CLOUDFLARE

E-Book

Ausfallzeiten den Kampf ansagen: Ein Leitfaden zur DDoS-Abwehr

Inhaltsverzeichnis

Durch Klicken gelangen Sie direkt zum gewünschten Abschnitt

Einführung: DDoS-Abwehr im Kontext hybrider Arbeit

Weil gut funktionierende und schnelle Anwendungen für Kunden immer wichtiger werden, nutzt ein durchschnittliches Unternehmen mittlerweile über 1.400 verschiedene Cloud-Dienste[1]. Eine Begleiterscheinung der Verlagerung in die Cloud und des damit einhergehenden Wandels ist allerdings eine Vergrößerung der Angriffsfläche: Mehr digitale Services bedeuten auch mehr Einfallstore für Angreifer. Dabei spielt auch die Verbreitung hybrider Arbeitsmodelle, bei denen Präsenzarbeit und Homeoffice kombiniert werden, während der Pandemiejahre eine Rolle.

All diese Faktoren erhöhen den Druck auf Unternehmen mit knappen Ressourcen. IT- und Sicherheitsabteilungen müssen nicht nur robustere Anwendungen und Netzwerke bereitstellen, sondern auch Nutzer und Geräte standortunabhängig vor Bedrohungen schützen, die immer wieder neue Gestalt annehmen.

Dazu zählen häufigere, längere und umfangreichere Distributed Denial of Service (DDoS)-Angriffe. So wurde von Cloudflare im Februar 2023 der bislang größte HTTPS-DDoS-Angriff aller Zeiten (mit 71 Mio. Anfragen pro Sekunde) entdeckt und abgewehrt. Unsere Daten zeigen außerdem für 2022 einen Anstieg hypervolumetrischer DDoS-Angriffe (von mehr als 100 Gbit/s) von einem Quartal auf das nächste.

Angesichts der aktuellen wirtschaftlichen Gegebenheiten und hybrider Arbeitsmodelle müssen Unternehmen ihre DDoS-Abwehr neu bewerten: das Risiko von Ausfallzeiten, Datendiebstahl, Netzwerkinfiltration und finanziellen Verlusten ist zu groß.

Untersuchungen zeigen, dass über 60 % der Ausfälle mehr als 100.000 US-Dollar und 15 % sogar jenseits von 1 Million US-Dollar kosten[2]. In einem Fall schlugen Ausfälle, die durch eine Serie von DDoS-Angriffen verursacht wurden, bei einem Unternehmen mit fast 12 Millionen US-Dollar[3] zu Buche.

Kein Unternehmen, gleich welcher Größe, kann es sich unter diesen Umständen leisten, auf DDoS-Abwehr zu verzichten. Und die Vergangenheit eingesetzten manuellen Methoden reichen heute nicht mehr aus. Hinter den Angriffen stecken zwar Menschen, ausgeführt werden sie aber von Bots. Gewinnen lässt sich dieser Kampf nur, indem man ebenfalls Bots einsetzt. Die Erkennung und Abwehr von Attacken muss so weit wie möglich automatisiert werden.

Folgende Themen werden in diesem E-Book behandelt:

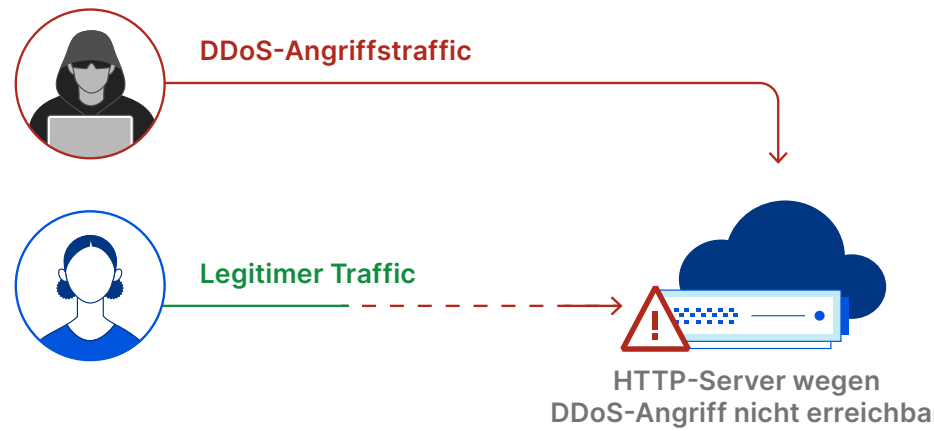
- Verschiedene Modelle für cloudbasierten DDoS-Schutz
- Die Beschränkungen von kontinuierlich aktivem cloudbasiertem Scrubbing
- Die Abwehr eines DDoS-Angriffs auf ein Fortune Global 500-Unternehmen mithilfe von Cloudflare

