BearingPoint

Remote Access neu gedacht:
Cyolo RPAM für Compliance, Sicherheit und Effizienz

Alexander Schwemberger

OT-Cybersecurity BearingPoint
November 2025

Agenda

1. Aktuelle Themen aus der Branche
   - Das Spielfeld der Cyberangriffe - die KI verändert alles
   - Ein kurzer praxisnaher Blick auf – NIS2
   - Cyber Resilience Act – Bürde oder Business Enabler?
2. Anwendungsfälle aus der Praxis
   - Ein Betreiber, (zu) viele Lieferanten
   - Maschineninseln
   - Air-gapped Hochkritische Umgebung
   - Sicherer Fernzugriff als Teil des Service Portfolios

Workshop Session 1

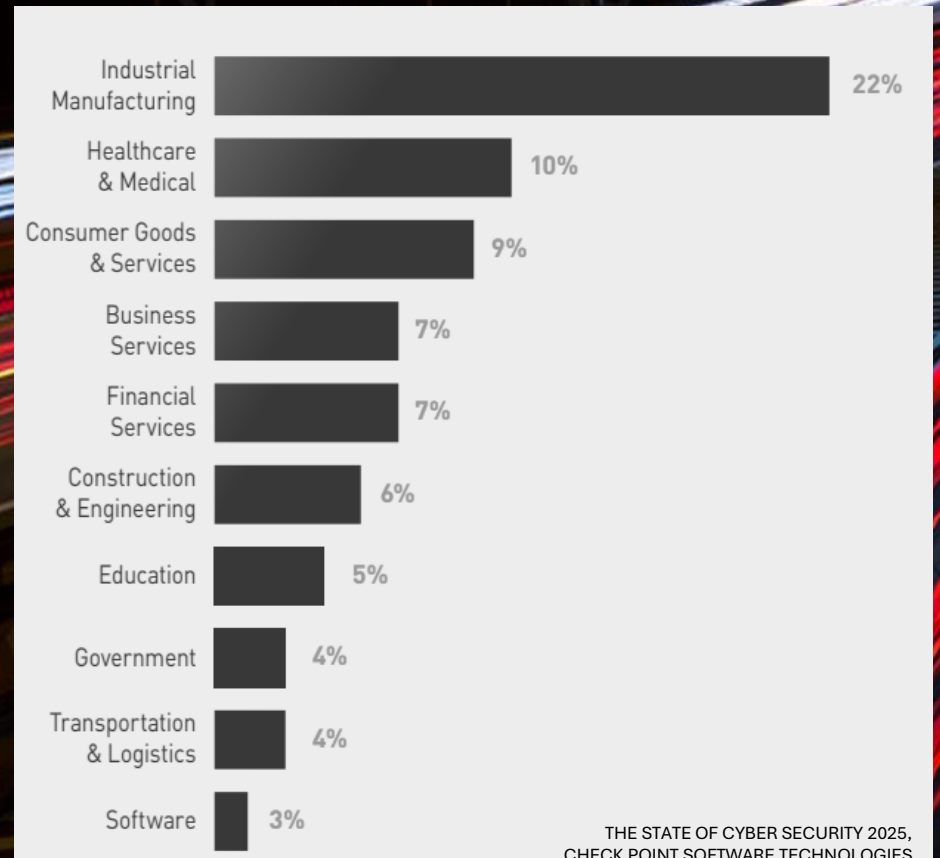
11:10 ; Raum C, Caroline Neufert BearingPoint
Sichere Produktion im vernetzten Zeitalter:
Schwachstellen erkennen, Angriffsflächen reduzieren

KI verändert das Spielfeld der Cyberangriffe

Es beschleunigt, skaliert und personalisiert Angriffe

- **KI als Werkzeug für Social Engineering**
  noch schneller und leichter zu realistische Phishing-Mails, CEO Fraud, Fake-Invoices, Deep Fake, fingierte Service Einsätze, schadhafte Software Updates und dergleichen
- **KI findet Schwachstellen in Open-Source-Komponenten**
  – diese kann sie automatisiert finden und ausnutzen
- **KI steigert Effizienz von Angriffen**
  automatisierte Exploit-Codes generieren, gezielte Verschlüsselung von Steuerungen
- **Ransomware in der OT**
  Stillstand von Fertigungslinien nach Ransomware Attacke, enorme Kosten von bis zu € 2,5 Mio bei einem Betrieb mit ca. € 50 Mio Umsatz

Welche Sektoren im Fokus von Ransomware Attacken stehen:

