(intel®)
experience
what's inside™

THE INTEL®
IOT GATEWAY

Internet of Things Group (IoTG)
Application-Ready Platforms

August 2015

LEGAL NOTICES AND DISCLAIMERS

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

Cost reduction scenarios described are intended as examples of how a given Intel®-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications, and roadmaps.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel does not control or audit third-party benchmark data or the websites referenced in this document. You should visit the referenced website and confirm whether referenced data are accurate.
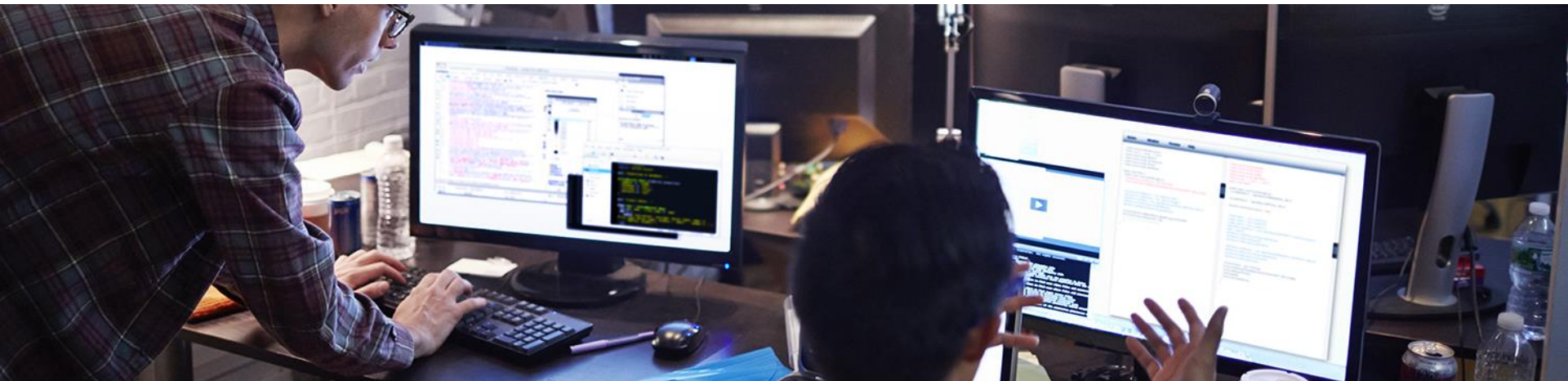
TABLE OF CONTENTS

INTERNET OF THINGS

Market Overview

CORPORATE OVERVIEW

IoT is a vital part of Intel.

Data Center   Client/Mobile Computing   IoT   Software and Services
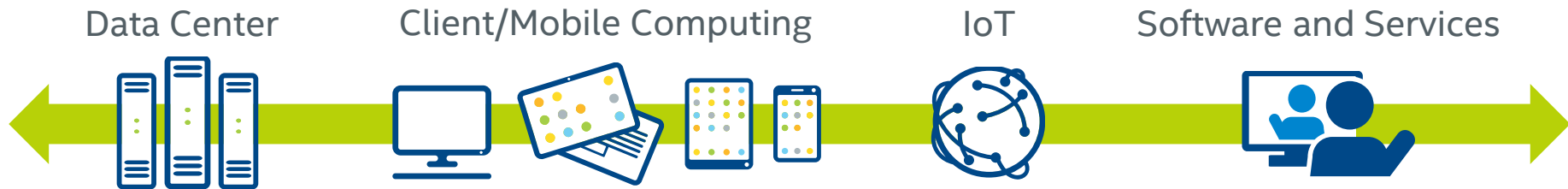
DEFINING THE INTERNET OF THINGS (IOT)
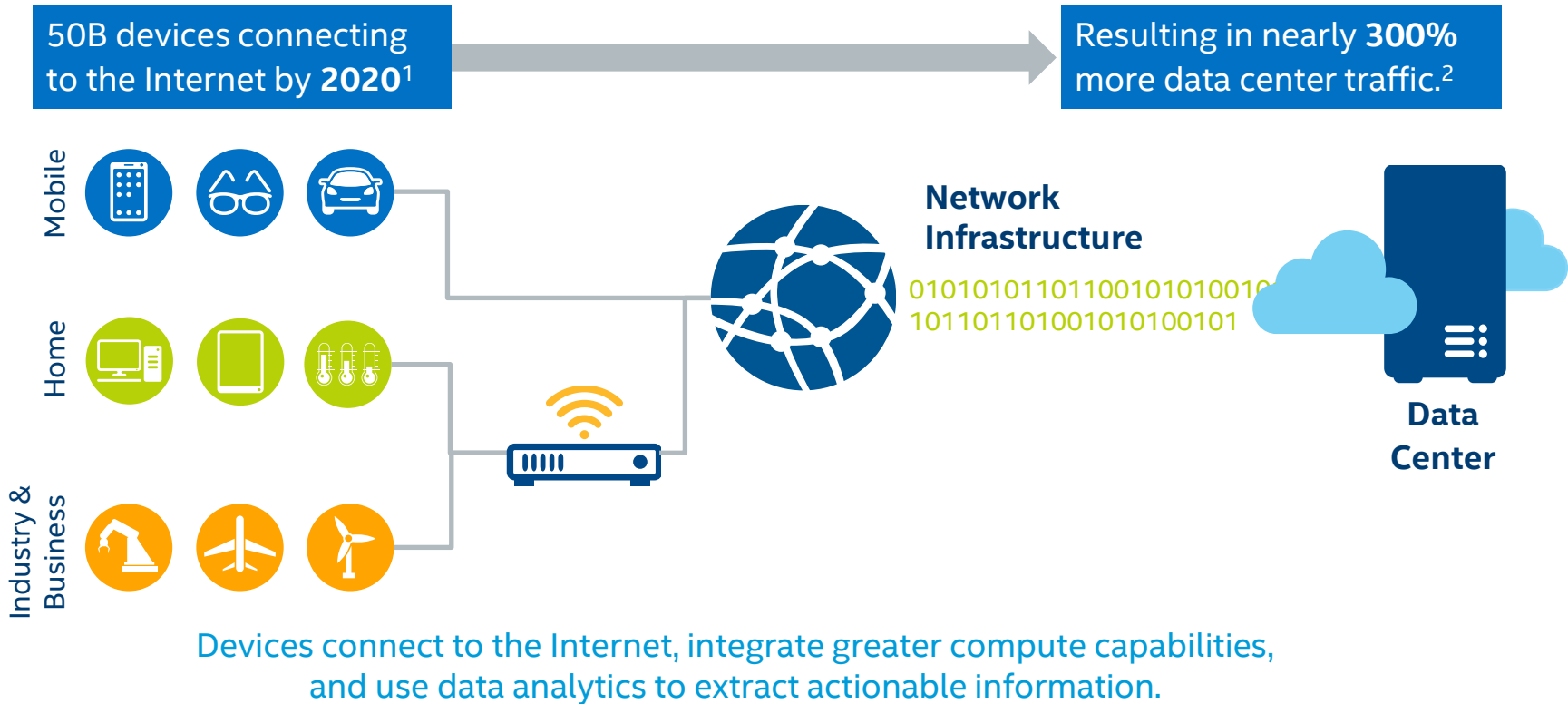
50B devices connecting to the Internet by 2020[1]

