CLOUDFLARE®

Sicherheit für Anwendungen in der Cloud

Schnelle, einfach bereitzustellende und skalierbare mehrschichtige Abwehr gegen DDoS, Datendiebstahl und böswillige Bots.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Sicherheit für Anwendungen in der Cloud

Schnelle und einfach bereitzustellende, mehrschichtige Abwehr für den Schutz vor DDoS, Datendiebstahl und böswillige Bots

Der Druck auf die Unternehmen zur Verbesserung ihrer Sicherheitsmaßnahmen nimmt immer mehr zu. Für diesen Druck gibt es drei Ursachen:

- Die Angreifer werden stärker, raffinierter und sind hoch motiviert.
- Die Angriffsfläche wird größer, weil von den Anwendungen immer mehr öffentliche APIs, eine größere SaaS-Implementierung und eine Integration in mehr Drittanbieteranwendungen bereitgestellt werden.
- Erhöhte öffentliche und behördliche Kontrolle von Daten, Privatsphäre und Sicherheit.

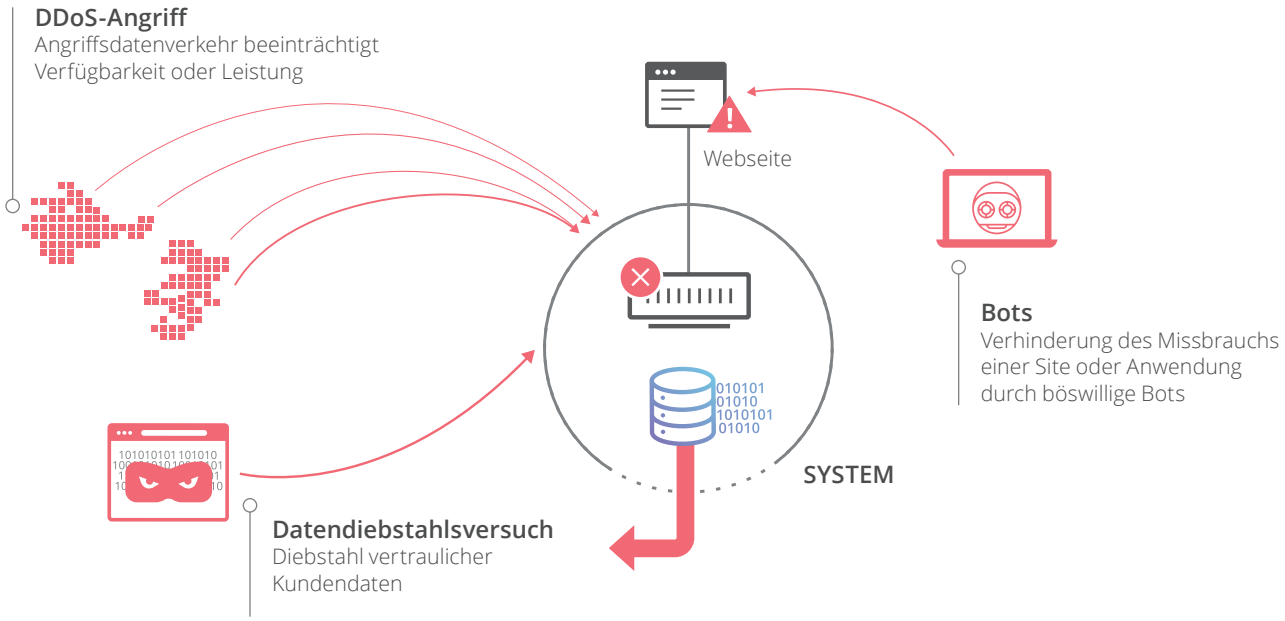
Die Angreifer erhöhen Häufigkeit und Umfang von DDoS-Angriffen (DDoS – Distributed Denial-of-Service). Durch die Nutzung von Botnets und der Millionen IoT-Geräte (IoT - Internet of Things), die inzwischen online sind, können sie volumetrische Angriffe leichter und mit größeren Auswirkungen ausführen.

