

Sicherheit modernisieren

Eine einzige Sicherheitsplattform. Vom Netzwerk bis zur Cloud. Von Anwendungen bis zur KI.

Nahtloser Schutz von Nutzern und Daten über Anwendungen und KI hinweg

Obwohl Unternehmen vor der Herausforderung stehen, den steigenden Anforderungen an bessere Nutzererfahrungen und Innovationen gerecht zu werden, entwickeln sich Cyberbedrohungen weiter und nehmen zu. Die heutige Umgebung muss in der Lage sein, sich vor zunehmend automatisierten Bedrohungen und der Verbreitung vernetzter Geräte zu schützen, während gleichzeitig die Einführung von KI beschleunigt und die komplexen Sicherheitsherausforderungen bewältigt werden, die mit Cloud-nativen Infrastrukturen verbunden sind.

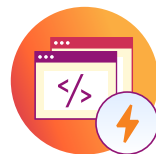


Minimieren Sie Sicherheitsrisiken und vereinfachen Sie Schutzmaßnahmen.

Die Komplexität der Sicherheitsabläufe hat zugenommen, da sich die Anzahl der Lösungen und Anbieter vervielfacht hat. Diese Komplexität begünstigt Angreifer, indem sie neue Möglichkeiten zur Ausnutzung von Sicherheitslücken schafft, da es für die Sicherheitsteams in Unternehmen schwieriger ist, sichere Umgebungen, Workloads, Daten und Personen zu verwalten und aufrechtzuerhalten.

- **Unterschiedliche Sicherheitslösungen** erfordern noch mehr Fachwissen und Ressourcen, um die wachsende Zahl von Sicherheitstools und -technologien zu verwalten.
- **KI-gesteuerte Angriffe** ermöglichen Angreifern Skalierung und Effizienz, um Angriffe schneller und kostengünstiger durchzuführen und ihre Reichweite über und innerhalb von Unternehmen zu erweitern.

Eine modernisierte Sicherheit ermöglicht es Unternehmen, digitale Erlebnisse durchgängig mit weniger Integrationsproblemen, geringeren Gesamtbetriebskosten (TCO) und einer schnelleren Markteinführung zu bieten – und gleichzeitig die Sicherheitsteams zu entlasten, damit sie sich auf wichtigere Aufgaben mit geschäftlicher Bedeutung konzentrieren können.



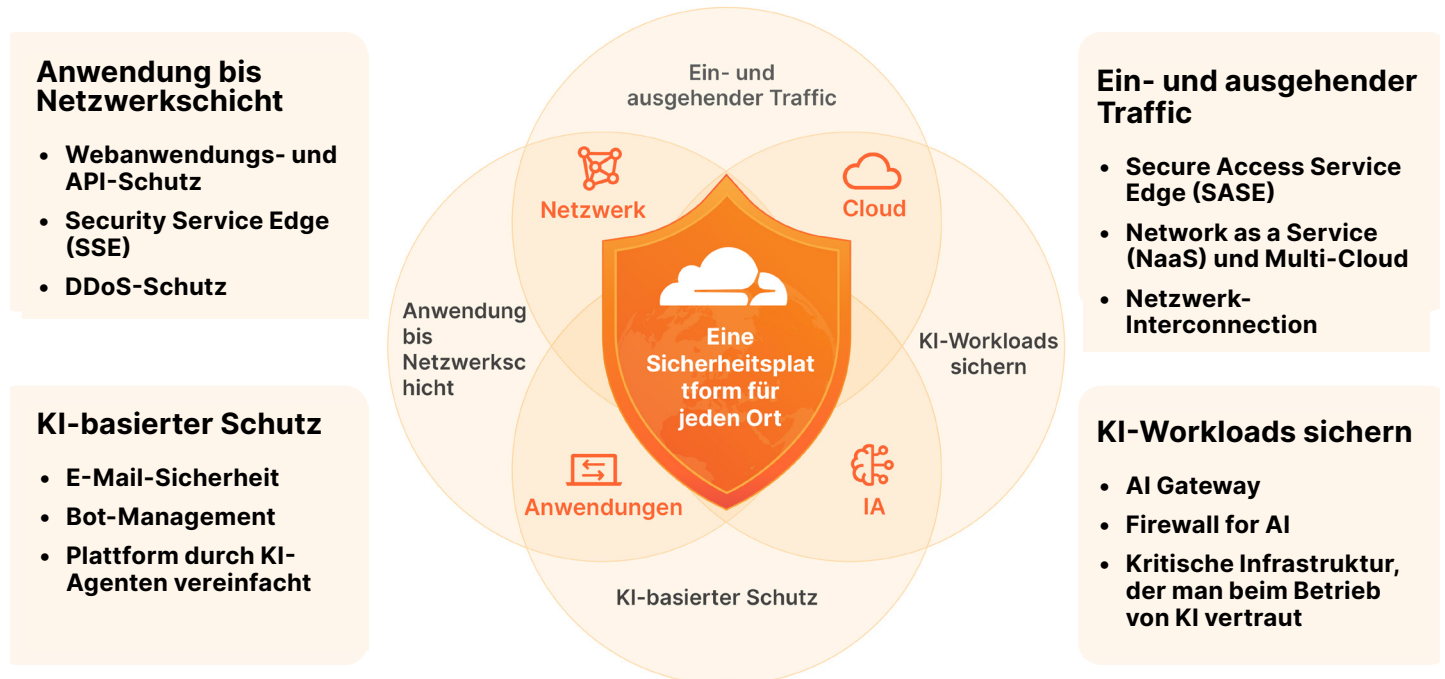
Beschleunigung der digitalen Transformation

