



**Souveränes Endgeräte Management**

**Kontrolle im Ernstfall, Sicherheit im Einsatz**

# Einsatzfelder digitaler Endgeräte

- Tablets & Smartphones
- Digitale Handfunkgeräte
- Bodycams
- Mobile Datenterminals/  
Laptops
- Barcode Scanner
- Ausweis-/  
Reisepasslesegeräte
- ANPR Kameras
- Kameradrohnen
- RFID-/NFC-Lesegeräte



# BOS-Breitband und Endgeräte

## Die unsichtbare Lücke

01

BOS-Strategien fokussieren auf Netze, Spektrum und Funkstandards.

02

Die operative Steuerungsebene liegt jedoch im Endpoint-Management.

03

Im UEM wird entschieden, wer mit welchem Gerät auf welche Daten zugreifen darf.

04

Fällt diese Ebene aus, sind Leitstellen, Streifen und Spezialkräfte direkt betroffen.

Fazit

Endgeräte-Management ist nicht nur IT-Support.  
Es ist Teil der BOS-Sicherheitsarchitektur.

# Device Management heute

Kernanforderungen an ein leistungsstarkes Unified Endpoint Management

## Automatisierung komplexer Workflows

- Automatisierte Gerätebereitstellung
- Schnelle, konsistente Inbetriebnahme
- Compliance-Prüfungen & Reaktionen

## Desired State & Declarative Management

- Schnelle & konsistente Richtlinienumsetzung
- Sicherheits- & Compliance-Durchsetzung

## Hohe Systemabdeckung & Verwaltung gängiger Endgeräteklassen

- Windows & Windows Server
- Apple inkl. DDM
- Android inkl. Mgmt API
- Linux
- Rugged Devices: Zebra OTA

## Modern Windows Management

- GPO based Baseline
- Application repositories built-in
- Update Management
- Device Provisioning capabilities
- Darkside Patch Management

# Risiko: Fremdzugriff durch Abhängigkeiten

heise online  
Keine Garantien: Microsoft muss EU-Daten an  
USA übermitteln

taz  
US-Sanktionen gegen Richter in EU  
Leben ohne Kreditkarte und  
Amazon

Augsburger Allgemeine  
Von Trumps Sanktionen getroffen:  
Französischer Richter kann nicht mal  
mehr bei Amazon bestellen

DIE ZEIT

**USA verhängen Sanktionen gegen  
IStGH-Chefankläger Khan**

DIE ZEIT

**Microsoft öffnet dem FBI die Tür**

**CLOUD Act** = Clarifying Lawful Overseas Use of Data Act

# Kriterien digitaler Kontrolle und Unabhängigkeit



## Datenschutz

---

- Schutz sensibler Daten
- Zugriffskontrollen
- Verschlüsselung
- Compliance

**Ziel: Schutz vor  
Datenabwanderung**



## Datenresidenz

---

- Kontrolle über Datenflüsse
- Verarbeitung im eigenen Rechtsraum
- Schutz vor extraterritorialen Zugriffen

**Ziel: Kontrolle über Daten  
und Rechtsraum**



## Betriebssicherheit

---

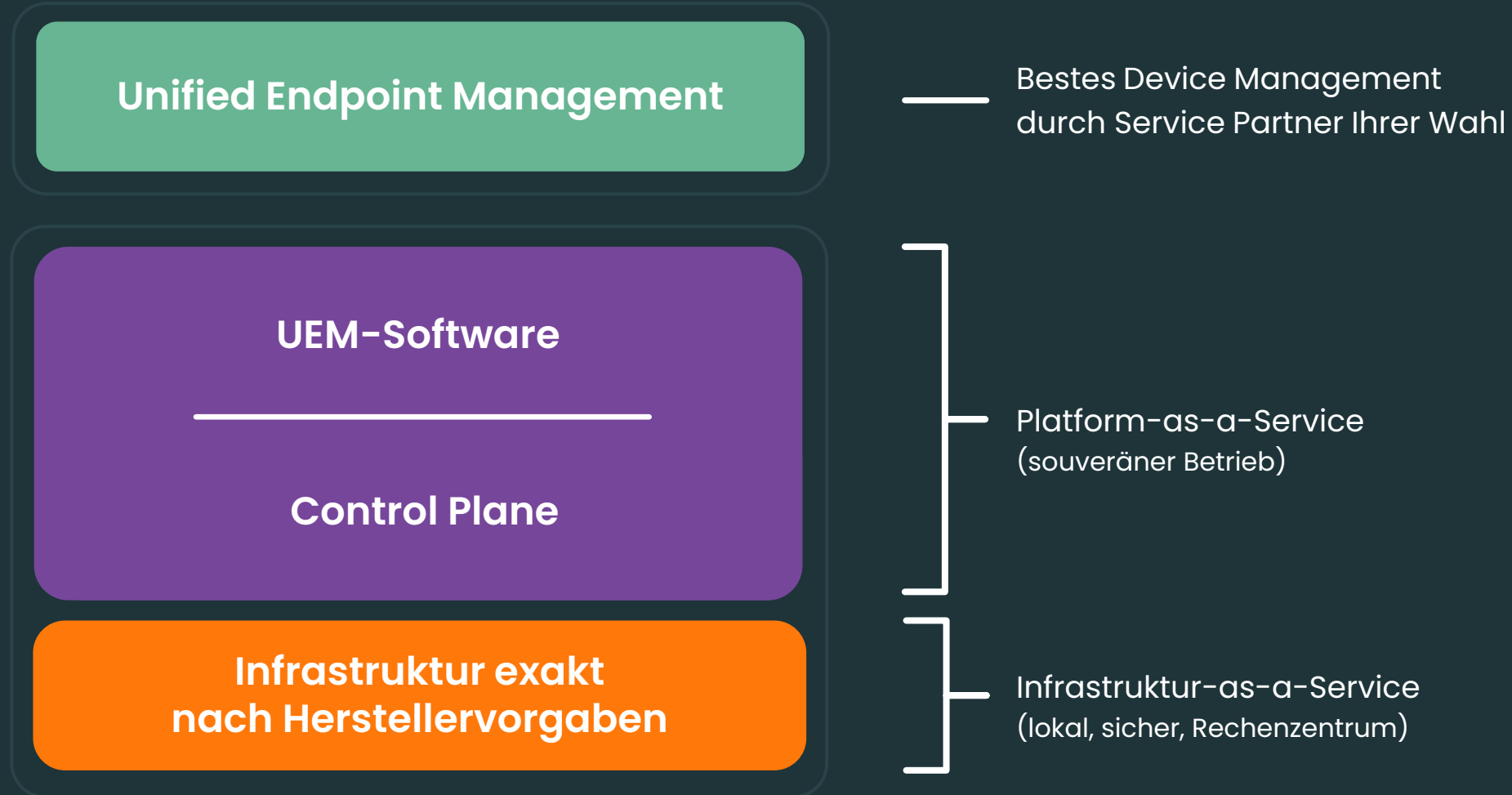
- Plattform bleibt ohne Hersteller handlungsfähig
- Exit-Strategien existieren
- Betrieb bleibt im eigenen Einflussraum möglich

