AVANTEC
Competence. Security. Trust.

Zero Trust – ein Paradigmawechsel

15. Juni 2023

Agenda und Vorstellung der Referenten

AVANTEC
Competence. Security. Trust.

- Einführung in Zero Trust
- Peter Hämmerli, Senior PreSales Engineer, AVANTEC AG

- Best Practices und Fallstudien für die Umsetzung von Zero Trust
- Marcel Kistler, Expert Strategic Consultant, AVENIQ AG

- 15:30 - Pause

- Vorstellung der Zscaler Zero Trust Exchange Plattform
- Christian Burgert, Senior Security Engineer, AVANTEC AG

- 16:45 - Diskussion und Fragerunde

- 17:30 - Aperitif

Kontaktinformationen unserer Referenten

AVANTEC
Competence. Security. Trust.

- Claudia Tilg, Key Account Manager, AVANTEC AG
- tilg@avantec.ch

- Peter Hämmerli, Senior PreSales Engineer, AVANTEC AG
- haemmerli@avantec.ch

- Marcel Kistler, Expert Strategic Consultant, AVENIQ AG
- marcel.kistler@aveniq.ch

- Christian Burgert, Senior Security Engineer, AVANTEC AG
- burgert@avantec.ch

- Markus Graf, CO-CEO, AVANTEC AG
- graf@avantec.ch

AVANTEC
Competence. Security. Trust.

Einführung in Zero Trust

Ausgangslage

Der digitale Fortschritt und die hybriden IT-Umgebungen stellen IT-Experten weltweit vor neue Herausforderungen.

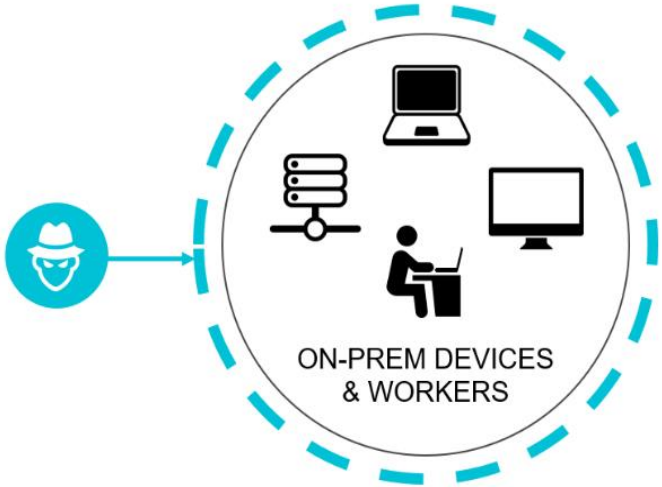
Abhilfe verspricht Zero Trust!

Was ist Zero Trust?

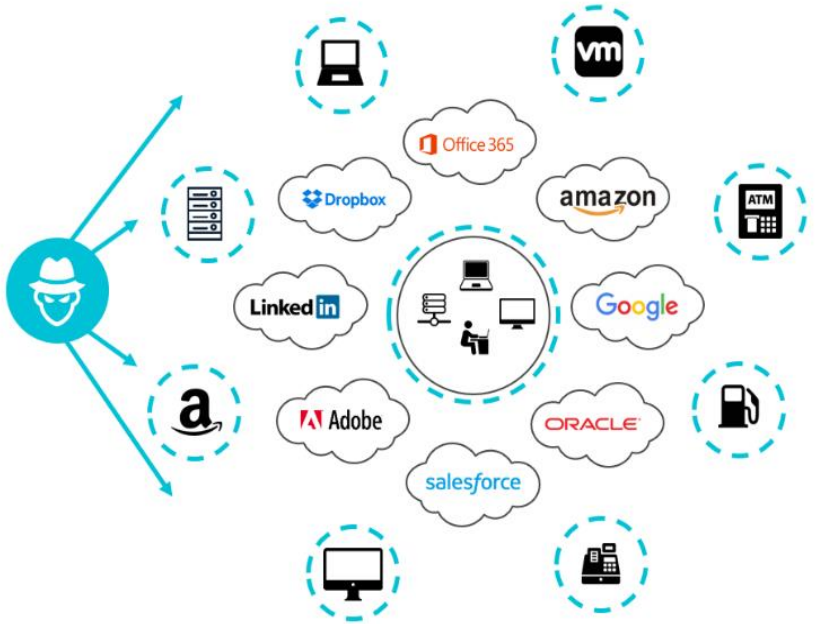
Das Problem: Der neue Perimeter ist der Endpoint

AVANTEC
Competence. Security. Trust.

Before



Today



Fragen

AVANTEC
Competence. Security. Trust.

- Wer von Ihnen setzt bereits in Ihrem Unternehmen ein hybrides Infrastrukturmodell ein?
- Wer von Ihnen hat sich bereits mit Zero Trust auseinandergesetzt?
- Wer von Ihnen setzt das Konzept als Strategie im Unternehmen ein?

Denkweise

AVANTEC
Competence. Security. Trust.

Perimeter-Security

Traditionell haben alle Unternehmen auf Firewalls als wichtigsten Netzwerkschutz gesetzt. Dabei galt der Ansatz, dass der Angreifer immer über den Perimeter (die Firewall) kommen wird.

Es galt auch, dass sämtliche Nutzer und Anwendungen innerhalb der eigenen Domäne als vertrauenswürdig einzustufen waren.

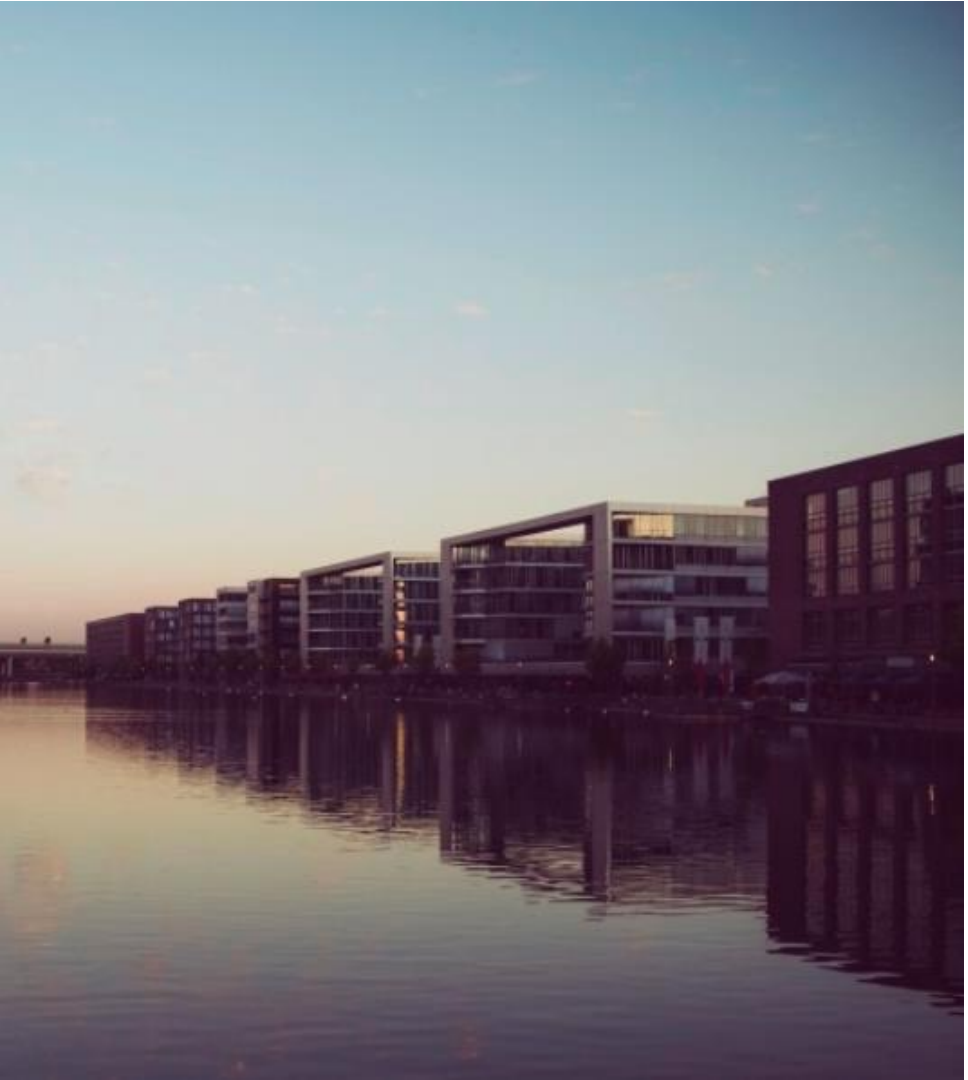
Diesen Ansatz gilt es zu überdenken.
Er bringt bei heutiger Bedrohungslage keinen ausreichenden Schutz!

