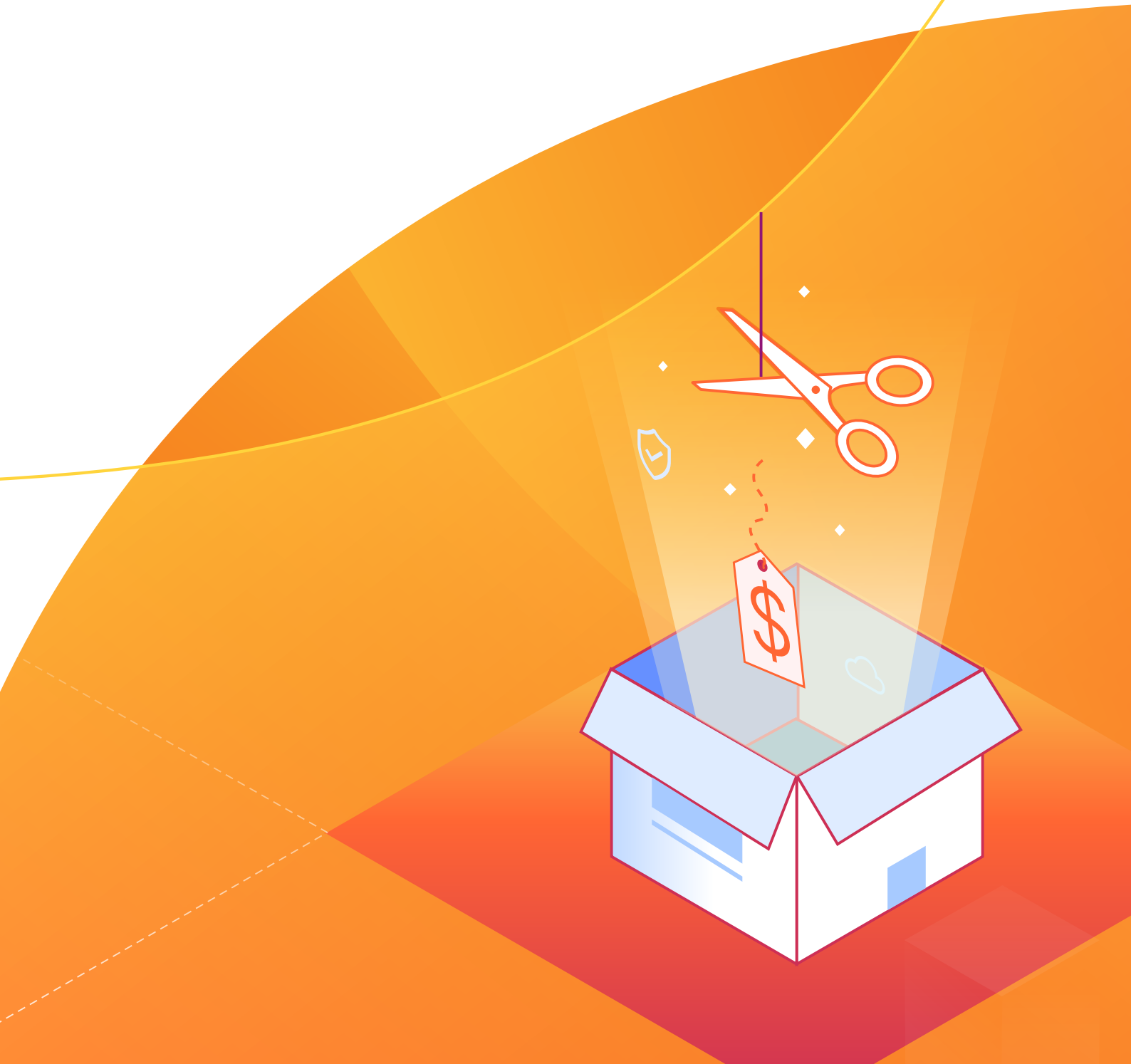
CLOUDFLARE

WHITEPAPER

Mit weniger mehr erreichen

7 Unternehmen verraten Ihre kostengünstigen Strategien für Anwendungssicherheit und -performance.



Inhalt

Kurzfassung

Die meisten IT-Architekturen sind zu kompliziert oder veraltet, um die Sicherheit in Webanwendungen einheitlich durchzusetzen. Sicherheitsteams sind gezwungen, isolierte Tools manuell zusammenzufügen, die nur einen begrenzten Überblick und ungenaue Kontrollmechanismen in Cloud-, Hybrid- und lokalen Umgebungen bieten, was die Geschäftstätigkeit beeinträchtigt.

