NXP SECURE PLATFORM: SECURING THE PRODUCT LIFE CYCLE

RAVI MALHOTRA
PRODUCT MARKETING

AMF-DES-T2683 | JUNE 2017

SECURE CONNECTIONS FOR A SMARTER WORLD

AGENDA

- What can be hacked ?
  - Hint: anything & everything …
  - and IoT makes it scarier
- How do you protect your system ?
  - Hint: leave no stone unturned ..
- Layerscape Secure Platform
  - Securing the entire product life-cycle

1990s – 2016

An Era of Security/Trust Breaches

As computer systems have grown more capable, complex...so have the **attacks**!

9 CERTIFICATES

Stolen across 7 different domains

COMODO Certification Authority Hack

4 MILLION

Employee federal records hacked

Department of Defense Hack

77 MILLION

Compromised accounts

Playstation Network Outage

45.7 MILLION

Credit cards stolen

TJX Hack – Albert Gonzalez

900,000

Deutsche Telekom customers affected in Germany

2,400

TalkTalk routers affected in the UK

Operation Shady Rat

85%

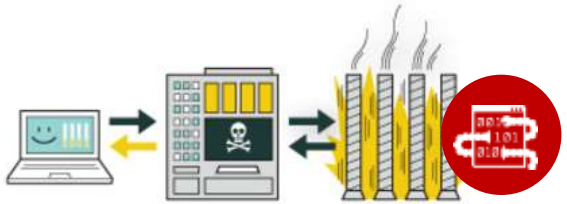
Share of infected computers – Iran, Indonesia, India

Stuxnet Worm (Targeting Industrial Systems)

71+ ORGANIZATIONS HIT

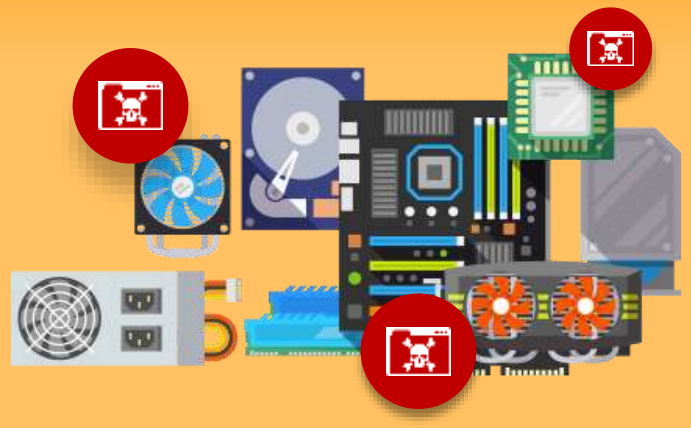
Defense contractors, United Nations, The Olympic Committee

Mirai Botnet Malware

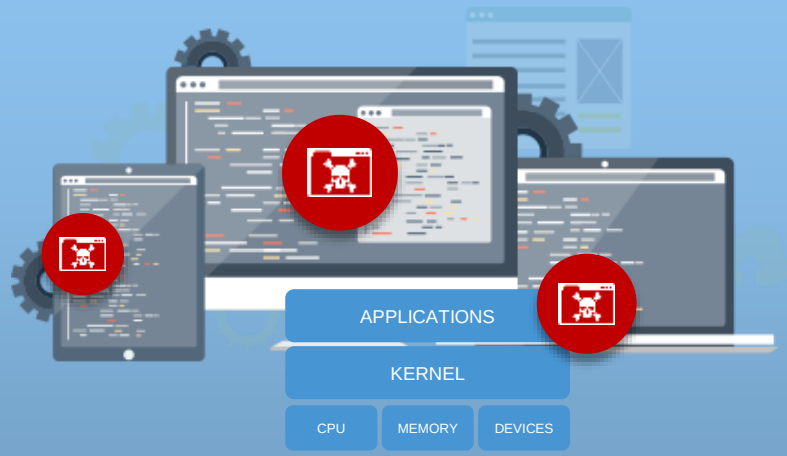


Each Breach Exposes a Different Aspect of **SYSTEM VUNERABILITY**

Design
Hardware | IO | Storage



Manufacturing
Key Generation | Provisioning | Updates



Software
Operating System | Applications | Permissions

Connectivity
Remote Access | Communications

Security needs to be **PERVASIVE**

EXPLOSION OF NODES

Not just a few PCs, but potentially hundreds of embedded devices in a home

Most devices have limited processing capabilities

Every device has multiple vulnerabilities that can compromise entire network

Security needs to cover **ENTIRE SYSTEM**

TRANSCENDS FROM DIGITAL TO PHYSICAL REALM

Not just credit card or personal information stolen

Can be life-threatening

Severe impairment of basic functions

Security must be **MEASURABLE**

PROLIFERATION OF STANDARDS, VENDORS

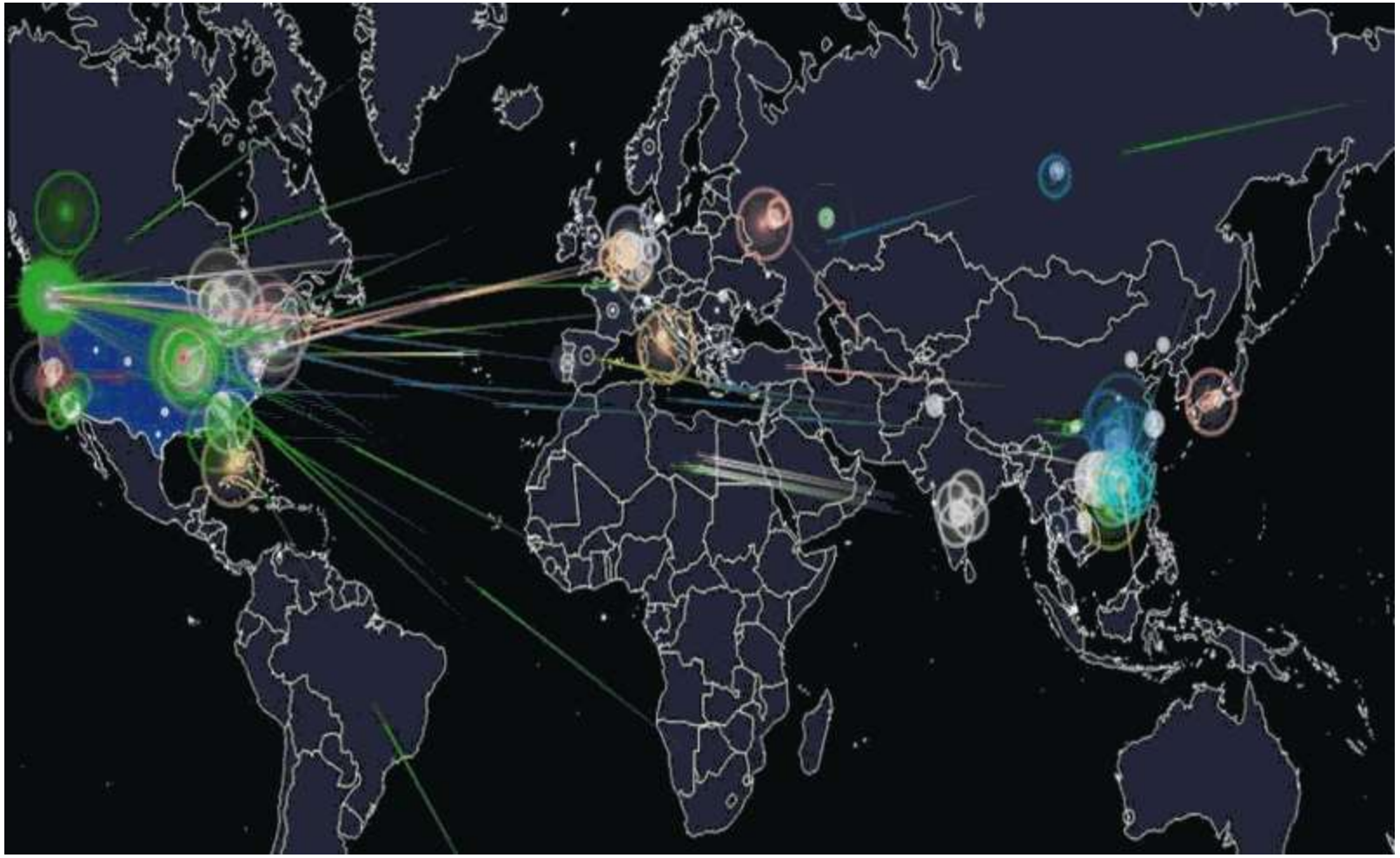
Everyone defaults to lowest common denominator – turn security off to get it to work