Das neue Leitmotiv

«Assume Breach»

Gehen Sie davon aus, dass nicht alle Sicherheitsvorgaben eingehalten wurden und dass die «Angreifer» bereits in Ihrer Domäne sind, resp. sich bereits auf Ihren Systemen eingenistet haben.

«Assume Breach» ist eine Denkweise, mit der neue IT-Architekturen und Security Designs sowie die Abwehrsysteme der Zukunft übereinstimmen sollten.



Abhilfe – Zero Trust?

AVANTEC
Competence. Security. Trust.

Zero Trust

Zero Trust soll Ihr Unternehmen wirkungsvoll schützen.

«Bei Zero Trust ist das **Vertrauen** dynamisch und veränderbar und wird innerhalb eines Netzwerks nicht mehr vorausgesetzt.»

Satja Nadella, CEO Microsoft (Nov. 2021)

Zero Trust

Zero Trust geht davon aus, dass das Vertrauen in Anwendungen, Dienste, Identitäten und Netzwerke jedes mal neu geprüft und gegebenenfalls eingeschränkt werden muss.

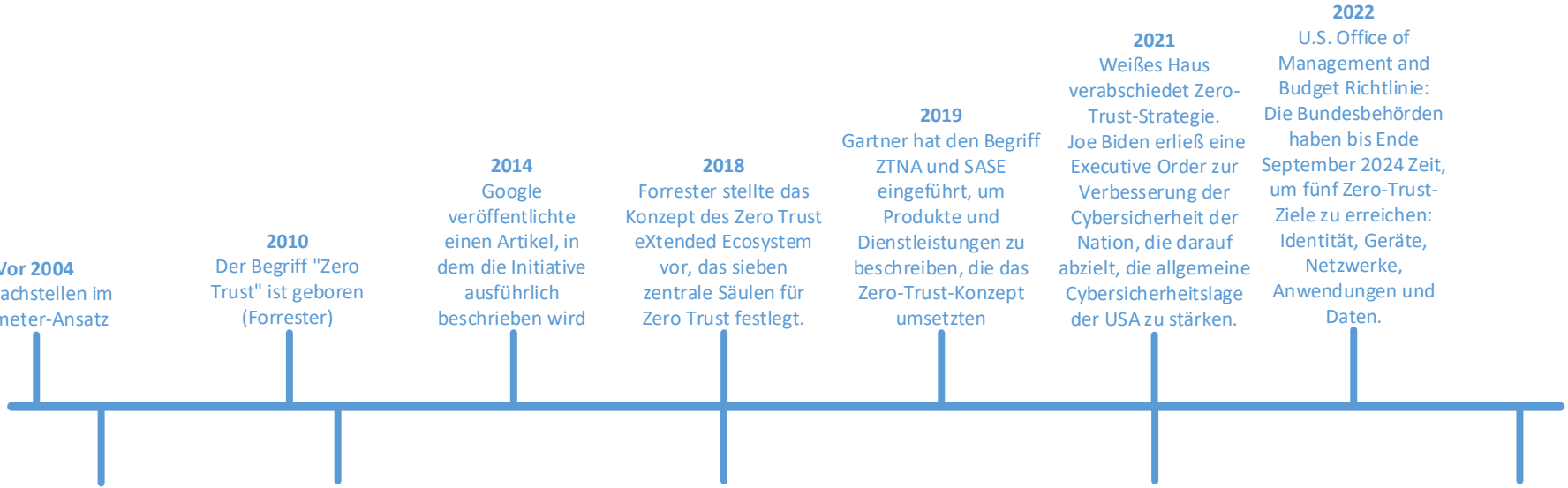
Interne als auch externe Zugriffe gelten immer als unsicher und wahrscheinlich bereits als kompromittiert.

Zero Trust beruht auf:

- **Richtlinien**
- **IT-Architekturen**
- **Technologien**

Die Entwicklung von Zero Trust

AVANTEC
Competence. Security. Trust.



Impacts für Zero Trust

AVANTEC
Competence. Security. Trust.

Die Impacts oder Motivationen, ein Zero-Trust-Konzept umzusetzen, kommen aus **Businessanforderungen:**

- Hybrid Cloud und X-as-a-Service
- Wachsende Remote-Useranzahl, BYOD und Modern Workplace
- Digitale Transformation
- Ransomware Angriff / Abwehr
- Compliance
- Business Continuity
- Cyberversicherung
- etc.

Fragen

AVANTEC
Competence. Security. Trust.

- Wer von Ihnen hat schon einen Ransomware-Angriff erlebt?
- Wer von Ihnen hat bereits eine Ransomware-Abwehrstrategie entwickelt und einen Reaktionsplan ausgearbeitet für den Fall, dass ein solcher Angriff passiert?
- Wer von Ihnen hat sich bereits Gedanken über eine Cyberversicherung gemacht oder sogar eine solche abgeschlossen?

Zero Trust als Marketing-Schlagwort

AVANTEC
Competence. Security. Trust.

«Zero Trust» wird als Marketing-Schlagwort missbraucht. Anbieter stiften beträchtliche Verwirrung, indem sie den Begriff zu Marketingzwecken wahllos auf alles anwenden, was mit Sicherheit zu tun hat. Gartner, 2019

Zero Trust kann man nicht kaufen, es ist kein fertiges Produkt und keine fixfertige Lösung. Ebenso kann Zero Trust nicht einfach implementiert und abgeschlossen werden.

Definition von Zero Trust vs. ZTNA

AVANTEC
Competence. Security. Trust.

Zero Trust Network Acces
ist die Technologie
Unternehmen
Implementierung eines
Sicherheitsmodells er
„Zero Trust“ ist ei
Sicherheitsmodell, da
ausgeht, dass Bedrohun
innerhalb als auch auße
Netzwerks vorhanden si
erfordert Zero Trust ein
Überprüfung jedes Nu
jedes Geräts, bevor si
Zugriff auf interne Res
autorisiert werde

Cloudflare: https://www.cloudflare.com/de-de/learning/access-management/what-is-ztna/

Zero trust (ZT) is the term for an
evolving set of cybersecurity
paradigms that move defens
from static, network- based
perimeters to focus on users
assets, and resources.
Zero trust focus on protectin
resources (assets, services,
workflows, network accounts, e
not network segments, as th
network location is no longer s
as the prime component to t
security posture of the resour

NIST: https://www.nist.gov/publications/trust-architecture

Zero trust network access (ZTNA) is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack.

Gatner: https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-

Definition von ZTNA vs. SASE

AVANTEC
Competence. Security. Trust.

- Definition «Secure Access Service Edge» (SASE) von Gartner:
  «SASE ist eine Lösung mit voller WAN-Funktionalität und umfassenden Netzwerk-Security-Features (wie SWG, CASB, FWaaS and ZTNA), um Secure Access Bedürfnisse des digitalen Business zu unterstützen.»

- Kombination von SD-WAN-Anbindung und «Security Service Edge» (SSE).

