T.I.S.P./T.P.S.S.E. Community Meeting 2025

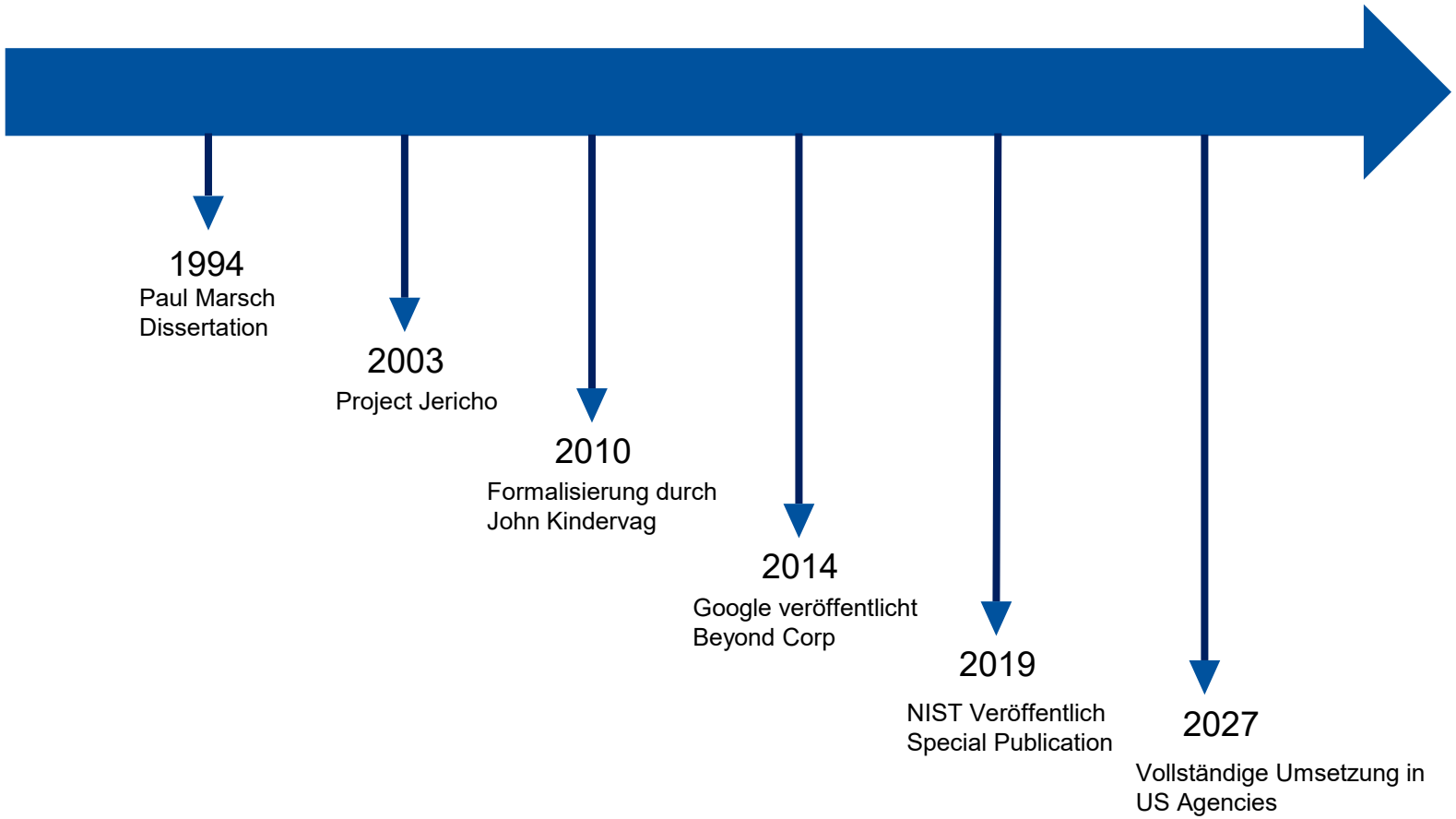
Berlin, 04. - 05.11.2025

Zero Trust – Verify Everything

Andreas Dietle, Giesecke + Devrient

Was ist Zero Trust (verify everything)

