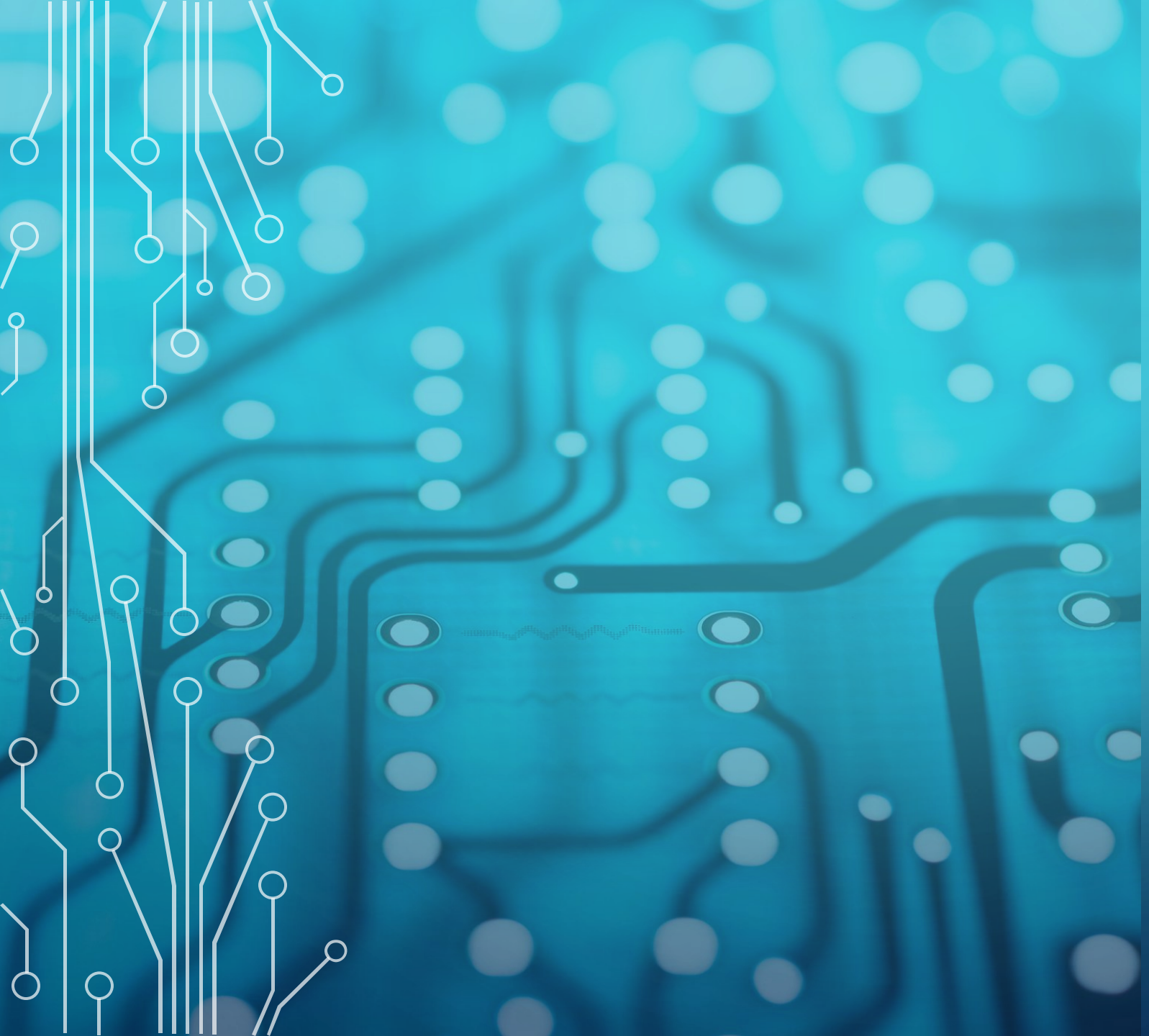
ZERO TRUST – ANSATZ UND PROTOTYP

BWCAMPUSNETZ, UNIVERSITÄTS-IT MANNHEIM, 2025



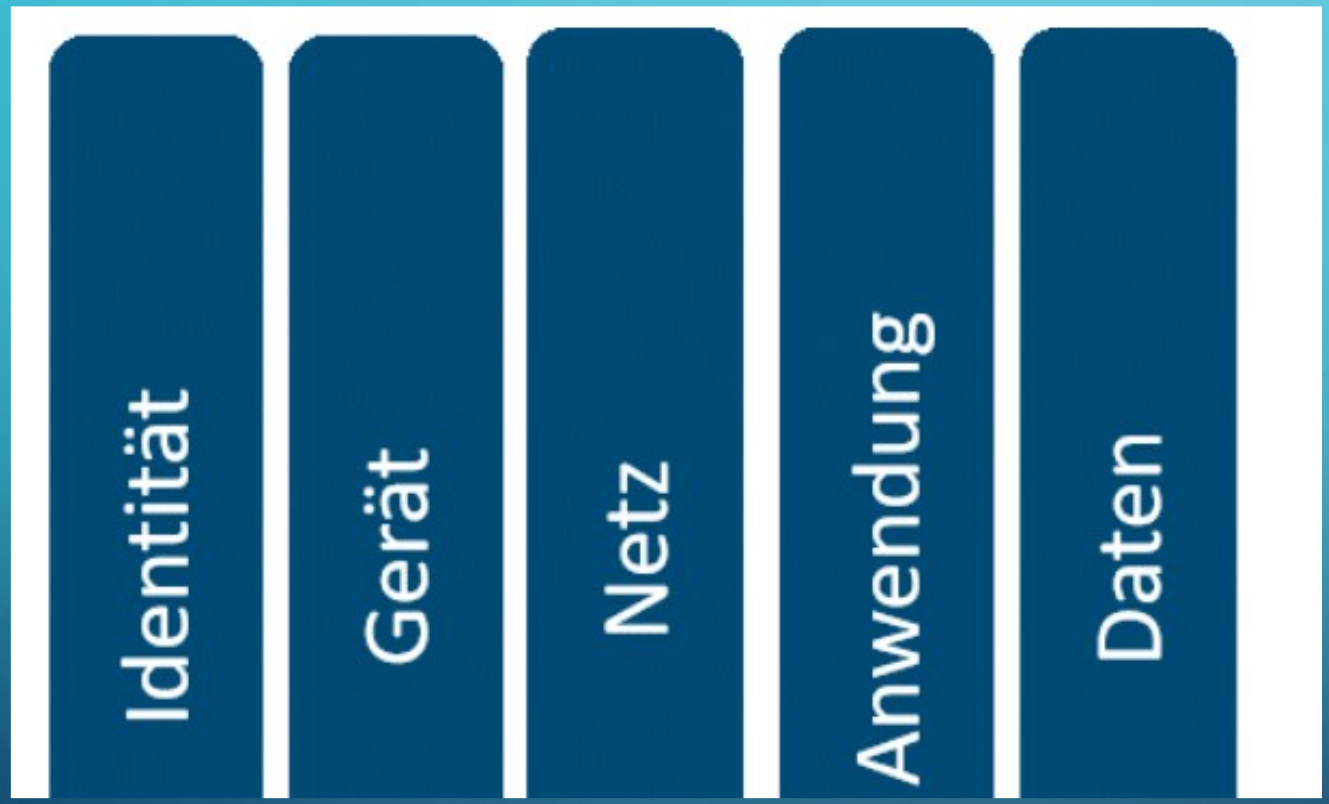
AGENDA