Zusätzlich zum größeren Umfang der Angriffe konzentrieren sich die Angreifer inzwischen nicht mehr auf die Netzwerkschicht, sondern auf die Anwendungsschicht. Die Erkennung von Angriffen auf die Anwendungsschicht bzw. von „Layer 7"-Angriffen ist schwieriger, die Angriffe benötigen weniger Ressourcen zum Lahmlegen einer Website oder Anwendung und sie unterbrechen den Betrieb.

Die Angreifer nutzen ihre Angriffe, um Sites zu blockieren oder vertrauliche Daten zu stehlen, zum Beispiel zum Erpressen von Lösegeld. Da sie von manchen Unternehmen bereits erfolgreich Lösegeld erpresst haben, sind die Angreifer inzwischen motivierter, organisieren sich besser und breiten sich aus.

Angesichts dieser zunehmenden Bedrohung müssen die Unternehmen ihre Abwehr gegen drei Hauptprobleme bzw. -bedrohungen verstärken:

- Einen DDoS-Angriff auf Anwendungen, Websites und APIs, durch den sich die Verfügbarkeit oder Leistung verschlechtert, was zu Umsatzeinbußen, höheren Betriebskosten und negativen Auswirkungen auf die Marke führt.
- Diebstahl vertraulicher Kunden- und Geschäftsdaten, wie zum Beispiel personenbezogener Daten oder geistigen Eigentums, was zum Verlust von Kunden und dem Vertrauen der Kunden führt.
- Böswillige Bots, die Kundenanwendungen durch Content Scraping, Kontoübernahmen und betrügerische Bezahlvorgänge missbrauchen.



Die finanziellen Kosten für einen DDoS-Angriff, einen Datendiebstahl oder böswillige Bots hängen vielleicht von Unternehmensgröße und Branche ab, die geschäftlichen Auswirkungen werden jedoch für alle Unternehmen immer deutlicher spürbar.

Laut einem IDC-Bericht von 2015 betragen die durchschnittlichen Kosten für einen Ausfall der Infrastruktur pro Stunde 100.000 US-Dollar.[1]

Bei einem Datendiebstahl können Benutzerinformationen gestohlen oder vertrauliche Kundendaten weitergeleitet werden, zum Beispiel die Kreditkartennummern und Kennwörter aus dem Datenspeicher einer Anwendung. Die durchschnittlichen globalen Kosten bei einem Datendiebstahl betrugen 2017 pro verlorenem oder gestohlenem Datensatz 141 US-Dollar und die durchschnittlichen Gesamtkosten für einen Datendiebstahl beliefen sich auf 3,62 Millionen US-Dollar.[2] Aufgrund der gestiegenen Kontrolle durch Regierungen und Medien haben auch kleine Datendiebstähle immer größere Folgen für die Unternehmen, nicht nur in Form finanzieller Strafen, sondern auch durch den Verlust des Vertrauens in der Öffentlichkeit.

Böswillige Bots können nicht nur das Konto eines Benutzers übernehmen, sondern auch Schäden durch betrügerische Einkäufe und Content Scraping verursachen. Betrügerische Zahlungen durch einen Bot, der wiederholt und automatisch begrenzt vorhandene Bestände kauft, kann die Marke eines Geschäfts beschädigen, potenzielle zukünftige Kunden vom Kauf abhalten und so zu niedrigeren Umsätzen führen, manchmal können dadurch sogar die Beziehungen zu den Lieferanten beeinträchtigt werden. Content Scraping kann besonders bei werbetreibenden Unternehmen direkt den Umsatz senken, zum Beispiel durch ein niedrigeres SEO-Ranking, das Senken des CPM-Werts (CPM - Cost-Per-Thousand Impressions) oder den Verlust von Werbetreibenden.