**Ziel: Sicherstellung der  
operativen Steuerungsfähigkeit**

# Souveräne UEM-Architektur für BOS



# Architektur im Überblick: Gewaltenteilung



# Integrierte Sicherheit **im Code verankert**

## **Tenant Kontext:**

Logische Trennung und sichere Isolation von Mandantendaten

## **Service-to-Service-Authentifizierung:**

Sichere und verschlüsselte Kommunikation zwischen Diensten

## **Row-Level Security:**

Granulare Zugriffsbeschränkungen auf Datenbankebene

## **Bring Your Own Key (BYOK):**

Kunden behalten volle Kontrolle über die Verschlüsselung



# Prüffrage 1 – Datensicherheit

## Haben wir die vollständige Kontrolle über sicherheitskritische UEM-Daten und deren Schutzmechanismen?

### Zu klären:

- Wer hat Zugriff auf sicherheitsrelevante Betriebsdaten?
- Wer kontrolliert kryptografische Schlüssel?

### Steuerungsziel „Information Security“:

Sicherstellen, dass sicherheitskritische Betriebsdaten (Gerätezustände, Schwachstellen, Patch-Status) nicht außerhalb der eigenen Kontrolle zugänglich sind.

## Prüffrage 2 – Data Residency und extraterritoriale Zugriffe

**Sind unsere UEM-Betriebsdaten vollständig innerhalb unseres Rechts- und Hoheitsraums verarbeitet und geschützt?**

### **Zu klären:**

- Wo werden UEM-Daten gespeichert und verarbeitet?
- Welche Datenflüsse existieren zu Hersteller-Clouds?
- Unter welchem Rechtsraum steht der Betreiber?

### **Steuerungsziel „Datenstandort“:**

Verhindern, dass sicherheitsrelevante Infrastruktur-Daten extraterritorialen Zugriffsgesetzen unterliegen.

## Prüffrage 3 – Betriebssicherheit und Handlungsfähigkeit

# Bleiben unsere Geräte auch bei Ausfall oder Dienstsperre handlungsfähig?

### Zu klären:

- Funktioniert das UEM ohne Hersteller-Cloud?
- Wie schnell kann ein alternatives Betriebsmodell aktiviert werden?

### Steuerungsziel „Business Continuity & Risk Mitigation“:

Sicherstellen, dass Device-Management und Sicherheitssteuerung auch im Krisenfall funktionsfähig bleiben

# Architektur-Checkliste



## Datenschutz

### Technische Souveränität:

- Administrative Kontrolle
- Control-Plane-Souveränität
- Kryptografische Kontrolle
- Richtlinien- und Compliance-Kontrolle



## Datenresidenz

### Datensoeveränität :

- Datenklassifikation
- Datenverarbeitung
- Rechtsraum und Betreiberstruktur
- Mandantentrennung



## Operative Sicherheit

### Betriebssouveränität:

- Betrieb ohne Hersteller
- Exit-Strategien
- Betriebsmodell
- Notfall- und Wiederanlaufkonzepte



**Heiko Friedrich**

---

[oss@de.thegema.com](mailto:oss@de.thegema.com)

# GEMA International

- Souveränes Endgeräte-Management in sicherheitskritischen Umgebungen
- Globale Managed-Mobility-Services: sicher, skalierbar und rechtskonform
- Langjährige Erfahrung in internationalen Großprojekten und Branchenvielfalt
- Weltweites End-User-Computing und Device-Management aus einer Hand
- Einheitliche Produktivität und Compliance für Unternehmen in allen Regionen der Erde



omnissa™



omnissa™