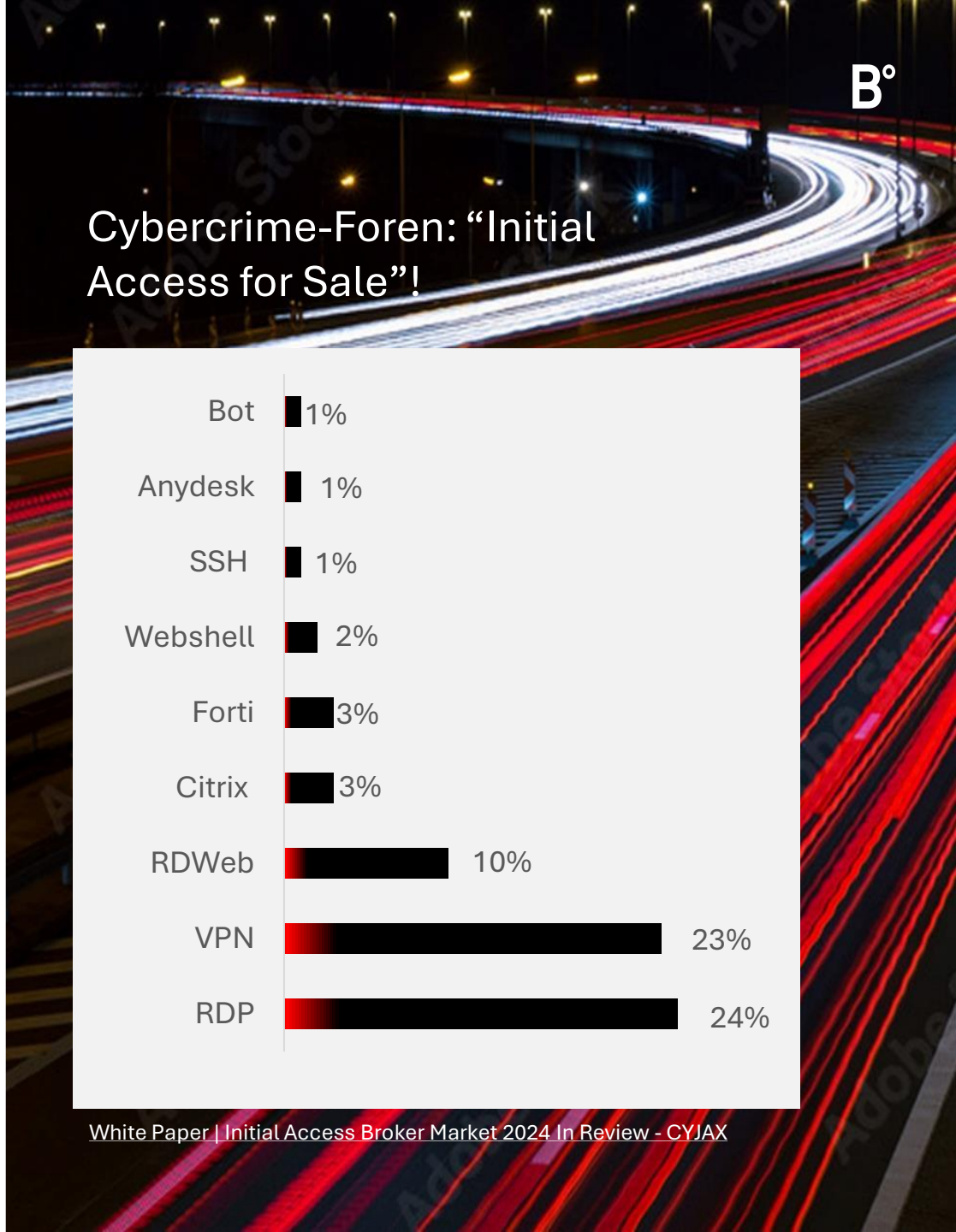


THE STATE OF CYBER SECURITY 2025,
CHECK POINT SOFTWARE TECHNOLOGIES

Regulatorischer Druck

NIS2 – Pflicht oder Chance?

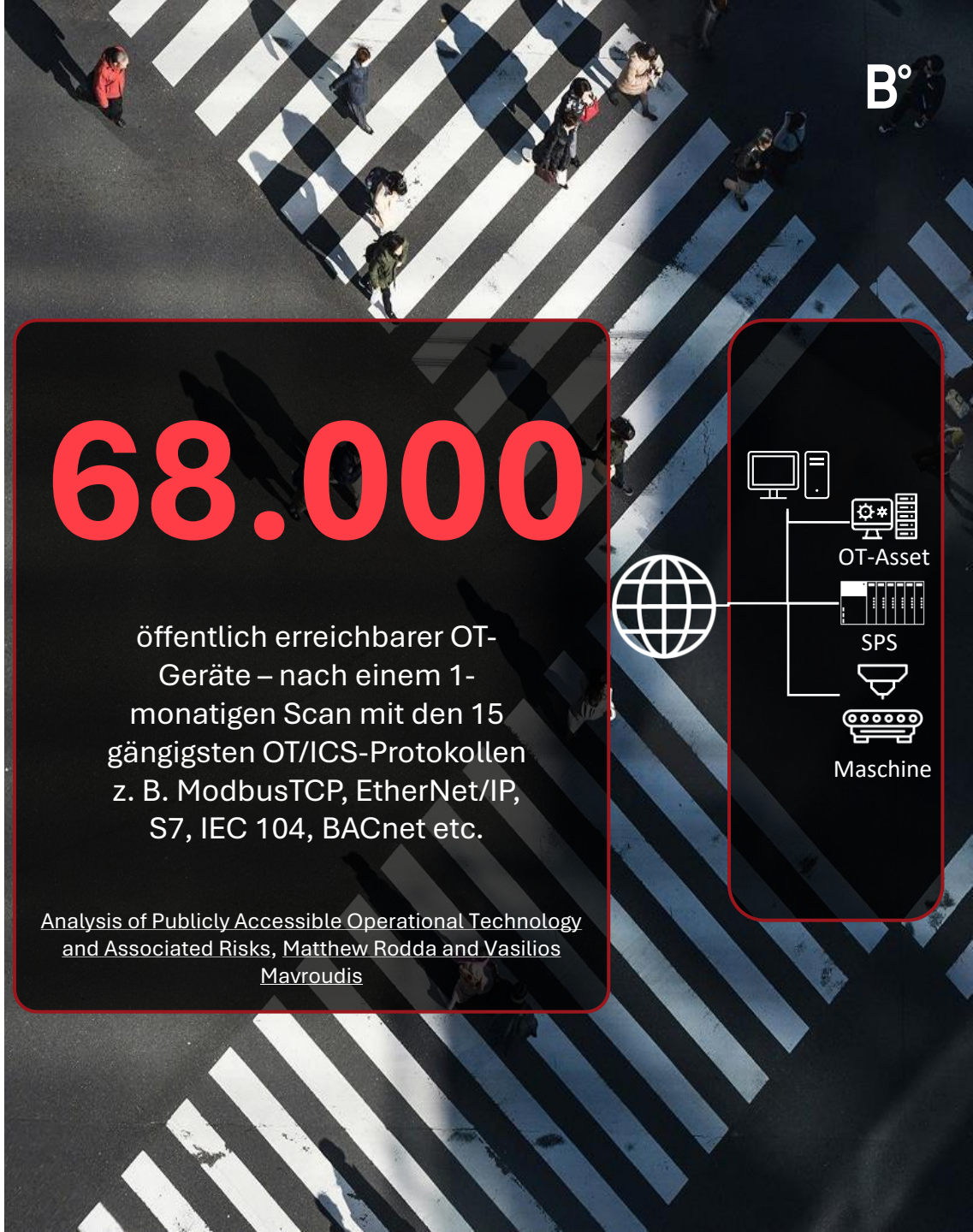
- **Absicherung der Lieferkette**
  auch Zulieferer und Partner müssen nachweislich Security-Standards erfüllen
- **Konzepte zur Nutzererkennung & Authentifizierung**
  keine „Shared-Service-Accounts“ mehr, sondern klare Identitäten, Multi-Faktor-Authentifizierung
- **Verpflichtendes Risikomanagement & Reporting**
  dokumentierte Prozesse (JIT-Access, Video Recording, Log Recording) und schnelle Incident-Meldung



Regulatorischer Druck

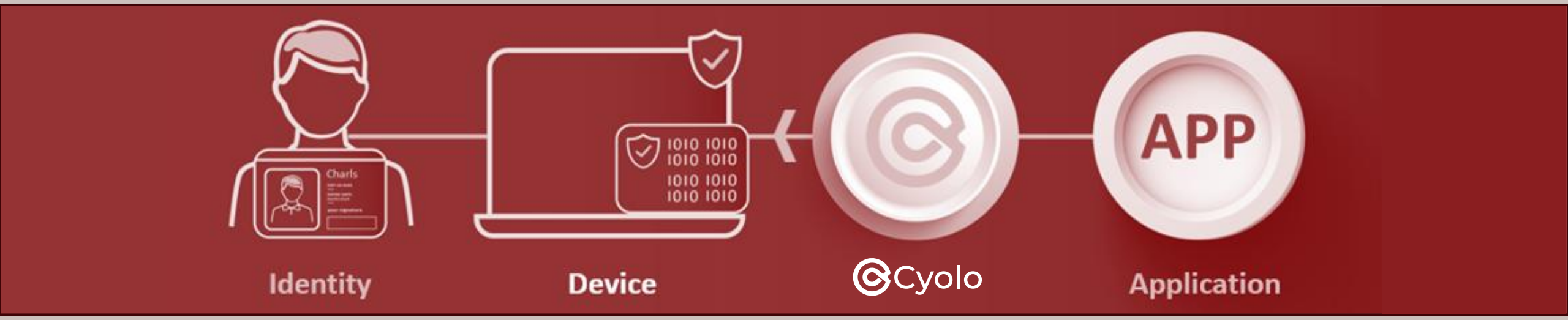
Cyber Resilience Act – Bürde oder Business Enabler?