Der Vorteil

Beim Kampf gegen die zunehmenden Gefahren und die gestiegenen Auswirkungen auf die Unternehmen dürfen sich diese nicht nur auf bestimmte taktische Probleme konzentrieren, sondern müssen nach einem Vorteil gegenüber den Böswilligen in einer sich wandelnden Bedrohungslandschaft suchen.

Drei wichtige Unterschiede sind **Größe, Leistung und Benutzerfreundlichkeit**.

Größe ist wichtig

Ein Vorteil von Cloudflare ist die Netzwerkgröße und die Schwankungsbreite des Datenverkehrs für die Datenanalyse. Cloudflare schützt über sechs Millionen Kundenwebsites und hat so einen Überblick über die aktuelle Entwicklung der globalen Bedrohungen. Auf der Basis dieser Erkenntnisse verteidigt Cloudflare seine Kunden durch DDoS-Schutzmaßnahmen und eine Web Application Firewall (WAF) proaktiv gegen Angriffe, die Ausfallzeiten und Umsatzeinbußen nach sich ziehen könnten.

Da es für die große Mengen ausgelegt ist, bietet das Cloudflare Netzwerk sowohl Geschwindigkeit als auch Stabilität. Damit alle Services für über 300 Milliarden Anfragen pro Tag bereitgestellt werden können, können die auf jedem Server im Rechenzentrum ausgeführten Services - wie DNS, Verschlüsselung und WAF - enorme Datenverkehrsaufkommen mit niedriger Latenz und hoher Verfügbarkeit verarbeiten.

Da die Größe der DDoS-Angriffe zunimmt, profitieren die Kunden von der Größe und Stabilität des Netzwerks. Mit seinen über 116 Rechenzentren und dem Anycast-Netzwerk kann Cloudflare auch die größten verteilten Angriffe abwehren.

Erhöhen der Leistung und Schützen der Anwendungen

Die Kunden mussten bisher immer einen Kompromiss zwischen Sicherheit und Leistung eingehen. TLS- und WAF-Lösungen sorgten oft für eine Verschlechterung der Leistung auf einer Site. TLS, ein Protokoll zur Verschlüsselung von Verbindungen, kann dazu führen, dass bis zu vier Round Trips nur zum Starten einer einzigen sicheren Sitzung erforderlich sind. Diese zusätzlichen Round Trips können die Latenzzeit erhöhen. Analog führt eine WAF zu zusätzlichen Verzögerungen, da von ihr jede Anforderung überprüft wird.

[1] IDC, DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified, Stephen Elliot, März 2015

[2] Ponemon Institute, 2017 Cost of Data Breach Study, Juni 2017

Cloudflare sorgt dafür, dass für die Sicherheit nicht Leistung geopfert werden muss. Anstatt die Leistung zu senken, können die Sicherheitsfunktionen von Cloudflare die Anwendungsleistung erhöhen, weil Sicherheitsservices mit niedriger Latenz mit der Beschleunigung des Datenverkehrs kombiniert werden. Die Unterstützung von TLS 1.3 und eine globale Sitzungswiederaufnahme können die Anzahl der Round Trips reduzieren und HTTP/2, das Multiplex-Downloads ermöglicht, verkürzt die Seitenladezeiten. Da Cloudflare die Sicherheitsservices mit Services für die Beschleunigung des Datenverkehrs kombiniert, wie zum Beispiel Caching und Smart Routing, ist die Leistung der Anwendungen höher als bei einer unsicheren Ausführung ohne Cloudflare.

Durch das Caching ist der statische Inhalt näher an den Besuchern einer Website. So wird nicht nur die Belastung der ursprünglichen Server reduzieren, sondern auch die Antwortzeit der Anwendung verkürzt. Mit Smart Routing wird der schnellste Weg von Cloudflare zum Ursprung ermittelt, was sowohl den dynamischen als auch den statischen Inhalt beschleunigt.

