INSEYA

simply secure

Umfassende Enterprise Mobility

Security + Architektur + Gerätemanagement + Geräte + Zubehör + Abos

Reto Heutschi
CEO & Co-Founder, Inseya

Tobias Ritter
Head of Engineering & Operations, Inseya

Pascal Briano
Head of Sales B2B, **mobilezone**

Inseya - Cybersecurity für die Cloud Ära

Inseya	Seit 2007, Inhabergeführt
Sitz	Bern, Schweiz
Marktfokus	Geschäftskunden mit Sitz in der Schweiz (HQ)
Tätigkeitsfeld	• Security Consulting • ***Enterprise Mobility*** • Secure Networking (SD-WAN / SASE / SSE) • Endpoint Security (EPP, AV, EDR, XDR)
DNA	• Kundenfokussiert und herstellerunabhänging • Beratung, Planung, Umsetzung • Betrieb der Security Services

Wie es alles entstand …

1978
Natel A

1983
Natel B

1993
Natel D
(GSM/digital)

Enterprise Mobility Gen 1

1999
BES

2002
GPRS

2003
EAS

2007
iPhone

mobileiron

INSEYA
simply secure

2009
Android

Knox

2013
Samsung
KNOX

2017
Stopp Win
Phone

Gen 2

ab 2021
Penetration Smartphones > 80%

1975
MSFT

1984
Macintosh

Active Directory

aws

ZERO TRUST

Office 365

Microsoft Intune

kubernetes

1999
MSFT
AD (Preview)

2006
Cloud
Computing

2008
MSFT
Azure

2010
Kindervag
ZT

2011
MS Intune

2012
AAD

2014
K8s

2015
Graph
API

2023
AAD -> Entra ID

Treiber der Enterprise Mobility Gen 2

Gen 1

M365

KIS

- Kalender, Kontakte UND OneDrive, Teams, etc.
- Prozessautomatisierung
  -> i.d.R. schützenswerte Daten

Gen 2

- Informationssicherheit / DLP
- Verfügbarkeit der Systeme
- Persönliches Login
- Mehr Smartphones

dect

5G

- Applikationen und Identitäten migrieren in die Cloud
- Technologien werden abgelöst

- Neue Architekturen für Daten/Systeme und UEM
- Identitäten On Prem und Cloud
- Mehr Smartphones

- Attraktive Geräte
- Smartphone/Tablets als Hub/Workplace
- Abos für Mitarbeitende und Familiy + Friends

- Moderne Flotte plus Zubehör
- Verwaltung (vieler) Abos

Weitblick ist der Schlüssel

Treiber

- Mehr Smartphones
- Moderne Flotte plus Zubehör
- Verwaltung (vieler) Abos
- Knappe Ressourcen in der IT

- Informationssicherheit / DLP
- Verfügbarkeit der Systeme
- Persönliches Login
- Neue Architekturen für Daten/Systeme und UEM
- Identitäten On Prem und Cloud
- Produktbundles der Hersteller (MSFT E3,5 / VM / Samsung KNOX)

Fokusthemen

- Prozessautomatisierung

- Architektur und Security
- Welches UEM?

Relevante Systeme

- ERP, z.B. SAP
- IdP
- ITSM
- Shop, Geräte- und Aboverwaltung; Logistik inkl. Reparatur
- ABM, Android Zero-Touch
- *Geräte*
- UEM, KNOX
- Applikationen

Strategische Grundsatzfragen

Rolle des Smart Devices

- kritisch?
- ergänzend?
- Hub?

