Security In The Age Of IoT

John Boudewijns

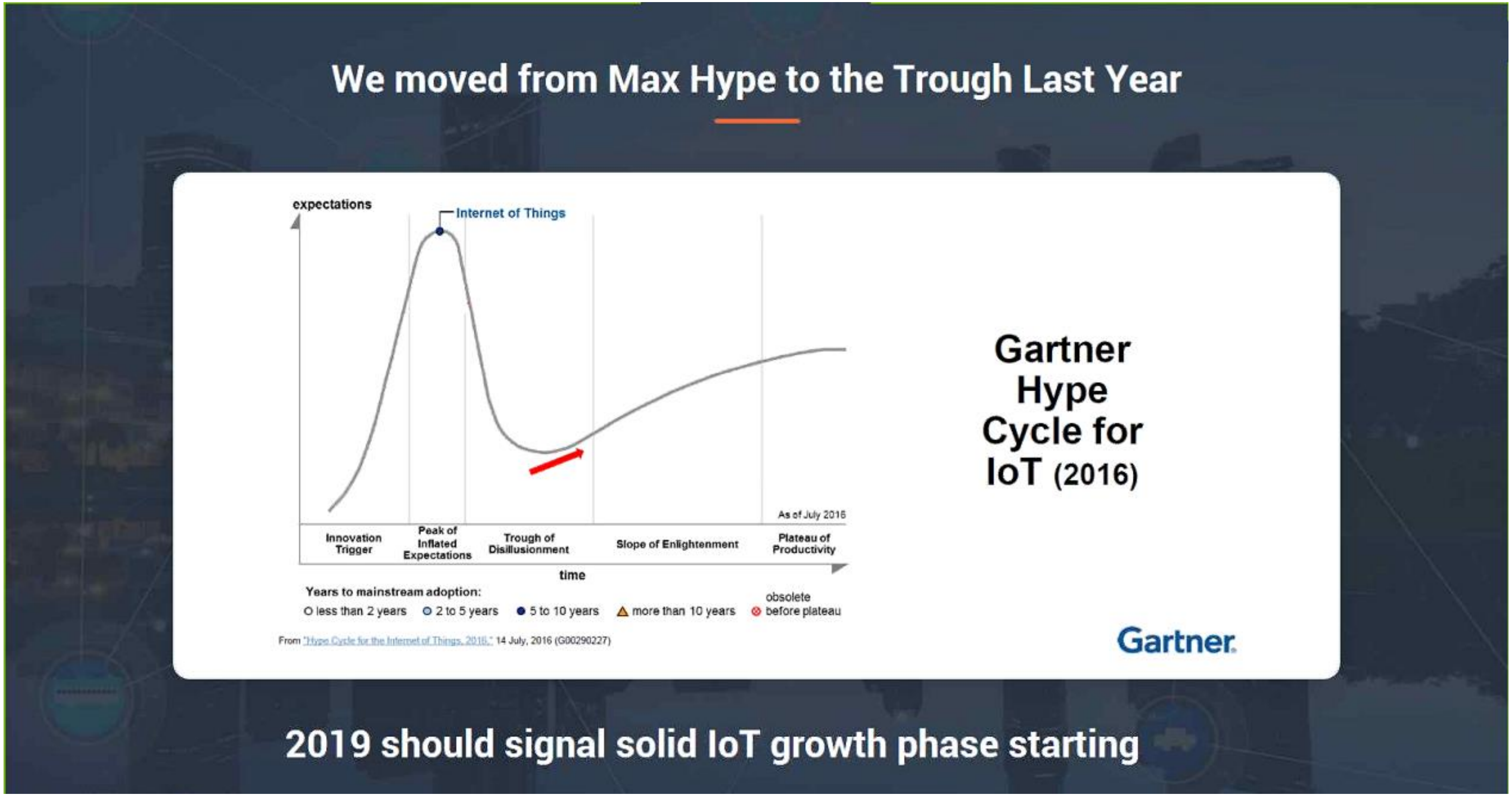
LANTRONIX®

CONNECT SMART. DO MORE.

D&E event 2018

The Internet of things (*IoT*) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data

IoT Market Adoption



We moved from Max Hype to the Trough Last Year

From "Hype Cycle for the Internet of Things, 2016," 14 July, 2016 (G00290227)

