

Cloudflare Page Shield

Sichert die Supply Chain Ihrer Webanwendungen ab und schützt Endnutzer vor clientseitigen Angriffen

Zunahme clientseitiger Angriffe

Blinde Flecken durch Drittanbieter-Abhängigkeiten

Um den Nutzern das Surfen so angenehm wie möglich zu gestalten, erweitern Unternehmen ihre Websites unter anderem um Chatbots und Analysefunktionen, für deren Bereitstellung sie auf externe Dienstleister oder Entwickler zurückgreifen. Angreifer wiederum versuchen, diese Drittanbieter-Abhängigkeiten zu infiltrieren, um die von Endnutzern auf der Website eingegebenen vertraulichen Daten zu stehlen, Schadsoftware zu installieren, Kryptomining zu betreiben oder spätere Attacken vorzubereiten.

Angriffe auf die Supply Chain erkennen und abwehren

Page Shield schützt die Endnutzer von Websites vor clientseitigen Angriffen, die auf anfällige JavaScript-Abhängigkeiten abzielen. Die Lösung erhält direkt vom Browser Informationen darüber, welche JavaScript-Dateien und -Module geladen werden, führt Analysen zur Erkennung von Schadskripten durch, erlaubt Ihnen einen Überblick über alle aktiven Skripte und ausgehenden Verbindungen und meldet, wenn eine JavaScript-Datei böses Verhalten an den Tag legt.

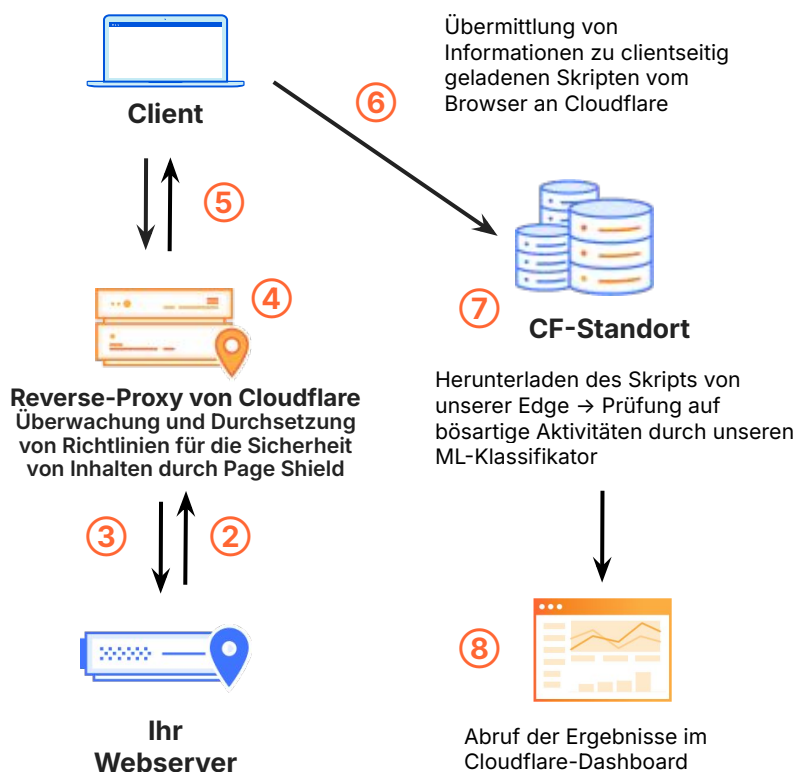


Abbildung 1: Architektur von Cloudflare Page Shield



Smarte Angriffsvorbeugung

Die kontinuierliche Überwachung von aktiven Skripten, Änderungen an Skripten und der von diesen hergestellten Verbindungen erlaubt einen vollständigen Überblick über die Webanwendungslieferkette und ermöglicht die Abwehr von Supply Chain-Angriffen.



Automatische Bedrohungswarnungen

Lassen Sie sich sofort benachrichtigen, wenn neue Skripte erkannt, als böse gekennzeichnet oder von unbekannten Domains geladen werden.



Rechtskonformität

Das mit Drittanbietern verbundene Risiko wird reduziert und Sie können die kundenseitigen Anforderungen von Vorschriften wie der DSGVO und [PCI DSS 4.0](#) erfüllen. Page Shield hilft Ihnen bei der Einhaltung dieser Vorgaben ohne zusätzlichen Aufwand.

Funktionen zur Übernahme der Kontrolle über die Supply Chain Ihrer Webanwendung und den Schutz der Browserumgebungen Ihrer Endnutzer

Page Shield	
Script Monitor	Zeigt Informationen zu den Drittanbieter-Skripten an, die auf den Seiten Ihrer Domain geladen werden.
Connection Monitor	Zeigt Informationen zu Verbindungen an, die von den Skripten auf den Seiten Ihrer Domain hergestellt werden.
Cookie Monitor	Zeigt Informationen zu Cookies an, die im HTTP-Traffic entdeckt wurden.
Seitenzuordnung	Zeigt an, auf welcher Seite ein Skript zuerst erschienen ist, und liefert eine Liste der neuesten Fälle, bei denen das Skript auf Ihren Seiten aufgetreten ist.
Warnmeldungen zu neuen Ressourcen und neuen Domains	Benachrichtigungen über neu entdeckte Skripte oder Skripte, die von unbekannten Domains geladen werden, können konfiguriert und individuell angepasst werden.
Erkennung von und Warnung vor schädlichen Skripten	Erkennt bösartige Skripte in Ihren Seiten mithilfe von Bedrohungsdaten und maschinellem Lernen.
Erkennung von Codeänderungen und Benachrichtigung	Erkennt alle Änderungen an den Skripten und Verbindungen, die auf Ihren Seiten geladen werden. Die Häufigkeit der Benachrichtigungen ist konfigurierbar.
Erkennung von schädlichen Verbindungen und Benachrichtigung	Erkennt, wenn ein Skript eine Verbindung zu einer bösartigen Domain herstellt, z. B. einer Command-and-Control-Domain oder einem Cloud-Speicher, bei dem eine Datenausschleusung zu vermuten steht.
Richtlinien	Die für Ihre Anwendungen zulässigen Ressourcen sind durch Content Security Policy (CSP)-Anweisungen in Richtlinien definiert. Mittels Richtlinien lassen sich Verstöße protokollieren und positive Sicherheitsmodelle durchsetzen, bei denen Ressourcen blockiert werden, die nicht auf einer Genehmigungsliste stehen.



Möchten Sie Page Shield in Aktion sehen? Dann melden Sie sich jetzt für unsere kostenlose [clientseitige Risikobewertung](#) an.