CLOUDFLARE

Zehn Methoden, um Ihren Mitarbeitern online Sicherheit und Geschwindigkeit zu bieten

Heutige Remote-Teams bestehen aus vielen unterschiedlichen Arten von Benutzern. Dazu gehören Angestellte, Auftragnehmer und Partner, die alle mit denselben Tools zusammenarbeiten. Wie können Sie angesichts der zunehmenden geografischen Verteilung Ihres Teams die Daten Ihres Unternehmens schützen, ohne die Effektivität der Benutzer zu beeinträchtigen?

Dieses E-Book enthält zehn bewährte Methoden, die leistungsstarke Unternehmen zum Schutz ihrer globalen Belegschaft umsetzen können, ohne dadurch Abstriche bei der Produktivität zu verzeichnen.

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

Inhalt

Einleitung

Es gab eine Zeit, als das Büro der Ort war, an dem gearbeitet wurde. Mitarbeiter, die von außerhalb Zugang zu internen Systemen brauchten, mussten sich mit träger Performance und komplexen VPNs abplagen, wenn sie sich überhaupt die Mühe machten.

Mittlerweile hat sich das Bild grundlegend geändert. Zuerst war es eine freie Entscheidung, jetzt wird es durch die Umstände bedingt: Belegschaften sind zunehmend mobil und über viele Standorte verteilt. Während es früher möglich war, einen Zaun um das Unternehmensnetzwerk zu ziehen, haben moderne Anwendungen und die Vielzahl der Geräte, die aus der Ferne auf sie zugreifen, die herkömmlichen Sicherheitsniveaus unbrauchbar gemacht. Das moderne Unternehmensnetzwerk ist das Internet, und zu seinem Schutz ist ein fundamental neuer Ansatz nötig.

In dieser Abhandlung werden die Grundlagen vorgestellt, die Sie brauchen, um die Online-Sicherheit Ihres Unternehmens heute und in Zukunft anzupassen. Sie lernen grundlegende Konzepte wie das **Zero-Trust-Sicherheitsmodell** kennen, werfen einen Blick auf neue Lösungen für alte Probleme und gewinnen die nötigen Kenntnisse, um Ihr Team in dieser sich rasant wandelnden Umgebung zu schützen.

Über Cloudflare

Cloudflare ist ein führendes Unternehmen für Sicherheit, Leistung und Zuverlässigkeit mit dem erklärten Ziel, das Internet besser zu machen.

Unsere integrierte Cloud-Plattform, die das Vertrauen von über 25 Millionen Websites und Webapplikationen genießt, hilft Marken und Händlern, die Performance ihrer Websites zu verbessern und gleichzeitig Kundendaten und Transaktionen zu schützen.

- Ein Netzwerk, das über 200 Städte und mehr als 90 Länder umfasst
- 99 % der Internetbenutzer in den Industrieländern werden innerhalb von 100 Millisekunden erreicht
- Im 4. Quartal 2019 wurden täglich durchschnittlich 50 Milliarden Cyber-Bedrohungen blockiert
- Eine Gesamtnetzwerkkapazität von 35 Tbit/s

Kapitel 1: Das Bild ändert sich

Schon vor der starken Zunahme der Remote-Arbeit entwickelten sich moderne Teams bereits in Richtung Mobilität und geografischer Verteilung. In der Vergangenheit konnte ein Unternehmen beruhigt davon ausgehen, dass Verbindungen zu seinen Netzwerken über firmeneigene Laptops und Handys laufen würden. Mittlerweile ist es jedoch viel üblicher geworden, dass Mitarbeiter ihre persönlichen Smartphones und Tablets benutzen, um Dokumente aufzusetzen, Videoanrufe zu tätigen und vieles mehr.