Resulting in nearly 300% more data center traffic.[2]

Mobile

Home

Industry & Business

Network Infrastructure

01010101101100101010010
10110110100101010100101

Data Center

Devices connect to the Internet, integrate greater compute capabilities, and use data analytics to extract actionable information.

Intel® IoT Platform
Secure, Scalable, Interoperable

The Intel® IoT Platform is an end-to-end reference model and family of products from Intel and the industry that provides a foundation for seamlessly and securely connecting devices, delivering trusted data to the cloud, and delivering value through analytics.

**VISUALIZE DATA AND MONETIZE INSIGHT**
Provide actionable information
Automate operations
Create services

CONNECT THINGS AND DEVICES
Capture sensor data
Machines take action

TURN DATA INTO INSIGHT
Process and store data
Perform cloud analytics
Manage devices and policies
Manage networks

IoT connectivity starts here

GATEWAYS
☑ Hardware verification
☑ Software verification

CLOUD MANAGEMENT

DATACENTER

STORAGE

ANALYTICS & APIs

INTELLIGENCE AT THE EDGE
Filter data
Perform edge analytics
Data informs and directs devices

END-TO-END SECURITY
Secure hardware, software, and data
Secure device management
Secure policy management
Safeguard scalable compute

WHY SMART MATTERS

Save on increasing data usage costs by filtering, aggregating, and analyzing data at the edge.
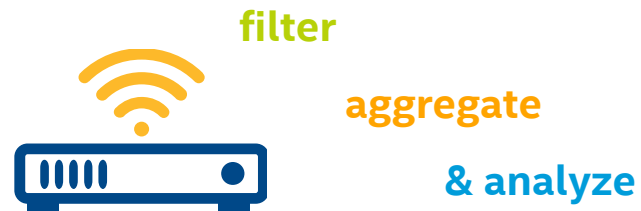
By 2018, 50% of IT networks will be **network-constrained.**[1] As a result, **40%** of IoT-created data will be stored, processed, analyzed, and acted upon close to or at the network edge.[2]
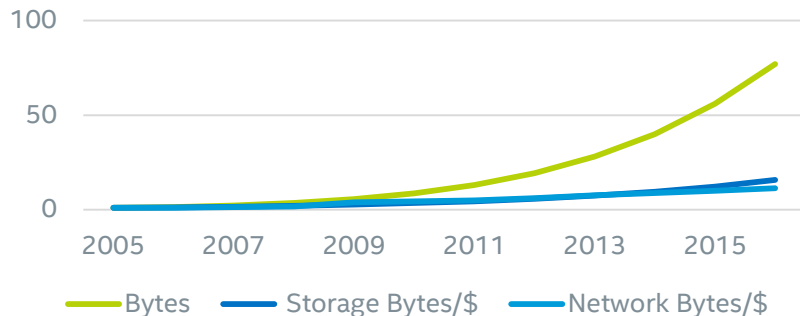
Data trends driving edge analytics

Identifying actionable intelligence at the edge saves costs and speeds time to value.