All diese Komplexität führte zu überlasteten Teams, wachsenden Schwachstellen, schädlicheren Angriffe und einem unhaltbaren Ressourcenaufwand, nur um mit den Bedrohungen von gestern Schritt zu halten.

Unternehmen müssen Webanwendungen und APIs unbedingt vor bösartigen Bots, DDoS-Angriffen, Code-Injection und anderen Schwachstellen schützen. Die Umsetzung einer soliden Strategie für Anwendungssicherheit kann jedoch eine echte Herausforderung sein, vor allem, wenn man mit knappen Budgets und begrenzten Personalressourcen zu kämpfen hat.

In diesem Whitepaper erwarten Sie echte Erfahrungsberichte von Unternehmen, die erfolgreich Effizienzgewinne erzielen und die Kosten ihrer Anwendungssicherheisstrategie reduzieren konnten. Diese Erfolgsgeschichten zeigen Unternehmen mögliche Wege auf, wie sie mit Praktiken der Anwendungssicherheit ihre Ausgaben senken können.

Wenn Sicherheits- und IT-Teams mit weniger mehr erreichen müssen

Wenn Unternehmen mit Budgetkürzungen konfrontiert sind, kann jede Abteilung davon betroffen sein. Ob aufgrund allgemeiner wirtschaftlicher Ungewissheit, sinkender Umsätze, organisatorischer Umstrukturierungen oder einer Vielzahl anderer Gründe – Sicherheits- und IT-Teams sind oft gezwungen, ihre Abläufe ohne die erhoffte Budgeterhöhung zu verbessern – oder noch schlimmer, sie müssen dies tun, während sie gleichzeitig drastische Kosteneinschnitte vornehmen müssen.

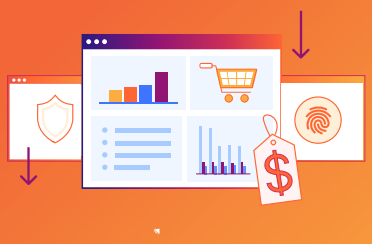
Doch bei der Anwendungssicherheit und -performance darf nicht gespart werden. Was die Sicherheit betrifft, so wird der Anwendungsschutz von Jahr zu Jahr komplizierter. Die Angriffe werden größer und komplexer als je zuvor, und mit dem Unternehmenswachstum wächst auch die Angriffsfläche. So ist beispielsweise die Zahl der gemeldeten CVEs zwischen 2022 und 2023 um 15 % gestiegen. Und obwohl mehr als 5.000 kritische Schwachstellen gemeldet wurden, liegt die durchschnittliche Zeit bis zur Veröffentlichung eines Patches für eine Webanwendungsschwachstelle mit kritischer Schwere nach wie vor bei etwa 35 Tagen, sodass die Anwendung in dieser Zeit ungeschützt bleibt.

Und was die Performance betrifft, so erwarten die Verbraucher, dass jedes digitale Erlebnis schnell, zuverlässig und personalisiert ist. Selbst geringfügige Verzögerungen können erhebliche Auswirkungen auf das Nutzerengagement und die Konversionsrate haben. Unternehmen haben das Nachsehen, wenn sie die Erwartungen ihrer Kunden nicht erfüllen können.

Angesichts des doppelten Drucks durch Budgetkürzungen und steigende Erwartungen müssen Sicherheits- und IT-Teams Wege finden, um mit weniger mehr zu erreichen. In diesem Whitepaper befassen wir uns mit Unternehmen, die wirksame, kosteneffiziente Anwendungssicherheits- und Performancemaßnahmen implementiert haben – ohne dabei auf Ergebnisse zu verzichten.

Wie Sie bei Ihren Maßnahmen für Anwendungssicherheit und Performance Einsparungen realisieren können

Um Webanwendungen und APIs vor modernen Bedrohungen zu schützen, benötigt man nicht nur eine mehrschichtige Sicherheitslösung, sondern auch eine, die es Unternehmen ermöglicht, unnötige Kosten einzusparen. Um dies zu erreichen, können Organisationen auf mehrere wichtige Strategien setzen. Dazu gehören die Konsolidierung von Anbietern, eine optimierte Zertifikatsverwaltung, ein dedizierter Schutz vor Angriffen, die die Traffic-Kosten in die Höhe treiben, und die Reduzierung der Egress-Gebühren.