➢ SASE ist Erweiterung vom ZTNA mit Focus auf die Cloud

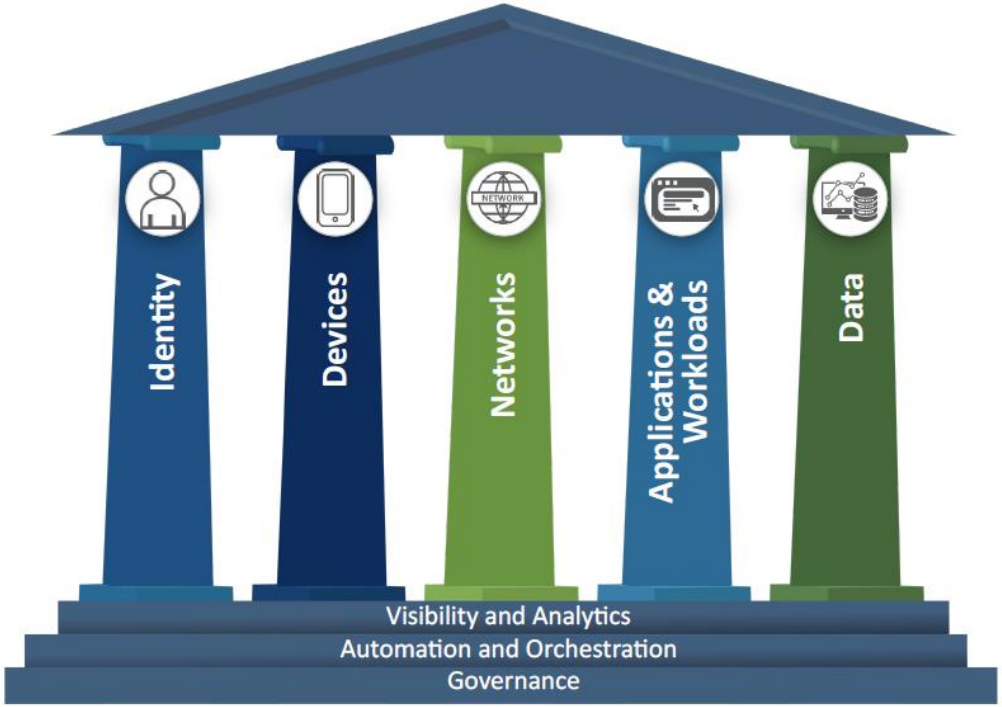
Frage

AVANTEC
Competence. Security. Trust.

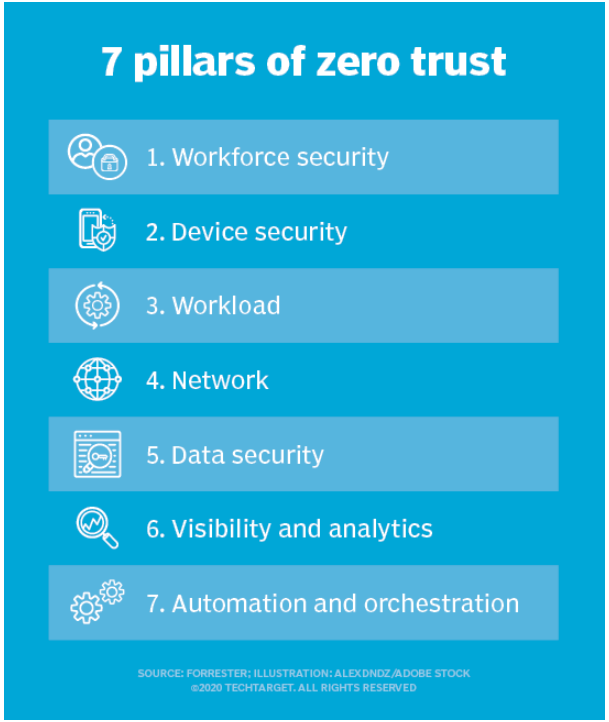
- Wer von Ihnen setzt bereits ZTNA oder SASE in Ihrem Unternehmen ein oder ist es bei Ihnen angedacht?

Die Säulen von Zero Trust

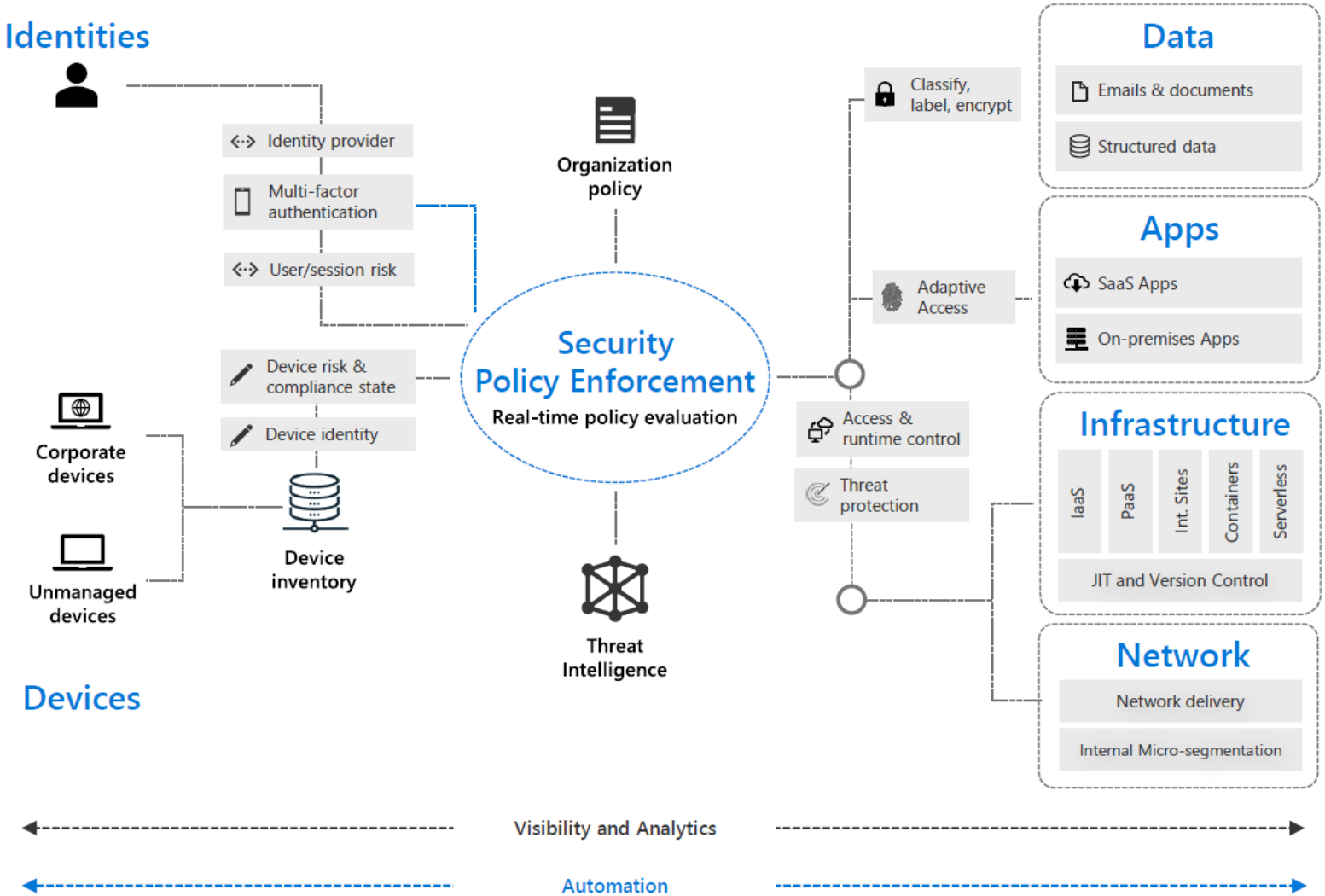
AVANTEC
Competence. Security. Trust.



Cybersecurity and Infrastructure Security Agency, USA



Forrester Research


Identities
Identity provider
Multi-factor authentication
User/session risk
Device risk & compliance state
Device identity
Corporate devices
Unmanaged devices
Device inventory
Devices
Organization policy
Security Policy Enforcement
Real-time policy evaluation
Threat Intelligence
Classify, label, encrypt
Adaptive Access
Access & runtime control
Threat protection
Data
Emails & documents
Structured data
Apps
SaaS Apps
On-premises Apps
Infrastructure
IaaS
PaaS
Int. Sites
Containers
Serverless
JIT and Version Control
Network
Network delivery
Internal Micro-segmentation
Visibility and Analytics
Automation

Zero Trust Maturität Levels

AVANTEC
Competence. Security. Trust.

Traditionell

- manuelle Konfigurationen, manuelle Reaktion auf Vorfälle und Fähigkeit zur Schadensbegrenzung
- statische Sicherheitsrichtlinien
- proprietäre und unflexible Durchsetzung von Richtlinien

Fortgeschritten

- zentralisierte Sichtbarkeit und Identitätskontrolle
- Durchsetzung von Richtlinien auf der Grundlage von lösungsübergreifenden Inputs und Outputs
- einige Reaktion auf Vorfälle aufgrund vordefinierter Abhilfemassnahmen

Optimal

- dynamische Richtlinien, basierend auf automatisierten / beobachteten Triggern
- Assets haben einen dynamischen Least-Privilege-Zugriff
- Ausrichtung an offenen Standards für säulenübergreifende Interoperabilität
- zentralisierte Visibilität mit Aufbewahrung historischer Daten für Reviews

Gestaltung der Zero Trust Architektur

AVANTEC
Competence. Security. Trust.