Größe

Stabilität immer im Mittelpunkt

Benutzerfreundlichkeit

Intuitive Benutzeroberfläche und API für flexible Konfiguration und Verwaltung

Geschwindigkeit

Leistungsfähige Sicherheit kombiniert mit Beschleunigung des Datenverkehrs

Verbesserung der Sicherheitsinfrastruktur durch Benutzerfreundlichkeit

Bei der Benutzerfreundlichkeit einer Sicherheitslösung für Benutzer und Administratoren geht es nicht nur um eine schöne Oberfläche; sie trägt auch zur Verbesserung der Sicherheitsinfrastruktur eines Unternehmens bei. Eine Untersuchung von Gartner geht davon aus, dass Firewalls bis 2020 zu 99 % aufgrund von Fehlkonfigurationen und nicht wegen Schwachstellen überwunden werden.[3]

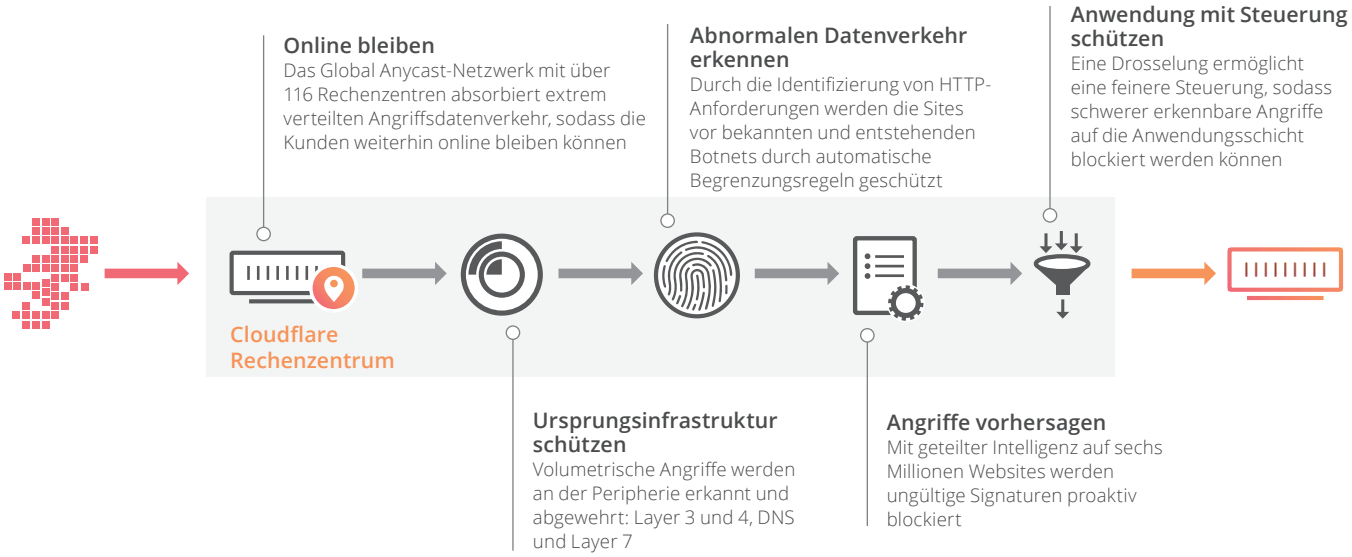
Eine gute Benutzererfahrung verringert Sicherheitsrisiken durch Fehlkonfigurationen und verbessert die Agilität in einer sich ändernden Bedrohungslandschaft. Die Konfiguration von Cloudflare kann in weniger als 5 Minuten abgeschlossen sein. Diese Benutzerfreundlichkeit ermöglicht es Unternehmen, die Verwaltung der Sicherheitsrichtlinien auf mehr Mitarbeiter auszuweiten, die keine Sicherheitsexperten sein müssen, die Zeit zum Ändern und Bereitstellen neuer Richtlinien zu reduzieren und zeitnahe Anpassungen der Sicherheitsinfrastruktur bei komplexen Anwendung zu verbessern.

