Warum “Zero Trust” in Zukunft wichtig ist

JAMF NATION LIVE

René Stiel

Sales Engineer
Jamf

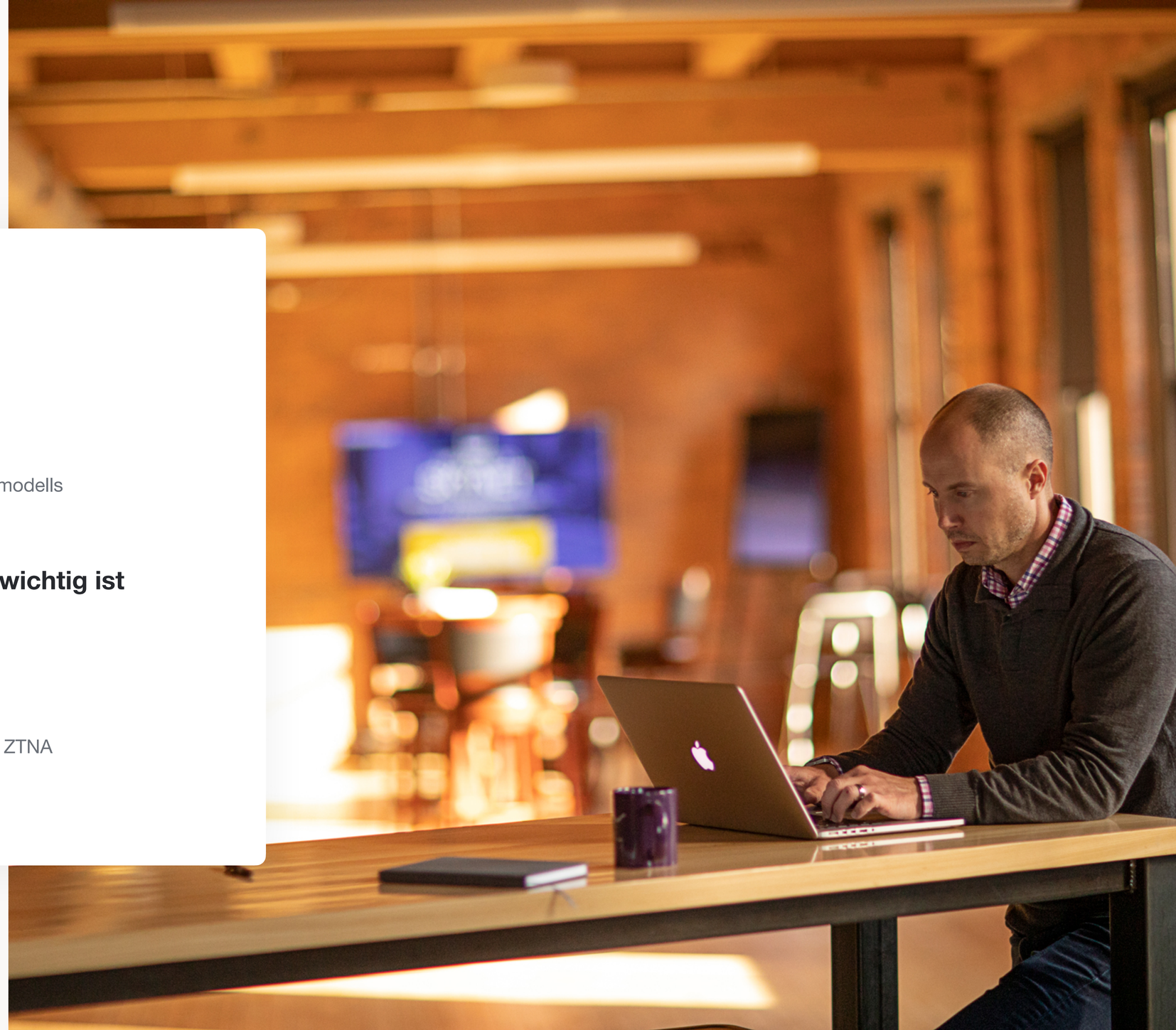
Agenda

1 | Warum nicht VPN?
VPN vs ZTNA

2 | Prinzipien “Zero Trust”?
Die Grundsätze eines Zero-Trust-Sicherheitsmodells

3 | Warum “Zero Trust” in Zukunft wichtig ist
Vorteile für Endbenutzer und IT-Teams

4 | Jamf Private Access
Ein kurzer Überblick über unseren Ansatz für ZTNA
als Teil unseres breiten Produktportfolios



Zero Trust Network Access (ZTNA) ist ein Produkt oder ein Dienst, der eine **identitäts-** und **kontextbasierte**, **logische Zugangsgrenze** um eine App oder eine Reihe von Apps schafft.

Zero Trust Network Access (ZTNA) ist ein Produkt oder ein Dienst, der eine **identitäts-** und **kontextbasierte**, **logische Zugangsgrenze** um eine App oder eine Reihe von Apps schafft.

Zero Trust Network Access (ZTNA) ist ein Produkt oder ein Dienst, der eine **identitäts-** und **kontextbasierte**, **logische Zugangsgrenze** um eine App oder eine Reihe von Apps schafft.

Die Unternehmensgrenzen haben sich verändert

Benutzer arbeiten von überall und nutzen zunehmend mobile Endgeräte

4x Remote-Arbeit hat sich im letzten Jahrzehnt mehr als vervierfacht

70% Der Arbeitnehmer sitzen nicht mehr hinter einem Schreibtisch

Daten bewegen sich außerhalb der Grenzen

Unternehmensanwendungen werden mobil

Apps sind überall, auch in der Cloud

85% Der Prozesse werden in die Cloud verlagert

72% Der Unternehmen untersuchen die Einführung von ZTNA

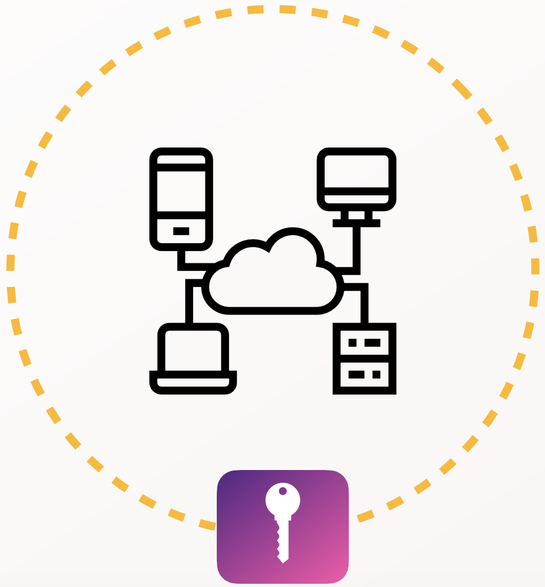
Apps sowohl on-premise als auch in der Cloud

Der bisherige Schutz ist nicht mehr ausreichend

Warum nicht VPN?