Bei der Entwicklung der Zero-Trust-Architektur müssen Sicherheits- und IT-Teams strategisch denken:

- Was soll geschützt werden?
- Vor wem soll es geschützt werden?

Definieren Sie Ihr Protect Surface, um Ihre Attack Surface massiv zu reduzieren

AVANTEC
Competence. Security. Trust.

Attack Surface ist die Gesamtzahl der Angriffsvektoren, die ein Angreifer nutzen kann, um ein Netzwerk oder Computersystem zu manipulieren oder Daten zu extrahieren.

Bei Zero Trust konzentrieren wir uns nicht auf die Attack Surface, sondern wir bestimmen, was wir schützen müssen.

Protect Surface umfasst in der IT, IoT und OT die kritischen und schützenswerten

- **D**aten: Welche Daten müssen geschützt werden?
- **A**nwendungen: Welche Anwendungen nutzen sensible Informationen?
- **A**ssets: Welche Assets sind besonders sensibel?
- **S**ervices: Welche Services können missbraucht werden, um den normalen Betrieb zu stören?

Herausforderungen Zero Trust umzusetzen

AVANTEC
Competence. Security. Trust.

Herausforderung	Lösungsansatz
Eine Zero-Trust-Strategie entwickeln	Einbezug von allen Stakeholdern Verständnis über neue Bedrohungsszenarien schaffen
Unterstützung der entscheidenden Kräfte im Unternehmen für sich zu gewinnen	Business-Owner und IT-Mitarbeitende einbeziehen
Budget und Ressourcen beschaffen	Langfristige Einsparungen durch Ablösung Legacy-Produkte einschätzen Der Shadow-IT entgegenwirken
IT-Change-Prozesse an Geschäftsanforderungen angleichen	Möglichkeit der Automatisierung und Orchestrierung
Erkennen schützenswerter Geschäftselemente	Verlustpotential und Schadensausmass für Unternehmen einschätzen Schwachstellen finden und Risiko eindämmen
Identifizieren von genutzten Applikationen und Diensten	Datenfluss abbilden, Shadow-IT identifizieren
Definieren von Anforderungen an neu zu beschaffende Sicherheitslösungen	Interoperabilität der Sicherheitslösungen

Zero Trust Einführung – Fazit

AVANTEC
Competence. Security. Trust.

- Zero Trust ist nicht nur ein Produkt oder eine Plattform, sondern ein Sicherheitsmodell
  - Es basiert auf «never trust», «always verify» und «assuming breach»
  - Zero Trust beinhaltet technologische und nicht-technologische Teile

- Der Versuch, Zero Trust als Produkt zu kaufen, führt zum Scheitern eines Zero-Trust-Projektes

- Unternehmen müssen eine ganzheitliche Strategie entwickeln, um zu einer Zero-Trust-Architektur zu gelangen, die mehr als nur Technologie und Schlagworte umfasst

- Ein Top-Down-Ansatz ist wichtig
  - So konzentriert sich die Einführung auf die geschäftsrelevanten Mehrwerte

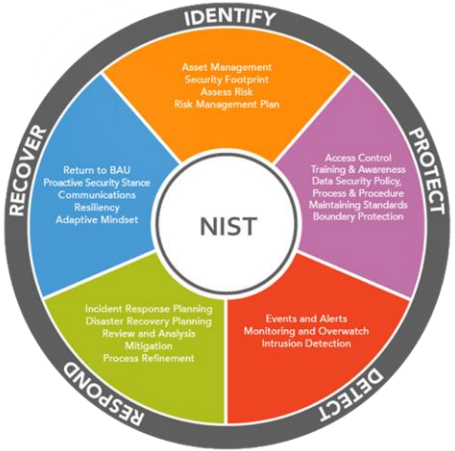
AVANTEC
Competence. Security. Trust.

Best Practices für die Umsetzung von Zero Trust

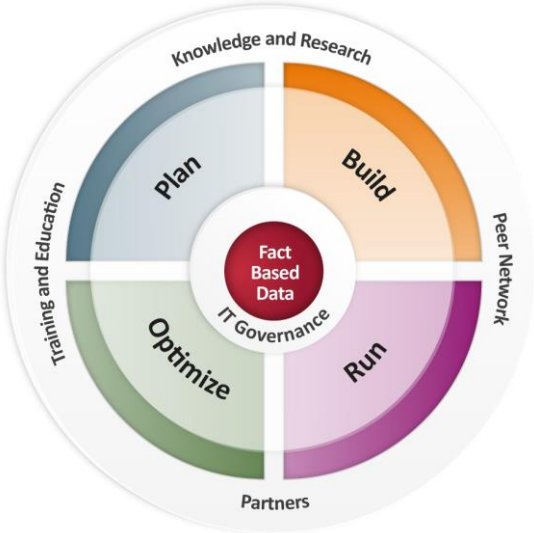
Hilfsmittel – NIST

National Institute of Standard and Technology US Department of Compentence

AVANTEC
Competence. Security. Trust.



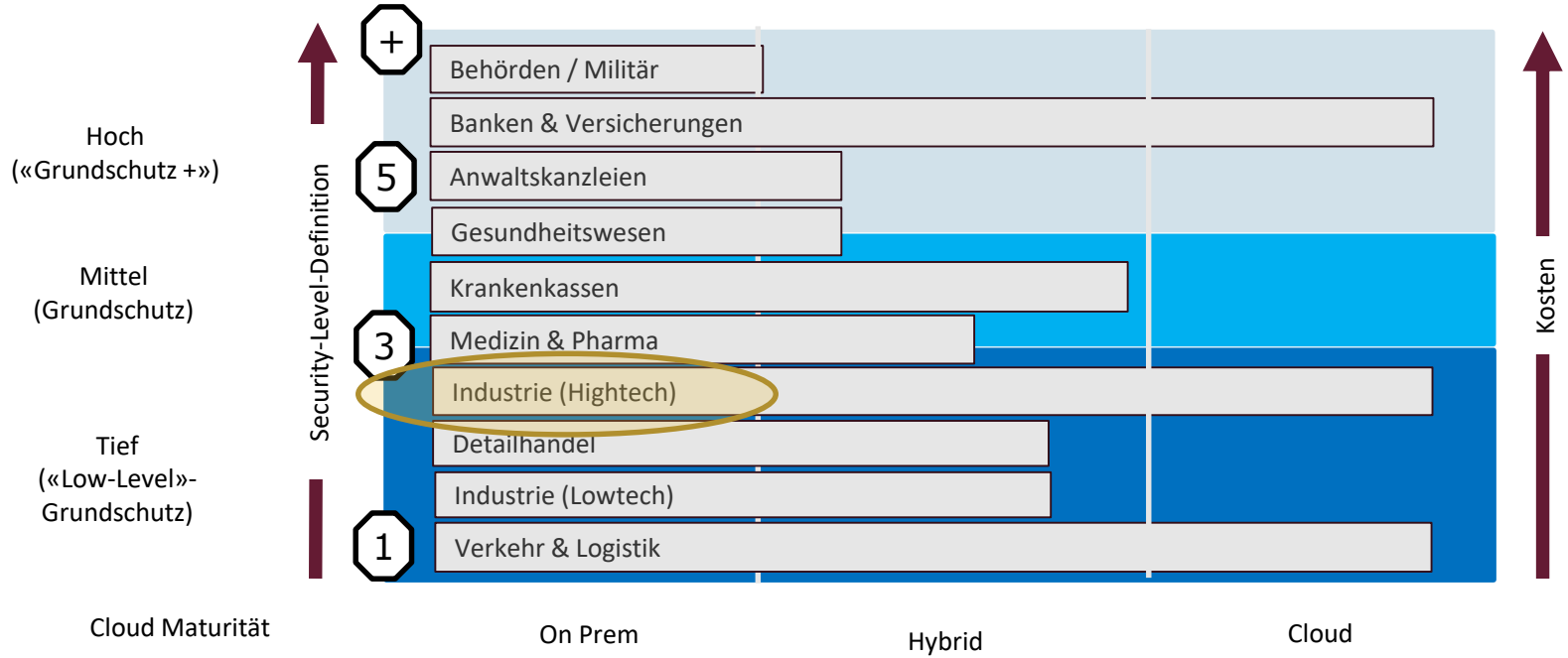
NIST-Cycle
Zero Trust



NIST-Framework
Project Management

Schritt 1: Zero Trust Level Definition

AVANTEC
Competence. Security. Trust.