Meilensteine in der Geschichte von Zero Trust

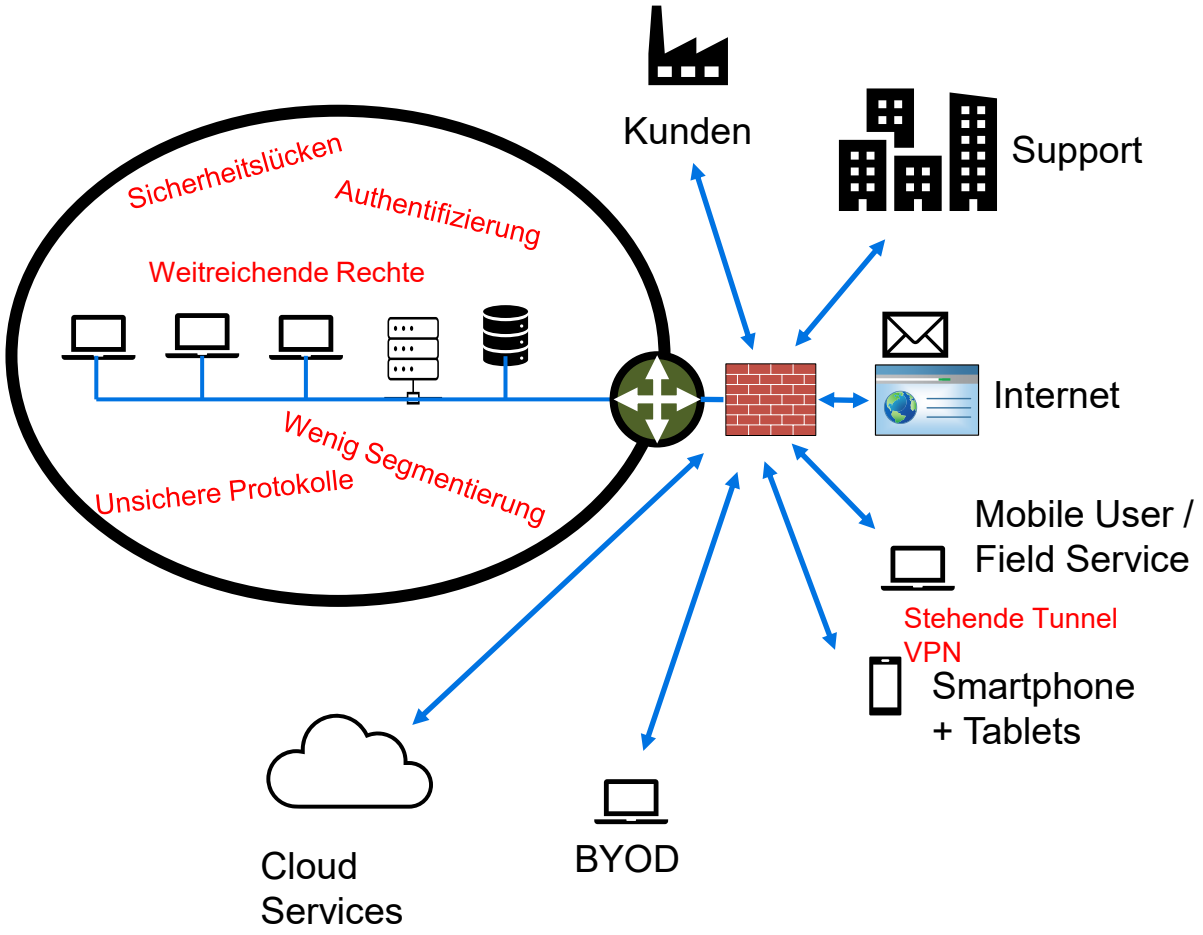


Historie

Perimeter Sicherheit

Intern = vertrauenswürdig

Extern = unsicher



Nachteile Perimetersicherheit

Perimeter Sicherheit

Zero trust

- Jede Verbindung untergräbt die Perimeter Sicherheit
- Lokationsorientiert
- Mangelnde Skalierbarkeit
- Eingeschränkte Möglichkeit von BYOD