No checks in place to ensure everyone follows basic processes

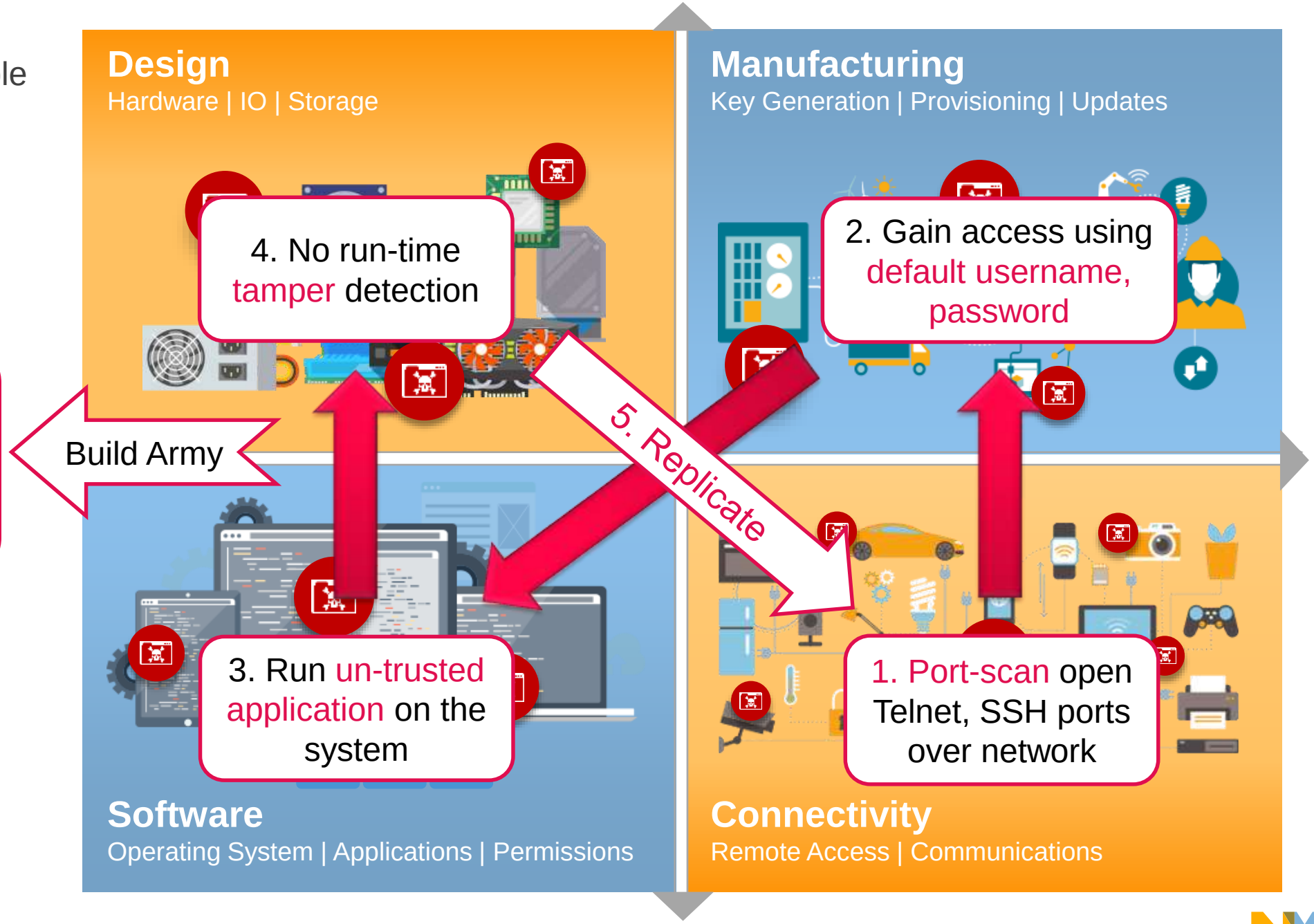
IoT Gone Wrong in Everyday Life

IoT manufacturers
focused on
FUNCTIONALITY,
EASE-OF-USE
OVER
SECURITY

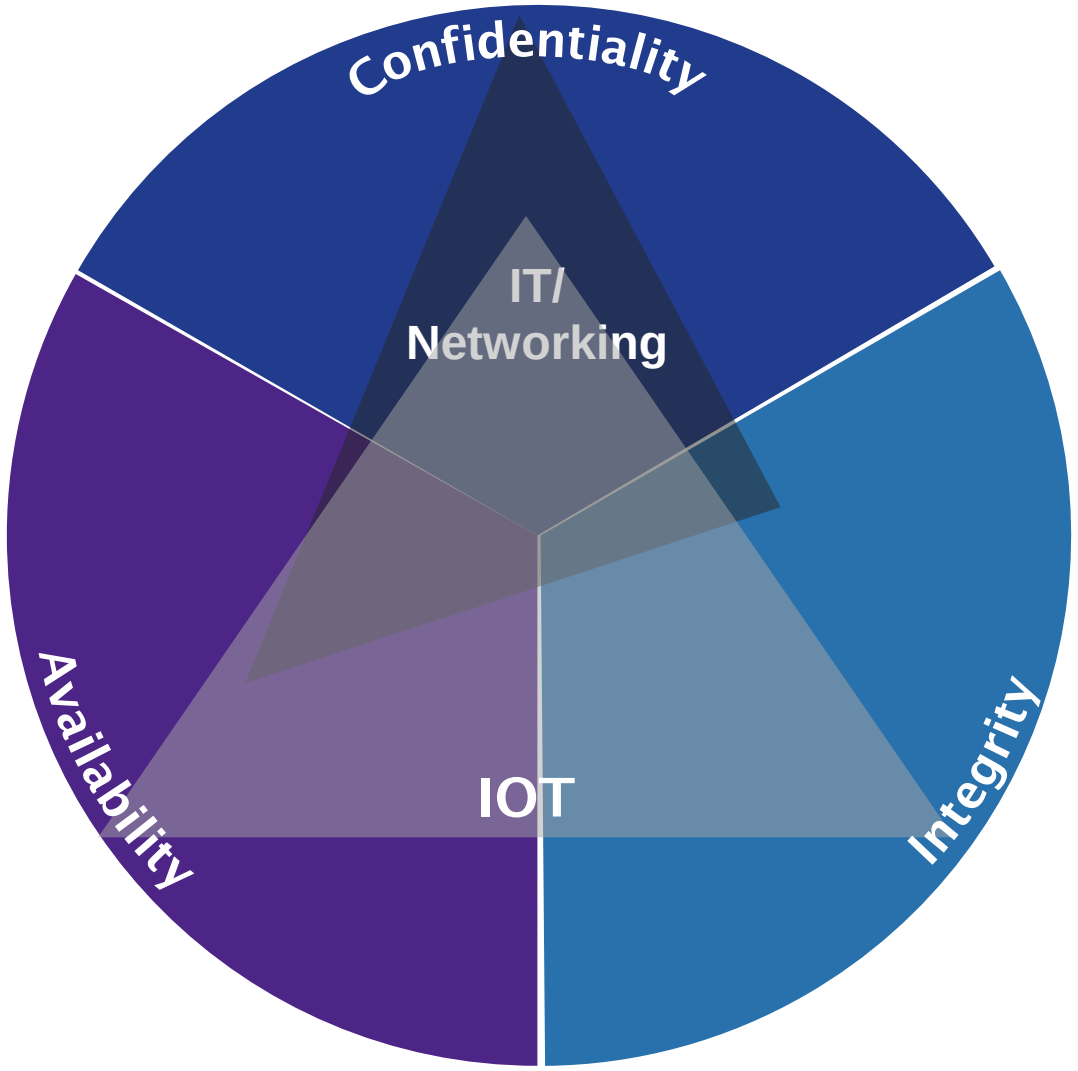
Mirai Botnet



How **MIRAI** was able to exploit these vulnerabilities.



IOT Shifts the Emphasis between key security elements



Classical IT and network security

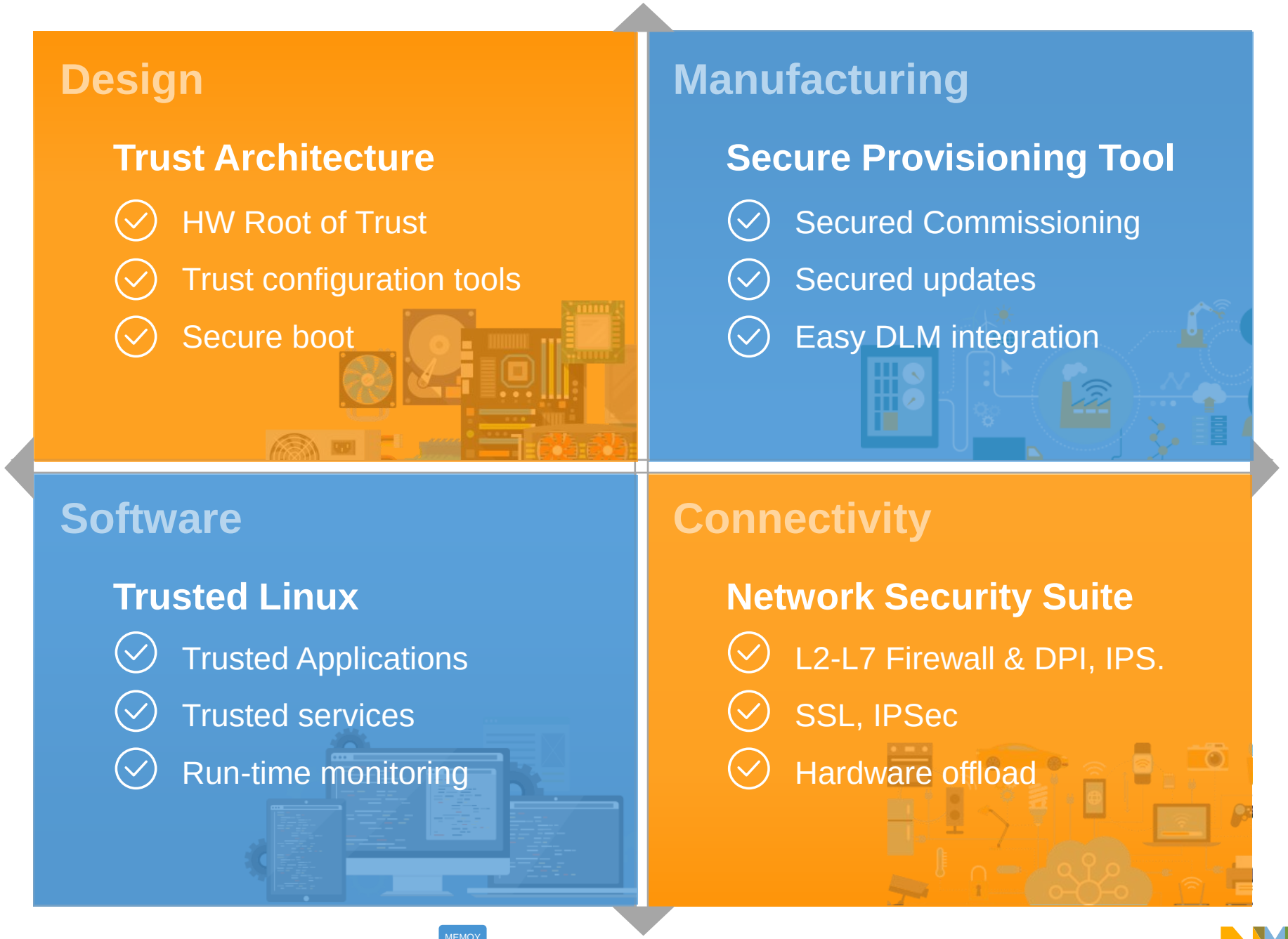
- Mostly about confidentiality
  - Firewalls to keep bad guys out
  - VPNs to let good guys in
  - Some data-at-rest protection
- Less focus on availability
  - DDOS and AV protection
- Little/no effort on business integrity
- Focus on acceleration vs. trust.

IOT

- Mostly about availability and integrity
  - Keep the Thing behaving correctly
  - Keep the Thing online
- Little data to exfiltrate
- Focus on trust rather than acceleration.

