CLOUDFLARE

WHITEPAPER

Hoffnung in Sicht: Stärkung der Cybersicherheit in wirtschaftlich unsicheren Zeiten

Inhaltsverzeichnis

Kurzfassung

Aufgrund der wirtschaftlichen Ungewissheit, mit der Unternehmen heute konfrontiert sind, schwindet auch ihre Planungssicherheit. Dies äußert sich oft in schrumpfenden Budgets und zwingt CIOs und Technikverantwortliche, neue Wege zu gehen.

Glücklicherweise können Führungskräfte dafür sorgen, dass sie für die Zeit nach den Umwälzungen gut aufgestellt sind, indem sie Budgets vorausschauend anpassen, Prozesse effizienter ausgestalten und Wachstumsziele erreichen, ohne die Ressourcen wesentlich aufzustocken.

In den folgenden Abschnitten werden wir die Faktoren herausarbeiten, die für die aktuellen Gegebenheiten und Marktbedingungen verantwortlich sind. Auf dieser Grundlage definieren wir anschließend fünf Schritte, mit denen Entscheidungsträger ohne Abstriche beim Sicherheitsniveau die Effizienz steigern können. Wenn Führungskräfte ihre Strategie im Bereich IT-Infrastruktur heute auf die neuen wirtschaftlichen Gegebenheiten abstimmen, stellen sie für ihre Unternehmen die Weichen für den Erfolg von morgen.

Einleitung

In den letzten Jahren hatten IT-Führungskräfte bei der Planung und Umsetzung ihrer Strategie eine Krise nach der anderen zu bewältigen. Sie mussten auf eine weltweite Pandemie und ihre Folgeerscheinungen, auf Lieferkettenengpässe, einen eskalierenden Konflikt in Osteuropa und zuletzt auf eine drohende Rezession reagieren. Um es mit den Worten des Stanford-Ökonomen Paul Romer zu sagen: „Es ist schrecklich, eine Krise zu verschwenden.“ (Quelle)
Die Entscheidungen, die CIOs hinsichtlich der Unterstützung ihrer Remote-Mitarbeitenden getroffen haben, werden langfristige und unbeabsichtigte Vorteile mit sich bringen, da sie diese Arbeitsplätze durch die Ermöglichung mobiler Arbeit attraktiver gemacht haben. Auch die aktuell im Kontext sich eintrübender Wirtschaftsaussichten getroffenen Entscheidungen in Bezug auf Sicherheit, Netzwerke, Fernzugriff, Speicher, Entwicklung und Infrastruktur werden dazu beitragen, dass sie aus dem Abschwung gestärkt hervorgehen und danach besser für ein nachhaltiges Wachstum gerüstet sein werden.

Die Zunahme mobiler Arbeit führte auch zu einem Boom bei Ransomware und komplexen Cyberbedrohungen, die neue Maßstäbe hinsichtlich Umsatzauswirkungen, Umfang und Raffinesse setzen (Quelle). Die Schwächung dessen, was vom Netzwerkperimeter übrig geblieben war, führte in Verbindung mit einer überdurchschnittlich hohen Personalfluktuation zu Sicherheitslücken und Verzögerungen bei der Umsetzung strategisch bedeutsamer IT-Projekte. Dies zwang die Unternehmen, nicht nur ihre Herangehensweise bei der Einstellung und Bindung von Mitarbeitenden zu überdenken, sondern auch bei der Kontrolle des Zugriffs auf ihre Systeme und Geräte. Die Pandemie brachte zwar einen dramatischen Anstieg der Internetkriminalität mit sich (Quelle), aber sie führte Unternehmen und ihren Vorständen auch die Dringlichkeit effektiver Cybersicherheitslösungen vor Augen. Die Zeit ist jetzt reif für eine strategischere Herangehensweise, im Rahmen derer auf lange Sicht eine besser geschützte, produktivere und in höherem Maße verfügbare hybride Arbeitsinfrastruktur geschaffen wird.

