SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

Zero Trust

Oliver Schersand | Syntax

SYNTAX

Syntax: Oliver Schersand, Head of GRC EU

ORACLE | Sell Partner
Expertise in Oracle Cloud Platform in North America

SAP Gold Partner

IBM Silver Business Partner

aws partner network
Advanced Consulting Partner
MSP Partner

Gold Microsoft Partner
Microsoft

1. Was ist Zero Trust?
2. Warum Zero Trust?
3. Komponenten
4. Grundsätze
5. Zero Trust Modell
6. Topology
7. Zero Trust Roadmap
8. Herausforderungen

Kapitel 1

Was ist Zero Trust?

Was ist Zero Trust?

Definition

Zero Trust ist ein Sicherheitskonzept in der Informationstechnologie, das darauf basiert, keinem Benutzer, Gerät oder Netzwerkverkehr innerhalb oder außerhalb des Netzwerks automatisch Vertrauen zu schenken.

Kapitel 2

Warum Zero Trust?

Warum Zero Trust?

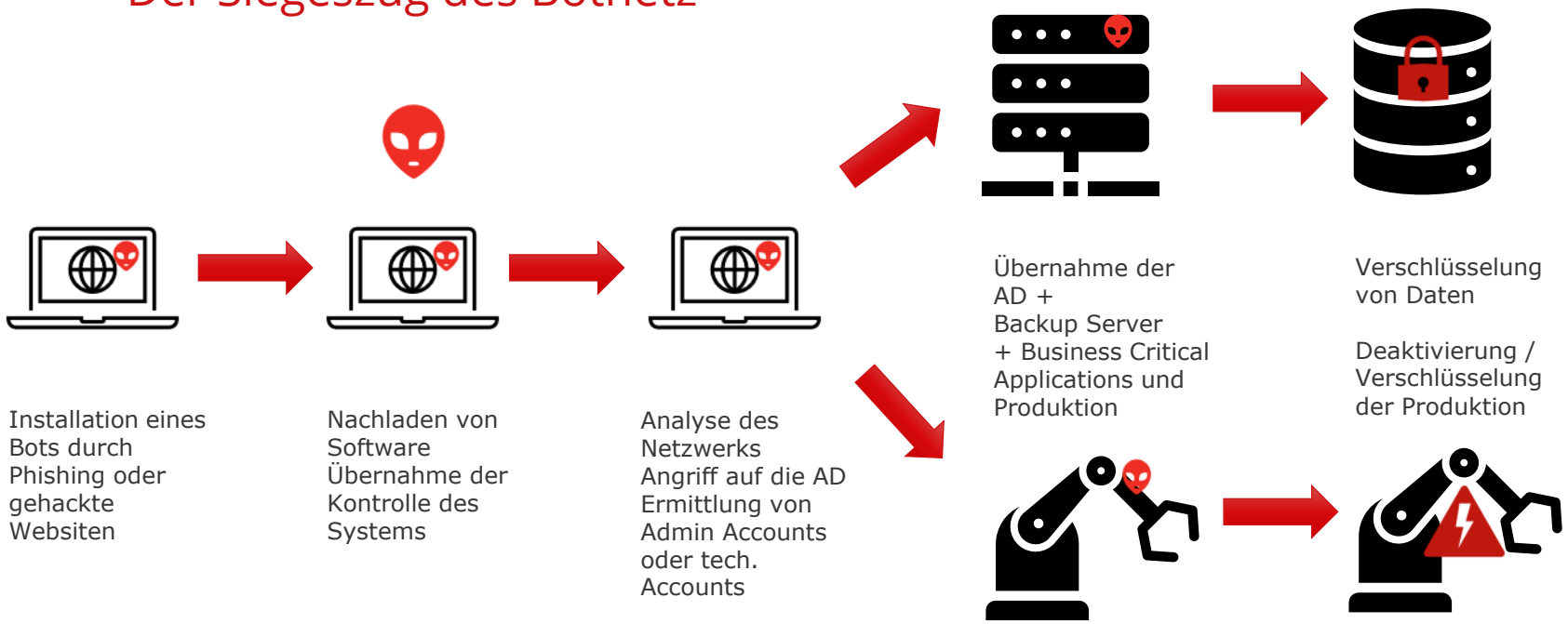
Hintergrund

DER ZERO TRUST ANSATZ IST DIE ANTWORT AUF DIE FOLGENDEN HERAUSFORDERUNGEN

- Typische Cyber-Angriffe nutzen Schwächen von klassischen IT Sicherheitsstrukturen aus.
- Umbau der klassischen IT in ein Multi Cloud / Multi Provider Ansatz.
- Mobilisierung der Arbeitswelt

