CLOUDFLARE®

# Lassen Sie sich nicht abhängen.

## Verbesserung der Performance Ihrer E-Commerce-Site und der Sicherheit für Mobilverbraucher

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

## Kurzfassung

Die Mobilnutzung steht kurz davor, zum wichtigsten Kanal bei E-Commerce-Strategien zu werden. 25 % der größten Einzelhändler in den USA wissen bereits, wie sie Mobil-Conversion-Rates in einem Wettkampf um alles oder nichts erhöhen können, sodass sie einen überproportionalen Teil des ansprechbaren Marktes ausmachen. Sie erhöhen die Kundentreue und erzeugen Produktklicks, indem sie schnelle und verfügbare Mobilsites und -apps bereitstellen. Cloudflare kann Sie bei der Erfüllung dieser wichtigen Anforderungen unterstützen durch:

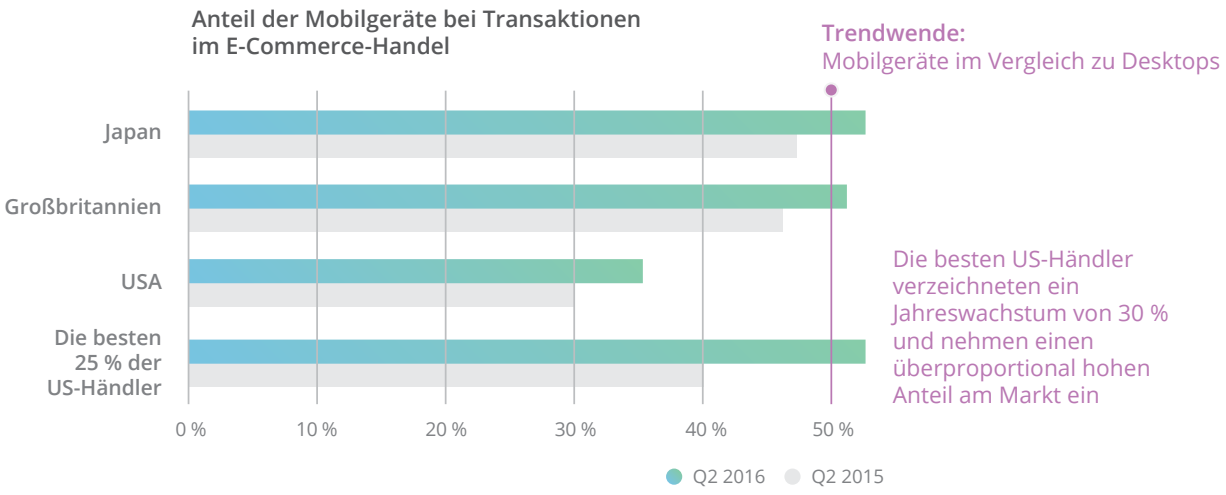
- eines der schnellsten Content Delivery Networks auf Basis von Anycast-Routing und der Möglichkeit, Inhalte zur Latenzreduzierung physisch in der Nähe der Kunden zwischenzuspeichern
- vorhersehbare und durchsichtige Preise
- Mobilbild- und -codeoptimierung sowie Support für IPv6 zur Latenzreduzierung für Mobilgeräte
- Schutz gegen DDoS-Angriffe auf die Schichten 3, 4 und 7 und gegen Anwendungsschwachstellen in Schicht 7 für erhöhte Verfügbarkeit
- richtige Verschlüsselung mit hoher Performance

Das Einrichten von Cloudflare zum Zugriff auf diese Funktionen ist für E-Commerce-Anbieter ein entscheidender Schritt, damit ihre Sites das ganze Jahr über schnell funktionieren und geschützt sind.

## M-Commerce steht kurz vor dem Durchbruch.

E-Commerce ist aufregend: Mit einem Wachstum von 14,6 % für 2015 im Jahresvergleich und einem Anteil von sage und schreibe 36,2 % am Einzelhandelswachstum 2015 in den USA hat es das konventionelle Geschäft weit übertroffen. Aber M-Commerce (das mobile Geschäft) ist noch aufregender, denn es wächst sogar noch mehr und steht kurz vor dem Durchbruch: Im 2. Quartal 2016 lag der Anteil von M-Commerce-Einzelhandelstransaktionen in Japan und dem Vereinigten Königreich zum ersten Mal bei über 50 % und übertraf damit Desktoptransaktionen. In den USA wächst der mobile Anteil an E-Commerce-Transaktionen mit atemberaubenden 17 % im Jahresvergleich. Zwar hinkt der mobile Anteil an E-Commerce-Transaktionen in den USA mit 35 % noch etwas hinterher, doch wird er sicher bald auch hier mit dem Wert der führenden Länder aufholen.