Verfügbarkeit

- Prozesse (Apps!)
- Organisation
- Systeme

Single OS/HW

- Nutzerakzeptanz
- Alle Funktionen möglich
- Einsparungen

Cloud

- Architektur
- IdP
- Werkzeuge (UEM)
- Erreichbarkeit der Daten

Rolle der IT

- was machen wir selbst
- wie stark begleiten wir die Nutzer

Fringe Benefits

- Attraktive Geräte
- Günstige Abos

Security

- auf dem Gerät
- auf den Apps und Applikationen

User Self Service

- Rolle der Nutzer
- Automatisierung

Geräte

- persönlich
- unpersönlich

BYOD

- ergänzend
- ersetzend

Erfolgsfaktoren für einen digitalen Wandel

Strategische Planung, zuverlässige Technologien sowie kompetente Partner sind unverzichtbare auf dem Weg einer effizienten, digitalen Transformation

Volle Integration in bestehendes ITSM-System

Mitarbeiterportal zur Bestellung von Mobile Devices

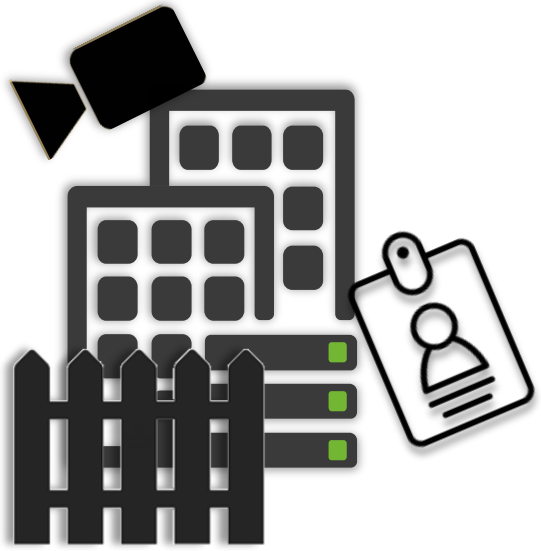
Sorglos den nächsten Schritt der Digitalisierung ohne administrativen Mehraufwand und volle Kontrolle über den Geräte-Lifecycle

Automatisierte Einbindung in Apple Business Manager oder Samsung Knox

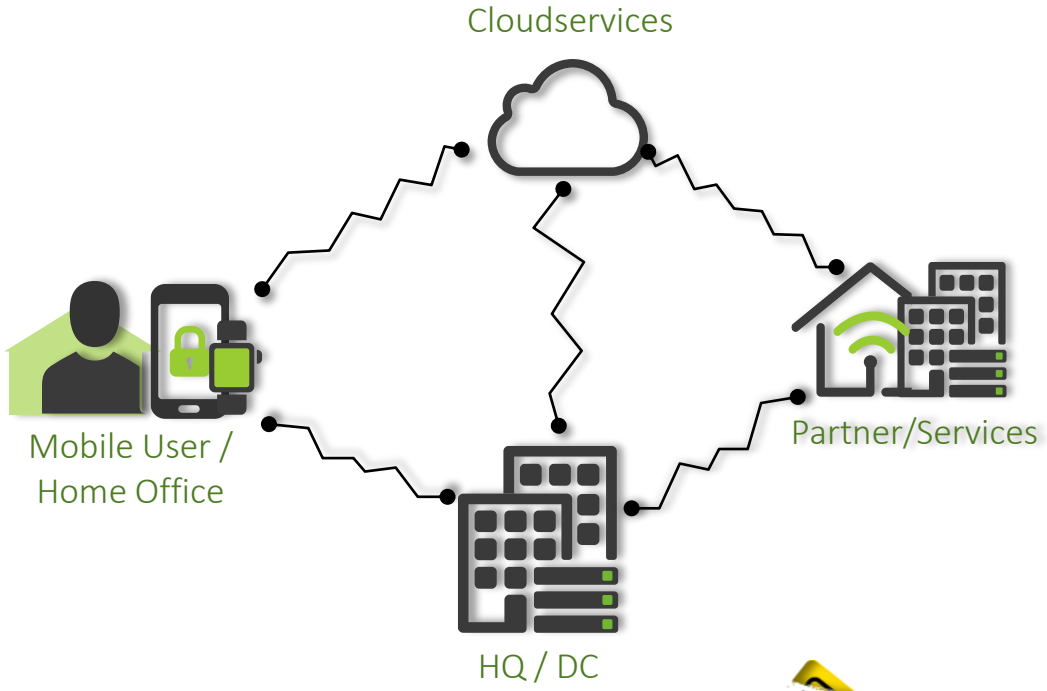
Während der Inbetriebnahme Sicherheitsmassnahmen durchsetzen z.B. mit dem Samsung Knox Service Plugin