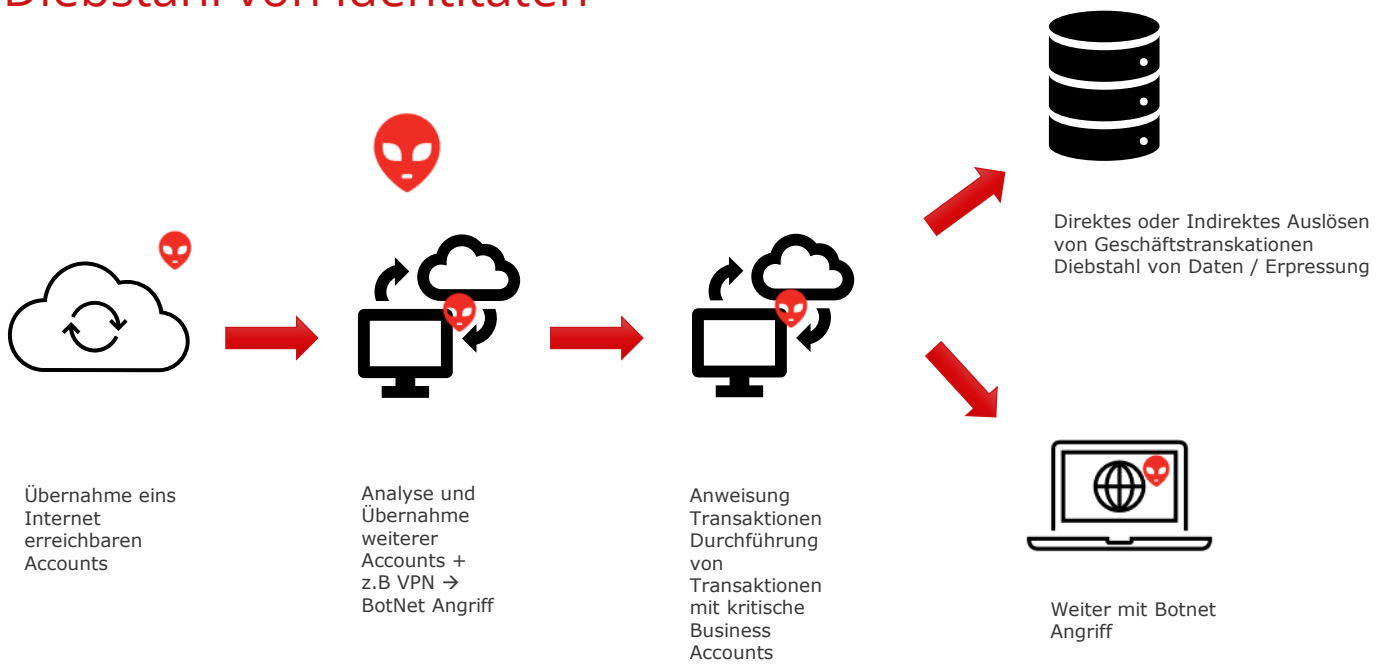
Warum Zero Trust?