SECURE PLATFORM

Covers every aspect of the Product Life-cycle



MEMOY

Our Competition has nothing like it…

Aspect	Intel, x86	Other ARM vendors (MRVL, BRCM, CAVM)	NXP Secure Platform
Secure Design	• Secure Boot • Weak partitioning	• Secure Boot	• Secure Boot • Anti-tamper • Secure Debug • Strong partitioning • Key protection • Run-time Integrity Check
Secure Manufacturing	• Requires external TPM chipset	• Requires external TPM chipset	• In-built key generation, storage. • Secure Provisioning Tool
Secure Software	• Trusted Execution mode (TXT, SGX)	• Trusted Execution mode (ARM TrustZone)	• Trusted Execution mode (ARM TrustZone) • Full TEE Software Suite • Trusted Linux
Secure Connectivity	• Software based Firewall, Security stacks • SW crypto, plain-text keys	• Software based Firewall, Security stacks • SW or HW crypto, plain-text keys	• Complete Network Security Suite with Hardware offload • Mature HW Crypto, black keys

Raspberry Pi 3 vs. LS1012A – a case study in security

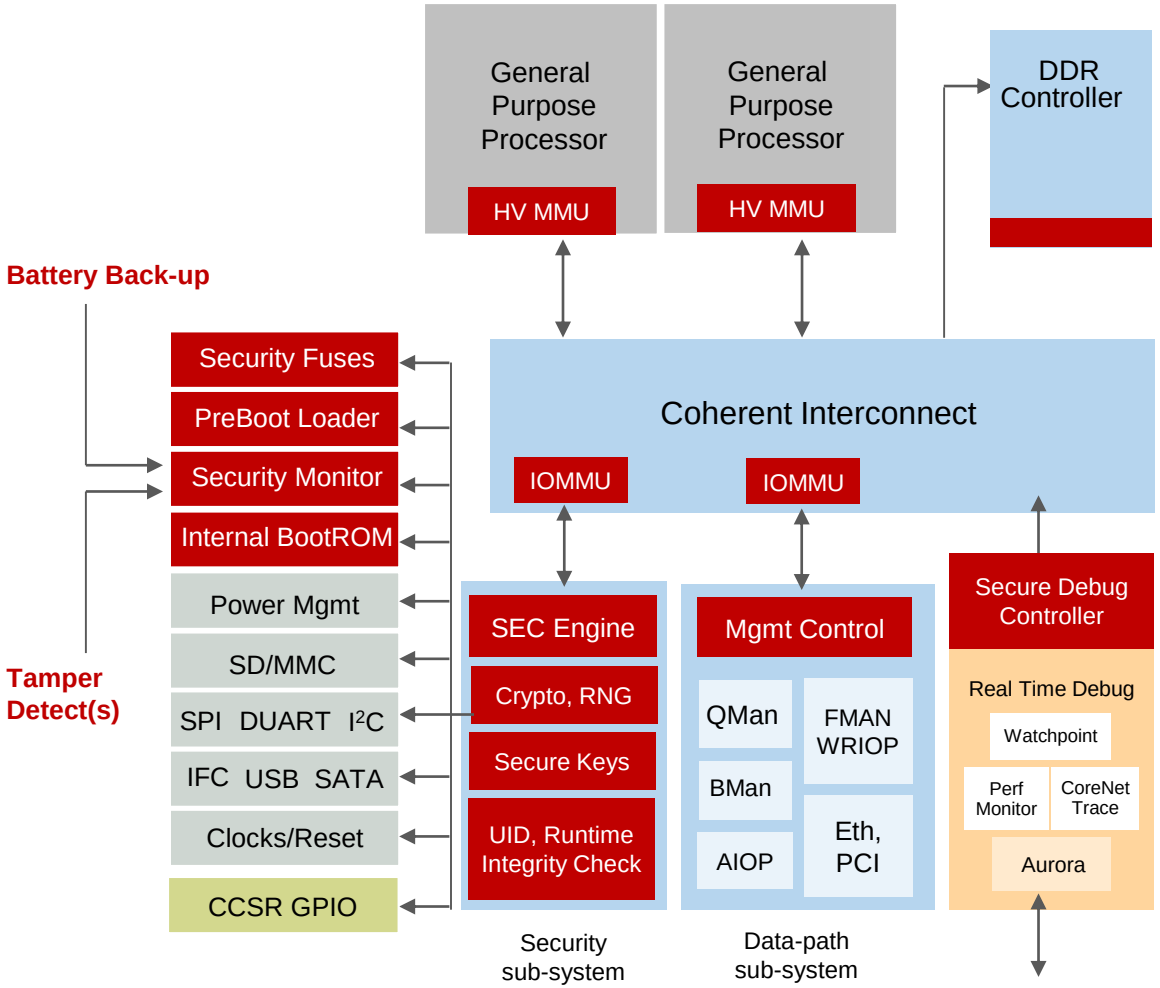
Aspect	Raspberry Pi 3 (BRCM)	LS1012A (NXP)
Secure Design	• Internal secure bootROM missing. • Keys stored in plain-text. • 3rd Party secure boot-loader on SD-card suspect to tampering.	• Internal secure bootROM part of every silicon. • Keys stored encrypted, only accessible via SEC engine. • Secure bootloader provided, verified by HW root of trust. • Run-time tamper detection.
Secure Manufacturing	• No support	• Secure provisioning tool, cloud integration.
Secure Software	• Poor Trust-Zone implementation • Easy to tamper SD-card config	• Robust Trust-Zone backed by Trust Architecture. • Trusted Linux with run-time enforcement.
Secure Connectivity	• No Crypto acceleration • Weak RNG	• Core-based and offload crypto acceleration. • NIST-certified RNG
Tools, Documentation	• None, very poor.	• Trust Configuration Tools • Trust Architecture User Guide

Linaro Conclusion: ..not securable TrustZone implementation, but great for education, learning...

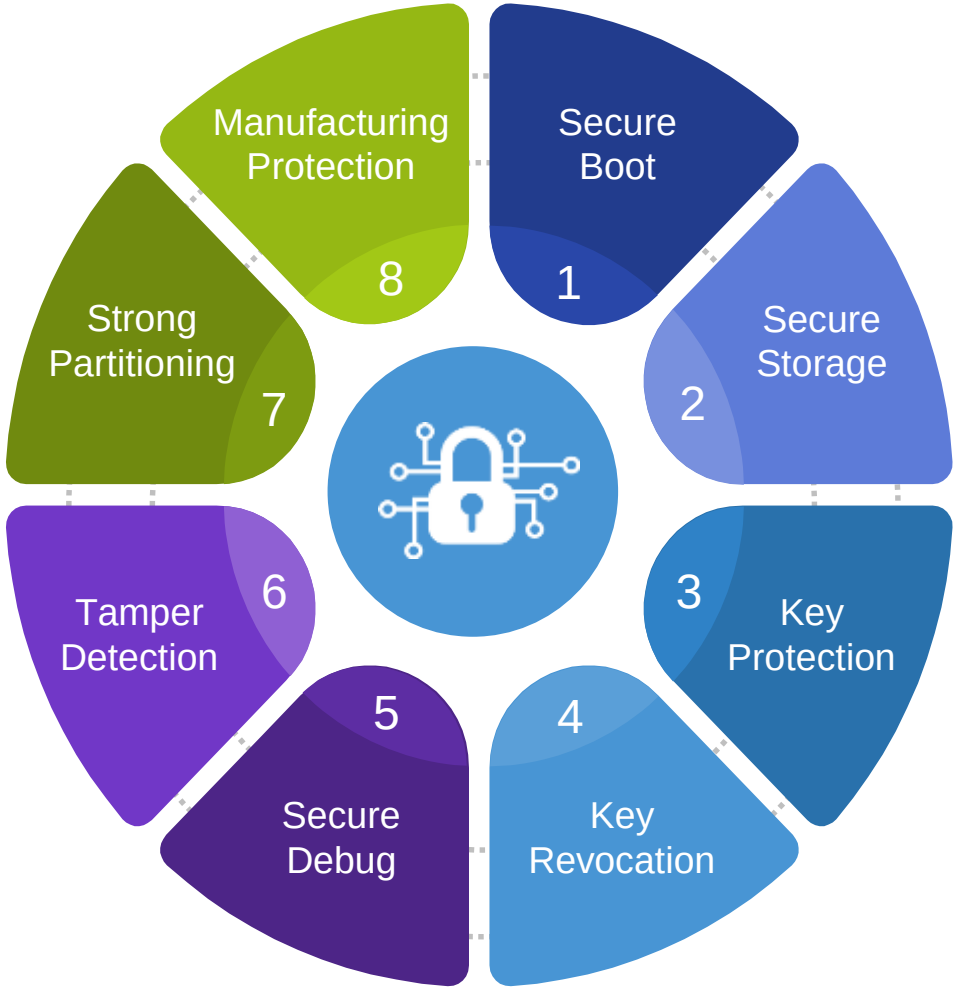
Source: https://www.slideshare.net/linaroorg/las16111-easing-access-to-arm-trustzone-optee-and-raspberry-pi-3

