KURZDARSTELLUNG

Die WAF von Cloudflare

Eine WAF für moderne Anwendungssicherheit

Herausforderungen bei der Anwendungssicherheit

Anwendungen sind für Unternehmen so wichtig wie eh und je. Sie werden deshalb von Angreifern unerbittlich ins Visier genommen, was eine größere Angriffsfläche bedeutet.

Die Anliegen sind unterschiedlich. Manche Firmen wollen sich vor neuen Zero-Day-Exploits schützen. Andere möchten Datenlecks oder Versuche, Abwehrmaßnahmen zu umgehen, erkennen können. Einigen geht es darum, Credential Stuffing zur Kontenübernahme zu verhindern oder Uploads in Anwendungen auf Malware zu überprüfen.

Gleichzeitig soll der Anwendungsschutz Teil eines umfassenderen, einheitlichen Sicherheitskonzepts sein, das auch API abdeckt, Bots stoppt und clientseitige Risiken reduziert. Für die Mitarbeitenden in der IT-Sicherheit darf dadurch aber kein übermäßiger zusätzlicher Aufwand entstehen.

Die WAF von Cloudflare

Die Web Application Firewall (WAF) von Cloudflare bildet den Grundpfeiler unseres erweiterten Sortiments an Sicherheitslösungen, das den Schutz und die Leistungsfähigkeit von Anwendungen gewährleistet. Nur die Cloudflare-WAF ermöglicht im Bereich Sicherheit einen vollständigen Überblick, bietet mehrstufigen Schutz vor OWASP-Angriffen und neuen Exploits, erkennt Ausweichmanöver und neue Angriffe mithilfe von maschinellem Lernen, blockiert die Kontenübernahme, registriert Datenlecks und mehr. So lassen sich Anwendungen an dem Ort schützen, an dem sie gehostet werden. Unsere hochwirksamen Funktionen für Anwendungssicherheit, z. B. API-Schutz und Bot-Abwehr, sind vollständig in unsere WAF integriert und greifen auf dieselbe leistungsstarke Rule-Engine zurück. Bereitgestellt wird dies alles über eine der weltweit ersten Connectivity Clouds.

Erkennung von Angriffen und einfache Einbindung

Wir bieten differenzierte Sicherheitsanalysen zur Visualisierung des gesamten Traffics – ob dieser Abwehrmaßnahmen unterzogen wurde oder nicht. Ein sofortiger Überblick über die Bedrohungslandschaft bringt messbaren Nutzen, weil sich damit der Angriffstraffic und die unmittelbar nach der Einbindung zu ergreifenden Schutzmaßnahmen ermitteln lassen.

Schneller Schutz vor neuen Angriffen

Angesichts zehntausender Sicherheitslücken pro Jahr fügt unsere WAF schnell neue verwaltete Regeln hinzu, um die Ausnutzung neu entdeckter (Zero-Day-)Sicherheitslücken zu verhindern. Unsere verwalteten Regeln blockieren Exploits und werden durch WAF-Angriffsscores ergänzt, die mithilfe von maschinellem Lernen ermittelt wurden, um Ausweichmanöver zu erkennen.

Bedrohungsdaten aus einem riesigen globalen Netzwerk

Je hochwertiger die zugrundeliegenden Daten, desto besser funktioniert ein Sicherheitsmodell. Unser riesiges globales Netzwerk fungiert als Proxy für 20 % des Internets, was uns einen einzigartigen Einblick in die Bedrohungslandschaft ermöglicht. Die dadurch gewonnenen Daten fließen in Machine Learning-Modelle ein, die wir ergänzend zu herkömmlichen signaturbasierten Methoden für eine hochpräzise Erkennung und Abwehr von Angriffsversuchen einsetzen.

 +49 89 2555 2276 | enterprise@cloudflare.com | cloudflare.com/de-de/

Herausforderungen bei der Anwendungssicherheit

Cloudflare bietet wirksameren Schutz

Wir ermöglichen effektivere WAF-Sicherheit mit mehrstufigem Schutz:

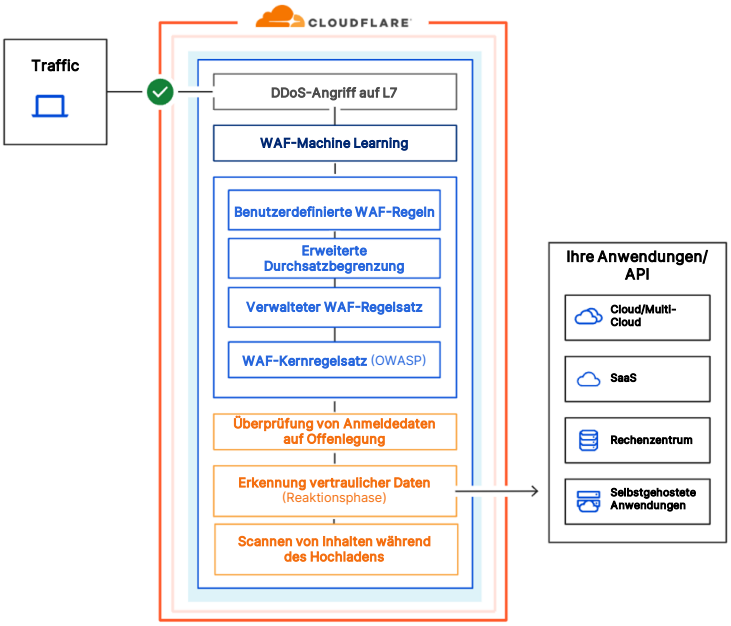
- Sicherheitsanalysen
- Mehrere verwaltete Regelsätze
- Benutzerdefinierte Regeln
- Erkennung mithilfe maschinellen Lernens
- Schutz sensibler Daten
- Überprüfung auf gestohlene Anmeldedaten
- Erweiterte Durchsatzbegrenzung
- Scannen von Uploads zum Schutz vor Malware

Cloudflare bietet kürzere Reaktionszeiten

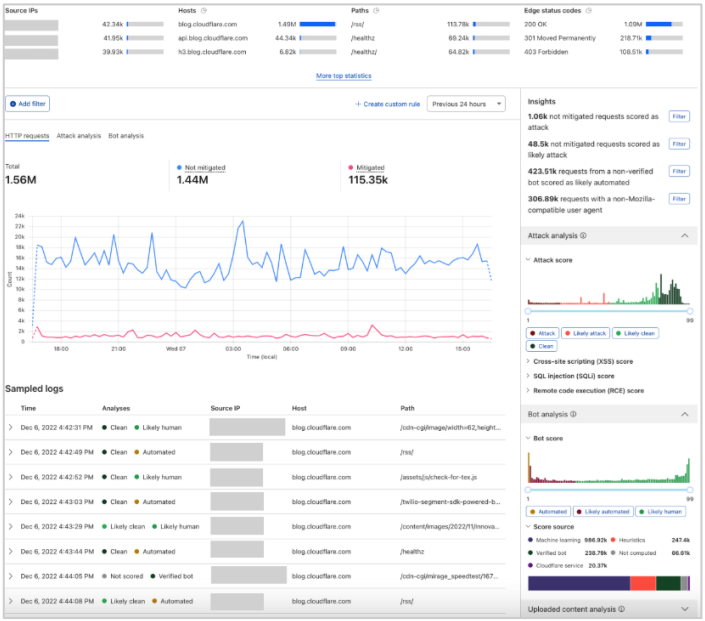
Wir schützen schneller vor Exploits. Bei schwerwiegenden Schwachstellen wie HTTP/2 Rapid Reset und Log4j wurden diverse verwaltete Regeln von uns einen ganzen Werktag früher durchgesetzt als von anderen WAF Anbietern.

Anwendungssicherheit ist bei Cloudflare vollständig integriert

Unsere WAF ist vollständig in den Rest unserer Produkte für Anwendungssicherheit eingebunden, einschließlich API Gateway und Bot-Verwaltung. Alles wird in einem einzigen Durchgang über die Connectivity Cloud von Cloudflare bereitgestellt.



WAF-Sicherheitsanalysen



Eine WAF für Sicherheit der Enterprise-Klasse

Für SIEM-Ingrationen geeignet und SOC-fähig

Unsere API und Rohdatenprotokolle ermöglichen eine unkomplizierte Verknüpfung mit SIEM oder die Versorgung von Security Operation Centers (SOC) mit Cloudflare-Bedrohungsdaten.

DevSecOps leicht gemacht

Dank einer sofort einsatzbereiten Terraform-Integration lässt sich Anwendungssicherheit mühelos in einen DevOps-Ansatz einbinden.

Unterstützt durch Cloudforce One

Anwendungssicherheit von Cloudflare umfasst Bedrohungsdaten von Cloudforce One, unserem Team für Bedrohungsanalysen, und nutzt zur Erkennung von Gefahren neue Erkenntnisse, Taktiken, Techniken und Methoden.