Wir präsentieren fünf Maßnahmen, mit denen Sie das Risiko für Ihre Firma reduzieren und Ihr Unternehmen besser auf die neuen Bedrohungen vorbereiten können, die sich gerade abzeichnen:

1. Vorhandene Sicherheitstools zur Erkennung von Überschneidungen überprüfen

Unternehmen profitieren erheblich von einer Konsolidierung ihrer IT-Sicherheitsdienstleister. Zwar kann kein einzelnes Tool jemals die von CISOs ersehnte „Universallösung“ sein, doch viele Sicherheitsverantwortliche glauben, dass ihr Unternehmen Geld für Programme vergeudet, die keinen optimalen Schutz bieten. Wenn Unternehmen verschiedene Programme von mehreren Anbietern nutzen, verschwenden ihre Mitarbeitenden wertvolle Zeit. Denn sie müssen die Tools beschaffen, implementieren und verwalten, Fehler beheben und mit einer großen Zahl unverbundener Systeme arbeiten, anstatt Infrastruktur und Daten abzusichern. Tatsächlich ergab eine Umfrage auf der RSA-Jahreskonferenz im Juni 2022, dass „die Hälfte (53 %) der befragten Unternehmen das Gefühl hat, mehr als 50 % ihres Cybersicherheitsbudgets verschwendet zu haben und Bedrohungen immer noch nicht abwehren zu können. 43 % der Umfrageteilnehmer sehen die größte Herausforderung beim Erkennen und Neutralisieren von Gefahren in der viel zu großen Menge an Tools, während 10 % der Unternehmen keine effektiven Werkzeuge für die Beseitigung von Cybersicherheitsbedrohungen besitzen.“ (Quelle) Wird auch nur eine Handvoll dieser Instrumente abgeschafft, erhöht sich dadurch die Sicherheit und gleichzeitig sparen die Mitarbeitenden Zeit.

Wenn man den Schwerpunkt von langfristigen auf kurzfristige Investitionen verlagert, verbessert sich damit sofort der Cashflow. Zudem wird die Festlegung auf mehrjährige Investitionen vermieden, die die geschäftliche Flexibilität einschränken. Eine Möglichkeit zur Vereinfachung besteht darin, die Abhängigkeit von herkömmlicher Hardware zu verringern. Die Umstellung von lokalen Servern auf „As a Service“-Lösungen kann dazu beitragen, dass vorrangige Initiativen auch bei Budgetkürzungen weiterhin finanziert werden. Mit einem „As a Service“-Modell profitiert man außerdem von den kürzeren Innovationszyklen, während das unvermeidliche und umständliche Patching veralteter Hardware entfällt. Dank schnellerer Innovationen und des Auslagerns der Fehlerbehebung können sich die Mitarbeitenden wieder auf die Aktivitäten konzentrieren, die das Unternehmen eigentlich ausmachen. In unsicheren Zeiten führen strategische Vereinfachung und Konsolidierung zum langfristigen Erfolg.

2. Fokus von Tools auf Daten ausweiten

Führungskräfte sollten erwägen, den Fokus zu verlagern. Denn wenn sie nicht nur die Tools selbst, sondern auch die Daten der Gesamtheit ihrer Sicherheitswerkzeuge besser integrieren, lassen sich Muster und Anomalien auf effizientere Weise zutage befördern. Früher haben IT-Sicherheitsteams kontinuierlich immer weitere Tools hinzugefügt, ohne zu berücksichtigen, wie sich ein Zuviel an Datensätzen an zu vielen Orten auf lange Sicht auswirkt. Das Ergebnis ist oft ein Flickenteppich von Produkten mit wenig bis nicht vorhandener Interoperabilität und schwer zu sichtenden Daten. Dadurch erhöhen sich die Gelegenheiten für menschliche Fehler, was die gewonnenen Erkenntnisse weniger belastbar und ungenauer macht. Von der für das Zusammenführen von Datensätzen und die Durchführung von Abfragen vergeudeten Zeit und den verschwendeten Ressourcen ganz zu schweigen. Diese Ressourcen könnten stattdessen für Geschäftsinitiativen mit größerer strategischer Bedeutung eingesetzt werden.