Grundlegende Schwächen von Legacy-VPN

UNSICHER BY DESIGN

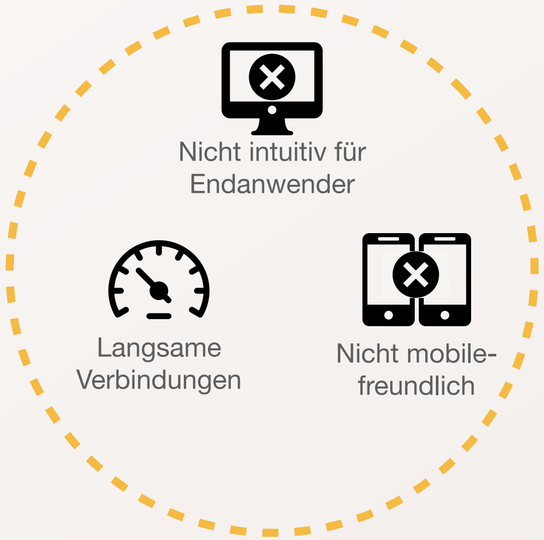


Vollständiger Netz-Zugriff bietet große Angriffsfläche

KOMPLEX ZU VERWALTEN

Große VPN Umgebungen erfordern ganze Teams zur Verwaltung

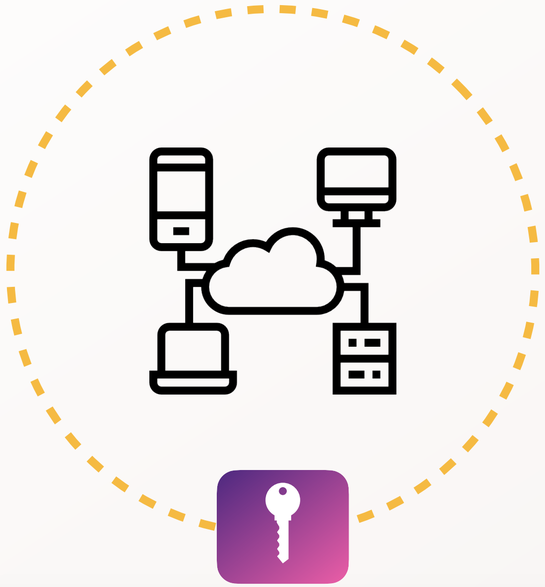
SCHLECHTE NUTZERERFAHRUNG



VPN hat **keinen** Fokus auf Benutzerfreundlichkeit

Grundlegende Schwächen von Legacy-VPN

UNSICHER BY DESIGN

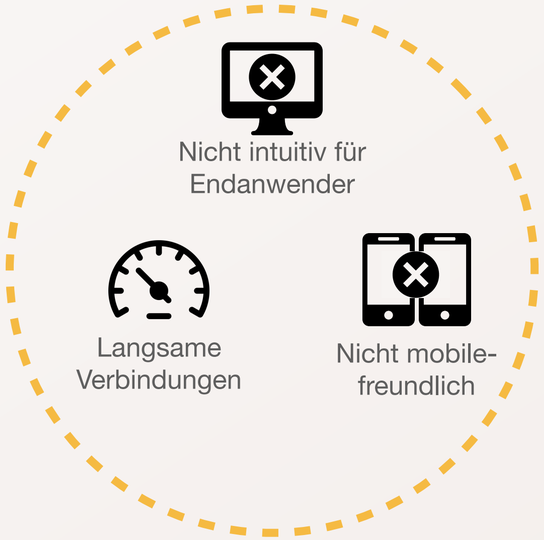


Vollständiger Netz-Zugriff bietet große Angriffsfläche

KOMPLEX ZU VERWALTEN

Große VPN Umgebungen erfordern ganze Teams zur Verwaltung

SCHLECHTE NUTZERERFAHRUNG



VPN hat **keinen** Fokus auf Benutzerfreundlichkeit

Prinzipien von “Zero-Trust”?

Prinzipien von ZTNA

Starke Sicherheit

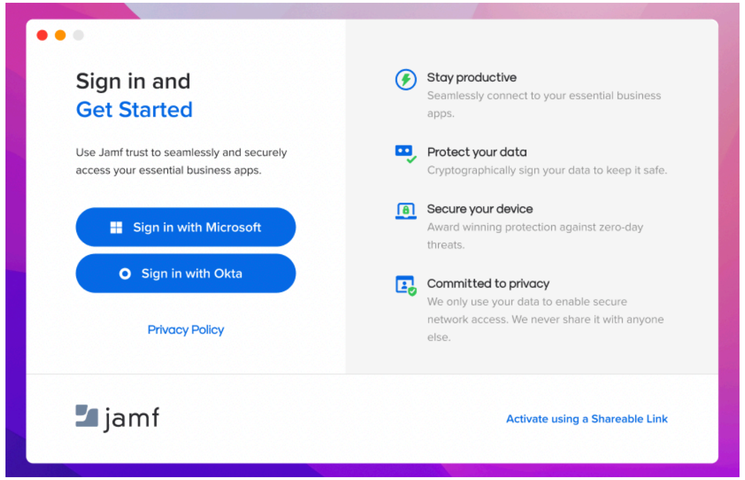
- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel



Eliminieren Sie implizites Vertrauen

Remote-Zugriff nur für autorisierte Benutzer

Identität verknüpft Zugriffswege explizit mit Zugriffsrechten

IDP-Integration sorgt für konsistente Benutzer- und Gruppenkonstrukte in Anwendungen und Zugriffsrichtlinien

Prinzipien von ZTNA

Starke Sicherheit

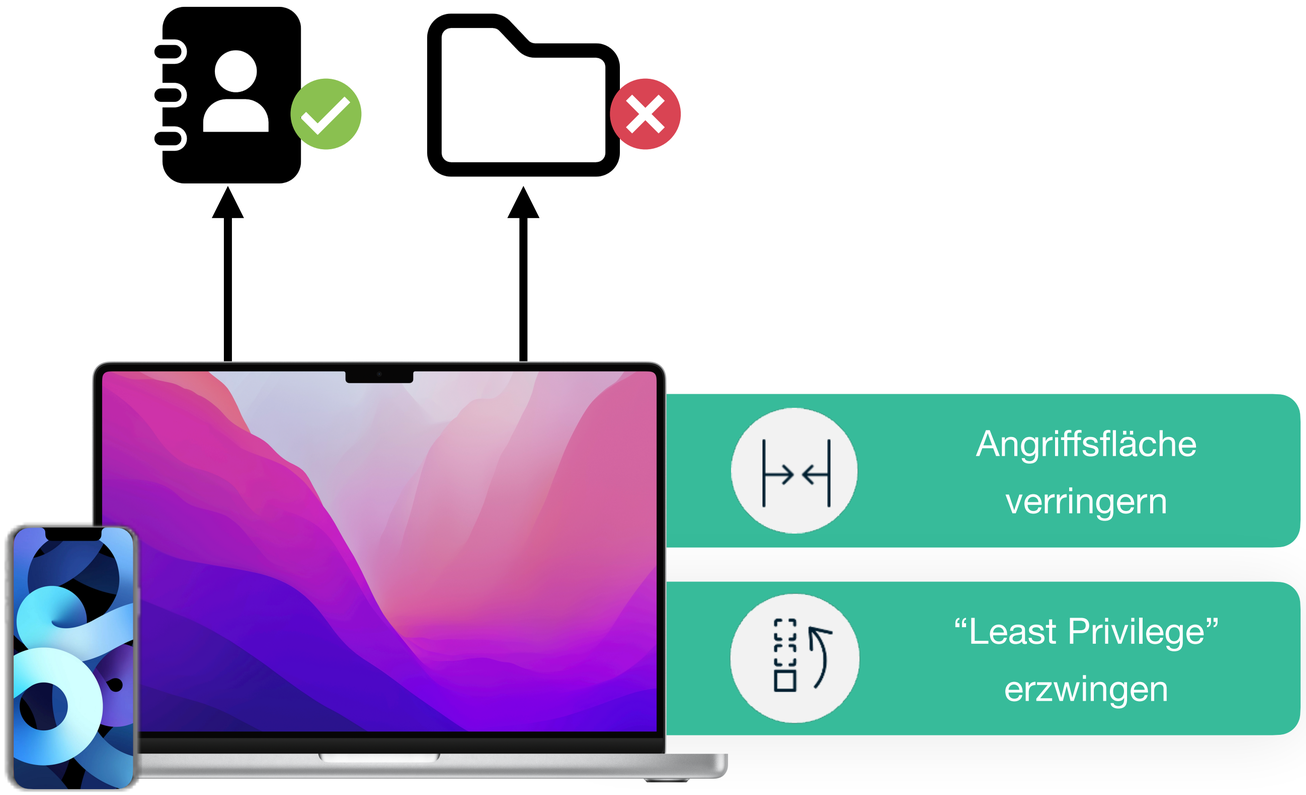
- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel



Prinzipien von ZTNA

Starke Sicherheit

- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel

High-risk Client

Geschützte Business Apps

Prinzipien von ZTNA

Starke Sicherheit

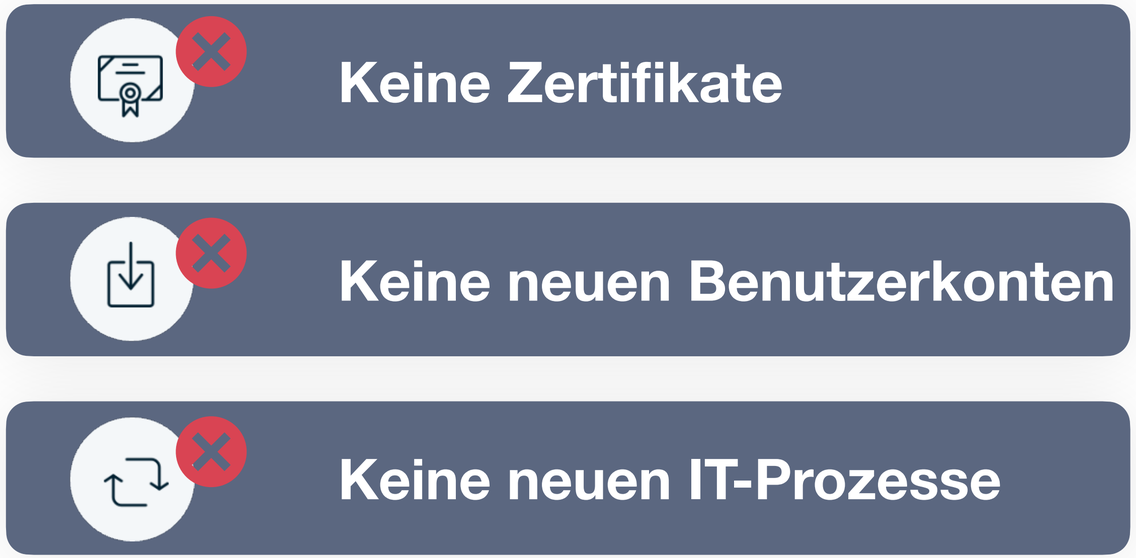
- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel



Prinzipien von ZTNA

Starke Sicherheit

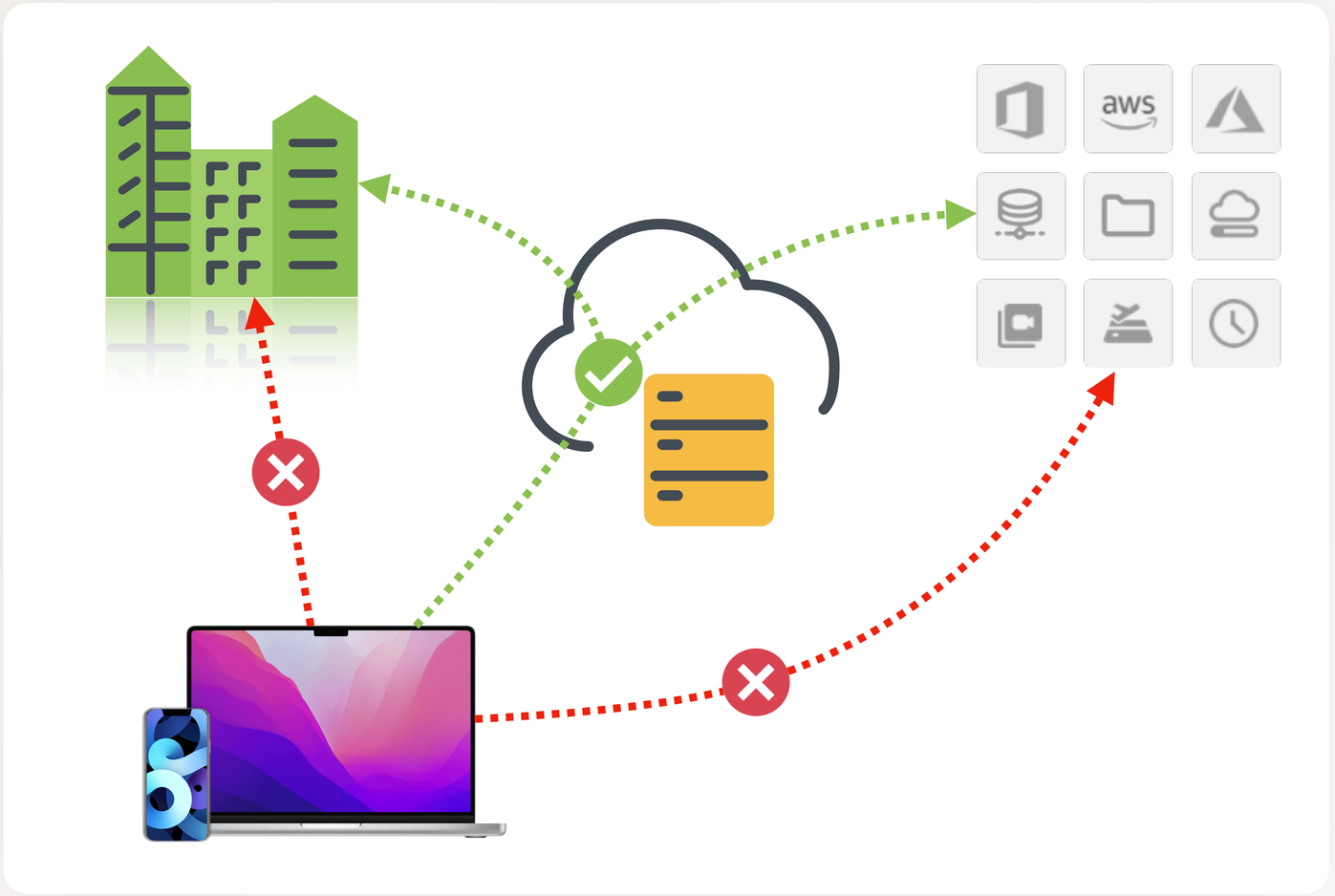
- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel



Prinzipien von ZTNA

Starke Sicherheit

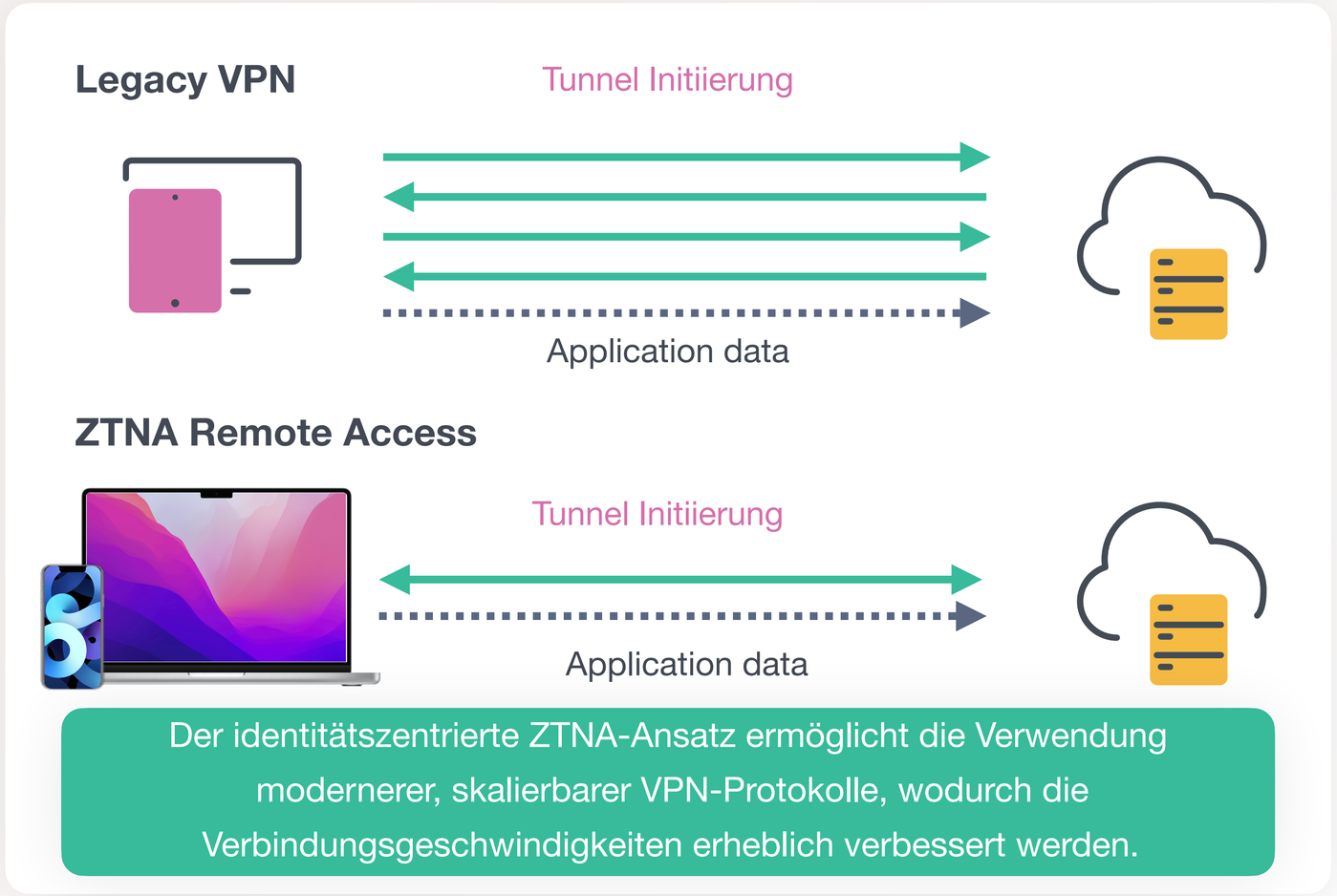
- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel



Prinzipien von ZTNA

Starke Sicherheit

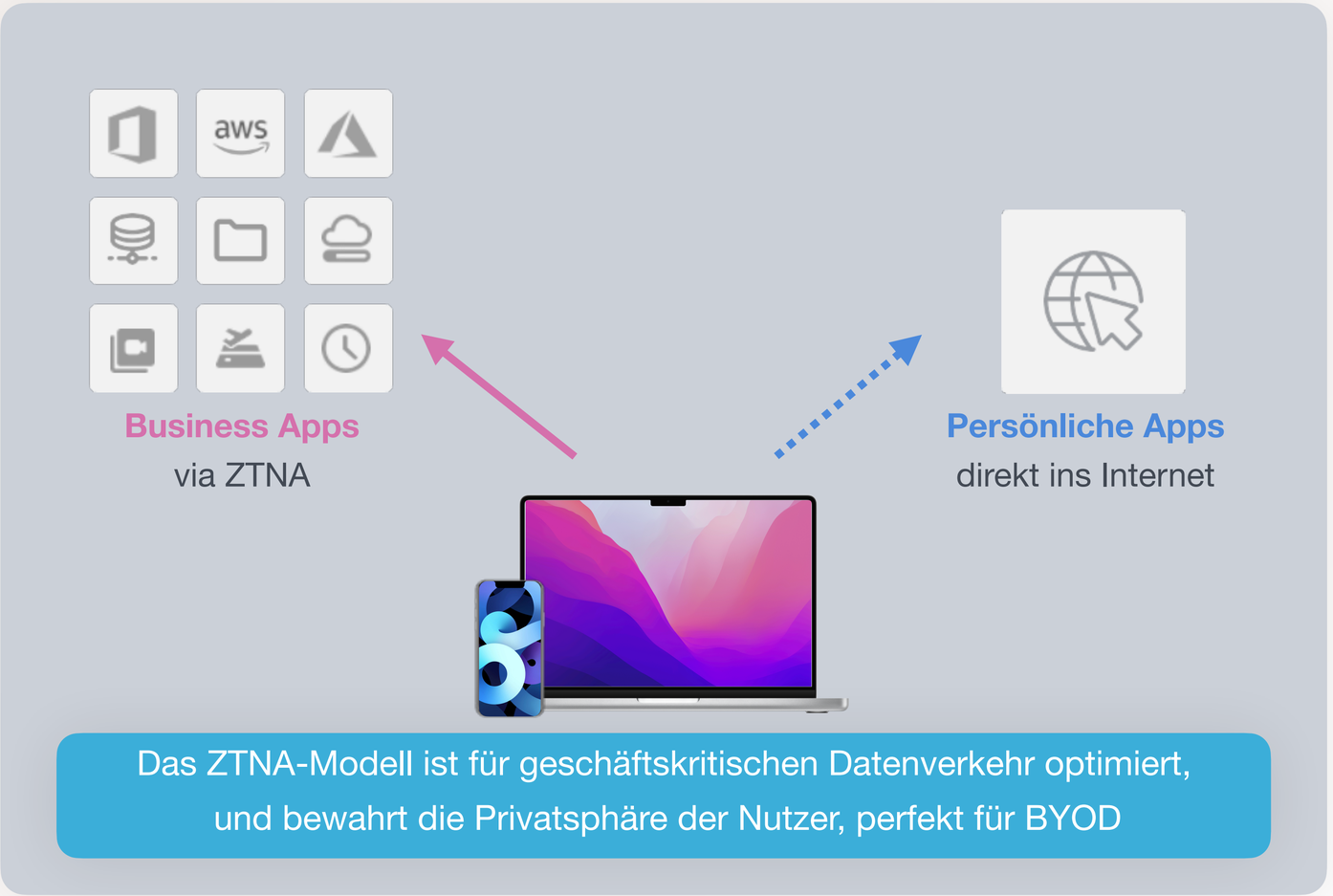
- Identitäts-zentriertes Sicherheitsmodell
- App-basierte Segmentierung
- Risiko-bewusste Zugriffsrichtlinien