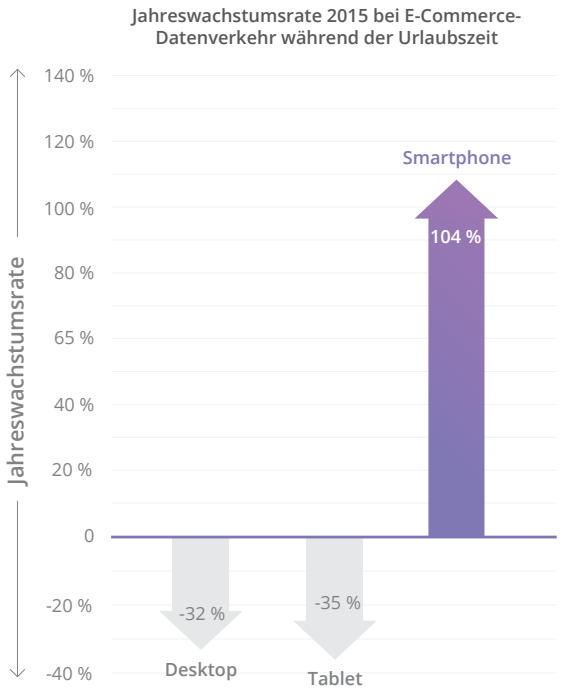
Das führende Viertel der Einzelhändler in den USA macht sich diesen Trend bereits zunutze und bietet die besten Mobilsites und -apps. So steigern diese Unternehmen die Kundentreue und erzeugen Produktklicks, um Conversion-Rates im Vergleich zu durchschnittlichen neuen Einzelhändlern um bis zu 90 % zu steigern. Das Resultat ist ein überproportionaler Anteil des Mobilgewinns – 52 % ihres E-Commerce-Vertriebs werden über Mobilnutzung erzeugt, die im Jahresvergleich mit atemberaubenden 30 % zunimmt.

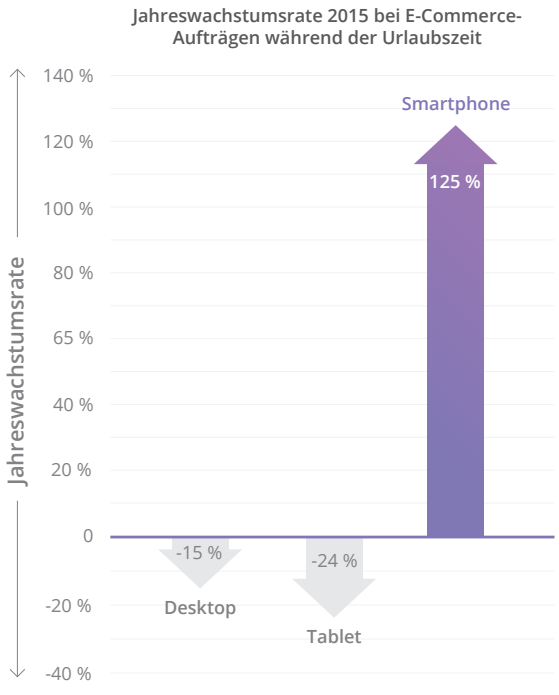


Es besteht also kein Zweifel: M-Commerce hat sich bereits zu einem wichtigen Vertriebs- und Marketingkanal entwickelt. Die Einzelhändler mit dem besten Mobilerlebnis sind die deutlichen Sieger und werden auch weiterhin einen bevorzugten Stellenwert im verfügbaren Markt einnehmen.

## Mobilnutzung ist im Festtagsgeschäft von höchster Bedeutung.

Das Online-Shopping zu den Festtagen (Cyber 5) brach 2015 alle Rekorde. Cyber Monday war der Tag mit den meisten Online-Ausgaben aller Zeiten in den USA. Dabei spielten Smartphones eine überaus wichtige Rolle – 49 % des Verkehrs lief über sie und 27 % der Bestellungen wurden über sie aufgegeben. Smartphoneverkehr und Bestellungen darüber nahmen rapide zu, während Desktop- sowie Tabletverkehr und Bestellungen darüber entsprechend abnahmen.