Senken Sie die Kosten durch eine Konsolidierung der Sicherheitsanbieter

Optimieren Sie Arbeits- und Infrastrukturkosten mit automatischer Zertifikatsverwaltung

Blockieren Sie Angriffe, die die Traffic-Kosten in die Höhe treiben

Eliminieren Sie unerwartete Gebühren und Kosten wie Bandbreiten-, Cloud- und Egress-Gebühren

Senken Sie die Kosten durch eine Konsolidierung der Sicherheitsanbieter

Eine kürzlich von Gartner durchgeführte Umfrage ergab, dass 75 % der Unternehmen eine Konsolidierung der eingesetzten Sicherheitsanbieter in Erwägung ziehen. Indem sie die Anzahl der Anbieter, auf die sie angewiesen sind, reduzieren, können Unternehmen die Supply Chain-Prozesse optimieren und eine höhere Effizienz erreichen, was sich in geringeren Kosten niederschlägt.

Chrono24, ein führender Online-Marktplatz für Luxusuhren, hat durch die Konsolidierung mit Cloudflare seine Abhängigkeit von mehreren Anbietern verringert. Vor der Umstellung verwendete Chrono24 eine CDN-Lösung von EdgeCast sowie DDoS-Abwehr und WAF von mehreren anderen Anbietern. Das Sammelsurium an Lösungen funktionierte schlecht, was zu erheblichen Latenzzeiten, schlechter Performance bei der Sicherheit und unnötig hohen Anbieterkosten führte.

Nach der Konsolidierung mit den Cloudflare-Lösungen – einschließlich CDN, WAF und DDoS-Abwehr – konnte Chrono24 die Kosten für die Sicherheit und Performance seiner Website um 67 % senken.

„Unsere Basiskosten sind jetzt viel niedriger, weil wir für Performance- und Sicherheitdienste nur noch einen Anbieter nutzen“, sagt Sven Ferber, Director of Technology. „Ich schätze, dass wir nur mehr ein Drittel der früheren Ausgaben haben.“

Durch die Anbieterkonsolidierung können Unternehmen ihre Einkaufs- und Verwaltungskosten sehr effektiv senken. Die folgenden drei Fragen helfen Ihnen bei der Planung einer möglichen Anbieterkonsolidierung:

1. Bietet Ihr Anbieter Bedrohungsschutz und verbessert er die Anwendungsperformance?
2. Können Sie Ihre Anwendungen und APIs von einer einzigen Konsole aus verwalten?
3. Können mehrere Teams in Ihrem Unternehmen denselben Anbieter nutzen, um ihr Budget effizienter einzusetzen?

Wenn Sie die oben genannten Konsolidierungstipps befolgen, können Unternehmen ihre Kosten senken, das Supply Chain Management vereinfachen und die Beziehungen zu wichtigen Anbietern stärken.

chrono24

Fazit

75 % der Unternehmen erwägen eine Anbieterkonsolidierung

Chrono24 konnte nach der Konsolidierung mit Cloudflare die Kosten für die Sicherheit der Website und die IT-Kosten um **67 %** senken

Indem sie die Anzahl der Anbieter reduzieren und Dienstleistungen konsolidieren, können Unternehmen **Kosten senken** und das Supply-Chain-Management vereinfachen

Optimieren Sie Arbeits- und Infrastrukturkosten mit automatischer Zertifikatsverwaltung

Für IT-Teams kann die Bereitstellung von Sicherheitskonfigurationen über mehrere Domains und geografische Regionen hinweg ein kostspieliger und zeitaufwändiger Prozess sein. Und versteckte Kosten können den Organisationen, die sie unterstützen, zusätzliches Kopfzerbrechen bereiten – insbesondere denjenigen, die mit Budgetbeschränkungen zu kämpfen haben.

Oft verbergen sich diese versteckten Kosten im Zertifikatsmanagement. SSL/TLS-Zertifikate sind die digitale Identität eines Netzwerks. Im Durchschnitt kann die Webpräsenz eines Unternehmens Hunderte, wenn nicht Tausende von Zertifikaten erfordern. Die Verwaltung dieser Zertifikate kann jedoch teuer werden, da sich die Arbeits- und Infrastrukturkosten summieren – ganz zu schweigen von den Umsatzeinbußen, die durch unerwartete Ausfälle von Zertifikaten entstehen können.