Verbesserte Verwaltung

- Schlankes Management
- Trust Broker/Software Defined Perimeter

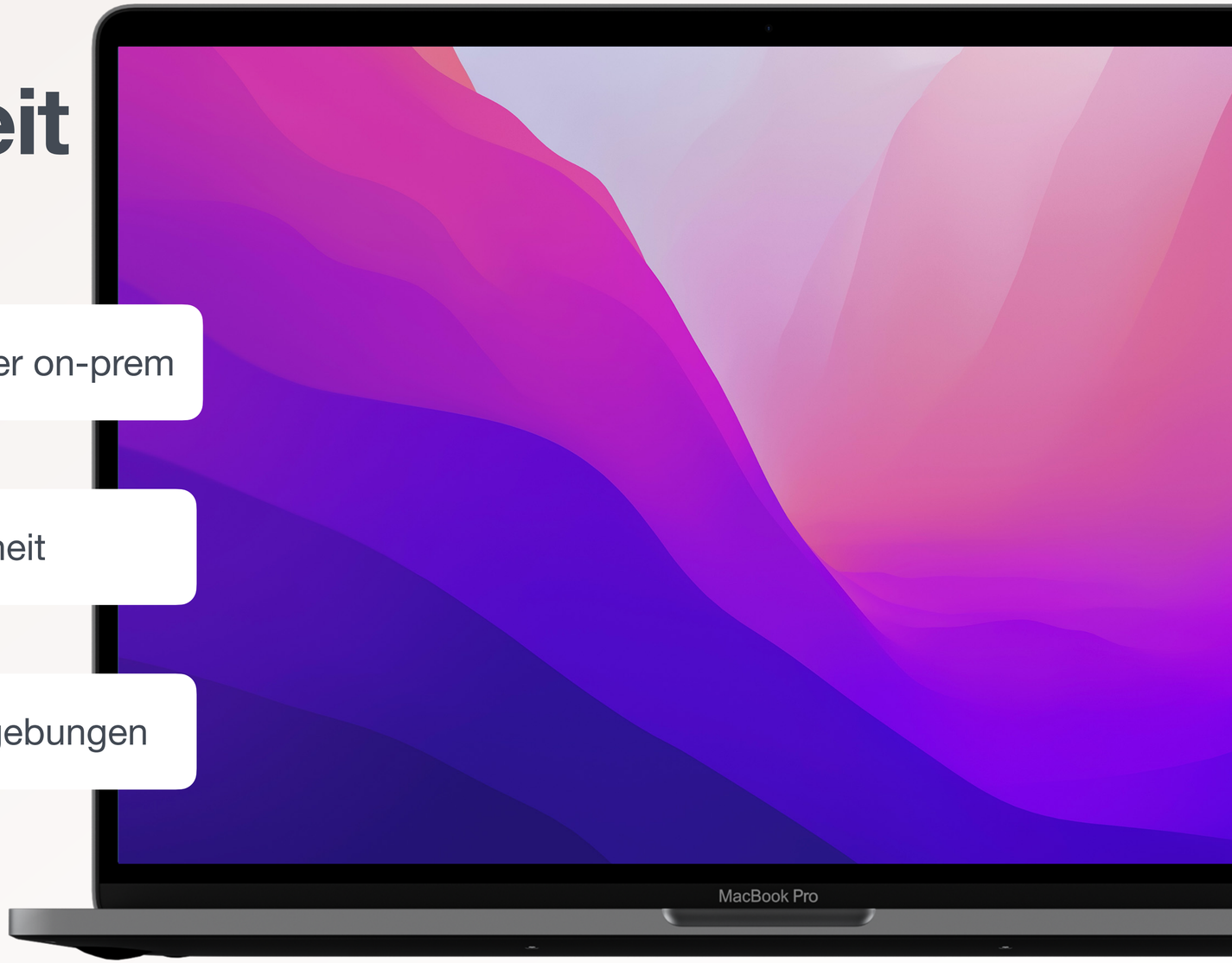
Fokus auf Benutzerfreundlichkeit

- Schnelle Verbindung
- Dynamischer Split-Tunnel

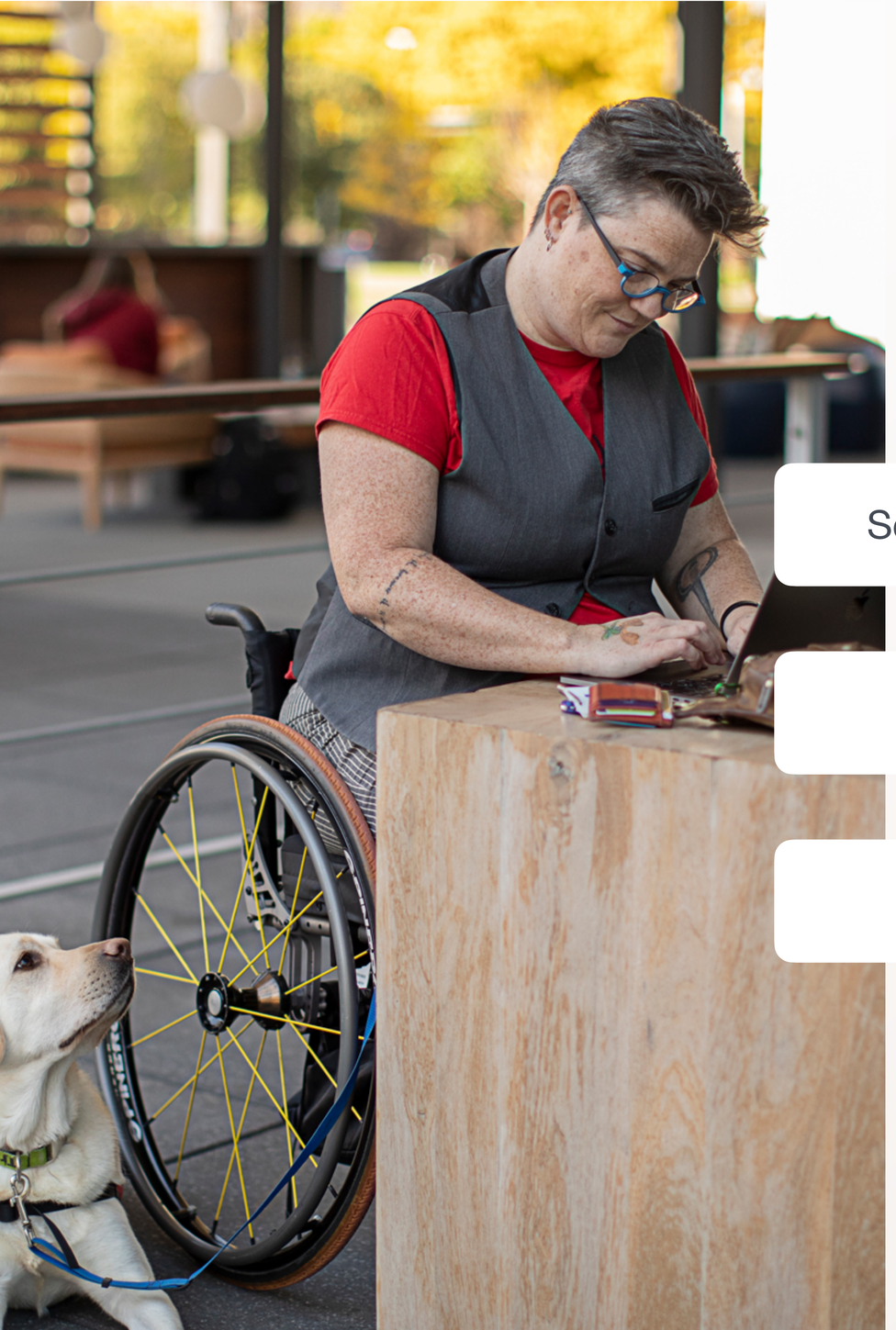


Warum “Zero Trust” in Zukunft wichtig ist

Vorteile
Organisations Sicherheit



- Einheitlicher Richtlinien basierter Zugriff für Cloud oder on-prem