Eine moderne Sicherheit untermauert die Fähigkeit eines Unternehmens, die geschäftlichen Anforderungen sicher zu erfüllen, und ermöglicht es, Folgendes einzuführen:

- Unübertroffene Skalierbarkeit, Flexibilität und Kosteneffizienz dank Cloud-Computing
- Kontinuierliche Validierung dank Zero Trust-Prinzipien
- Architekturen mit integriertem Schutz in cloudbasierten, Edge-basierten und digitalen Workflows
- KI zur Erkennung und (vorbeugenden) Bekämpfung von Cyberbedrohungen
- KI zur Steigerung der betrieblichen Effizienz und Effektivität beim Konfigurieren und Bereinigen von Sicherheitsrichtlinien
- Verlässliche Data Governance- und Compliance-Funktionen

Eine modernisierte Sicherheit schafft ein Gleichgewicht zwischen der Notwendigkeit digitaler Innovation und der Notwendigkeit, robuste Cybersicherheitsmaßnahmen zu gewährleisten. Unternehmen erhalten also die Zeit, um resilient und wettbewerbsfähig zu bleiben.

Eine einzige Sicherheitsplattform. Vom Netzwerk bis zur Cloud. Von Anwendungen bis zur KI.



Die einheitliche Sicherheitsplattform von Cloudflare skaliert nahtlos vom Netzwerk zur Cloud und schützt alle Benutzer und Daten über Anwendungen und KI hinweg. Sie nutzt ein intelligentes und programmierbares globales Cloud-Netzwerk, um eine Reihe unterschiedlicher Technologien zu vereinen, KI-gestützte Bedrohungsdaten für unkomplizierten, hochwirksamen Schutz zu bieten und KI-gestützte Erkennungen von Datenverlusten für verteilte Organisationen jeder Größe bereitzustellen.



Sichern Sie den ein- und ausgehenden Datenverkehr

vom Netzwerk zur Anwendungsschicht, um mit den vorhandenen Teams und dem Budget die Einheitlichkeit und Abdeckung verteilter IT-Umgebungen zu erhöhen.



Sichern Sie die KI-Workloads von Modellen bis zur Inferenz, um die KI-Akzeptanz mit sicheren, zuverlässigen Inferenzen und geschützten, bereinigten Daten für vertrauenswürdige KI-Modelle zu erhöhen.



KI-gestützter Schutz und die Beobachtbarkeit, die durch die Größe unseres globalen Netzwerks unterstützt werden, reduzieren die durchschnittliche Zeit, um zukünftige kritische Vorfälle zu erkennen, zu reagieren und zu bewältigen.

Cloudflare bietet einen integrierten Ansatz zur Modernisierung der Sicherheit, der die Bereitstellung vereinfacht, die Transparenz erhöht und die Gesamtbetriebskosten senkt, während gleichzeitig die verschiedenen Anbieter und Tools eliminiert werden, die mit herkömmlichen, fragmentierten Lösungen erforderlich sind. Durch die Bereitstellung von Sicherheit in geringer Entfernung zum Endnutzer und der angeforderten Ressource gewährleistet Cloudflare Resilienz und umfassenden Schutz vor den sich weiterentwickelnden Bedrohungen. Das Ergebnis: Eine Sicherheitsplattform. Vom Netzwerk bis zur Cloud. Von Anwendungen bis zur KI.