Infrastruktur im Umbruch

Gen 1: Daten & UEM On-Premises



Gen 2: Hybride Daten und Services



Infrastruktur im Umbruch

Technische-Herausforderungen aus der Praxis

- Hybride Infrastrukturen – Zugriff mit Intune auf Daten und Services On-Premises & in der Cloud
- Sichere Bereitstellung & Zugriffe für Daten und Services – Mobile Daten und Services sicher Bereitstellen mit Zugriffskonzept
- Conditional Access im Zusammenspiel mit Microsoft Entra MFA
- Fragen die IT-Verantwortliche kritisch stellen sollten

Hybride Infrastrukturen

Zugriff mit Intune auf Daten und Services On-Premises & in der Cloud

Ausgangslage

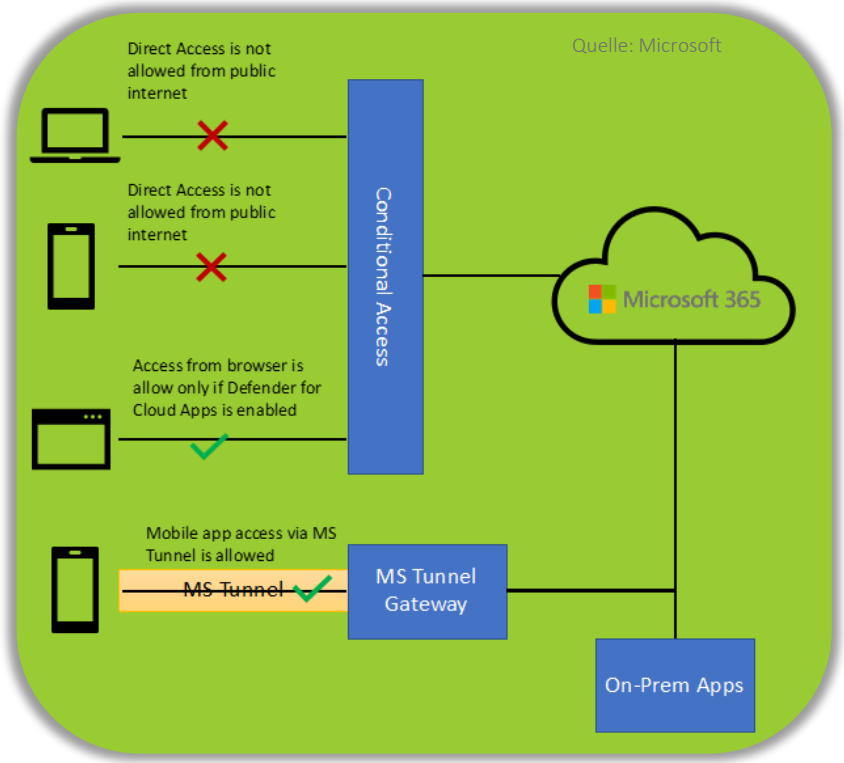
- Migration zu Microsoft Intune mit Microsoft Tunnel für Microsoft Intune in Betrieb
- Verwendung von Azure App-Proxy nicht möglich
- VPN-Zugriff auf Daten und Services On-Premises aber auch in der Cloud via Browser

Herausforderung

- On-Demand VPN lässt sich nicht homogen Konfigurieren
- Split Tunneling Rules werden bei Per-APP-VPN unter iOS deaktiviert

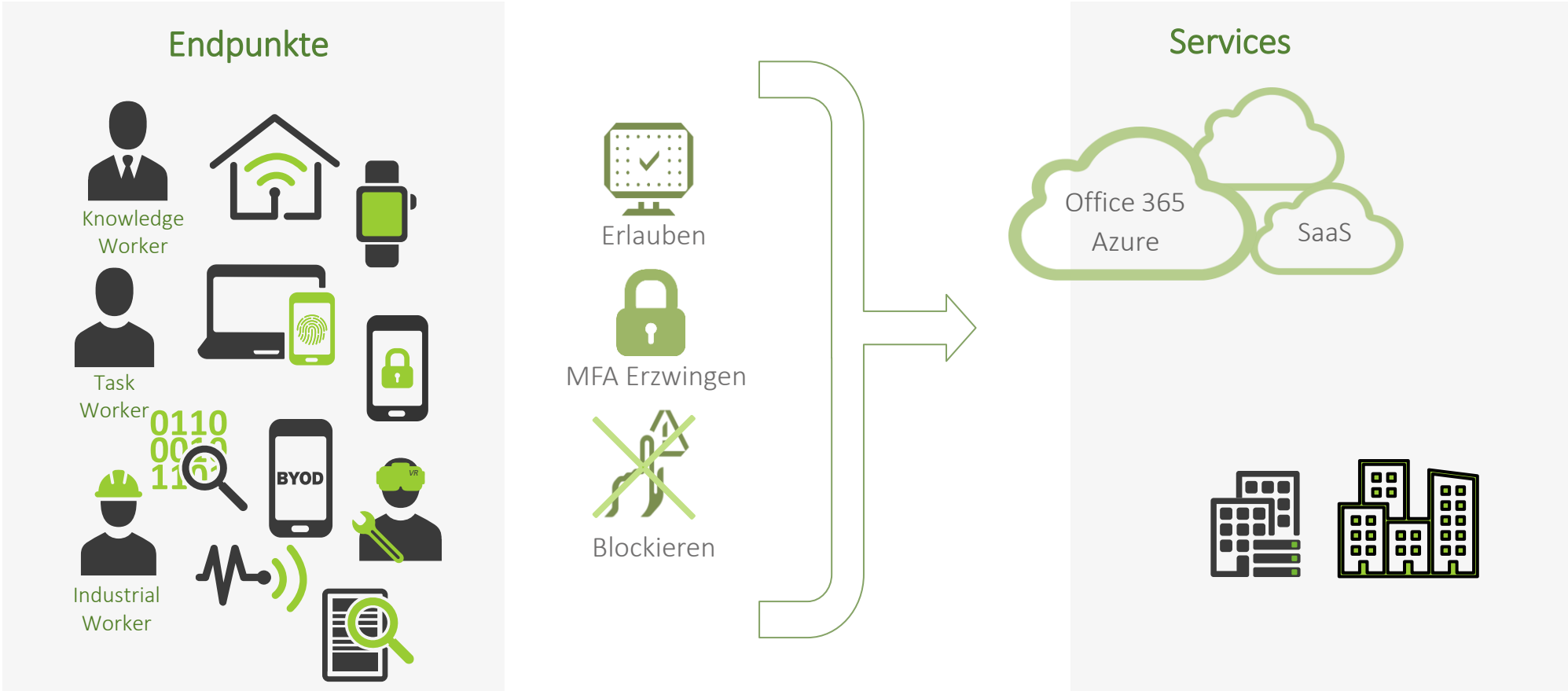
Lösung

- Interner Traffic über Safari (VPN) und Traffic in die Cloud über EDGE
  → ermöglicht gleichzeitig Entra-ID Authentifizierung



Sichere Bereitstellung & Zugriffe für Daten und Services

Mobile Daten und Services sicher Bereitstellen mit Zugriffskonzept



Sichere Bereitstellung & Zugriffe für Daten und Services

Conditional Access im Zusammenspiel mit Microsoft Entra MFA: Zwei Faktoren für ein Halleluja

Ausgangslage

- Sicherer Zugriff auf Daten und Services in M365

Herausforderung

- Unterschiedliche Plattformen und Bereitstellungsmodelle (COPE, BYOD…)
- ZeroTrust-Konzept soll verfolgt werden

Lösung

- Separate Policies für Remote-Worker sowie Compliance-Anforderungen und Administratoren
- Compliance Abhängigkeit von Apps wie z.B. Defender voraussetzen → Compliance-Status wird dauerhaft geprüft

Sichere Bereitstellung & Zugriffe für Daten und Services

Beispielhafte MAM-Bereitstellung

- Spezifische Conditional Access *„Mobile Remote Worker“* Policy

- Zugriff auf Outlook mit Compliance-Vorrausetzung Microsoft Defender

Technische-Herausforderungen aus der Praxis

Fragen die IT-Verantwortliche kritisch stellen sollten

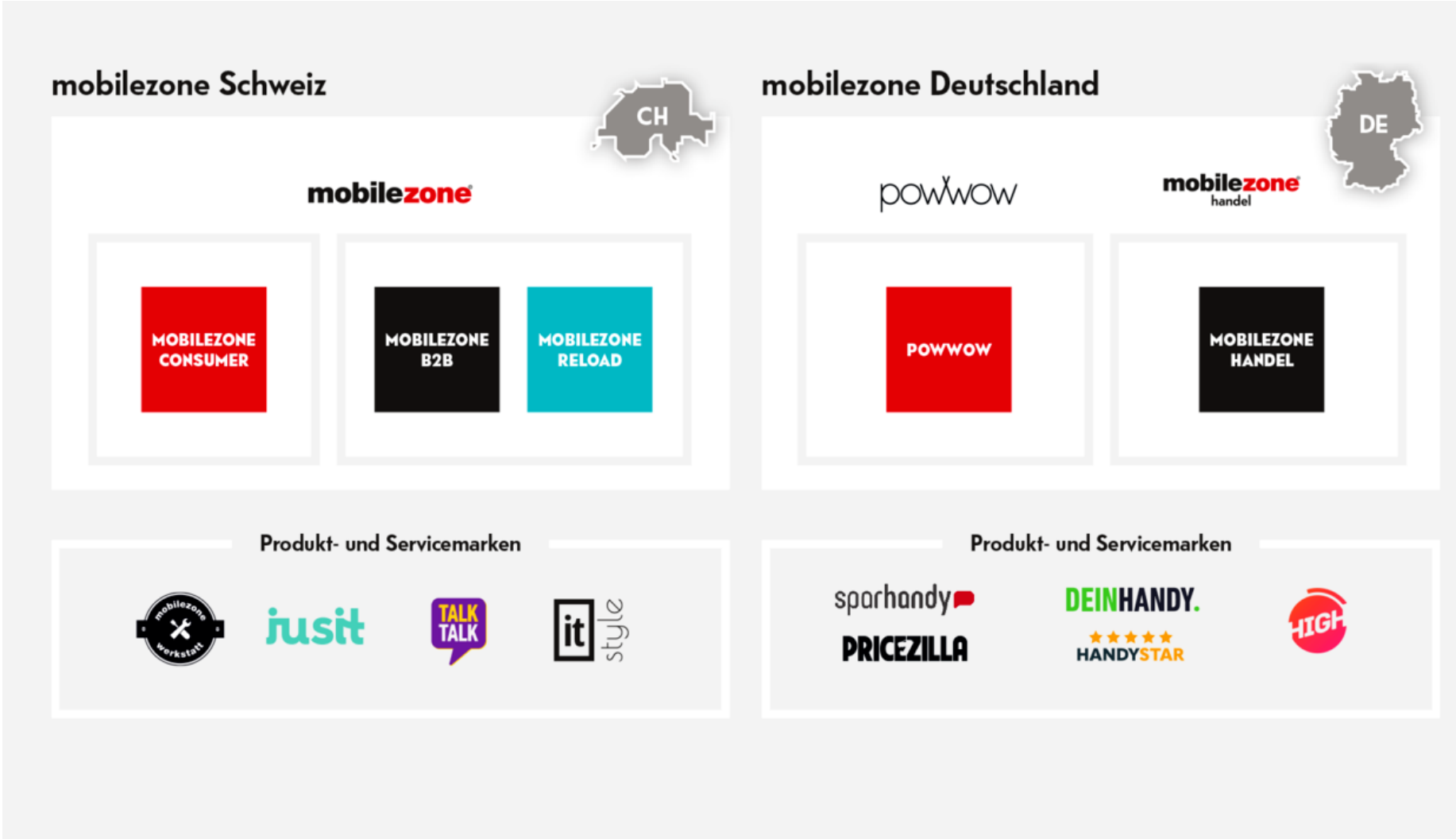
- Auf Intune setzen und auf zusätzlichen Anwendungsfälle und Features verzichten
- Zwei Systeme einsetzen. Einmal Intune für die «einfachen» Anwendungsfälle und ein zweites System für die komplexen Anwendungsfälle. Dies bedeutet aber auch, zweifaches Knowhow, doppelte Dokumentation, umständlichere Prozesse, usw.
- Full Fledged UEM-System für die Verwaltung der mobilen Geräte einsetzen und betreiben
- Hat mein Unternehmen die Fachkräfte/Personalressourcen um:
  - die technischen Hürden bewerten und anschliessend nehmen zu können
  - den Überblick über die Rollen- und Zugriffskonzepte zu behalten
  - die IT-Sicherheit bei diesem Unterfangen sicherzustellen
- Wie weit kann der Endanwender eingebunden und der Prozess automatisiert werden

Grundsatzentscheid:
Welches UEM ist das richtige für unsere Bedürfnisse

Rolle der IT
- was machen wir selbst
User Self Service
- Rolle der Nutzer
- Automatisierung

Marktgebiete

mobilezone



mobilezone business

Der führende Dienstleister für Enterprise Mobile Solutions

- Provider- und herstellerunabhängige Beratung aus einer Hand
- Flächendeckende Präsenz in der Schweiz
- Persönliche Beratung und Betreuung vor Ort
- Viersprachige Kundendienst-Organisation
- 140 Mitarbeitende für Beratung, Services und Technik
- Seit über 20 Jahren im B2B-Markt

Unsere Angebote im Überblick

Beschaffung

Device as a Service

Fleet Management

Mitarbeiterangebote

Reparatur und Gerätetausch

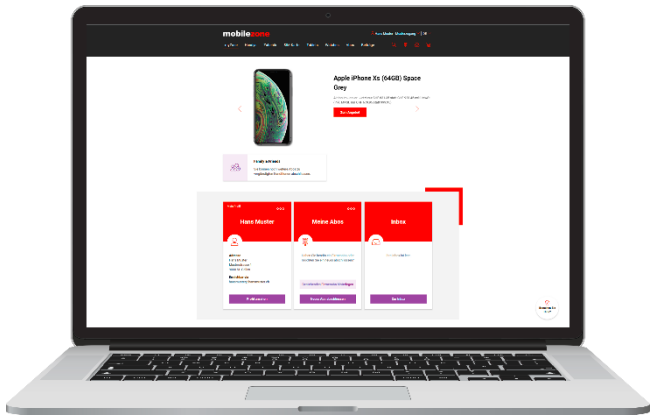
Enterprise Mobility Management

Digitale Abläufe dank Anwenderportal

mobilezone

Mitarbeitende

- Geräte und Zubehör bestellen
- Abos bestellen und mutieren
- Apps herunterladen
- Supportanfragen
- Rechnungen kontrollieren



Enduser Support

- Telefonischer Support
- Tickets bearbeiten
- Abos anpassen
- Nummern aktivieren
- Soforthilfe bei Schadenfällen

Reparatur und Abholstationen

- Reparaturen entgegennehmen
- Austauschgeräte übergeben

HR Manager

- Ein- und Austritte bearbeiten
- Nummern portieren

Controller

- Reports erstellen
- Daten abrufen

Fleet Manager

- User und Accounts verwalten
- Geräte ausrollen (One Touch)
- Geräte und Apps verwalten
- Security Einstellungen
- Reports erstellen

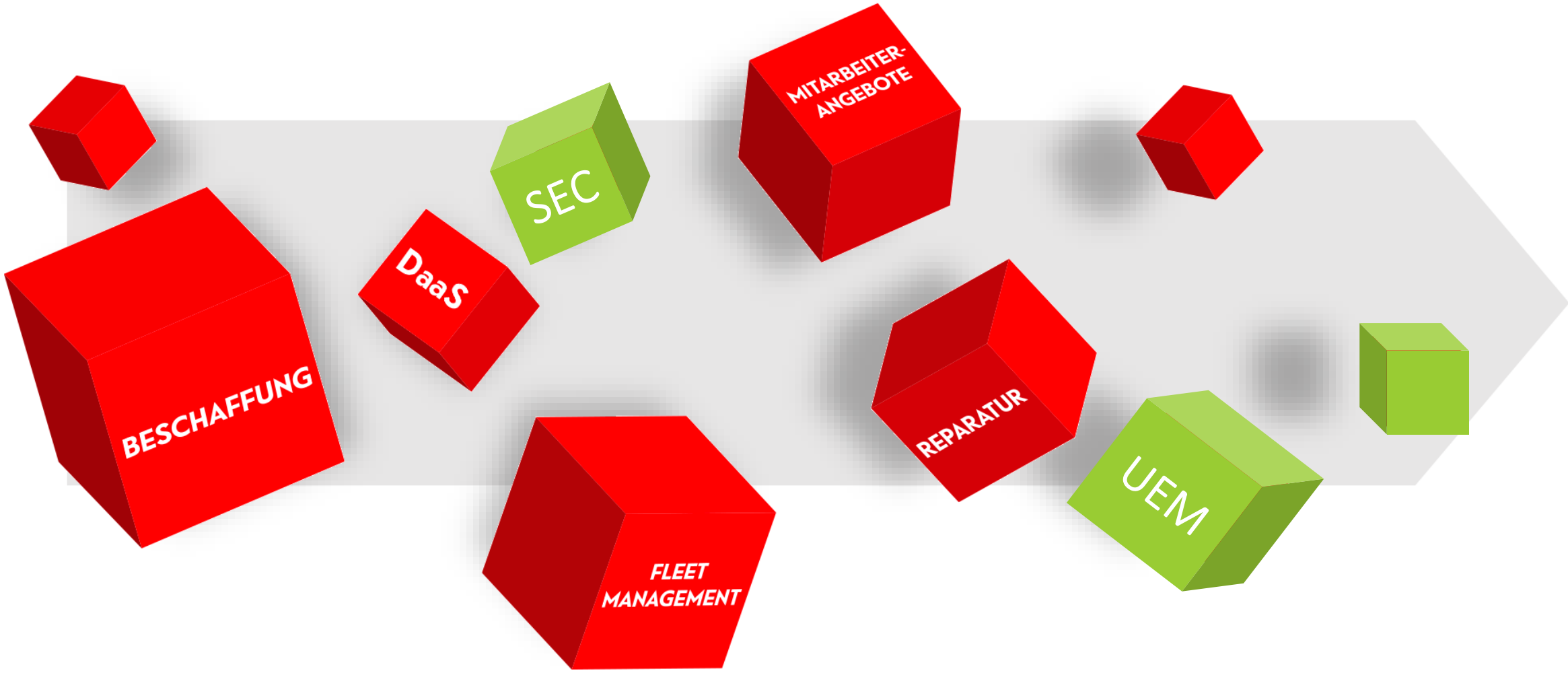
Quick - Dive

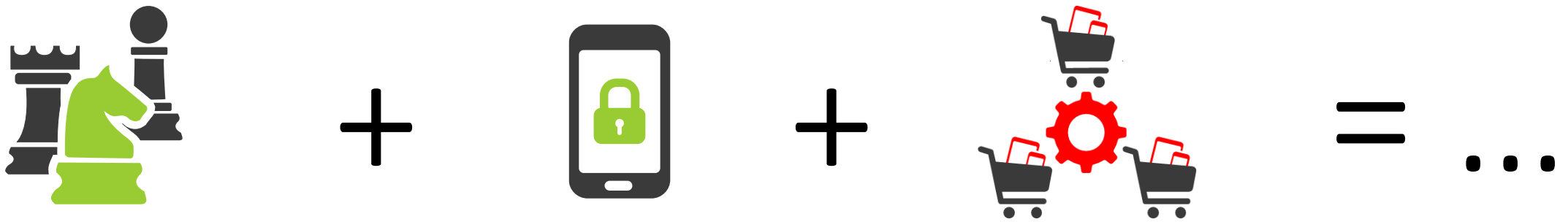
mobilezone

Video fehlt

Komplett Modular im Baukastenprinzip

mobilezone





Doppelte Kompetenz = Ihr Vorteil

