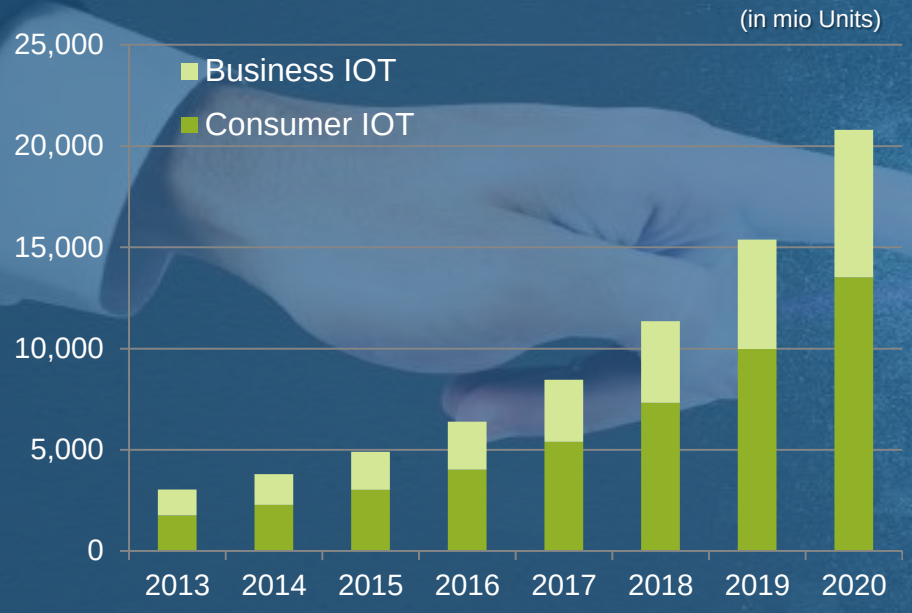
SECURE INDUSTRIAL VISIBILITY FOR MACHINE MANUFACTURERS

Volker Gerstenberger
Director Product & Solution Marketing, Giesecke & Devrient

June 8, 2016

IOT - ENDLESS OPPORTUNITIES

Gartner forecast on IoT installed base



Source: Gartner Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2015

In a recent study of IoT devices

- 70% contained Security exposures
- 25% holes or risks of compromising the home network, on average, found for each device
- 80% did not require passwords of sufficient complexity and length
- 90% collected at least one piece of personal information
- 70% allowed an attacker to identify a valid account through account enumeration