Während aber die Praxis, ein eigenes Gerät zu verwenden, in mancherlei Hinsicht von großem Vorteil für die Bequemlichkeit und die Produktivitätssteigerung ist, bereitet sie gleichzeitig den Mitarbeitern der IT-Abteilungen viele schlaflose Nächte. Für Administratoren ist es schwierig (bzw. unmöglich), für all diese Geräte effektive Sicherheitsrichtlinien aufzustellen und durchzusetzen, und Mitarbeiter sind unter Umständen wenig geneigt, auf ihren persönlichen Geräten Sicherheitssoftware zu installieren.

Darum ist es sinnvoll, Sicherheit auf Unternehmensebene umzusetzen und ein Modell anzunehmen, bei dem alle Geräte von Natur aus als nicht vertrauenswürdig betrachtet werden – weil es so schwer ist, sie abzusichern.

Tipp Nr. 1

Angesichts der Vielzahl an verbundenen Geräten ist es unmöglich, jeden Endpunkt zu sichern. Daher müssen Sicherheitsanalyse und -durchsetzung auf Netzwerkebene durchgeführt werden.

Kapitel 1: Das Bild ändert sich (Fortsetzung)

Leider haben diese Bedenken für Unternehmen jeder Größe Gültigkeit. Cyberangriffe sind auf dem Vormarsch und böswillige Akteure versuchen, Sicherheitslücken auszunutzen, die sich eventuell bei der schnellen Umstellung auf die Arbeit im Homeoffice aufgetan haben, während Teams durch andere Aufgaben abgelenkt werden. Tatsächlich nahm die Anzahl der Angriffe zwischen Januar und März 2020 zeitweise um 70 % zu.

Dieser rasante Übergang zur Remote-Arbeit stellt zusammen mit dem Anstieg von Online-Bedrohungen ein akutes Problem für viele IT-Teams dar, für das wahrscheinlich neue Lösungen erforderlich sein werden. Und obwohl Veränderung nie leicht ist, können sich hierbei Gelegenheiten zu zusätzlichen Verbesserungen Ihres Unternehmens ergeben.

Tipp Nr. 2

Bei der Neubewertung Ihres Sicherheitsniveaus sollten Sie moderne SaaS-Lösungen in Betracht ziehen, von denen heute viele stabiler sind als frühere Versionen.

Kapitel 2: Eine Toolbox für alle

Bei der Umstellung auf Remote-Arbeit wollen Sie sich wahrscheinlich die Tools, auf die sich Ihr Team tagtäglich verlässt, noch einmal genauer ansehen. Dabei wird vermutlich Software, die Zusammenarbeit in Echtzeit ermöglicht, ganz oben auf der Liste stehen. Und es wird wichtig sein, Sicherheitslösungen zu identifizieren, die Hand in Hand mit neu eingesetzten Tools arbeiten.

Wenn Sie sich neue Lösungen ansehen, sollte dabei die Benutzerfreundlichkeit einer der wichtigsten Gesichtspunkte sein. Ihre Teammitglieder werden unterschiedliche technische Kenntnisse haben, und alle eventuellen Hindernisse, auf die sie stoßen, werden sich unmittelbar auf die Produktivität und die Arbeitsmoral auswirken. Daher ist es wichtig, einen Ansatz zu entwickeln, der so intuitiv und benutzerfreundlich wie möglich ist.

Wenn Ihr Sicherheitsniveau Ihrem Team Kopfschmerzen bereitet, wird Ihre IT-Abteilung einer schweren Belastung ausgesetzt. Es ist möglich, dass Mitarbeiter auf die Nutzung interner Tools vollständig verzichten (oder – was schlimmer ist – versuchen, sie zu umgehen).

Eine Startrampe für die Produktivität

Während Sie die digitale Toolbox Ihres Teams weiterentwickeln, können Sie die Nutzung der Werkzeuge zusätzlich anregen, indem Sie sie nur einen Mausklick entfernt bereitstellen. Moderne Authentifizierungssysteme bieten Ihrem Team eine Auswahl an Tools (nämlich diejenigen, zu denen sie Zugriff haben). Sie enthalten Deep Links, die den Benutzer direkt zum richtigen Dashboard bringen – ohne verschachtelte Lesezeichen oder langwierige Anmeldeprozesse.

