Securing the Connection to the Cloud

Jeff Steinheider

Director Product Marketing
Industrial Applications Processors
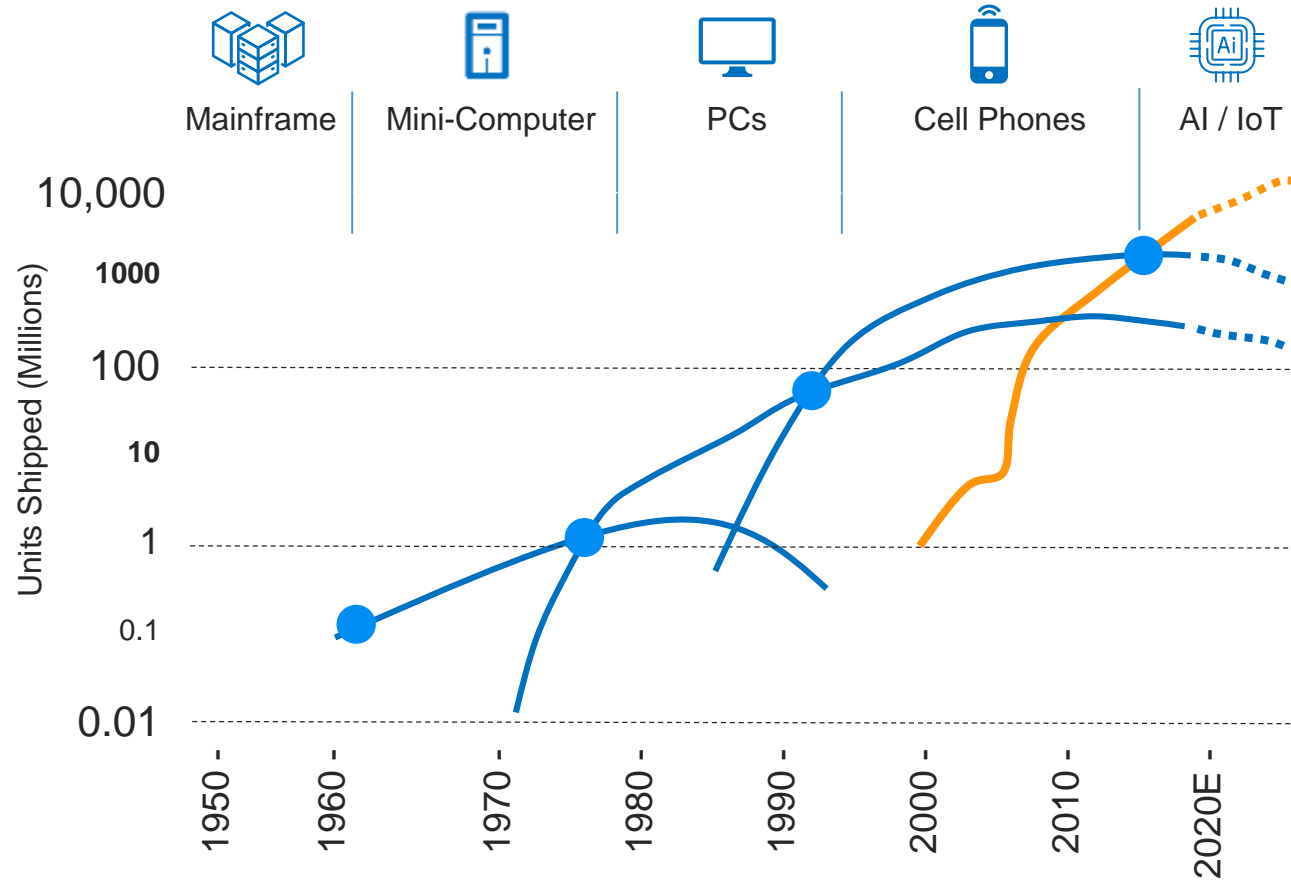
June 2019 | Session #AMF-EDG-T3667

NXP

SECURE CONNECTIONS
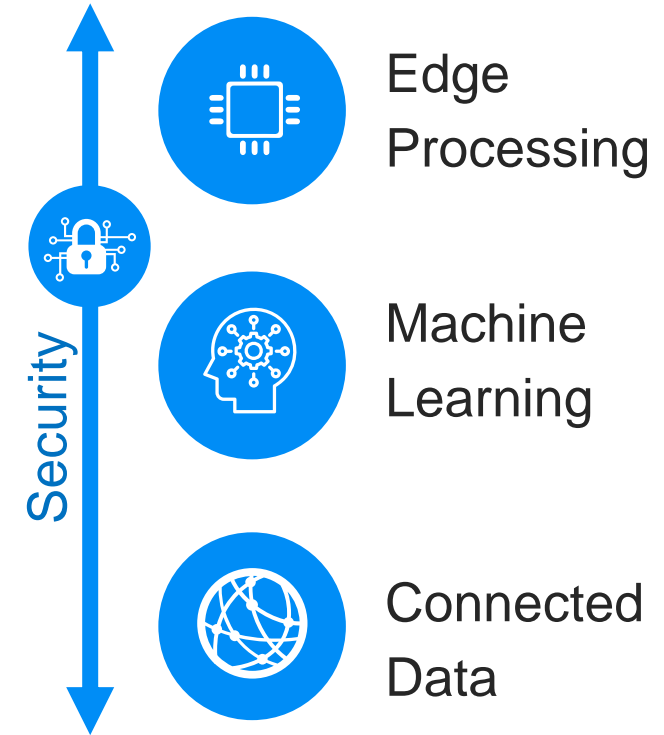FOR A SMARTER WORLD

Agenda

- Security at the Edge

- NXP Secure Gateways With the LS1012A

- Software Solutions for Secure Cloud Connected Devices

- Turnkey Systems

The AI / IoT Era is Driving Growth for Connected Devices

Mainframe | Mini-Computer | PCs | Cell Phones | AI / IoT

Units Shipped (Millions)

10,000
1000
100
10
1
0.1
0.01

1950 - 1960 - 1970 - 1980 - 1990 - 2000 - 2010 - 2020E -

"The 4th Tectonic Shift in Computing"