SHOPYY, eine E-Commerce-Plattform, verwendet Cloudflare, um die Verwaltung von SSL-Zertifikaten zu automatisieren, einschließlich der Erstellung und dem Schutz privater Schlüssel, der Domain-Validierung, der Ausstellung, Erneuerung und Neuausstellung.

Anfangs verwendete SHOPYY ein kostenloses Tool zur Verwaltung von Zertifikaten, das ihnen unzuverlässige Zertifikate mit kurzer Gültigkeitsdauer bot. Infolgedessen musste SHOPYY zusätzliche Mitarbeiter einstellen, um das Zertifizierungsmanagement und den Erneuerungsprozess zu überwachen.

SHOPYY vertraut die Zertifikatsverwaltung via Cloudflare SSL für SaaS Cloudflare an, so dass nur ein einziger interner Mitarbeiter für die Pflege des gesamten Prozesses benötigt wird.

„Durch den Einsatz von Cloudflare-Produkten konnten wir allein die Kosten für Betrieb und Wartung um 60 % senken“, sagt Gründer und CTO Yuanming Chen.

Eine ineffektive Zertifikatsverwaltung kann sich auch auf den Umsatz auswirken, da die Zertifikate ablaufen. LendingTree, ein Online-Marktplatz für Kredite, verwendet die TLS-Zertifikate von Cloudflare, um Geld zu sparen und Ausfälle zu vermeiden.

„Wir haben Tausende von verschiedenen Internet-Websites. Bei dieser Größenordnung war es nur eine Frage der Zeit, bis wir ein Zertifikat nicht rechtzeitig erneuern würden“, sagt Application Security Lead John Turner. „Durch den Einsatz der sich automatisch erneuernden TLS-Zertifikate von Cloudflare sparen wir etwa 50.000 USD pro Jahr, sowohl an Verwaltungskosten als auch an entgangenen Einnahmen durch Ausfälle aufgrund abgelaufener Zertifikate.“

Der Einbau eines effektiven Systems zur Zertifikatsverwaltung kann auch dabei helfen, die Ressourcen angemessen zu verteilen. Das in Deutschland gegründete Unternehmen mogenius, eine automatisierte Plattform für die Bereitstellung von cloudbasierten Anwendungen, automatisiert sein Zertifikatsmanagement mit Cloudflare — so kann das Unternehmen mehr Zeit für die Entwicklung seines Kerngeschäfts aufwenden.

„Würden wir all das, was Cloudflare für uns erledigt, intern verwalten, würde das mindestens 20 % unserer Zeit in Anspruch nehmen“, sagt Jan Lepsky, Mitgründer und CPO. „**Mit Cloudflare können wir uns auf die Optimierung der Cloud-Entwicklung und der Bereitstellungspipelines für unsere Kunden konzentrieren.“**

Die Auslagerung der Zertifikatsverwaltung ist für Unternehmen von entscheidender Bedeutung, um versteckte Kosten zu vermeiden und einen reibungslosen Geschäftsbetrieb zu gewährleisten. Ineffiziente, manuelle oder lückenhafte Zertifizierungsverfahren führen zu hohen Arbeits- und Infrastrukturkosten, Umsatzeinbußen aufgrund abgelaufener Zertifikate und einer verschwenderischen Ressourcenverteilung.

Durch die Implementierung einer Zertifikatsverwaltung mit Funktionen wie SSL für SaaS oder TLS-Zertifizierungen können Unternehmen erhebliche Kosten sparen und ihr Geschäftsergebnis verbessern.

SHOPYY

lendingtree

mogenius

Fazit

Mit Cloudflare SSL für SaaS konnte SHOPYY die Betriebs- und Wartungskosten um 60 % senken

Mit Cloudflare TLS spart LendingTree 50.000 USD pro Jahr an Verwaltungskosten und entgangenen Einnahmen

Cloudflare ermöglicht es mogenius, die Zertifikatsverwaltung zu automatisieren und so 20 % seiner Zeit für sein Kerngeschäft zu nutzen

Blockieren Sie Angriffe, die die Traffic-Kosten in die Höhe treiben

Mit der zunehmenden Nutzung von APIs wächst auch die Angriffsfläche. Bösartige Bots, DDoS-Angriffe und andere Bedrohungen können Anwendungen und APIs gefährden – und Führungskräfte und Technikverantwortliche sind sich der erheblichen Auswirkungen bewusst, die diese Angriffe auf ihr Unternehmen haben können.

