

Zukunftssichere IT-Sicherheit im Gesundheitswesen

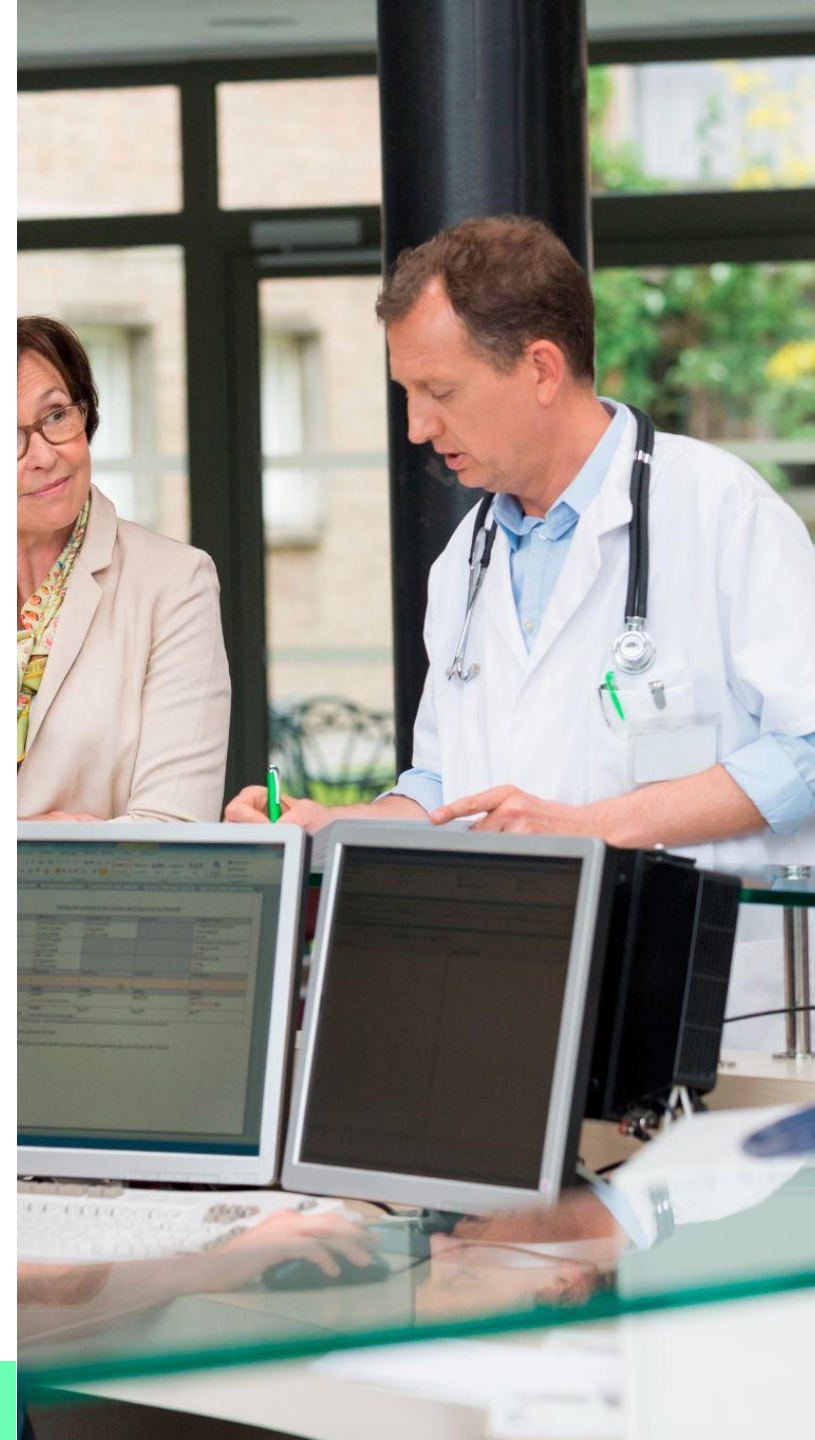
Armin Becker
Markus Ocker

Februar 2025



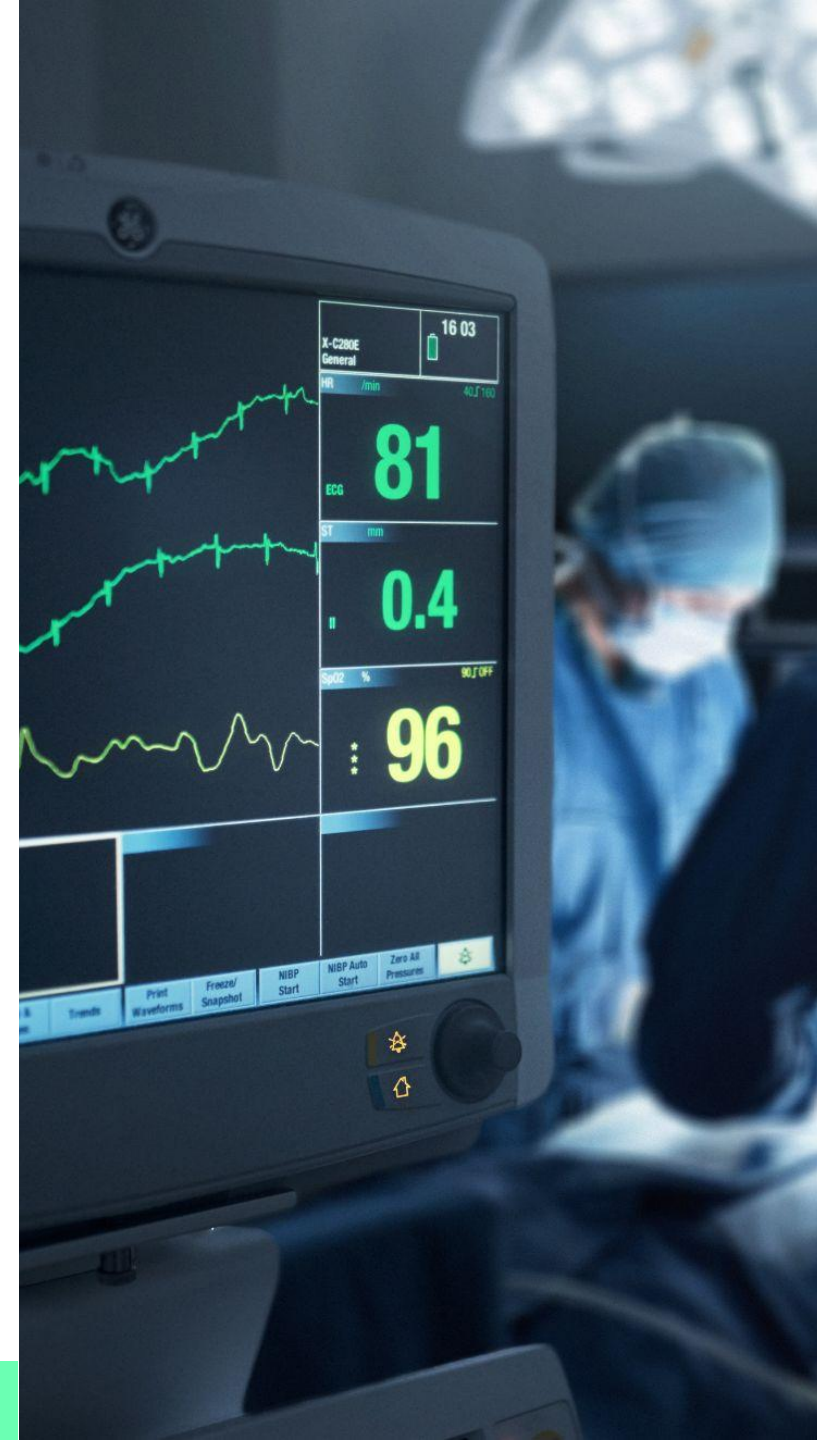
Agenda

1. Herausforderungen im Gesundheitswesen
2. Zscaler im Überblick & Kritis
3. Anwendungsfälle
4. Kundenbeispiel



Herausforderungen im Deutschen Gesundheitswesen

- Bereitstellung einer **BSIG** konformen Infrastruktur (KRITIS, ISO Konformität für Medizingeräte)
- **SICHERE** Elektronische Patientenakte (ePA, E-Rezept)
- Sichere **Vernetzung** des Gesundheitswesens
- **Traditionelle Infrastruktur** und Softwarelandschaft (auch Medizinprodukte)
- **Zukauf, Schließung** und **Zusammenlegung** von Häusern mit langen Laufzeiten und einer hohen Komplexität
- Zunehmende Verbreitung von **Telemedizin** und mobilen Arbeitsplätzen
- **KI/ML- gestützte Systeme** in der Forschung & Diagnostik
- Die fortschreitende Digitalisierung erhöht die **Angriffsfläche**, dadurch häufiger **Sicherheitsvorfälle**, incl. Gefahr durch Abfluss von **Patientendaten**