Security
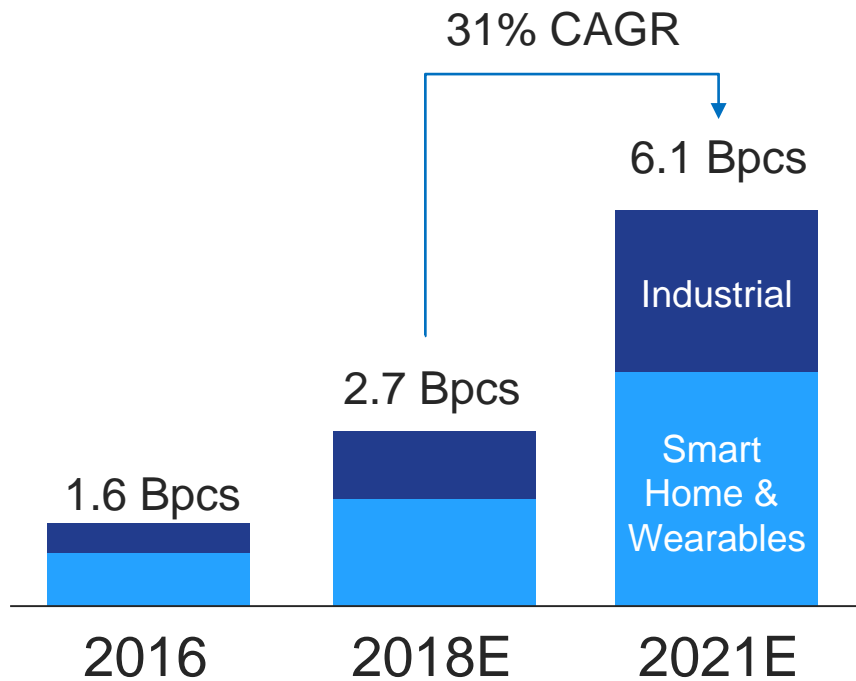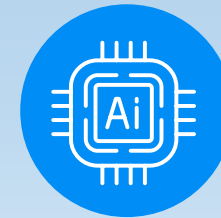
Edge Processing

Machine Learning

Connected Data

1. Jeffreies

AI / IoT Disruption is the New Growth Engine[1,2,3,4]…

… Changing the Rules of Engagement with the Market

IoT Endpoints, Worldwide

31% CAGR

6.1 Bpcs

Industrial

2.7 Bpcs

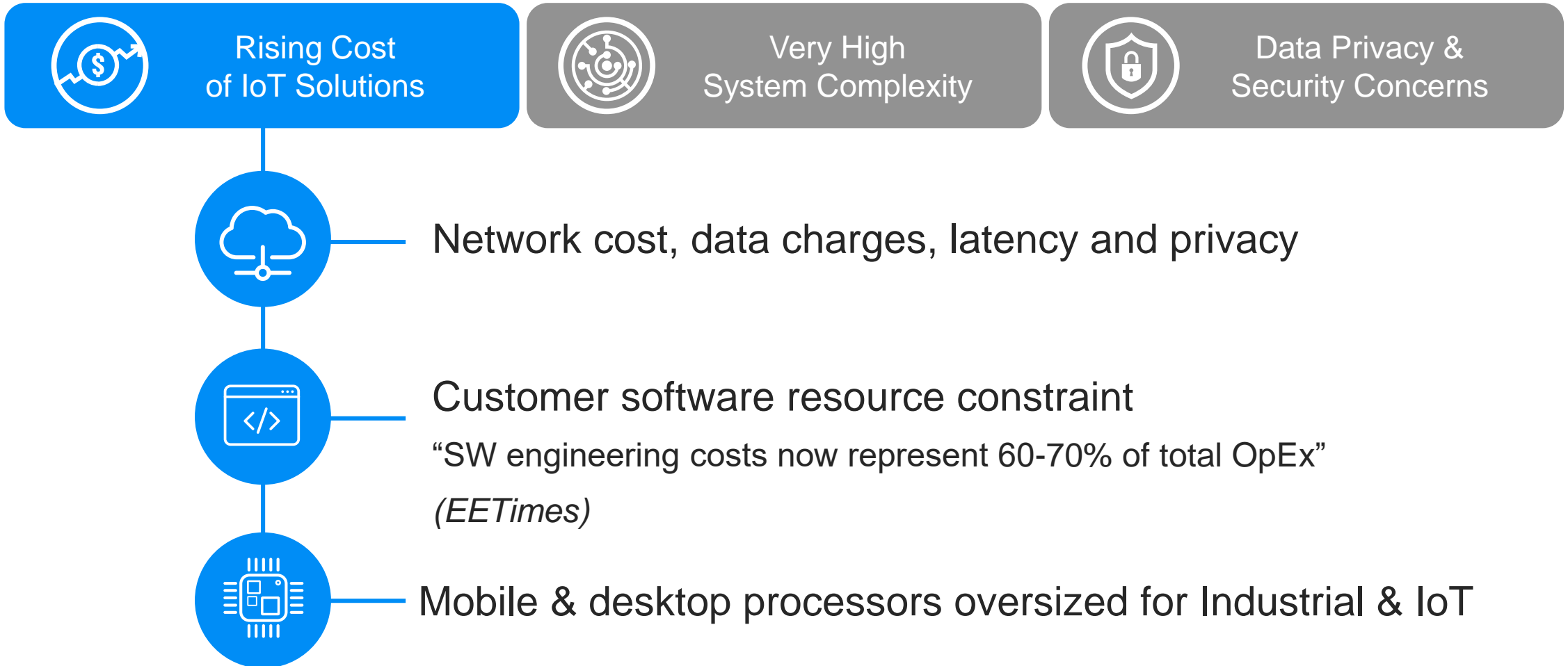Smart Home & Wearables

1.6 Bpcs

2016   2018E   2021E

Less diverse end devices
Concentrated customer base
Defined ecosystem

Very diverse end devices
Fragmented customer base
Wide range of applications & ecosystem

NXP

Customer Pain Point: Rising Cost of IoT Solutions[1]

Rising Cost of IoT Solutions	Very High System Complexity	Data Privacy & Security Concerns

Network cost, data charges, latency and privacy

Customer software resource constraint

"SW engineering costs now represent 60-70% of total OpEx"

(EETimes)

Mobile & desktop processors oversized for Industrial & IoT

1.   Source: AspenCore Study 2017

Customer Pain Points: System Complexity & Security[1]

Very High System Complexity

"70% of embedded developers decide on the processor's ecosystem first"

2017 Embedded Developers Survey

- Diverse cloud & AI solutions

  aws Bai百度 Google IBM Microsoft Alibaba

- Fragmented connectivity protocols

  Bluetooth WiFi ZigBee THREAD GROUP ZWAVE sigfox LoRa

- Operating system & software portability

  Amazon freeRTOS Zephyr ANDROID Linux Green Hills SOFTWARE

Data Privacy & Security Concerns

Data Breach Examples

Retail / Healthcare
Jun 2018, Feb 2015, May 2014, Sep 2014 , Dec 2013

Social Media / Search
June 2016, Aug 2013

Banking / Credit Rating
July 2017, June 2014

Airlines
Sep 2018

Government regulations

US-CERT GDPR The General Data Protection Regulation China Cyberspace Adm.