Mit diesen Vorteilen will Cloudflare seine Kunden vor den drei wichtigsten Herausforderungen schützen: DDoS-Angriffe, die die Leistung und Verfügbarkeit ihrer Anwendungen beeinträchtigen, Diebstahl von Kundendaten durch breitgefächerte Angriffe und Missbrauch der Website durch böswillige Bots.

Schutz Ihrer Anwendung vor DDoS-Angriffen

Bei einem DDoS-Angriff wird durch extrem hohen Datenverkehr versucht, eine Site oder einen Service zu blockieren. Die Überlastung der Ursprungsserver durch diesen böswilligen Datenverkehr führt dazu, dass die Zielanwendung langsam wird oder für Endbenutzer nicht mehr verfügbar ist. Cloudflare bietet dagegen eine mehrschichtige Verteidigung.

[3] Gartner, Inc., One Brand of Firewall Is a Best Practice for Most Enterprises, Adam Hils and Rajpreet Kaur, 5. Juni 2017



Globales Anycast-Netzwerk

Das Anycast-Netzwerk aus über 116 Rechenzentren vergrößert die Oberfläche, auf die Cloudflare DDoS-Angriffe verteilen kann. In Anycast teilen mehrere Geräte die gleiche IP-Adresse. Wenn eine Anfrage an eine Anycast-IP-Adresse gesendet wird, wird sie vom Router an die nächstgelegene Maschine im Netzwerk gesendet. So werden extrem verteilte Angriffe durch Botnets abgemildert, weil ein Teil des DDoS-Datenverkehrs von jedem unserer Rechenzentren absorbiert wird und nicht auf einen einzigen Punkt konzentriert werden kann.

Intelligente und automatische Risikoreduzierung an der Peripherie

Da Cloudflare die Übersicht über 6 Millionen Sites hat, kann der DDoS-Schutzservice auf der Basis von Angriffen auf eine Site eine Heuristik zum Schutz vieler anderer Sites entwickeln.

Durch die automatische Identifizierung der Netzwerkdurchsätze und des HTTP-Angriffsdatenverkehrs wird der Angriffsdatenverkehr ermittelt und gestoppt, bevor die Sites der Kunden durch ihn geschädigt werden.

Da solche umfassenden Angriffe an der Peripherie des Netzwerks aufgehalten werden, bleiben die Ursprungsserver des Kunden geschützt und online.

Integriertes Paket aus DNS-, Netzwerk- und Layer 7-Schutz

Da jeder Edge-Server über ein integriertes Paket aus Sicherheitsservices verfügt, zum Beispiel DNS, Firewall, Drosselung und WAF, kann Cloudflare nicht nur verteilten Schutz bieten, sondern auch eine mehrschichtige Abwehr gegen unterschiedliche Arten von DDoS-Angriffen, insbesondere gegen DDoS-Angriffe auf DNS, Netzwerk und die Anwendungsschicht (Layer 7).

Der verteilte DNS-Service von Cloudflare kann Angriffe gegen Domain Name Server (DNS) abwehren. Netzwerkangriffe, zum Beispiel auf Layer 3 und 4, werden nicht nur automatisch blockiert, sondern von den Kunden kann auch konfiguriert werden, dass böswillige Quellen unter Verwendung von IP, Ursprungsland oder ASN über eine IP-Firewall blockiert werden. Für die Sicherheitseinstellungen können die Erkenntnisse von Cloudflare über die Reputation einer IP-Adresse auf den 6 Millionen Websites verwendet werden, um schädlichen Datenverkehr proaktiv zu erkennen.