Intelligent gateways...

filter

aggregate

& analyze

data **before** sending to the cloud.
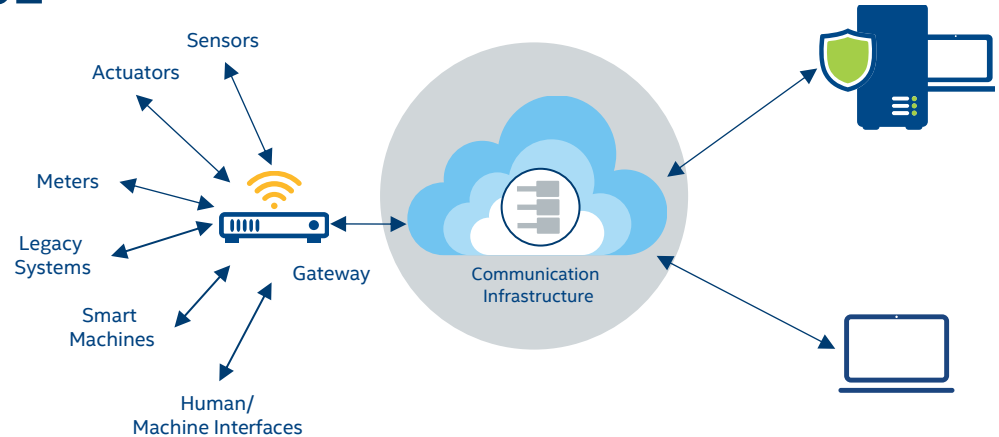
INTEL® IOT GATEWAY

Enabling Actionable Intelligence

THE IOT GATEWAY ADVANTAGE

Gateways have been used in business and industry for decades to enable machine-to-machine (M2M), Integrated Services Router (ISR), and cellular connectivity.

IoT Gateways are used to connect edge devices to the cloud and help filter data in areas such as:
- Industrial
- Smart Building
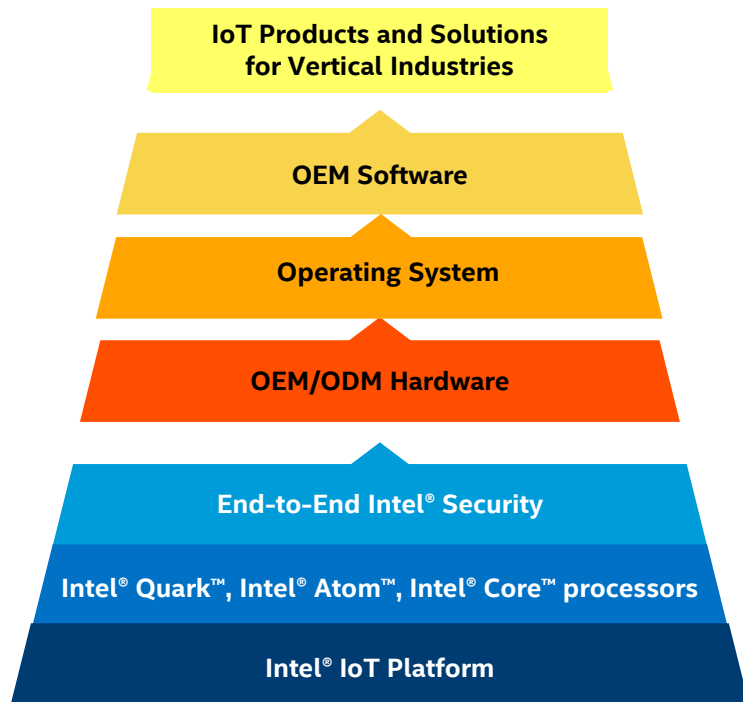- Retail
- Transportation
- Finance
- Healthcare

Sensors

Actuators

Meters

Legacy Systems

Gateway

Smart Machines

Human/ Machine Interfaces

Communication Infrastructure

Intel® IoT Gateway-based solutions provide standard features, plus:
- Strengthen security through silicon-based security capabilities
- Enable near-real-time edge analytics for actionable insight at the edge
- Support micro services and vertical packages
- Enable deployment of new applications/services
- Are field-programmable

INTEL + ECOSYSTEM = IOT VALUE

- Intel provides the reference architecture and foundational technologies.

- Our vast ecosystem delivers various hardware and software components for customers to build final IoT solutions.

IoT Products and Solutions for Vertical Industries

OEM Software

Operating System

OEM/ODM Hardware

End-to-End Intel® Security

Intel® Quark™, Intel® Atom™, Intel® Core™ processors

Intel® IoT Platform

INTEL® IOT GATEWAY BENEFITS

	Performance at the edge	that enables near-real-time analytics, local decision making, and tighter process controls.
	Advanced security	for trusted data from edge to cloud and protection from costly attacks.
	Scalability	for varying levels of gateway performance, with a broad range of support from Intel® Quark™, Intel® Atom™, and Intel® Core™ processors.
	Manageability	for secure remote upgrades and services.
	Faster, more flexible deployment	with a platform that supports your choice of operating systems and ecosystem applications.

SECURITY IS CRITICAL

Connecting "things" to the Internet that have never been connected is valuable, but also introduces risk.

Source: McAfee Labs Q1 '14

46% Increase in new malicious signed binaries

236 New threats every minute, or almost four every seconds

49% Growth in new threats attacking the master boot record and an all-time high for a single quarter

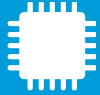> *"The ability to attack will outpace the ability to defend."*
>
> *—Rand Group*

> *"It takes 20 years to build a reputation and **five minutes to ruin it**. If you think about that, you'll do things differently."*
>
> *—Warren Buffet on Target Corp*

PROTECTING THE EXECUTION, STORAGE, AND TRANSFER OF DATA

1 **Security built into the hardware:** Hardware integrity must be enforced to ensure the device has not been altered.

2 **Secures OS and applications:** The gateway itself must have a secure operating system to ensure that data is safely stored.

3 **Secures data from chip to cloud:** Data must be transmitted securely from sensor to data center, even when one or more gateways must process it on the way.