Wie cloudbasierte DDoS-Abwehr funktioniert

Ein DDoS-Angriff ist ein böswilliger Versuch, den normalen Datenverkehr eines angegriffenen Servers, Diensts oder Netzwerks zu stören, indem das Ziel oder die umliegende Infrastruktur mit Internet-Traffic regelrecht überschwemmt wird. Eine gut funktionierende DDoS-Lösung zeigt Ihnen genau an, wann, wo und wie ein solcher „Stau“ auftritt. Außerdem absorbiert sie den schädlichen Datenstrom und leitet ihn so um, dass der legitime Traffic nicht beeinträchtigt wird. Ins Fadenkreuz geraten häufig Ziele mit hohem Datenverkehrsaufkommen, aber auch ungeschützte Internetpräsenzen und Netzwerke.

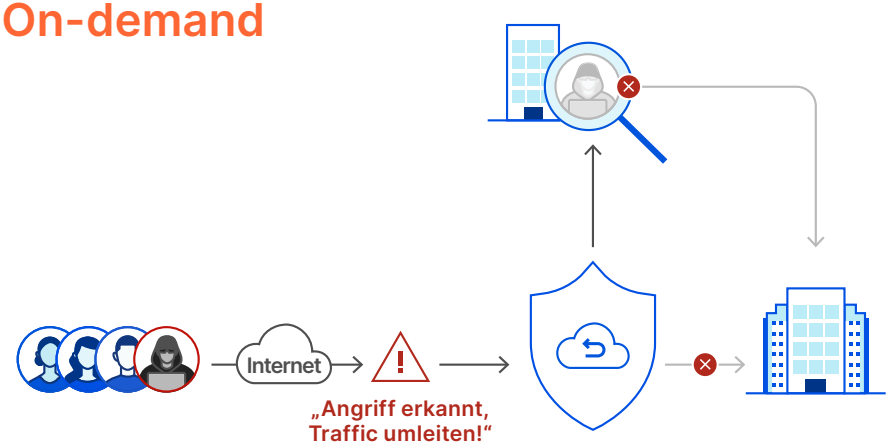
DDoS-Angriffe sind zwar kein neues Phänomen, doch sie zu stoppen, erfordert neue Ansätze. Mit der Verlagerung von Anwendungen in die Cloud ist auch der Markt für lokale DDoS-Lösungen geschrumpft[4]. Stattdessen wenden sich immer mehr Unternehmen für DDoS-Schutz der Cloud zu.

Bei vielen Varianten des cloudbasierten Schutzes platziert sich ein Cloud-Anbieter vor die Anwendungen und die Infrastruktur eines Unternehmens, um den gesamten Datenverkehr zur „Bereinigung“ an ein Scrubbing-Center weiterzuleiten. Nur der legitime Traffic wird an den Kunden zurückgeschickt. Dieses „cloudbasierte Scrubbing“ kann auf zwei Arten erfolgen: ***auf Abruf*** (On-demand) oder ***kontinuierlich*** (Always-on).