Trust Architecture

Hardware based security features to ease the development of trustworthy systems



All QorIQ SoCs support Trust Architecture



Trust Tools & Secure Boot

Secure chain of trust

- Internal Secure Boot
- External Secure Boot – Uboot, UEFI
- Partitioning of run-time environment

Rich set of configuration tools

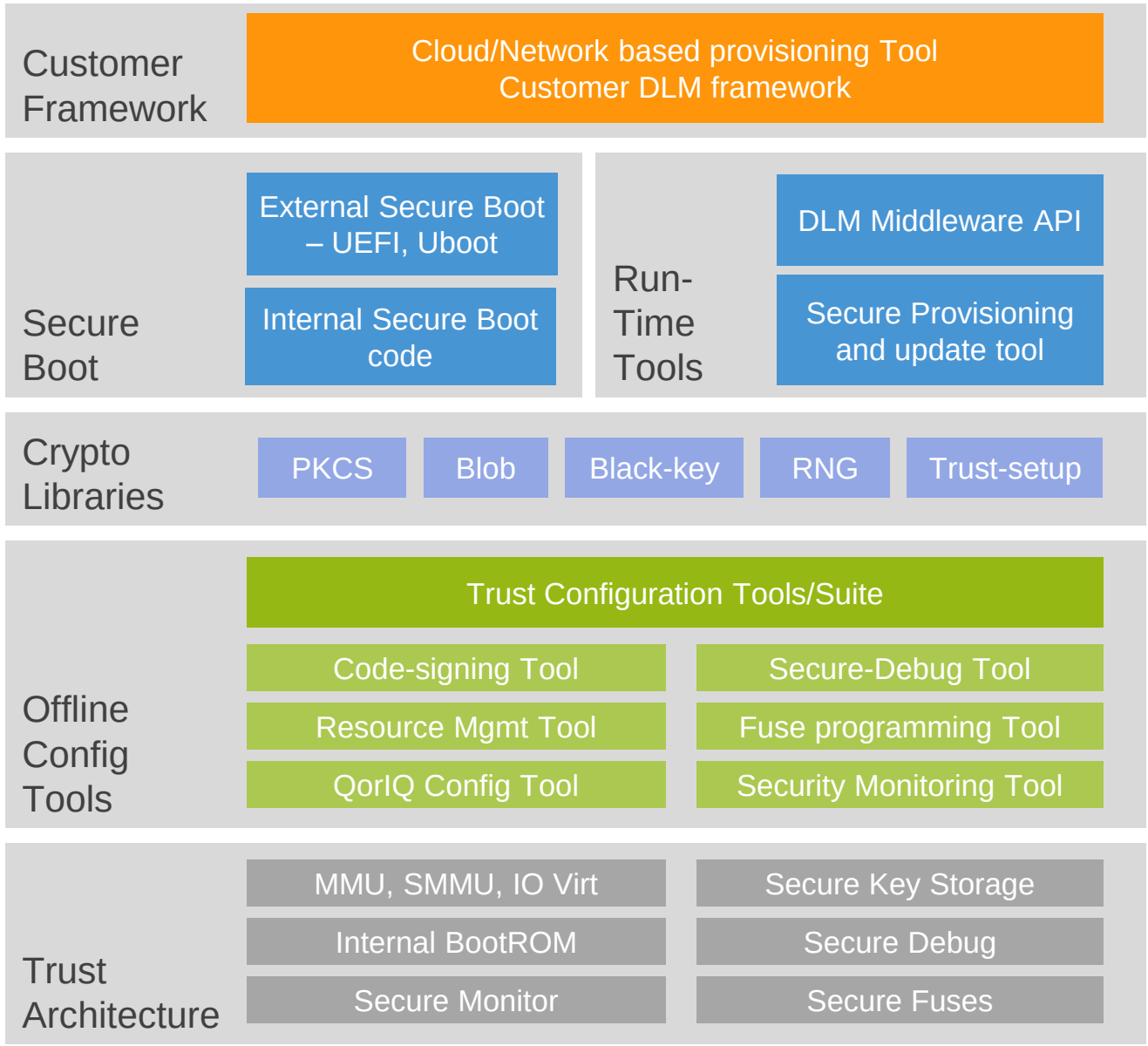
- Programming keys, policies
- Code-signing
- Low-level programmability with ease of use

DLM Middleware

- Hooks up with Cloud provisioning agents
- Flexible API to hook into customer DLM