Mit Cloudflare erreichen Kunden:

25 %

geringere Wahrscheinlichkeit für einen IT-Sicherheitsvorfall bei Webanwendungen

29 %

höhere Effizienz der Sicherheitsabteilung

13 %

Steigerung der Effizienz des IT-Teams

238 %

Investitionsrendite über 3 Jahre und Amortisationszeit von weniger als 6 Monaten

Quelle: Forrester TEI-Studie

Wichtige Fallstudien



OKLAHOMA
Office of Management
& Enterprise Services

Die Abteilung Information Services des Office of Management and Enterprise Services des US-Bundesstaats Oklahoma überwacht die Infrastruktur und Technologie, die fast 180 staatliche Behörden, Gremien und Kommissionen sowie die über vier Millionen Einwohner des Bundesstaates sichert und verbindet.

In der Vergangenheit verfügte jede staatliche Organisation über ihre eigene Infrastruktur. Dadurch entstand ein Sammelsurium an On-Premise-Cloud- und Hybrid-Systemen, die auf Großrechnern, Windows- und Linux-Servern und sogar auf einigen Macintosh-Workstations liefen. Das hat uns in eine Situation gebracht, in der alte Systeme versuchen, mit unseren modernen Architekturen zu interagieren.

Wichtigste Vorteile

- **Geringere Kosten und Zeit:** Die Zusammenführung des US-Bundesstaats Oklahoma auf Cloudflare ermöglicht eine optimierte Verwaltung und Kostensenkungen.
- **Stärkeres Sicherheitsniveau der Behörden:** Die Sicherheitslage des gesamten Bundesstaates und die nationale Sicherheit werden verbessert.
- **Verbesserte Markteinführung:** Bietet zusätzliche Sicherheit für die Schichten 1–7 der öffentlichen Infrastruktur des US-Bundesstaats Oklahoma.

Eingesetzte Produkte: Cloudflare führte DNS, WAF und Bot-Management mit einer einzigen Steuerungsschnittstelle und unbegrenzter Skalierbarkeit ein.

Kontaktieren Sie uns, um zu erfahren, wie Sie Ihre Sicherheit modernisieren können.



+49 89 2555 2276



enterprise@cloudflare.com



www.cloudflare.com/de-de/



Indeed ist die weltweite Nummer 1 unter den Stellenbörsen. Das 2004 gegründete Unternehmen mit Sitz in Austin, Texas, beschäftigt mehr als 15.000 Mitarbeitende in Nordamerika, im asiatisch-pazifischen Raum und in Europa. Mehr als 350 Millionen Besucher nutzen Indeed jeden Monat, um nach Jobs zu suchen, Lebensläufe einzustellen, Unternehmen zu recherchieren und vieles mehr. Und über 3,5 Millionen Arbeitgeber finden hier ihre Kandidaten. Indeed ist für sein benutzerfreundliches Design und seine fortschrittlichen Technologien für die Jobsuche und -vermittlung bekannt und unterstützt Arbeitssuchende in über 60 Ländern und 28 Sprachen.

Wichtigste Vorteile

- **Beschleunigung der Transformation durch Ablösung eines alten VPNs:** Innerhalb von etwas mehr als drei Monaten hat Indeed sein VPN vollständig abgeschafft. Dazu gehörten die Migration Hunderter bereits bestehender Zugriffsrichtlinien und die Einführung von Cloudflare für über 13.000 Mitarbeitende und Auftragnehmer auf der ganzen Welt. Heute verwendet Indeed das Infrastructure-as-Code-Tool Terraform, um den Großteil der laufenden Verwaltung zu automatisieren, einschließlich des Onboardings neuer Nutzer und der Konfiguration neuer Richtlinien.
- **Reduziertes Risiko und verbesserte Benutzererfahrungen mit ZTNA:** „Im Vergleich zum VPN berichten unsere Nutzer überall von einer viel besseren und durchgängigeren Zugriffserfahrung mit Cloudflare“, sagt Matthew Ortiz, Senior Manager der Informationssicherheits-, Engineering- und Betriebsteams von Indeed, der insbesondere weniger Latenzzeit und zuverlässigere Verbindungen nannte, vor allem in Regionen, die traditionell Probleme mit dem VPN hatten.
- **Generative KI-Risiken identifizieren und mindern:** „Trotz ihrer vielen legitimen Nutzer ist KI ein großes Sicherheits- und Datenschutzproblem“, sagt Ortiz. „Cloudflare hilft uns dabei, die Risiken von Schatten-KI herauszufinden und nicht genehmigte KI-Apps und Chatbots zu blockieren.“