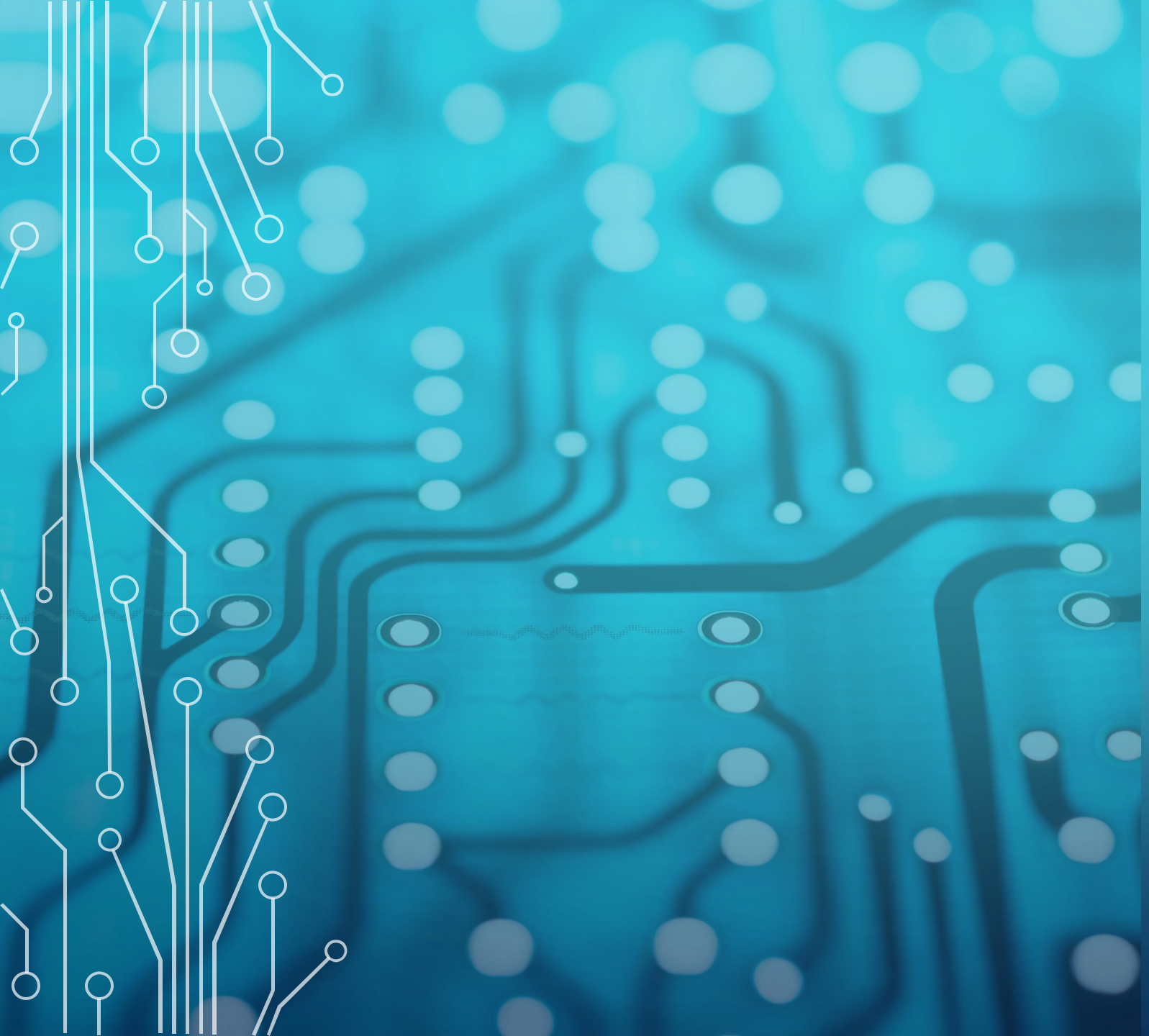
- **Ein bisschen Theorie**
- Zero Trust an der UNIT
- Fragen und Diskussion

GRUNDPRINZIPIEN ZERO TRUST MODELL

- Vertrauen nicht voraussetzen (never trust, always verify)
- Minimale Berechtigungen (Least Privilege)
- Mikrosegmentierung
- Kontinuierliche Überwachung (Continuous Monitoring)
- Sicherheitsrichtlinien durchsetzen (Enforce Security Policies)