Schätzungen zufolge belaufen sich die Kosten, die Unternehmen durch die Unsicherheit bei API entstehen, auf bis zu 75 Mrd. USD pro Jahr.

Diese Angriffe führen zu Credential Stuffing und DDoS-Angriffen und können nicht nur den Service für legitime Benutzer unterbrechen, sondern zwingen Organisationen auch dazu, die Kosten für den durch den Angriffsverkehr verursachten Datenverkehr zu tragen.

LendingTree gab erhebliche Summen für einen früheren Sicherheitsanbieter aus, der bei DDoS-Angriffen hohe Preise verlangte. Dieses Modell verursachte nicht nur enorme Überschreitungskosten, sondern führte auch dazu, dass legitimer Traffic blockiert wurde.

„Jedes Mal, wenn wir einen neuen TV-Spot oder eine neue Social-Media-Kampagne starteten, überstiegen die Anfragen das willkürliche Limit, das wir gemäß der Vorgaben des Anbieters festgelegt hatten. Der Partner interpretierte die Traffic-Spitze also als DDoS-Angriff und blockierte folglich legitimen Traffic“, erinnert sich John Turner, Application Security Leader. „**Dabei haben wir nicht nur potenzielle Kunden verloren, sondern auch das Geld, das wir ausgegeben haben, um sie auf unsere Website zu bekommen ... und unser Anbieter stellte uns diesen ‚Service‘ dann sogar noch als ‚DDoS-Schutz‘ in Rechnung.“**

Um diese Ineffizienzen zu beseitigen, setzte LendingTree auf die Bot Management- und Rate-Limiting-Funktionen von Cloudflare. **Innerhalb von 48 Stunden ging ein Angriff auf einen bestimmten API-Endpunkt um 70 % zurück, und in weniger als fünf Monaten sparte LendingTree 250.000 USD, indem es den Missbrauch von API-Endpunkten stoppte.**

Als die Online-Gaming-Holding Flutter Entertainment feststellte, dass fast 70-90 % ihres Traffics bösartig war, musste rasch eine Lösung gefunden werden, um bösartige Bots zu filtern und zu blockieren. Nach der Implementierung von Cloudflare Bot Management konnte **Flutter seinen bösartigen Traffic um 90 % reduzieren, und so jedes Jahr mehr als 2 Mio. GBP sparen.**

Mit Bot-Management und DDoS-Schutz können Unternehmen Angriffe und API-Missbrauch verhindern und die Ausgaben für Angriffe reduzieren. Bei der Suche nach Sicherheitsanbietern sollten Unternehmen nach Anbietern suchen, die:

- Machine Learning nutzen, um auf der Grundlage beobachteter Traffic-Daten Tarifgrenzen festzulegen
- Über geografische und IP-Standort-basierte Durchsatzbegrenzungen hinausgehen, da moderne Angriffe die IP-Beschränkungen leicht umgehen können
- Sicherstellen, dass Entwickler den gesamten Traffic von Webanwendungen und öffentlichen APIs durch eine WAF und ein API-Gateway leiten
- DDoS-, WAF- und API-Gateway-Tools für eine mehrschichtige Bedrohungsabwehr integrieren
- Latenzzeiten reduzieren, indem sie sicherstellen, dass der Traffic des Unternehmens dort geschützt wird, wo er bereitgestellt wird
- DDoS-Abwehr ohne Volumensbegrenzung bieten, damit Sie keine Überschreitungsgebühren zahlen müssen

Die Implementierung der richtigen Anbieter-/Sicherheitsstrategie kann zu Einsparungen von Tausenden, wenn nicht Millionen von Dollar pro Jahr führen.

Flutter™

Fazit

Unsichere APIs kosten Unternehmen **jährlich bis zu 75 Mrd. USD**

Die Implementierung der richtigen Tools für Anwendungssicherheit kann zu **Einsparungen von Tausenden, wenn nicht Millionen von Dollar pro Jahr führen**

Dank des DDoS-Schutzes konnte LendingTree einen Angriff auf eine bestimmte API innerhalb von 48 Stunden um 70 % reduzieren und in weniger als fünf Monaten 250.000 USD einsparen, indem es die Angriffe stoppte

Cloudflare Bot Management half Flutter, seinen bösartigen Traffic um 90 % zu reduzieren und jährlich mehr als 2 Mio. GBP einzusparen

Eliminieren Sie unerwartete Gebühren und Kosten wie Bandbreiten-, Cloud- und Egress-Gebühren

Viele Sicherheitsdienste sind von der Cloud abhängig, und viele Cloud-Anbieter verlangen von Unternehmen Gebühren für Speicherplatz und Rechenleistung. Darüber hinaus müssen Unternehmen oft Gebühren für das Übertragen von Daten aus dem Speicher bezahlen.