- **Anforderungen an Produkte SBOM**
  Software Bill of Materials – volle Transparenz über verwendete Komponenten (open source, proprietary, libraries, dependencies)
- **BOM für Hardware/Services**
  Offenlegung von Abhängigkeiten einzelner Assets im „Produkt“
- **Sichere Updates & Services**
  Hersteller müssen Sicherheit über den gesamten Lebenszyklus gewährleisten
- **Security by Design**
  Geräte & Systeme müssen mit eingebauter Sicherheit entwickelt werden
- **Die Herausforderung:**
  Aufwand & Komplexität für Unternehmen auf ein praxistaugliches Minimum halten



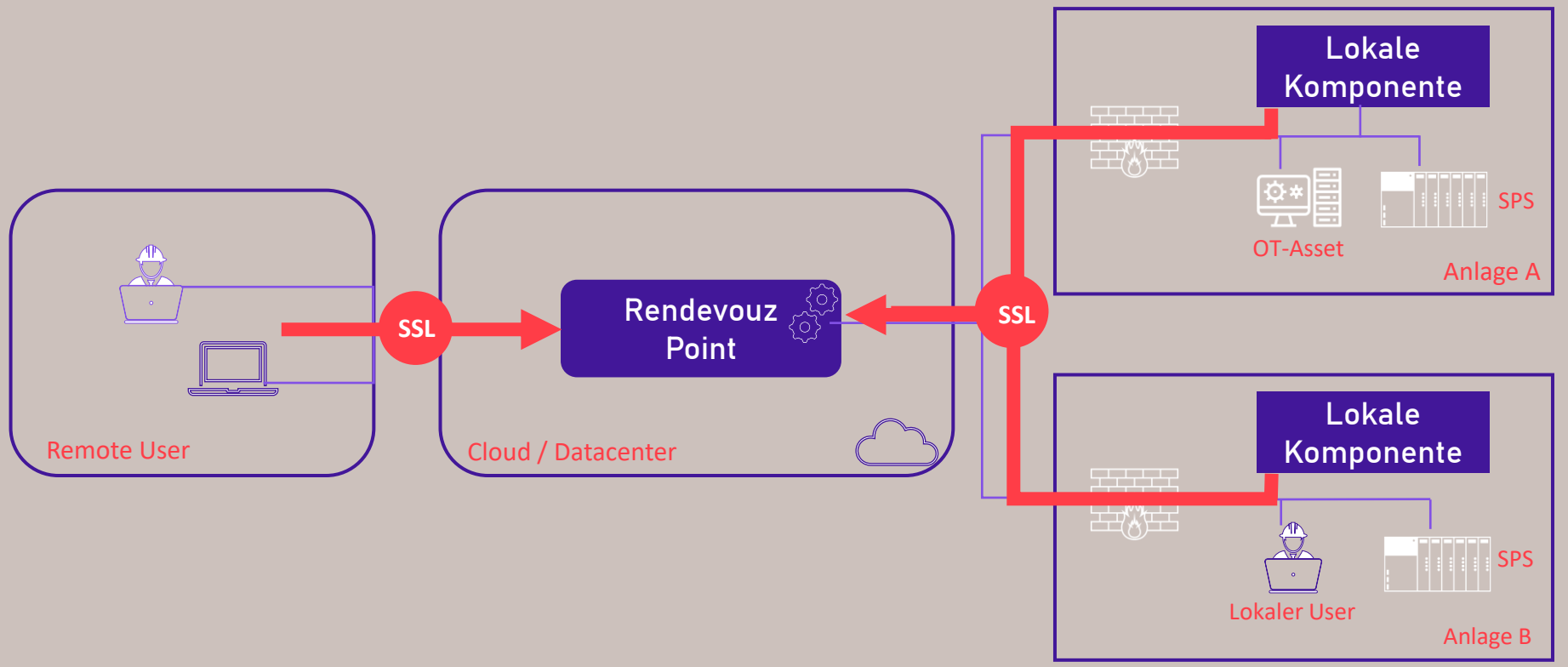
Dies stellt keine rechtlich verbindliche Aussage dar sondern eine persönliche Einschätzung

Architektur moderner Fernzugriffslösungen



Architektur moderner Fernzugriffslösungen

Durch eine „two-tier architecture“, also eine mehrschichtige Architektur, wird die Exponierung nach außen vermieden und die Angriffsfläche reduziert.