> Wir schätzen die Sicherheit, die wir jetzt durch Cloudflare haben, weil wir uns darauf verlassen können, dass wir vor jeder Art von bösartigen DDoS-Angriffen geschützt sind.
>
> BUKCRAFT | LEE MCNEIL, CTO

Konfigurierbare volumenbasierte Vorsorge

Obwohl die Kunden durch die DDoS-Lösungen von Cloudflare automatisch vor volumetrischen Angriffen auf Netzwerke und Anwendungen geschützt werden, benötigen manche Kunden konfigurierbare Steuerungen, um sich vor weniger umfangreichem, aber trotzdem böswilligem Datenverkehr zu schützen.

Da die Kunden die Schwellenwerte für die Anforderungsrate, die Ziel-URI und die Anforderungsattribute anpassen können, zum Beispiel Methode oder Antwortcode, können sie ihre Abwehr abhängig von ihrem Anwendungs- und Datenverkehrsprofil optimieren.

Reduzierung der Gefahr von Datendiebstahl durch mehrschichtige Abwehr

Angreifer nutzen oft mehrere Angriffsvektoren, wenn sie versuchen, Kundendaten zu stehlen. Um sich zu schützen, benötigen die Unternehmen eine mehrschichtige Abwehr.

ANGRIFFE	LÖSUNGEN VON CLOUDFLARE
1. Einschleusen schädlicher Nutzdaten über Formulare und APIs	**Blockierung der OWASP Top Ten-Sicherheitslücken und von entstehenden Angriffen auf Anwendungsebene durch die WAF**
2. Abfangen unverschlüsselter vertraulicher Daten, die von Kunden eingegeben wurden	**Blockierung von Snooping durch Verschlüsselung über SSL/TLS**
3. Brute-Force-Angriffe auf Anmeldeseiten	**Anmeldeschutz durch Drosselung**
4. Fälschungsversuche von DNS-Antworten zum Abfangen von Kundenanmeldedaten	**Vermeidung gefälschter Antworten durch robusten DNS und DNSSEC**

Reduzierung von Spoofing durch sichere DNS

Beim Cache Poisoning oder auch „Spoofing“ werden ahnungslose Besucher einer Site dazu verleitet, vertrauliche Daten wie Kreditkartennummern auf einer Site einzugeben, die angegriffen wird. Diese Art von Angriff tritt auf, wenn ein Angreifer den Cache eines Domain Name Servers mit falschen Datensätzen füllt. Bis der Cache-Eintrag abläuft, werden vom Namensserver die gefälschten DNS-Datensätze zurückgegeben. Anstatt zur richtigen Site weitergeleitet zu werden, werden die Besucher zur Site des Angreifers weitergeleitet, auf der der Angreifer dann an die vertraulichen Daten gelangt.

Bei Verwendung von DNSSEC werden die DNS-Datensätze mithilfe kryptographischer Signaturen überprüft. Durch die Überprüfung der Signatur, die einem Datensatz zugeordnet ist, kann bei der DNS-Namensauflösung überprüft werden, ob die angeforderten Informationen vom maßgeblichen Namensserver und nicht von einem dazwischen befindlichen Angreifer (Man-in-the-middle-Angreifer) stammen.

Verringerung von Spoofing durch Verschlüsselung

Die Angreifer können Kundensitzungen abfangen oder überwachen (Snoop), um vertrauliche Kundendaten zu stehlen, unter anderem Anmeldeinformationen wie zum Beispiel Kennwörter oder auch Kreditkartennummern. Bei einem Man-in-the-middle-Angriff wird dem Browser eine Verbindung zum Server über einen verschlüsselten Kanal und dem Server eine Verbindung zum Browser vorgetäuscht, beide sind jedoch mit dem Angreifer verbunden, der sich zwischen ihnen befindet (Man-in-the-middle). Der gesamte Datenverkehr verläuft über diesen Man-in-the-middle, der so alle Daten lesen und ändern kann.

Die Kunden können die Übertragung der Benutzerdaten durch schnelle Verschlüsselung bzw. Beendigung, leichte Zertifikatsverwaltung und Unterstützung der neuesten Sicherheitsstandards schützen.