Das Prinzi … ne
zunächst a …
Zugriffsant …

Grundprinzipien

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Verify explicitly

Für jede Anfrage nach einer Resource

- Identität der Benutzer (Person / Dienst)
  - Starke Authentifizierung NIST AAL2 oder höher
  - Einmalige Anmeldung (SSO)
- Geräte Konformität
  - Geräteklasse (PC, Mobile, BYOD)
  - Sicherer Startprozess
  - Status der Aktualisierungen
  - Anti Schadsoftware Status
  - Maschinen Authentifizierung
  - Etc.

Grundprinzipien

Leased privilege

You shall not pass

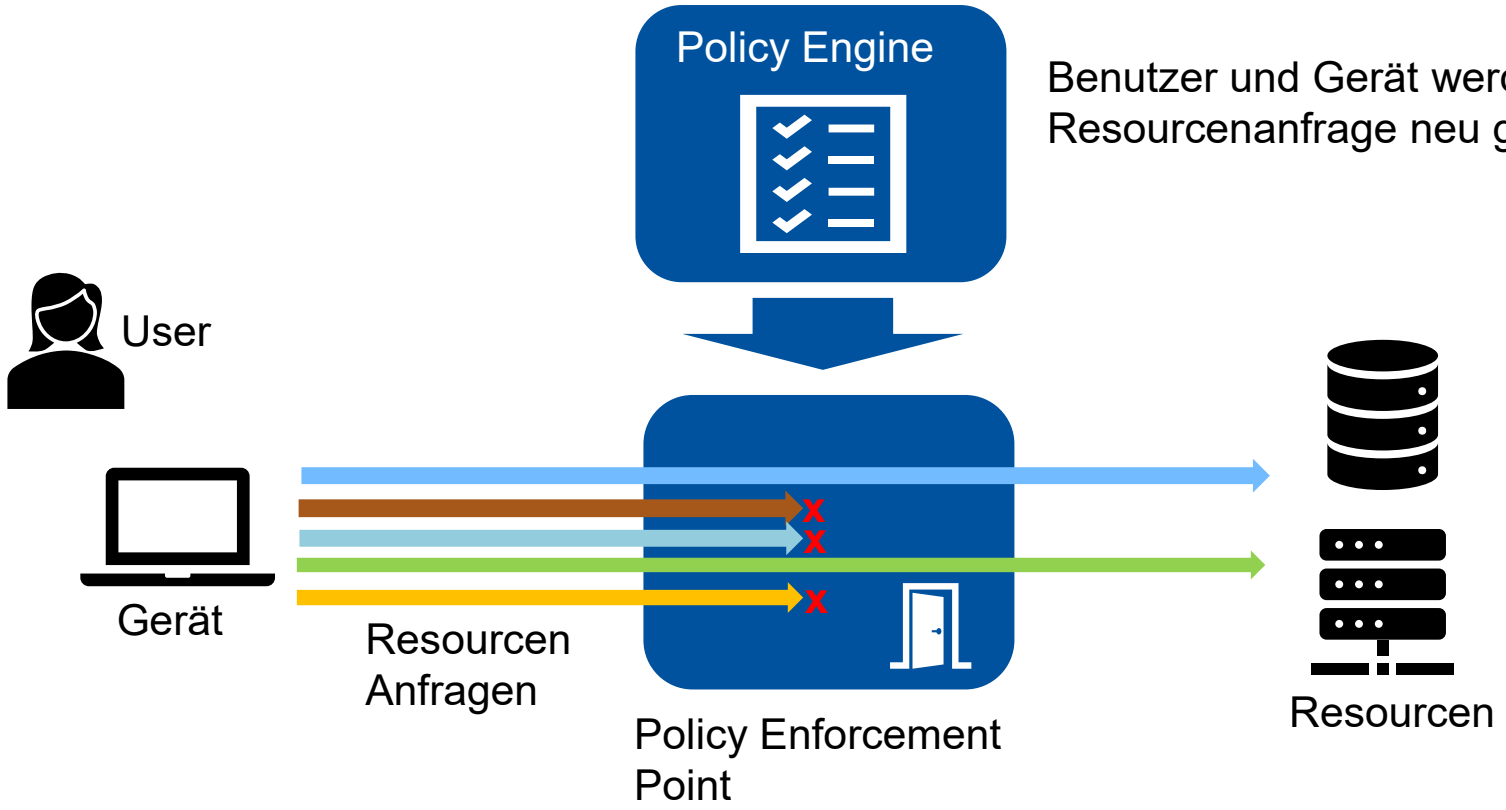
- Zugriffskontrolle
  - Benutzer + Systeme
  - Rollenbasiertes Zugriffsmanagement (PAM)
  - Minimale Zugriffsrechte (JEA)
  - Zeitliche Begrenzung (JIT)