4 **Enabling ecosystem security:** Standardized Intel solutions allow augmented security with third-party solutions.

Security and privacy are the top two inhibitors of the success of IoT deployments.

Recent survey of more than 450 IT and business leaders[1]

From the Field

- A lack of security in implanted **medical devices** opens the door for malicious activity that could put patient health at risk.

- **Industrial devices**, if tampered with, can leak sensitive operational data.

- Hackers may breach **retail devices** to gain insight into sales patterns, change prices, or hide inventory.

IOT GATEWAY USE CASES

Energy grids lose ~6% during transmission and distribution.[1]

ENERGY
Environmental data logging; substation monitoring and remote access; grid efficiencies

Intel® IoT Gateway

INDUSTRIAL AND MANUFACTURING
Assembly line equipment reporting; inventory management; automation

HVAC systems account for 41% of energy used in U.S. buildings.[2]

Enhanced driver coaching can save nearly 7% on fuel costs.[3]

RETAIL
Point of sale, vending machines, supply chain

SMART BUILDING
Energy use monitoring, and sensors in heaters, boilers, chillers, etc., to find inefficiencies

TRANSPORTATION
Fleet management and tracking, urban congestion management, freight tracking

Gateways "bolt on" to existing assets to capture existing data and meet the needs of the install base.

1. http://www.eia.gov/tools/faqs/faq.cfm?id=105&t=3
2. 2010 U.S. Department of Energy
3. https://www.youtube.com/watch?v=-o4V19Ttr0I

INTEL® IOT GATEWAY EXPANDING PORTFOLIO

Optional Capabilities and Services
Capabilities & Services (Cloud, Manageability, Security, Analytics)

Open Source OS

ubuntu

Commercial OS

Microsoft

Core	Enterprise

WIND

"Flex"	"Pro"

intel Quark

intel inside™ ATOM™

intel inside™ CORE™

Today: McAfee ePO*, Intel® IoT Platform software and services (Edge Application Platform, Intel IoT Analytics)

Coming soon: More open source OS offerings, vertical-specific binaries, and more!

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Microsoft OS* not enabled on Intel® Quark™.

Intel Confidential   intel   16

INTEL® IOT GATEWAY WITH WIND RIVER

WIND

WIND RIVER PORTFOLIO

Preintegrated, prevalidated hardware with critical software components.

Wind River 'Flex'

Entry Offering

- Free commercial offering with option to purchase:
  - Maintenance & support
  - Gold support
  - McAfee Embedded Control*
- Prevalidated base evaluation OS
- Includes open source security

Wind River 'Pro'

Premium commercial offering

- Aggressive tiered pricing model
- Prevalidated enhanced evaluation OS
- Includes:
  - 1 year of Gold support
  - Wind River development tools
  - McAfee Embedded Control*
  - HW-based security w/verified boot

INTEL® IOT GATEWAY WITH WIND RIVER PRO SOFTWARE STACK

■ = Third Party

Third-Party Ecosystem Apps and Services, SI/ITOs, Customers

Manageability

Wind River Helix
Device Cloud* agent

OMA DM TR-069
Web Config

Run-Time Environment

Lua*   Java*   OSGI*

Security

Data

DM-Crypt   OpenSSL   IP Tables
IPSec VPN   Encrypted Storage

OS and Apps
McAfee Embedded Control*
(with whitelisting)
Grsecurity
Signed RPM Package

HW
Discrete TPM   Secure Boot

Connectivity

2G/3G/4G
Bluetooth
Ethernet
ZigBee stack
Serial/USB
VPN
WiFi Access Point
MQTT

Wind River Intelligent Device Platform XT* featuring Wind River Linux*

Intel® BSP: Board and Modules (Intel® Quark™ SoC, Intel® Atom™ Processor, Intel® Core™ Processor)
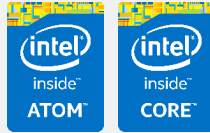
WIND

Development Environment

INTEL® IOT GATEWAY WITH WIND RIVER: NEW FEATURES

3.0 AUGUST 3

- Early access program
- Linux 7*, 3.14 Kernel*
- 64bit WRL7
- OS runtime image
- 7 Atom™ BSPs updated, 1 Core™ (ADLink)
- Wind River Helix* Device Cloud OTA OS update
- Initial agent-agnostic OTA manageability APIs (app updates)
- Enabled generic script-based mechanism to execute boot time
- Intel® IoT Gateway Developer Hub (Beta)
- Updated McAfee Embedded Control* (6.6) and Triage Tool*
- Security upgrade capabilities for Flex (McAfee Application Control*)

3.1 SEPT/OCT

- Wind River Linux 7*
- Remote factory reset
- OTA SW & OS update and rollback with Wind River Helix* Device Cloud
- Multiple Quark™ BSPs updated
- Plug-n-play Intel® IoT Commercial Developer Kit
- Intel® IoT Platform Marketplace
- Intel® IoT Gateway Developer Hub
- Marvell, Redpine Signals Wifi Modules *(trending)*
- 6LoWPAN *(trending)*
- TBD *(Additional items under review)*

WIND RIVER HELIX* DEVICE CLOUD AGENT

Enable IoT devices to securely connect to a centralized console,
for device management and solution extensibility.
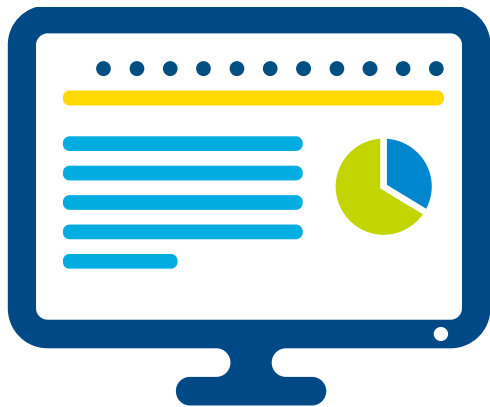
Available preconfigured on
Intel® IoT Gateways.

