

Cloudflare im Dienst des Gesundheitswesens

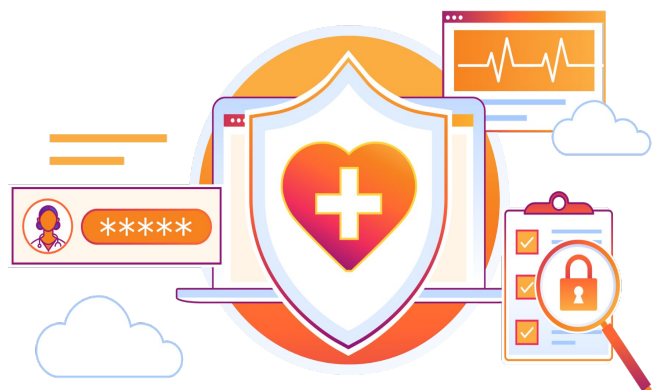
Patientendaten in verschiedenen Umgebungen schützen und eine verlässlichere virtuelle gesundheitliche Versorgung ermöglichen

Höhere Sicherheit und Geschwindigkeit für Ihre digitale Umgebung

Anbieter von Gesundheitsdienstleistungen haben im Digitalbereich große Ambitionen, sehen sich aber bei der Erreichung dieser Ziele mit zahlreichen Herausforderungen konfrontiert, um die sie nicht zu beneiden sind:

- Schutz ihrer Netzwerke vor wiederholten **Datenlecks** und Ransomware
- Ermöglichung **eines reibungslosen Anwendungszugriffs (teilweise aus der Ferne)** für diverse Drittanbieter unterschiedlichster Art
- Dauerhafte Gewährleistung einer zuverlässigen **virtuellen Betreuung** auch bei Angriffen und unvorhersehbarem Nutzerverhalten
- Schutz des Unternehmens – und Verwaltung seines zunehmend komplexeren IT-Stacks während einer Expansion im Rahmen von **Fusionen und Übernahmen**

In einem gewissen Umfang steht der Erreichung aller dieser Ziele ein Verlust der Kontrolle über die digitale Umgebung im Wege oder anders ausgedrückt: die Schwierigkeit, eine wachsende Panoplie an Anwendungen, Clouds, Nutzern, Geräten, Netzwerkinfrastrukturen und mehr zu verwalten.



Die **Connectivity Cloud** von Cloudflare kann dabei helfen, Ordnung in dieses digitale Wirrarr zu bringen. Es handelt sich um eine übergreifende Plattform mit cloudnativen Sicherheits- und Verbindungsdiensten, die alles ortsunabhängig schützen, vernetzen und beschleunigen. Sie unterstützen Dienstleister im Gesundheitswesen dabei, Patientendaten abzusichern, ein reibungsloses Funktionieren der Technik für medizinisches Personal zu gewährleisten und eine erstklassige virtuelle Versorgung zu ermöglichen – all dies mit größerer Flexibilität und Kontrolle.

Das bietet die Connectivity Cloud von Cloudflare Dienstleistern im Gesundheitssektor:



Hybride Einsetzbarkeit

Cloudflare-Dienste sind an keinen bestimmten Cloud-Anbieter gebunden und können auch mit lokaler Infrastruktur verwendet werden. Komplexe Umgebungen lassen sich über eine einzige Steuerungsebene verwalten. Jeder Sicherheits- oder Netzwerkdienst von Cloudflare kann über eine einzige Benutzeroberfläche oder API kontrolliert werden.



Bessere Bedrohungsdaten

Cloudflare analysiert riesige Mengen und diverse Arten von Traffic. Damit können wir die Erkenntnisse, die unseren Sicherheitsdiensten für Webanwendungen, Netzwerke und Zero Trust-Modelle zugrunde liegen, automatisch aktualisieren und Sie beim Schutz Ihrer Nutzer, Anwendungen und Daten unterstützen.