Schritt 2: Zero-Trust Definitions

Definieren Ihrer Zero Trust Layers & Levels

AVANTEC
Competence. Security. Trust.

Security Layer	Level 1	Level 2	Level 3	Level 4	Level 5	Level 5+
1. Identitäten	IST				SOLL	
2. Geräte	IST		SOLL			
3. Applikationen	IST		SOLL			
4. Infrastruktur	IST		SOLL			
5. Daten	IST				SOLL	
6. Netzwerk	IST		SOLL			

IST
SOLL

Level:
1. Traditional
2. Standard
3. Managed
4. Optimized
5. Secured
5+ High Secured

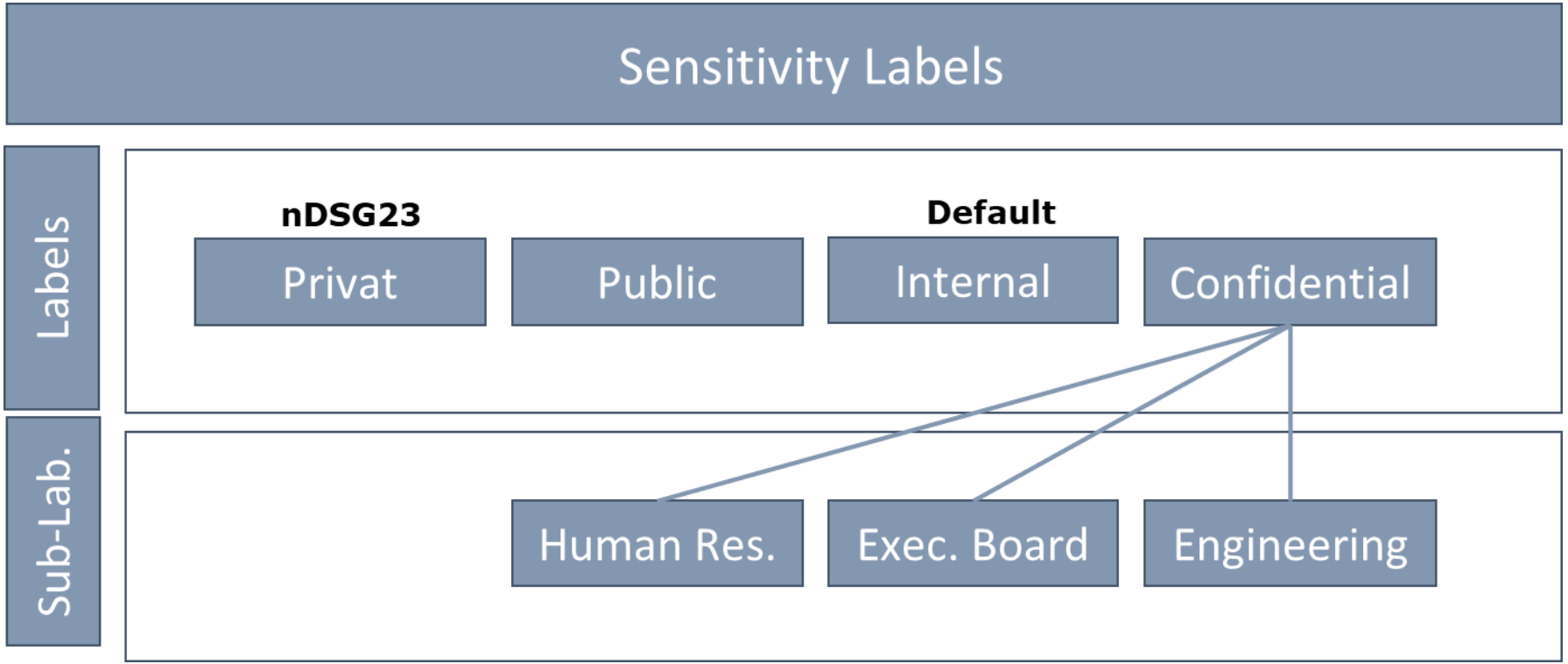
Schritt 3: Zero Trust – Maturitäts-Assessment

AVANTEC
Competence. Security. Trust.

	Traditional	Advanced	Optimal
Device	• Devices sind «domain joined» • Devices benötigen Netzwerkzugriff	• Devices sind «hybrid joined» • Devices sind registriet bei Cloud Identity Provider	• Deviced sind «cloud joined» • Endpoint Threat Protection ist aktiviert
User	• Kein SSO zwischen Cloud und On Premises • Identity Risk ist stark limitiert	• Cloud Identity - Federated mit On Premises AD • Conditional Access Policy Gate • Analytics verbessert die Visibilität	• Passwordless ist aktiviert • Benutzeranalyse in Echtzeit
Network	• Minimale Threat Protection • Configuration Management ist manuell	• Cloud-Micro-Segmentierung • Interne Traffic Encryption	• Micro-Perimeter • Interne und externe Traffic Encryption
Application	• On-Prem Apps erreichbar über VPN • Cloud Shadow IT-Risk • Cloud App sind für Benutzer erreichbar	• On Prem Apps sind gesichert über SSO • Cloud Shadow IT-Risks werden überwacht	• Alle Apps sind erreichbar über Privileged Access • Dynamic Control im Einsatz für alle Cloud Apps
Data	• Zugriff ist kontrolliert über Perimeter • Sensitivity Labels werden manuell gesetzt	• Daten sind klassifiziert und bezeichnet • Zugriffe werden kontrolliert über Verschlüsselung	• Datenklassifizierung über Machine Learning • Zugriffssteuerung über Cloud Security Policy • DLP Policies mit Verschlüsselung und Tracking

Schritt 4: Information Protection & Governance

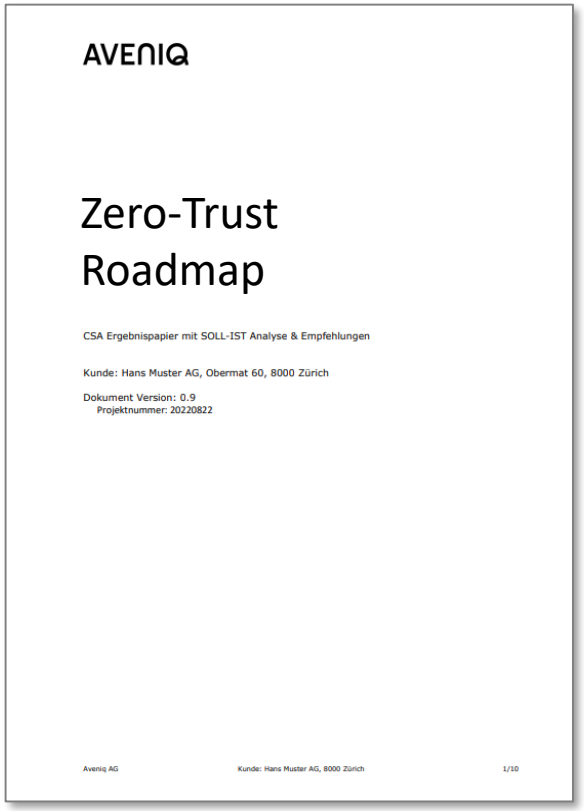
AVANTEC
Competence. Security. Trust.



Schritt 5: Zero Trust Roadmap

AVANTEC
Competence. Security. Trust.