- Kontinuierliche Überprüfung der Gerätesicherheit
- Absicherung/Darkening von Cloud- und Hybrid-Umgebungen



Vorteile Benutzererfahrung

Schnell - kein “Wheel of Death” mehr, wenn man versucht zu arbeiten

Transparent für den Endbenutzer “native experience”

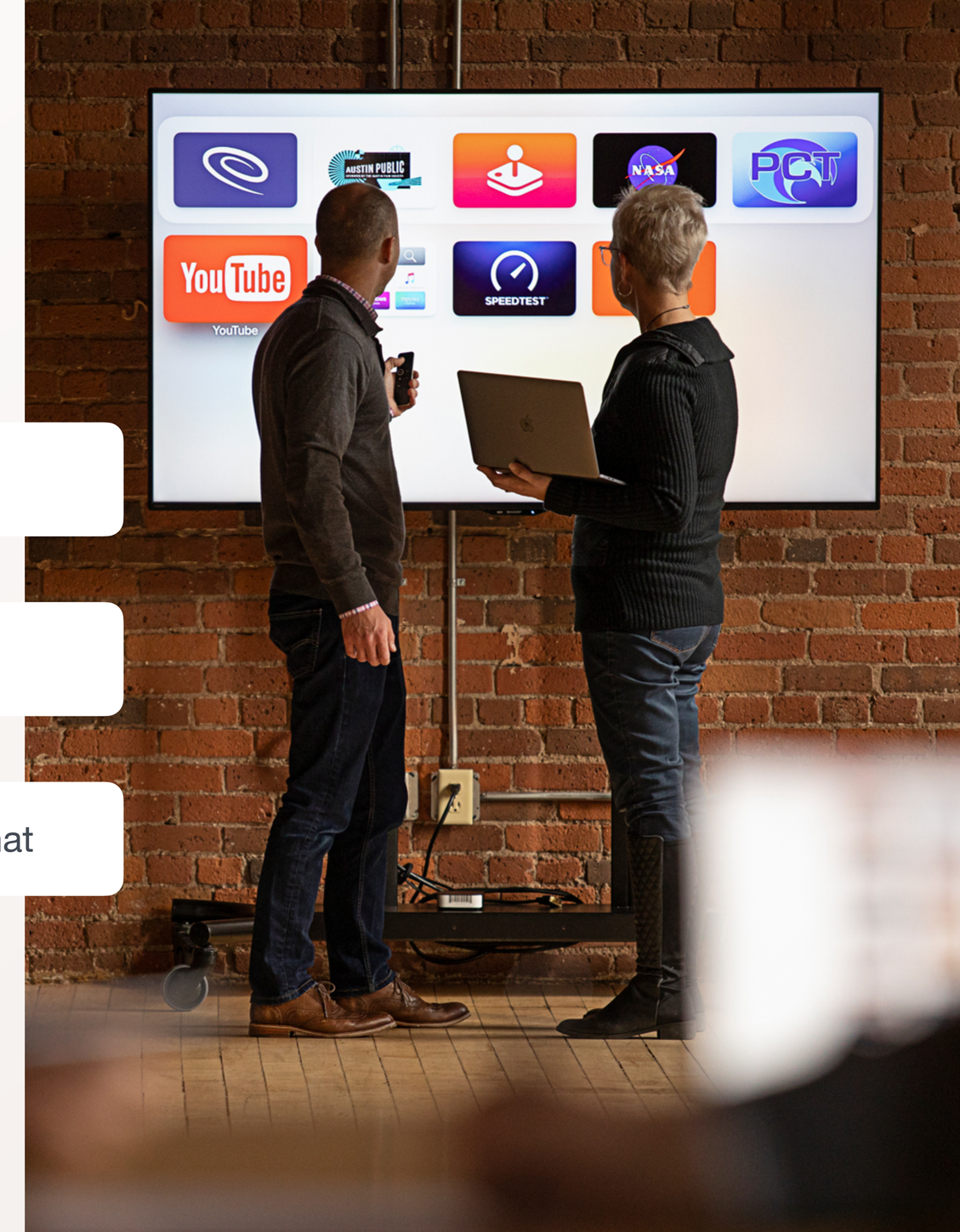
Einfache Einrichtung & “remediation”