Einsatz von Software-as-a-Service

Glücklicherweise gibt es viele ausgereifte SaaS-Lösungen (Software as a Service), die von Grund auf um das Prinzip herum aufgebaut sind, die Zusammenarbeit von Benutzern an unterschiedlichen Standorten zu ermöglichen.

Das SaaS-Modell unterscheidet sich vom herkömmlichen Ansatz, bei dem Software gekauft wird, in mehrfacher Hinsicht auf grundlegende Weise:

- Anstatt die Tools auf Ihren eigenen Servern zu hosten und instand zu halten, greift Ihr Team sicher von Servern, die vom Software-Provider verwaltet werden, auf sie zu. So kann der Provider kontinuierlich Updates und Verbesserungen an der Software vornehmen, ohne dass das zusätzliche Arbeit für Sie bedeutet.

- Anstelle einer großen Vorauszahlung berechnen SaaS-Provider gewöhnlich eine viel kleinere, regelmäßig zu erstattende Gebühr. Dadurch werden Tools möglich, die sonst unter Umständen unbezahlbar wären.

Namhafte SaaS-Tools sind von Anbietern wie Salesforce, Box und Googles G-Suite (einschließlich Google Docs and Sheets) erhältlich, neben denen noch unzählige fachbezogene Tools zur Verfügung stehen. Selbst wenn Sie in einer relativ spezialisierten Branche arbeiten, ist es gut möglich, dass es eine maßgeschneiderte SaaS-App für Sie gibt.

Ein weiterer positiver Aspekt liegt darin, dass sich SaaS-Tools viele UX-Konventionen mit Verbraucheranwendungen teilen, so dass die meisten Ihrer Teammitglieder keine Probleme damit haben werden.

Kapitel 3: Loslösung vom VPN

VPNs haben sich ihren Platz in den Annalen der Konnektivitätsgeschichte verdient. Seit Jahrzehnten sorgen sie für die Sicherheit der Unternehmen, und viele Firmen verlassen sich auch heute noch auf sie.

Leider bringen VPNs massenweise Probleme mit sich.

An erster Stelle steht dabei die mangelnde Benutzerfreundlichkeit: VPNs sind bekanntlich schwer bereitzustellen und zu benutzen. Angesichts von Konfigurationshürden, Zuverlässigkeitsproblemen und monströsen Anmeldevorgängen sind VPNs eine Schikane für jeden und werden oft zu einer enormen Belastung für Ihre IT-Abteilung.

Sogar wenn Ihr VPN wie beabsichtigt funktioniert, verursacht es Latenz, die von einem geringen Ärgernis bis zur vollständigen Lahmlegung des Systems reichen kann. Konstruktionsbedingt filtern VPNs den gesamten Datenverkehr durch dieselbe Leitung, und wenn Ihre Mitarbeiter remote arbeiten, muss jedes Paket zurück zu Ihrem VPN-Gerät im Unternehmenssitz geroutet werden, bevor es seine Reise zur vorgesehenen Zieladresse antreten kann. Das verursacht Latenz und Frustration, insbesondere für global verteilte Teams.

Was noch schlimmer ist: VPNs setzen ein Sicherheitsmodell ein, das keinen Sinn mehr macht. Jeder, der sich erfolgreich mit einem Unternehmens-VPN verbindet, wird als vertrauenswürdig betrachtet – ohne weitere Kontrollen nach der erstmaligen Verbindung. Die Probleme mit diesem übermäßig freizügigen Modell werden durch die von VPNs unterstützte, wenig zuverlässige Protokollierung noch verschärft, bei der die IP-Adresse eines Benutzers registriert werden kann, jedoch keine der Anwendungen oder Daten, auf die zugegriffen wurde. . Dadurch wird es schwer für Sicherheitsteams, Protokolle von Benutzeraktivitäten für Konformitätszwecke zu erstellen, und ganz besonders mühsam, die Schritte von Benutzern nachzuverfolgen, falls der Verdacht besteht, dass ein Konto eventuell missbraucht wurde.