Gartner

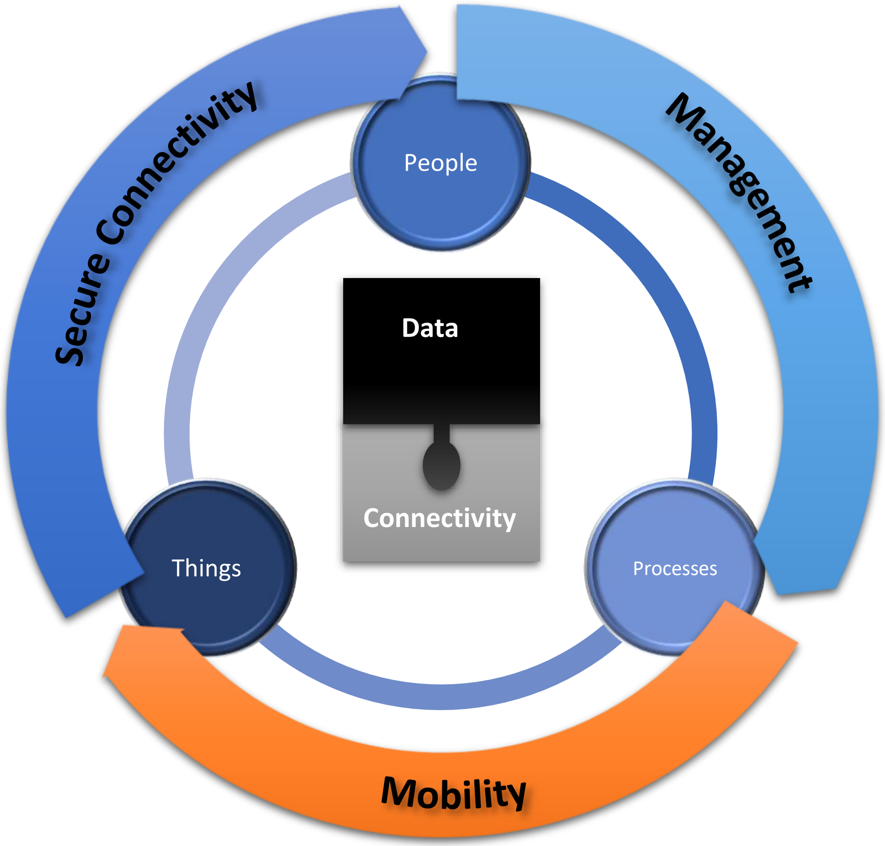
Gartner Hype Cycle for IoT (2016)

2019 should signal solid IoT growth phase starting

Bringing About the IoT

- New business opportunities and revenue models
  - Shortened time-to-market
  - Realized ROI on R&D

- Effective utilization of enterprise assets
- Employee productivity gains
- Improved customer experiences and retention
- Improvement in process efficiencies
  - Secure Connectivity
  - Mobility
  - Analytics



Secure Connectivity

- Certificate Management
- Enterprise WLAN Security
- FIPS 140-2 Compliance
- SSL/TLS
- Identity and Access

Management

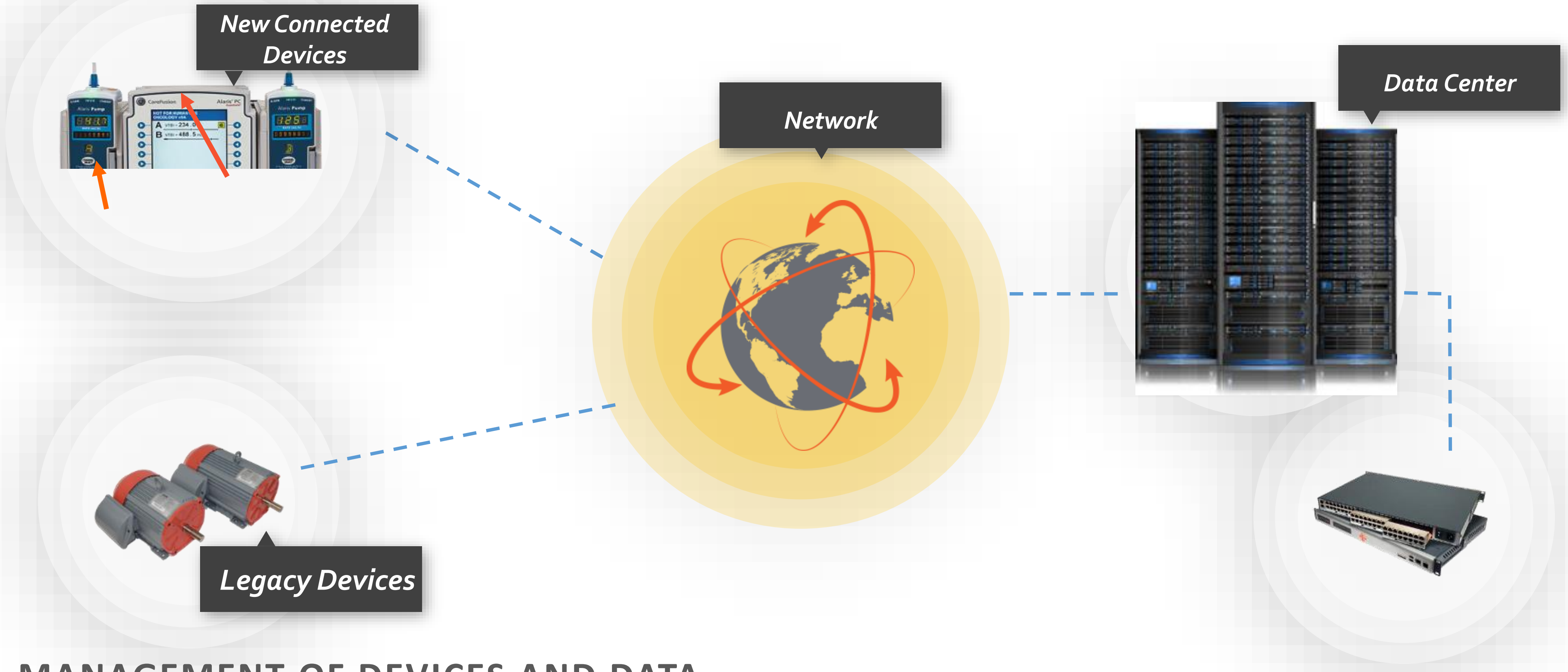
- Web Services API
- OTA Firmware Upgrades
- Zero Touch Provisioning