Blockieren böswilliger Nutzdaten durch automatisch aktualisierte und skalierbare WAF

Die Angreifer nutzen die Sicherheitslücken der Anwendungen zum Übertragen böswilliger Nutzdaten, die vertrauliche Daten aus der Datenbank oder dem Browser des Benutzers extrahieren oder Malware einspeisen, die die Zielsysteme infiziert.

Eine Web Application Firewall (WAF) überprüft den Webdatenverkehr und sucht dabei nach verdächtigem Datenverkehr; sie kann auf der Basis der von Ihnen festgelegten Regeln automatisch unzulässige Anfragen herausfiltern. Sie sucht nach GET- und POST-basierten HTTP-Anfragen und verwendet dazu einen Regelsatz, zum Beispiel den ModSecurity-Kernregelsatz, von dem die wichtigsten 10 Sicherheitslücken nach OWASP (OWASP Top Ten) abgedeckt werden, um zu ermitteln, welcher Verkehr blockiert, überprüft oder zugelassen werden sollte. Sie kann Kommentar-Spam, Cross-Site-Scripting-Angriffe und SQL-Injection blockieren.

Die Cloudflare WAF aktualisiert die Regeln auf Basis der Bedrohungen, die von den 6 Millionen Kunden erkannt wurden, und kann die Kunden ohne Beeinträchtigung der Anwendungsleistung schützen, weil die Latenz für die Überprüfung niedrig und mit einer Beschleunigung des Datenverkehrs verknüpft ist.

Reduzierte Kontoübernahmen durch Schutz der Anmeldung

Angreifer können einen „Wörterbuchangriff“ (Dictionary Attack) ausführen, bei dem die Anmeldungen mit gelöschten Anmeldeinformationen automatisiert werden, um sich anhand eines solchen „Brute-Force-Angriffs“ Zugang zu einer anmeldegeschützten Seite zu verschaffen. Cloudflare ermöglicht den Benutzern das Anpassen von Regeln zur Drosselung, um solche schwer abzuwehrenden Angriffe zu erkennen und zu blockieren.

Schutz durch Überwachung und Bewertung

Mit der Überwachung einer Website auf Sicherheitslücken, der Bewertung des Sicherheitszustands eines Unternehmens und der Integration in den Entwicklungsprozess stellen die Drittanbieter-Apps von Cloudflare eine zusätzliche Schicht an proaktivem Schutz dar.

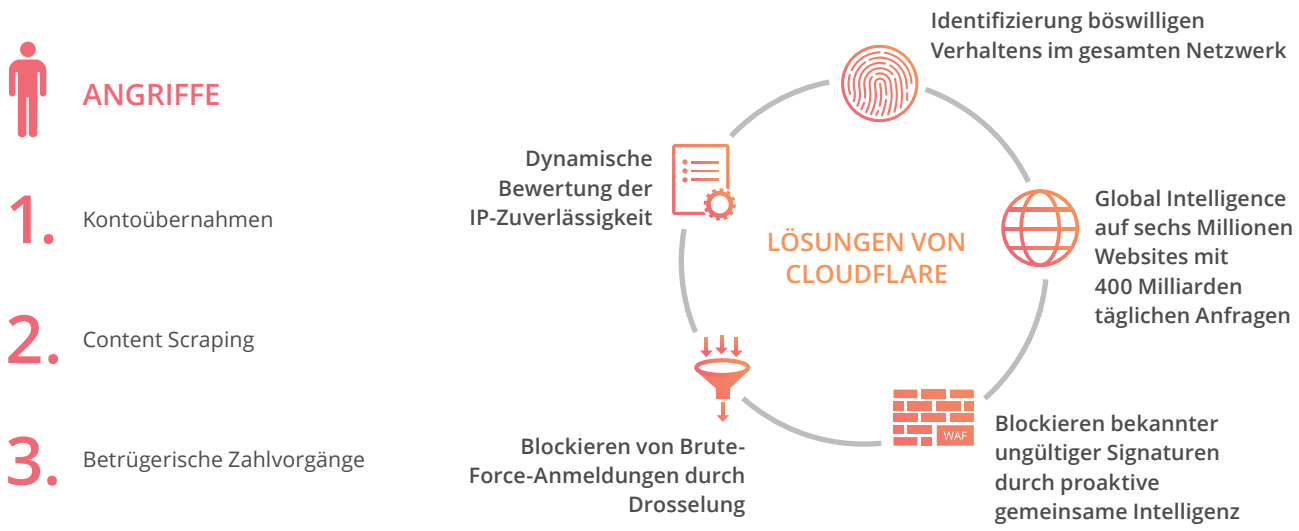
> Aufgrund der Sicherheitsfeatures von Cloudflare brauchten sich unsere Entwickler keine Sorgen mehr darum machen, dass die Site online bleibt und konnten sich auf andere Verbesserungen der Site konzentrieren.