Der Siegeszug des Botnetz



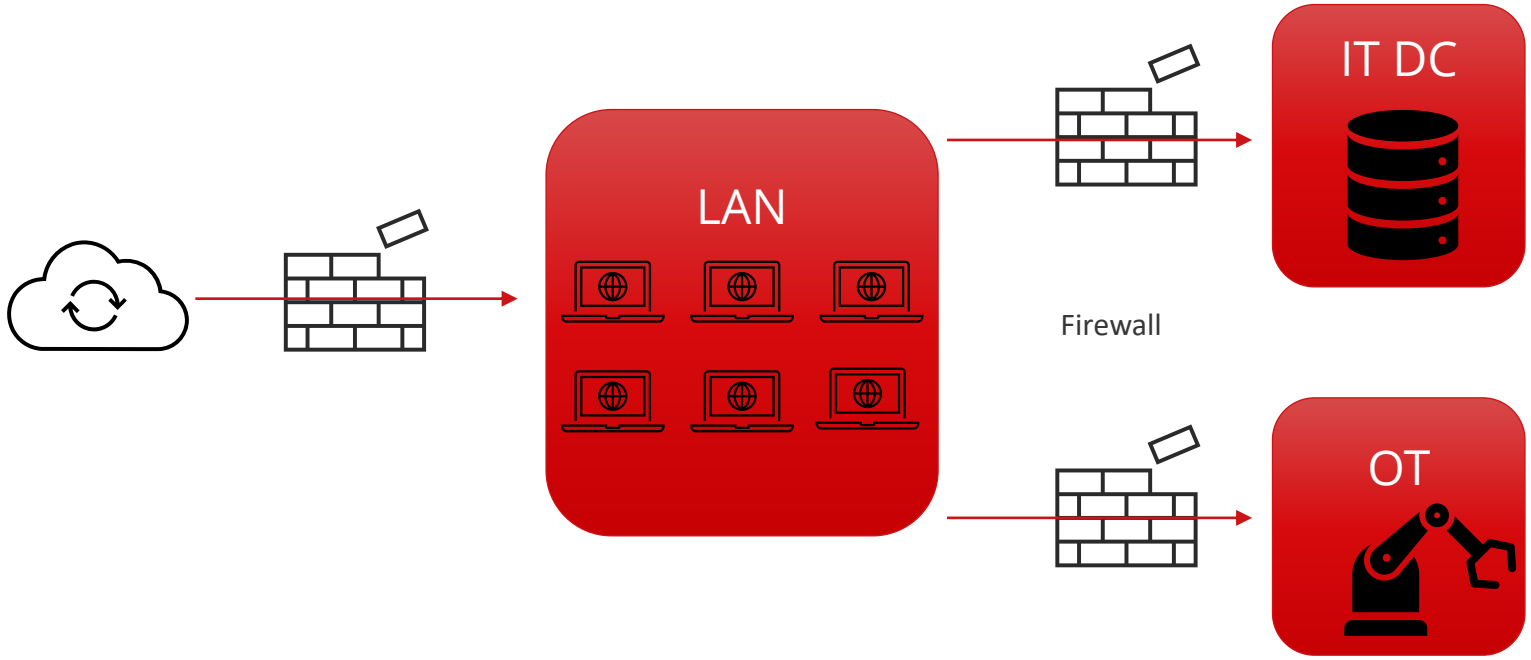
Warum Zero Trust?