Allgemeine Bedrohungslage

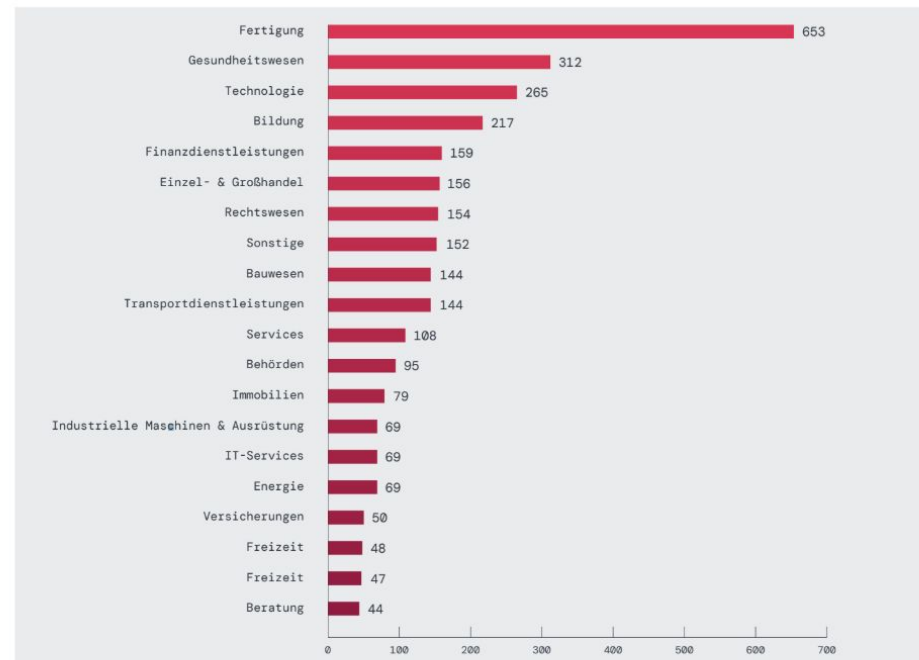
Medizinprodukte sind ein beliebtes Ziel für Cyberkriminalität. Mit 150 Schwachstellen in Medizinprodukten (Stand 2020 BSI). Laut [Zscaler Threatlabz aus 2024](#) ist die Gesundheitsbranche unter den Top 10 auf Platz 2.

Es zeigt: Patientendaten sind ein sehr wertvolles Gut

Branchen, die am stärksten von Ransomware betroffen sind

Top 10 Branchen mit den meisten Ransomware-Angriffen, basierend auf Data Leak-Websites

1. Fertigung
2. Gesundheitswesen
3. Technologie
4. Bildung
5. Finanzdienstleistungen
6. Einzel- & Großhandel
7. Rechtswesen
8. Sonstiges
9. Bildungswesen
10. Transportdienstleistungen



2024 Zscaler, Inc. All rights reserved

Missing Link: Ransomware-A

Krankenhäuser gefährden Me

Erste Untersuchungen in den USA zeigen, dass Ra
Sterblichkeit von Patienten negativ beeinflussen l



(Bild: Ground Picture/Shutterstock.com)

28.01.2024, 08:00 Uhr Lesezeit: 9 Min.

Von Imke Stock

BR24 Bayern

Bayern

22.1

Na

Zeh
Lan
mel

Von

Übe

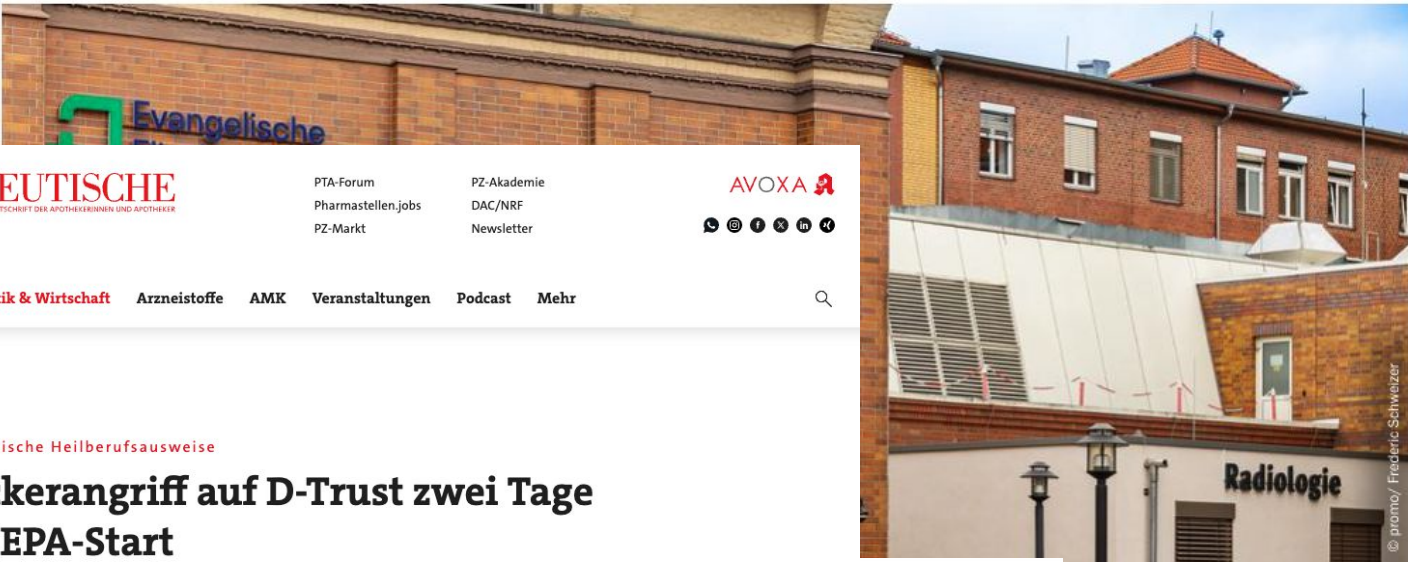
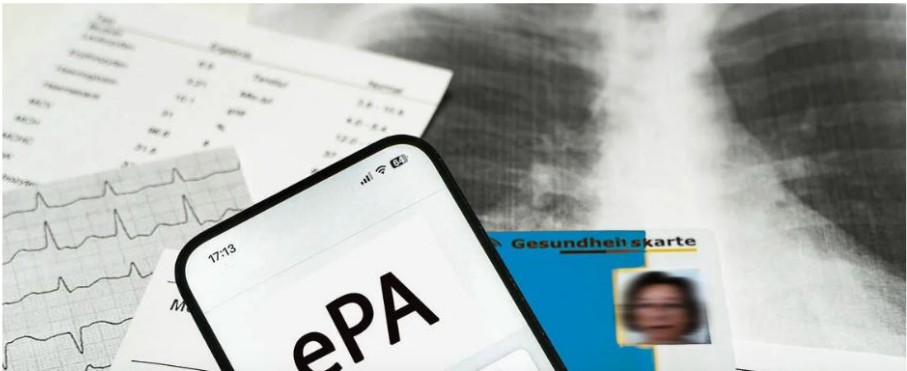
Elektronische Heilberufsausweise

Hackerangriff auf D-Trust zwei Tage vor EPA-Start

Kurz vor dem Start der Testphase für die elektronische Patientenakte (EPA) haben Hacker vorige Woche den Dienstleister, der elektronische Heilberufsausweise ausgibt, angegriffen. Die Gematik geht davon aus, dass sich dies nicht auf die Sicherheit der Telematikinfrastruktur (TI) auswirkt. Ob Bundesgesundheitsminister Lauterbach vor dem EPA-Start von der Attacke wusste, bleibt unklar.

Cornelia Dölger 20.01.2025 14:00 Uhr

f x in x w e p SEITENINHALT



Anmelden ABO



nesstift uft stabil“

ers angegriffen.
e Situation.

n Visier isen an

weise
ern für
sen sein.