5 SÄULEN – ZERO TRUST MATURITY MODEL





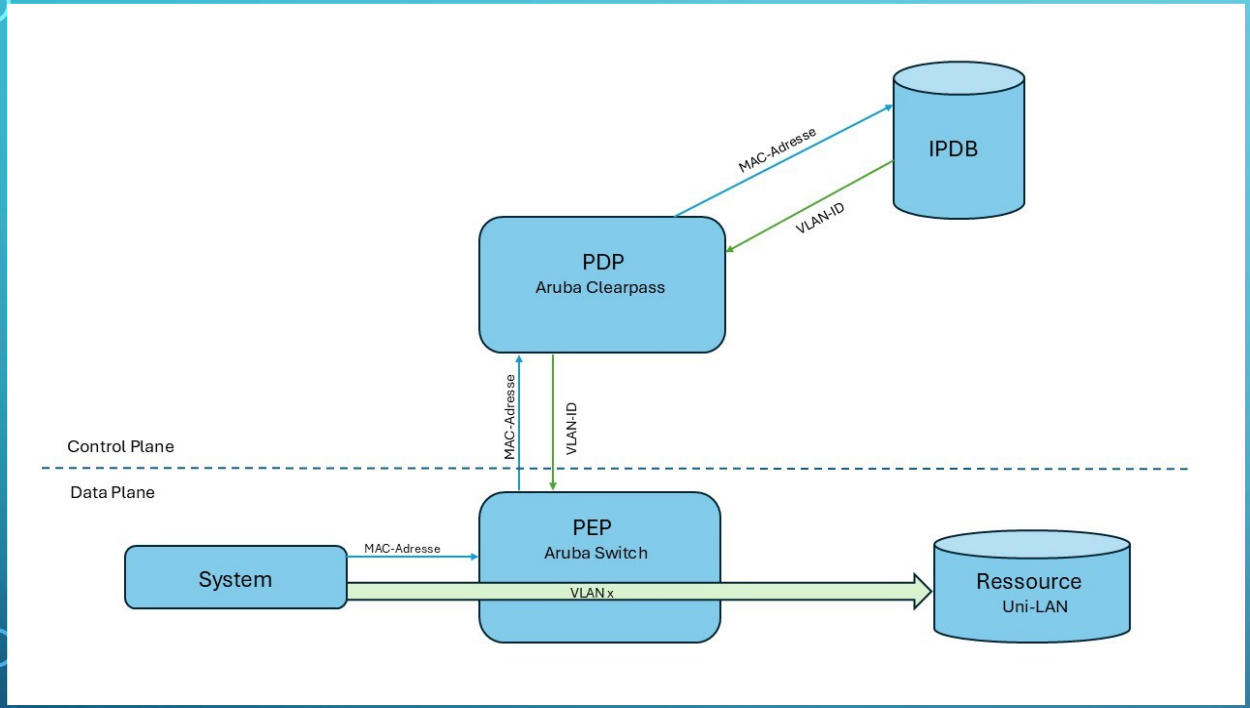
AGENDA

- Ein bisschen Theorie
- **Zero Trust an der UNIT**
- Fragen und Diskussion

SITUATION UNIT – WIE MACHEN WIR ZERO TRUST?

- Eindeutige Nutzeridentität (Uni-ID) für alle
- Zugriffsrechte basierend auf Attributen der Uni-ID → Verantwortlichkeiten, Flavours
- Geräte werden über MAC oder Uni-ID (802.1x) zugeordnet
- Gerätesicherheit muss mit einfließen (Endgerätemanagement)
- Auch benötigt: Überwachung, Protokollierung, User Awareness, Audits
- Projekte: Netzharmonisierung mit HP/Aruba, MFA, Endgeräteverwaltung, IDM Flavour Konzept, Erweiterung des zentralen Loggings