Es gibt auch noch ein weiteres und grundlegendes Problem im Zusammenhang mit VPNs. In der Vergangenheit konnte ein Unternehmen erwarten, eine Handvoll interner Anwendungen auf seinen eigenen Servern zu hosten, und VPNs hatten die Aufgabe, vertrauenswürdige Mitarbeiter mit diesen Ressourcen zu verbinden. Heute verlassen sich die meisten Unternehmen dagegen auf eine Kombination aus Anwendungen, die auf ihrer eigenen Infrastruktur laufen, der öffentlichen Cloud und SaaS-Anwendungen – was mit einem herkömmlichen VPN unmöglich zu schützen wäre.

Sogar wenn Ihr VPN wie beabsichtigt funktioniert, verursacht es Latenz, die von einem geringen Ärgernis bis zur vollständigen Lahmlegung des Systems reichen kann.

Tipp Nr. 3

Wenn Ihre Infrastruktur nicht mehr dem Modell mit der Burg und dem Wassergraben ähnelt, dann ist es an der Zeit, dass Sie Ihre Schutzoptionen neu bewerten.

Kapitel 3: Loslösung vom VPN (Fortsetzung)

Zero Trust: ein neues Modell für eine neue Ära

Im Laufe der letzten Jahre hat ein neuer Ansatz zur Online-Sicherheit die Art und Weise verändert, auf die sich Unternehmen in der modernen, vernetzten Welt schützen. Dabei geht es um eine Idee, die als Zero-Trust-Sicherheit bezeichnet wird.

Anstelle des von VPNs verwendeten Modells mit der Burg und dem Wassergraben wird bei Zero Trust niemals Vertrauen vorausgesetzt. Jede Anfrage an jede Anwendung wird digital abgefragt, unabhängig davon, woher sie kam oder wohin sie geht.

Das Zero-Trust-Modell wurde zuerst von Google in einer 2016 veröffentlichten Forschungsarbeit bekanntgemacht, in der beschrieben wird, wie der Technikgigant sein internes Sicherheitsmodell so umgestaltet hat, dass es „sowohl interne als auch externe Netzwerke vollständig als nicht vertrauenswürdig betrachtet". Seitdem wurde Zero Trust von vielen anderen führenden Unternehmen übernommen.

Dieses neue, dezentralisierte Authentifizierungsmodell ist auch für Konfigurationen mit mehreren Anwendungen geeignet, die lokale, Cloud- und SaaS-Infrastrukturen überspannen.
Das bedeutet, dass Sie gleichzeitig die neueste Cloud-Software zusammen mit den alten, lokal gehosteten Anwendungen einsetzen können, von denen Teile Ihres Unternehmens vielleicht noch abhängen. Dabei wird alles mit der modernsten Verschlüsselungstechnologie gesichert und ist für Ihr Team von überall aus erreichbar (soweit Sie den entsprechenden Regelsatz aufgestellt haben).

In diesem Zusammenhang ...

Tipp Nr. 4

Bieten Sie Ihren Teammitgliedern ein Authentifizierungserlebnis, mit dem sie vertraut sind und das ihnen nicht im Weg steht, damit sie ohne Probleme weiterarbeiten können.

Kapitel 3: Loslösung vom VPN (Fortsetzung)

Geben Sie Ihrem Team die Tools und die Daten, die es braucht – und nicht mehr

Eine der heikelsten Angelegenheiten eines jeden Unternehmens ist es, sicherzustellen, dass alle Teammitglieder Zugriff auf die Tools und Daten haben, die sie benötigen – mehr aber auch nicht. Je größer das Team, desto komplizierter wird diese Aufgabe. Ebenfalls ist es wichtig, Zugriffsberechtigungen möglichst schnell widerrufen zu können, sobald Mitarbeiter oder Vertragspartner das Unternehmen verlassen.

Die Verwaltung dieser Zugriffskontrollen erweist sich für IT-Unternehmen auf der ganzen Welt oftmals als Herausforderung, die mitunter noch dadurch verschärft wird, dass jeder Mitarbeiter über mehrere Konten für verschiedene Tools in unterschiedlichen Umgebungen verfügt.