Zscaler im Überblick & KRITIS



Digitales Gesundheitswesen erfordert Transformation



Neue Geschäftswelt

Nutzung disruptiver Technologien, um **agiler und wettbewerbsfähiger** zu werden



Mobilität



Cloud



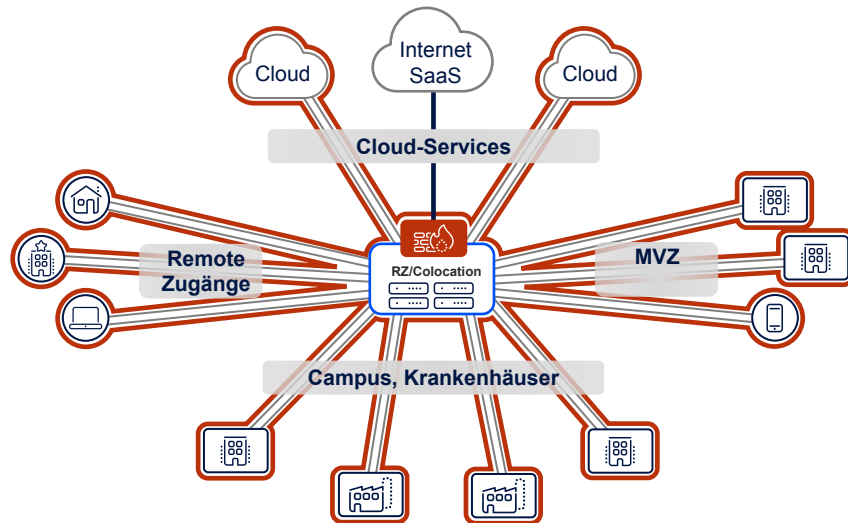
IoT/OT



KI/ML

klassische Netzwerk- und Sicherheitsarchitekturen werden zum Risiko.

Traditionelle Netzwerk- und Firewall-Architektur



Ein vertrauenswürdiges privates Netzwerk verbindet alles

Sicherung des Netzwerks mit Perimeter-Firewalls

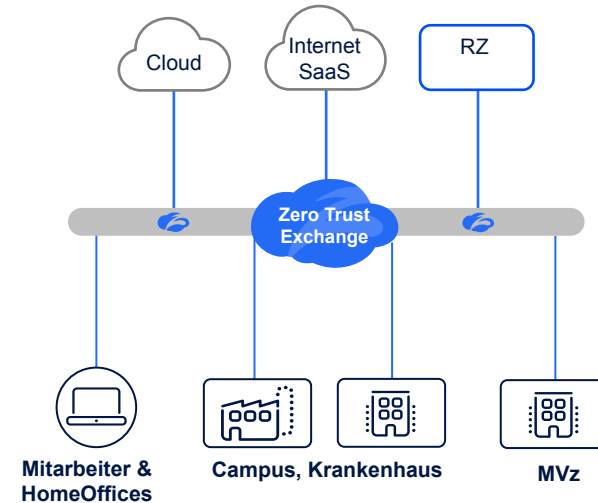
Funktionierte früher gut, wird **jetzt aber zum Risiko**

Hohe Kosten, Sicherheitsrisiko, schlechte User Experience

Eine neue Cyber-Architektur
ist Notwendig



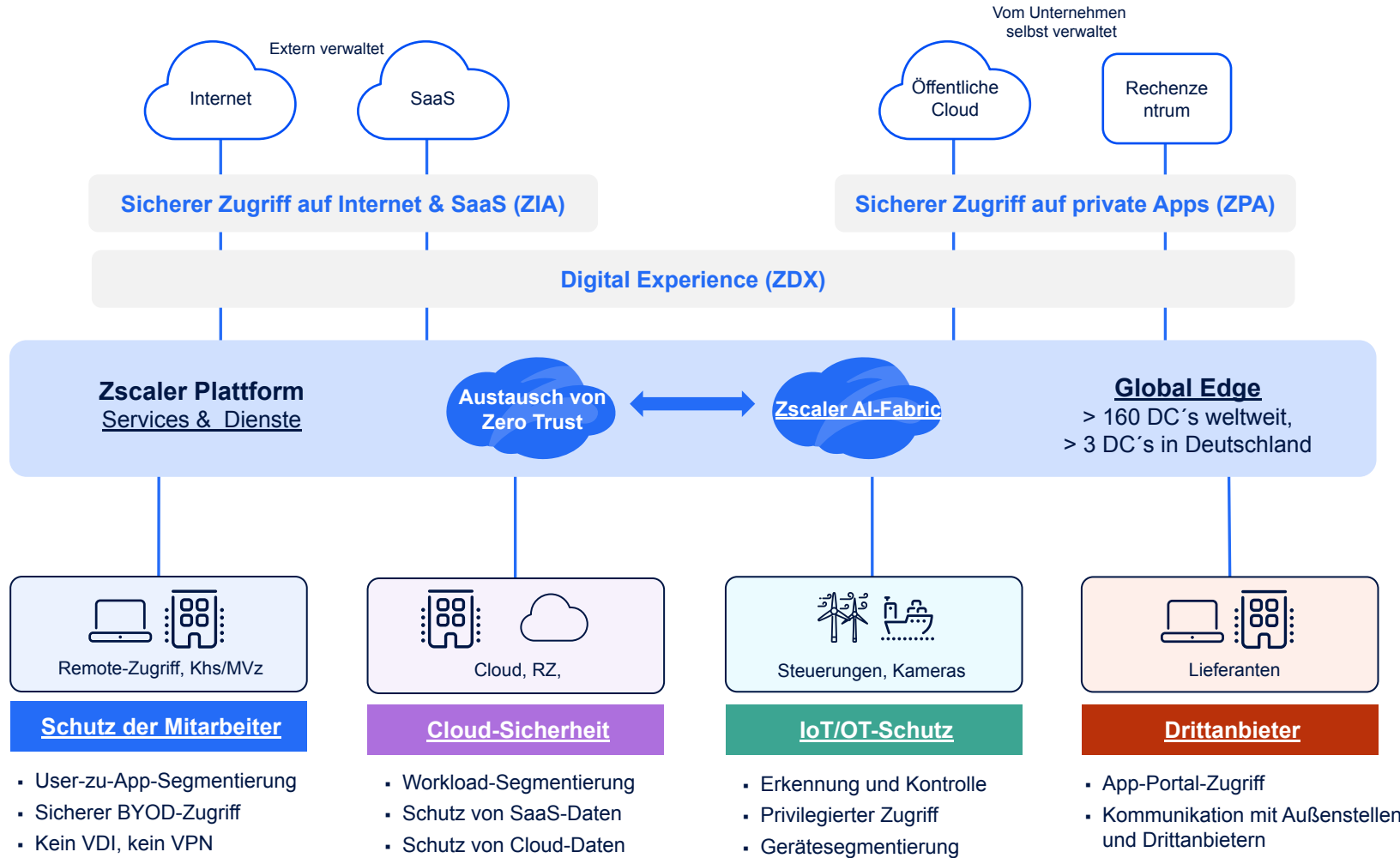
Die Zscaler-Vision: Eine neue Architektur für Netzwerke und Sicherheit



Schaltzentrale zur Verbindung von Usern, Geräten und Workloads
über jedes Netzwerk anhand von Business-Policies

**Reduzierte Betriebskosten, Erhöhung der Sicherheit,
hervorragende User Experience**

Integrierte Plattform sichert vier kritische Bereiche



Speziell entwickelte Zero-Trust-Architektur

Mandantenfähige Architektur

Gewährleistet Performance + Skalierbarkeit

PolicyNow™: Änderungen werden in Echtzeit umgesetzt

Von Grund auf Widerstandsfähig

- Einzige Security Cloud mit Business Continuity Planning und Disaster Recovery

Schutz Ihrer Daten

Verschafft Konformität für DSGVO, BSIG, NIS, KRITIS und andere Datenschutzvorschriften

Vier Kernlösungen

Schutz vor Cyberbedrohungen

Schutz der Daten

Zero Trust Networking

Risikomanagement

Integrierte & umfassende Lösungen



Schutz vor Cyberbedrohungen

Keine Kompromisse und lateralen Bewegungen

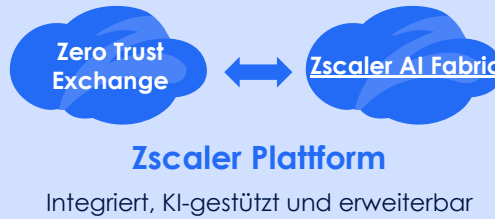
- AppCloaking™ (Angriffsfläche minimieren)
- Inline-Bedrohungsschutz (Kompromittierung verhindern)
- **Segmentierung (Laterale Bewegungen verhindern)**
- Schützt die gesamte Kommunikation vor Bedrohungen



Schutz der Daten

Verhindert Datenverluste - inline & via API

- **Daten schon bei der Übertragung sichern**
- **Sichere SaaS-, Cloud- und Endgerätedaten**
- Schutz für BYOD ohne VDI
- Sicherer Einsatz von generativer KI



Zero Trust Networking

Verbindung mit Anwendungen statt Netzwerken

- Sichere Kommunikation mit Zweigstellen und Fabriken
- Sichere Kommunikation mit der Cloud
- **Sichere Kommunikation mit IoT/OT**
- End-to-End-Performance



Risikomanagement

Visibilität und Handlungsempfehlung zur Reduzierung des Gesamtrisikos

- **Risikobewertung (Risk360™)**
- **Vereinheitlichtes Schwachstellenmanagement**
- Angriffsflächen-Management
- Vorhersage von Sicherheitsverstößen

Was die Zscaler-Plattform reduziert

~~Ausgehende DMZ~~
Sicheres Web-Gateway, Firewall/IPS

~~Eingehende DMZ~~
VPN, VDI, DDOS, Load Balancers

~~Private Netzwerke~~
SD-WAN, MPLS, ExpressRoute usw.