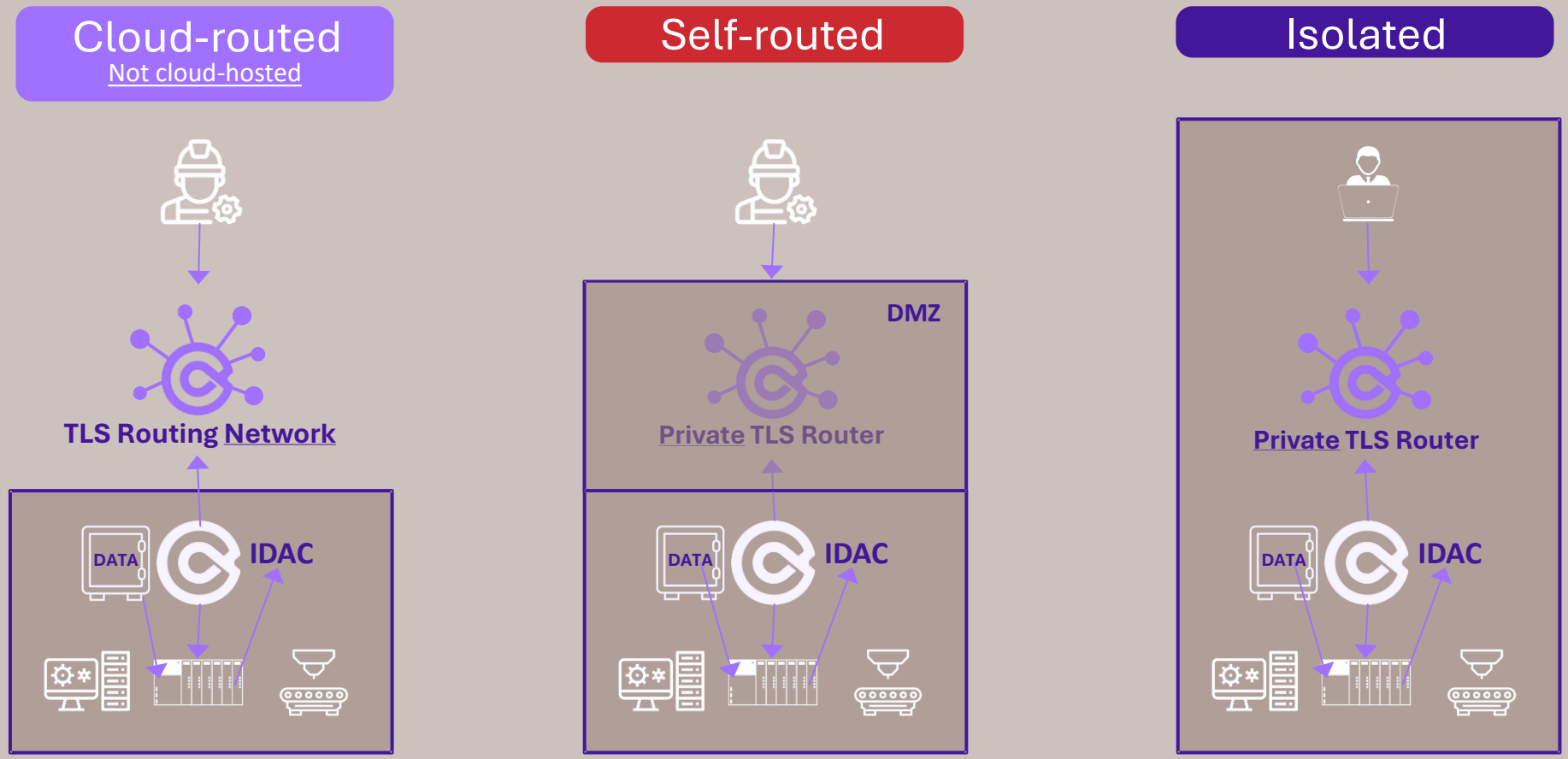


Was gilt es zu bedenken?

- Daten-Speicherort
- Cloud-abhängigkeit
- Multi-Mandanten
- Protokolle
- Hardware
- Integrationen
- Connectivity
- Approval Art
- Security (SIEM, Log, Recording)
- „Just in time“ Zugang
- Notfall – Link
- Kaskadierende Freigabe
- …