Quickly develop
Build and deliver secure applications
and services—*fast*

Easily integrate data
Link data to existing enterprise
systems with Intel® Mashery™ API
Management

Manage remotely
Cloud-based provisioning; centralized
management and services delivery

WIND RIVER FEATURES

Categories	Features	Flex	Pro
Preintegrated Agents	Helix* Device Cloud (EMS), ePO, EAP	✓	✓
Secure the Communications	IP Tables	✓	✓
	SSL	✓	✓
Secure the Device	Secure Boot	✓	✓
	TPM 1.2 Cert Management	✓	✓
	IMA Whitelisting	✓	^
	McAfee Embedded Control* (MEC)	Upgrade	✓
Secure the Data	Dm-crypt	✓	✓
	SRM Signing Tool	✓	✓
	Certificate Management	✓	✓
	Application Integrity Measurement	✓	✓
	Grsecurity	✓	✓
	EAL4-Ready (Privacy)	✓	✓
Development Tools	Workbench*	N/A	✓
	OpenJDK, Lua*, Python*	✓	✓
	ProSyst OSGI*	N/A	✓
Manage the Device	Work Systems: OMA DM, TR-069	N/A	✓
Protocols	Exegin Zigbee	N/A	✓
	Yanzi 6loWPAN	N/A	✓
Communications	MQTT, BlueZ, Multiwan	✓	✓

^Linux* IMA Whitelisting is disabled with McAfee embedded Control*

WIND RIVER LICENSE OPTIONS

Software Kit*	Description	ID	License Term	Support Period
Flex	Free, no support**, unlimited license	IoTGTWY.FLX1	Perpetual (unlimited)	Perpetual
Flex with Support	Option to include support ($)	IoTGTWY.FLXS1	Perpetual (unlimited)	1 year
Pro Evaluation	Evaluation version, limited license, includes support (<$20)	IoTGTWY.PROE1	6 months	6 months
Pro	Includes development, production, and support	IoTGTWY.PRO1	Perpetual (unlimited)	1 year

*Additional Pro SKUs available for system integrators who wish to evaluate the platform but do not intend on distributing the SW
**includes critical security patches at no cost

BUILD VS. BUY:

Embedded Wind River Linux*: Lowering Total Cost of Ownership

BUILD

Complicated to build

Mostly unknown to your development team

Steep learning curve

Time-consuming to run

Difficult to maintain and support

Custom distribution

VS.

BUY

Faster setup and deployment

Faster time to market

In production for many years

In service sometimes for decades

Lower maintenance costs

Easier to maintain

Expert support

Lower TCO

SAVE TIME AND MONEY

Two key benefits of commercial-grade Linux*

98% Reduction in production and maintenance costs[1]

30% Acceleration in build cycles[1]

AVAILABLE INTEL® IOT GATEWAY SECURITY FEATURES

Hardware Resiliency (Intel® SoC HW root of trust and Grub-IMA)	OS and Applications Resiliency (Intel SoC HW root of trust and Grub-IMA)	Data Resiliency Protection (at rest and securing network comms) and resiliency (firewall)
Discrete TPM[1] Locking and storing private materials inside the trusted platform module	**McAfee** Embedded Control of Linux* IMA[2]** Provides system integrity and change control (e.g.., whitelisting)	**DM-crypt** SW stack to enable data at rest protection
Secure Boot What you intend to have booted is what's being booted	**Grsecurity** Allows programs to execute as least privilege policy	**Open SSL and IPSec VPN** Create private tunnels to raise assurance of the target destination
	Signed RPM Packages Gateway confirms signature before it applies RPM system	**IPTables** Linux*[3] firewall and network routing software

1, Note that Discrete TPM is not supported in PRC. DK100 & 300 are the only Intel-branded dev kits that support TPM.
2. McAfee Embedded Control includes McAfee Whitelisting. Linux* IMA is an alternative for countries where McAfee Embedded Control may be unavailable.
3. Protecting the Firmware with security rooted in the HW. The ODM must **enable** these features in order to have the OEM realize the benefits

Intel Confidential   25

INTEL® IOT GATEWAY WITH MICROSOFT

Microsoft

INTEL® IOT GATEWAYS: MICROSOFT

Enable secure connectivity and edge computing.

Intel® is enabling Windows 10* IoT-based gateways to provide greater OS choice for OEMs and end customers.

Calypso Island is an enabling program for Windows 10* IoT-based gateways using Intel® Atom™ and Intel® Core™ processors.

Easily enable secure edge-to-cloud connectivity with data processed in the cloud or on the gateway, resulting in lower latencies and reduced data costs.

INTEL® IOT GATEWAYS: MICROSOFT

KEY FEATURES:

- Scalability from Intel® Atom™ to Intel® Core™ processors
- Secure boot
- Intel® AES-NI for enhanced encryption
- TPM 1.2 and 2.0
- Measured boot
- Device attestation
- Data encryption
- Antimalware, antivirus, whitelisting integration
- Supporting a robust ecosystem of applications

IDEAL FOR:

This program enables Intel's customers and partners (ODM, OEM, SI) to offer a Windows*-based gateway to end customers who prefer a Microsoft solution in a wide variety of markets.