~~Endpoint Agents~~
NAC, VPN, DLP, Monitoring

Reduzierung, Simplifizierung, Standardisierung und Automatisierung: Alisa Chung, ehemalige Shell CIO

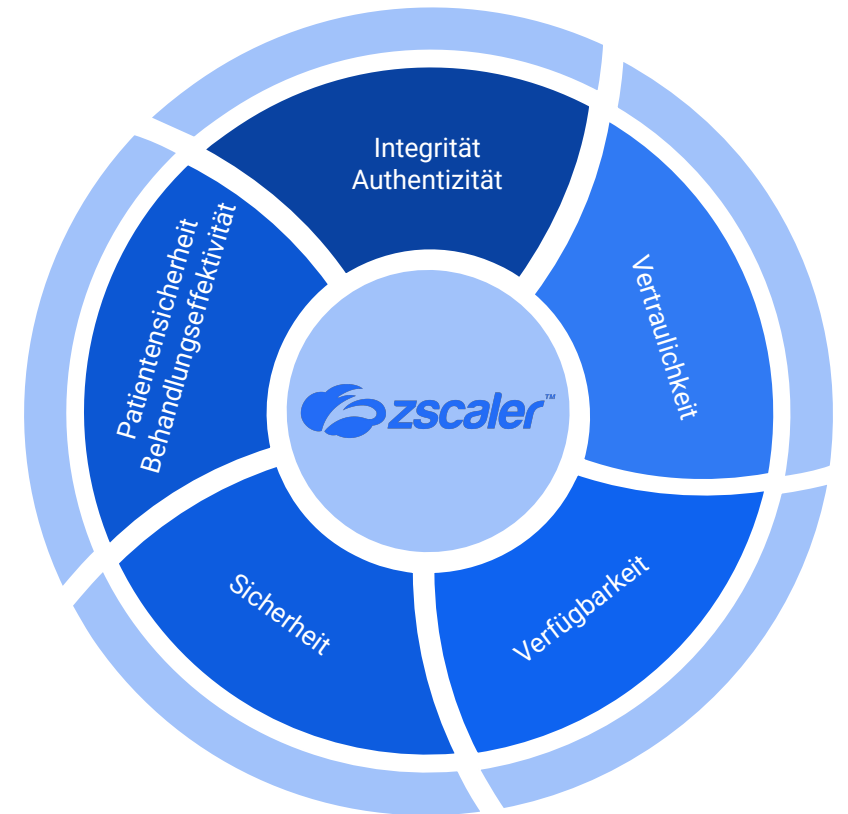
Integrität/Authentizität: Eindeutige Identität der Benutzer und Durchsetzen von Unternehmensrichtlinien

Vertraulichkeit: Schutz von sensiblen Dokumenten und Patientendaten durch Zscaler Data Protection

Verfügbarkeit: Verteilte Multimandantenarchitektur. Zusätzliche Verfügbarkeit und Handlungsfähigkeit durch eine lokale Instanz im eigenen Rechenzentrum

Sicherheit: Sicherer und effizienter Zugriff auf alle Anwendungen (Web, SaaS, Cloud, On-Premises) von jedem Endgerät und Standort. Cyberattacken werden durch einen VPN-losen Zugriff und Abwehrtechniken wie SSL Inspection, Sandboxing, Browser Isolation, Advanced Threat Protection uvm. sichergestellt

Patientensicherheit/Behandlungseffektivität: Ein ganzheitliches Monitoring der Sicherheit und Benutzererfahrung stellt eine hohe Produktivität sicher und ermöglicht Ärzten und Pflegekräften mehr Zeit am Patienten



KRITIS Anforderungen



Zscaler unterstützt in vielen Bereichen des Anforderungskataloges um einen Betrieb einer kritischen Infrastruktur nach §8a Absatz 1 BSIG herstellen zu können



Nummer	Referenz	Zscaler
2.1	Informationssicherheitsmanagementsystem (ISMS)	✓
2.2	Asset Management	✓
2.3	Risikoanalysemethode	✓
2.4	Continuity Management	✓
2.5	Technische Informationssicherheit	✓
2.6	Personelle und organisatorische Sicherheit	✓
2.8	Vorfallserkennung und Bearbeitung	✓
2.9	Überprüfung im laufenden Betrieb	✓

Verweis: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html

Zertifizierungen



Wir investieren in den Deutschen Markt

Zertifizierungen



BSI C5



ISO 27001



ISO 27701



SOC 2



Sensitive Data
Handling
Assessment



DCSO



FedRAMP-High



- **Zertifizierungen und Testate für BSI C5, ISO 27001 und ISO 27701 (Voraussetzungen, um den IT-Grundschutz und die DSGVO einzuhalten)**
- **160+ Rechenzentren weltweit, davon 4 in Deutschland (2x Frankfurt, 1x München, 1x Düsseldorf) ermöglichen digitale Souveränität**
- **200 Zscaler Mitarbeiter in Deutschland. Weltweiter 24x7x365 Support.**

Anwendungsfälle



Schutz der Patientendaten



SaaS Daten

CASB

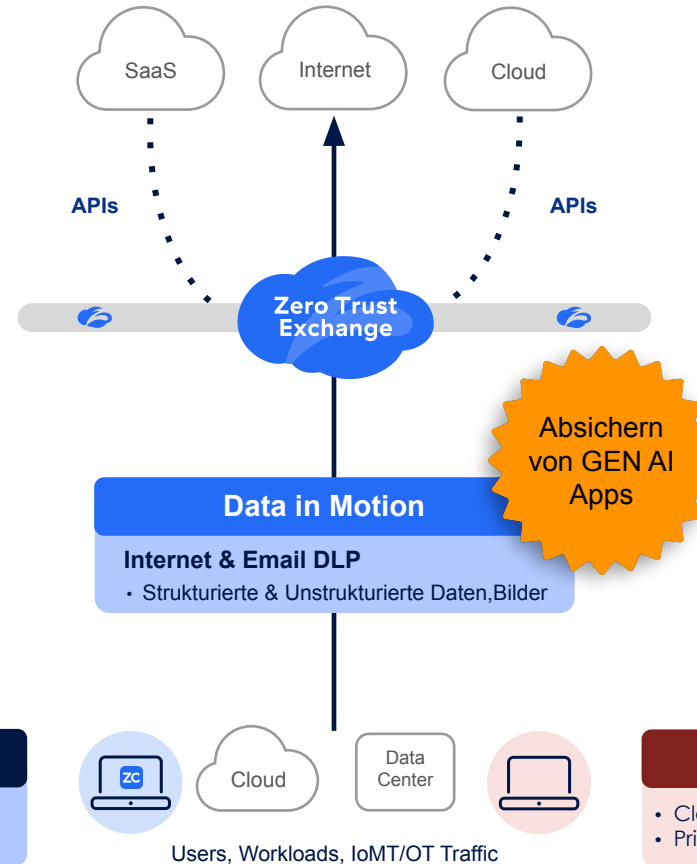
- Shadow IT / unsichere Applikationen
- Collaboration (Teams/Zoom)

SSPM

- Schutz vor falscher Konfiguration, setzen falscher Berechtigungen, compliance

SaaS Versorgungskette

- Sichere SaaS zu SaaS Integration



Data at Rest

Service und Data Discovery

- Storage Einheiten, VMs, Datenbanken
- Sensible Patienten

Posture Control

- Berechtigungen, Fehlkonfiguration, Schwachstellen, Zugriffsverhalten
- Berechtigungen, Fehlkonfiguration