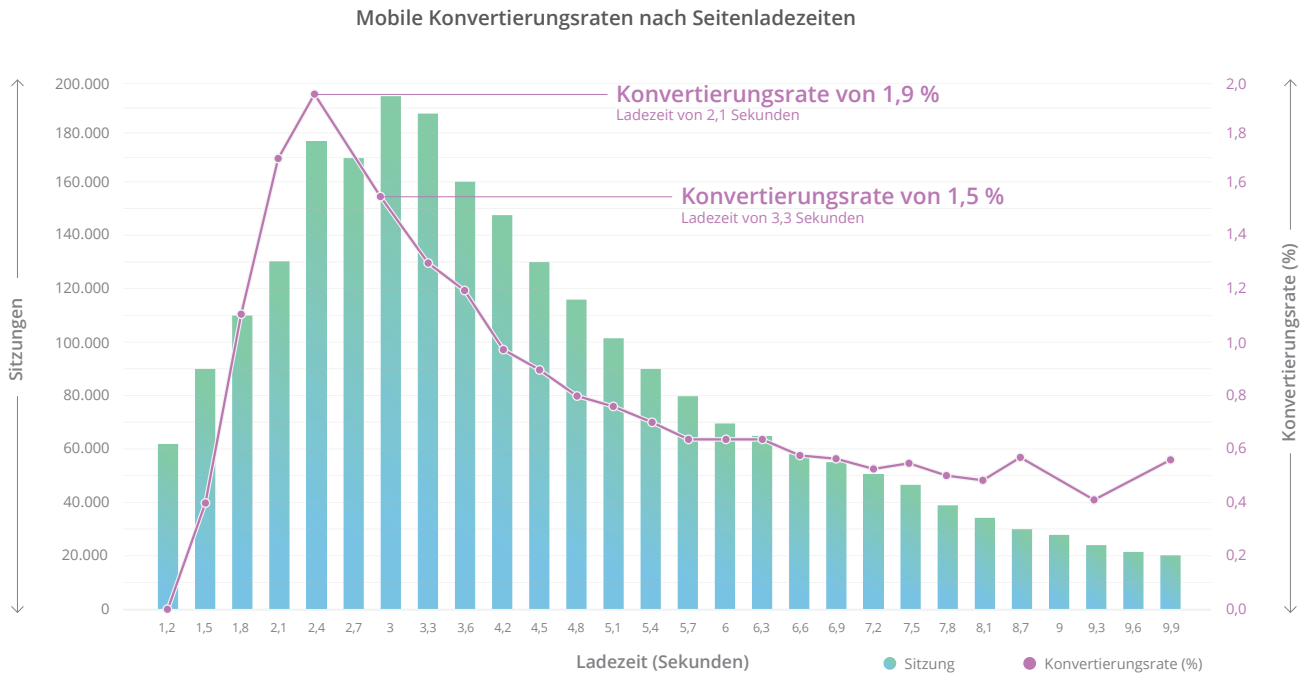



Die Shoppingperiode Cyber 5 2015 zeigte erneut, dass die Einzelhändler mit dem besten Mobilerlebnis die Preise abräumen. Beispielsweise wuchs Amazon während Cyber 5 2015 um 24,1 % gegenüber derselben Periode 2014. Während der bevorstehenden Festtage werden Einzelhändler, die sowohl über physische Standorte als auch einen Online-Shop verfügen, wahrscheinlich einen höheren Online-Verkehr als Besuche im Geschäft verzeichnen. Damit ist das Mobilshoppingerlebnis für das Wachstum unabdingbar.

## Der Einfluss von Latenz und Verfügbarkeit auf Conversion-Rates

Wodurch heben sich führende E-Commerce-Einzelhändler von anderen ab? Sie bieten die besten Mobilsites und -apps, um ihre Conversion-Rates zu steigern. Die Mobil-Conversion-Rates sind noch immer niedrig und stehen in direkter Verbindung mit Performance und Verfügbarkeit der Mobilsite/-app. Beispielsweise erreichte die Conversion-Rate für einen führenden Online-Einzelhändler mit einer durchschnittlichen Seitenladezeit von 2,4 Sekunden ihren höchsten Wert bei 1,9 %. Bei einer Seitenladezeit von 3,3 Sekunden, die nur etwa 1 Sekunde länger ist, sank die Conversion-Rate um 27 %.