TIMING:

Microsoft-enabled gateways begin in Q4 2015 on Intel® Atom™ processors, and will extend to 6th gen Intel® Core™ in 2016.

INTEL® IOT GATEWAY
WINDOWS 10* IOT CORE SOFTWARE STACK

= Third Party

Ecosystem Apps and Services, SI/ITOs, Customers

Manageability

System Center ConfigMgr (SCCM)*, Microsoft Intune*, Microsoft Windows* Update*, Windows as a Service*, McAfee ePO*/Agent*

Windows ICD*, OMA DM*, PowerShell*

Run Time Environment

Win32

Universal Application

Console Application (Limited)

Security

Data
CryptoAPI*, IPSec VPN*, MS Direct Access*, Windows Firewall*, Windows BitLocker*

OS and Apps
Code Integrity, Virtualization-Based Security, USB Down & Keyboard Filters, Health Attestation

HW
Discrete TPM   UEFI Secure Boot

Connectivity

Bluetooth, Ethernet, WiFi, Cellular (data only), VPN

AllSeen AllJoyn/Device System Bridge

Windows 10* IoT Core

Intel BSP: Board and Modules (Intel® Atom™ Processor)

Development Environment

Visual Studio

INTEL® IOT GATEWAY
WINDOWS 10* IOT ENTERPRISE SOFTWARE STACK

▢ = Third Party

Ecosystem Apps and Services, SI/ITOs, Customers

Manageability

System Center ConfigMgr (SCCM)*, Microsoft Intune*, Microsoft Windows* Update*, Windows as a Service*, McAfee ePO*/Agent*

Windows ICD*, OMA DM*, WMI*, PowerShell*

Run-Time Environment

Win32
Win64

Universal Application

Console Application

Security

Data
CryptoAPI*, IPSec VPN*, MS Direct Access*, Windows Firewall*, Windows BitLocker*, McAfee Endpoint Security*

OS and Apps
Device Guard* (Code Integrity*, AppLocker*, Defender*, Virtualization-Based Security), UAC, McAfee Endpoint Security*, McAfee Application Control*, USB/Shell Lockdown & Keyboard Filters, Health Attestation

HW
Discrete TPM   UEFI Secure Boot

Connectivity

Bluetooth, Ethernet, WiFi, Cellular (data only), VPN

AllSeen AllJoyn/Device System Bridge

Development Environment

Visual Studio

Windows 10* IoT Enterprise

Intel BSP: Board and Modules (Intel® Atom™ Processor, Intel® Core™ Processor)

WINDOWS 10* IOT CORE AND IOT ENTERPRISE FEATURES

PLATFORM

Feature	Windows 10* IoT Core	Windows 10* IoT Enterprise
Royalty / Cost	Free (makers and device builders)	Entitlement
License Activation	None	Required
MSFT Certification	None	Required
CPU Architectures	x86 / ARM 32-bit	x86 32-bit / 64-bit
IA Platforms	Intel® Atom™: Bay Trail (1H 2015)	Intel® Core™: Broadwell (2H 2015) Intel® Atom™: Bay Trail (1H 2015)
Virtualization	None	Windows HyperV*
Display	Headed / Headless	Headed

SECURITY

Feature	Windows 10* IoT Core	Windows 10* IoT Enterprise
OS Hardening	Virtualization Based Security	Device Guard (Virtualization Based Security), User Account Control (UAC)
Software Integrity / OS Lockdown	Code Integrity, USB Lock Down & Keyboard Filters	Device Guard (Code Integrity, AppLocker, Defender), Write Filters, Kiosk, USB Lock Down & Keyboard Filters, McAfee Endpoint Security, McAfee Application Control
Secure Boot	UEFI Secure Boot	UEFI Secure Boot
Measured Boot	Measured Boot (Bitlocker)	Windows* Measured Boot (Bitlocker, Anti-Malware)
Firewall	Windows* Firewall	Windows* Firewall, McAfee Endpoint Security
Device Attestation	Active Directory, Health Attestation	Active Directory, Health Attestation
Data at Rest	Windows* Bitlocker	Microsoft Windows* Bitlocker
Data in Transit	CryptoAPI, Microsoft* Direct Access, VPN	Microsoft* CryptoAPI, IPSec VPN, Microsoft Direct Access
TPM	TPM 2.0	TPM 1.2 / 2.0

WINDOWS 10* IOT CORE AND IOT ENTERPRISE FEATURES

MANAGEMENT

Feature	Windows 10* IoT Core	Windows 10* IoT Enterprise
OS Deployment/ Distribution	• Windows Imaging Configuration Designer (ICD)* • Deployment Image Servicing and Management (DISM)* • Binary Full Flash Update	• Windows Imaging Configuration Designer (ICD) • Deployment Image Servicing and Management (DISM) • System Center/Third-Party OS Deployment • CD & USB Binary Install/Setup
OS Update/Patch	Microsoft Windows Update, Microsoft Intune*/System Center*, McAfee ePO*	
OS Upgrade (e.g. 2.x -> 3.x)	Windows as a Service* (TBD), Microsoft System Center*, Microsoft Intune*	
App Deployment, Update	Microsoft Intune*/System Center*, ICD* Configuration Packs, Windows Update*	Windows Store*, MSFT OneGet*, Intune*/System Center*, McAfee ePO*
Configuration Management	CDI* Configuration Packs, Microsoft Intune*/System Center*, Third-Party	Microsoft Intune*/System Center*, McAfee Agent*/ePO*, Customer BKM
Remote Management	Windows PowerShell*, Microsoft Intune*/System Center*, Third-Party through API	Windows PowerShell*, Remote Desktop*, Microsoft Intune*/System Center*, Third-Party