Geringere Kosten

Sie reduzieren Ihre Ausgaben für Sicherheit und IT und gewinnen außerdem an Agilität, wenn Sie kritische Dienste in unserer Connectivity Cloud zusammenführen. Cloudflare bringt laut der von Forrester durchgeführten „[Total Economic Impact](#)“-Studie bei einer Amortisationsdauer von weniger als sechs Monaten eine Investitionsrendite von 238 % über einen Zeitraum von drei Jahren.

Verfügbarkeit patientenseitiger Anwendungen vor Angriffen schützen

Cloudflare verhindert mit den folgenden Lösungen, dass bösartiger Traffic und Bots Ausfälle verursachen oder Anmeldeportale angreifen:

- **DDoS-Abwehr:** Dank unserer Netzwerkkapazität von mehr als 321 Tbit/s können wir selbst den größten und hartnäckigsten Angriffen automatisch standhalten.
- **Bot-Management:** Mit Telemetriedaten zu Bedrohungen von Millionen von Internetpräsenzen im Cloudflare-Netzwerk lassen sich die raffiniertesten Schadbots leicht blockieren.

Schnelle und zuverlässige digitale Dienste für Patienten

Cloudflare sorgt mit folgenden Produkten dafür, dass virtuelle Anwendungen im Gesundheitswesen stabil laufen:

- **Content Delivery Network:** Inhalte werden von unserem globalen Netzwerk mit mehr als 330 Städten zwischengespeichert und bereitgestellt.
- **Lastverteilung:** Datenverkehr wird auf smarte Weise über Hybrid-Cloud-Umgebungen verteilt. (Um jegliche Bedenken auszuräumen, bieten wir auch ereignisbasierten technischen Support, obwohl dieser nicht unbedingt notwendig ist.)
- **Smart Routing:** Cloudflare deckt rund 20 % des gesamten Web ab und nutzt die dadurch zur Verfügung stehenden Informationen, um dynamische Inhalte über die schnellsten Pfade zu leiten.
- **Medienübertragung:** Beim Videostreaming und Senden von Bildern erfolgt die Formatierung für verschiedene Browser und Verbindungsarten automatisch.

Außerdem lassen sich diese Dienste standardmäßig an jedem Standort unseres Netzwerks ausführen. Somit bieten wir eine hervorragende Performance überall auf der Welt ohne Bindung an bestimmte Dienste oder langwierige Umleitung des Datenverkehrs, die bei Anfragen von Kunden zusätzliche Latenz verursacht.

Patientendaten werden vor Offenlegung geschützt

Cloudflare schützt mit folgenden Funktionen Patientendaten vor ungewollter Offenlegung im Internet:

- **Web Application Firewall:** Cloudflare blockiert täglich Hunderte Milliarden Cyberbedrohungen. Die dabei erhobenen Telemetriedaten helfen unseren Machine Learning-Modellen, mehr Zero-Day-Sicherheitslücken und andere Bedrohungen mit geringerem manuellem Aufwand zu neutralisieren.
- **API Gateway:** Damit lassen sich mühelos Schatten-API aufspüren, die API-Nutzung überwachen und API-Nutzungsrichtlinien durchsetzen.
- **Page Shield:** Unsere Bedrohungsdaten können eingesetzt werden, um sich vor clientseitigen Angriffen zu schützen, die auf anfällige JavaScript-Abhängigkeiten abzielen.

Darüber hinaus helfen die **SASE-Dienste** von Cloudflare, unter anderem den Zugriff auf SaaS-Anwendungen, die Cloud-Nutzung, den E-Mail-Verkehr und Netzwerkschwachstellen zu schützen und zu überwachen. Die Lösungen kommen ohne VPN aus, welches die Nutzererfahrung beeinträchtigen und übermäßigen Netzwerkzugriff erlauben würde.

„Cloudflare sorgt dafür, dass unsere Patientendaten sicher sind, und hilft uns bei der Aufrechterhaltung unseres Netzwerkperimeters. So können wir uns darauf konzentrieren, Technologie bereitzustellen und das Vertrauen der Patienten zu wahren.“

Wisut Ua-Anant

Chief Digital MarTech Officer, Bumrungrad International Hospital

