

Gefahren unentdeckter APIs

Entwicklungsteams veröffentlichen neue APIs häufig, ohne anderen Kollegen in der IT Bescheid zu geben. So kann es passieren, dass das Unternehmen bezüglich solcher APIs im Dunkeln tappt und diese daher weder verwaltet noch geschützt werden.

Angst vor Authentifizierungsfehlern, Datenlecks und Missbrauch

Wenn APIs einmal erkannt wurden, müssen sie durch Authentifizierung, Schemavalidierung, Erkennen von Datenausschleusung und weiteren Tools vor Angriffen und Missbrauch geschützt werden.

Überwachung der API-Performance

Angesichts der großen geschäftlichen Bedeutung von APIs müssen Unternehmen, wenn sie die Überwachung und den Schutz dieser Schnittstellen sichergestellt haben, ihre Performance im Auge behalten. Dies geschieht anhand von Parametern wie Anfragenmenge je Endpunkt, Fehlerquoten und Latenz.

Cloudflare API Shield

Verwalten und sichern Sie die APIs, die Ihr Geschäft beflügeln

Wichtigste Funktionen	
Aufspüren und Verwalten von APIs	
Aufspürung und Schema-Learning	Entdecken Sie API-Endpunkte im aktiven Einsatz und die zugehörigen Schemata durch auf Machine Learning und Heuristiken basierende Modelle.
Sequenz- und Performance-Analytics	Die wichtigsten Abläufe im Verhalten von API-Aufrufen ermitteln und die Performance von API-Endpunkten analysieren (z. B Anfragen, Latenzzeit, Fehlerrate, Antwortgröße usw.).
Entwicklerportal und -verwaltung	Verwalten Sie interaktive API-Dokumentation und hosten Sie sie auf Ihrer Domain mit Cloudflare Pages.
API-Sicherheitsniveau	
Erkennung von BOLA-Angriffen	
Authentifizierungsstatus	Risiko-Scans, die Fehlkonfigurationen bei der Authentifizierung in APIs erkennen und warnen, z. B. keine Authentifizierung oder gemischte Authentifizierung (wobei nur für einige API-Aufrufe an einen Endpunkt Zugriffsrechte erforderlich sind)
Schutz sensibler Daten	Erkennen Sie sensible Daten in API-Antworten, die Ihren Ursprung verlassen, und warnen Sie pro Endpunkt.
API-Laufzeitschutz	
Überprüfung der Authentifizierung	Authentifizieren und validieren Sie den API-Traffic mit mTLS-Zertifikaten, JSON Web Tokens (JWT), API-Schlüsseln und OAuth 2.0 Tokens, um Anfragen von illegitimen Clients zu blockieren.
Schemavalidierung	Verwenden Sie API-Schemata, um gültige API-Anfragen zu akzeptieren und fehlerhafte Anfragen und HTTP-Anomalien zu blockieren. Dies ergänzt das negative Sicherheitsmodell von Cloudflare WAF für umfassende Sicherheit.
Schutz vor REST- und GraphQL-Missbrauch	Stoppen Sie volumetrischen und sequenziellen Missbrauch mit Vorschlägen zur Durchsatzbegrenzung pro Endpunkt. Erweitern Sie den Schutz vor Denial of Service (DoS)-Angriffen auf GraphQL-Endpunkte.

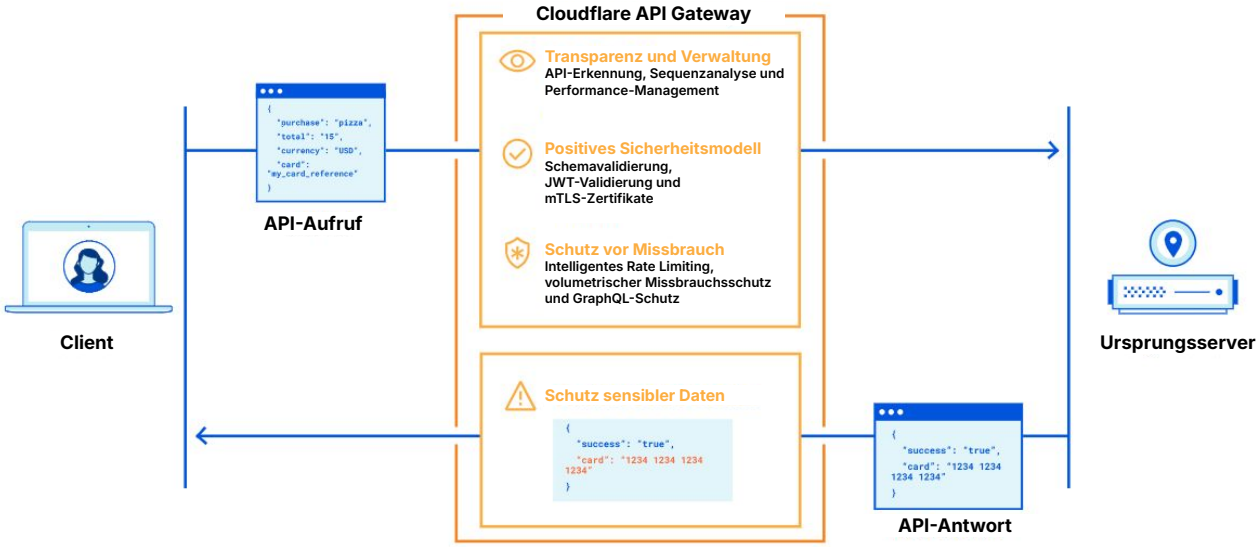

Abbildung 1: Architektur von Cloudflare API Shield

Cloudflare in der Pole Position

Das Cloudflare-Portfolio für Anwendungssicherheit hat für seine Stärke und Bandbreite zahlreiche Auszeichnungen erhalten. Cloudflare wurde in der jüngsten „Forrester Wave: Web Application Firewalls“ als ein Leader ausgezeichnet. Gartner wurde 2023 im Gartner® Peer Insights™-Bericht „Voice of the Customer“ für DDoS-Abwehrlösungen zum „Customer's Choice Leader“ für DDoS-Abwehrlösungen gekürt. Forrester hat Cloudflare in „The Forrester Wave™: Bot Management Software“ aus dem dritten Quartal 2024 als einen „Strong Performer“ eingestuft. IDC bezeichnete Cloudflare als einen „Major Player“ im „IDC MarketScape 2024“ für Unternehmensplattformen mit Webanwendungs- und API-Schutz (Web Application and API Protection – WAAP).