Actionable Insights

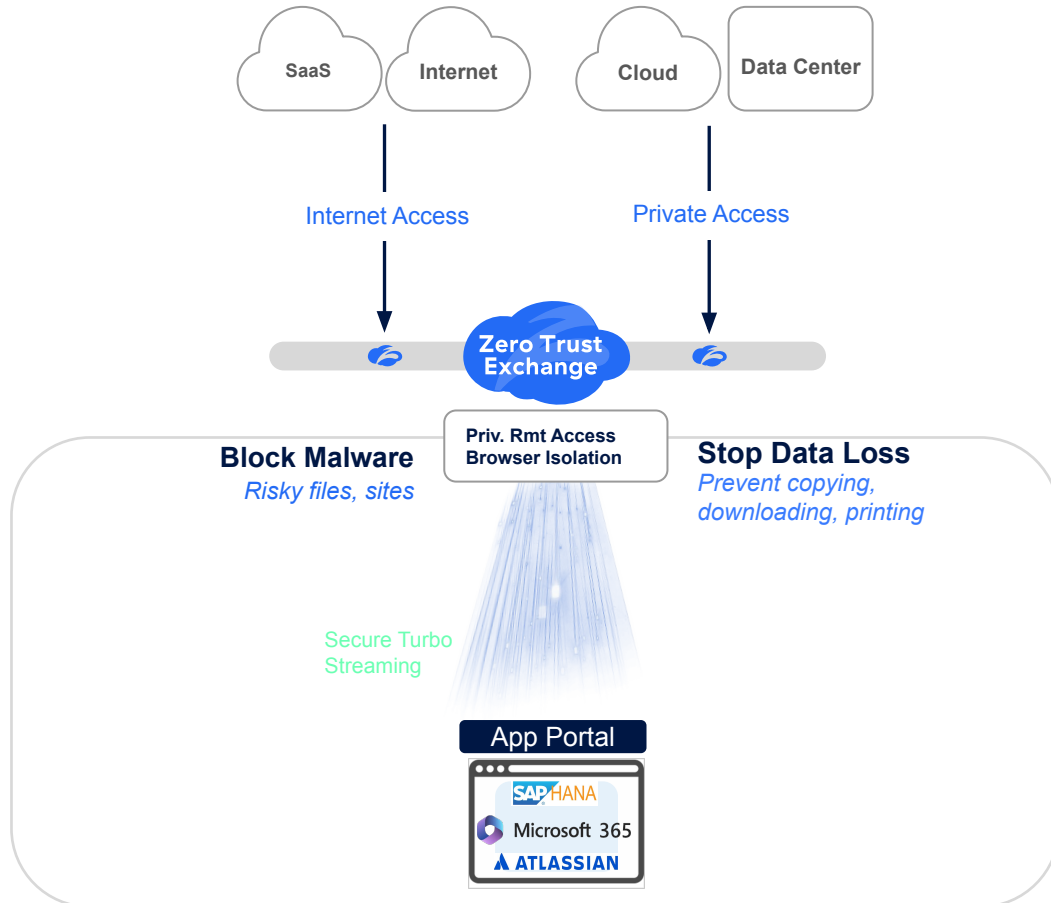
- Korrelieren, Priorisieren, und automatisch Beheben

Reduktion der Punktprodukte
Verringerung der Kosten, Komplexität und des Risikos

Automated AI data discovery & Classification
Schnell ausgerollt und einfach zu verwalten

Automation einer Vorfallsmeldung
Benutzerschulung und Eskalation

Zugänge für Drittanbieter und Remote Zugriffe



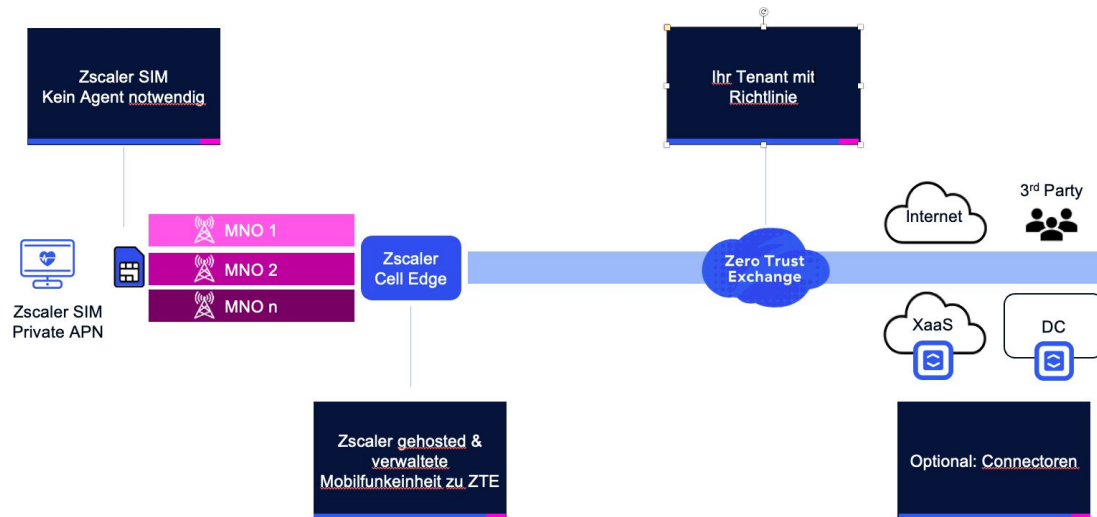
Herausforderung

- Die Geräte benötigen **Zugriff auf sensible Daten** wie z.B. KIS oder Wartungszugriff auf Telemedizin (PACS/Schnellschnitt)
- Außerhalb der **Kontrolle** der Krankenhaus IT
- Traditionell mit VDI oder Drittanbieter Lösungen (**kostenintensiv und komplex**)

Lösung

- **Zscaler Zero Trust Zugriff** mit **Browser Isolation** und agentenlosen Zugriff auf SaaS-/Private-Apps
- Verhindert das Herunterladen von **Malware** oder **sensiblen Daten** auf das Endgerät
- **Privilegierter Fernzugriff** über eine Portallösung (SSH/RDP)

Medizingeräte mit 5G (Z-SIM) und Fernwartung



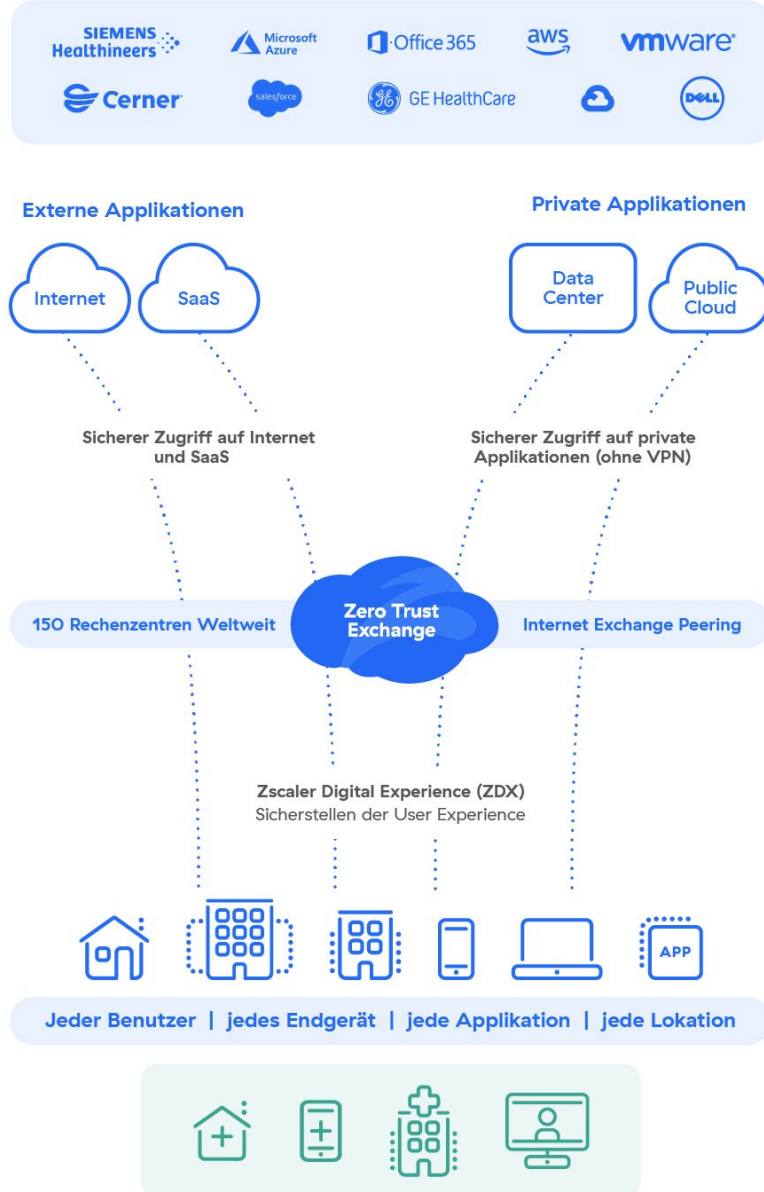
Herausforderung IoMT

- **Investitionsschutz** und damit Nutzung veralteter Betriebssysteme wie z. B. embedded OS
- Medizingeräte dürfen **nicht eigenständig** gewartet werden
- **Unzureichend geschützte** Fernzugriffe