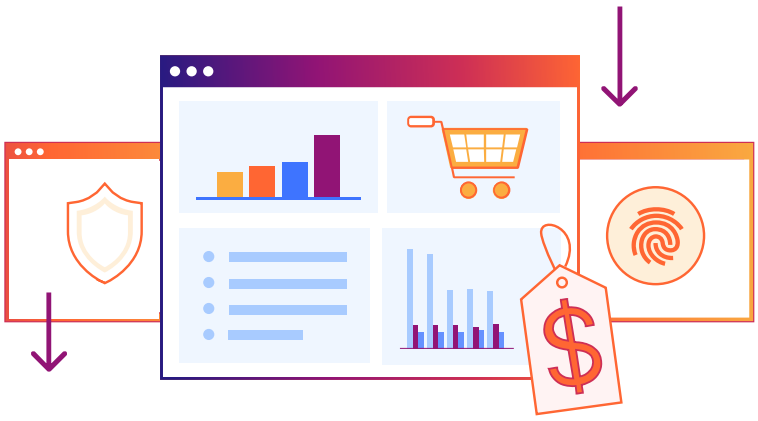
Die Egress-Gebühren werden nach mehreren Faktoren berechnet, z. B. nach Kundenkategorie, Abonnementtyp und übertragenem Datenvolumen. Aus diesem Grund sind diese Gebühren in der Regel schwer vorherzusagen – und das kann Unternehmen teuer zu stehen kommen, wenn sie sich zu summieren beginnen. Tatsächlich schätzt IDC, dass die Egress-Gebühren mindestens 6 % der Kosten für Cloud-Speicher ausmachen.

Vor diesem Hintergrund entschied sich PagesJaunes, ein europäisches Digitalverzeichnis und lokaler Suchdienst, für die Implementierung des Cloudflare CDN, um die Bandbreitengebühren zu senken und die Cache- und DNS-Verwaltung zu verbessern.

„Wir haben schnell gemerkt, dass der vom Cloudflare CDN absorbierte Traffic dazu führte, dass unsere Infrastruktur weniger belastet und widerstandsfähiger wurde“, betont Loïc Troquet, Head of Architecture, Performance and Security. **„70 % der Bandbreite musste nicht mehr von der Infrastruktur von Solocal bereitgestellt werden.“**

Und Bandbreiteneinsparungen führen zu Kosteneinsparungen. Nach der Übernahme der CDN-, DNS-, WAF- und DDoS-Abwehrservices von Cloudflare konnte das Online-Lern- und Studientool **Quizlet täglich mehr als 10 TB an Gesamtbandbreite einsparen und senkte zudem die Kosten für Netzwerk-Egress-Gebühren von Google Cloud Services um mehr als 50 %.**

Durch die Implementierung von Strategien und Praktiken zur Anwendungssicherheit können unerwartete Egress-Gebühren vermieden werden.



PagesJaunes

Quizlet

Fazit

Die Umsetzung von Strategien zur Anwendungssicherheit, wie z. B. die Auswahl des richtigen CDN-Anbieters, kann unerwartete Egress-Gebühren verhindern

Mit dem Cloudflare CDN hat PagesJaunes seinen Bandbreitenverbrauch um 70 % reduziert

Quizlet nutzte Cloudflare, **um täglich mehr als 10 TB an Bandbreite einzusparen** und senkte die Egress-Gebühren an Google Cloud Services um mehr als 50 %, was zu monatlichen Einsparungen von Tausenden von Dollar führte

Anwendungssicherheit vereinfachen und Kosten senken – dank Cloudflare

Mit Cloudflare können Unternehmen Strategien zur Anwendungssicherheit integrieren, um die Effizienz zu steigern und die Kosten zu senken. Das integrierte Cloudflare-Portfolio für Anwendungssicherheit vereint erstklassige DDoS-Abwehr ohne Volumensbegrenzung, eine Web Application Firewall, die die fortschrittlichsten Angriffe stoppt, proaktive API-Sicherheit, Bot-Management mit Bedrohungsdaten und fortschrittliche Erkennung von Angriffen auf der Client-Seite.

Neugierig?

Kontaktieren Sie uns

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

BDES-5972.2024MAY31