NXP Solutions for Edge Computing

IoT Nodes

NXP SW Platform
- Middleware
- RTOS
- Thin Edge Agent

NXP Kinetis, LPC, i.MX-RT Family

Edge Gateways

HOME GATEWAY

ETHERNET SWITCH

WIRELESS ROUTER

INDUSTRIAL CONTROLLER

Customer Solution
- App
- App
- App

NXP SW Platform
- Middleware
- RTOS, Linux, Android
- Edge Agent

NXP Layerscape, i.MX Family

Cloud Infrastructure

Data Analytics

Machine Learning

Multiple Cloud Frameworks

Application Management

Secure Device Management

NXP EdgeScale Suite
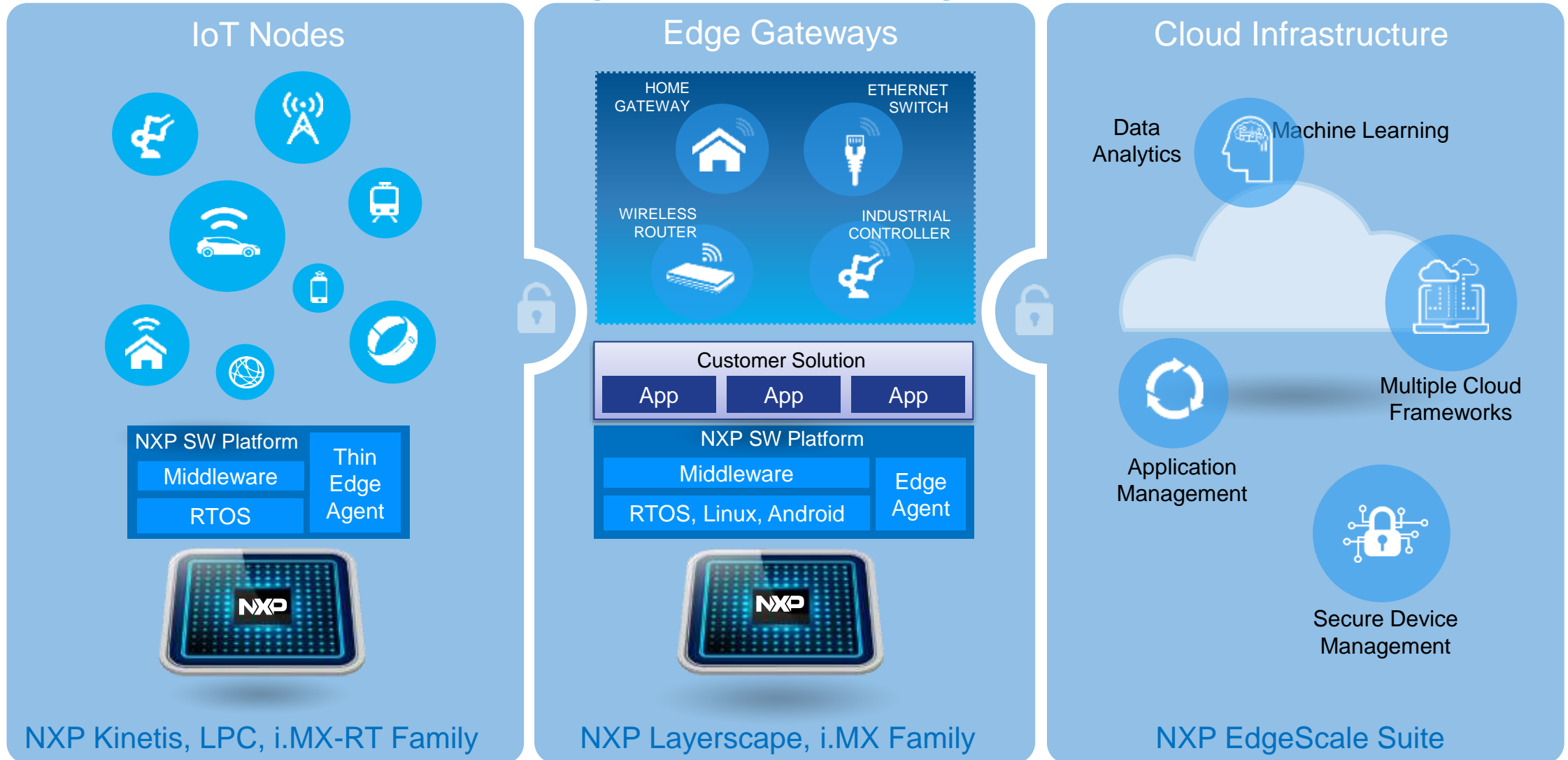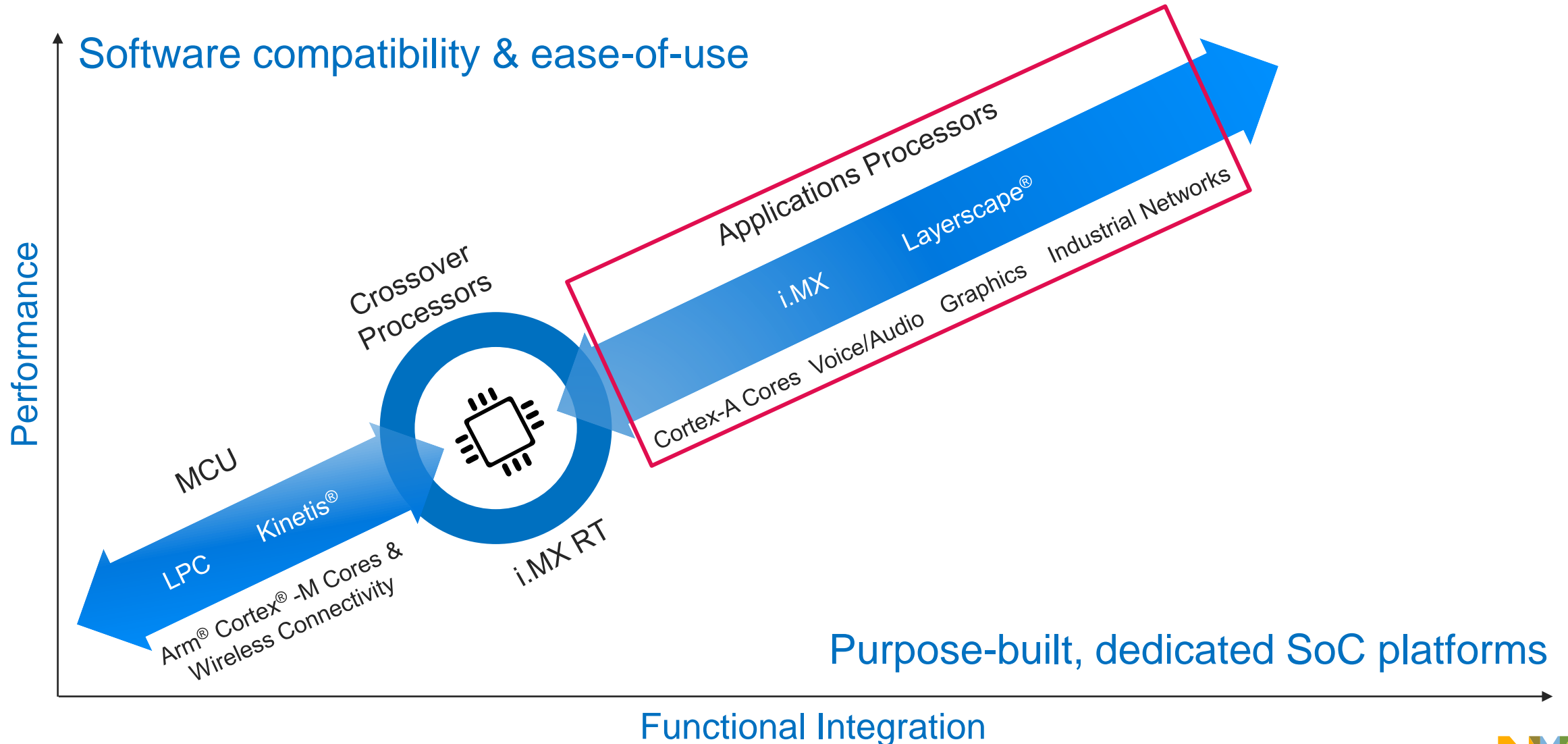
LS1012A: First 64-bit Single Core ARM Cortex A53 Processor