Nahtlose, automatisierte Prozesse

Grossartiges Nutzererlebnis

Tiefer Betriebsaufwand

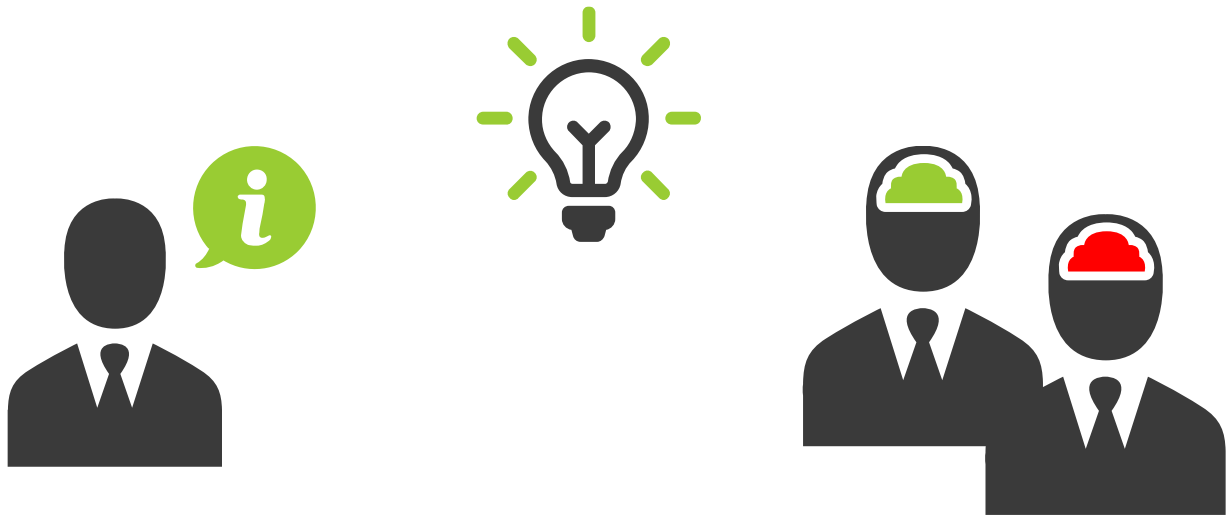
Doppelte Kompetenz

Starke Security bei hoher Usability

Investitionssicherheit mit den Richtigen Tools

Viele erfolgreiche Umsetzungen

Testen Sie uns!



Melden Sie sich für einen kostenlosen, stündigen Austausch zum Thema Enterprise Mobility bei

adrian.gerber@inseya.ch oder pascal.briano@mobilezone.ch

Herzlichen Dank für Ihre Aufmerksamkeit

INSEYA

simply secure

Besten Dank für Ihre Aufmerksamkeit!