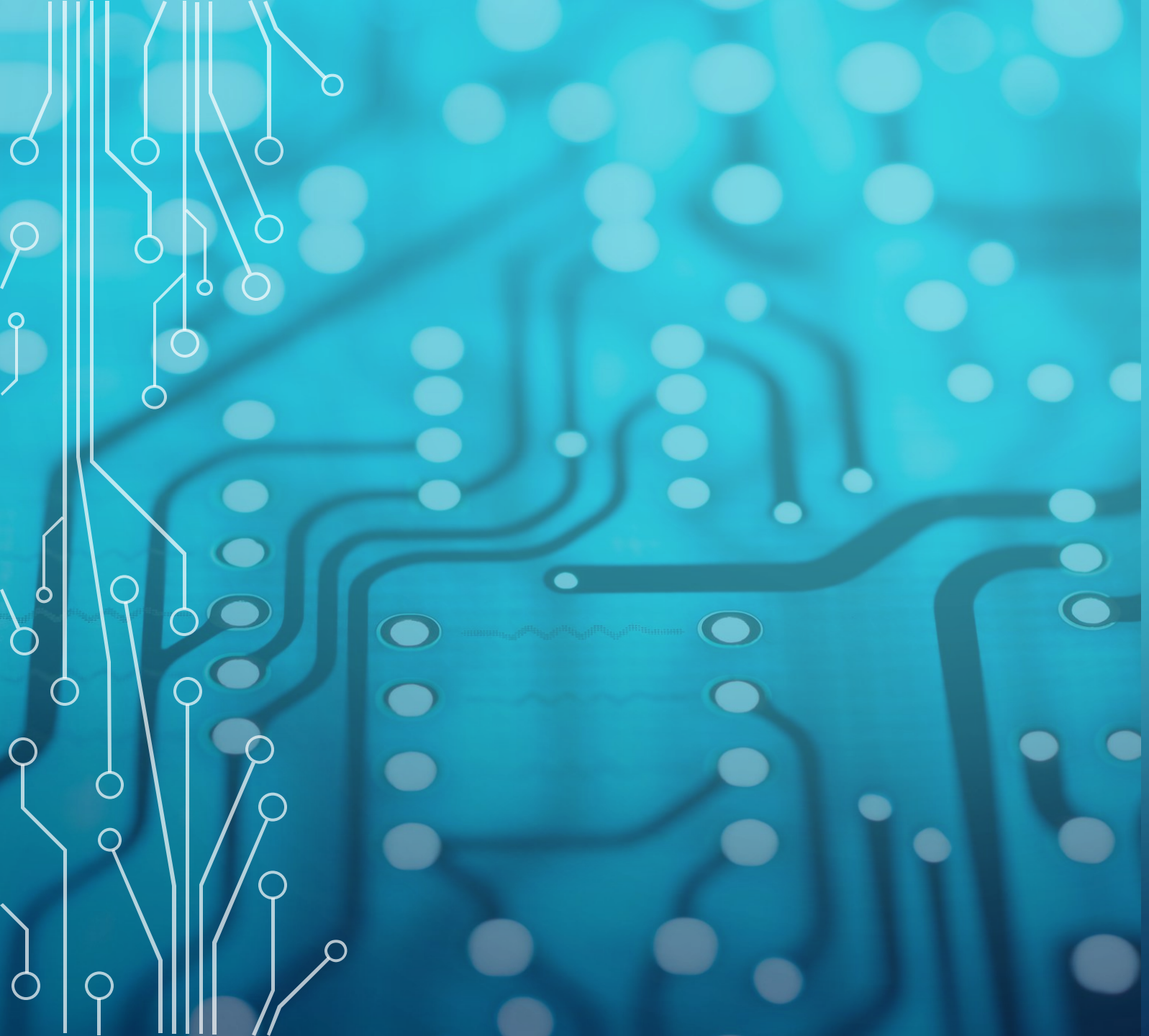
PROOF OF CONCEPT (POC)



- Säulen Identität, Gerät und Netz
- Basierend auf Geräteeigenschaften registrierter Geräte (LAN) oder Uni-IDs (WLAN)
- Mit HW- und SW-Komponenten von HP/Aruba

ENDZIEL UND DER WEG DORTHIN

- PoC hat funktioniert und soll in Zukunft ausgeweitet werden
- Geräteinformationen wie Patchlevel aus der Endgeräteverwaltung dazu
- Flavour Konzept als Berechtigungsmodell
- Integration ins Monitoring und Logfileauswertung



AGENDA

- Ein bisschen Theorie
- Zero Trust an der UNIT
- **Fragen und Diskussion**

FRAGEN UND DISKUSSION