Leverage Trust Architecture

- HW Root of trust
- Secure provisioning and monitoring



Trusted Linux

Enhances standard off-the-shelf Linux

Ensures Trusted Applications

- Isolation of resources
- Verified installation
- Controlled launch

Ensures Trusted Data

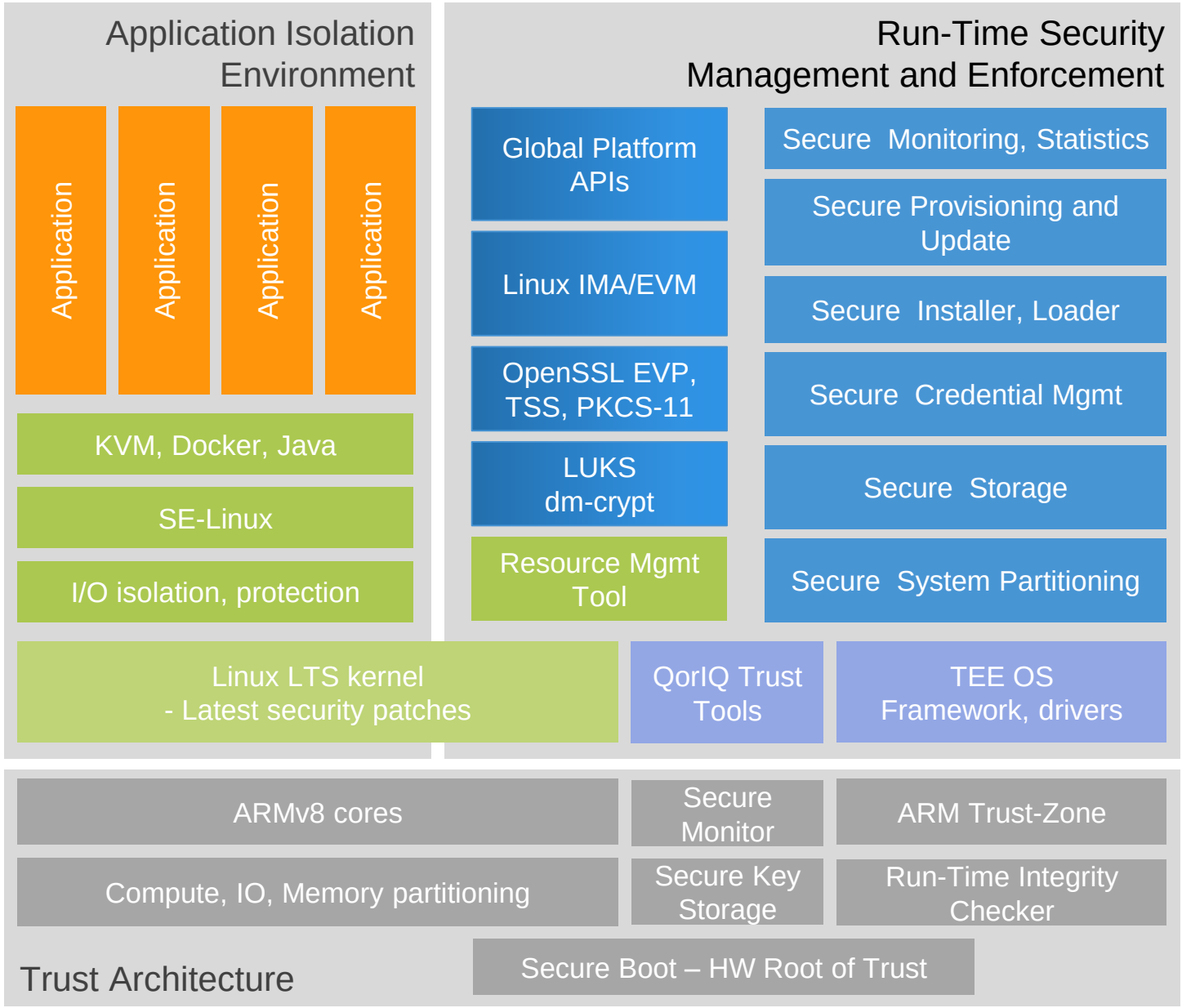
- Isolated, encrypted user data.
- Isolated, secure credentials
- Controlled access

Ensures Trusted System

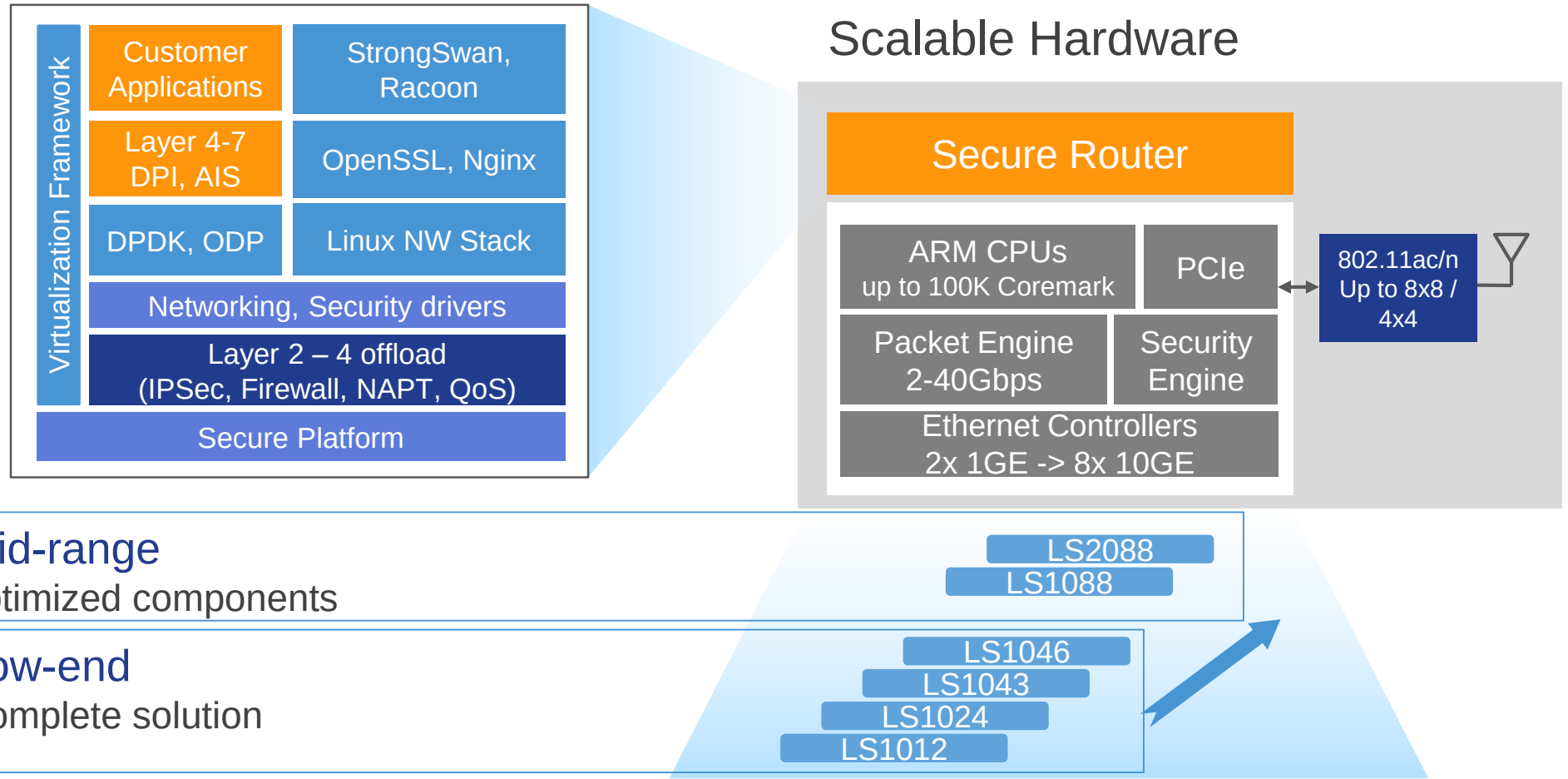
- Run-time monitoring and statistics
- Firmware update, commissioning

HW Assist by Trust Arch

- HW root of trust during boot process
- Run-time integrity check for kernel, TEE
- Secure monitor, tamper detect