Zwar lassen sich durchaus kreative Lösungen für Interoperabilitätsprobleme finden, z. B. das manuelle Zusammenführen von Datensätzen oder der Import und Export von CSV-Dateien. Aber von der Effizienz einmal abgesehen liegt der Wert von Sicherheitstools in den Daten, die diese Systeme verarbeiten, erstellen und für diejenigen bereitstellen, die für die Gefahrenabwehr zuständig sind. Sind die Daten überall verstreut (und werden sie nicht klassifiziert, abgesichert und sorgfältig verwaltet), werden dadurch ansonsten aufschlussreiche Erkenntnisse verfälscht – vor allem, wenn Daten in nicht berücksichtigter Schatten-IT angesiedelt sind. Wenn verschiedene Werkzeuge konsolidiert werden und man sorgfältig auf die Interoperabilität des Sicherheitsstacks achtet, sinkt die Wahrscheinlichkeit für menschliche Fehler und die Daten sind besser geschützt. Denn selbst mit den besten der heute verfügbaren Tools führen isolierte und in Schatten-IT verborgene Datensätze dazu, dass die gewonnenen Erkenntnisse von schlechterer Qualität sind.

Im Hinblick auf Effizienz muss bedacht werden, wozu ein Zuviel an Tools im Zeitalter von Zero Trust führt. Zero Trust bedeutet „niemals vertrauen, immer verifizieren“. Mit einer größeren Zahl von Tools brauchen Ihre Mitarbeitenden daher länger, um sich bei Systemen anzumelden, zu authentifizieren und darauf zuzugreifen, bevor sie überhaupt mit ihrer Arbeit beginnen können. Je geringer die Zahl an Systemen, mit denen die Beschäftigten in Berührung kommen, desto mehr Zeit sparen und desto schneller arbeiten sie. Unbedingt bedacht werden sollte, dass die Daten in diesen Systemen und die Anzahl der Systeme, auf die die Mitarbeitenden zur Bearbeitung einer bestimmten Aufgabe zugreifen müssen, letzten Endes darüber entscheiden, ob Teams zeitnah und zielführend Maßnahmen gegen Bedrohungen ergreifen können, anstatt einfach nur darauf zu reagieren.

3. Cloud- und „As a Service“-Modelle für maximale Innovationskraft und geringstmögliche Komplexität einsetzen

Zum Erhalt der Wettbewerbsfähigkeit ist Innovation erforderlich. Ein Unternehmen, das nicht im Cybersicherheitsgeschäft tätig ist, hat es schwer, beim Thema Sicherheit auf dem Laufenden zu bleiben. Dafür fehlen die Zeit, das Budget oder die Ressourcen. Solche Firmen kennen weder die neuesten Schwachstellen und Risiken (Common Vulnerabilities and Exposures – CVEs) oder Angriffstrends, noch wichtige Patches, mit denen die Sicherheit der gesamten Infrastruktur gewährleistet wird. Mit „As a Service“-Modellen (wo immer möglich) profitieren Entscheidungsträger von kontinuierlichen Innovationen, und dies ohne Kompromisse oder schwierige Entscheidungen in Bezug auf technische Schulden.

Zu bedenken ist auch, dass einige Sicherheitsservices Gebühren für das Überschreiten von Traffic-Obergrenzen erheben und andere für die Bandbreite. Empfehlenswert ist zudem ein genauer Blick darauf, was ein Unternehmen monatlich oder jährlich zahlt. Vielleicht ist es mehr, als den Entscheidungsträgern bewusst ist. In einem solchen Fall könnte nach Lösungen ohne Überschreitungsgebühren gesucht werden. So wird nicht nur Geld gespart, sondern Ausgaben lassen sich langfristig zuverlässiger kalkulieren, was eine bessere Zukunftsplanung ermöglicht.

Cloud-Dienste dieser Art geben Unternehmen außerdem Spielraum, um zu wachsen und zu schrumpfen. Denn sie verpflichten sich nicht zu teurer Hardware und dem damit verbundenen mühsamen Lifecycle-Management. In Zeiten der Ungewissheit müssen Unternehmen agil bleiben und auf veränderte Marktbedingungen reagieren können. Bei begrenztem Cashflow ist die Fähigkeit, Kosten zu verringern oder ganz einzusparen, ein strategischer Vorteil, der den Unterschied zwischen knappem Überleben und Erfolg ausmachen kann – unabhängig von der aktuellen Marktlage.