World's Lowest Power 64-bit ARM Based Processor

Core complex
- 1x 64-bit Cortex-A53 with Neon SIMD engine
- Speed up to 800 MHz
- Parity-protected 32 KB L1 instruction and 32 KB L1 data cache
- 256 KB L2 cache with ECC protection

Basic peripheral and Interconnect
- 1x USB 3.0/2.0 controller with integrated PHY
- 1x USB 2.0 controller with ULPI
- 2x eSDHC controllers supporting SD 3.0, eMMC 4.4 and eMMC 4.5 modes
- Five SAI supporting I2S

Networking elements
- 2x quad-speed Ethernet MACs supporting 2.5G, 1G, 100M, 10M
- Supports RGMII, SGMII 1G, SGMII 2.5G
- Up to 2 x SGMII supporting 1 or 2.5 Gbps
- 1x PCI Express Gen 2 controller
- 1x SATA Gen 3.0 controller

Accelerators and Memory Control
- 1x 16-bit DDR3L Controller up to 1.0 GT/s
- Security Engine (SEC)
- QorIQ Trust architecture: Secure boot, ARM Trust zone and security monitor

Qualification
- Commercial and extended temperature

Target Applications
- Trust-enabled IoT Gateways
- Consumer NAS
- Mobile NAS
- Ethernet drives for data center storage
- Entry-level broadband Ethernet gateways
- Building and Factory automation

Development platforms:
- LS1012A-RDB
- FRWY-LS1012A
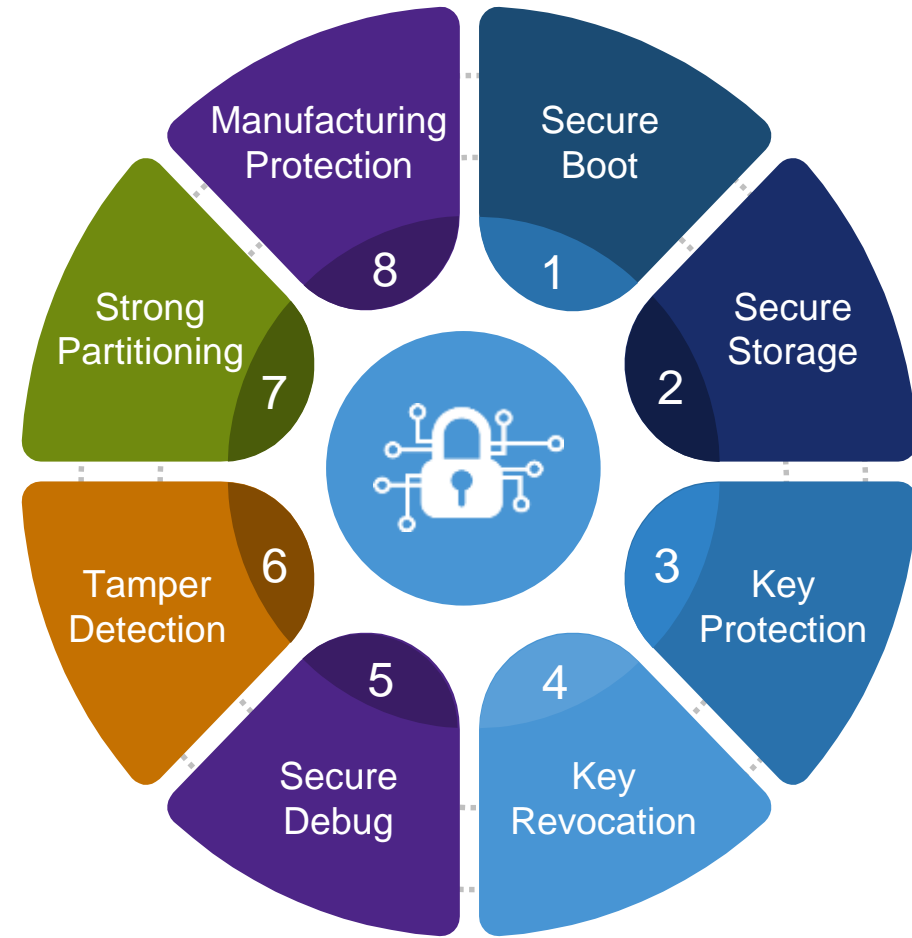
Trust Architecture Provides a Trusted Platform

Hardware based security features to ease the development of trustworthy systems

SoC

Battery Back-up

Tamper Detect(s)

- Security Fuses
- PreBoot Loader
- Security Monitor
- Internal BootROM
- Power Mgmt
- SD/MMC
- SPI DUART I²C
- IFC USB SATA
- Clocks/Reset
- CCSR GPIO

General-Purpose CPU Core — HV MMU

General-Purpose CPU Core — HV MMU

DDR Controller

Coherent Interconnect

IOMMU   IOMMU

Security sub-system
- SEC Engine
- Crypto, RNG
- Secure Keys
- UID, Runtime Integrity Check