Darstellung eines DDoS-Angriffs auf Anwendungsschicht, der die Bereitstellung eines Diensts für legitime Nutzer verhindert

On-demand

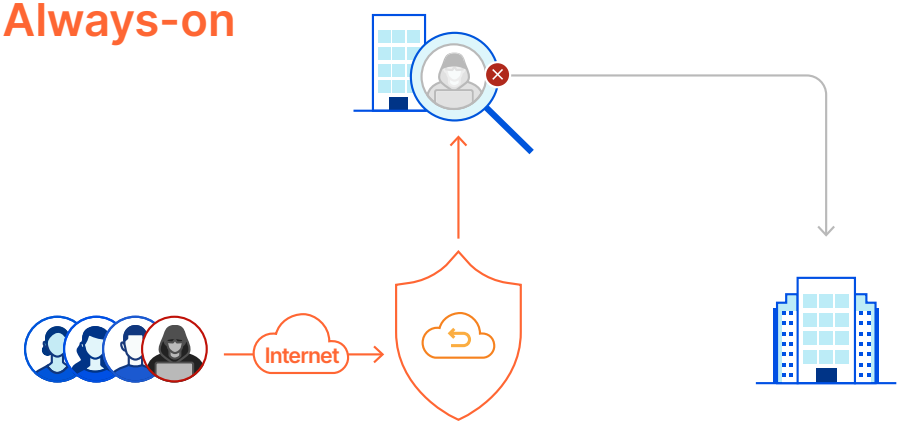


In „Friedenszeiten“ sorgt cloudasiertes On-Demand-Scrubbing dafür, dass der gesamte Datenverkehr Anwendungen und Infrastruktur ohne Umleitung erreicht. Nur bei einem laufenden DDoS-Angriff wird der Traffic zum Cloud Scrubbing-Provider umgeleitet.

Überschreitet der eingehende Datenverkehr einen vorkonfigurierten Schwellenwert (z. B. 70 % der Verbindungskapazität) oder wird ein umfangreicher Angriff festgestellt, wird der auf Abruf verfügbare Cloud-Abwehrmodus aktiviert und der Traffic zur Überprüfung an das nächstgelegene Scrubbing-Center umgeleitet.

VS.

Always-on



Bei diesem im Wesentlichen interventionsfreien Ansatz des cloudbasierten Scrubbing wird der Datenverkehr immer zur Überprüfung auf Bedrohungen über das Rechenzentrum Ihres Cloud-Anbieters geleitet – auch in „Friedenszeiten“.

Ein Always-on-Modell trägt dazu bei, die Zeit von der Erkennung bis zur Schadensbegrenzung ohne Dienstunterbrechung so kurz wie möglich zu halten.

Das On-demand- und das Always-on-Verfahren bieten zwar unterschiedliche Vorteile, können aber unter verschiedenen Umständen auch an ihre Grenzen stoßen – wie im nächsten Abschnitt beschrieben.

Wo cloudbasiertes Scrubbing häufig an seine Grenzen stößt

Herausforderungen des cloudbasierten On-demand-Scrubbing

Verzögerte Reaktion im Angriffsfall:

- Bei einem On-demand-Modell muss der Datenverkehr bei einem DDoS-Angriff an den Cloud-Anbieter umgeleitet werden, was mehrere Minuten dauern kann. Hinzu kommt die Zeit, die benötigt wird, um manuell auf den Angriff zu reagieren (also beispielsweise den Anbieter aufzufordern, die Abwehr zu aktivieren). Wird der On-demand-Schutz nicht rechtzeitig aktiviert, kann das schwerwiegende Folgen haben.

Langfristig steigende Kosten:

- Anbieter von cloudbasierter Abwehr auf Abruf rechnen oft nach Byte des Angriffstraffics ab. Als Kunde zahlt man zwar nur für das, was man tatsächlich in Anspruch nimmt, aber wenn ein Unternehmen häufiger Ziel von DDoS-Angriffen wird, könnte sich diese Option unter dem Strich als kostspieliger erweisen.

Unbemerkte Angriffe:

- DDoS-Angriffe, die die festgelegte Auslastungsschwelle nicht überschreiten, können unentdeckt bleiben und die Netzwerkverbindungen trotzdem so beanspruchen, dass der legitime Datenfluss beeinträchtigt wird.
- Netzwerkverbindungen werden auch nicht auf Angriffe auf höheren Protokollschichten auf SSL- und Anwendungsebene überwacht.