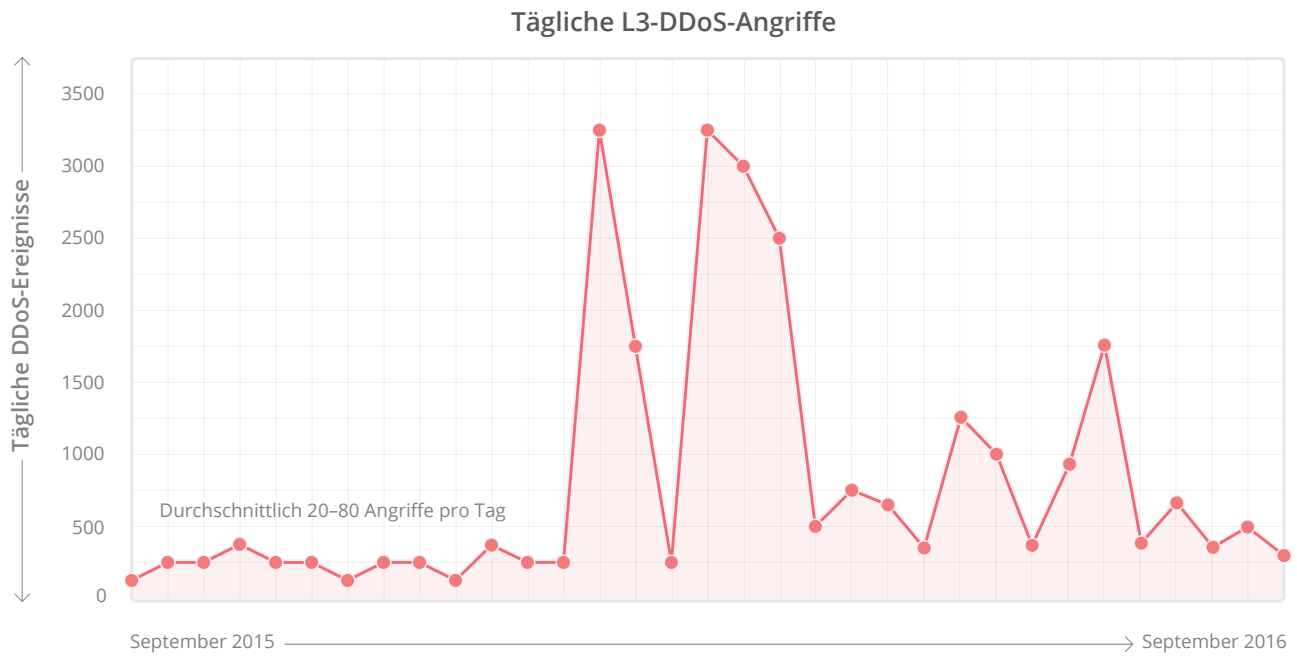



Viele Beispiele aus der Branche verdeutlichen den Zusammenhang zwischen Siteperformance und Conversion-Rate.

- Amazon erhöhte den Umsatz um 1 % pro 100 ms geringerer Sitelatenz.
- Yahoo erhöhte den Verkehr um 9 % pro 400 ms geringerer Sitelatenz.
- Die Conversion-Rates bei Walmart fielen deutlich beim Anstieg der Siteladezeit von 1 auf 4 Sekunden.

Generell berichtet Google, dass eine Site von 100 bis 400 Millisekunden einen messbaren Einfluss auf das Kundenverhalten hat und eine Site, die um 250 Millisekunden langsamer ist als die der Konkurrenz, weniger häufig besucht wird.

Zusätzlich zur Latenz durch die Sites/Apps selbst können Distributed Denial-of-Service(DDoS)-Angriffe dafür sorgen, dass die Site vollkommen ausfällt. Durch die Netzwerke von Cloudflare fließen fast 10 % des internationalen Internetverkehrs, so können wir Angriffe herausfiltern und genau messen. Im letzten Jahr stellte Cloudflare fest, dass die Anzahl und Intensität der Angriffe mit bis zu 1.400 DDoS-Angriffen täglich zunahm – insgesamt 400 Gbit/s an eingehendem Verkehr und Angriffe mit 200 Mio. Paketen pro Sekunde.




Angriffe finden normalerweise nicht nur einmal statt und die Opfer werden in der Regel mehrmals pro Jahr angegriffen. Erfahrungen von Cloudflare zeigen, dass diesen Angriffen jeder zum Opfer fallen kann – sowohl große als auch kleine Unternehmen. Unter vielen Rechtsprechungen sind DDoS-Angriffe zwar illegal, dennoch gibt es DDoS-as-a-Service-Anbieter, die Abonnements teilweise schon ab 5 oder 10 US-Dollar pro Monat anbieten.

Sogar die Website von Amazon (99 Milliarden US-Dollar Einzelhandelsumsatz 2015) war in der Vergangenheit mehrere Male aus unbekannten Gründen nicht verfügbar. Beispielsweise fiel Amazon.com 2013 für geschätzte 15–45 Minuten aus, was das Unternehmen 1,8–5,3 Millionen US-Dollar an verlorenen Abschlüssen kostete, wenn wir von den 117.882 US-Dollar pro Minute an durchschnittlichen Abschlüssen des Unternehmens ausgehen. Die durch Ausfälle verursachten Kosten für E-Commerce-Anbieter sind während der Festtage ggf. sogar noch höher – denn 33 % des Jahresumsatzes von Amazon wurden im vierten Quartal 2015 verzeichnet. Das liegt an der Saisonabhängigkeit des Geschäfts. Weitere negative Auswirkungen von Systemausfällen sind die Beeinflussung der Kundenzufriedenheit, des Rankings bei Suchmaschinen und der Investorbeziehungen.