Data-path sub-system
- Mgmt Control
- QMan
- BMan
- AIOP
- FMAN WRIOP
- Eth, PCI

Secure Debug Controller

Real Time Debug
- Watchpoint
- Perf Monitor
- CoreNet Trace
- Aurora

All QorIQ SoCs support Trust Architecture

1. Secure Boot
2. Secure Storage
3. Key Protection
4. Key Revocation
5. Secure Debug
6. Tamper Detection
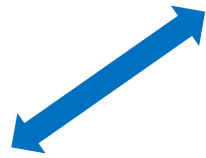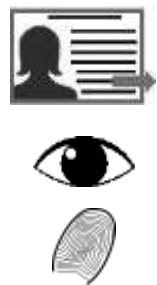7. Strong Partitioning
8. Manufacturing Protection

Edgescale for Remote Cloud Connected Devices

Management and Security Challenges

Traditional PC, Mobile devices

- Multiple authentication mechanisms
- Cloud based security and application management

Edge computing devices

- Traditionally embedded devices
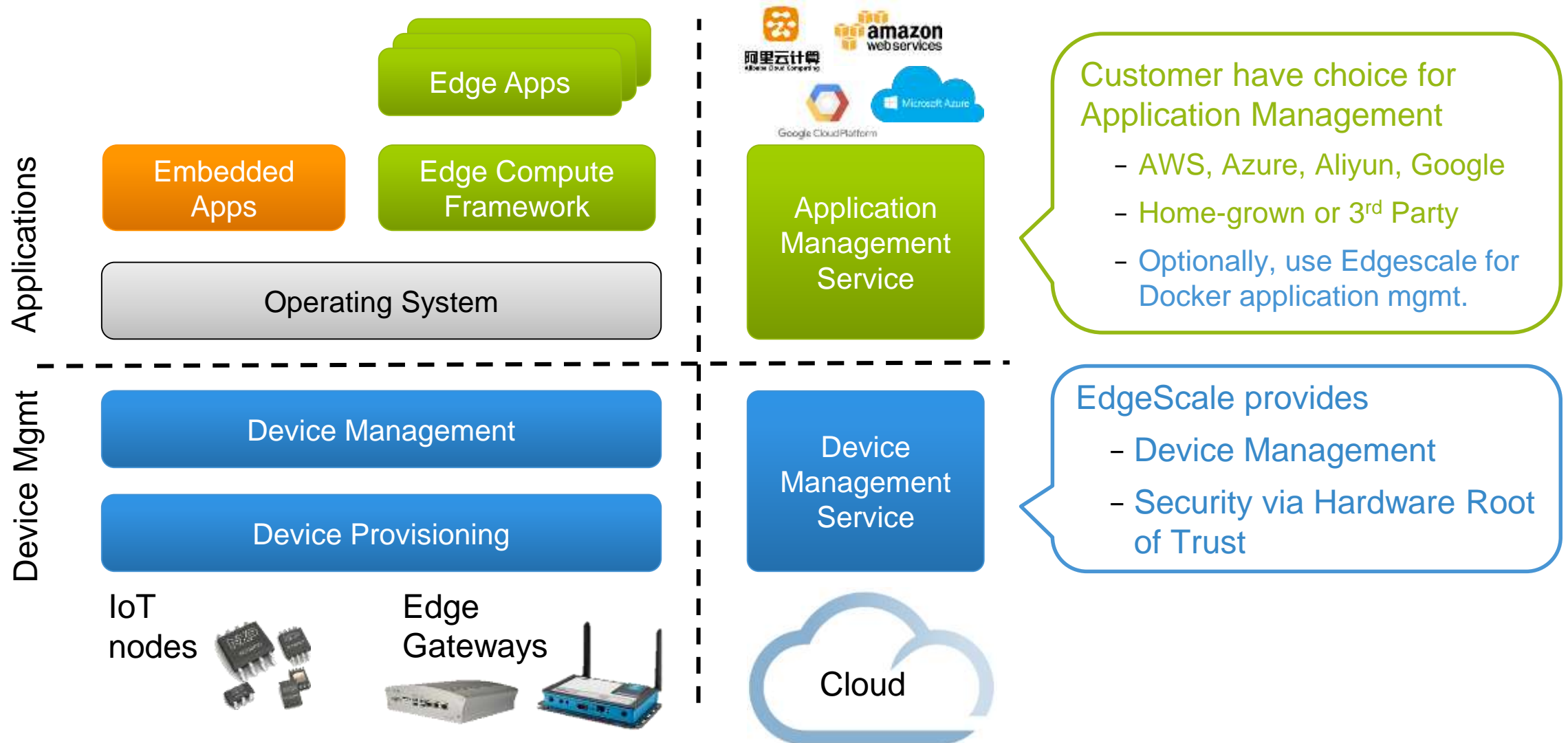- No physical access/lack display
- Many (10s, 100s, 1000s) per user

EdgeScale

Solution: Cloud based Management & Security for Edge

- Manage devices, apps remotely
- Secure provisioning, upgrades

EdgeScale for Device Management

Applications

- Edge Apps
- Embedded Apps
- Edge Compute Framework
- Operating System

Device Mgmt

- Device Management
- Device Provisioning

IoT nodes

Edge Gateways

Application Management Service

Device Management Service

Cloud

Customer have choice for Application Management
- AWS, Azure, Aliyun, Google
- Home-grown or 3rd Party
- Optionally, use Edgescale for Docker application mgmt.

EdgeScale provides
- Device Management
- Security via Hardware Root of Trust

Edge Computing Frameworks

EdgeScale enables multiple Compute frameworks to run at the same time, and can dynamically provision them.

IBM Cloud   AliYun   Google Cloud   Microsoft Azure   Private Cloud   Amazon AWS

IBM Apps	AliYun Apps	Google Apps	Azure Apps	Customer Apps	AWS Apps	AWS Apps
IBM IoT SDK	Alibaba IoT SDK	Google IoT SDK	Azure IoT SDK	Private IoT SDK	AWS IoT SDK	Greengrass
Docker	Docker	Docker	Docker	Docker	Docker	

Docker Engine	Protocol Adaptor	Data processing	Data filter

Cgroup, Namespace	File-System	Network Stack	Ethernet, Crypto	Trust Zone	Secure Device Mgmt

Kernel

Bluetooth   NFC   THREAD   WiFi   ZigBee®   . . .   EtherCAT.   PROFINET

Common Software Platform

EdgeScale – Flexible Architecture

Multiple compute and usage models

Customer Private Cloud

AliYun

Amazon AWS

Google Cloud

Microsoft Azure

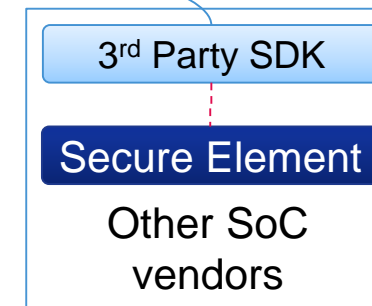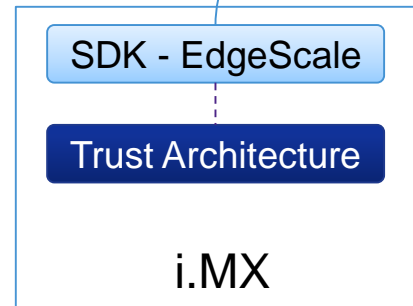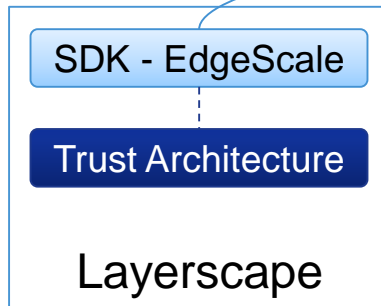Edge Compute Frameworks