Diebstahl von Identitäten



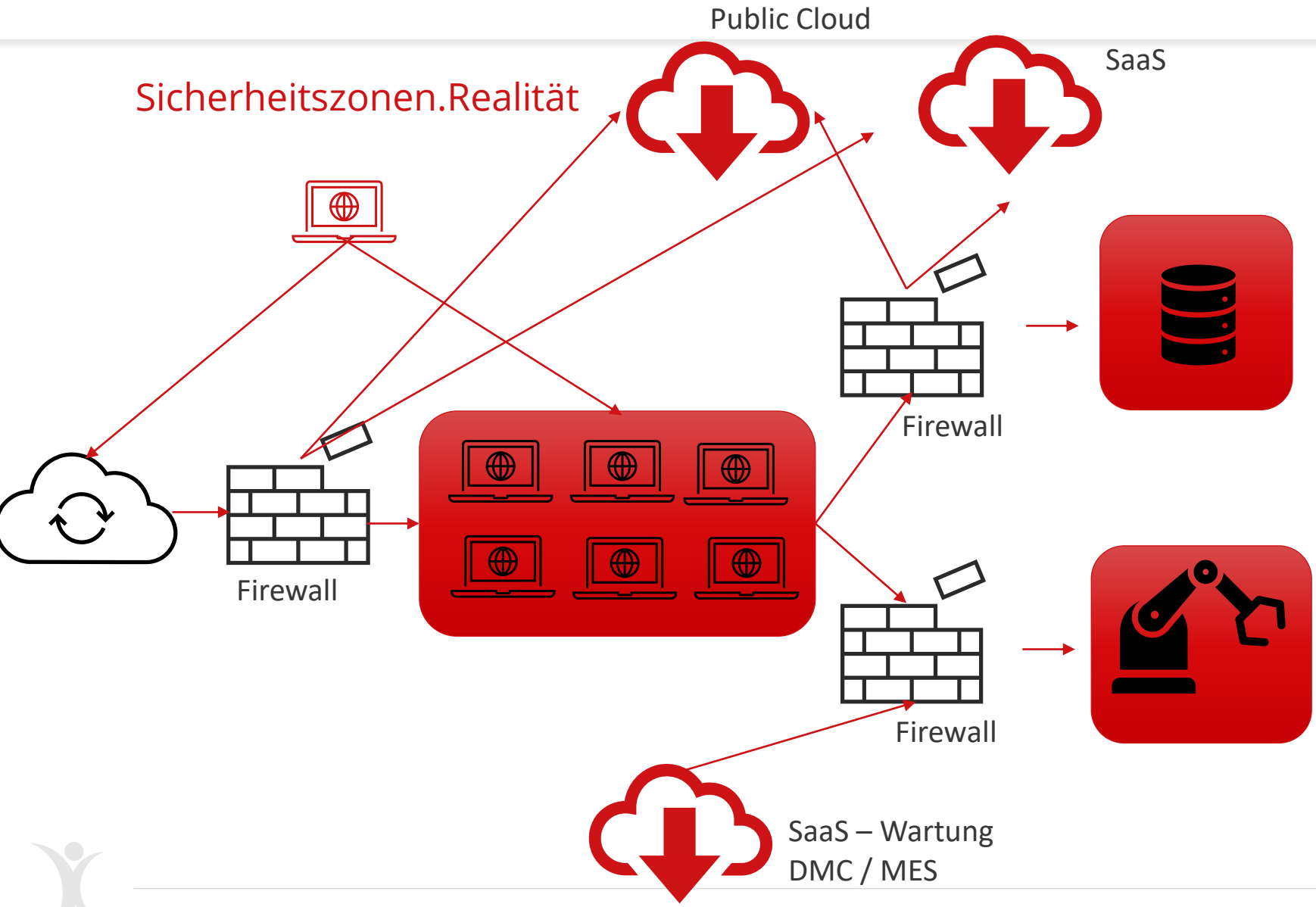
Warum Zero Trust?

Sicherheitszonen.Idee



Warum Zero Trust?

Sicherheitszonen.Realität



Kapitel 3

Zero Trust - Die Komponenten

Die Komponenten

Identity
Nutzer
Berechtigungen

Device
Server,
Handy,
PC

Anwendung

Netzwerk
Firewall,
Segmentation

Daten
Data Flow
Encryption

Infrastruktur
Automatisation
,Orchestration
& Analytics
Reaction
Compliance

Kapitel 4

Zero Trust - Grundsätze

Grundsätze

Identitäten: Starke Mechanismen um Identität festzustellen sowie Überwachung aller Aktionen inklusive des Berechtigungskonzept

Devices: Kontinuierliche Überwachung der Compliance und Untersuchung auf Schwachstellen und ungewöhnliches Verhalten

Netzwerk: Nur verschlüsselte Verbindung. Kontinuierliche Überwachung und automatisierte Reaktion. Segmentierung und Mikrosegmentierung

Anwendung: Welcher Benutzer braucht wann welchen Zugriff auf welche Anwendung. Integration des Anwendungsüberwachung.