Erstellen einer umfassenden Zero-Trust Roadmap



AVENIQ

Zero-Trust Roadmap

CSA Ergebnispapier mit SOLL-IST Analyse & Empfehlungen

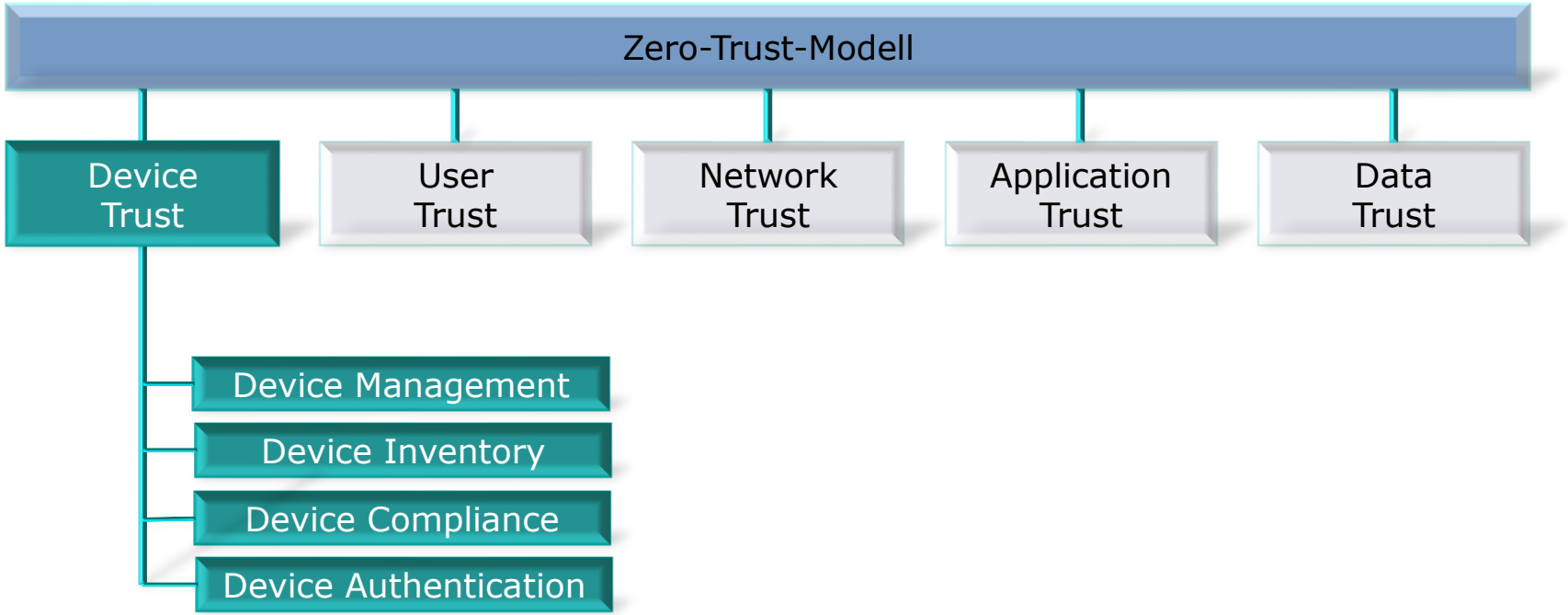
Kunde: Hans Muster AG, Obermat 60, 8000 Zürich

Dokument Version: 0.9
Projektnummer: 20220822

Aveniq AG Kunde: Hans Muster AG, 8000 Zürich 1/10

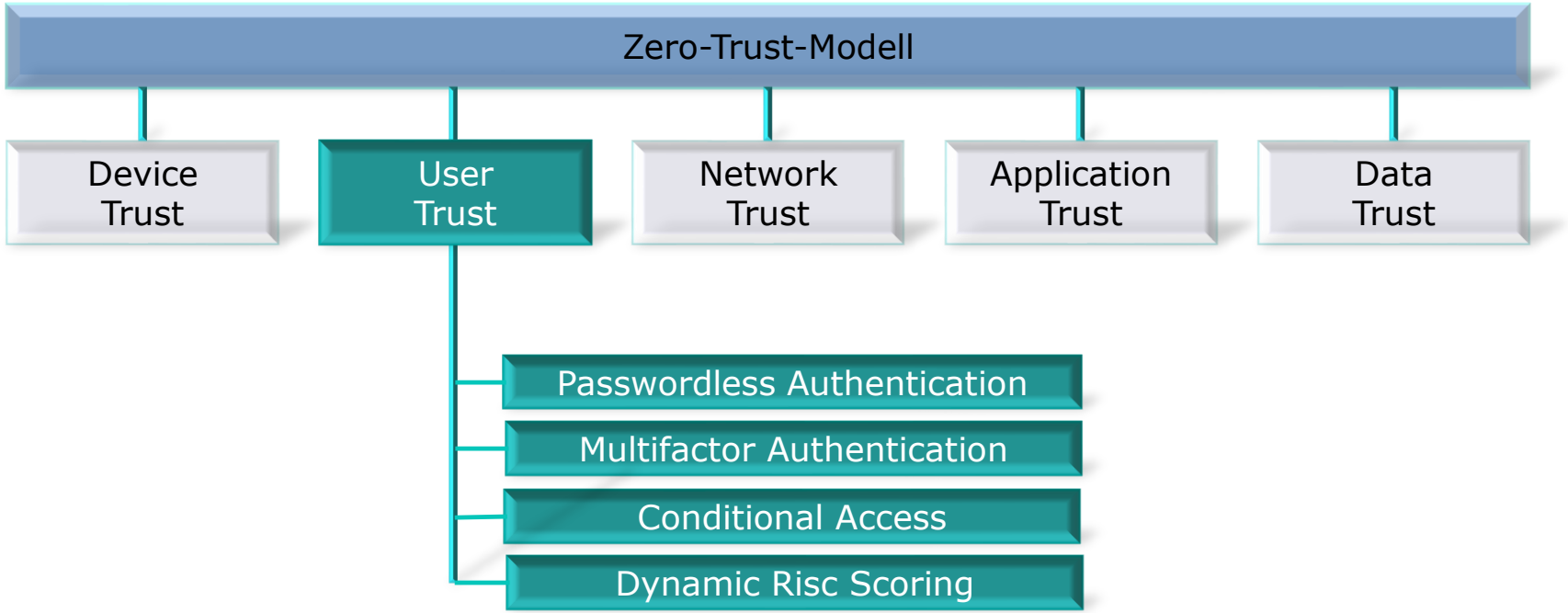
Zero Trust «Roadmap»

AVANTEC
Competence. Security. Trust.



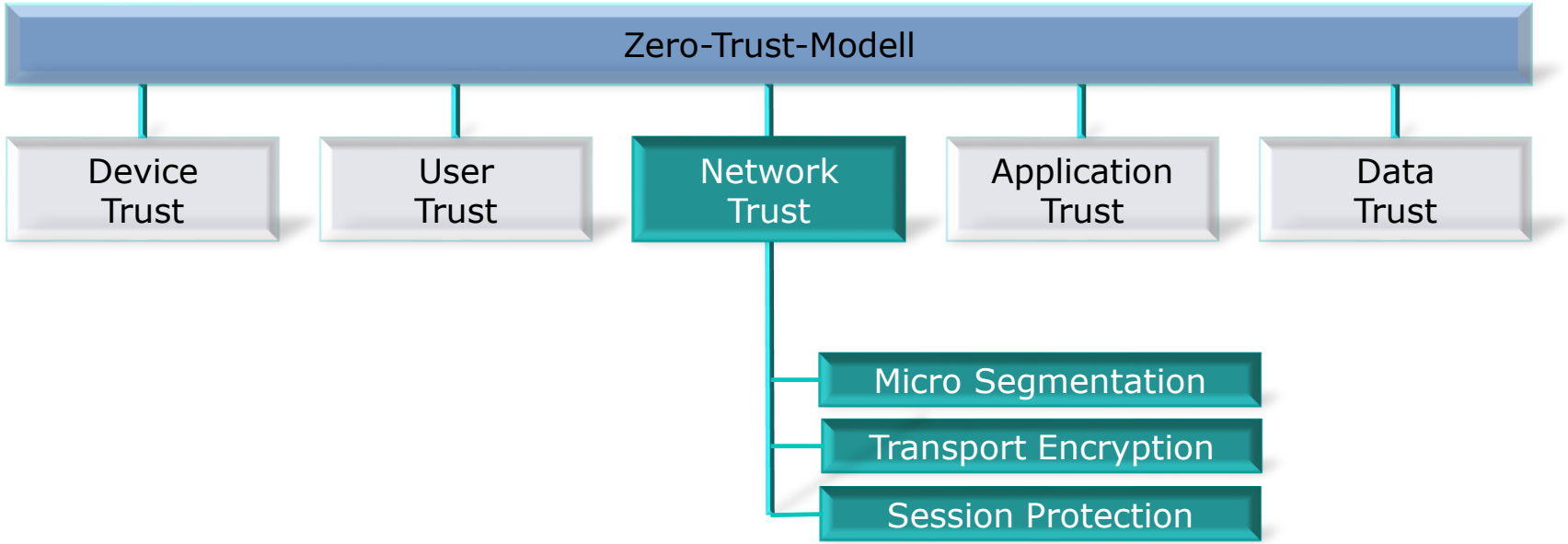
Zero Trust «Roadmap»

AVANTEC
Competence. Security. Trust.