Network Security Suite



Secure Provisioning Tool

Supports different provisioning modes

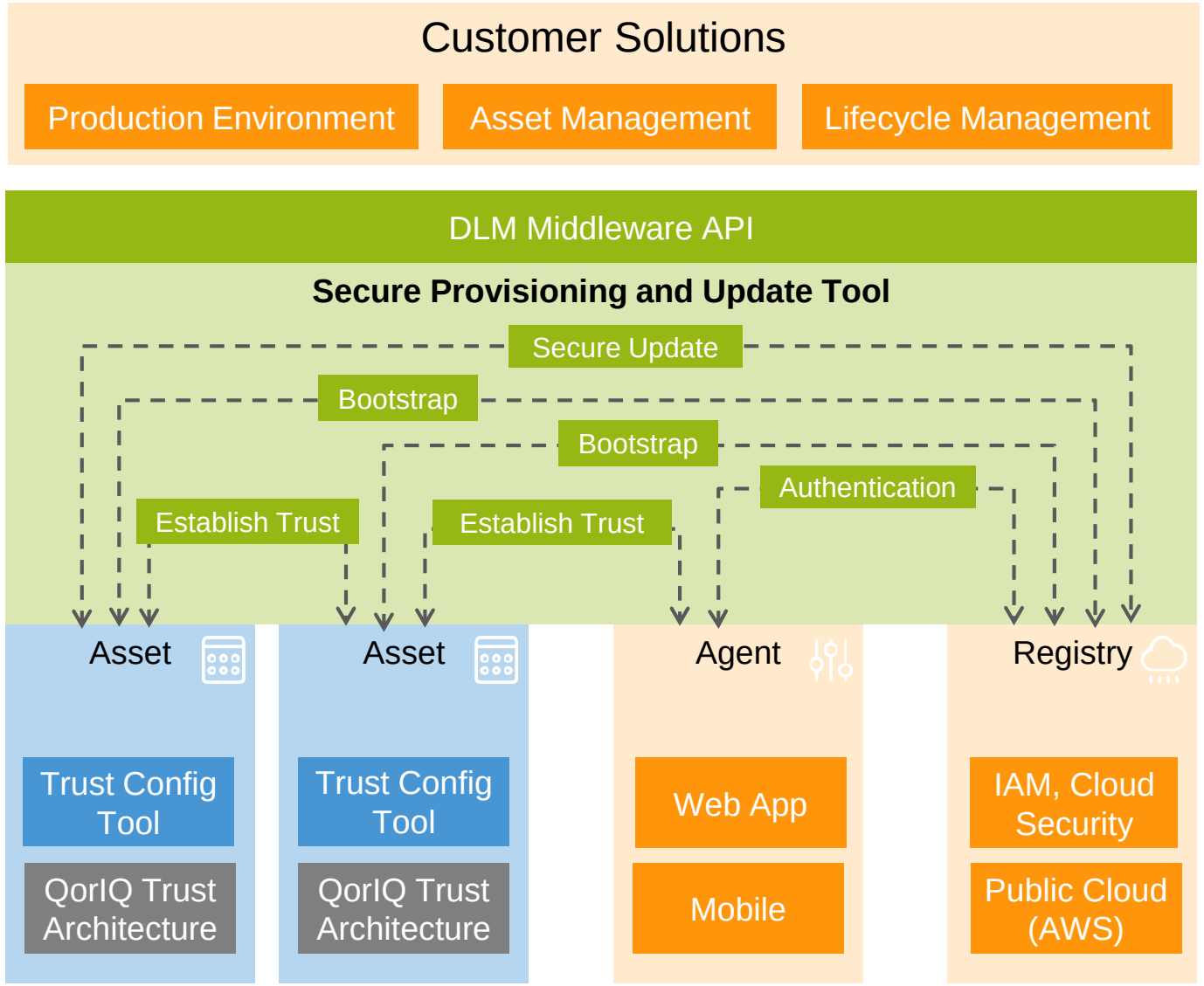
- Manual/Agent-based
- Automatic/network-based
- Subscription/cloud-based

Ready for both

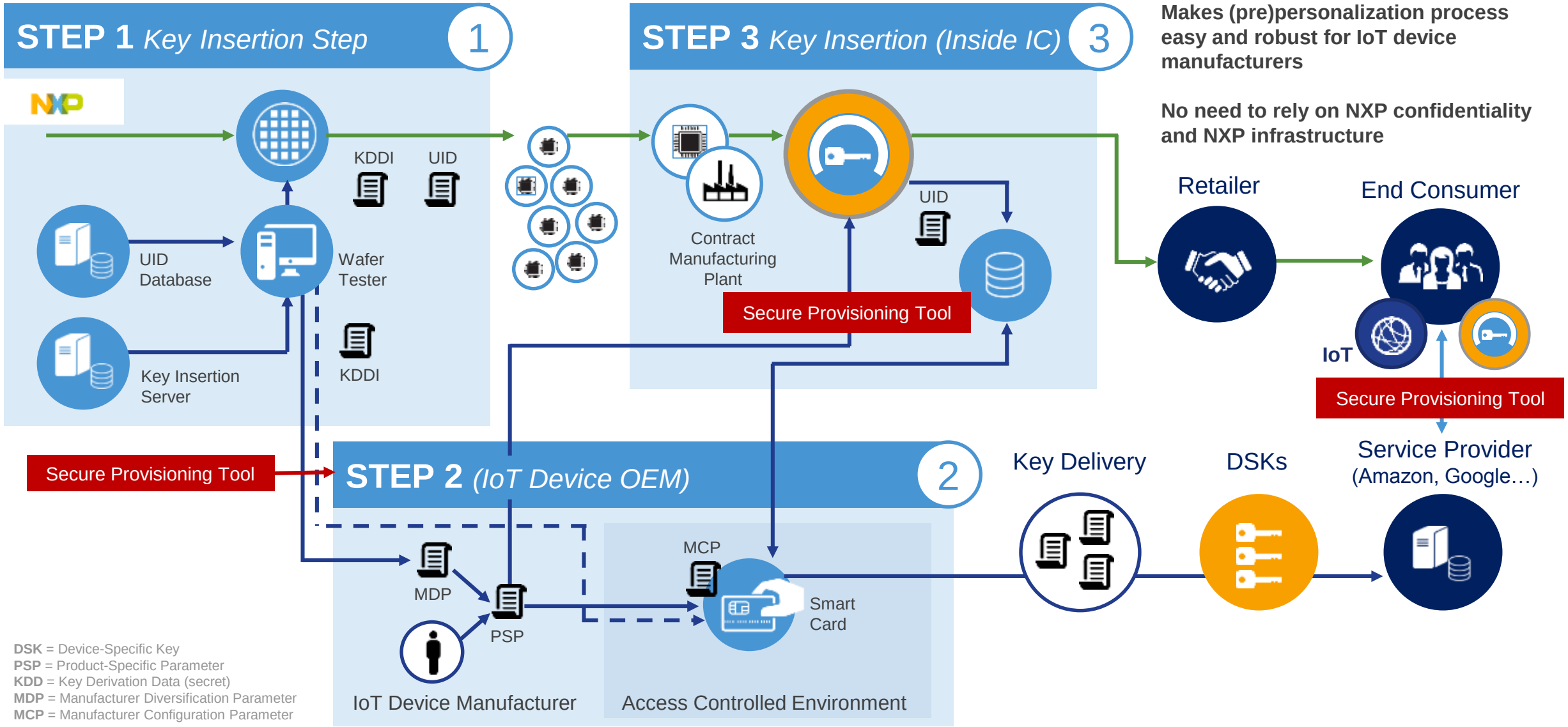
- Industrial deployments
- Consumer deployments