Daten: (automatisierte) Klassifizierung der Daten, Verschlüsselung bei der Speicherung und in der Übertragung. Vereinheitlichung des Zugriffskonzept von Infrastruktur und Anwendungen. Automatisierte Erkennung von Missbrauch

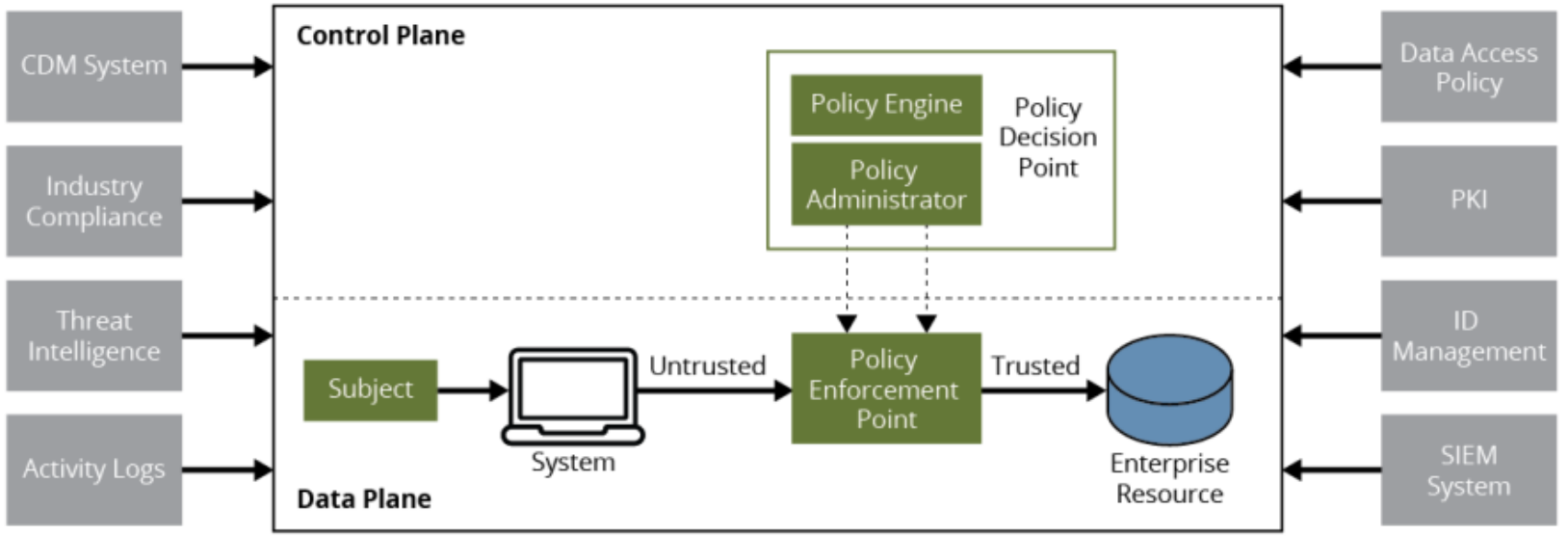
Infrastruktur: Automatisierte Härtung und kontinuierliche Überwachung, Reporting und automatisierte Reaktion auf typische Angriffe. Orchestrierung der gesamten Sicherheitsarchitektur