Vorteile
IT & Security Teams

Einfache Bereitstellung, Verwaltung und Skalierung

Zentrale Kontrolle und Sichtbarkeit

Gewissheit, dass jedes Gerät das richtige Sicherheitsniveau hat



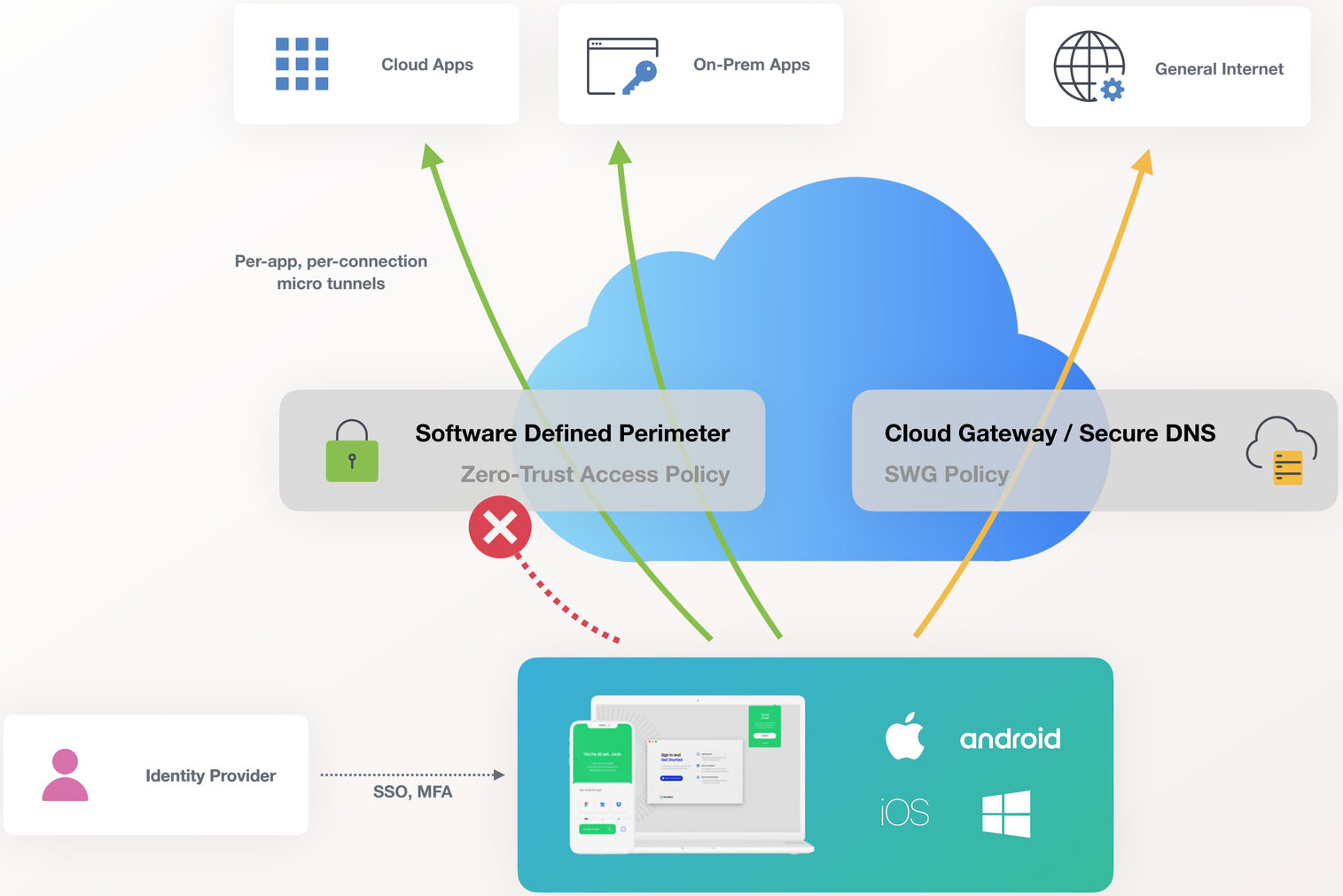
Was bedeutet dies für **BYOD?**

- Unternehmen brauchen eine klare Strategie für die Verwaltung von Geräten außerhalb der traditionellen Netzwerkgrenzen
- Benutzer können mit beliebigen Geräten auf Unternehmensressourcen zugreifen
- Unterstützt die Kosteneffizienz, die durch BYOD erreicht wird

Jamf Private Access

JAMF NATION LIVE

Jamf Private Access



Next-Gen Konnektivität

- Schneller, nahtloser, sicherer Zugriff auf jede art von Anwendung
- Layer 3 Micro-Tunnel / Segmentierung
- Single Packet Authentifizierung

Zero Trust Access Policy

- App-basierte Zugriffsrichtlinien
- Kontinuierliche Überprüfung
- Kontextbasierte Risikobewertung
- Internet-Richtlinien über Cloud SWG oder direktes Routing

Seamless User Experience

- Identitätszentriertes Onboarding
- Einheitliche Richtlinien und UX für alle Geräte
- Positives Feedback: "Ich merke nicht einmal, dass es läuft”

Zusammenfassung

Zero Trust

“Never Trust, Always Verify”

Always Verify

Der Zugriff auf alle Ressourcen muss auf sichere Weise und von einem sicheren Endgerät aus erfolgen, unabhängig vom Standort - Immer authentifizieren und autorisieren

Least Privilege

Die Zugangskontrolle erfolgt auf einer "Need-to-know"-Basis, die mit der Identität eines Benutzers und den Zugriffsberechtigungen dieses Benutzers zusammenhängt.

Assume Breach

Überprüfen Sie die Ende-zu-Ende-Verschlüsselung und nutzen Sie Analysen, um Transparenz zu erhalten. Unternehmen müssen den gesamten Datenverkehr untersuchen und protokollieren, um zu überprüfen, ob die Benutzer die richtigen Dinge tun

Vielen Dank

Jamf Security Cloud Architecture

Jamf Private Access