DLM Middleware

- Hooks up with Cloud provisioning agents.
- Flexible API to hook into customer DLM



A Secure Distributed Manufacturing Model



DSK = Device-Specific Key
PSP = Product-Specific Parameter
KDD = Key Derivation Data (secret)
MDP = Manufacturer Diversification Parameter
MCP = Manufacturer Configuration Parameter

Security Consulting and Services

Our Security Technology

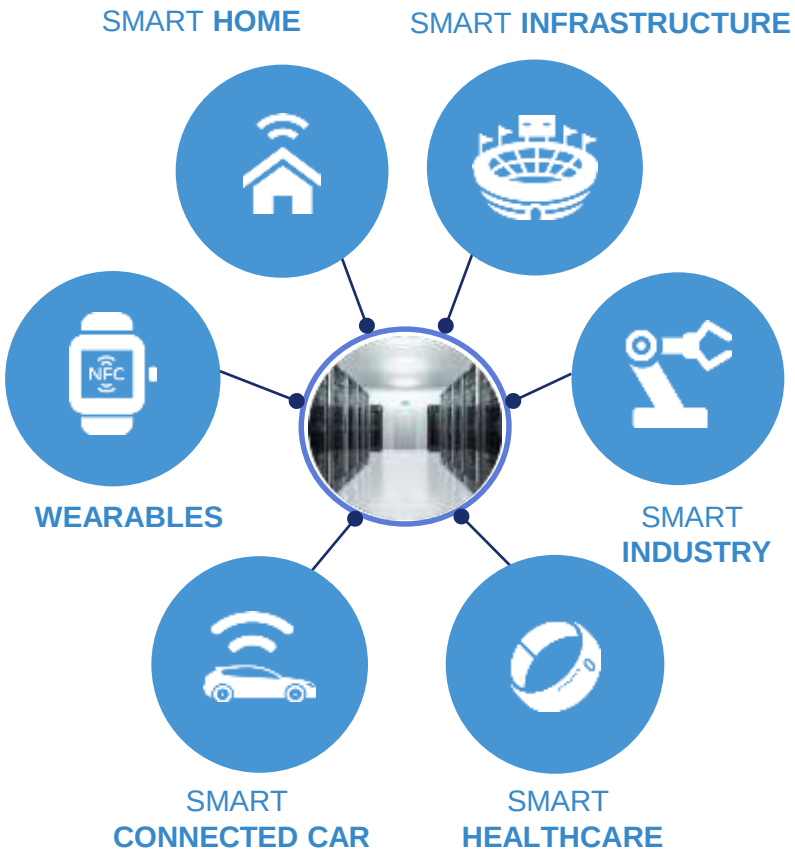
Application Identification	Device Identification
Certification	Compliance
Cryptography Acceleration	Network Security
NFC	RFID
Secure Boot	Secure Keys
Secure Memory	Secure Update
Trusted Execution	Unique Chip Identity

Our Security Expertise

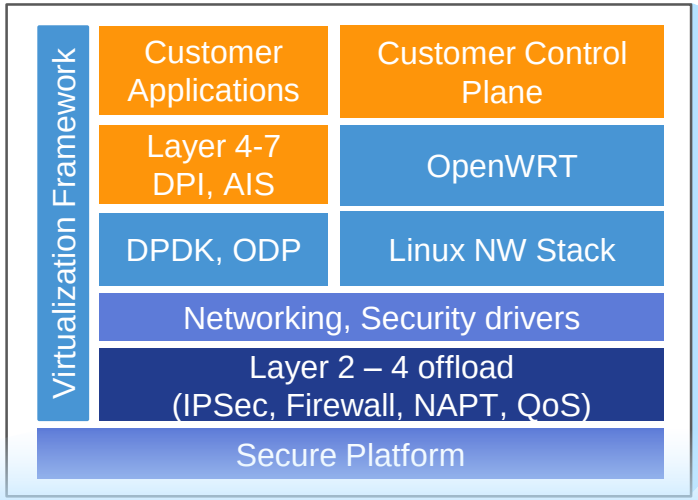
E-Passport | Mobile Transactions | Banking

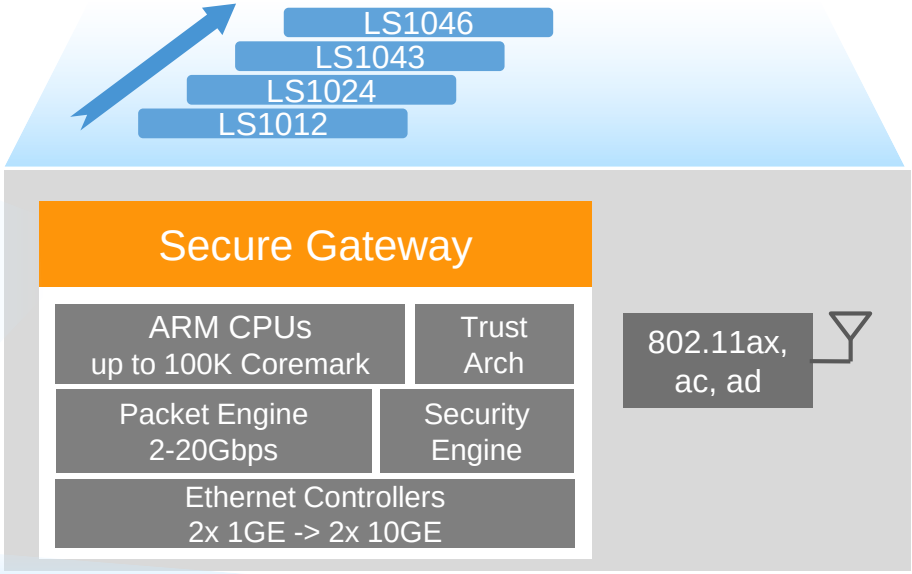
Security Consulting and Services can
get you to revenue faster

Your Smart Connected Product



Secure Platform in a Gateway





Secure-Boot is just the beginning – Security needs to cover the entire System.

Secure Boot

QorIQ Trust Architecture provides HW Root of Trust.

Anti-cloning features.

Anti-rollback to vulnerable firmware.

Persistent secret storage not visible to hackers.

Secure Provisioning

Secure signing of images and key provisioning.

3-way secrets isolation between NXP, ODM and customer.

Secured firmware upgrades

Trusted Linux

Secure run-time system operations.

Secure credential management – e.g. DRM keys.

Detect tampering of software via integrity checks.

Decrypt system firmware on-the-fly

Application Isolation

Isolate and host multiple services in containers, VMs.

Verify applications before install and launch.

HW level resource isolation and management.

Crypto Acceleration

NIST certified Security engine with rich algorithm support.

True Random Number Generation with 100% entropy

Integrated with Linux IPSec and OpenSSL.

Summary

Security/Trust

More important in todays world than ever before

An integral part of product development and deployment lifecycle

Must be easy to use

Layerscape Secure Platform

A suite of Hardware, Software and Process capabilities.

Covers every aspect of product lifecycle

Embedded into every QorIQ system solution

Security Consulting and Services to help you get to revenue faster

SECURE CONNECTIONS
FOR A SMARTER WORLD