Deployment Optionen

Secure Remote Access



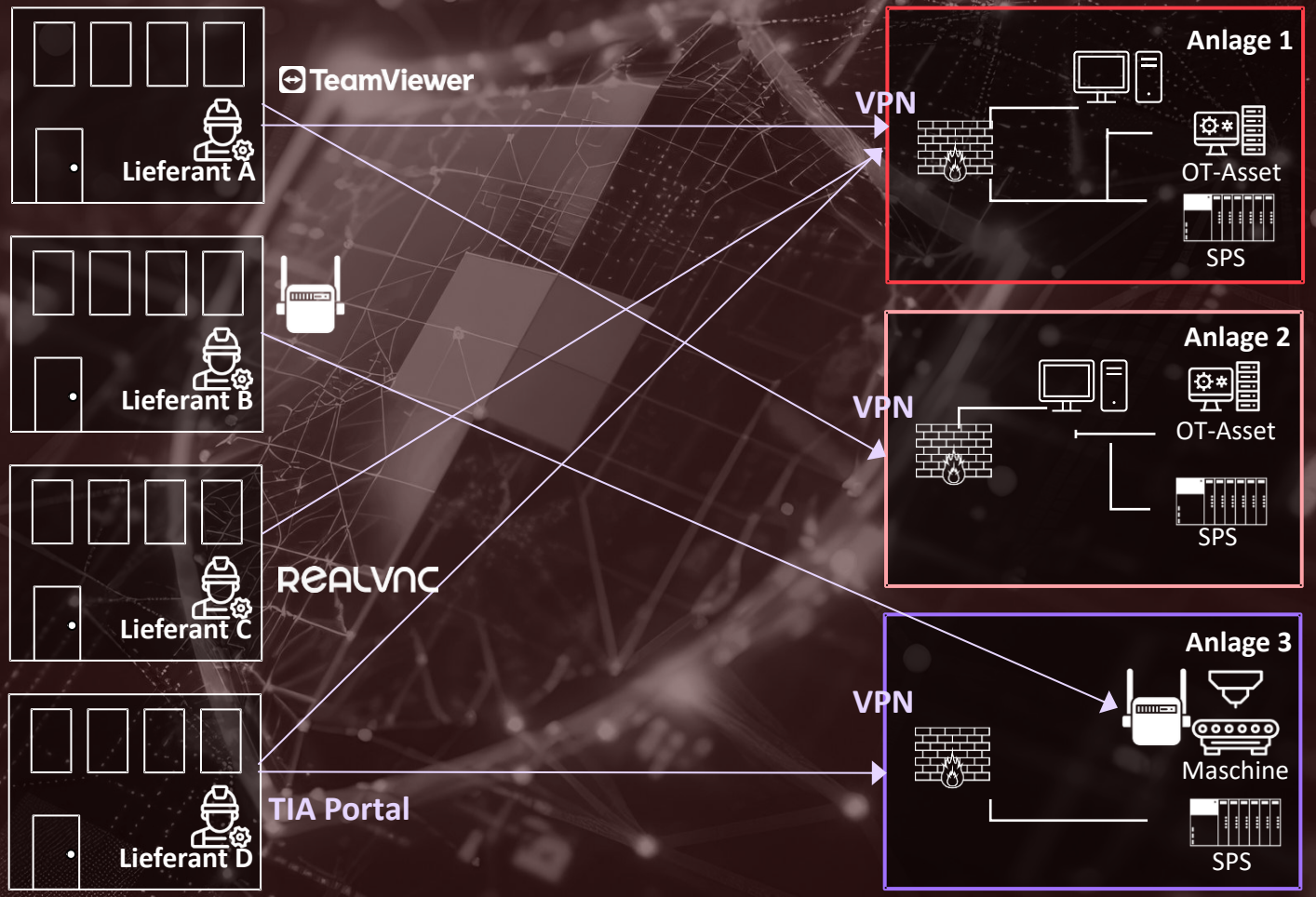
Anwendungsfall 1

Ein Betreiber, viele Lieferanten

Anwendungsfall – Ein Betreiber, viele Lieferanten

Herausforderung

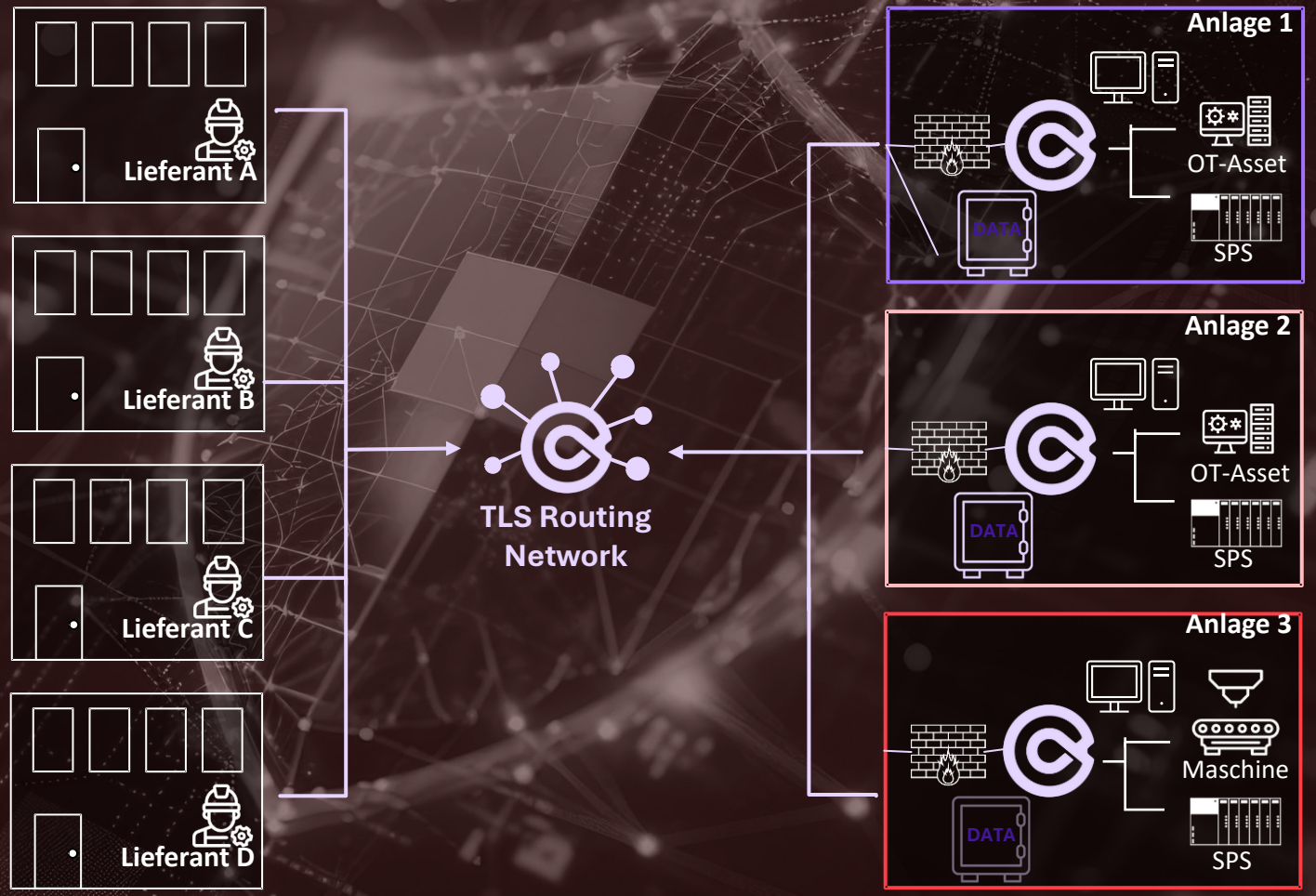
- Betreiber von mehreren Anlagen (Europa)
- Wildwuchs an Fernzugriffsmethoden
- Keine einheitliche Steuerung und Kontrolle
- Öffentliche Angriffsfläche
- Hoher manueller Aufwand für Freigabe
- Multi-Faktor Sonderfall



Anwendungsfall – Ein Betreiber, viele Lieferanten

Lösung

- Zentralisierte RPAM Lösung
- Unterstützung aller benötigten Methoden/Protokolle (client-less)
- Multi-Faktor über mehrere Parteien
- Zentrale Benutzerverwaltung via ADs
- Bestehende VMs oder dedizierte Hardware