Source: HP

SECURITY THREATS ON INDUSTRIAL IOT

ENABLING SECURE SMART SERVICES

Connect

Collect

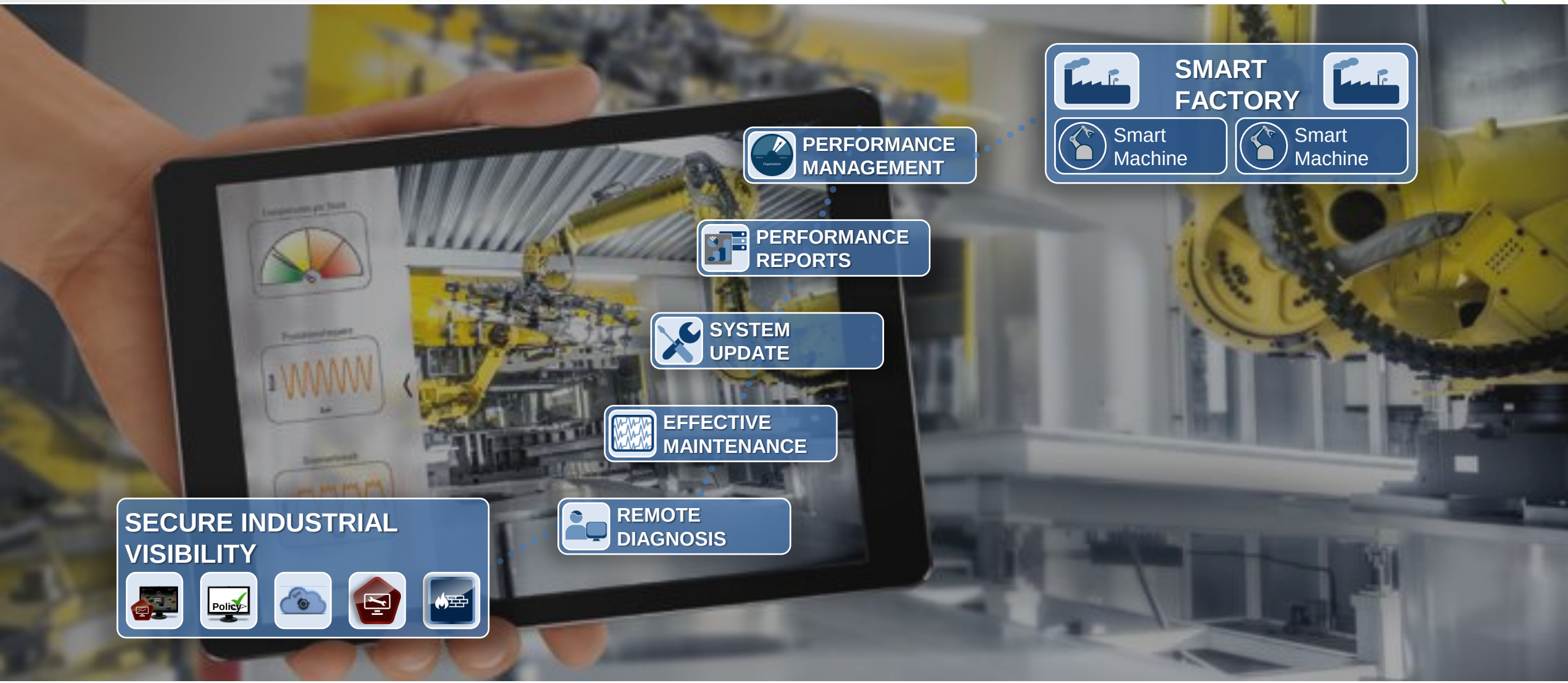
Consume

Connectivity

Identity

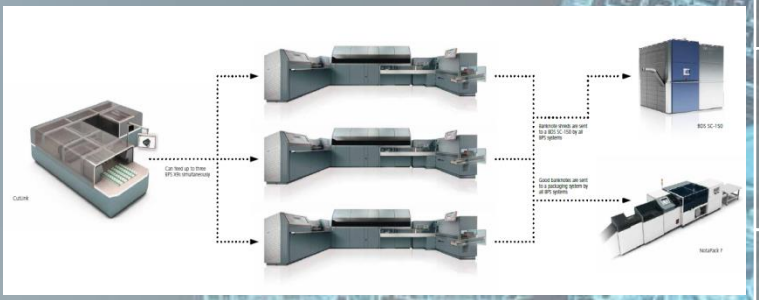
Security

THE ROAD TO INDUSTRY 4.0



MACHINE MANUFACTURER BENEFITS

Deployment setup



Use cases

- Remote Diagnosis and Assistance
- Effective Maintenance
- System Update
- Performance Reports
- Performance Management