Herausforderungen bei cloudbasiertem Always-on-Scrubbing

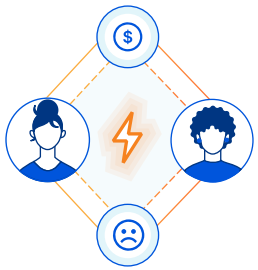
Beeinträchtigung der Nutzererfahrung durch höhere Latenz:

- Viele Anbieter von cloudbasierten DDoS-Abwehrlösungen setzen für die Bereinigung des Netzwerktraffics eine Reihe von weit von dessen Ursprungsort angesiedelten Rechenzentren ein. Eine geringere Zahl von Scrubbing-Zentren bedeutet in der Regel eine höhere Latenz. Auch die Umleitung des Traffics selbst kann Latenz und spürbarer Verzögerungen verursachen.
- Hinzu kommt, dass solche Scrubbing-Zentren häufig nur Traffic auf Netzwerkschicht überprüfen. Der Datenverkehr von Funktionen, die auf anderen Schichten angesiedelt sind, z. B. die Web Application Firewall oder das Zwischenspeichern von Inhalten, wird in der Regel in einem anderen Rechenzentrum verarbeitet, was die Latenz noch einmal erhöht.

Höhere Gesamtbetriebskosten:

- Bei dauerhaft aktiven cloudbasierten Scrubbing-Lösungen mit begrenzter Netzwerkkapazität werden die Bandbreitenbeschränkungen möglicherweise in Form von höheren Preisen an die Kunden weitergeben. Es können auch Gebühren für Fachdienstleistungen anfallen.

Zeit ist Geld: die geschäftlichen Folgen von Ausfällen und Latenz

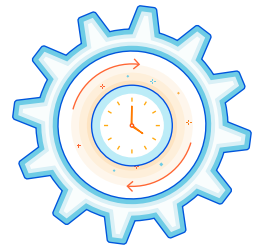


91 % der Unternehmen geben an, dass **einstündige Ausfälle** aufgrund von Geschäftseinbußen, Beeinträchtigungen der Produktivität und Abhilfemaßnahmen bis zu 300.000 US-Dollar kosten[5]

Sind bekannte E-Commerce-Unternehmen von Ausfällen betroffen, kann das mit bis zu **220.000 US-Dollar** pro Minute zu Buche schlagen[6]

90 % der Kunden verlassen eine Website, wenn sie nicht innerhalb einer aus ihrer Sicht angemessenen Zeit geladen wird, und **57 % wenden sich einem vergleichbaren Konkurrenzanbieter zu**[7]

44 % der Gamer, die von Latenz betroffen sind, **brechen deshalb ein Spiel ab**, um es später noch einmal zu versuchen; **24 % wenden sich einem anderen Spiel zu**[8]



64 % der IT-Entscheidungsträger geben an, dass die Notwendigkeit, ein schnelleres und einfacheres Kundenerlebnis zu bieten, eine **„erhebliche oder große Belastung für die technische Infrastruktur“** darstellt[9]

Das Potenzial cloudbasierter DDoS-Abwehr voll ausschöpfen und ausfallbedingte Umsatzeinbußen vermeiden

So schützt unsere Cloud-Plattform mit Unterstützung eines smarten globalen Netzwerks vor DDoS-Bedrohungen:

Cloudbasiertes On-demand-Scrubbing ist auf menschliches Eingreifen angewiesen, wodurch sich die Zeit bis zur Abwehrreaktion verlängert. Im Gegensatz dazu ist ein cloudbasierter Always-on-DDoS-Schutz umfassender. Allerdings greifen viele Anbieter solcher Lösungen auf weit entfernte Scrubbing-Zentren zurück, wodurch sich die Latenz für den Nutzer erhöht.