Mobility

- Direct mobile device access
- Mobile friendly WebService APIs
- Libraries for Quick Provisioning
- Sample

Internet Of Things Simplified

1. CONNECTIVITY FROM THE DEVICE TO THE DATA CENTER

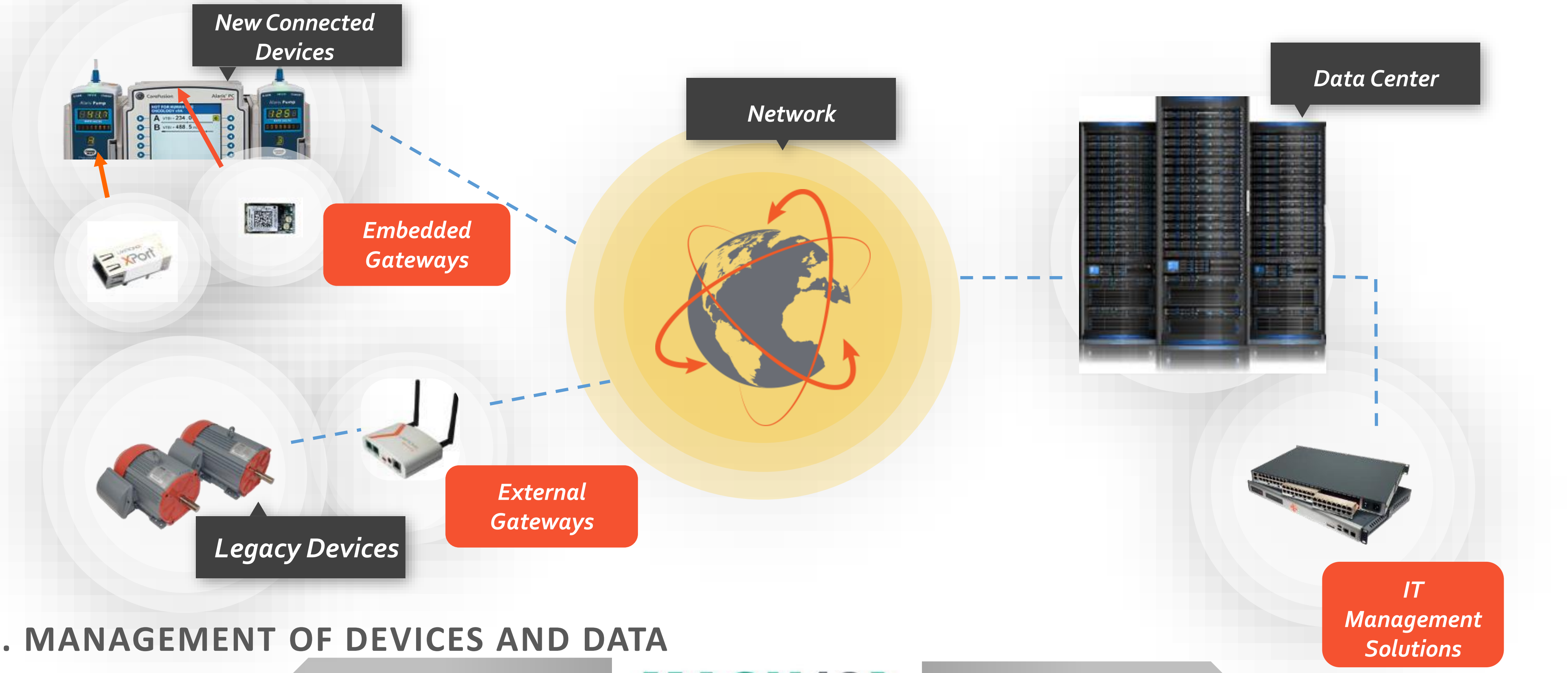


2. MANAGEMENT OF DEVICES AND DATA

MACH10

Internet Of Things Simplified

1. CONNECTIVITY FROM THE DEVICE TO THE DATA CENTER



New Connected Devices

Embedded Gateways

Legacy Devices

External Gateways

Network

Data Center

IT Management Solutions

2. MANAGEMENT OF DEVICES AND DATA

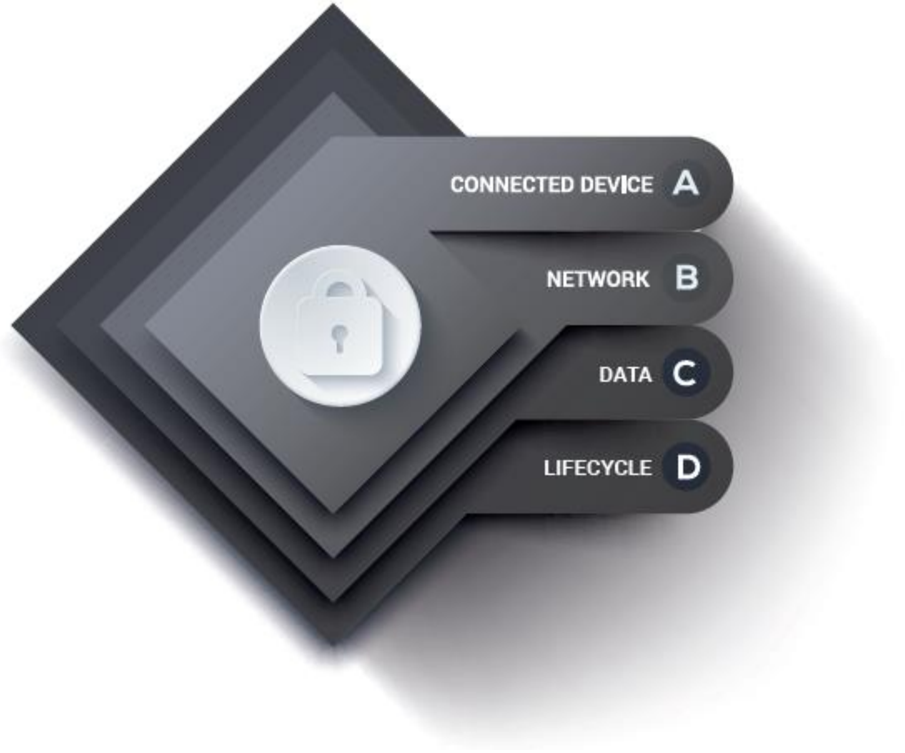
MACH10

D&E event 2018

1. CONNECTIVITY FROM THE DEVICE TO THE DATA CENTER

The Multi-Layered Approach To IoT Device Security

- Securing The Connected Devices
  - Trusted Boot/Secure Boot
    - Embedded devices should have secure certificate storage, which is programmed during manufacturing to establish the root of trust
  - Application Whitelisting
  - Access Control
    - OEMs should select devices that allow them to configure multiple users and assign them granular permissions to access various functions of the device
- Securing The Network
- Securing The Data
- Securing The Lifecycle



D&E event 2018

Building The Secure Device Security Framework

ENCRYPTION

Data encryption technologies such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) and X.509 PKI for data encryption throughout the network (data in motion)

AUTHENTICATION

Standard and Enterprise Wi-Fi security such as PSK, Wi-Fi Protected Access 2 (WPA2)-Enterprise and Extensible Authentication Protocol (EAP) for secure Wi-Fi network connectivity

VERIFICATION

Secure Boot that cryptographically verifies firmware and software packages at boot time and Secure Firmware-Over-The-Air (FOTA) update ensures only authorized firmware gets programmed

Secure credential storage that protects critical key and password information on the device (data at rest)

COMPLIANCE

The Federal Information Processing Standard 140-2 (FIPS 140-2) certification, which is a U.S. and Canadian co-sponsored security standard for hardware, software, and firmware solutions that ensure end users receive a high degree of security, assurance, and dependability