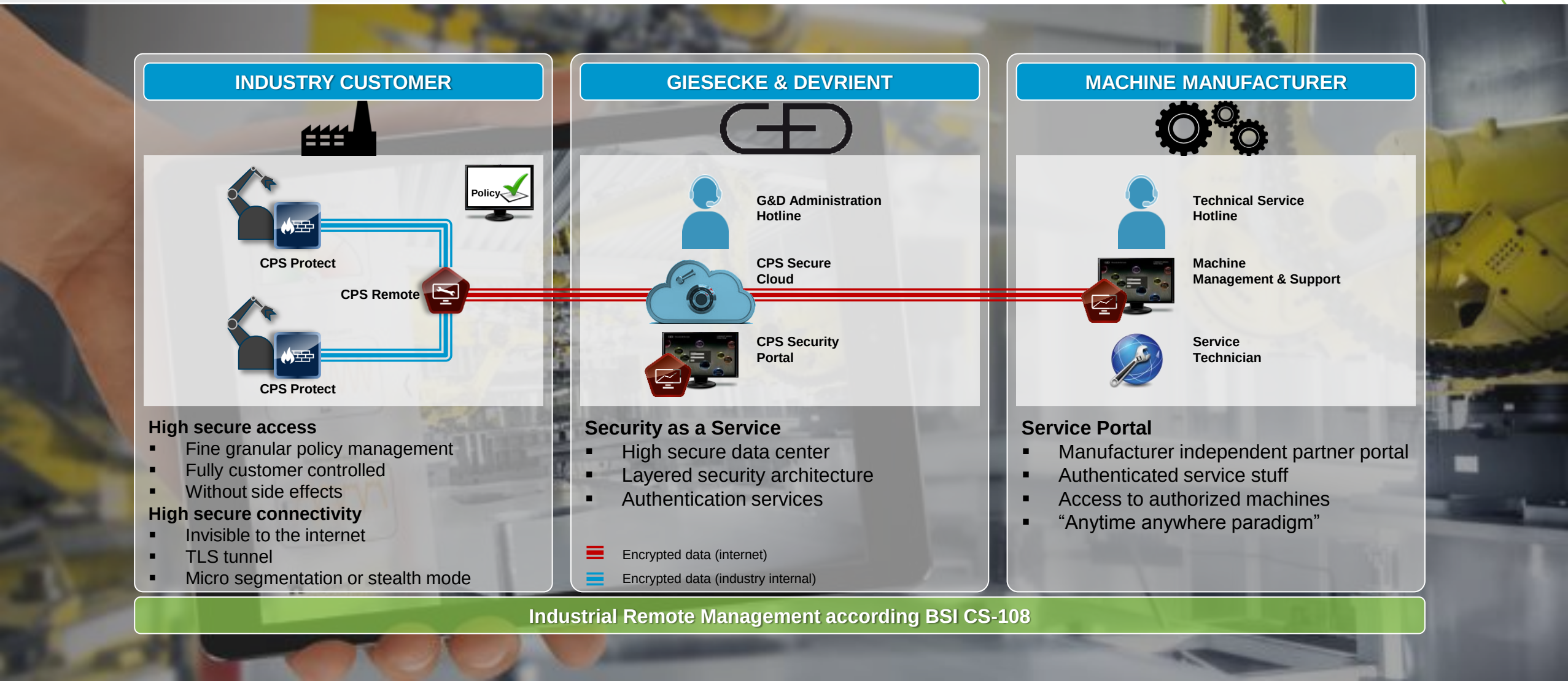
Solution components

- CPS Security Portal
- CPS Policy Management
- CPS Secure Cloud
- CPS Remote
- CPS Protect

Benefits

1. Minimize your TCO
2. Increase protection
3. Manage multiple sites
4. Gain visibility and control of usage
5. Protect your remote and roaming staff

THE ROAD TO INDUSTRY 4.0



High secure access
- Fine granular policy management
- Fully customer controlled
- Without side effects

High secure connectivity
- Invisible to the internet
- TLS tunnel
- Micro segmentation or stealth mode

Security as a Service
- High secure data center
- Layered security architecture
- Authentication services

Service Portal
- Manufacturer independent partner portal
- Authenticated service stuff
- Access to authorized machines
- “Anytime anywhere paradigm”

G&D AND PTC – ENABLING SECURE IOT SERVICES

Flexible Connectivity

M2M SIMs, eUICCs
eSIM management
Device configuration
Secure personalization
Industry grade logistics

Scalable Security

Secure environments (i.e. Smart Cards, USB Token, SIM, SIM, eUICC, eSE, TAK)
Secure personalization
Remote software update and remote maintenance

The different vertical markets in the IOT require adequate and scalable security solutions to achieve necessary convenience demanded by the customer

Trusted Identity

Secure environments (i.e. Smart Cards, USB Token, SIM, eUICC, eSE, TEE)
Identity management for users, devices and machines
Secure key management
Trusted service management

For embedded systems with a requirement for high security the dedicated combination of hardware and software is essential to achieve this protection

G&D AND PTC – ENABLING SECURE IOT SERVICES

Giesecke & Devrient

- Flexible Connectivity (eSIM Management)
- Scalable Security (SW, HW)
- Secure Service Management
- Trusted Identity for IoT devices
- Firmware update over-the-air
- Secure communication channels

PTC®

- Application Development Platform (AEP)
- IoT Application Enablement & Integration
- Big Data Analytics
- Data abstraction
- Augmented Reality
- Digital Twin

KEY TAKE AWAYS

IoT Novice

First IoT projects initiated but not yet up and running

Start thinking about the security requirements of your current AND future use cases

IoT User

Running IoT operations without special security requirements

Check out G&D's flexible connectivity solutions

IoT Advanced

Multiple IoT operations up and running with specialsecurity requirements

Learn more about G&D's flexible connectivity and scalable security solutiutions

IoT Expert

Multiple IoT operations up and running with high security demoands from the customer

Find out more about G&D's high security offening

liveworx.com

LIVE WORX 16™

Please use the mobile app to rate this session

Access the latest schedule and join the conversation on social media **#LIVEWORX #IoT**.