Kapitel 5

Zero Trust - Modell

Zero Trust Modell

NIST 800-207 Framework

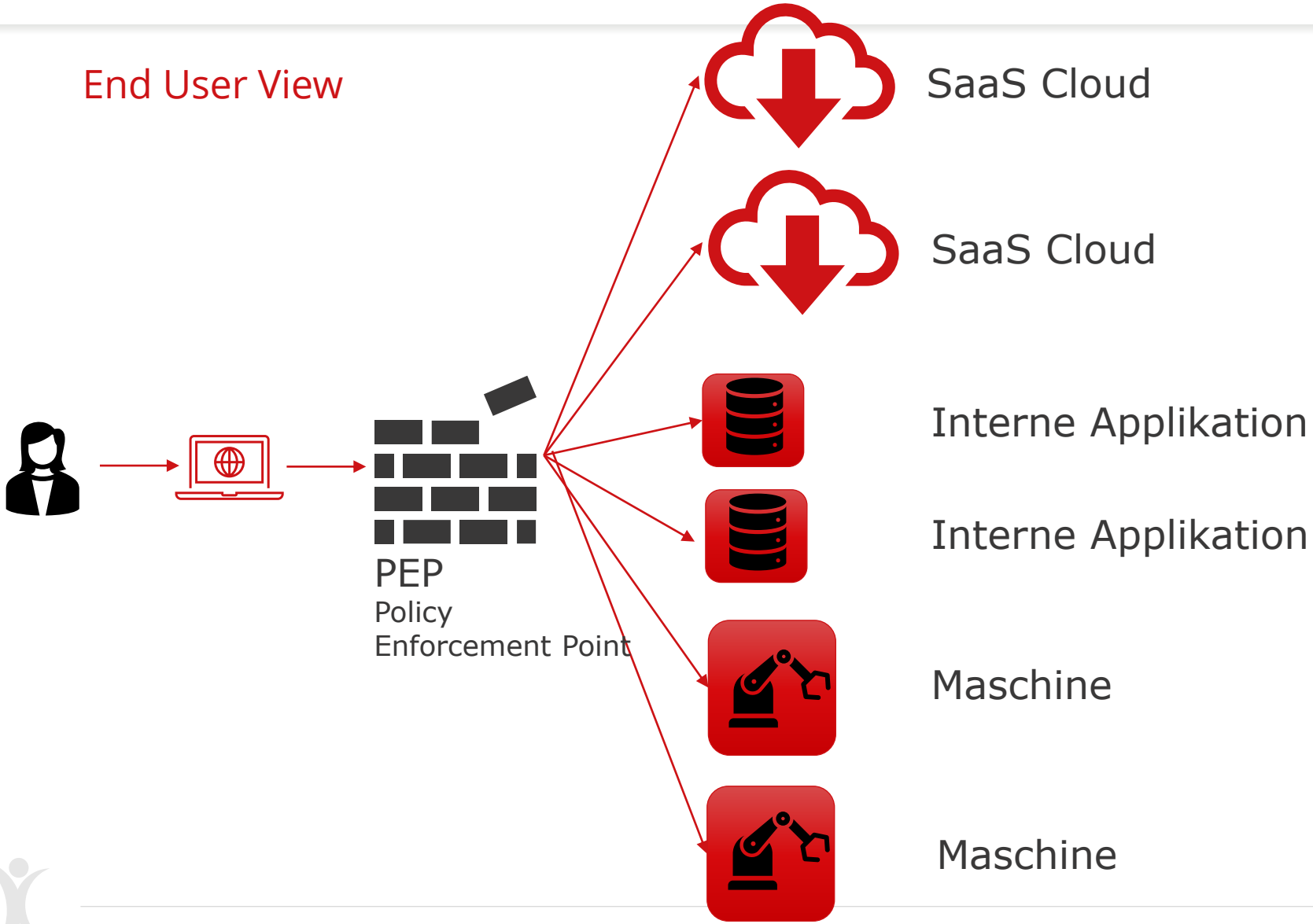


Kapitel 6

Zero Trust - Topology

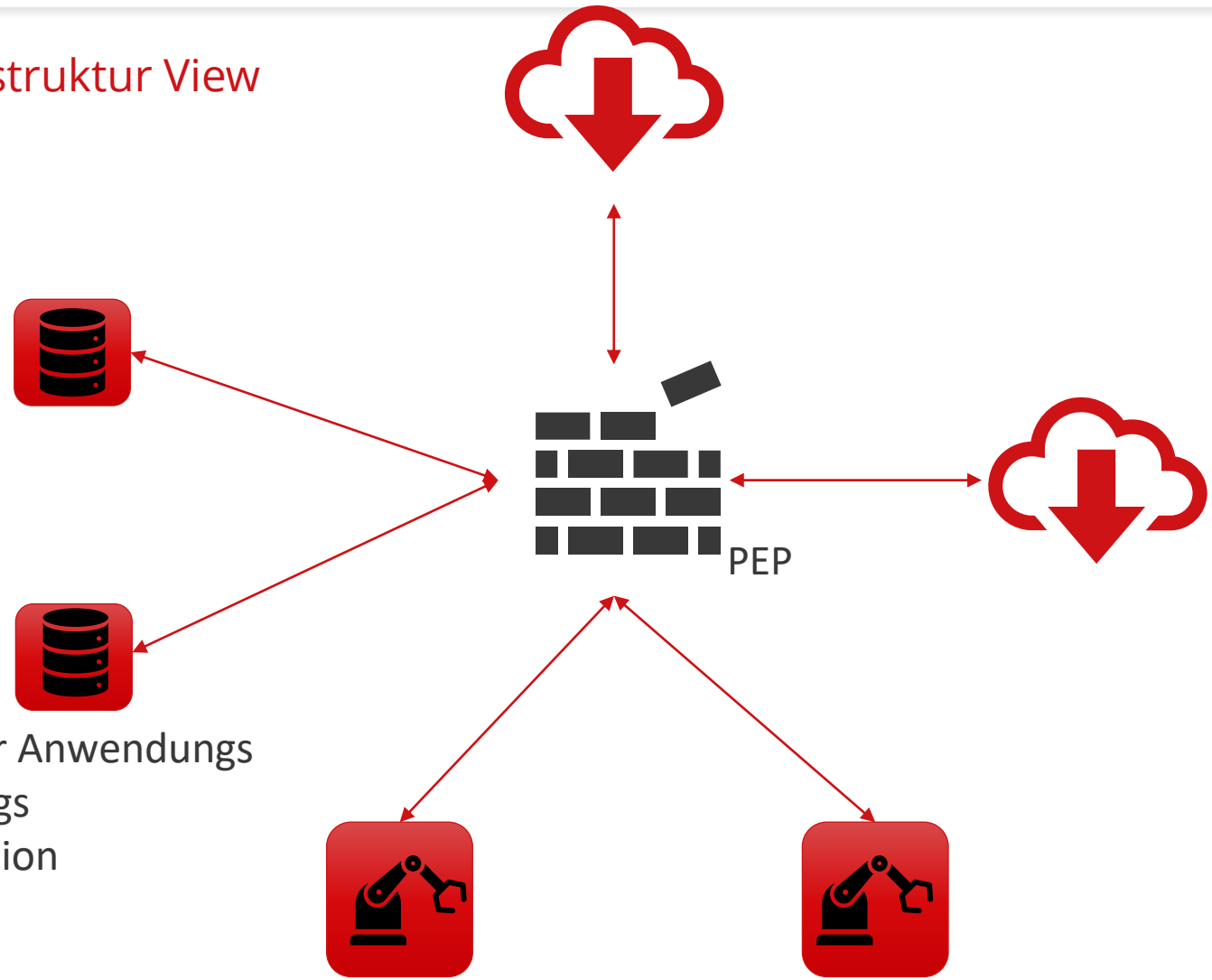
Topology

End User View



Topology

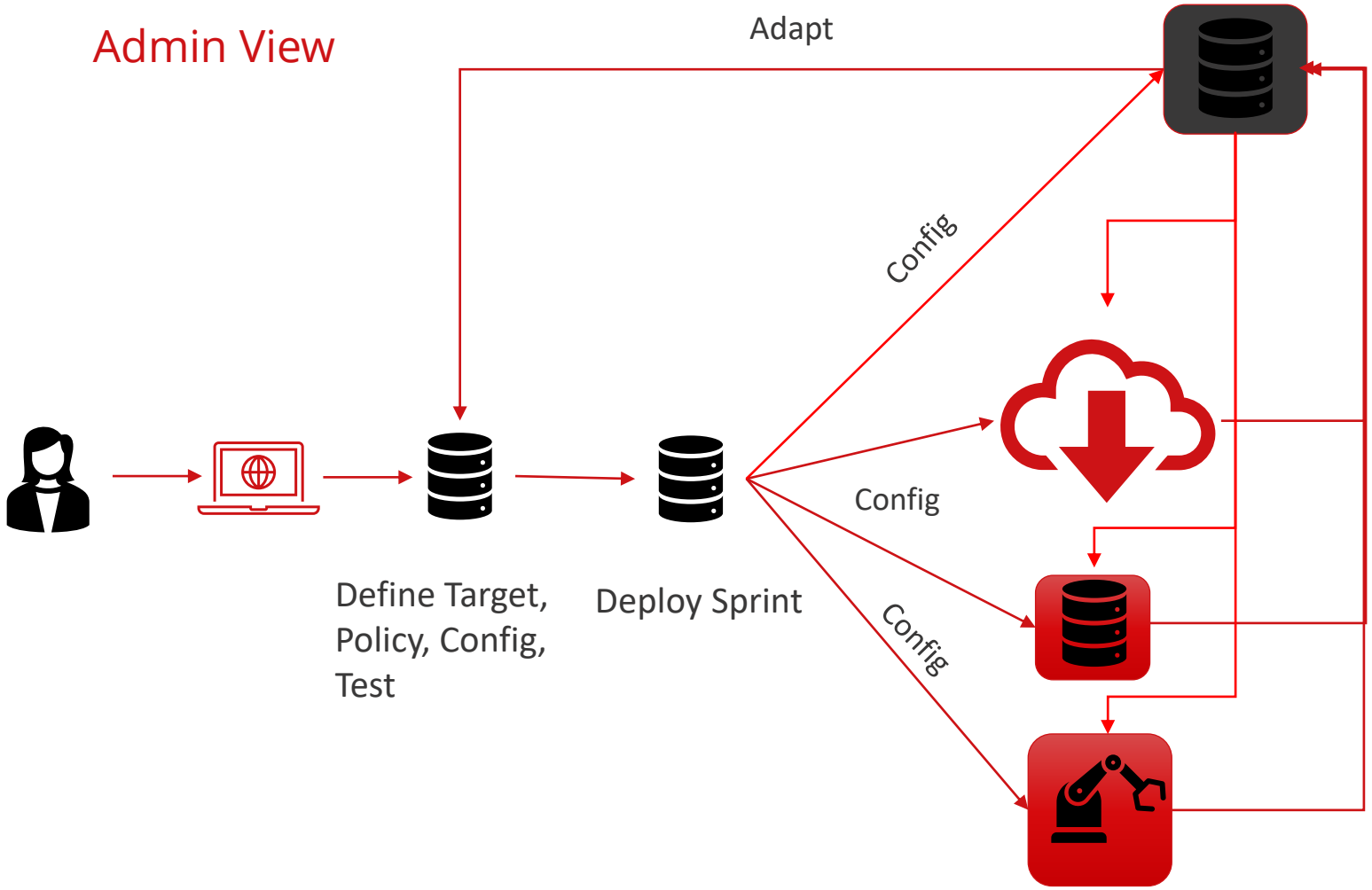
Infrastruktur View



Kontrolle der Anwendungs
- Anwendungs
Kommunikation

Topology

Admin View



Kapitel 7

Zero Trust - Roadmap

Roadmap

Risiko orientierter Ansatz

Vorbereitung: IT Security / Anwendungssicherheit / OT Security müssen die gleiche Definition der Datenklassifizierung besitzen.

Klassifizierung: Daten und Anwendungen müssen bezüglich Ihres Risiko klassifiziert werden.