Dashboard, CLI

RESTful APIs

Common device management service

EdgeScale Device Management Services

Hardware Root of Trust

Multiple platforms supported

SDK - EdgeScale

Trust Architecture

Layerscape

SDK - EdgeScale

Trust Architecture

i.MX

3rd Party SDK

Secure Element

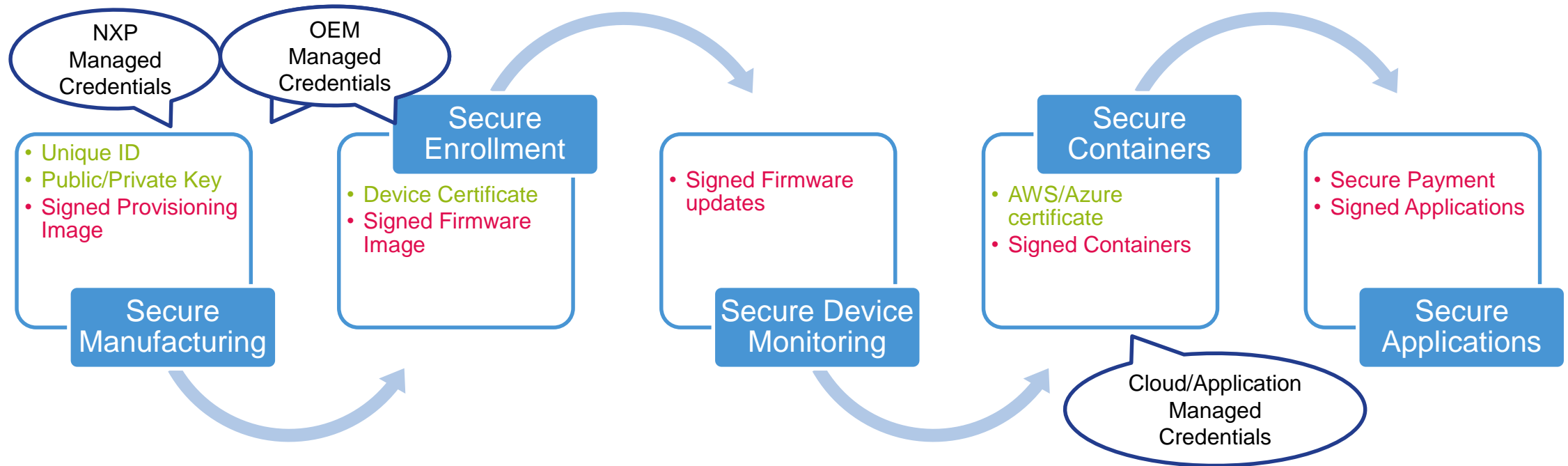Other SoC vendors

NXP

Managing Edge nodes vs. IoT end-nodes

- IoT end-nodes have device manageability capabilities: provisioning, OTA firmware updates, monitoring

- IoT end-nodes can be managed directly from the cloud, or via an Edge Gateway

- IoT end-nodes may support targeted applications managed directly from the cloud – e.g. AWS GG

NXP EdgeScale

IoT End-node
- Custom AWS Apps
- AWS GG
- Custom middleware
- RTOS
- EdgeScale 'Thin' Client
- Secure Firmware

Edge Gateway
- Azure Apps
- AWS Apps
- Azure
- AWS GG
- Pvt Apps
- Private
- User-space, Docker, Kubernetes
- Linux
- EdgeScale Client
- Secure Firmware

Application Management Services
- AWS Cloud
  - AWS Apps
- Azure Cloud
  - Azure Apps

Application Management Services
- Pvt Apps
- Container Deployment Service
- Remote Build Services

Device Management Services
- Secure Device Monitor Service
- Secure Firmware Service
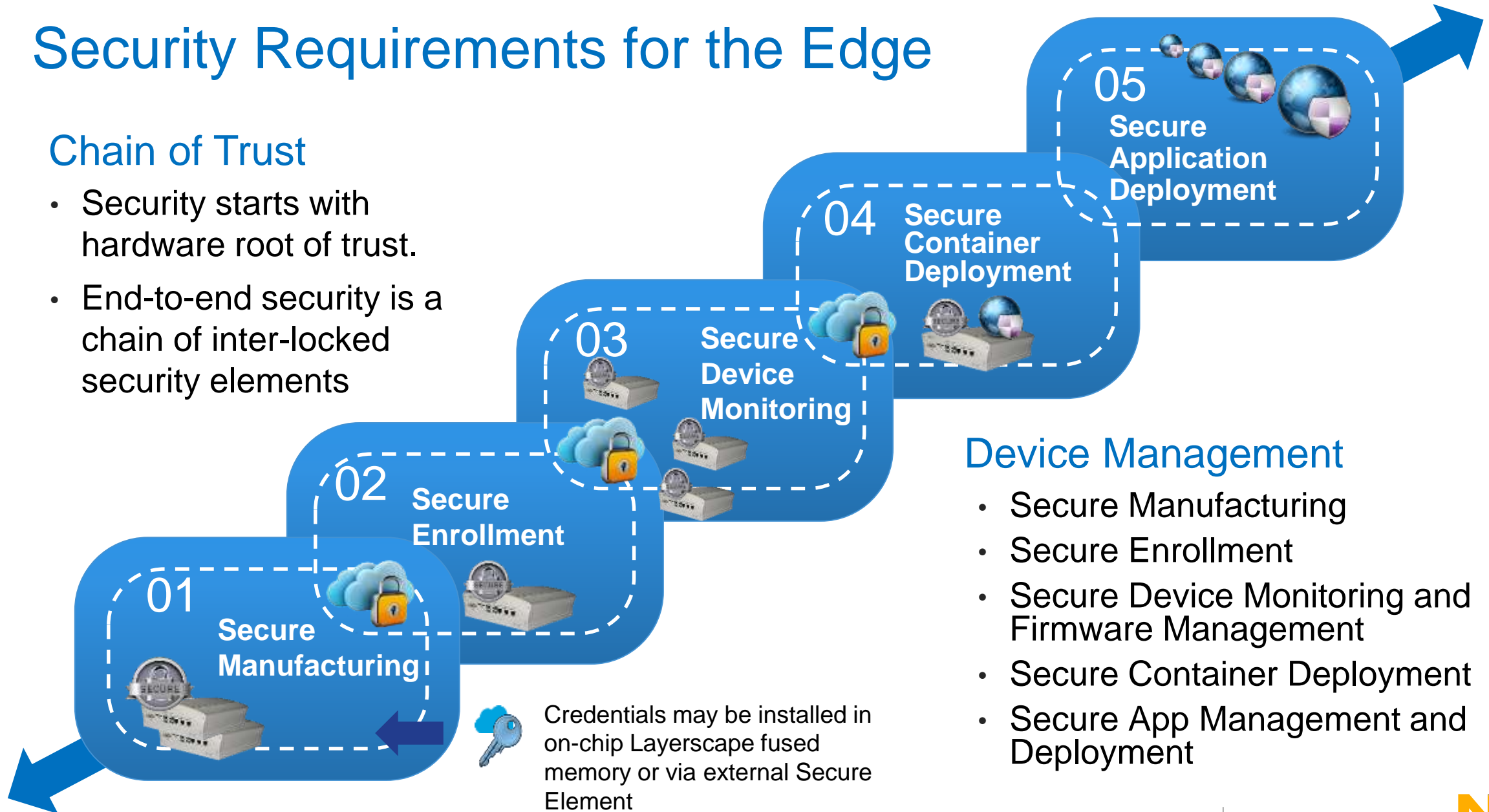- Secure Enrollment Service