Cloudflare begegnet diesen Einschränkungen mit einer einheitlichen Sicherheitsplattform, die drei Ebenen des DDoS-Schutzes (Schicht 3, 4 und 7) und Datenverkehrsbeschleunigung für lokale, in der Cloud gehostete und hybride Netzwerke umfasst. Der Angriffstraffic wird in der Nähe seines Ursprungs abgewehrt, um Endnutzern hohe Performance und reibungslos funktionierende Dienste bieten zu können.

Netzwerkgestützte Sicherheit

Cloudflare verfügt über **Rechenzentren in mehr als 285 Städten** und eine **Netzwerkkapazität von 197 Tbit/s** (im Gegensatz dazu verfügt ein anderer bekannter „Always-on"-DDoS-Abwehrdienst über weniger als 40 Scrubbing-Zentren und eine Netzwerkkapazität von 20 Tbit/s).

Angriffe werden automatisch von unserem Netzwerk absorbiert, bevor sie Ihres erreichen, und der meiste bösartige Datenverkehr wird in **weniger als drei Sekunden** blockiert. Eine Umleitung von Traffic ist nicht notwendig.

Benutzerfreundlichkeit, Transparenz und Selbstständigkeit

Der DDoS-Schutz von Cloudflare wird im „as a Service"-Modell bereitgestellt, weshalb keine Investitionskosten anfallen und auch kein Hardware-Lebenszyklusmanagement erforderlich ist.

Außerdem handelt es sich um eine **in Eigenregie nutzbare Lösung** mit benutzerdefinierten Konfigurationsfunktionen, die alle in **einem einzigen Dashboard** vereint sind.

Bedrohungsdaten im passenden Maßstab

Mehr sehen, mehr schützen: Fast 20 % des Internets laufen auf Cloudflare. Unsere Kunden profitieren von der Größe unseres globalen Netzwerks, das **täglich über 112 Mrd. Cyberbedrohungen blockiert**, und den daraus gewonnenen Erkenntnissen.

Fortschrittliche Modelle maschinellen Lernens verbessern kontinuierlich unsere Abwehr, sodass wir neuen Bedrohungen immer einen Schritt voraus sind.

Branchenweit anerkannte DDoS-Abwehr

Cloudflare wurde zum **Marktführer („Leader") im GigaOm Radar Report 2022 für DDoS-Schutz** gekürt. Unter den neun verglichenen Anbietern haben wir die beste Gesamtbewertung erhalten. Cloudflare wurde auch als **„Leader" in „The Forrester Wave™: DDoS Mitigation Solutions" des ersten Quartals 2021** eingestuft.

Zudem hat Cloudflare die höchstmögliche Punktzahl in 15 Kategorien, darunter den Bereichen Security Operations Center, Reaktionsautomatisierung und Performance, erhalten.

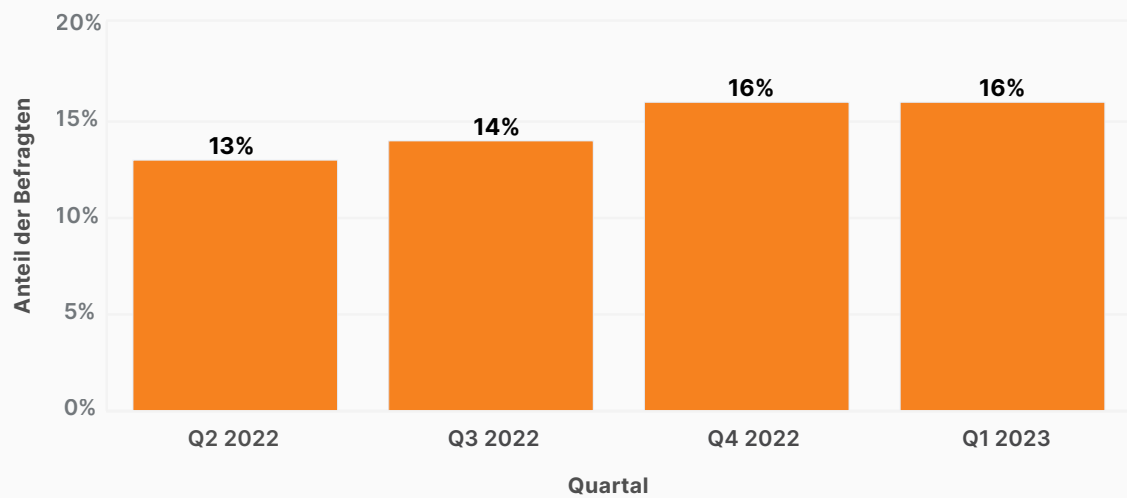
Fallstudie: Ransom-DDoS-Angriff auf ein Unternehmen der Fortune Global 500

Bei einem Ransom-DDoS (RDDoS)-Angriff, versuchen Kriminelle, Geld zu erpressen, indem sie einen Menschen oder ein Unternehmen mit einem DDoS-Angriff bedrohen. Die Zahl der Ransom-DDoS-Angriffsversuche stieg im Laufe des Jahres 2022 stetig an – und mehr als 16 % der Cloudflare-Kunden erhielten im ersten Quartal 2023 eine entsprechende Drohung oder Lösegeldforderung im Rahmen eines DDoS-Angriffs.

Ransom-DDoS-Angriffe werden zwar oft mit Ransomware-Angriffen verwechselt, doch sie funktionieren anders und sind einfacher auszuführen: Sie erfordern weder, dass das Opfer durch einen Trick dazu gebracht wird, eine E-Mail zu öffnen oder auf einen Link zu klicken, noch dass in das Netzwerk eingedrungen wird oder dass ein Zugang zu Firmenressourcen besteht. Die zunehmende Verfügbarkeit von Ransomware as a Service hat Ransom-DDoS zu einer aufwands- und risikoarmen Option für Angreifer gemacht.

Ransom-DDoS-Angriffe und -Bedrohungen aufgeschlüsselt nach Quartal

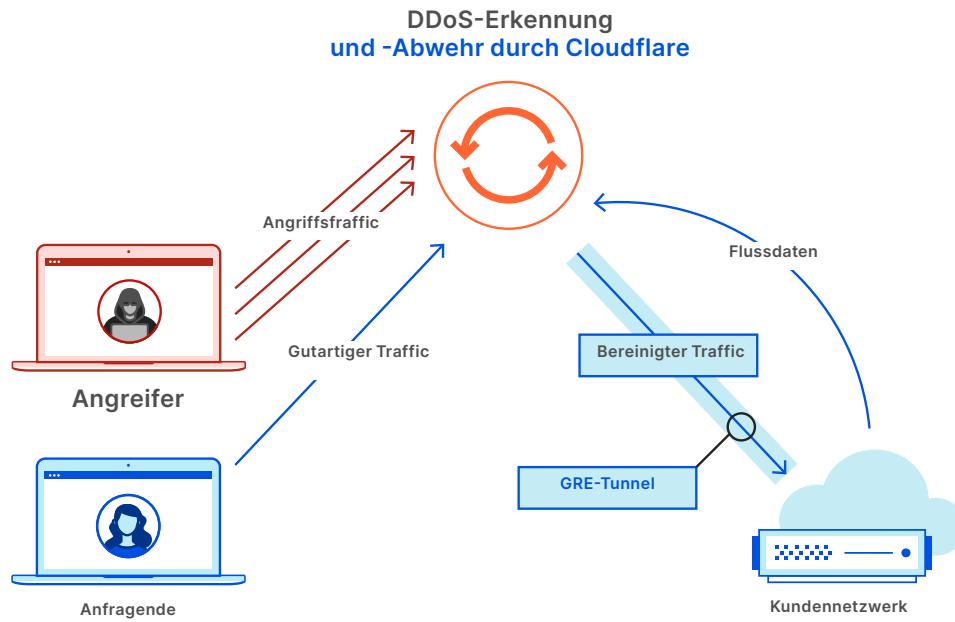
Anteil der Befragten, die nach eigenen Angaben von einem Ransom-DDoS-Angriff betroffen oder bedroht waren



Ende 2020, bevor Cloudflare für die DDoS-Abwehr eingesetzt wurde, war ein großes Unternehmen der Fortune Global 500 Ziel eines RDDoS-Angriffs von Kriminellen, die behaupteten, die Lazarus Group zu sein (eine Cybercrime-Gruppe, die angeblich von der nordkoreanischen Regierung geleitet wird). Die Angreifer schickten zunächst eine E-Mail, in der sie Bitcoin forderten und der Firma eine Woche Zeit gaben, um zu zahlen. Andernfalls, so hieß es, würde ein zweiter größerer Angriff erfolgen und das Lösegeld würde steigen.

Nachdem das Unternehmen die Lösegeldforderung erhalten und einen erheblichen Anstieg des Datenverkehrs in einem seiner internationalen Rechenzentren registriert hatte, wandte es sich an seinen Anbieter von auf Abruf verfügbaren Scrubbing-Zentren. Es dauerte über 30 Minuten, bis der Dienst des Anbieters aktiviert und der Datenverkehr an das Scrubbing-Center umgeleitet wurde. Die Aktivierung des On-demand-Dienstes verursachte außerdem Netzwerkausfälle und führte zu mehreren Zwischenfällen.

Nach dem ersten Angriff und den Problemen mit dem On-demand-Anbieter entschied sich das Unternehmen für Cloudflare Magic Transit, den rund um die Uhr aktiven Cloudflare-Schutz vor DDoS-Angriffen auf Netzwerkschicht. Obwohl die Angreifer einen zweiten, großen Angriff in Aussicht gestellt hatten, kam es nie dazu.



Cloudflare Magic Transit für DDoS-Schutz auf Netzwerkschicht

„Einer der wichtigsten Unterschiede ist die Analyse der Angriffe und des Traffics, die uns unser bisheriger Anbieter nicht bieten konnte. Wir stellen fest, dass Angriffe, von denen wir gar nichts wissen, automatisch abgewehrt werden."

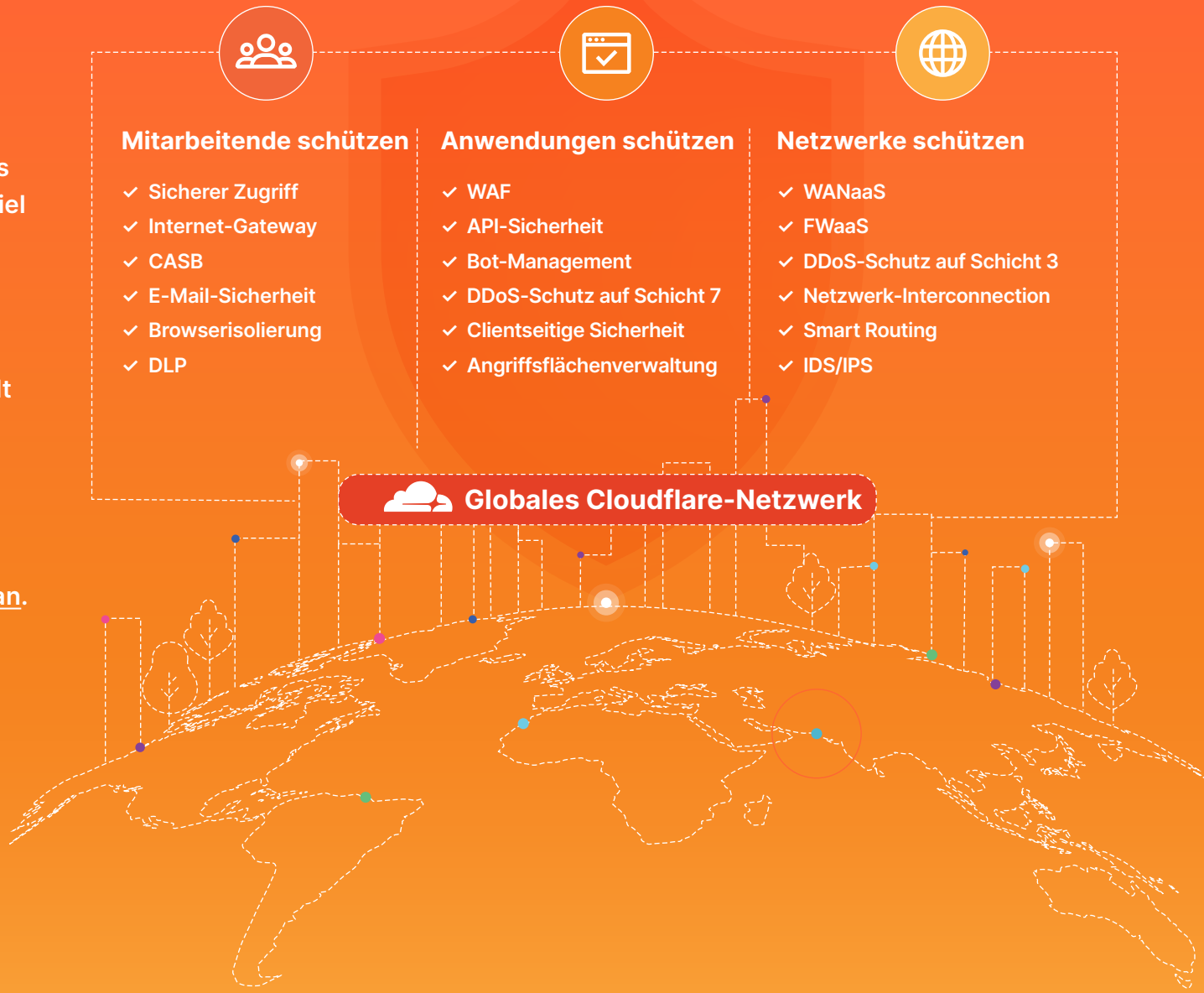
Incident Response- und Forensics-Team
eines Fortune Global 500-Unternehmens