APPLICATION DEVELOPMENT

Feature	Windows 10* IoT Core	Windows 10* IoT Enterprise
Application Development	IDE: Visual Studio* App Types: • UAP (Background, Foreground/Headed) • Console Application (Limited) • Services (Limited) Scripts / Runtimes • Native: Windows PowerShell* • Batch Console Application for Third-Party Interpreters TBD, although not natively supported	IDE: Visual Studio* + Ecosystem of Third-Party IDEs App Types: • UAP (Foreground) • Windows Apps (Win32*) • Console Application • Services Scripts / Runtime: • Native: Windows PowerShell*, Batch, VBScript*/Windows Script Host* • Third-Party: Java*, JavaScript*, Python*, Node.JS*, Ruby*, plus vast ecosystem of more options

INTEL® IOT GATEWAY WITH SNAPPY UBUNTU CORE*

ubuntu

WHAT IS SNAPPY UBUNTU CORE*?

The smallest, leanest, safest Ubuntu ever, optimized for IoT devices.

- A new rendition of Ubuntu* with transactional updates

- A minimal OS image with the same Ubuntu* libraries but applications are provided through a simpler mechanism

- Snappy apps and Ubuntu Core* itself can be upgraded automically and rolled back if needed

- Snappy applications are confined by Canonical's AppArmor* kernel security system

  - Delivering rigorous MAC-based isolation and human-friendly security profiles

  - Applications are completely isolated from one another

IDEAL FOR:

Customers who prefer Ubuntu* community and commercially supported versions.

SNAPPY UBUNTU CORE*

Snappy Ubuntu Core* delivers security, reliable updates, and the Ubuntu* ecosystem, bringing the cloud platform to a wide range of IoT, connected devices, and autonomous machines.

- A single identical platform from cloud to device.

- Present the exact same APIs and receive identical security updates on devices and on the cloud.

- Save costs by forwarding only relevant data to the cloud.

ROBUST SECURITY

- Hardware-enhanced encryption on Intel® IoT Gateways

- Automatic updates to address systemic vulnerabilities

- Best-in-class application isolation based on kernel containers, minimizing the impact of errors and vulnerabilities in third-party applications.

SNAPPY ARCHITECTURE

Four layers that make up a Snappy deployment:

1. Enablement or BSP—provided by ODM/OEM or Canonical ($)

2. The system layer (OS)—provided by Canonical

3. An optional layer of frameworks that extend the base system—produced by vendors in collaboration with Canonical

4. One or more Snappy applications— provided by vendors, written directly, etc.

Apps	Apps	Apps
Frameworks	Frameworks	Frameworks
Ubuntu OS (Snappy Ubuntu Core)		
Enablement (BSP)		
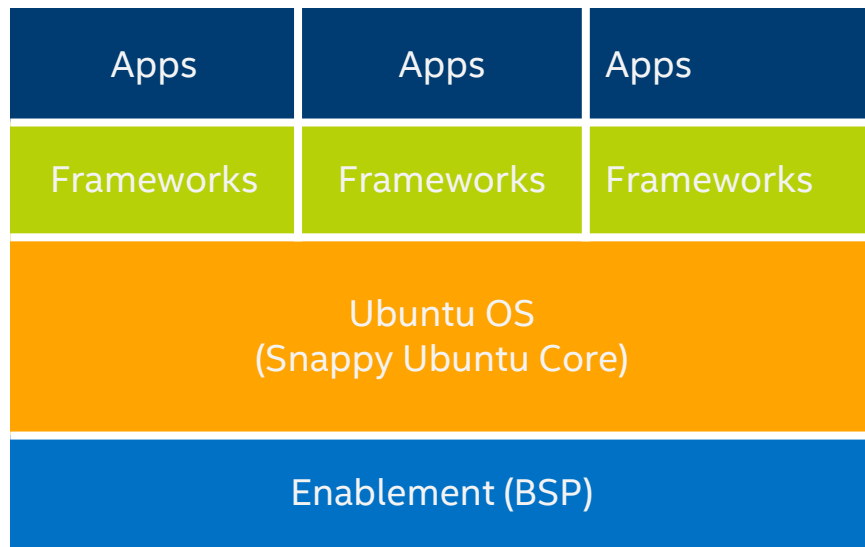
SNAP STORE

Deliver innovative applications for a wide range of IoT solutions and vertical markets, including home, health, media, security, lighting, energy management, and industrial

- **Easy:** Snaps can packaged and published in minutes.

- **Flexible:** Snaps can be quickly deployed, and easily rolled back.

- **Fast:** Updates can be done faster and easier, enabling innovation.

- **Secure**: Snaps run in Snappy's application isolation model.

INTEL® IOT GATEWAYS

"One easy-to-use, secure, open source, and universal platform on top of Intel IoT gateways will unleash innovation like never before."
Maarten Ectors, VP IoT, Next-Gen Networking and Proximity Cloud, Canonical

SNAPPY FRAMEWORKS

- Direct extension of the Ubuntu Core*

  - Primarily provide mediation of shared resources (device files, sensors, etc.)