Lösung

- Anbindung an **Zero Trust Exchange**
- Bereitstellung eines **privilegierten Fernzugriffs**
- **Durchsetzung** der Unternehmensrichtlinien
- **Sichtbarkeit** durch Analyse der Authentifizierung
- **Eingrenzung** eines Betriebes auf Ebene des Krankenhausgeländes durchsetzbar

Zusammenlegung & Schließung von Häusern und Integration von MVZs



Herausforderung

- **Integration** bestehender Architekturen sehr komplex
- Schaffen von **sicheren Zugriffsmöglichkeiten**
- In MVZs fehlt Infrastruktur (Netzwerk, Server, Backup)
- **Teure** Leitungsanbindung und erhöhter Einsatz von Hardware
- **Lange Laufzeiten** und umfangreiche Projekte (1-2 Jahre)

Lösung

- Zscaler **Zero Trust Exchange** benötigt nur eine Identität (iDP)
- **Sichere und schnelle Anbindung** der Standorte über Connectoren
- **Verringerung der Integrationszeiten** (Wochen/wenige Monate)
- **Reduktion von Hardware** (VPN/Firewall/MPLS etc.)

Kundenbeispiel



Schritt 1

Reduzierung von Infrastruktur & Bandbreite / Einheitliche Nutzung der aktuellen Lösungen / Vorbereitung für mehr SaaS (e.g. M365)

Schritt 2

Ablösung VPN Lösungen / Einführung einer rollenbasierten Zugriffssteuerung (Zero Trust) / Schnelle Integration von Arztpraxen & BYOD

Schritt 3

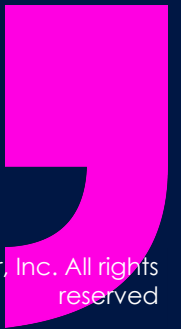
Rollenbasierte Zugriffssteuerung (Zero Trust) egal wo der User ist / Schnelle Integration von Drittanbietern & Zusammenlegung von Häusern/ Reduzierung von MPLS durch Internet-only Standorte

Schritt 4

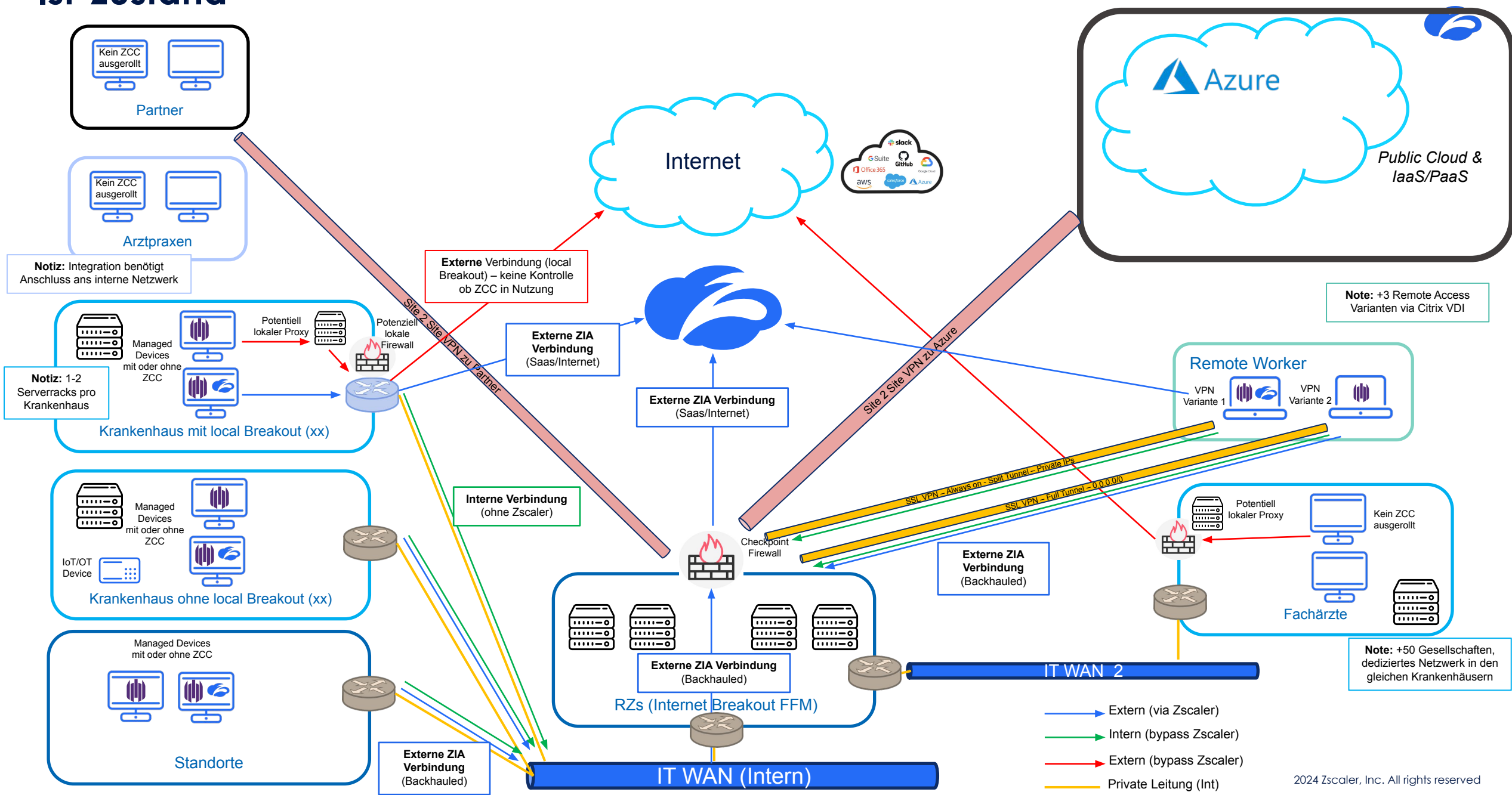
Erweiterung von Zero Trust auf Workloads & IoMT/ Unterstützung von Cloud Smart / Reduzierung von Administrations- und Update-Tätigkeiten / Arbeiten wie im Internet Cafe