Chain of Trust

- Hardware forms the Root of trust
- Multiple layers of tamper-detection - each level validates the next
- Multiple levels of secrets – can revoke at any layer
- Mutual authentication between device and cloud using Asymmetric cryptography

Security Requirements for the Edge

Chain of Trust

- Security starts with hardware root of trust.

- End-to-end security is a chain of inter-locked security elements

05 Secure Application Deployment

04 Secure Container Deployment

03 Secure Device Monitoring

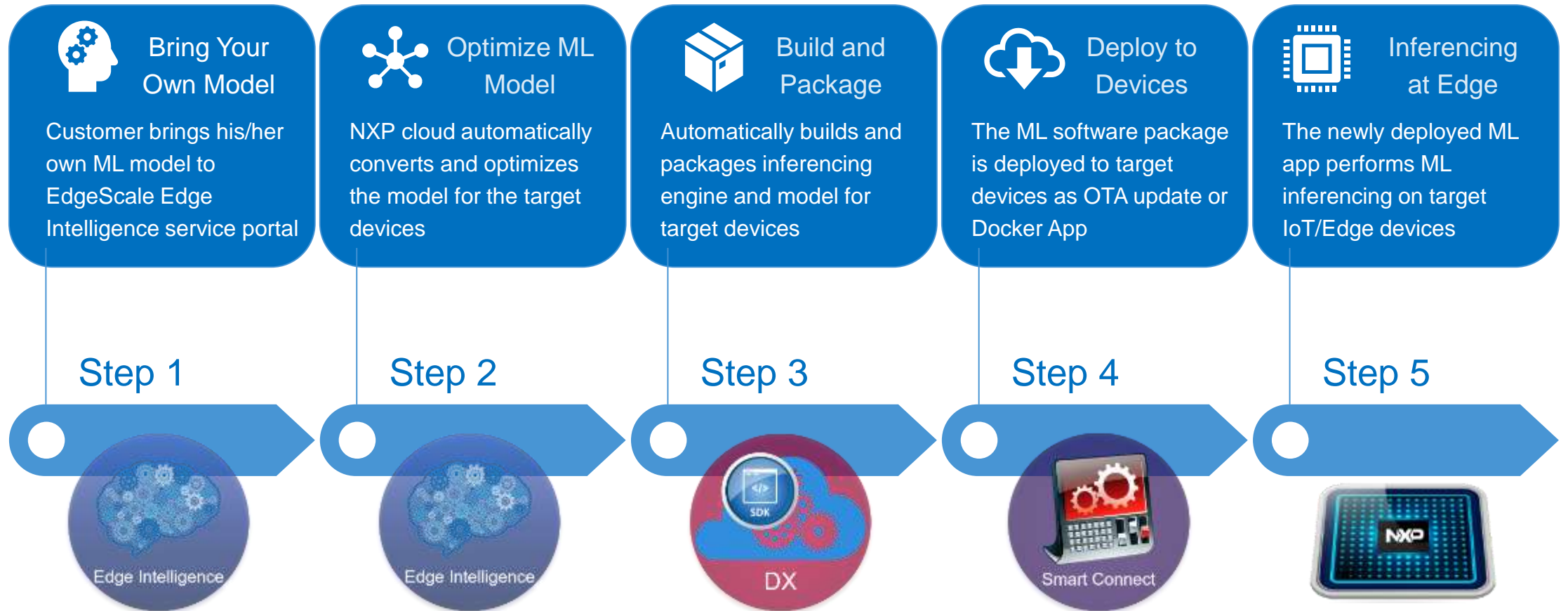**02 Secure Enrollment**

01 Secure Manufacturing

Credentials may be installed in on-chip Layerscape fused memory or via external Secure Element

Device Management

- Secure Manufacturing
- Secure Enrollment
- Secure Device Monitoring and Firmware Management
- Secure Container Deployment
- Secure App Management and Deployment

AI/ML DX Example – Bring Your Own Model

Step 1	Step 2	Step 3	Step 4	Step 5
Bring Your Own Model Customer brings his/her own ML model to EdgeScale Edge Intelligence service portal	**Optimize ML Model** NXP cloud automatically converts and optimizes the model for the target devices	**Build and Package** Automatically builds and packages inferencing engine and model for target devices	**Deploy to Devices** The ML software package is deployed to target devices as OTA update or Docker App	**Inferencing at Edge** The newly deployed ML app performs ML inferencing on target IoT/Edge devices

Uniquely Positioned for Industrial & IoT Edge Compute

Broadest Portfolio
MCU / Crossover / Application Processors
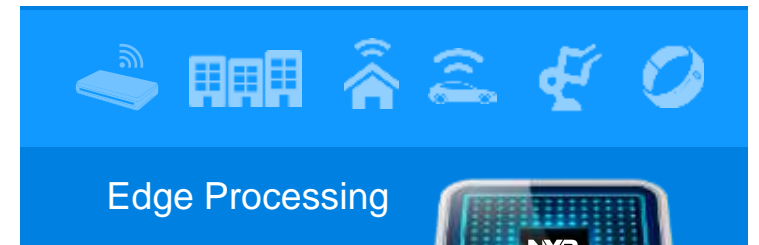
Complete Solutions
SDK / HW / SW & Ecosystem