4. Nutzererlebnis von Mitarbeitenden verbessern

Forbes schreibt: „Unsere Umfrage hat ergeben, dass komplexe, mehrstufige Anmeldeprozesse Mitarbeitende frustrieren, ihre Zeit verschwenden, ihre Produktivität beeinträchtigen und sie dazu veranlassen, wichtige arbeitsbezogene Aufgaben aufzugeben. […] Die größte Ironie dabei ist, dass fast 40 % der Arbeitnehmenden sagen, sie hätten die Einrichtung neuer Sicherheitsapps für die Arbeit wegen mühsamer Anmeldeprozesse aufgeschoben, delegiert oder gänzlich vermieden. Das ist so, als würde man sein Haus mit dem stabilsten, höchsten und sichersten Tor schützen, das sich für Geld nur kaufen lässt, und noch einen laserspeienden Drachen davor postieren – nur um es nachts unverschlossen zu lassen.“ Für diejenigen, die für die digitale Verteidigung zuständig sind, ist es ineffizient und schwer nachzuvollziehen, welches Tool welche Funktion erfüllt. Ein Übermaß an Dashboards und Speicherorten für Daten schafft in jedem Unternehmen große Sicherheitsrisiken und blinde Flecken. Firmen, die Cybersicherheitsbedrohungen immer einen Schritt voraus sein wollen, müssen wissen: Jeder Klick und jeder Tastenanschlag kostet wertvolle Zeit, Energie und Konzentration. Diese fehlen dann bei der Reaktion auf kritische Ereignisse. Für eine bessere und effizientere Mitarbeitererfahrung muss die Unternehmensleitung genau prüfen, wie viele Tools für eine effektive Verteidigung wirklich benötigt werden. Was lässt sich abschaffen oder konsolidieren, damit einem schwerwiegenden Sicherheitsvorfall schneller begegnet werden kann, anstatt einfach nur darauf zu reagieren?

Auch mobile Mitarbeitende außerhalb des Technikbereichs und ohne Verteidigungsrolle steigern Ihre persönliche Produktivität gerne mit Schatten-IT oder Umgehungsmethoden. Zero Trust-Kontrollen sind zwar insbesondere in einem Remote-Kontext vielversprechend für die Stärkung der Unternehmenssicherheit, aber nicht alle Zero Trust-Ansätze sind gleich. Je komplizierter der Zugang zu den benötigten Tools, desto wahrscheinlicher finden Angestellte einen Weg, die Sicherheitskontrollen zu umgehen. Führungskräfte sollten sich also nicht nur mit der Wirksamkeit von Sicherheitsprodukten befassen, sondern auch auch deren Benutzerfreundlichkeit achten. Denn wer die Nutzererfahrung der Mitarbeitenden nicht berücksichtigt, erhöht das allgemeine Risiko für das Unternehmen.

5. Nach Sicherheitsservices suchen, die die Netzwerkperformance nicht beeinträchtigen

Es geht nicht nur um die Tools selbst, sondern auch darum, wie diese konfiguriert und verwaltet werden, denn das macht manchmal den Unterschied. Gegebenenfalls sollten die aktuellen Konfigurationen und Anpassungen geprüft werden, weil sich dadurch möglicherweise die Performance noch erhöhen lässt. Ist keine Steigerung mehr möglich, sollte nach Lösungen gesucht werden, die von Anfang an auf Performance ausgelegt sind. Denn wer sich erst nachträglich dahingehend Gedanken macht, erreicht selten das erhoffte Ziel. Wenn es um die Performance eines Netzwerks geht, kann eine schlechte Architektur nicht im Nachhinein „umprogrammiert“ werden. Genauso wie sich die Baupläne eines Gebäudes nur begrenzt überarbeiten lassen, wenn das Fundament erst einmal steht, müssen auch Netzwerke von Grund auf für ein Höchstmaß an Performance konzipiert werden.

