CLOUDFLARE

Web Application Firewall

Schützen Sie Ihre Website vor SQL-Einschleusung, Cross-Site-Scripting und mehr.

Die Web Application Firewall (WAF) von Cloudflare schützt Ihre Website vor SQL-Einschleusung, Cross-Site-Scripting (XSS) und Zero-Day-Angriffen, inklusive OWASP-identifizierter Schwachstellen und Bedrohungen, die auf die Anwendungsschicht abzielen. Zu unseren Kunden gehören die Alexa Top 50, Finanzinstitutionen, E-Commerce-Unternehmen und große Firmen. Unsere WAF ist vollständig in unseren DDoS-Schutz integriert, wehrt täglich Millionen von Angriffen ab und lernt automatisch mit jeder neuen Bedrohung.

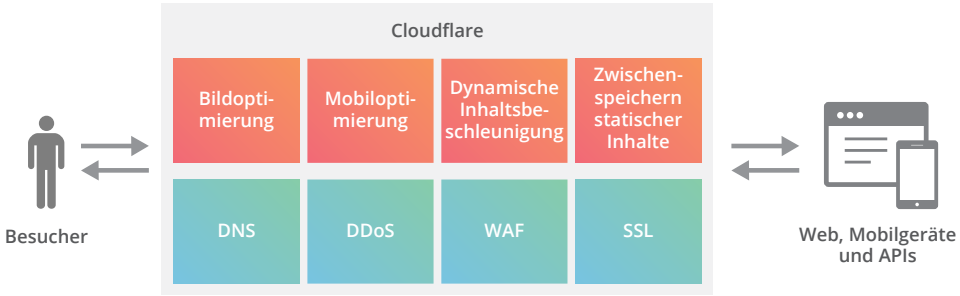
Stabile Regelengine zur Anpassung an Ihre Bedürfnisse

Unsere WAF führt einsatzbereite ModSecurity-Regelsätze aus und schützt Sie so vor den kritischsten OWASP-identifizierten Sicherheitsrisiken bei Webanwendungen. Sie kann auch mit Ihren vorhandenen Regelsätzen und benutzerdefinierten Regeln verwendet werden. Alle Regeln werden in unter 30 Sekunden umgesetzt.

Cloudbereitstellung mit DDoS-Abwehr und CDN

Als cloudbasierter Service ist für die Cloudflare-WAF keine Hard- oder Software-Installation und -wartung erforderlich. Sie kann mit einem einzigen Klick bereitgestellt und an Ihre Bedürfnisse angepasst werden.

Durch die Integration in den allgemeinen Cloudflare-Service erhalten Sie zusätzliche Funktionalität ohne weitere Kosten. Sie können Ihre Website vor DDoS-Angriffen schützen und unser globales Content Delivery Network nutzen, um sie zu beschleunigen.



Highlights:

- **Automatischer Schutz** vor diversen Bedrohungen mit starken Standardregelsätzen und enormen Anpassungsmöglichkeiten für vollständig in die DDoS-Abwehr integrierte Sicherheit der Schicht 7
- **Atemberaubend schnelle Verarbeitung in 0,3 ms** mit sofortigen globalen Aktualisierungen
- **Kosteneffektive Compliance mit PCI-DSS-Anforderung 6.6** und PCI-Compliance dank Cloudflare-WAF
- **Echtzeitberichterstattung** mit stabiler Protokollierung
- **Cloudbereitstellung** ohne zusätzlich Hard- bzw. Software oder Abstimmung