Insgesamt ist es für E-Commerce-Anbieter, die ihre Conversion-Rates speziell während der Festtage erhöhen möchten, ausschlaggebend, interessante Sites/Apps bereitzustellen, die gegen DDoS-Angriffe geschützt sind, um so die Verfügbarkeit zu gewährleisten.

## Essenzielle Technologien für schnelle und sichere Mobilsites

Mit Cloudflare können Sie Ihre M-Commerce-Sites und -Apps ohne zusätzliche Hardware, Installation von Software oder Änderung auch nur einer Zeile Ihres Codes beschleunigen und schützen.

Der erste Schritt ist die Verwendung des Content Delivery Network (CDN) von Cloudflare, eines der weltweit größten Netzwerke mit über 10 Billionen Anforderungen pro Monat – das entspricht fast 10 % aller Internetanforderungen für über 2,5 Milliarden Benutzer auf der ganzen Welt. Das CDN von Cloudflare wird laut Cedexis immer wieder als eines der schnellsten CDN mit Median-Reaktionszeiten von 34 ms (in den USA) eingestuft. Einige der wichtigsten Funktionen sind:

### Anycast-basiertes Routing

Das Cloudflare-CDN verwendet ein Routingschema namens Anycast, während der Großteil des Internets noch immer mit einem Mechanismus namens Unicast funktioniert. Bei Unicast wird jedem Knoten im Netzwerk eine einzigartige IP-Adresse zugewiesen. Router erstellen eine Karte der weltweiten IP-Adressen und damit einen Überblick über die kürzesten Pfade zwischen den verschiedenen Hops zum letztendlichen Ziel. Dieses liegt aber unter Umständen am anderen Ende des Kontinents oder irgendwo sonst auf der Welt, wodurch zusätzliche Hops erforderlich werden, die wiederum die Latenz erhöhen. Mit Anycast, dem von Cloudflare verwendeten Routingschema, erhalten mehrere Geräte im CDN dieselbe IP-Adresse. So können Router Anforderungen direkt an den physisch nächsten Server senden und die Latenz verringern.

### Zwischenspeicherung von Inhalten

Das Cloudflare Anycast-Netzwerk funktioniert gemeinsam mit der Zwischenspeicherung von Inhalten. Nachdem eine Anforderung von Anycast an den physisch nächsten Server geleitet wurde, steht eine Kopie der zwischengespeicherten Inhalte auf dem Server zum Zugriff bereit. Der Vorteil dieses Verfahrens ist, dass Objekte näher an den anfordernden Besuchern liegen, sodass die Bereitstellung beschleunigt und das Laden am Ursprungswebserver verringert wird. Cloudflare bietet Funktionen zum automatischen Zwischenspeichern statischer Inhalte und mit Railgun auch einen Mechanismus zum Zwischenspeichern dynamischer Inhalte.

Cloudflare analysiert den Verkehr, der wieder durch die Server im CDN geleitet wird, um so die statischen Bereiche der Ursprungssite zu finden. Diese werden dann für kurze Zeit im CDN zwischengespeichert. In der Regel können 66 % der Webinhalte (durch das „automatische Zwischenspeichern statischer Inhalte“) zwischengespeichert werden, die übrigen 34 % allerdings nicht – sie müssen vom Ursprungswebserver abgerufen werden. Railgun wurde entwickelt, um die Bereitstellung von Inhalten, die nicht zwischengespeichert werden können, zu beschleunigen, sodass sozusagen das gesamte Web zwischengespeichert werden kann. Dabei wird erkannt, dass Webseiten, für die keine Zwischenspeicherung möglich ist, sich nicht sonderlich schnell ändern und die geringfügigen Abweichungen zwischen den Versionen der Webseiten von den Cloudflare-CDN-Servern identifiziert werden können. Cloudflare komprimiert die Änderungen dann mit einer Rate von bis zu 99,6 % und sendet sie über die Verbindung. So wird die Performance um bis zu 700 % verbessert. Für die Verwendung von Railgun ist die Installation einer Softwarekomponente auf dem Ursprungsserver erforderlich.

> „Die Kosten für Bandbreite nehmen immer mehr zu. Da ist die Verwendung eines CDN wie dem von Cloudflare zur Bereitstellung von Bildern für Benutzer am Edge sowohl kosteneffektiv als auch dazu geeignet, die Latenz für unsere mobilen Kunden zu verringern.“
>
> Chris Smith, Director of E-Commerce bei Big 5 Sporting Goods

### Pauschalpreise

Um Teil des Internets sein zu können, kauft Cloudflare Bandbreite, auch als Transit bekannt, von einer Reihe verschiedener Anbieter. Cloudflare kauft Transit pauschal auf Basis der in einem bestimmten Monat verwendeten Kapazität und zahlt dabei für einen bestimmten Zeitraum für die maximale Auslastung. Der von Cloudflare gezahlte Tarif schwankt in verschiedenen Regionen auf der Welt zwar stark, aber zum Zwecke der einfachen Preisgestaltung berechnet Cloudflare Kunden einen Pauschalpreis, unabhängig davon, in welchen Teil der Erde der Verkehr geleitet wird. Anders als bei einigen Cloudservices, die nach einzelnen Bits abrechnen, die über ein Netzwerk gesendet werden, sind die monatlichen Rechnungen von Cloudflare vorhersehbar. Cloudflare arbeitet auch weiterhin an der Reduzierung von Transitpreisen und der Erhöhung von Peering, um den besten Service zum niedrigsten Preis bieten zu können.