Grundprinzipien

Assume Breach

- Maßnahmen
  - Micro Segmentierung
  - Abschalten unsicherer Protokolle
  - Verschlüsselung des Datenverkehres
  - Monitoring
  - EDR / XDR

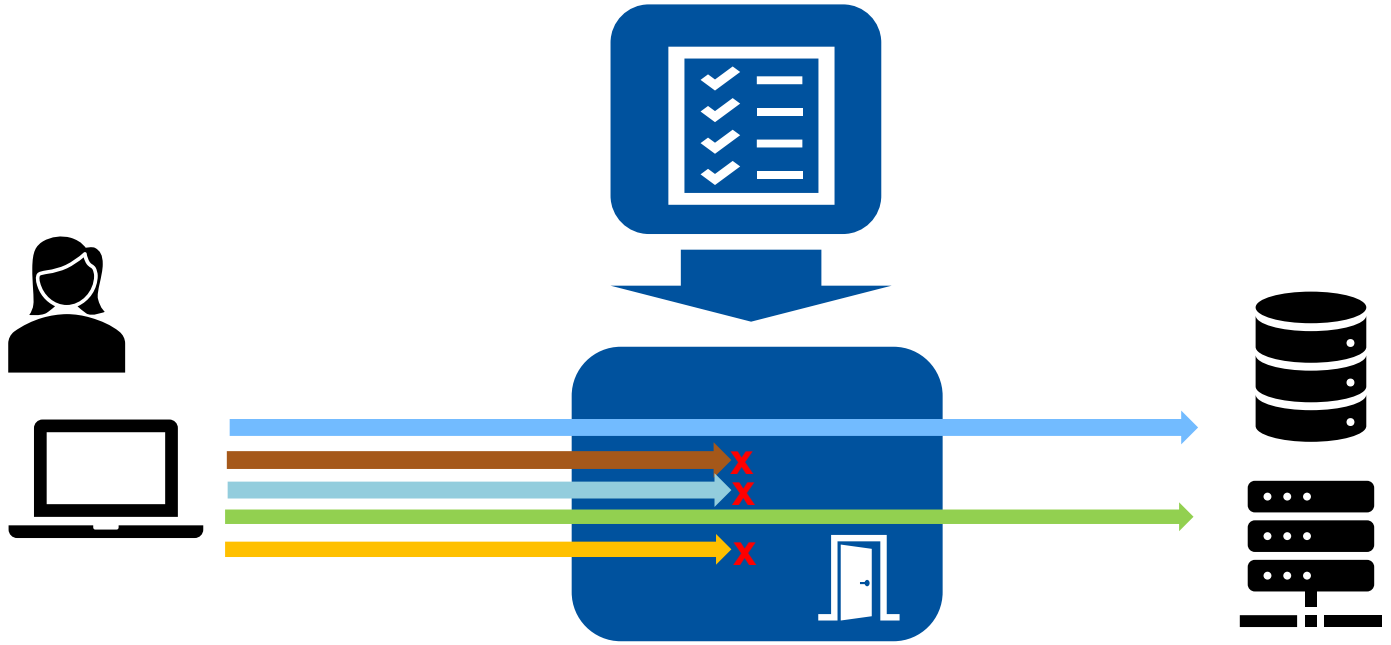
Kernkomponenten von Zero Trust*



*Auf Basis des NIST Framework

Regeln Beispielhaft

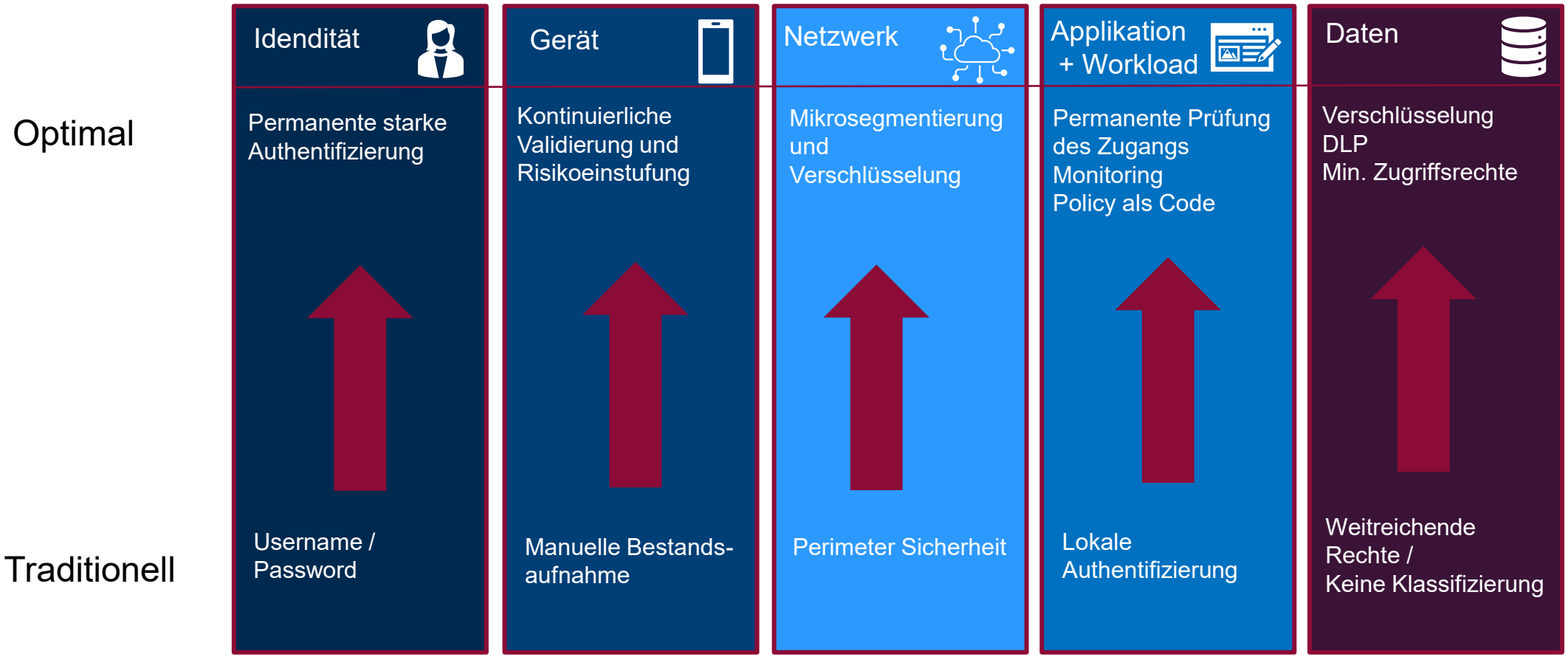
- **Authentifizierung**
  - OTP Token
  - Zertifikat
- **Status des Gerätes**
  - Managed,
  - Patchlevel
  - PC
  - Mobilgerät
- **Mitarbeiter**
  - Interne
  - Externe
- **Zugriffsanfrage**
  - Intranet
  - Kronjuwelen
  - HR
- **Geo Lokation**
  - Embargoländer
  - Nur Europa / Deutschland



Regeln übersichtlich gestalten!