Ein internationales Edge-Netzwerk, bei dem Daten möglichst nah an ihrem Ursprung verarbeitet werden, bietet Unternehmen sowohl in der Gegenwart als auch für die Zukunft einen strategischen Vorteil. Im MIT Technology Review heißt es: „Die Verarbeitung großer Datenmengen kann zu Performanceproblemen führen. Als Reaktion darauf greifen viele Unternehmen auf das Edge-Computing zurück, das Daten nah an ihrem Ursprung verarbeitet. Dies ermöglicht schnelle Analysen und Reaktionen in Echtzeit, während gleichzeitig die Anforderungen an Datenschutz und Sicherheit eingehalten werden.“ (Quelle) Wer sich für Lösungen entscheidet, die bereits auf den Architekturen von morgen aufbauen, verschafft seinen Mitarbeitenden den strategischen Vorteil einer besseren Netzwerk-Performance und opfert dafür weder Datenschutz noch Sicherheit.

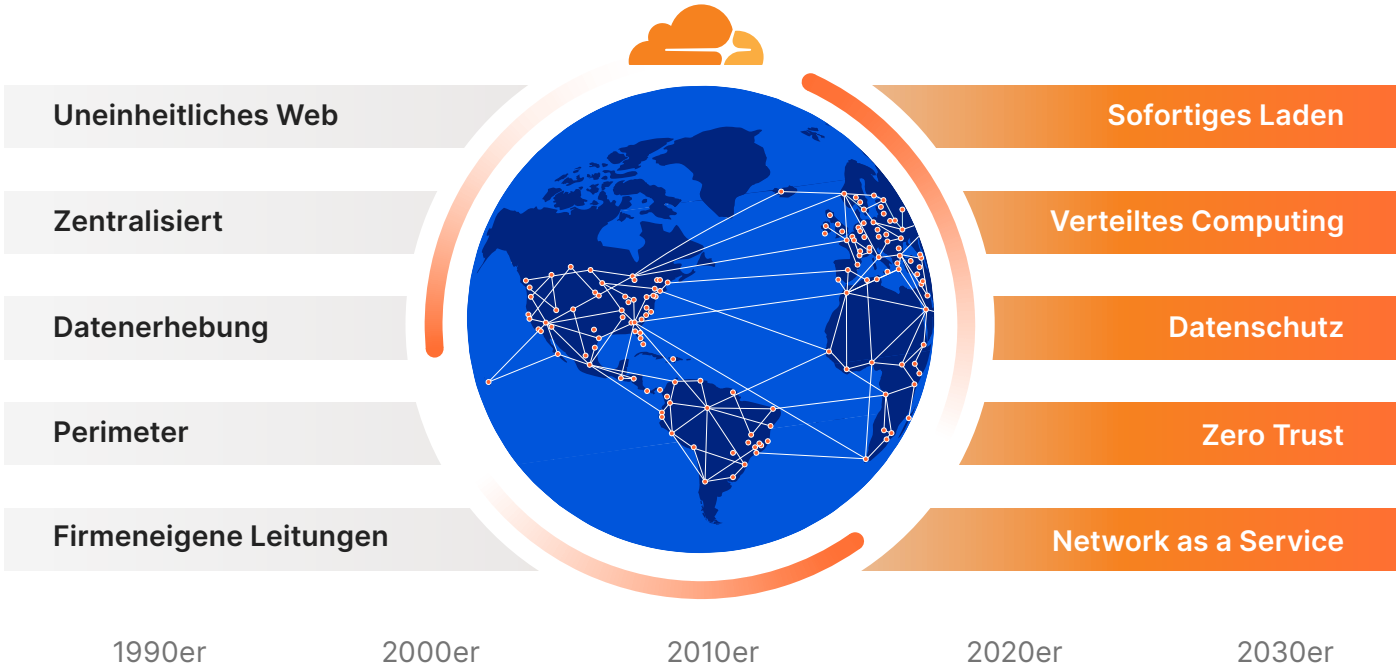
Hier noch einmal die Schritte im Überblick, mit denen sich die Cybersicherheit in unsicheren Zeiten steigern lässt:

1. **Vorhandene Sicherheitstools zur Erkennung von Überschneidungen überprüfen**
   - Konsolidieren überlappender Tools
   - Verlagern von langfristigen auf kurzfristige Investitionen
2. **Fokus von Tools auf Daten ausweiten**
   - Eine Interoperabilität von Tools sorgt für höhere Belastbarkeit und Genauigkeit von Daten
   - Präzisere Datensätze und Berichte ermöglichen wertvollere Erkenntnisse, die für das Erreichen geschäftlicher Ziele entscheidend sind
3. **Cloud- und „As a Service"-Modelle für maximale Innovationskraft und geringstmögliche Komplexität einsetzen**
   - Wenn Unternehmen nicht auf Cybersicherheit spezialisiert sind, profitieren sie von der Auslagerung von Fehlerbehebung, Wartung und Upgrades auf „As a Service"-Angebote
   - Cloud- und „As a Service"-Modelle bieten die nötige Flexibilität für agiles Handeln in einem wechselhaften wirtschaftlichen Kontext
4. **Nutzererlebnis von Mitarbeitenden verbessern**
   - Eine zu große Anzahl von Tools an zu vielen Orten schafft blinde Flecken bei der Sicherheit und frustriert Mitarbeitende – ihr Nutzererlebnis lässt sich aber durch eine Konsolidierung und Vereinfachung verbessern
   - Mehr Benutzerfreundlichkeit erhöht die Mitarbeiterbindung und Angestellte greifen bei der Erledigung ihrer Aufgaben seltener auf Schatten-IT zurück
5. **Bei aktuellen Cybersicherheitslösungen nach versteckten Kosten und Potenzial zur Performancesteigerung suchen**
   - Vorhandene Tools sollten daraufhin überprüft werden, ob sich die Performance noch verbessern lässt, wobei eine schlechte Architektur nicht nachträglich optimiert werden kann
   - Mit Tools, die für den globalen Maßstab entwickelt wurden und sich in größtmöglicher Nähe zum Standort der Endkunden befinden, können Unternehmen ein erstklassiges und sicheres Kundenerlebnis bieten

Der Mehrwert von Cloudflare

Cloudflare wurde 2010 in der Zeit nach der Wirtschaftskrise des Jahres 2008 gegründet, um den Wechsel von On-Premise-Infrastruktur zur Cloud voranzutreiben. Wir haben die Plattform von Cloudflare mit dem kühnen Ziel entwickelt, ein besseres Internet zu schaffen. Die Produkte von Cloudflare schützen und beschleunigen alles, was mit dem Internet verbunden ist, ohne dass Hardware hinzugefügt, Software installiert oder eine Zeile Code geändert werden muss.

Bei mit Cloudflare betriebenen Websites erfolgt das Routing des gesamten Traffics über unser intelligentes globales Netzwerk, das mit jeder Anfrage hinzulernt. Wir helfen unseren Kunden, auf smartere Weise zu arbeiten, ihre Produkte besser und schneller zu entwickeln und auf sichere Weise zu wachsen. Cloudflare schützt und beschleunigt heute Millionen von Websites.



Kontrolle

Profitieren Sie von der Leistungsfähigkeit eines integrierten globalen Netzwerks, das umfassende Konnektivität, Sicherheit und Rechenleistung bietet und Ihnen die Kontrolle über die Richtlinien überlässt.

Flexibilität

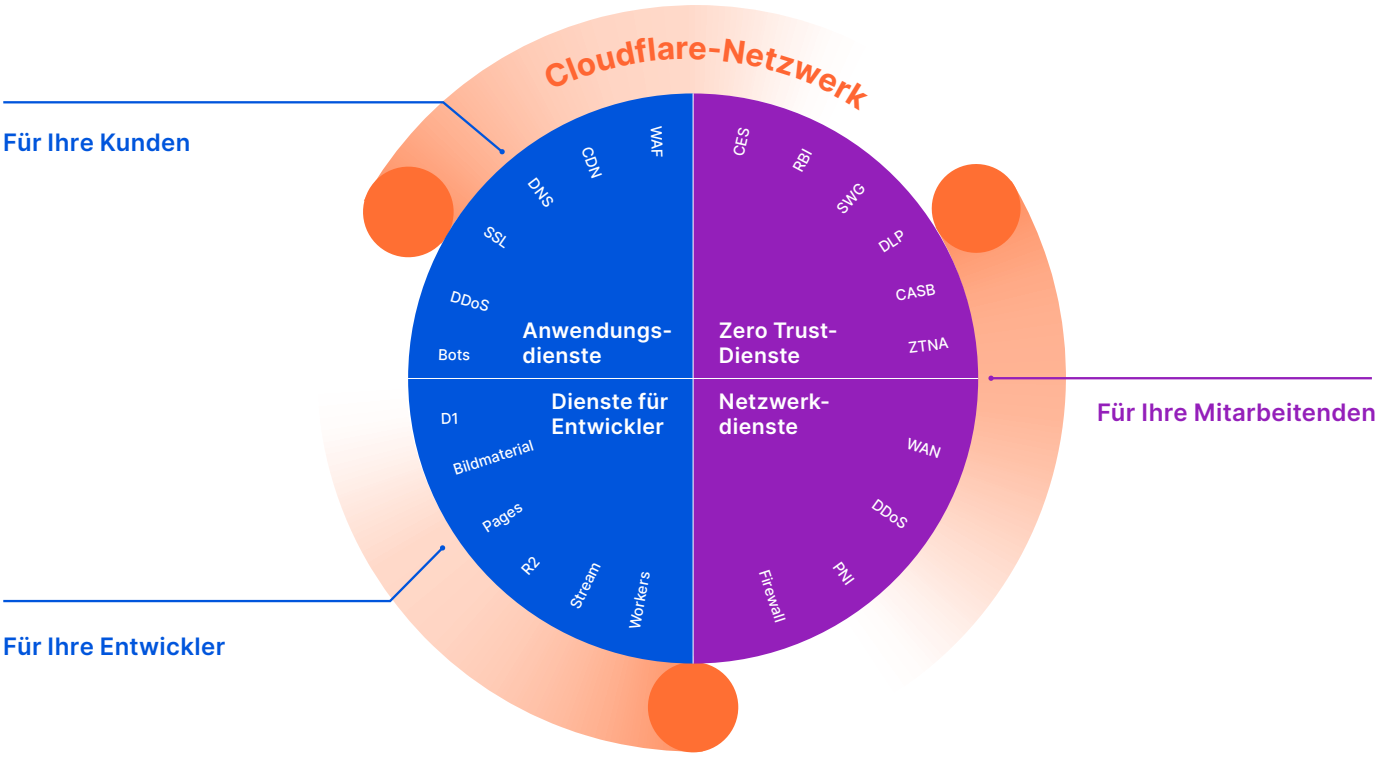
Cloudnative Dienste bedeuten, dass keine Vorabinvestitionen erforderlich sind. Sie können die Nutzung je nach aktuellem Geschäftsbedarf mühelos erhöhen oder verringern.

Planungssicherheit

Transparente und vorhersehbare Rechnungen – ohne unerwartete Kosten wie z. B. unbegrenzte Gebühren für ausgehenden Datenverkehr. Keine Notwendigkeit, jetzt Investitionen für Hardware zu tätigen, die erst nächstes Jahr geliefert wird.

Cloudflare bietet ein weltweites Netzwerk für sichere, vertrauliche, schnelle und zuverlässige Internetverbindungen mit jedem Gerät.

- **Absicherung** von Websites, APIs und Internetanwendungen
- **Schutz** von Unternehmensnetzwerken, Mitarbeitenden und Geräten
- **Erstellung** und **Bereitstellung** von Code, der an der Netzwerk-Edge ausgeführt wird