Wichtigste Funktionen	Vorteile
Sicherheit	
Deep Packet Inspection für Anwendungen/ Schicht 7	Schutz Ihrer Standard- und Benutzerwebanwendungen vor SQL-Einschleusung, Cross-Site-Scripting und Tausenden weiteren Bedrohungen
SSL	Terminierung von SSL-Verbindungen ohne Mehraufwand oder zusätzliche Latenz, Anwendung Ihrer WAF-Richtlinie auf SSL-verschlüsselten Verkehr ohne Upload von Zertifikaten und Investition in kostspielige Hardwarelösungen
Für GET- und POST HTTP/S-Anforderungen	Abdeckung des HTTP/S-Verkehrsbereichs
URL-spezifische Benutzerregelsätze	Ein-/Ausschluss spezifischer URLs oder Subdomänen für WAF-Schutz zum Testen von Domänen oder Ein-/Ausschluss spezifischer Subdomänen
Integrierte DDoS-Abwehr	Vollständiger Stack-Schutz gegen DDoS ohne zusätzliche Implementierung
IP-Reputation-Datenbankintegration	Echtzeitdaten zu über 1 Mrd. einzigartiger IPs zum Schutz vor schädlichem Verkehr ohne zusätzliche Implementierung
Virtuelles Patching	Beheben von Schwachstellen vor dem Patching Ihres Servers bzw. der Aktualisierung Ihres Codes für zusätzliche Zeit zum Patching und Testen von Updates
Beschränkung nach IP oder Geolocation	Black-/Whitelisting für Verkehr von spezifischen IP-Adressen oder aus spezifischen Ländern zum Schutz gegen Hacker mit bestimmten IPs oder aus bestimmten Ländern
Wenige falsch positive Ergebnisse	Allgemeine Falsch-positiv-Rate von 1:50 Mio. zur Sicherstellung, dass legitimer Verkehr bei Ihnen ankommt
Vollständige Integration in CDN-Service für Transformierung ausgehender Inhalte	Weniger Weblatenz für Ihre Sitebesucher ohne zusätzliche Implementierung
Regelsätze	
Automatisches Lernen gemeinsam mit sicherheitsgestützter Recherche	Schutz gegen Zero-Day-Schwachstellen oder neue Bedrohungen – durch von unserem Sicherheitsteam automatisch bereitgestellte Patches
Kompatibilität mit ModSecurity-Logik und -Format	Einfacher Import vorhandener Regelsätze zum Beibehalten des vorhandenen Schutzes
OWASP ModSecurity-Grundregelsätze	Standardmäßiger Schutz ohne zusätzliche Gebühren gegen OWASP-Schwachstellen – den kritischsten Fehlern, die durch das Open Web Application Security Project (OWASP) identifiziert werden
Zero-Day-Regelsätze von Cloudflare	Standardmäßiger Schutz durch das Cloudflare-Sicherheitsteam ohne zusätzliche Gebühren gegen Bedrohungen, die bei unserer gesamten Kundschaft identifiziert werden
Plattformspezifische Regelsätze für wichtige CMS- und E-Commerce-Plattformen	Einsatzbereiter Schutz ohne zusätzliche Gebühren für Plattformen wie WordPress, Joomla, Plone, Drupal, Magneto, IIS
Benutzerdefinierte Regeln	Standardmäßige Abdeckung von für Ihre Webanwendung einzigartigen Situationen ohne zusätzliche Gebühren für Business- und Enterprise-Kunden
WAF-Einstellungen	
Blockierung	Abwehren eines Angriffs zur Verhinderung von Aktionen, bevor Ihre Website erreicht wird
Simulation	Test falsch positiver Ergebnisse durch Aufzeichnung der Reaktion auf mögliche Angriffe ohne Herausforderung oder Blockierung
Herausforderung	Aufforderung von Besuchern, auf einer Herausforderungsseite ein CAPTCHA zum weiteren Zugriff auf Ihre Website einzugeben
Schwellenwert-/Empfindlichkeitseinstellung	Festlegen von Regeln zur Auslöseempfindlichkeit
Benutzerdefinierte Blockierungsseiten	Benutzerdefinierte Seiteneinstellung für blockierte Besucher, z. B.: „Unter dieser Telefonnummer erhalten Sie Unterstützung.“ – für Enterprise-Kunden
Berichterstellung	
Echtzeitprotokollierung	Mehr Sichtbarkeit zur Feinabstimmung der WAF
Zugriff auf nicht aufbereitete Protokolldateien	Tiefgreifende Analyse aller WAF-Anforderungen für Enterprise-Kunden
Administration	
Hochverfügbarkeit auf Grundlage der Service-Angebot-SLA	100 % Verfügbarkeitsgarantie für Business- und Enterprise-Kunden mit finanziellen Abschlägen, wenn diese nicht erfüllt wird
Keine zusätzliche Hard- bzw. Software oder Abstimmung	Anmeldung durch einfache Änderung des DNS
PCI-Zertifizierung	Level-1-Service-Anbieterzertifizierung des Cloudflare-Service