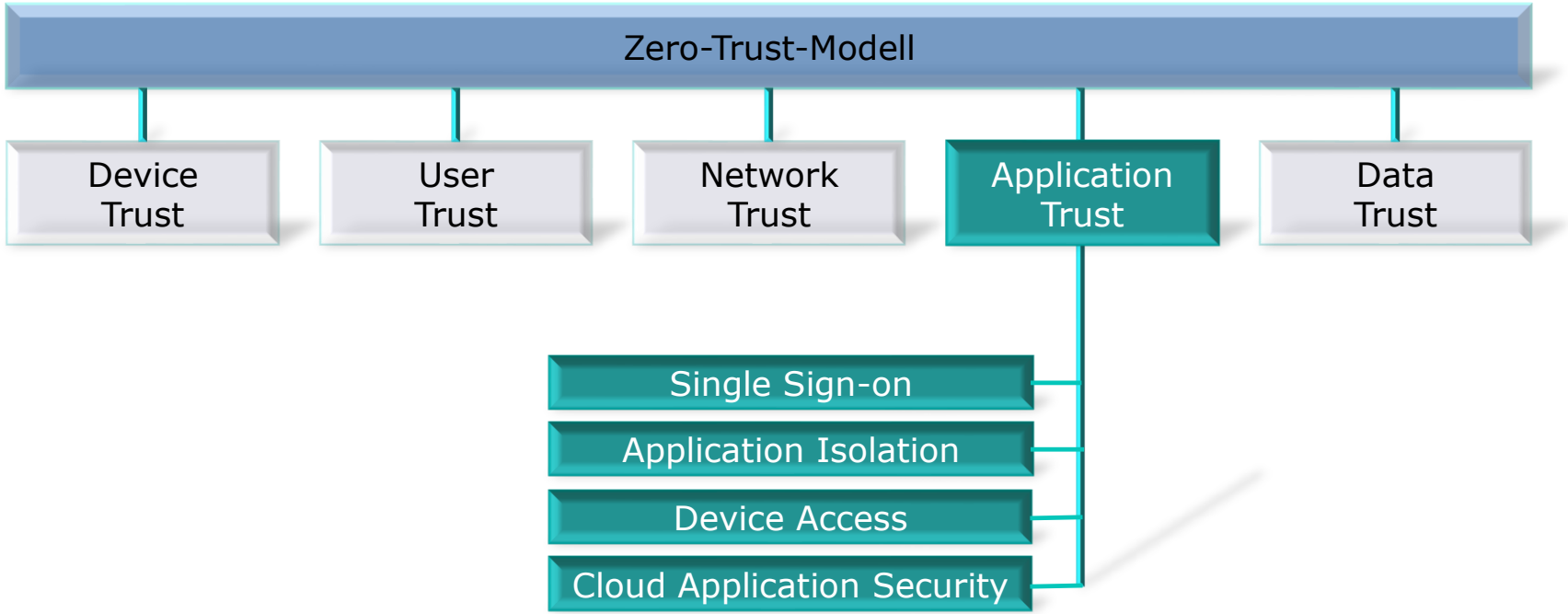
Zero Trust «Roadmap»

AVANTEC
Competence. Security. Trust.



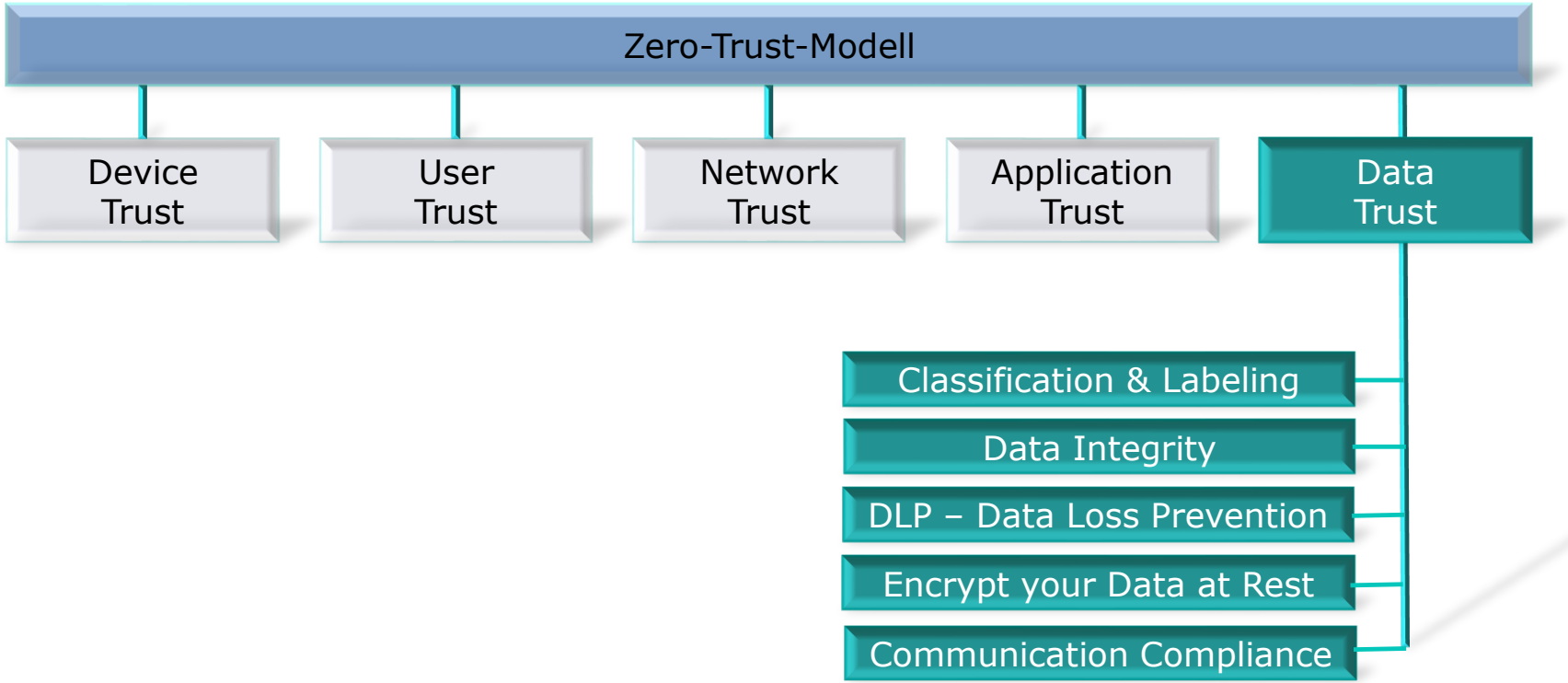
Zero Trust «Roadmap»

AVANTEC
Competence. Security. Trust.



Zero Trust «Roadmap»

AVANTEC
Competence. Security. Trust.



Beispiel aus der Praxis

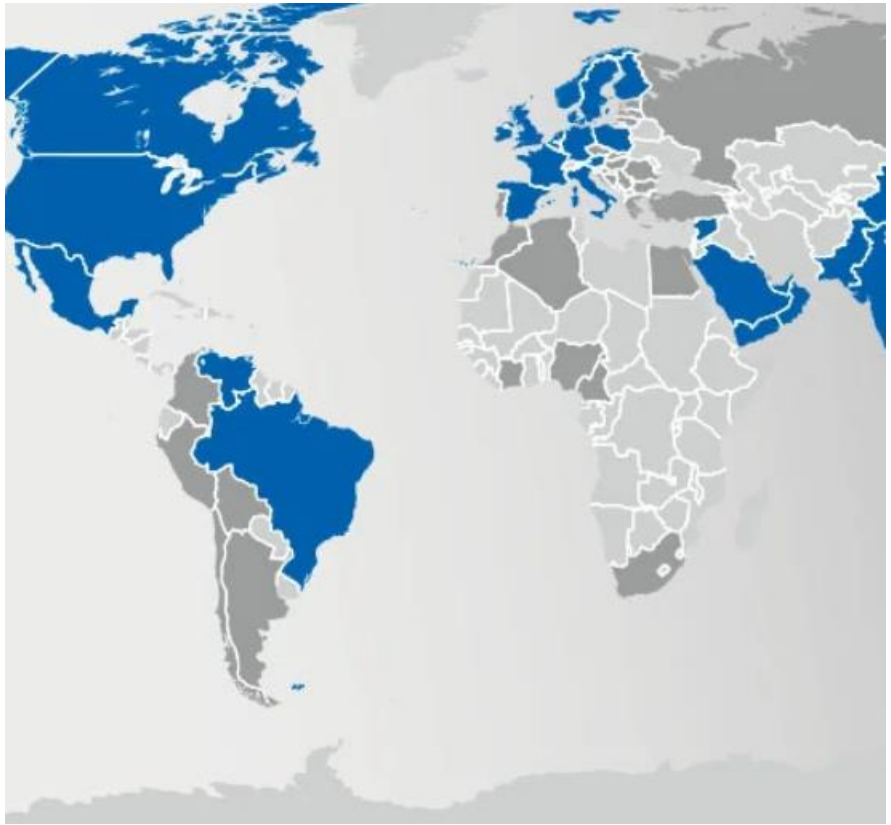
AVANTEC
Competence. Security. Trust.