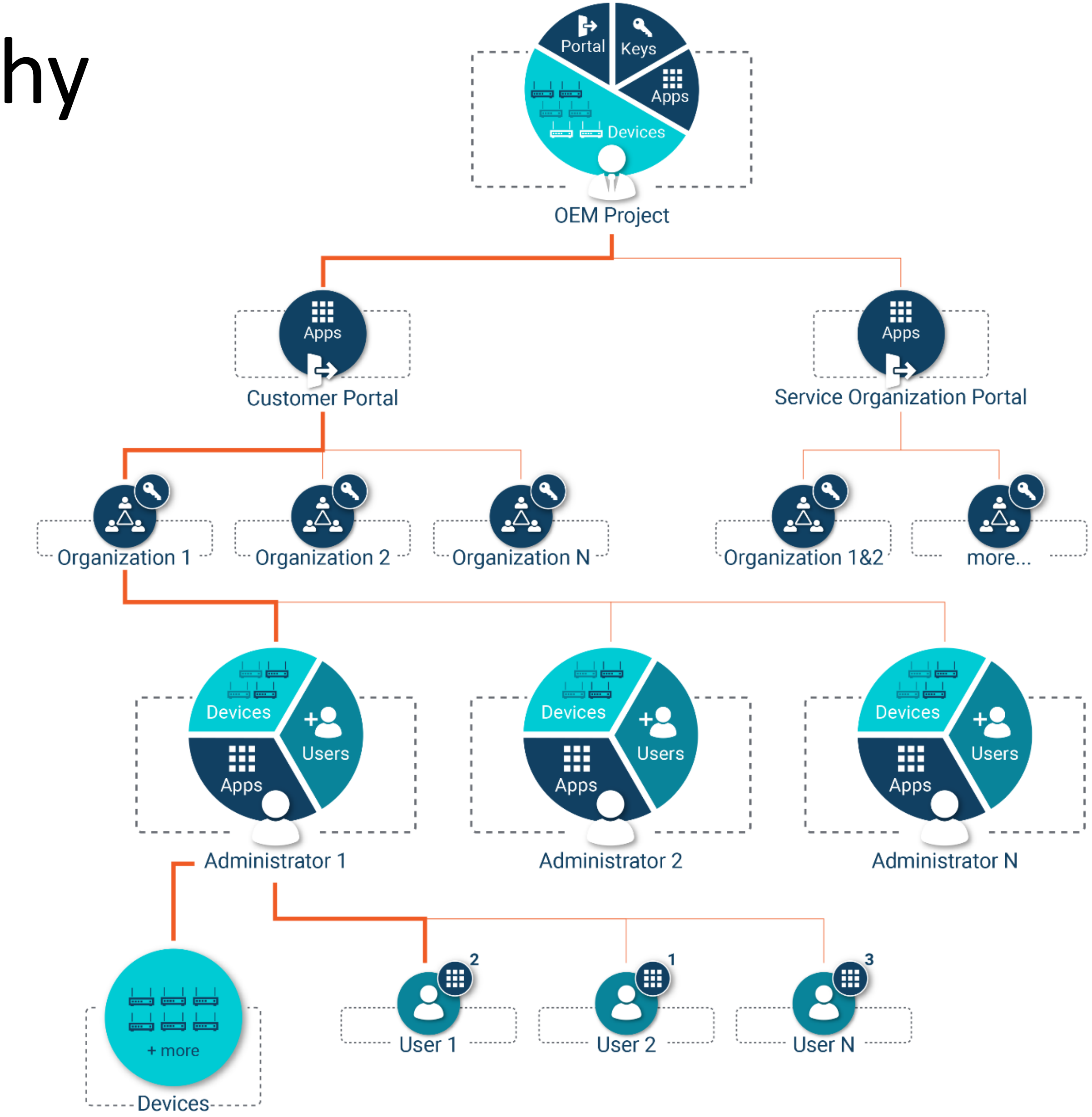
2. MANAGEMENT OF DEVICES AND DATA

Management Hierarchy

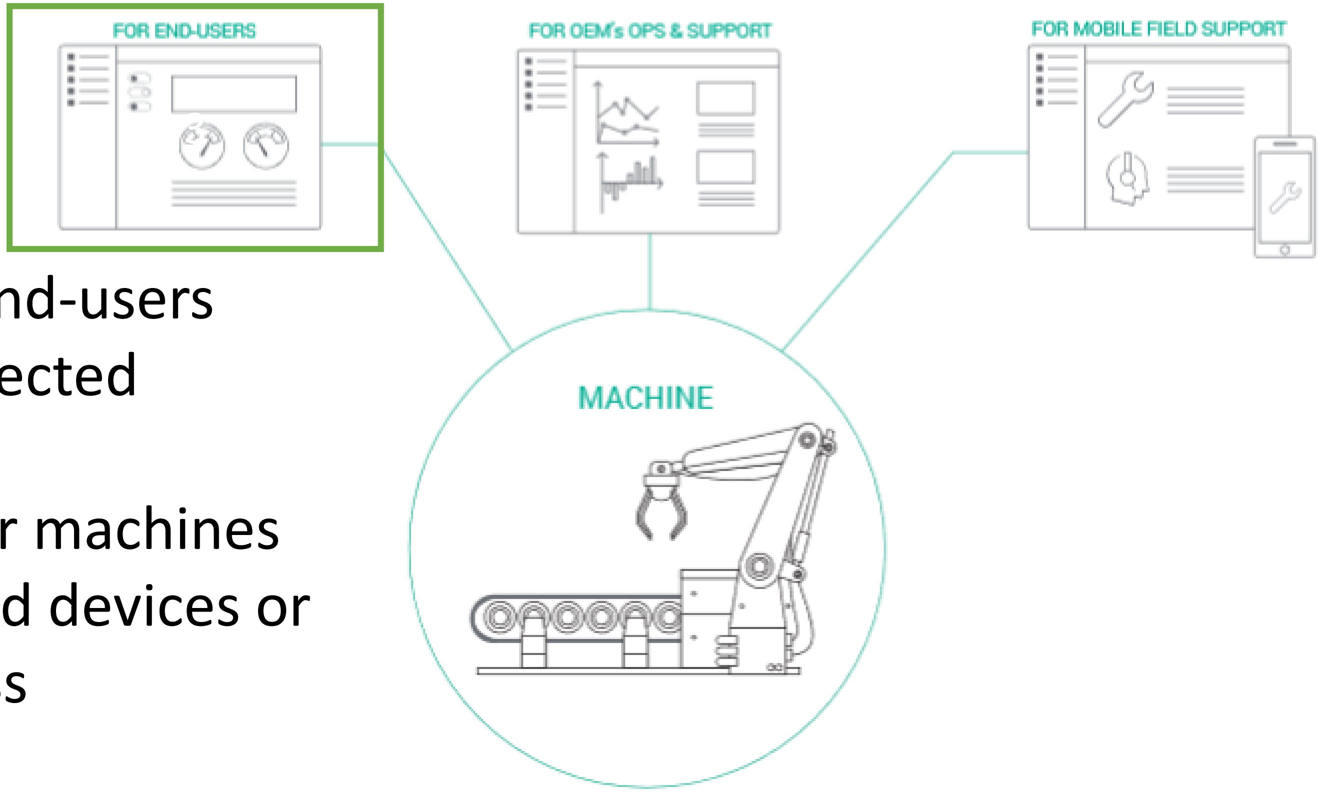
Project Administrator Level

Organization Administrator Level

User Level



Need For Three Different Device Management Software Applications