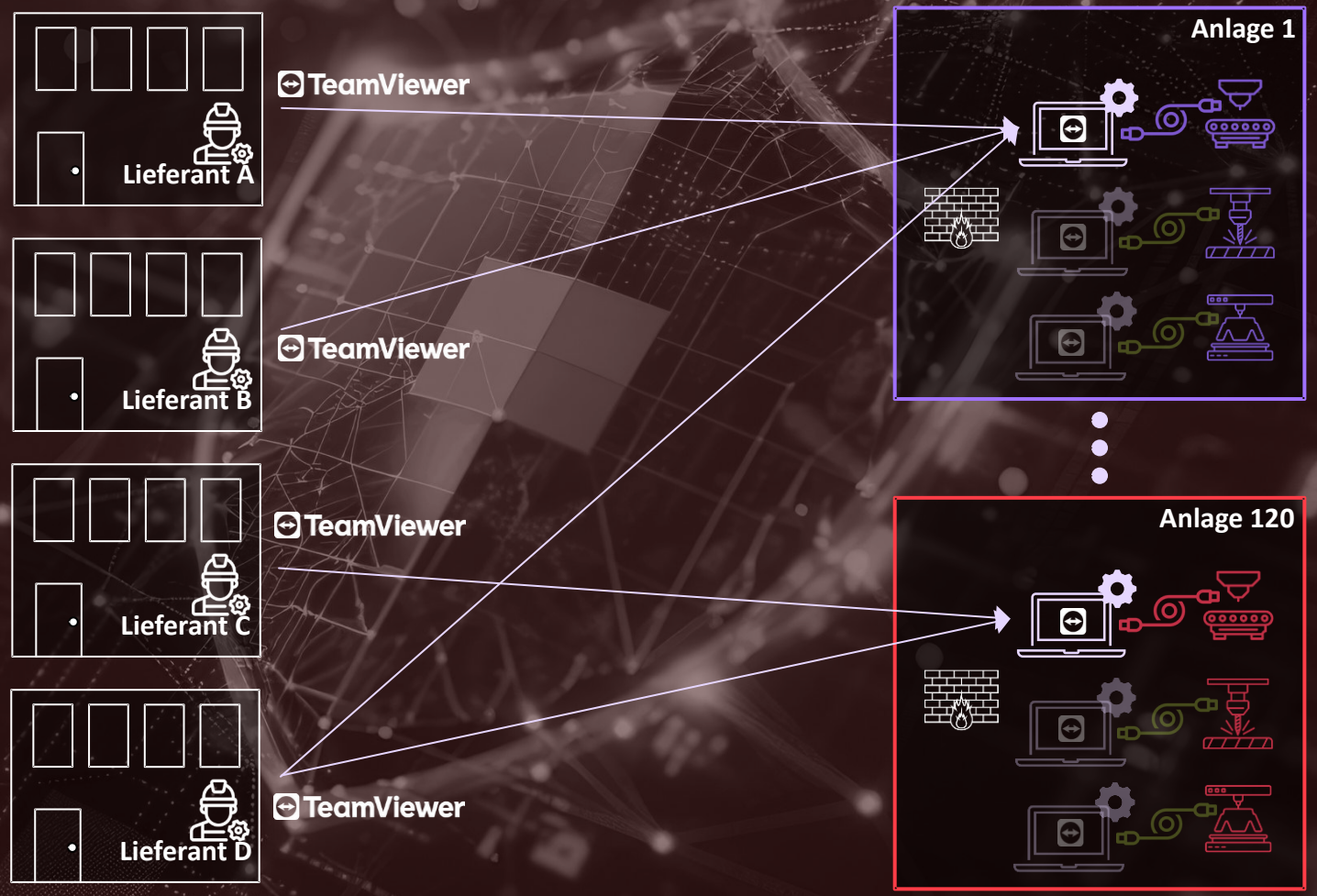
Anwendungsfall 2

Maschineninseln

Anwendungsfall – Maschineninseln

Herausforderung

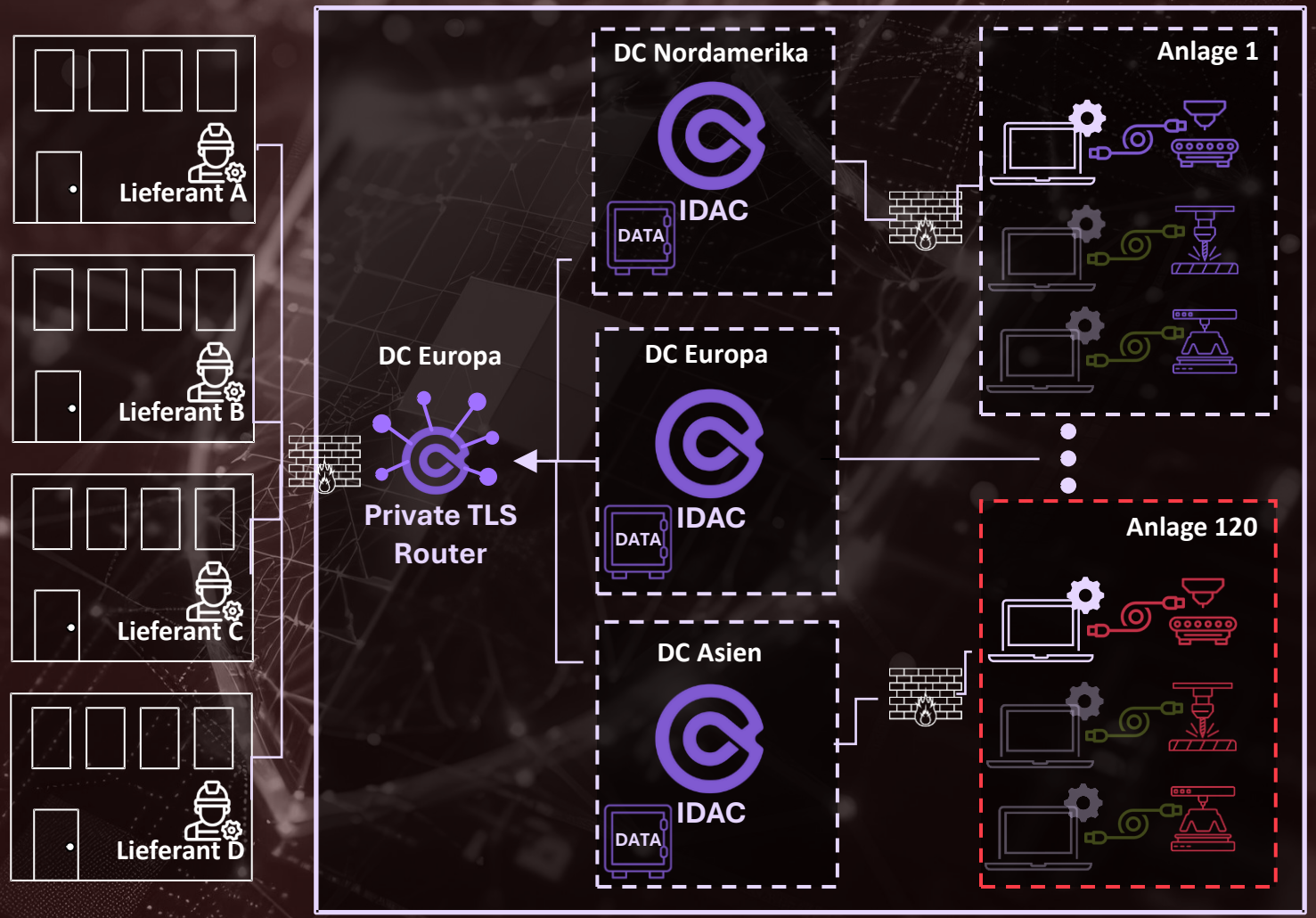
- Betreiber von über hundert Anlagen weltweit
- Legacy Maschineninseln ohne Konnektivität
- Teamviewer Notlösung
- Abhängigkeit zu Hersteller (Daten, ...)



Anwendungsfall – Maschineninseln

Lösung

- Ein gehostetes Private Gateway (Routing) im Kunden-DC
- Dezentral gehostete IDACs in drei Regionen
- Zwei mobile Laptops pro Werk als Connection Targets
- Zentrale Benutzerverwaltung via AD
- Device Posture Check



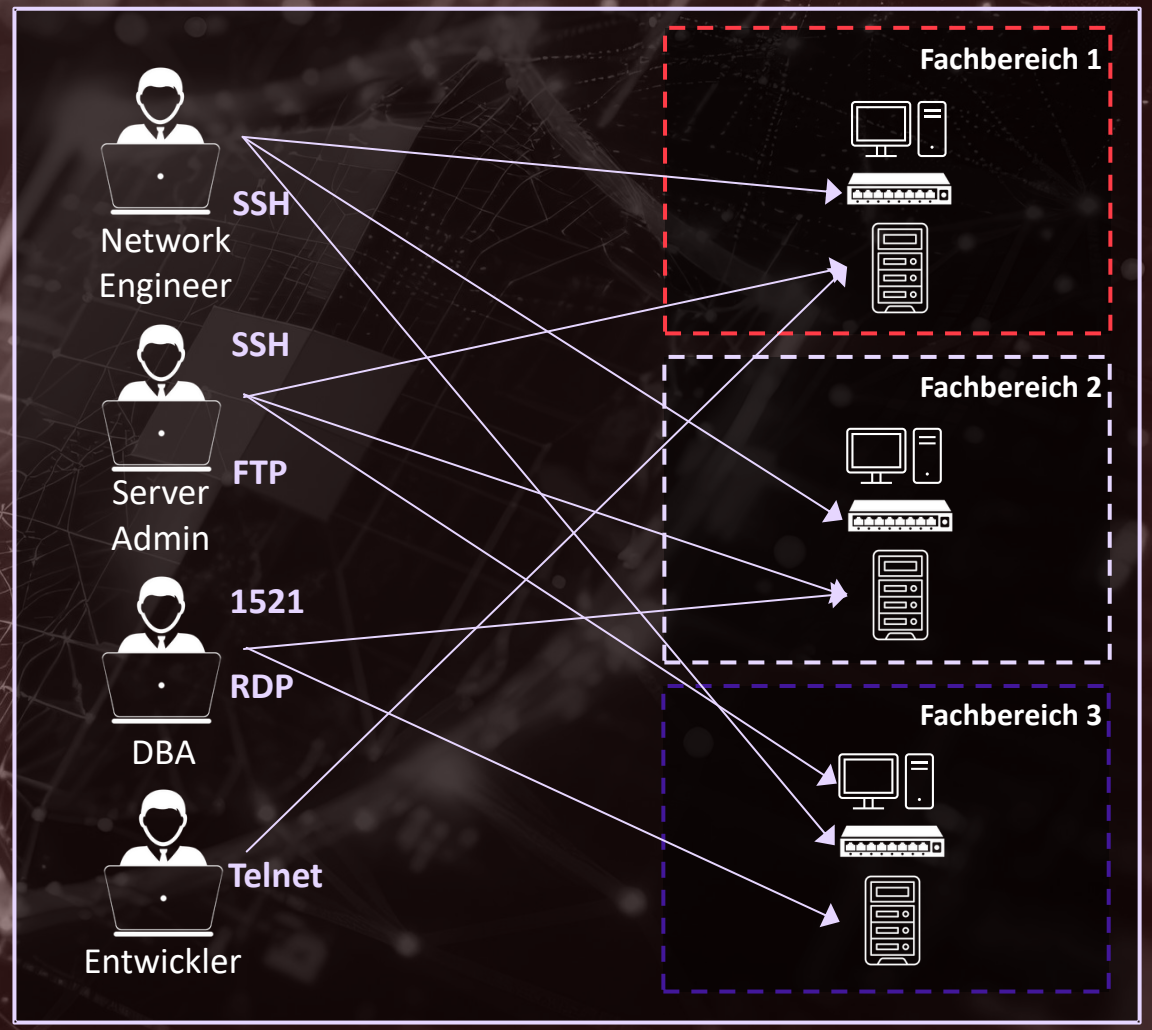
Anwendungsfall 3

Air-gapped
Hochkritische
Umgebungen

Anwendungsfall – Air-gapped

Herausforderung

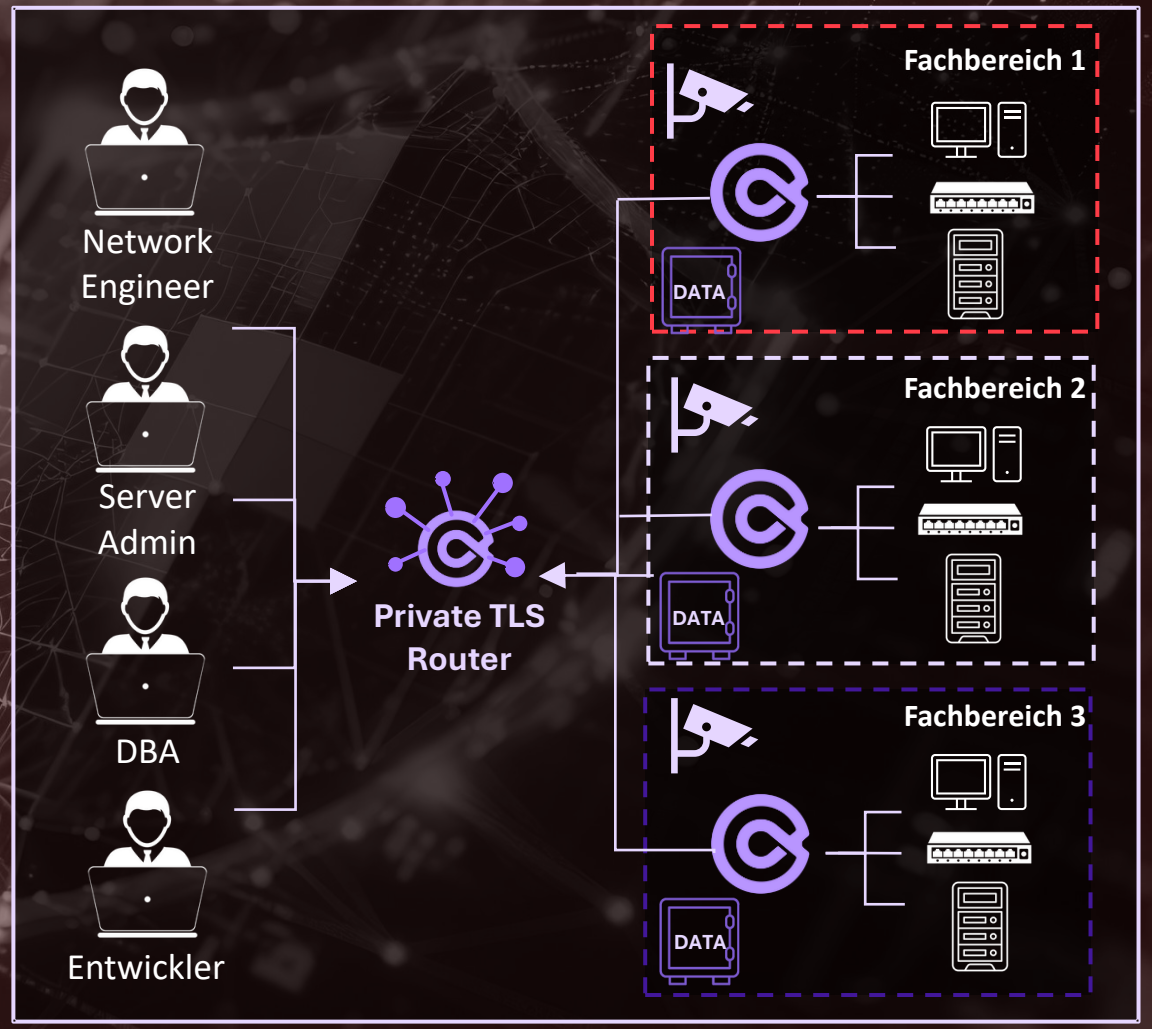
- Betreiber hochsicherer Umgebung
- Strikte no-Cloud policy – Umgebung fully air-gapped
- Fernzugriffe für eigene Mitarbeiter im Haus
- Drei strikt getrennte Bereiche mit eigener Verwaltung
- Auditing, Logging und Videoaufzeichnung als zentrale Anforderung



Anwendungsfall – Air-gapped

Lösung

- Ein gehostetes Private Gateway (Routing)
- im Kunden-DC
- Dezentral gehostete IDACs in eigenen Netzen
- Drei getrennte Tenants mit eigener Verwaltung
- Vollständiges Auditlog und Recordings
- Zentrale Benutzerverwaltung via AD
- Zentrale Rechteverwaltung