Fazit

DDoS-Angriffe treten seit der Pandemie immer häufiger auf und nehmen an Komplexität zu. Umso wichtiger ist es, dass der legitime Datenverkehr weiterhin sein Ziel erreicht, damit Sie keine Gewinneinbußen verzeichnen. Dank unserer Fähigkeiten, Angriffe schnell und mühelos abzuwehren und dabei die Latenzprobleme und hohen Kosten anderer Anbieter zu vermeiden, fällt mit Cloudflare die Entscheidung für einen cloudbasierten Always-on-Ansatz leicht.

Wenn Sie mehr über den Schutz vor Netzwerk-DDoS-Angriffen mit Cloudflare erfahren möchten, fordern Sie eine Demo an.

Wenn Sie mehr über ein einziges globales Netzwerk mit integrierter Zero Trust-Funktionalität, DDoS-Abwehr, Netzwerk-Firewalling und Trafficbeschleunigung erfahren möchten, klicken Sie hier.



Quellen

1 Langrock, Sam. „The Cloud has Complicated Attack Surface Management.“ Recorded Future, 3. April 2023, https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management

2 „Uptime Institute’s 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short.“ Uptime Institute, 8. Juni 2022, https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Cimpanu, Catalin. „Bandwidth.com expects to lose up to $12M following DDoS extortion attempt.“ The Record, 1. November 2021, https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 Holmes, David and Blankenship, Joseph, et al. „The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021,“ Forrester, 3. März 2021

5 Didio, Laura. „The Cost of Enterprise Downtime,“ TechChannel, 30. September 2021. https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6 „The Cost of Downtime for the Top US Ecommerce Sites“, Gremlin, letzter Zugriff am 8. Mai 2023, https://www.gremlin.com/ecommerce-cost-of-downtime

7 Crets, Stephanie. „Most consumers abandon a slow-loading ecommerce site.“ DigitalCommerce360, 21. August 2020. https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Duperre, Mathieu. „44 percent of gamers respond to latency by quitting their games — what can we do to stop this?“ PocketGamer.biz, 24. Oktober 2022, https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9 „Infinity Data and the battle to conquer latency.“ Hazelcast and Intel, November 2019. https://hazelcast.com/resources/infinity-data-report

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

CLOUDFLARE