## Optimierung von Bildern und Code

Mit Polish, Mirage und Auto-Minify bietet Cloudflare ein Dreierteam zur Latenzreduzierung. Diese Funktionen sind vor allem bei Mobilgeräten ausschlaggebend, auf denen eine begrenzte Bandbreite zur Verfügung steht.

Polish beseitigt Metadaten und komprimiert Bilder zur Reduzierung ihrer Größe. Es kann im verlustfreien Modus ausgeführt werden, in dem unnötige Größe durch Bildüberschriften und Metadaten ohne Verlust tatsächlicher Bilddaten entfernt wird. Dabei werden die Dateien durchschnittlich um 21 % verkleinert. Im verlustbehafteten Modus wendet Polish zusätzlich zu den Verfahren des verlustfreien Modus einen Komprimierungsalgorithmus auf bestimmte Bilder an. Die Bilder werden ohne wahrnehmbare visuelle Unterschiede genau so angezeigt wie vorher auch, aber die Dateigröße ist durchschnittlich um 48 % geringer. Bilder machen bei den Daten einer typischen Website über 50 % aus.

Mirage verwaltet die Art, auf die Bilder auf Mobilgeräten geladen werden. Dabei wird schnell die Erscheinung einer vollständigen Seite angezeigt, sodass Benutzer sofort mit ihr interagieren können, und nach und nach der Rest der Seite im Hintergrund gefüllt, ohne das Benutzererlebnis zu stören.

- Mirage verwendet Lazy Loading zur Priorisierung der Ladeabfolge von Bildern, die im sichtbaren Bereich liegen, also tatsächlich vom Browser angezeigt werden. Dann werden die anderen Bilder auf der Seite geladen, die vom Browser nicht angezeigt werden – je nach Bedarf oder freien Netzwerkressourcen.
- Für Mobilgeräte sind aufgrund der geringeren Bildschirmgröße kleinere Bilder erforderlich. Mirage verringert die Größe eines Bildes auf dem Server in der Regel auf bis zu 1 % der vollständigen Auflösung und sendet zuerst das verkleinerte Bild. Nach dem Rendern der Seite mit den verkleinerten Bildern werden diese mit den Versionen in vollständiger Auflösung ersetzt. Bilder werden zunächst mit geringer Auflösung angezeigt und dann scharf.
- Anstatt eine neue Anforderung für jedes Bild zu initiieren, werden Bilder mit nur einer Anforderung vom Cloudflare-Netzwerk geladen. Sogar Seiten mit Hunderten von Bildern können mit gerade einmal zwei Anforderungen im Browser gerendert werden. Auch Benutzer mit schlechten Mobilverbindungen können so sofort mit der Seite interagieren und müssen nicht erst darauf warten, dass die vollständigen Bilder geladen werden.

Durch Auto Minify werden schnell alle unnötigen Zeichen wie Leerräume aus HTML-, JavaScript- und CSS-Dateien entfernt, wodurch Dateien um 20 % verkleinert werden können, ohne die Funktionalität zu beeinträchtigen. Die Auto Minify-Implementierung von Cloudflare ist mit Leichtigkeit 100-mal schneller als der ähnlichste Ansatz.

## Support für IPv6

Durch Real User Monitoring-Messungen von Facebook und LinkedIn wurde festgestellt, dass bei den 4 größten Mobilnetzwerken in den USA die Ladezeiten von Mobilseiten über IPv6 um gut mehr als 10 % kürzer sind als über IPv4. Während sich die Einführung von IPv6 über mehrere Jahrzehnte erstreckt und die allgemeine Auffassung herrscht, dass es nur langsam geht, verlaufen 60 % der Android- und über 20 % der iPhone-Anforderungen bei den 4 größten Mobilnetzwerken der USA über IPv6 auf zweischichtigen Sites (Stand: 05.04.2016). Cloudflare bietet bereits seit 2012 vollständigen IPv6-Support sowie ein IPv6-auf-IPv4-Gateway und stellt Kunden diesen Service mit „nur einem Klick“ zur Verfügung. Unterstützt der Ursprungsserver IPv6, findet für Besucher mit IPv6-Verbindung über das Protokoll eine End-to-End-Weiterleitung statt. Wenn der Ursprungsserver nur IPv4 unterstützt, nimmt Cloudflare den Besucher über IPv6 auf und stellt dann nahtlos eine Anforderung über IPv4 an den Server. Bei festen Anforderungen von Anwendungen nach IPv4, die auf dem Ursprungsserver ausgeführt werden, bietet Cloudflare außerdem Pseudo-IPv4. Durch diese Option werden Anforderungen mit einer „Pseudo“-IPv4-Adresse bei Verbindungen, die über IPv6 hergestellt werden, HTTP-Überschriften hinzugefügt.