Seamless Cloud Connectivity
& Lifecycle Management

High-precision
Analog & Audio/Video/Display

Security & Privacy
Embedded & Systems Level

Systems Level Integration

Comprehensive Software Environment

Edge Compute Ecosystem

Edge Processing

Turnkey Solutions for Cloud Connectivity

Scalys TrustBox based on NXP LS1012A
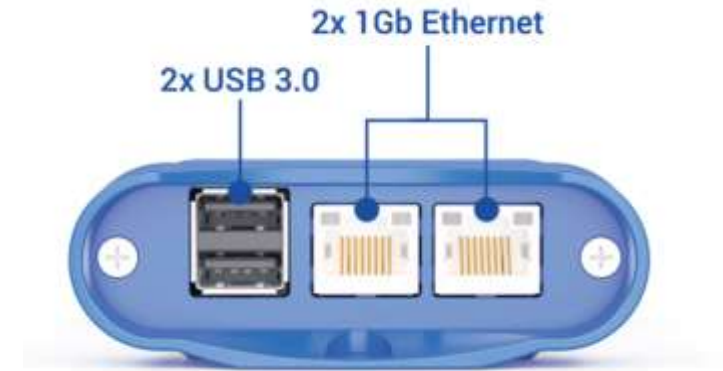
Scalys TrustBox

- Based on NXP LS1012A

- CES2019 Best Of Innovation: Cybersecurity and Personal Privacy

- Available world wide in Arrow store end of June 2019

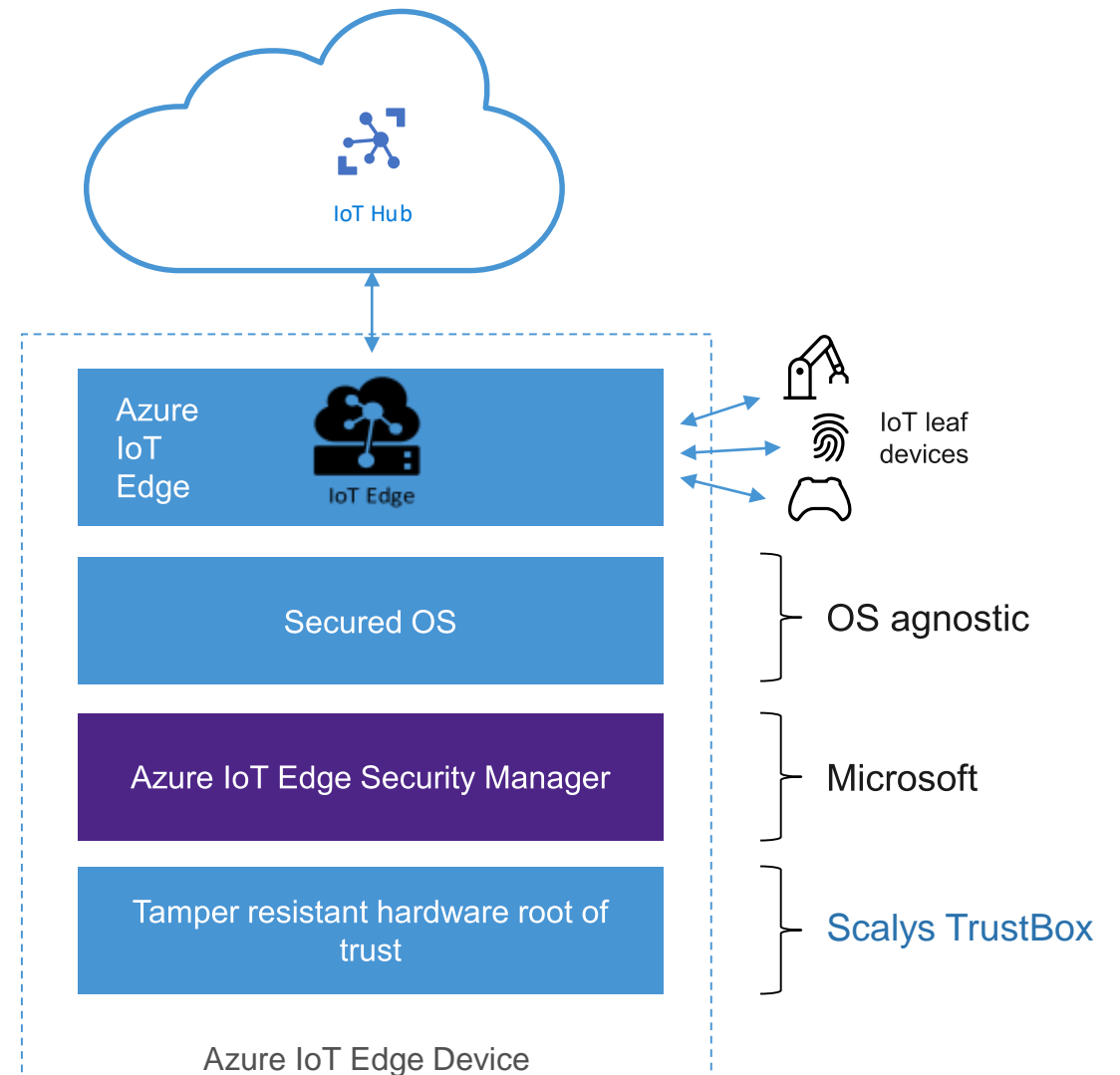Dimensions:
135mm x 85mm x 30mm

Scalys TrustBox Features
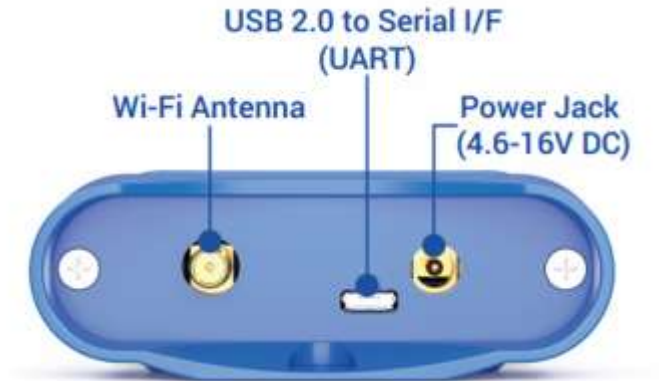
Microsoft Azure IoT Edge

Cooperation with Microsoft to support "Open Enclave" on TrustBox

Open Enclave adds additional security software to Azure IoT Edge

Azure IoT Edge and Open Enclave pre-installed

Summary

- The IoT and AI Era will drive the next wave of growth for embedded devices
- NXP offers solutions for securely connecting edge devices to the cloud
- The LS1012 is an excellent choice for secure IoT gateways

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD