IBM Webinare für Kunden

Software Group Industry Solutions

Ansgar Schurek, Senior Client IT Architect - IBM Software Group

29.05.2013

Sicherheit mobiler Geräte in der Fertigungs- und Prozessindustrie

Agenda

1. Mobile Geräte in der Automatisierungsindustrie
2. Herausforderungen und Risikien
3. Lösungsansätze und Nutzen
4. Referenzen
5. Weiterführende Informationen und IBM Ansprechpartner

Agenda

1. **Mobile Geräte in der Automatisierungsindustrie**
2. Herausforderungen und Risikien
3. Lösungsansätze und Nutzen
4. Referenzen
5. Weiterführende Informationen und IBM Ansprechpartner

Mobile Trends haben signifikante Auswirkungen auf Unternehmen

Mobile ermöglicht das "Internet der Dinge"

Global Machine-zu-Machine Verbindungen werden von 2 Milliarden in 2011 auf **18 Milliarden** in 2022 anwachsen [5]

Mobile ist der primäre Kanal

91% der mobilen Nutzer haben ihr Gerät zu 100% ihrer Zeit in Armreichweite [1]

Mobile vermittelt durch-gängige Markenerfahung

90% der Nutzer nuzten mehrere Kanäle, die zusammengeführt werden und eine einheitliche Markenerfahung bieten [4]

Erkenntnisse aus mobilen Daten eröffnen neue Geschäftschancen

75% der mobilen Einkäufer reagieren auf Standort-basierte Nachrichten [2]

Mobile steuert Geschäftstransaktionen

96% Steigerung der mobilen Umsätze an Cyber Monday Verkäufen von 2011 bis 2012 [3]

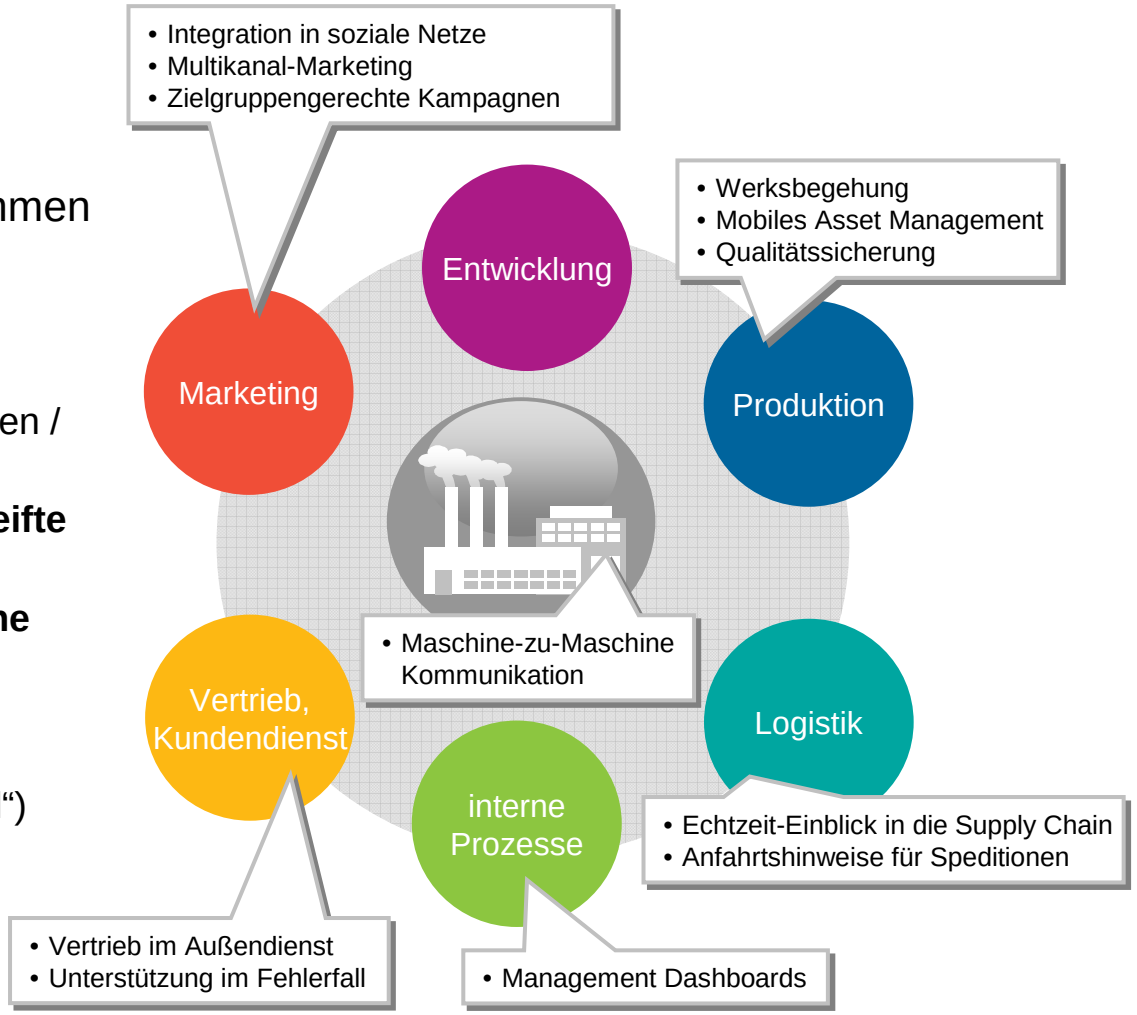
Quellen:

1. "China Mobile 50k Survey"; Morgan Stanley Research, 2011
2. JiWire Mobile Audience Insights Report Q4 2011
3. IBM Coremetrics Retail Data, IBM Pressemitteilung vom 24.11.2012
4. IBM Global Technology Outlook 2013
5. GSMA, Machina Research

Die Automatisierungsindustrie bietet viele Einsatzszenarien für mobile Geräte

Typische Kennzeichen von Unternehmen der Automatisierungsindustrie

- **Komplexe** Organisationsstrukturen
- **Weiträumige** Verteilung der Lokationen / Fertigungsstätten
- Steuerung der Abläufe durch **ausgereifte Prozesse**
- Viele Prozesse bedingen **menschliche Interaktionen**, die oft nur zeitversetzt durchgeführt werden können
- Information werden **geliefert** („push“) oder müssen **angefragt** werden („pull“)



Im Bereich der Maschie-zu-Maschine Kommunikation sind wesentliche Impulse von der „Industrie 4.0“ Initiative zu erwarten

- **Industrie 4.0** ist eine Initiative der **deutschen Regierung**, vertreten durch die deutsche Akademie der Technikwissenschaften (acatech), und der **deutschen Industrie**, vertreten durch die Verbände **ZVEI, VDMA** und **BITKOM**
- Von Seiten der Industrie zielt die Initiative vor allem auf den Aufbau von gemeinsamen, konsensfähigen Infrastrukturen – für die **Steuerung** und **Kommunikation** zwischen **Produktionsakteuren**
- Maschinen, Lagersysteme und Betriebsmittel werden zu **Cyber-physical Systems**, die **eigenständig** Informationen austauschen, Aktionen auslösen und sich gegenseitig selbständig steuern
- **Intelligente Produkte** sind eindeutig identifizierbar, jederzeit lokalisierbar und kennen ihre Historie, ihren aktuellen Zustand sowie alternative Wege zum Zielzustand
- Eingebettete **Produktionssysteme**
  - sind **vertikal** mit betriebswirtschaftlichen Prozessen innerhalb von Fabriken und Unternehmen vernetzt
  - sind **horizontal** zu verteilten in Echtzeit steuerbaren **Wertschöpfungsnetzwerken** verknüpft
  - erfordern ein **durchgängiges Engineering** über die gesamte Wertschöpfungskette
  - bilden neue Arten der Wertschöpfung und neue Geschäftsmodelle

Plattform INDUSTRIE 4.0

Agenda

1. Mobile Geräte in der Automatisierungsindustrie
2. **Herausforderungen und Risikien**
3. Lösungsansätze und Nutzen
4. Referenzen
5. Weiterführende Informationen und IBM Ansprechpartner

Mobile Geräte bringen einzigartige Security Herausforderungen mit sich

Mobile Geräte werden gemeinsam genutzt

- Persönliche Telefone und Tablets werden mit der Familie geteilt
- Unternehmens-Tablets mit Kollegen
- Soziale Normen im Umgang mit mobilen Geräten

Mobile Geräte haben mehrere Rollen

- Arbeitsgerät
- Unterhaltungsgerät
- Persönliche Organisation

} Sicherheitsprofil pro Rolle?

Mobile Geräte sind verschiedenartig

- BYOD (Bring Your Own Device) diktiert verschiedene Betriebssysteme
- Hersteller diktiert verschiedene Betriebssystem-Versionen

Mobile Geräte werden an verschiedenen Lokationen genutzt

- Eine einzige Lokation kann öffentliche, private und Funkverbindung bieten
- Erhöhte Abhängigkeit vom Unternehmens-WiFi
- Geräte können leichter abhanden kommen

Mobile Geräte priorisieren den Nutzer

- Konflikte mit Benutzererlebnis werden nicht toleriert
- Betriebssystem Architektur legt Benutzer als steuernde Macht fest
- Schwierigkeit Regeleinhaltung zu erzwingen, z.B. App Listen

Mobile Security – Was sind die Bedrohungen?

Malware

- Viren und Würmer
- Trojaner
- Spyware

Direkte Attacken

- Attackierung der Device Interfaces
- Netzwerk Denial of Service („DoS“)
- bösartige SMS

Verlust und Diebstahl

- Zugriff auf sensible Daten

Abhören der Datenkommunikation

- ”Erschnüffeln” von Daten bei Übertragung oder Empfang

Abgrabung und missbräuchliche Verwendung

- Online Datenräuber
- unerwünschte Kommunikation
- Datenabfluss

Auch wenn Mitarbeiter oft denken, dass mobile Geräte nicht angegriffen werden, sind sie in der Realität leichte Ziele für Hacker

Die Sicherheitsbedrohung ist real ...

Quellen:
1. Ponemon Institute, Global Study on Mobility Risks, Februar 2012
2. Ponemon Institute, Cost of Data Breach Study, 2012
3. Verizon, 2013 Data Breach Investigations Report, 2013

Agenda

1 Mobile Geräte in der Automatisierungsindustrie

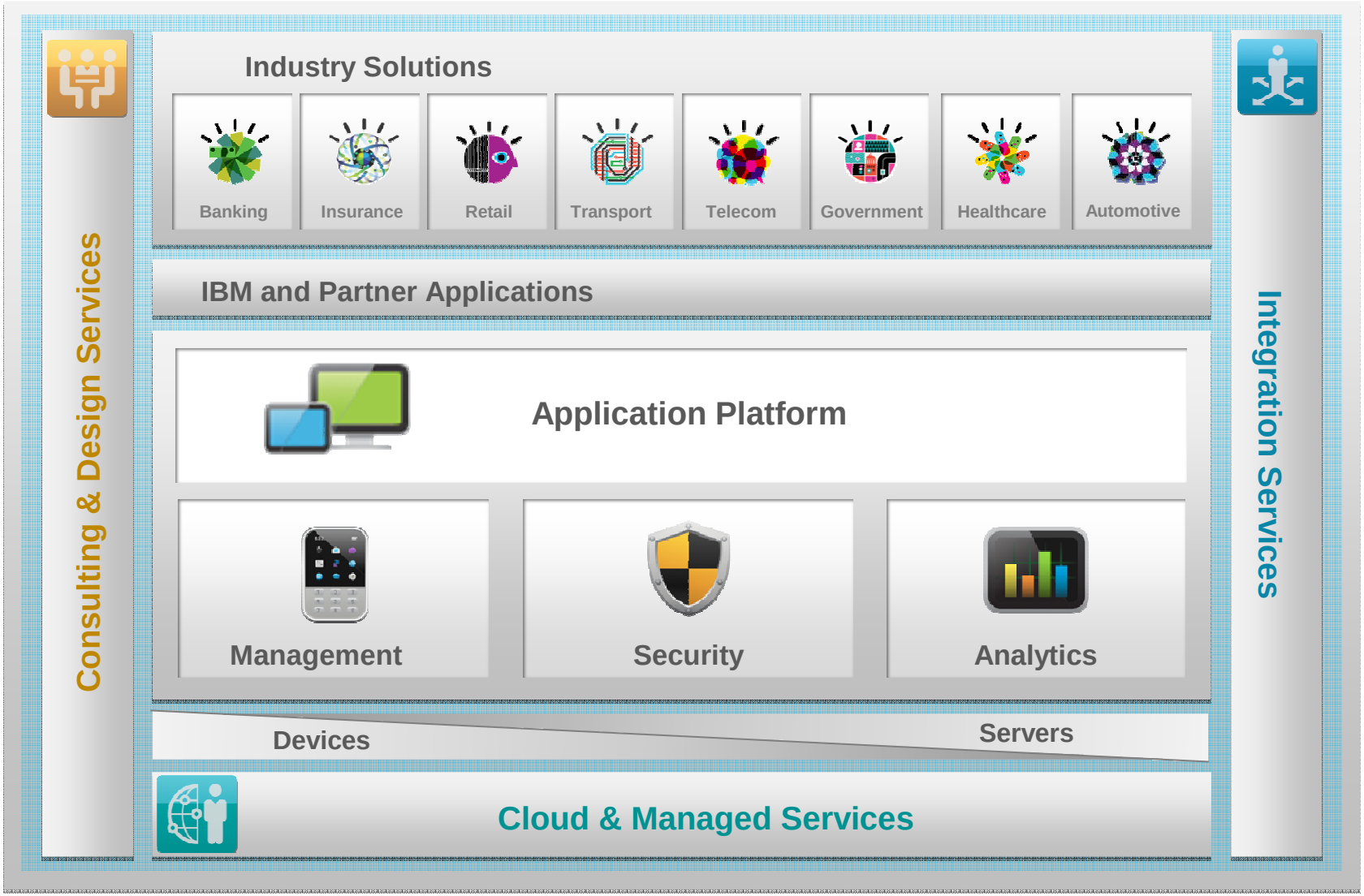
2 Herausforderungen und Risikien

3 Lösungsansätze und Nutzen

4 Referenzen

5 Weiterführende Informationen und IBM Ansprechpartner

IBM MobileFirst Überblick



IBM MobileFirst Ansatz für Security & Management

Device Management

Security für das mobile Gerät und für Daten

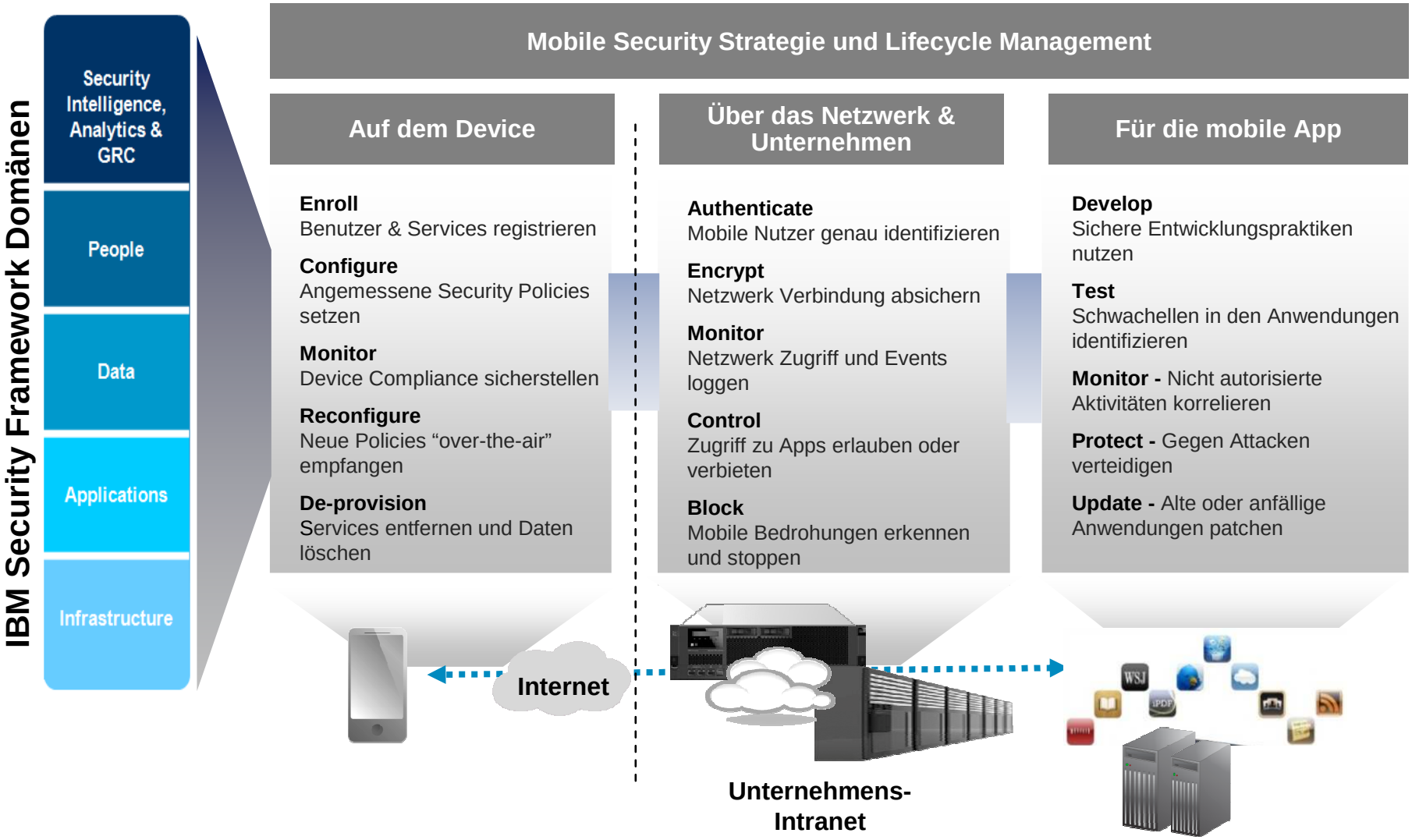
Netzwerk, Daten- und Zugriffs-Security

Sichtbarkeit und adaptive Security Richtlinien (“Policies”)

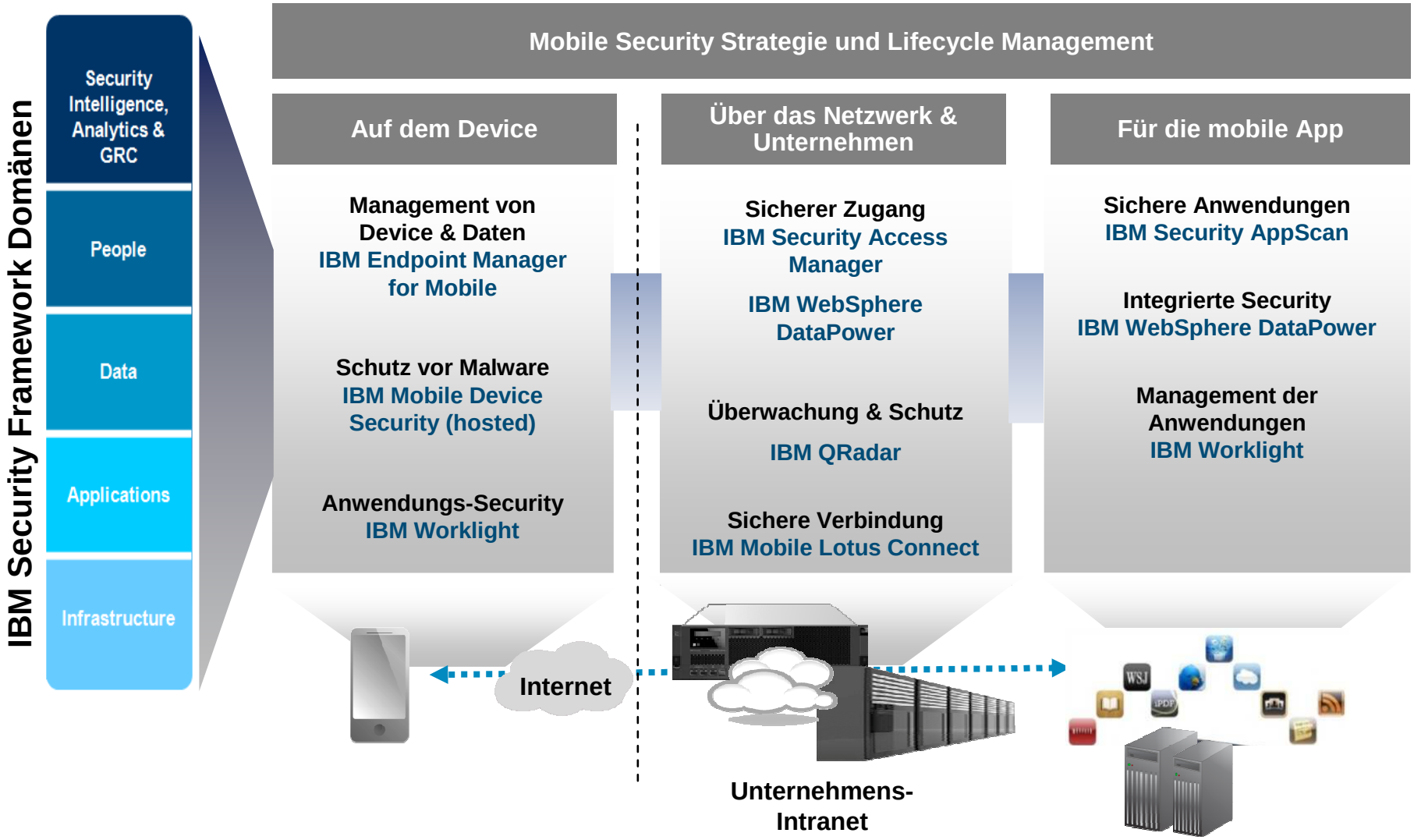
Application Layer Security

Entwicklung und Test von Anwendungen

Aspekte zur Absicherung mobiler Unternehmen



IBM MobileFirst Angebot zur Absicherung mobiler Unternehmen



Sichtbarkeit und Kontrolle über alle mobilen Devices in Echtzeit

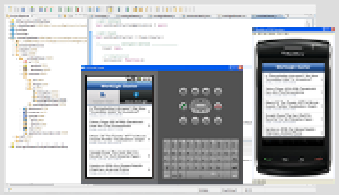
IBM Endpoint Manager for Mobile Devices

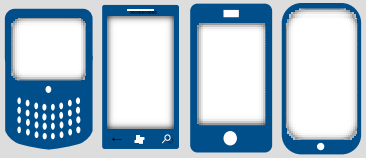
- Management der von den **Mitarbeitern genutzten** mobilen Geräte im Unternehmen
- Versorgung von **Patches, Upgrades**
- **Integration mit Backend** IT Management Systemen wie Service Desk, CMDB, und SIEM
- Security **Threat Erkennung** und automatische Einleitung von Gegenmaßnahmen
- Unterstützung diverse Plattformen, z.B. **iOS, Android, Symbian, BlackBerry, Windows Phone, Windows RT**
- Gemeinsame Infrastruktur zum Management **aller Endpoints** im Unternehmen (mobil und stationär)
- hohe **Skalierbarkeit** der Lösung (bis zu 250.000 Endpunkte pro Server)

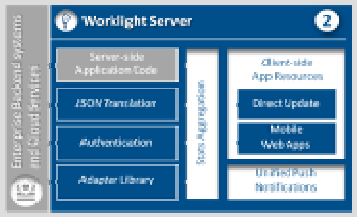
Eine sicherere Plattform für die Entwicklung und den Betrieb von mobilen Anwendungen

IBM Worklight

- Vollständige Mobile Application Plattform bestehend aus den Komponenten:
  - **Worklight Studio:** Entwicklungsumgebung für die Cross-Plattform Entwicklung von mobilen Anwendungen
  - **Worklight Server:** Mobile Middleware mit Unterstützung für Push Notification, Versionsverwaltung, Sicherheit und Integration
  - **Worklight Runtime Components:** Bibliothek und API's für den Zugriff auf Native Gerätefunktionalität und den Worklight Server
  - **Worklight Console:** Web basierte Konsole zur Administration der mobilen Anwendung und des Worklight Server
- Nutzung offener **Standards** (HTML5, Dojo, PhoneGap, Eclipse, etc.)
- Verschiedene **Security Features**, z.B. verschlüsselter offline Cache, Authentication Framework, Direct update
- Vielzahl unterstützter **Devices**: Android, iOS, Windows 8, Windows RT, Windows Phone, BlackBerry, Java ME







Security und Privacy über den gesamten mobile App Lebenszyklus zum Schutz empfindlicher Geschäftssysteme

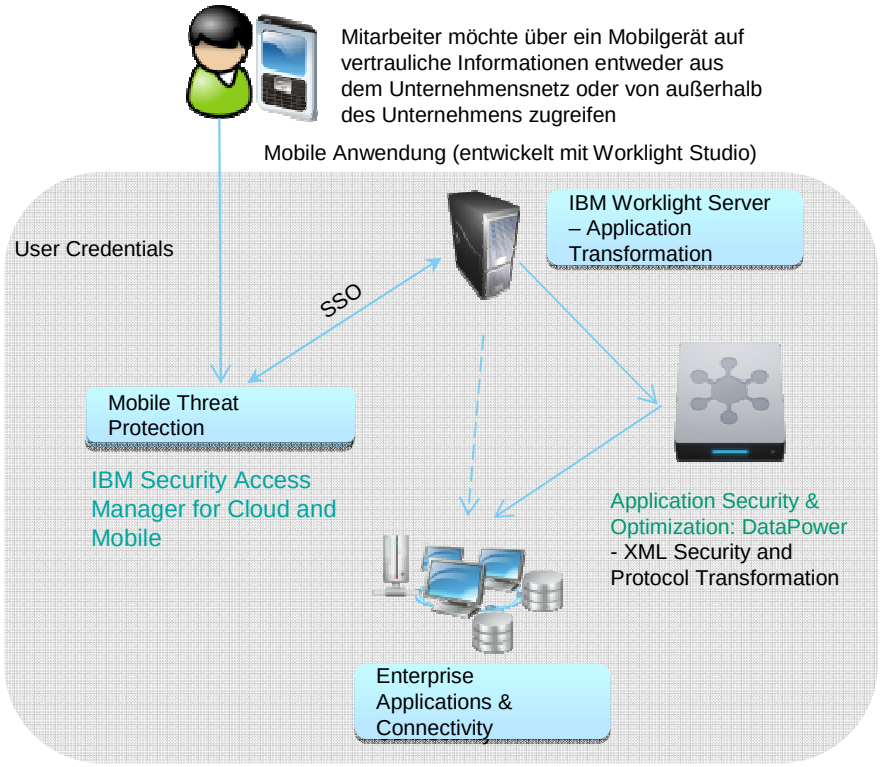
IBM Security AppScan Source

- **Automatisierung** von arbeitsintensiven **Security-Tests** und **-Audits**
- Hilft bei Erkennung, Analyse und Beseitigung von **Security Schwachstellen**
- Ermöglicht **“Secure by Design"** Prozess in der Software Entwicklung von mobilen Anwendungen
- Unterstützung von **iOS** und **Android** Umgebungen
- Unterstützung verschiedener App-Typen: **Web**, **nativ** und **hybrid**
- Erstellung von **Reports** mit priorisierten Metriken

Bessere Identifikation von Security Risiken bei mobilen Zugriffen

IBM Security Access Manager for Cloud and Mobile

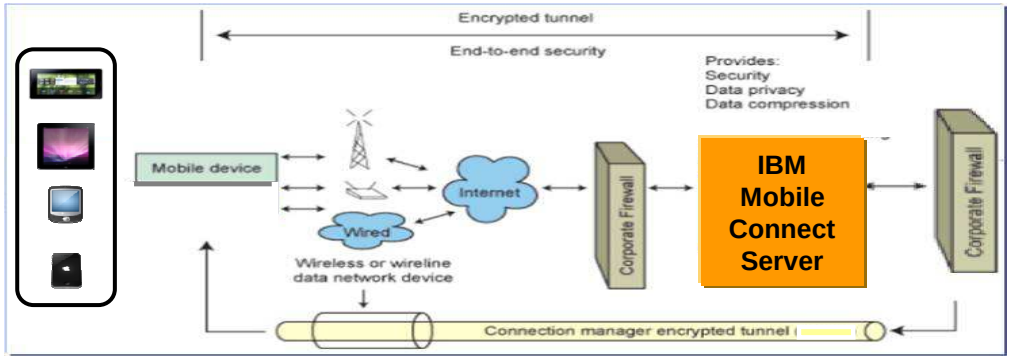
- Mobiler Zugriffsschutz mit **Single Sign-on** und **kontextbasierter** Zugangskontrolle
- **Dynamische Bewertung** des Sicherheitsrisikos einer Zugriffs-anforderung
- Sicherstellung, dass **Gerät und Nutzer** authentisiert und autorisiert sind
- **Flexibilität** bei Authentisierung: User ID/Password, OTP, Biometrics, Zertifikat, eigene Verfahren
- Schutz der Applikationen von bekannten Bedrohungen durch **Analyse** des HTTP **Verkehrs**



Eine sichere mobile Verbindung

IBM Mobile Connect

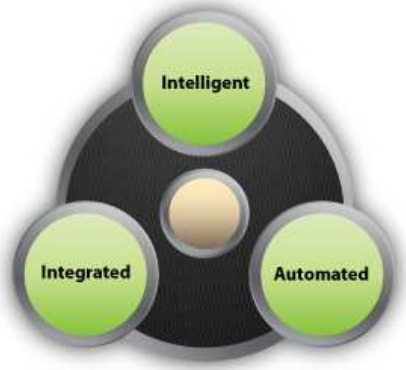
- Komplettlösung für ein **mobiles Virtual Private Network (VPN)**
- Ermöglicht eine **sichere Verbindung** zu Unternehmensanwendungen von mobilen Geräten
- Schutz von sensiblen Daten mit **Client-** oder **clientlosem Zugriff**
- **Starke Authentisierung** und **Verschlüsselung** der Durchgangsdaten
- Unterstützung für verschiedene **Betriebssysteme**, Mobilgeräte und Netze



Eine anpassbare Security Überwachung

IBM Security QRadar

- Liefert **mobile Security Intelligenz** durch Monitoring der von anderen mobile Security Systemen gesammelten Daten
- Schafft **Transparenz** und erkennt **Bedrohungen**
- Integrierte, intelligente und belastbare **Plattform** für:
  - Suche
  - Filtern
  - Regel-Beschreibung
  - Reporting Funktionen
- Eine **einzige Benutzerschnittstelle** für:
  - Log Management
  - Risk Modeling
  - Vulnerability Prioritization
  - Incident Detection
  - Impact Analysis Aufgaben



Agenda

1 Mobile Geräte in der Automatisierungsindustrie

2 Herausforderungen und Risikien

3 Lösungsansätze und Nutzen

4 **Referenzen**

5 Weiterführende Informationen und IBM Ansprechpartner

Die interne Mobile Strategie der IBM

- IBM hat eine interne **„bring-your-own device" (BYOD) Strategie**
- Mitarbeiter sind hochgradig mobil (flexible Arbeitsplätze, Außendienst etc.)
  - **440.000** Mitarbeiter weltweit
  - **120.000** Benutzerzugänge zum IBM Netzwerk durch mobile Geräte
  - **40.000** benutzen Smartphones, die von IBM gestellt werden
  - **80.000** verwenden eigene Geräte (auf eigene Kosten)
- **Historisch** hatte IBM eine **vom Unternehmen gesteuerte**, auf BlackBerrys basierende Mobilstrategie
- Mit der Zeit kamen iPhones und andere Geräte **durch die Mitarbeiter** hinzu
- IBM's BYOD Strategie erlaubt den Mitarbeitern nach ihren Wünschen und Bedürfnissen zu arbeiten
- Als Rahmenwerk im Umgang mit mobilen Geräten dienen **"secure computing guidelines"**
- **IBM Endpoint Manager for Mobile Devices** und **IBM Mobile Connect** sind großflächig ausgerollt

IBM Endpoint Manager + Guidelines

Ein Energieversorger verwaltet mobile Geräte ohne die bestehende Infrastruktur zu erweitern

- Unternehmen
  - Energieversorger mit **25,000 Mitarbeitern** und 4.5 Mio Kunden im Südwesten der USA
  - Führend in “Clean Energy” mit hoher Versorgungsstabilität
- Herausforderung
  - **Migration** von traditionellen Endgeräten zu **mobilen Geräten**
  - Unterstützung über **20.000 Geräte**, viele **BYOD**
  - Schneller **Rollout** (wenige Tage)
  - Beachtung interner **Security Policies** und externer Auflagen
- Lösung
  - Erweiterung der existierenden IBM **Endpoint Manager** Umgebung um **IEM for Mobile Devices**
  - **Skalierbarkeit** bis 250.000 Endpunkte ohne neue HW

CeBIT 2013 Showcase: „Security at Manufacturing“

- Herausforderung
  - **Fertigungsysteme** werden zunehmend Ziel von **Hacker-Angriffen**
  - Hohes **Risiko**, da Fertigungssysteme i.d.R. nicht mit Fokus auf Security entwickelt wurden
- Lösungsansatz
  - Zentrales Monitoring sowie Asset und Vulnerability-Management durch “**Security Information & Event Management**” **(SIEM)** System
  - **Analyse** des Netzwerk Verkehrs („Payload“) auf Anomalien
  - Erkennung von **Malware** wie Stuxnet, Duqu, Flame etc. durch ihre spezifischen Eigenschaften (Flow Analysis)
  - Erkennung **nicht autorisierter Devices**
  - Intelligente **Korrelation** von Events aus verschiedenen Quellen
- Produkte
  - Verwendung von **IBM QRadar** als zentrales SIEM Werkzeug (non-intrusive)

Showcase auf CeBIT 2013

Security Dashboard

Agenda

1. Mobile Geräte in der Automatisierungsindustrie
2. Herausforderungen und Risikien
3. Lösungsansätze und Nutzen
4. Referenzen
5. **Weiterführende Informationen und IBM Ansprechpartner**

Weitere Infos und Quellen

- IBM X-Force 2012 Trend and Risk Report, März 2013
  - www.ibm.com/services/us/iss/xforce/trendreports/

- IBM Mobile Security Informationen
  - IBM GTS White Paper: “Securing mobile devices in the business environment” public.dhe.ibm.com/common/ssi/ecm/en/sew03027usen/SEW03027USEN.PDF

- IBM MobileFirst Strategie und Portfolio
  - IBM MobileFirst Homepage: www.ibm.com/mobilefirst
  - Informationen zu Produkten: Einstieg über IBM MobileFirst Homepage, dann „Offerings“ und zu den Abschnitten blättern:

IBM MobileFirst Security

IBM MobileFirst Management

Vielen Dank für Ihre Aufmerksamkeit!

Ansgar Schurek
SW Client Architect
IBM Software Group

IBM Deutschland GmbH
Laatzener Straße 1
30539 Hannover

Telefon: +49-7034-643-2924
eMail: ansgar.schurek@de.ibm.com

Fragen und Antworten