Industriekunde

4'500 Mitarbeitende weltweit

50 Standorte International

Zero Trust Einführung Weltweit

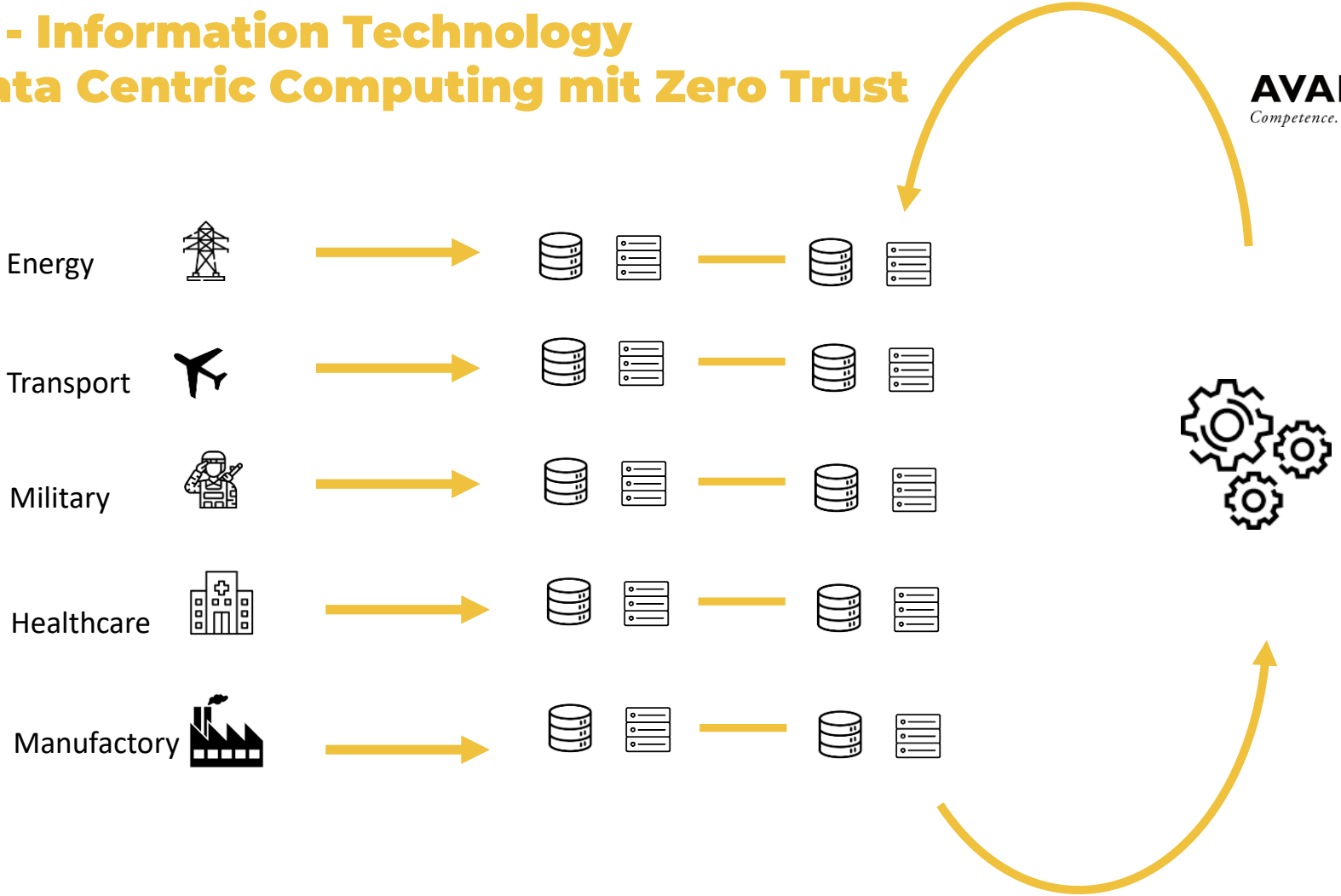


IT - Information Technology
Zero Trust Einführung & Strategie

AVANTEC
Competence. Security. Trust.

IT - Information Technology
Data Centric Computing mit Zero Trust

AVANTEC
Competence. Security. Trust.



OT – Operational Technology
Physische Prozesse

AVANTEC
Competence. Security. Trust.

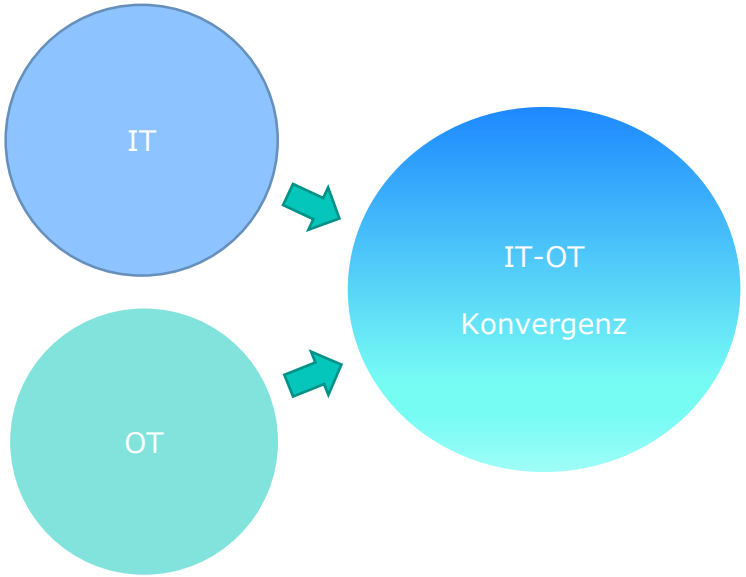
OT – Operational Technology
Monitoring and Control Based Computing

AVANTEC
Competence. Security. Trust.

IT - OT Konvergenz
Mehrwert von Zero Trust durch Konvergenz

AVANTEC
Competence. Security. Trust.

Industrie 4.0



Zero Trust Best Practices – 10 Schlüsselelemente

AVANTEC
Competence. Security. Trust.

1. Security-Strategie Anpassung: «Der neue Perimeter ist das Device»
2. Security-Strategie Anpassung: «Assume Breach» weg von der Verteidigung, hin zur Detection
3. Definieren Sie Ihre «Zero Trust Maturität»
4. Definieren Sie Ihre Security-Referenz-Architektur «Cover the place»
5. Definieren Sie Ihr Sensitivity- & Retention-Labels
6. Definieren Sie Ihre Communication-Compliance
7. Aktivieren Sie «Multi-Factor-Authentication» für alle Benutzer und Administratoren
8. Ersetzen Sie alle Passwörter – verwenden Sie «Passwordless»
9. Segmentieren Sie Ihr Netzwerk in «Mikrosegmente & Applikations-Zonen»
10. Steuern Sie alle Benutzer, Zugriffe und Geräte über Security Policy Enforcement

Zero Trust Best Practices – Fazit

AVANTEC
Competence. Security. Trust.

- Ziehen Sie einen erfahrenen Berater bei, der Sie bei der Ausarbeitung der für Sie geeigneten Strategie unterstützt und Sie während dem Projekt begleitet.
- Definieren Sie Ihren Security-Level Bedarf
- Nehmen Sie sich die Zeit, die es braucht, um das Prinzip von Zero-Trust sauber zu planen bevor Sie mit der Umsetzung beginnen.
- Führen Sie Zero Trust schrittweise ein, dabei kann die Reihenfolge individuell auf Ihre jetzige Situation angepasst werden.
- Jede Umgebung ist anders – definieren Sie Ihr «Security Big-Picture»

AVANTEC
Competence. Security. Trust.

Pause