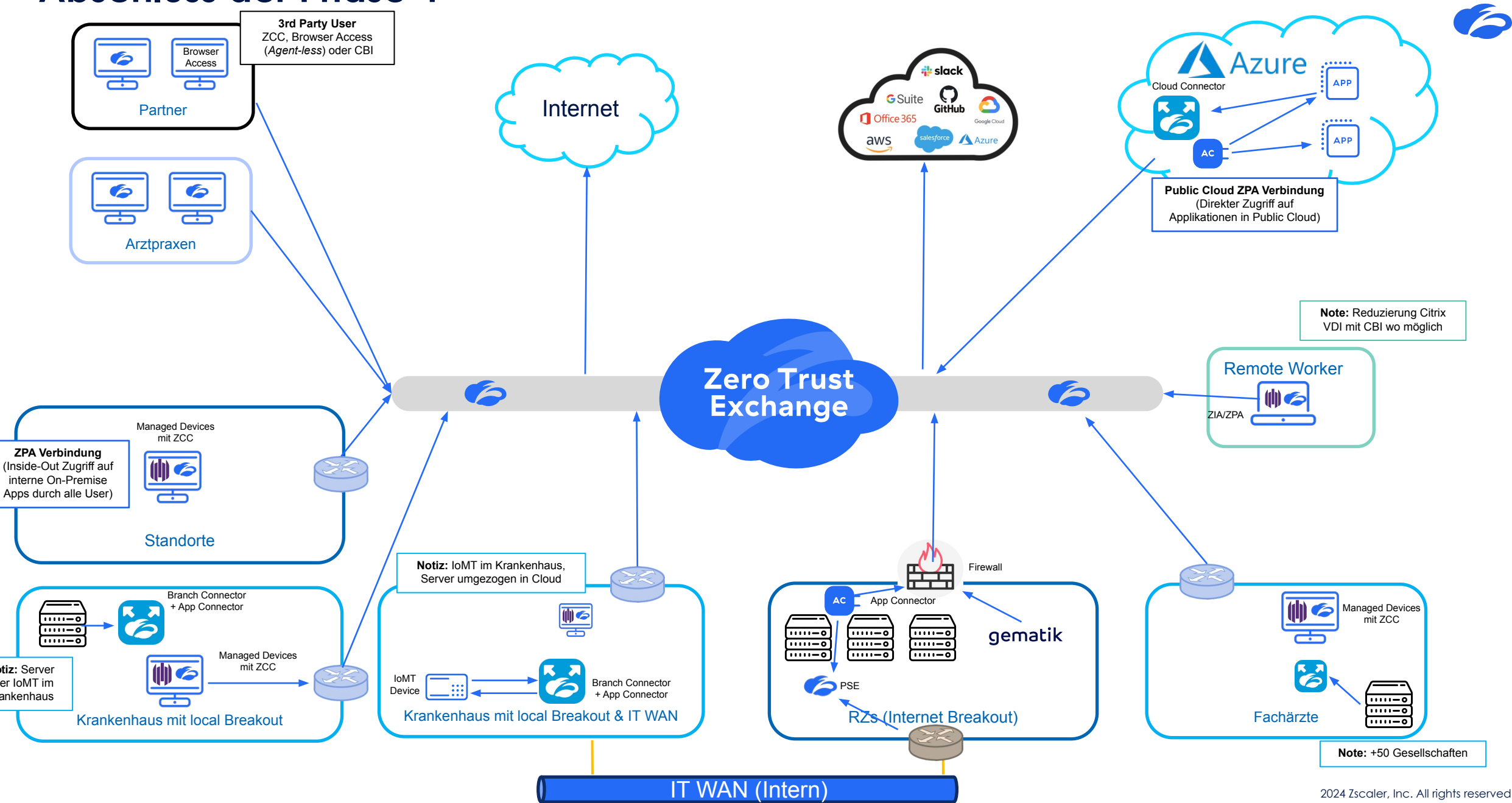
Die Transformation in 4 Schritten



Ist-Zustand



Abschluss der Phase 4



Ihre Anforderungen, unsere Antworten



Schutz vor Cyberangriffen

- Reduzieren der Angriffsfläche. Verbindung des Benutzers mit der Anwendung und nicht mit dem Netzwerk
- Verbindungen von außen nicht sichtbar
- Schutz der Patientendaten vor unbefugten Zugriff (Data Protection)

Erschließung von neuen Anwendungsfällen

- Anbindung von gängigen Systemen in der Telemedizin, Remote Radiologie, Remote Monitoring, IoMT/OT (Medizingeräte)
- Sichere Einbindung AI-gestützter Cloudlösungen wie Google Health uvm.

Reduzieren der Infrastrukturkosten und schnelle Integration weiterer Standorte (M&A)

- Reduktion von Kosten und Komplexität durch Einsparung von Hardware und Netzwerkadministration
- Schnelle Integration weiterer Krankenhäuser, MVZs, Arztpraxen und Reha Einrichtungen

Optimierung der Benutzererfahrung

- Sicherer Zugriff für Ärzte, Pflegepersonal, Patienten und externe Anbieter. Unabhängig von der Ressource, Endgerät oder Standort
- IT Transparenz für den Krankenhausbetrieb und damit mehr Zeit am Patienten

Weiterführendes Material



Absicherung medizinischer Endgeräte in medizinischen Einrichtungen

Wie Sie mit Zscaler sensible
Patientendaten schützen und Ihre
Security auf ein neues Level heben



Gesundheitsversorgung

Durch Zero Trust Schatten-IT in der Medizintechnik vorbeugen

17.01.2025 · Ein Gastbeitrag von Markus Ocker · 7 min Lesedauer ·

Die Vernetzung medizinischer Geräte bietet Chancen, erhöht jedoch die Sicherheitsrisiken, z. B. durch veraltete Betriebssysteme und eine unzureichende Verschlüsselung. Mit einer Zero-Trust-Sicherheitsplattform sind sowohl die Krankenhaus-IT als auch die Patientendaten sicher.



Das Interesse der Malware-Akteure am Gesundheitswesen steigt.
(© deimos.az – stock.adobe.com / KI-generiert)



SOLUTIONS CONSULTING
WHITE PAPER

Zero Trust im Gesundheitswesen

Keine Kompromisse bei der
Sicherheit von Medizintechnik

Verfasser

Markus Ocker, Solution Engineer Public Sector, Zscaler
Mark Rosche, Transformation Architect, Zscaler

Ausgabe 1.0 | Dezember 2024

©2024 Zscaler, Inc. Alle Rechte vorbehalten.

2024 Zscaler, Inc. All rights reserved

Chancen und Innovationen für das
moderne Gesundheitswesen

Treffen Sie Zscaler auf der DMEA 2025

Besuchen Sie uns an unserem Stand:
Halle 04 Stand C-103



DMEA
Berlin • 8–10 April 2025
Connecting Digital Health



Fragen?

Lösungen bei einem Katastrophenfall für Behörden



Blackout (RZ Ausfall oder Verbindung)

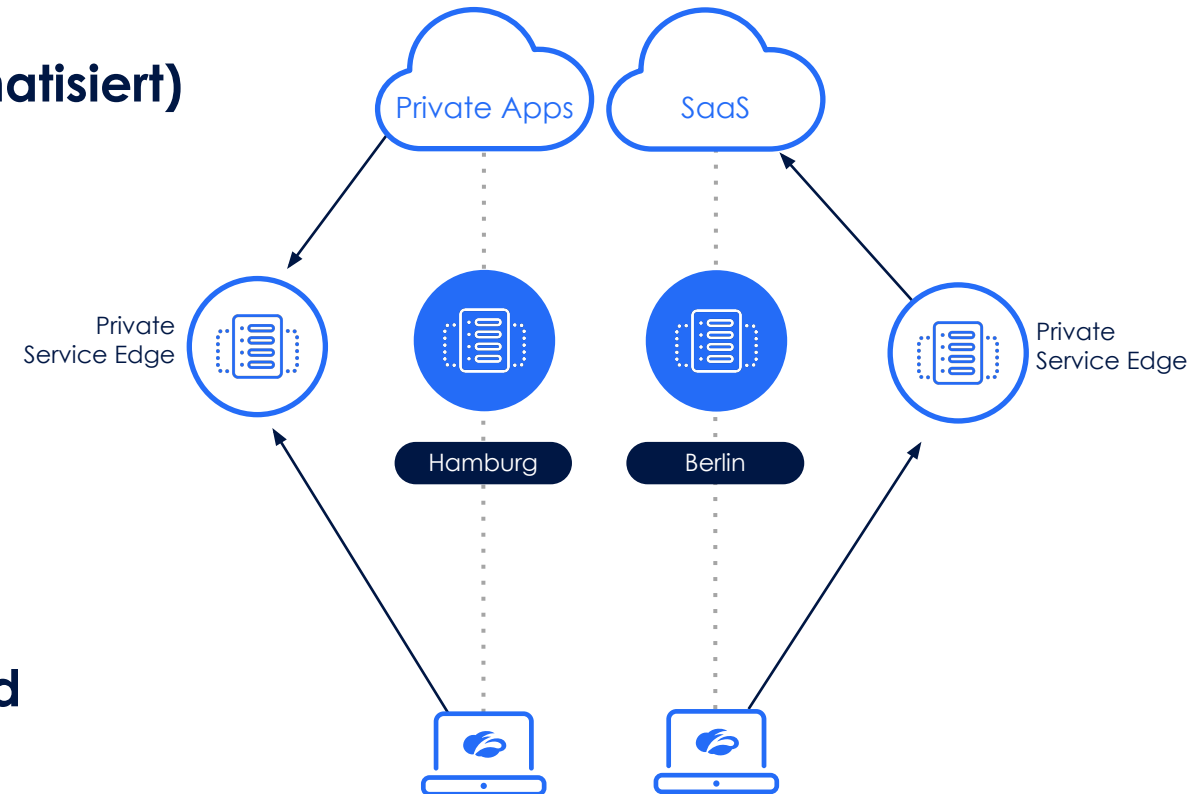
- Failover von WAN Routen (Manuell oder automatisiert)
- Client Connector Auto Failover

Brownout (Hot Cluster/Verbindung)

- Dynamische Standortwahl nach Leistung und Verfügbarkeit
- Lastenausgleich

Katastrophenfall (Ausfall der Cloud/Verbindung)

- Aufrechterhaltung des Betriebs
- Trennung von physischer Umgebung und Cloud
- Failover auf die private Infrastruktur