Absicherung von Internetanwendungen	
Mehrstufige Abwehrmaßnahmen dank diverser WAF-Regelsätze	Um jede Art von Angriff zu stoppen, werden bösartige Payloads in jedem beliebigen Teil einer Anfrage mit unterschiedlichen Regelsätzen blockiert: 1. Von Cloudflare verwaltete Regeln 2. OWASP Core Ruleset 3. Benutzerdefinierte Regelsätze Neue verwaltete Regeln werden zunächst mit riesigen Mengen von Traffic getestet, damit es zu möglichst wenig Fehlalarmen kommt.
Aktualisierung der Regeln zum Schutz vor Zero-Day-Sicherheitslücken	Die Regeln werden von den Cloudflare-Sicherheitsteams ständig aktualisiert, um vor neuen Angriffen und Zero-Day-Schwachstellen zu schützen, bis Patches oder Updates verfügbar sind.
Erkennung mithilfe maschinellen Lernens	Ausweichmanöver können mit Machine Learning-Modellen unterbunden werden, die mehrstufige Regelwerke ergänzen. Für Regeln sind vier Scores zur Angriffsbewertung verfügbar: für XSS-Angriffe, für SQLi-Angriffe, für RCE-Angriffe sowie ein übergeordneter WAF-Angriffscore.
Plattformspezifische Regelsätze für wichtige CMS- und E-Commerce-Plattformen	Direkt einsatzbereiter Schutz ohne zusätzliche Gebühren für Plattformen wie WordPress, Joomla, Plone, Drupal, Magneto oder IIS.
Konfiguration benutzerdefinierter Regeln	Bei der Implementierung von Regeln oder Regelsätzen kann mit den folgenden Aktionen ein positives oder negatives Sicherheitsmodell angelegt werden: BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA, CUSTOM RESPONSES.
Erweiterte Durchsatzbegrenzung	Missbrauch von Anwendungen und API sowie DDoS- und Brute-Force-Angriffe werden durch eine Durchsatzbegrenzung für einzelne IP-Adressen oder anhand von Header-Attributen (z. B. Schlüssel, Cookie, Token), ASN oder Land unterbunden.
Schutz sensibler Daten	Rückmeldungen mit vertraulichen Angaben wie personenbezogenen Informationen, Finanzdaten, Kreditkartennummern oder API-Schlüsseln werden blockiert.
Überprüfung von Anmeldedaten auf Offenlegung	Credential Stuffing-Angriffe mit gestohlenen Anmeldedaten werden vor der Übernahme von Endnutzerkonten erkannt.
Scannen von hochgeladenen Inhalten	Im Rahmen der WAF-Inhaltsprüfung werden hochgeladene Dateien auf Malware gescannt. Die daraus gewonnenen Informationen können gemeinsam mit anderen Parametern der Anfrage in benutzerdefinierte Regeln einfließen.
SSL/TLS	SSL-Traffic kann für Anwendungen vollständig ausgelagert und konfiguriert werden.
Weniger Fehlalarme	Neue Regeln werden mit großen Mengen Traffic getestet, um eine geringe Zahl von Fehlalarmen sicherzustellen.
Support von gRPC und Websocket	Für gRPC- und Websocket-Endpunkte kann Traffic über einen Proxy geleitet und abgesichert werden.
Benutzerdefinierte Blockierseiten	Blockierseiten mit passenden Angaben für Besucher lassen sich individuell gestalten.
Vollständige Integration mit der übergeordneten Cloudflare-Produktsuite	Es besteht die Möglichkeit, die Anwendungsperformance zu verbessern, den Traffic geografisch umzuleiten und Edge-Computing einzusetzen.

Überblick, Reporting und Programmierbarkeit	
Sicherheitsanalysen	Visualisierung aller potenziellen Angriffe, die durch maschinelles Lernen eine Einstufung erhalten haben.
Echtzeit-Protokollierung und Zugang zu Rohdatenprotokollen	Sie erhalten einen besseren Überblick zur Feinabstimmung der WAF und können eingehende Analysen aller WAF-Anfragen durchführen.
Payload-Protokollierung	Schädliche Payloads werden zur Vorfallanalyse protokolliert und verschlüsselt.
SIEM-Integrationen	Protokolle können direkt an bestehende SIEM übertragen oder von diesen bezogen werden.
Terraform-Integration	Anwendungssicherheit ist in CI/CD-Arbeitsabläufe integrierbar.
Management	
Steuerung über eine einzige Schnittstelle	Die Steuerung wird durch eine einzige Benutzerschnittstelle zur Implementierung und Verwaltung der globalen Sicherheit und Performance von Anwendungen optimiert.
Verwaltung auf Kontoebene	Dank einer einzigen WAF-Konfiguration auf Kontoebene für alle Domains kann Zeit gespart werden.
Hohe Verfügbarkeit mit SLA	Es wird 100%ige Verfügbarkeit garantiert und bei Verstoß gegen SLA wird eine Entschädigung gezahlt.
Keine zusätzliche Hard- bzw. Software oder Feinabstimmung erforderlich	Die Lösung ist mit einer einfachen DNS-Änderung implementierbar.
PCI-Zertifizierung	Cloudflare verfügt über eine Zertifizierung als Level 1-Dienstleister.
FedRAMP-Autorisierung	Unsere Anwendungssicherheit umfassende Produktreihe „Cloudflare for Government“ verfügt über eine FedRAMP-Autorisierung.

Haben wir Sie neugierig gemacht? Dann registrieren Sie sich für unsere Demo-Reihe zu Anwendungssicherheit.

 +49 89 2555 2276 | enterprise@cloudflare.com | cloudflare.com/de-de/