Mit dem richtigen Authentifizierungssystem verlaufen Onboarding und Offboarding viel reibungsloser. Jedes neue Teammitglied und jeder neue Auftragnehmer erhält schnell und unkompliziert die Zugangsrechte für die benötigten Anwendungen und kann mithilfe eines Launchpads problemlos darauf zugreifen. Verlässt jemand das Team, lässt sich eine einzelne Konfigurationsänderung auf alle Anwendungen übertragen, so dass keine Ungewissheit mehr zurückbleibt.

Tipp Nr. 5

Setzen Sie eine moderne Zero-Trust-Sicherheitslösung ein, um zu gewährleisten, dass jede Anfrage an Ihr Netzwerk vollständig geschützt wird.

Kapitel 3: Loslösung vom VPN (Fortsetzung)

Auftragnehmer und andere Drittanbieter

Ein ähnliches Problem, dem sich viele Unternehmen ausgesetzt sehen, ist die Verwaltung von Auftragnehmern und anderen Drittanbietern. Ein langer On- und Offboarding-Prozess kann einige der Vorteile untergraben, die durch externe Mitarbeiter erzielt werden – abgesehen davon wollen diese vor ihrem Arbeitsbeginn wahrscheinlich auch nicht unbedingt allzu viele Etappen durchlaufen. Und genauso wie im Fall von Angestellten dürfen Ihre Auftragnehmer und Drittanbieter nur Zugriff zu den Daten und Tools haben, die sie brauchen, und zwar so lange, wie sie sie brauchen.

Moderne Authentifizierungslösungen erlauben Ihren Auftragnehmern, sich mit Konten anzumelden, die sie bereits haben – z. B. Gmail, Facebook oder LinkedIn. Sie erhalten dabei denselben Grad an Sicherheit, Protokollierung und abgestuften Berechtigungen, den Sie erzielen, wenn Sie neue Konten auf Ihren eigenen Systemen anlegen.

Manche Authentifizierungssysteme unterstützen auch einmalige Passcodes, wobei der Vertragspartner per E-Mail einen temporären Code erhält, der ihm befristeten Zugriff auf bestimmte Systeme ermöglicht. Dies ist eine weitere Option, um den Workflow Ihrer Auftragnehmer zu rationalisieren, ohne dabei die Sicherheit zu kompromittieren.

Tipp Nr. 6

Rationalisieren Sie das On- und Offboarding Ihrer Auftragnehmer, indem Sie ihnen ermöglichen, sich mit bereits vorhandenen Konten oder einmaligen Passcodes anzumelden.

Kapitel 3: Loslösung vom VPN (Fortsetzung)

Sicherung Ihres Netzwerks

Neben einem modernen Authentifizierungssystem ist es entscheidend, die Kontrolle über die Daten zu behalten, die in Ihr Netzwerk gelangen und es verlassen.

In der Vergangenheit haben Zweigstellen ihren gesamten internetgebundenen Datenverkehr an ein zentrales Rechenzentrum in oder in der Nähe der Unternehmenszentrale gesendet. Administratoren waren für die Konfiguration zuständig, um sicherzugehen, dass alle Anfragen über eine sichere Hardware-Firewall geleitet wurden. Die Hardware-Firewall betrachtete jede Anfrage, führte eine Inline-SSL-Überprüfung durch, wendete DNS-Filter an und stellte sicher, dass das Unternehmensnetzwerk vor Sicherheitsbedrohungen geschützt war. Diese Lösung funktionierte, wenn Mitarbeiter vom Büro aus auf geschäftskritische Anwendungen zugriffen und sich die Anwendungen nicht in der Cloud befanden.