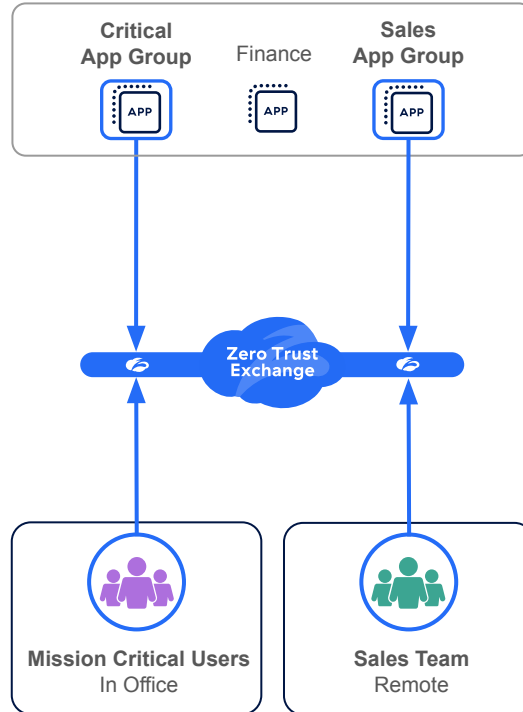


Hohe Verfügbarkeit und Verlässlichkeit



Benutzer Segmentierung

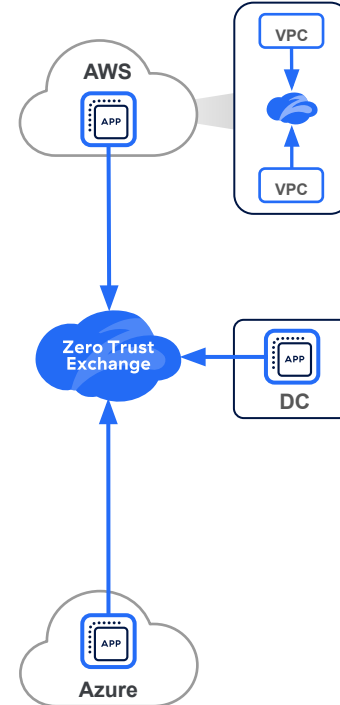
Remote, Im Office



Only Mission Critical Users can access Critical Apps
Sales Team can only access Sales Group Apps

Workload Segmentierung

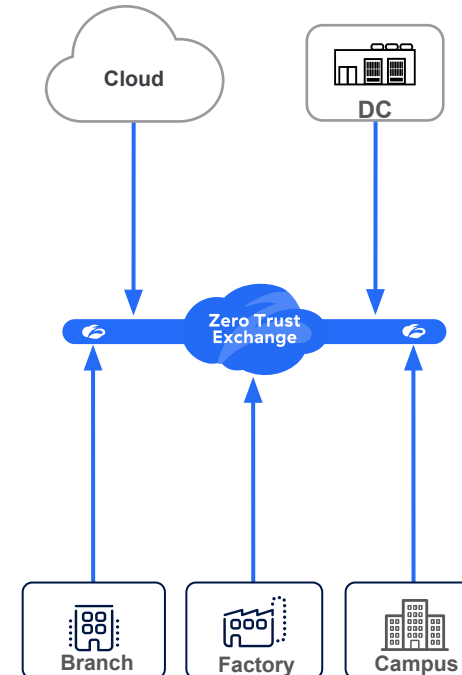
Cloud, DC, Branch



VPC to VLAN
VPC to VPC / VNET
Workload to Workload

Branch/Campus Segmentierung

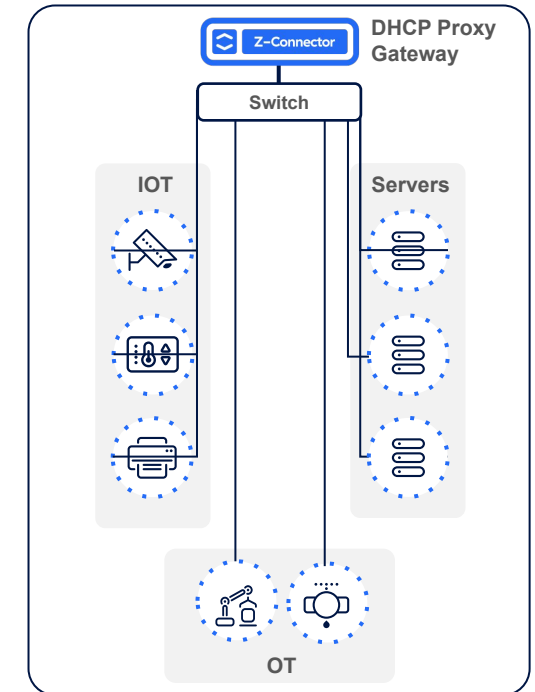
Between branches, campus, cloud, DC



Zero Trust SD-WAN (No Site-to-Site VPN / MPLS)
Each branch is a Starbucks

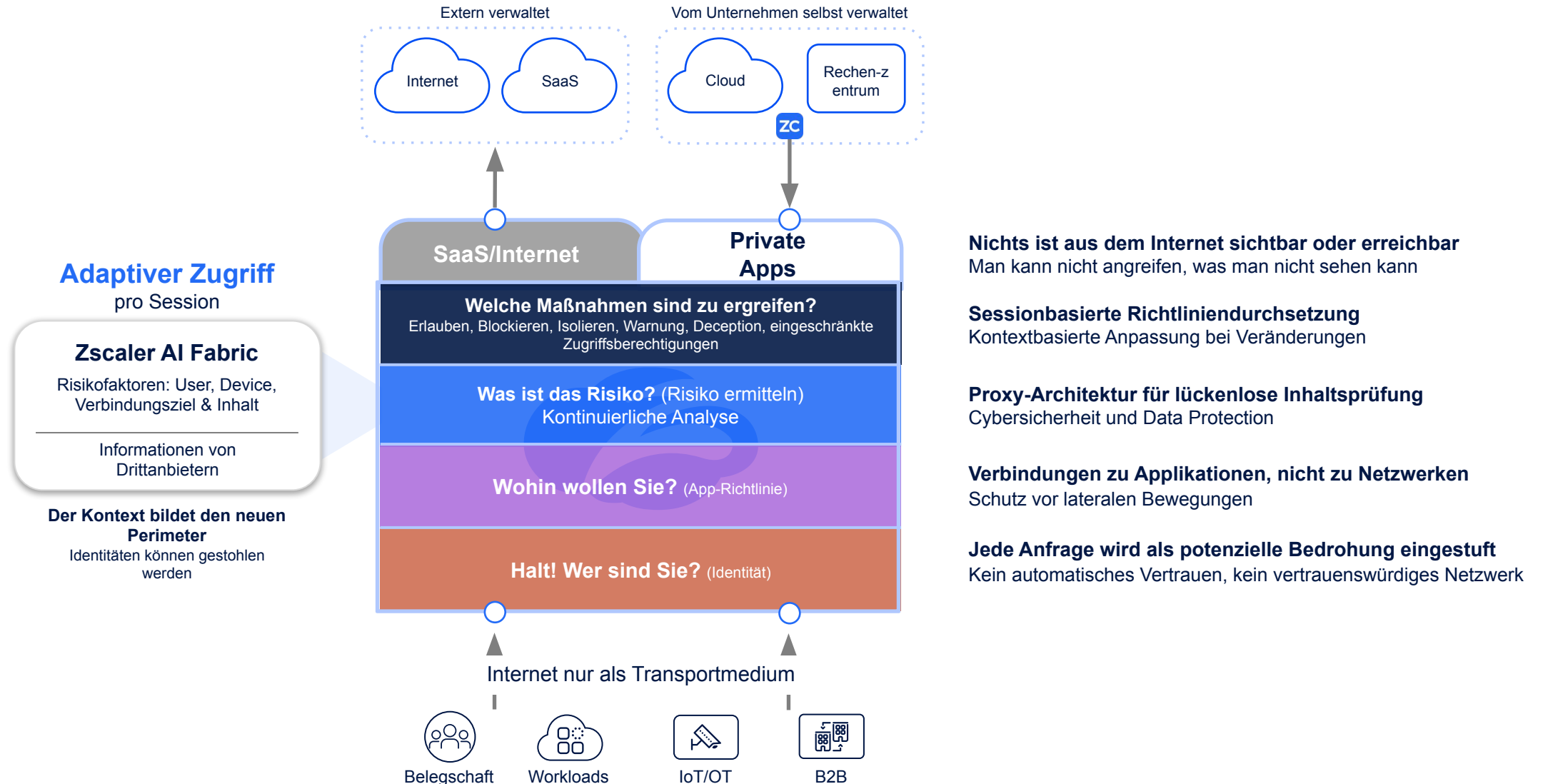
Geräte Segmentierung

Inside branch, factory, campus



Automated IoT / OT Segmentation
Segment of 'one' for every device

Die sichere Infrastruktur von Morgen



Eine Zero-Trust-Architektur ist das Gegenteil von Firewalls. Sie kann nicht nachträglich als Ergänzung zu Firewalls und VPNs eingerichtet werden