Selektion: Festlegen der Benutzer, Devices, Anwendungen und Daten die als erstes in das Zero Trust Framework übernommen werden müssen.

Roadmap

Komponenten der Strategie

Splitten des Projekts in die 6 Bereiche des Zero Trust

- User, Devices, Netzwerk, Anwendungen, Daten, Infrastruktur

Selektion der Tools pro Bereich

All selektierten Tools Infrastruktur müssen integriert werden.

- Automatisation & Orchestration &
- Visiblity & Monitoring
- Korrektion von Einstellung
- Automatisiert Reaktion auf Securit Events.
- Überwachen von Schwachstellen
- DLP, EDR, SIEM, IPS .....

Definition eine Phasen Modell diese Tools auszurollen.

Herausforderungen

Zero Trust integrierte fast alle Security Tools in ein Gesamtkonzept.

Zero Trust erfordert ein übergreifendes Verständnis welcher Mitarbeiter benötigt welche Anwendung und welche Rechte in welchen Anwendungen.

Zero Trust erfordert eine **sehr präzise Übersicht** über die **Devices und Anwendungen und Daten** eines Unternehmens

Zero Trust erfordert ein genaues Verständnis der Kommunikationsbeziehungen zwischen Anwendungen.

Zero Trust transformiert die eigenen Anwendungen in ein Saas Ansatz. D.h die interne IT muss „cloud native“ denken und Arbeiten.

Zero Trust **transformiert den klassischen Netzwerk** Ansatz in das Access Concept eines SaaS Anbieters.

Zero Trust erfordert Anwendung, Devices in einem Cloud Native Ansatz zu managen.