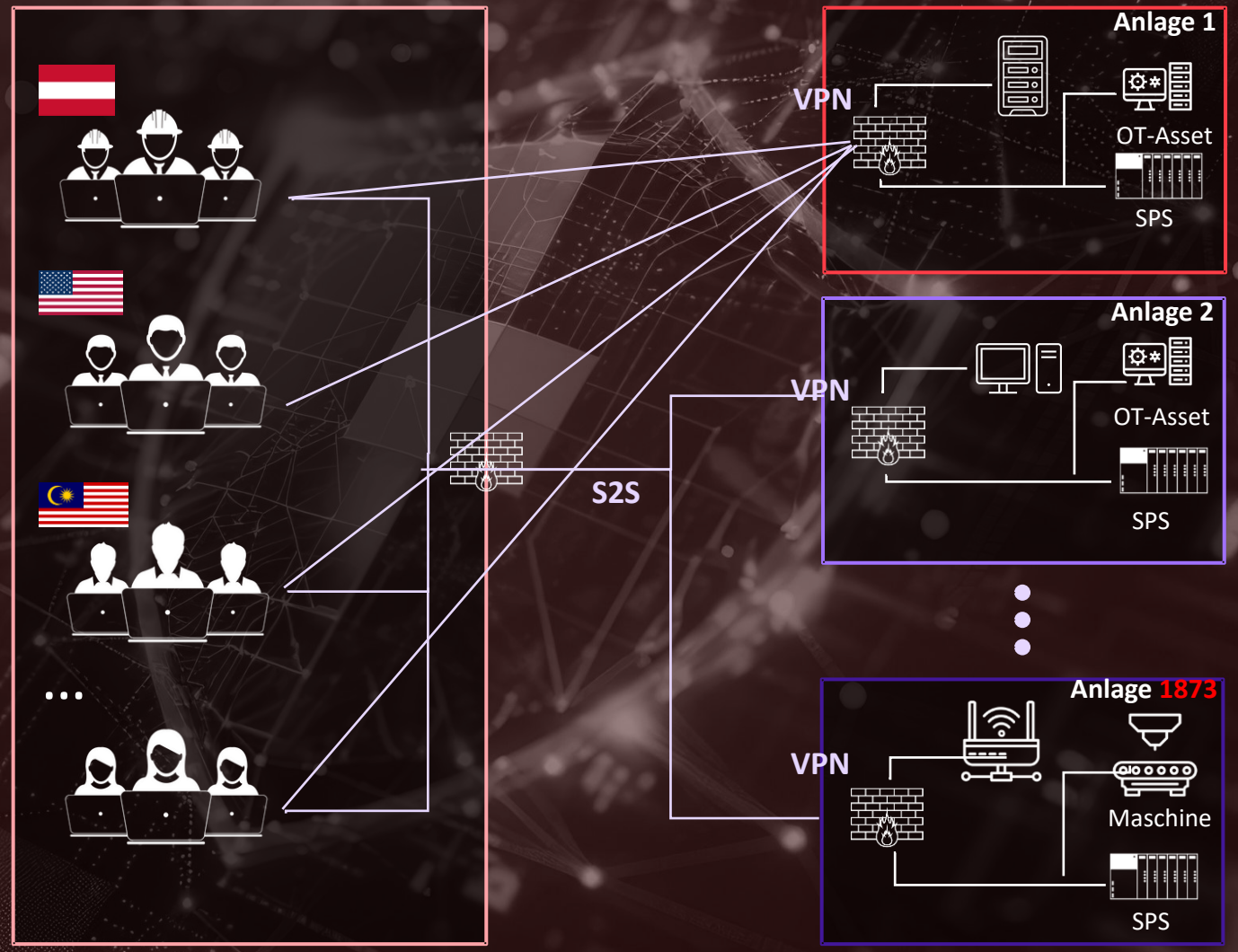
Anwendungsfall 4

Sicherer Fernzugriff als Teil des Service Portfolios

Anwendungsfall – RPAM für Anlagen- und Maschinenbauer

Herausforderung

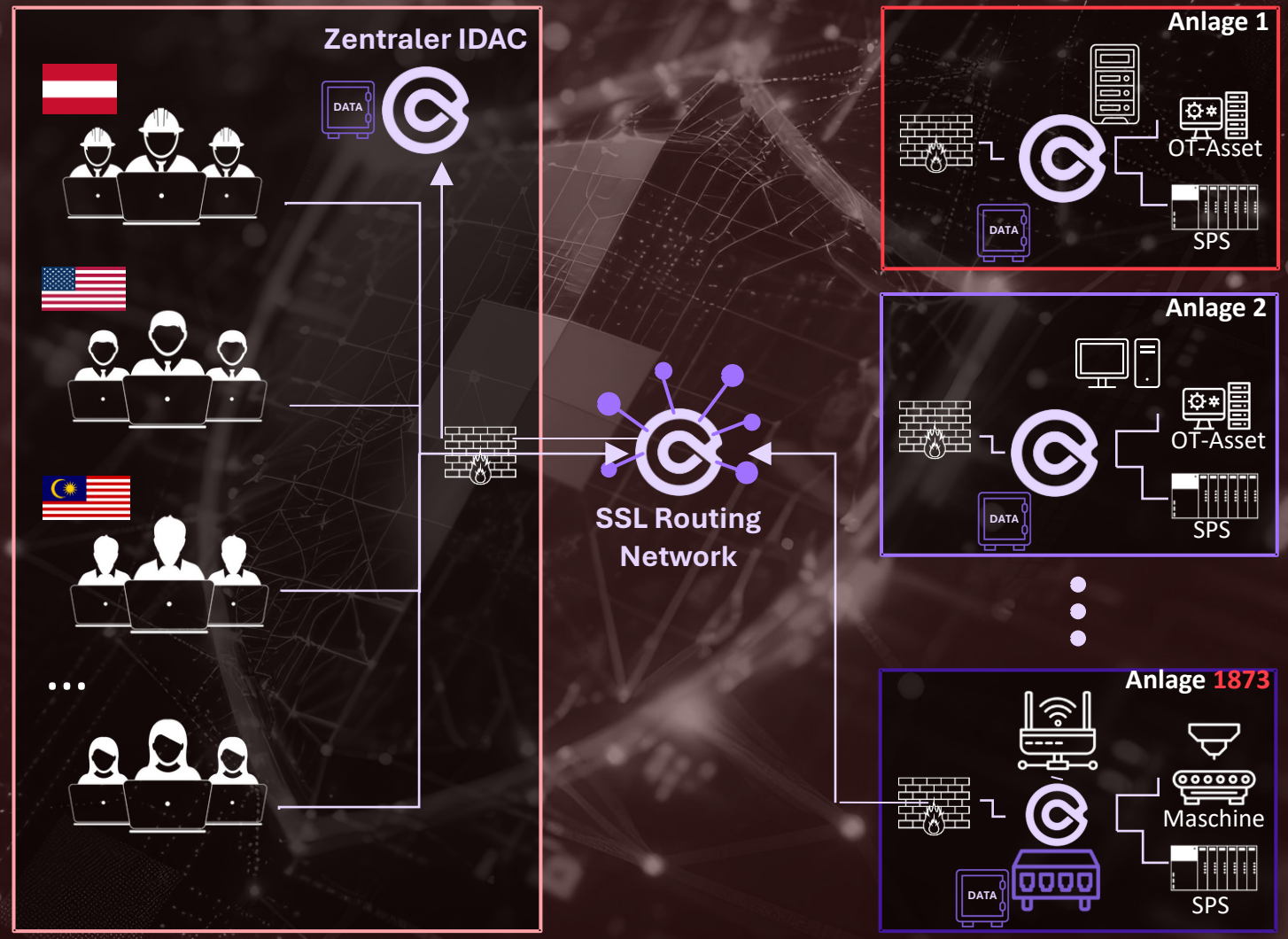
- Tausende Kundeninstallationen weltweit
- Site 2 Site VPNs / Vielzahl an VPN Clients
- Hunderte Engineers global verteilt
- Vielseitige Protokolle
- Nativer Protokollzugriff
- Supply Chain Security Bedenken
- Öffentliche Angriffsfläche
- Regulatorik und Kundenanforderungen



Anwendungsfall – RPAM für Anlagen- und Maschinenbauer

Lösung

- Zentrale RPAM Lösung
- Virtualisiert oder Industrial PC
- Multiple Mandanten
- Datenhoheit bei Kunden
- Vereinheitlichter Zugriff
- Granulare Kontrolle
- Approval Workflow
- Passwort Vaulting



BearingPoint

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf Ihre Kontaktaufnahme:

Alexander Schwemberger
alexander.schwemberger@bearingpoint.com
https://www.linkedin.com/in/schwembergera/

BearingPoint

Guido Erroi
guido@cyolo.io
https://www.linkedin.com/in/guidoerroi/

Cyolo