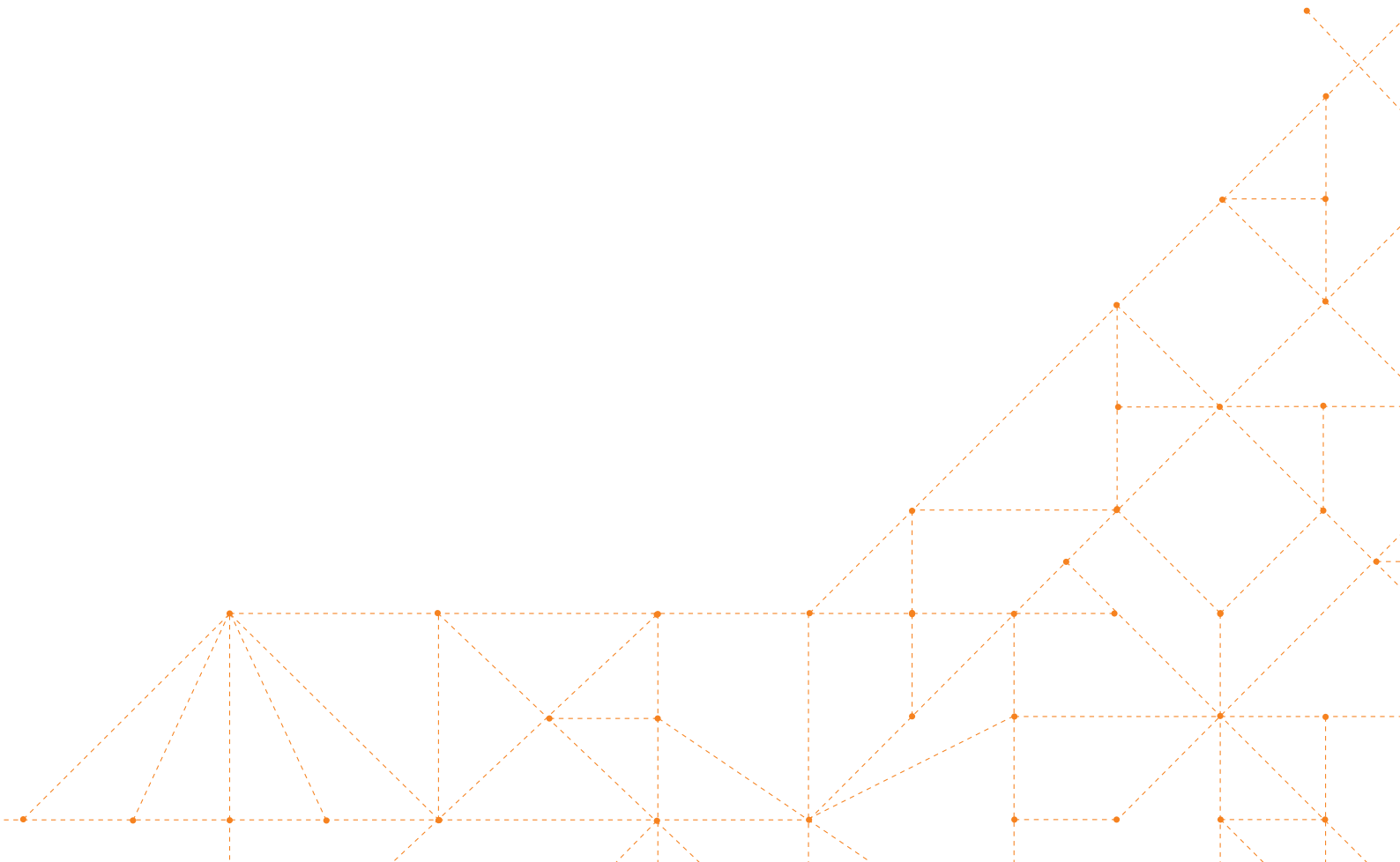
Unsere Plattform

Über Cloudflare

Cloudflare wurde im Jahr 2010 gegründet, um die Verlagerung von On-Premise-Infrastruktur in die Cloud voranzutreiben. Wir haben die Cloudflare-Plattform von Grund auf entwickelt – im vollen Bewusstsein, dass wir ein sehr ehrgeiziges Ziel verfolgen: den Aufbau eines besseren Internets. Die Cloudflare-Produktsuite schützt und beschleunigt jede Internetanwendung, ohne dass Hardware hinzugefügt, Software installiert oder eine Zeile Code geändert werden muss.

Bei mit Cloudflare betriebenen Internetpräsenzen erfolgt das Routing des gesamten Traffics über ein intelligentes globales Netzwerk, das mit jeder Anfrage hinzulernt. Wir helfen unseren Kunden, smarter zu arbeiten, ihre Produkte besser und schneller zu entwickeln und auf sichere Weise zu wachsen. Cloudflare schützt und beschleunigt heute Millionen von Internetpräsenzen.

Mehr erfahren Sie unter www.cloudflare.com/de-de/



CLOUDFLARE

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

REV:BDES-4327.2023MAR10