SaaS-Anwendungen haben dieses Modell zunichtegemacht, als die Bereitstellung über die Cloud zum neuen Standard für Workforce-Anwendungen wurden. Als geschäftskritische Anwendungen in die Cloud verlagert wurden, stieg die Anzahl der internetgebundenen Anfragen aus allen Büros. Auch die Kosten gingen in die Höhe. In den letzten zehn Jahren sind die SaaS-Ausgaben in allen Unternehmenssegmenten um mehr als 1615 % gestiegen. Das bisherige Modell, bei dem der gesamte Internetverkehr über zentralisierte Standorte zurückgeführt wurde, konnte mit der digitalen Transformation, die alle Unternehmen zurzeit durchlaufen, nicht Schritt halten.

Diese Probleme werden durch geografisch verteilte Büros und Remote-Mitarbeiter verschärft, die ihren Netzwerkverkehr an die Hardware-Firewall ihres Unternehmens zurücksenden müssen. Diese befindet sich oft in der Unternehmenszentrale, manchmal jedoch am anderen Ende der Welt. Bisher wurde dieses Problem dadurch gelöst, dass MPLS-Verbindungen von Zweigstellen zum Hauptsitz hinzugefügt wurden. MPLS-Verbindungen sind jedoch teuer, und die Konfiguration und Bereitstellung kann lange dauern. Als Ergebnis geben Unternehmen Millionen für veraltete Lösungen aus, oder sie bleiben langsam, wodurch die Produktivität der Mitarbeiter gesenkt wird.

Ein weiteres Problem bei älteren Hardware-Firewalls besteht darin, dass sie nicht für die Umgebung des modernen Internets entworfen wurden, in der sich Bedrohungen ständig weiterentwickeln.

Zum Beispiel existieren etwa 84 % der Phishing-Sites weniger als 24 Stunden (Quelle), und ältere Hardware-Firewalls sind nicht schnell genug, um ihre statischen Regeln so zu aktualisieren, dass Phishing-Angriffe verhindert werden können. Wenn sich Sicherheitsbedrohungen im Internet wie bewegliche Ziele verhalten, können ältere Hardware-Geräte, die auf statischen Modellen zur Filterung von böswilligem Datenverkehr beruhen, nicht mehr mithalten. Infolgedessen bleiben Mitarbeiter auch dann anfällig für neue Bedrohungen, wenn Unternehmen internetgebundenen Datenverkehr an einen einzigen Standort zurückführen.

Die Cloudflare-Lösung: Cloudflare for Teams

Cloudflare for Teams

Wenn Ihnen die in diesem E-Book beschriebenen Probleme bekannt vorkommen, ist es gut möglich, dass Cloudflare for Teams die Lösung ist, nach der Sie suchen.

Cloudflare betreibt eines der größten Netzwerke der Welt: Es erstreckt sich über 200 Städte in über 90 Ländern und wird von über 26 Millionen Websites und Webapplikationen genutzt.
Cloudflare bietet eine Vielzahl von Diensten, die Sicherheit, Performance und Zuverlässigkeit umfassen, und wird von vielen der weltweit größten Marken genutzt – darunter 10 % der Fortune-1000-Unternehmen.

Cloudflare for Teams setzt die Leistungsfähigkeit von Cloudflares proprietärer Technologie ein und stellt sie Ihnen zum Schutz Ihres Teams, Ihres Netzwerks und Ihrer Daten zur Verfügung.

Tipp Nr. 7

Gewährleisten Sie ein effizientes und sicheres On- und Offboarding durch den Einsatz einer Sicherheitslösung mit differenzierten Zugriffskontrollen.

Cloudflare Access

Einfacher, sicherer Zugriff für interne Apps.

Ein Dashboard. All Ihre internen Apps.

Eine zentrale Oberfläche zum Schutz der Anwendungen Ihres Teams.

- Sicherung lokaler Anwendungen mit SSO in Stunden anstatt Monaten
- Einheitliche Zugriffskontrollen für On-Premise-, Private-Cloud- und Public-Cloud-Ressourcen
- Verwaltung des Zugriffs auf interne Apps auf Benutzer- und Anwendungsbasis

Zero Trust. 100 % Sicherheit

Erweitern Sie die Zero-Trust-Sicherheit auf private Anwendungen.

- Minimierung der exponierten Anwendungsoberfläche zum Schutz Ihrer Assets vor Angriffen
- Implementierung eines softwaredefinierten Sicherheitsperimeters ohne Codeänderungen
- Festlegung diskreter Schutzperimeter für wichtige Anwendungen

Unterziehen Sie Ihr VPN einer Performance-Verbesserungs-Kur

Ersetzen Sie Ihr Unternehmens-VPN durch SaaS-ähnliche Benutzerfreundlichkeit für alle internen Anwendungen.

- Authentifizierung von Benutzern überall auf der Welt mit Cloudflares globalem Netzwerk
- Hohe Benutzerakzeptanz und Reduzierung der IT-Kosten dank einer nahtlosen und vertrauten Anmeldeerfahrung
- Verbesserung der Performance für Endbenutzer mit dem verteilten Netzwerk und intelligenten Routing von Cloudflare

Tipp Nr. 8

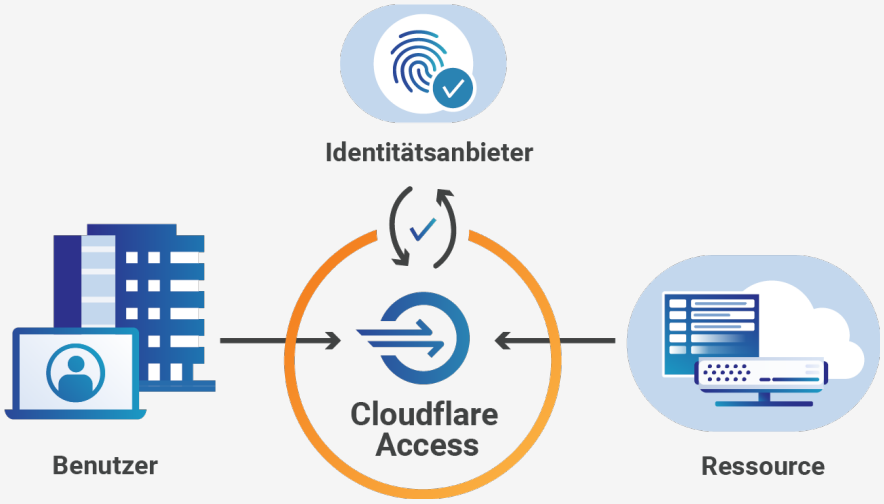
Halten Sie Ausschau nach einer integrierten Plattform zum Schutz Ihres Teams.

Cloudflare Access

Drittbenutzer? Bürger erster Klasse.

Binden Sie Partner und Auftragnehmer nahtlos ein, ohne unternehmensspezifische Anmeldekonten erstellen und verwalten zu müssen.

- Gleichzeitige Integration mehrerer Identitätsanbieter
- Einsatz beliebter Identitätsanbieter für externe Benutzer, während Ihre Mitarbeiter Ihr Unternehmens-SSO verwenden
- Sichere Verbindungen von jedem Gerät aus, ohne dass ein spezieller Software-Agent erforderlich ist



Überwachen Sie Anmeldevorgänge – und alles andere.

Protokollieren und überprüfen Sie jedes Ereignis.

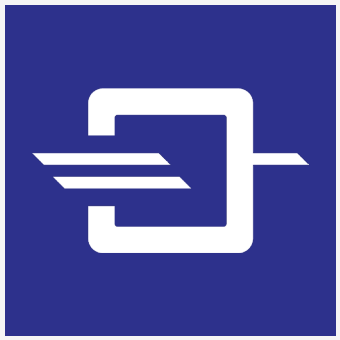
- Erstellung von Protokollen für Anmeldungen, Zugriffsanforderungen und Richtlinienänderungen in all Ihren internen Anwendungen – alles an einer Stelle
- Suche und Prüfung von Protokollen im Dashboard
- Integration in SIEMs für Transparenz im Unternehmen

Tipp Nr. 9

Ersetzen Sie Ihr Unternehmens-VPN durch eine SaaS-ähnliche Benutzerfreundlichkeit für all Ihre internen Anwendungen.

Cloudflare Gateway

Ein sicherer Weg ins Internet.



Ein sicherer Hafen im offenen Internet.

Schützen Sie Ihre Benutzer bei ihrer Navigation im Internet.

- Fernhalten böswilliger Inhalte von Ihrem Netzwerk durch DNS-Filterung
- Vollständige Übersicht über den Datenverkehr in und außerhalb Ihres Netzwerks
- Eliminierung von Zero-Day-Bedrohungen durch die Verlagerung der Webcode-Ausführung von den Browsern der Benutzer auf die Cloudflare-Edge

Für die Cloud gebaut. Nicht für die 90er Jahre.

Reduzieren Sie die Komplexität, die Ausgaben und die Latenz Ihres Netzwerks mit dem globalen Netzwerk von Cloudflare.

- Verwaltung, Bereitstellung und Überwachung Ihrer Sicherheitsrichtlinien am selben Ort
- Ausschaltung der Rückführung von Datenverkehr zur Unternehmenszentrale – internetgebundener Traffic geht direkt zu Cloudflare
- Verbesserung der Performance von Anwendungen im Internet mit der Argo-Smart-Routing-Technologie

Tipp Nr. 10

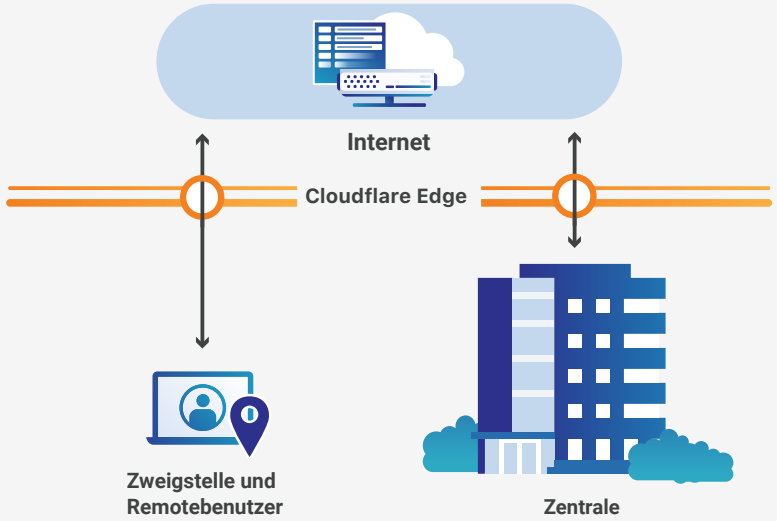
Tauschen Sie umständliche Firewall-Geräte gegen die einfache Überprüfung und Filterung des Datenverkehrs.

Cloudflare Gateway

Mehr Geschwindigkeit, weniger Kosten.

Reduzieren Sie die Ausgaben für teure MPLS-Verbindungen und veraltete On-Premise-Hardware.

- Sie brauchen keine Firewall der nächsten Generation mehr, wenn Sie die Cloudflare-Edge zur Überprüfung des Datenverkehrs einsetzen.
- Vermeiden Sie hohe MPLS-Gebühren durch Eliminierung des Daten-Backhauls ins Büro.
- Integrieren Sie SD-WAN-Provider, um den Datenverkehr sicher durch Cloudflares Netzwerkrand zu routen.



Beobachten Sie Ihre Daten mit Argusaugen.

Erhalten Sie mit SSL-Inspektion Transparenz über Ihren gesamten Internet-Traffic.

- Aufspüren verschleierter Bedrohungen mithilfe von Deep Packet Inspection
- Identifizierung von Geräten, die durch Malware, Command-and-Control-Callbacks oder andere Sicherheitsbedrohungen gefährdet sind
- Identifizierung von genehmigten SaaS-Anwendungen
- Visualisierung Ihres gesamten Internet-Traffics
- Übertragung von Protokollen zu Ihrem SIEM