### DDoS-Schutz für Schichten 3 und 4 – Anycast-Netzwerkstabilität mit automatischer Lernplattform

Zusätzlich zum Content Delivery Network (CDN) von Cloudflare ist der nächste Schritt zum Schutz von Sites/Apps vor Angriffen das Sicherstellen der Verfügbarkeit. Der fortschrittliche Cloudflare-DDoS-Schutz wird als Service am Netzwerk-Edge bereitgestellt, entspricht dem Entwicklungsstand sowie dem Ausmaß der Bedrohungen und kann zur Abwehr von DDoS-Angriffen aller Arten und Größen verwendet werden. Cloudflare verhinderte bereits viele der größten DDoS-Angriffe mit teilweise mehr als 400 Gbit/s.

DDoS-Angriffe auf die Schichten 3 und 4 sind in der Regel volumetrische Angriffe wie DDoS-Verstärkung, DDoS-Überflutung und DDoS-SYN-Überflutung. Diese können ein typisches Unicast-basiertes Netzwerk überfordern, doch das Anycast-basierte Netzwerk von Cloudflare vergrößert automatisch die Oberfläche, indem der Angriffsverkehr zur schlichten Absorption auf alle 100 Cloudflare-Rechenzentren und ein vielseitiges Set aus Verbindungen mit hoher Bandbreite zu anderen Netzwerken verteilt wird. Außerdem bietet Cloudflare eine automatische Lernplattform, auf der der Netzwerkverkehr in Echtzeit analysiert wird, um anomale oder schädliche Anforderung zu erkennen. Sobald ein neuer Angriff identifiziert wird, sperrt Cloudflare diese Angriffsart automatisch sowohl für die entsprechende Website als auch für die gesamte Community.

Selbst aus der Kostenperspektive beeinflussen Angriffe Cloudflare in der Regel nicht: Cloudflare kauft pauschal beachtliche Mengen an Bandbreite und bezahlt den höheren Betrag an eingehendem bzw. ausgehendem durchschnittlichen Verkehr über einen Monat hinweg. Cloudflare fungiert als Proxy zur Zwischenspeicherung, daher ist der ausgehende Verkehr unter normalen Umständen größer als der eingehende, in der Regel beträgt er etwa das 4- bis 5-Fache. Bei einem Angriff nähern sich diese Zahlen einander etwas an, aber ein Angriff ist so gut wie nie groß genug, um die Gesamtkosten von Cloudflare für Bandbreite zu erhöhen. Diesen Vorteil gibt Cloudflare auch an die Kunden weiter, denen durch einen erhöhten Netzwerkverkehr bei einem DDoS-Angriff keine zusätzlichen Kosten entstehen.

Das Cloudflare-Netzwerk sowie die Community wachsen stetig und so wird es immer schwieriger, effektive DDoS-Angriffe auf Cloudflare-Benutzer durchzuführen.

### DDoS-Schutz für Schicht 7 – Ratenbegrenzung mit IP-Reputation-Datenbank

Wie bei volumetrischen Angriffen auf die Schichten 3 und 4 auch, wird bei DoS-Angriffen auf Schicht 7 ein hohes Anforderungsvolumen verwendet, sodass tatsächliche Benutzer nicht auf eine Website zugreifen können. Bei DoS-Angriffen auf Schicht 7 werden viele Anforderungen, die dem Muster von normalem, nicht schädlichem Verkehr entsprechen, von einer IP-Adresse aus gesendet und sind somit schwer abzuwehren.

Der Traffic Protector von Cloudflare – im Moment über ein Early Access-Programm verfügbar – überwacht die Anzahl der Anforderungen an eine Site von jeder IP-Adresse und identifiziert Sites, von denen pro Minute übermäßig viele Anforderungen ausgehen. Sobald eine verdächtige IP-Adresse erkannt wurde, wird der Verkehr von dieser etwa 5 Sekunden lang über eine Zwischenseite geleitet, um einige mathematische Herausforderungen zu bearbeiten. Schlägt dieser Vorgang für die Anforderung fehl, wird die IP-Reputation durch den Traffic Protector herabgestuft und für Verkehr von dieser Adresse wird bei jedem Zugriffsversuch eine CAPTCHA-Seite angezeigt.

Erkennt Cloudflare eine IP-Adresse, die scheinbar schädliche Anforderungen sendet, wird diese in der IP-Reputation-Datenbank von Cloudflare gespeichert. Je nach Bedrohungseinstufung gehen Anforderungen entweder durch oder es wird ein CAPTCHA angezeigt. Schlägt dieses fehl und wird die IP-Adresse als schädlich identifiziert, wird die Anforderung am Cloudflare-Edge für das gesamte Netzwerk abgewehrt, sodass die gesamte Cloudflare-Community davon profitiert.

### Angriffe auf Nicht-DDoS-Schwachstellen in Schicht 7 – Web Application Firewall

Angriffe auf die Anwendungsschicht (Schicht 7) sind die komplexeste Art von Angriffen und hochentwickelt. Sie ahmen die gewöhnliche Nutzung einer Anwendung nach und umgehen so die meisten Schutzvorrichtungen gegen DDoS-Angriffe sowie Sicherheitsservices für Schwachstellen. Typisch dafür sind unter anderem SQL-Einschleusung und Cross-Site-Scripting (XSS). Dabei können Angreifer unter Umständen auf Kunden- oder andere Anwendungsdaten zugreifen und diese manipulieren.

Diese Bedrohungen wehrt Cloudflare mithilfe der Web Application Firewall (WAF) ab. Durch sie werden der OWASP-Grundregelsatz, einsatzbereite Regeln von Cloudflare und benutzerspezifische Regeln implementiert, die von der Community bzw. von Kunden erstellt wurden. Neue Regeln von Cloudflare werden innerhalb von nur 30 Sekunden auf alle Cloudflare-Serverknoten propagiert und durch die WAF selbst entsteht eine zusätzliche Latenz von unter 1 ms pro Anforderung für Sicherheit ohne Abstriche bei der Performance. So schützt Cloudflare Kunden vor Zero-Day-Schwachstellen wie Shellshock und dem Heartbleed-Bug.

„Wir nehmen die Beeinträchtigung durch DDoS-Angriffe sehr ernst. Sogar in Fällen, in denen unsere Domäne einem DDoS-Angriff ausgesetzt war, konnte Cloudflare uns schnell schützen, um unseren Kunden ein herausragendes Erlebnis zu bieten. Der größte Vorteil von Cloudflare ist, dass wir vollkommen beruhigt sein können, da das Netzwerk überwacht wird und es eine Möglichkeit gibt, Angriffe abzuwehren."

Chris Smith, Director of E-Commerce bei Big 5 Sporting Goods

### TLS 1.3 und HTTP/2 mit Server-Push

Verschlüsselung ist für ein vertrauensvolles Shoppingerlebnis ausschlaggebend und mit den aktuellen SSL-Verbesserungen kann sie richtig eingesetzt werden sowie die Performance optimieren. Durch Transport Layer Security 1.3 (TLS) werden nicht sichere Funktionen früherer TLS-Versionen beseitigt und die Latenz reduziert, indem der Protokollumweg halbiert wird. Cloudflare stellte TLS 1.3 als erstes Unternehmen bereit und hat stark zu diesem Standard beigetragen. Auch bei der Bereitstellung von HTTP/2, das nur mit TLS funktioniert, stand Cloudflare an erster Stelle. HTTP/2 trägt zu einer höheren Performance bei, speziell bezüglich der Latenz, die von Endbenutzern bei Verwendung eines Browsers wahrgenommen wird. HTTP/2 funktioniert gemeinsam mit Server-Push. Dabei kann ein Server Ressourcen senden, die vom Client noch nicht angefordert wurden, um die Performance für Endbenutzer noch weiter zu verbessern. TLS 1.3 und HTTP/2 mit Server-Push sind nur zwei der Beispiele für die Arbeit von Cloudflare daran, ständig neue Technologien in das Netzwerk zu integrieren.

### Kernpunkte

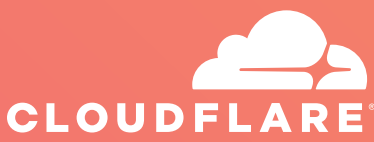
Melden Sie sich bei Cloudflare an und verbessern Sie so die Performance Ihrer Mobilsite und -apps, während sie gleichzeitig vor DDoS-Angriffen und Anwendungsschwachstellen geschützt werden. Die Einrichtung ist ganz einfach und dauert in der Regel weniger als 5 Minuten. Die Tarife – von kostenfrei bis Enterprise – finden Sie unter www.cloudflare.com.

## Wenn Sie weitere Informationen zu Cloudflare wünschen, nehmen Sie Kontakt mit uns auf:

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



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