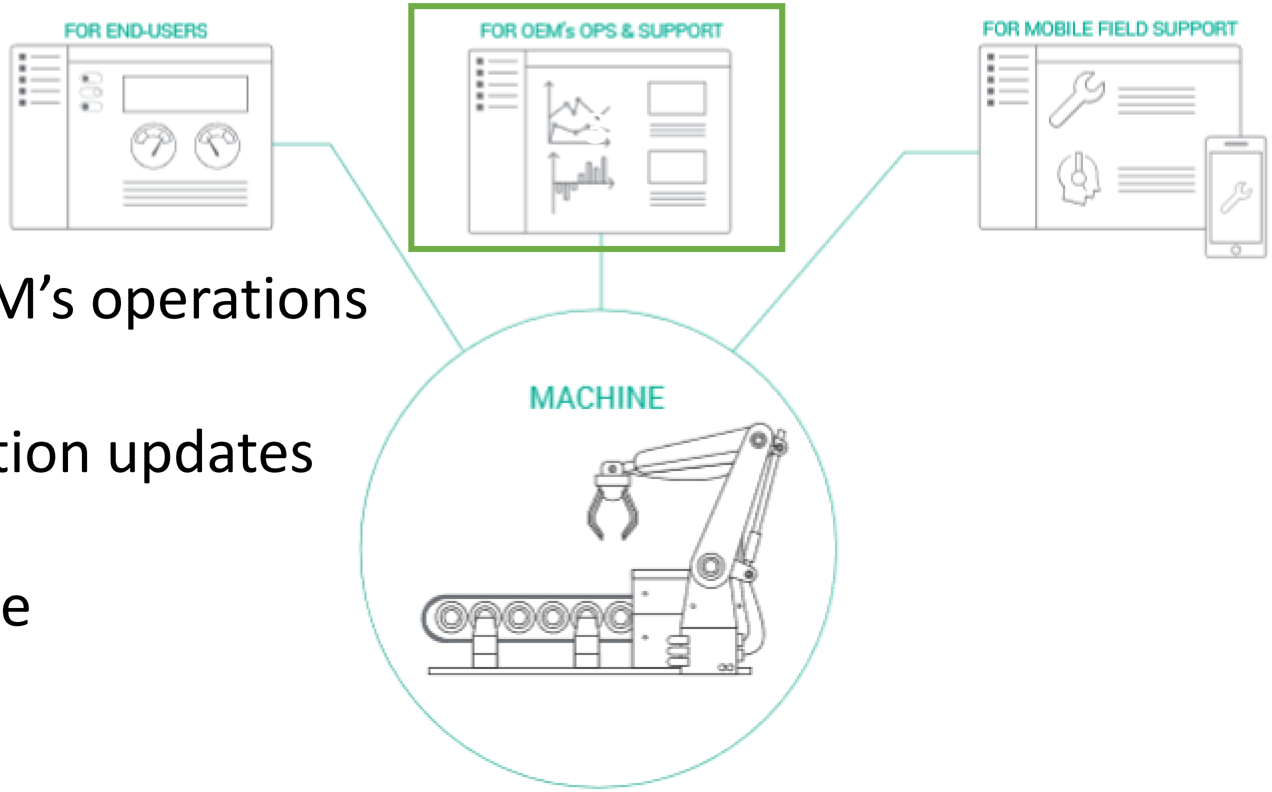


Device management software for end-users

- Provision and configure the connected devices or machines
- Operate the connected devices or machines
- Integrate data from the connected devices or machines with other line of business applications

D&E event 2018

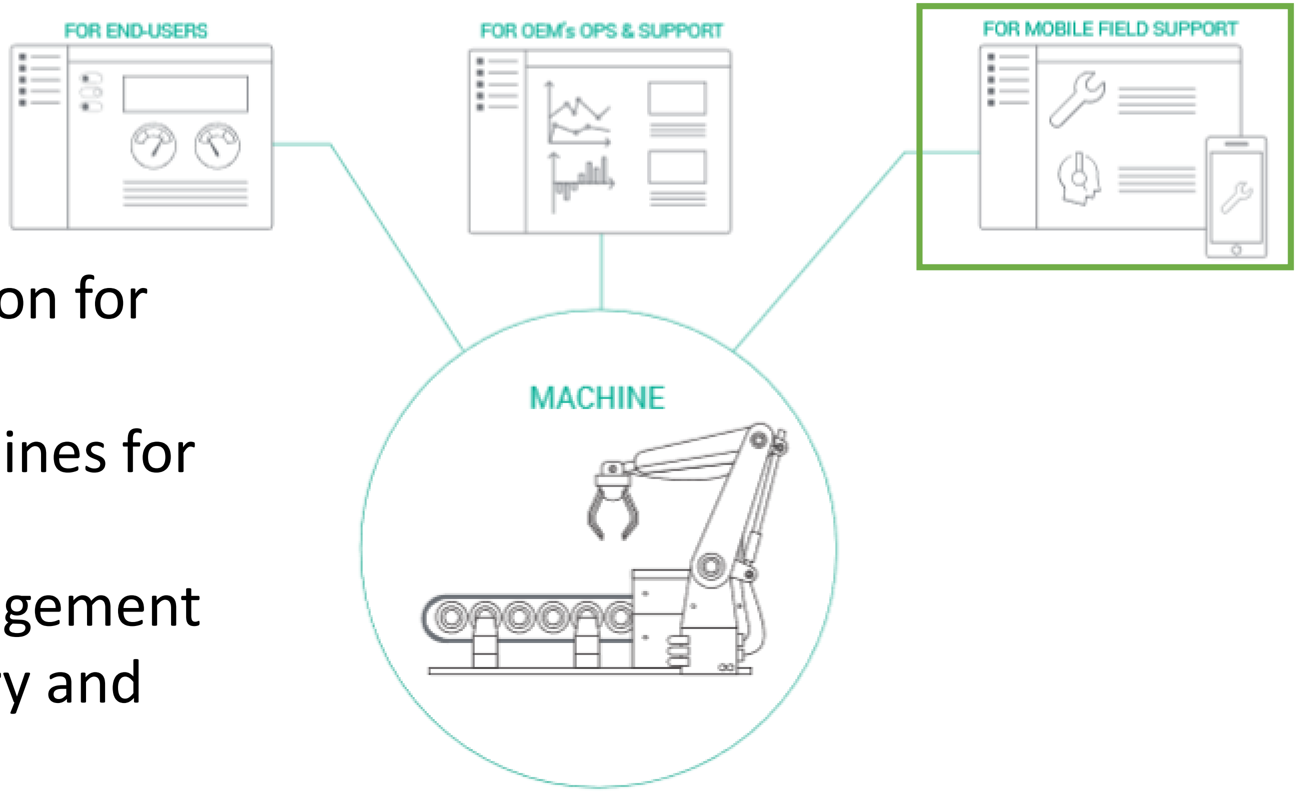
Need For Three Different Device Management Software Applications



Device management software for OEM’s operations and support teams

- Centralized firmware and configuration updates
- Remote diagnostics and support
- Device data collection and predictive maintenance

Need For Three Different Device Management Software Applications

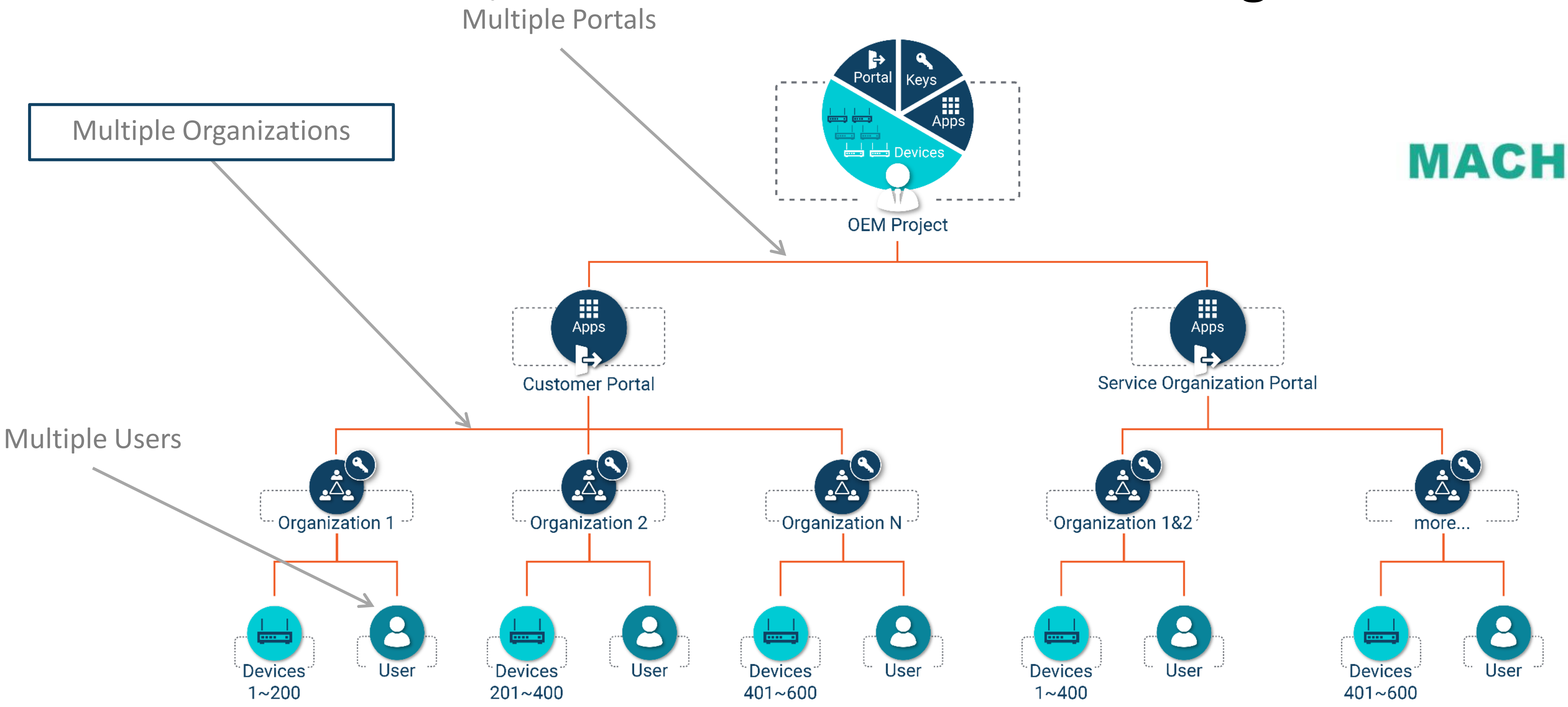


Device management mobile application for field support teams

- Directly connect to devices or machines for quick diagnosis
- Connect to centralized device management software for device or machine history and documentation
- Re-configure and provision devices or machines

D&E event 2018

Lantronix MACH10, a Secure Multi-Tenant Management Platform



Multiple Portals

Multiple Organizations

Multiple Users

Portal

Keys

Apps

Devices

OEM Project

Apps

Customer Portal

Apps

Service Organization Portal

Organization 1

Organization 2

Organization N

Organization 1&2

more...

Devices 1~200

User

Devices 201~400

User

Devices 401~600

User

Devices 1~400

User

Devices 401~600

User

MACH10

D&E event 2018

Choosing Your IoT Supplier

- Need a reliable, mission critical, industrial design Wi-Fi or wired ethernet solution?
- Connectivity software is not your core competency or priority?
- Your products have long lifecycles and you need a reliable Wi-Fi / Ethernet solutions provider with the relevant modular RF certifications?
- Did you experience the pain of trying to DIY and realize that working with a partner is better and more cost-effective?
- **Secure IoT gateways connecting your devices safely to a secure management Platform**

Learn all about:

A ‘ready-to-go’ **Management Platform** that seamlessly connects your **IoT Gateways**

At **www. Lantronix.com**

LANTRONIX

CONNECT SMART. DO MORE.

Get your free trial set up with ACAL BFI and Lantronix here at the D&E Event !!