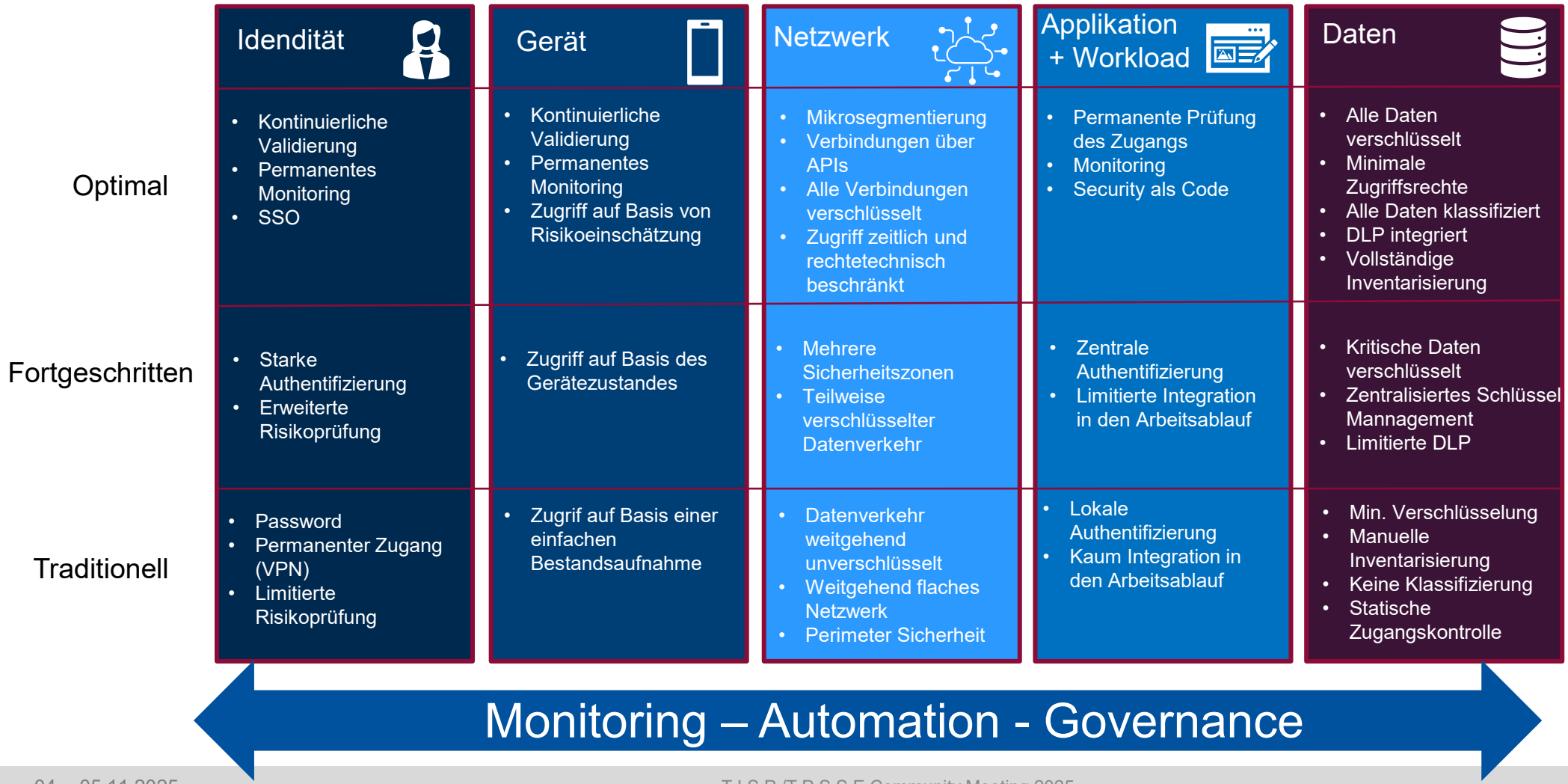
Reifegradmodell Zero Trust Beispiele

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Reifegradmodell Zero Trust

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Herausforderungen

- Verfügbarkeit und Sicherheit der Control Plane
- Altsysteme -> Hybridlösungen
- Fehlende Standardisierung
- Fehlende Interoperabilität
- Umsetzung On Premise sehr schwierig