Gazeta Esportiva | DAVID VERZOLLA
Head of Technology

Vermeidung von Missbrauch durch Bots

Die Häufigkeit, die Ausgereiftheit und die Beeinträchtigung der Kunden durch drei Arten von Missbrauch durch Bots nehmen zu. Aus diesem Grund muss eine Lösung zur Vermeidung von Bots aus verschiedenen Elementen für die verschiedenen potenziellen Angriffsprofile bestehen.

Die häufigsten Angriffe sind Kontoübernahmen, Content Scraping und betrügerische Zahlungen. Für alle drei können unterschiedliche Bot-Stile verwendet werden, von denen jeder Einzelne mithilfe einer anderen Methode erkannt und verhindert werden kann.



Volumenbasierte Erkennung und Vermeidung

Da manche Bots automatisiert sind und eine Site mit einem hohen Volumen angreifen, um ihr Ziel zu erreichen, können diese Angriffe durch eine volumenbasierte Automatisierung erkannt und vermieden werden. Bei Brute-Force-Anmeldungen kommt es zum Beispiel zu viel mehr fehlgeschlagenen Anmeldungen von einer einzelnen IP-Adresse als von einem normalen Benutzer. Diese Typen von Kontoübernahmeversuchen können durch volumenbasierte Schwellenwerte erkannt werden. Analog wird bei Angriffen durch Content Scraping auf Seiten, die nicht mehr gefunden werden können (Fehler 404), ein viel größeres Volumen generiert, als bei einem normalen Benutzer.

Blockierung auf Basis bekannter ungültiger Signaturen

Wenn von Cloudflare auf einer der geschützten 6 Millionen Websites ungültige Signaturen von böswilligen Bots erkannt werden, werden sie auf allen anderen blockiert.

Fazit

Um ihre Sicherheit zu bewahren und in einer sich wandelnden Bedrohungslandschaft immer auf dem neuesten Stand zu bleiben, benötigen Unternehmen Leistung, intelligente Sicherheit in großem Umfang und mehrschichtige Abwehrmaßnahmen, um sich vor DDoS-Angriffen, Datendiebstahl und böswilligen Bots zu schützen.

Da der Mensch dabei immer eine wichtige Rolle spielen wird, haben die Benutzerfreundlichkeit beim Bereitstellen und Konfigurieren und die Optimierung der Sicherheitsrichtlinien große Auswirkungen auf die gesamte Sicherheitsarchitektur, da so Falscheingaben verringert werden und mehr Mitarbeiter ohne Gefahren oder unnötige Reibungsverluste auf Änderungen reagieren können.

Cloudflare bietet mit seiner Cloud-Sicherheit Schutz vor den immer raffinierteren DDoS-Angriffen, Datendiebstahlsversuchen durch böswillige Angreifer und dem Missbrauch durch Bots.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com