  - Developed by parties with a contractual relationship with Canonical

- First framework is Docker*

- Many more frameworks being developed

More details: https://developer.ubuntu.com/en/snappy/guides/frameworks/

DEVELOP AND DEPLOY

Intel® IoT Commercial Developer Kit

INTEL® IOT GATEWAY ECOSYSTEM

Choose from our vast ecosystem of ODM parnters

ODM SOLUTIONS DIRECTORY

Click a design to get product details

http://iotsolutionsalliance.intel.com/solutions-directory

Explore our easy-to-use online catalog of Intel® IoT Gateway products from ODMs.
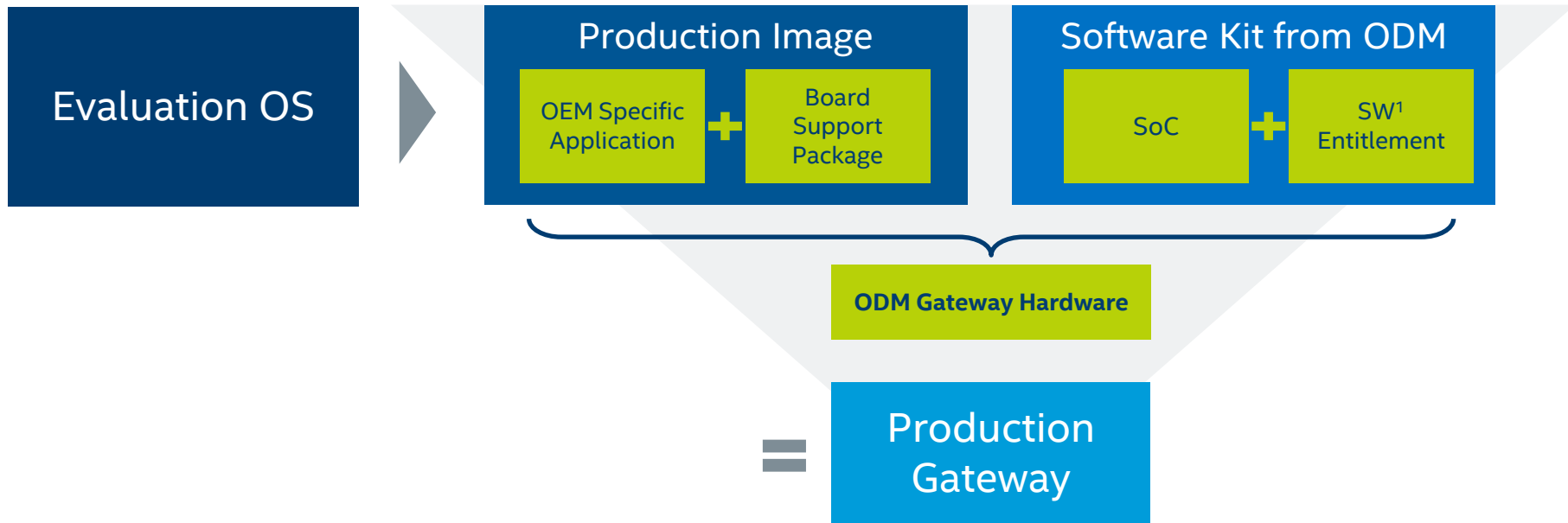
PATH TO PRODUCTION: DEFINITIONS

1 **Evaluate**

- Interest in seeing what Intel has to offer for gateways
- First time exploring Intel platform and its capabilities
- Playing with the HW and evaluation SW
- If you have an app, see how your app runs on the platform and the HW

Decision Point: HW & SW combination meets my needs, the price and support options are right for my company, and I'm ready to build my solution.

2 **Develop**

- Decide what production HW you want, what sensors you need
- Build the full solution in dev environment (port app + cloud connectivity, manageability, etc.)
- Add any extra HW support and libraries required for your app
- Generate and test your production runtime image

Decision Point: My solution does all that I expect it to do.

3 **Deploy**

- Order your final production HW quantities
- Send your production runtime Image to the ODM
- Ensure the production runtime image functions on production HW as expected
- Deploy!
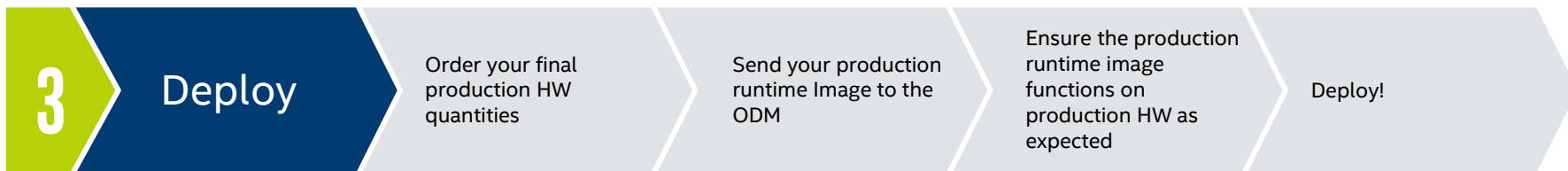
UNDERSTANDING THE INGREDIENTS OF A PRODUCTION GATEWAY

Evaluation OS

Production Image
- OEM Specific Application + Board Support Package

Software Kit from ODM
- SoC + SW[1] Entitlement

ODM Gateway Hardware

= **Production Gateway**

Over the next few sections, we'll see how this is handled for Intel® IoT Gateways with Wind River, Microsoft, and Canonical individually.
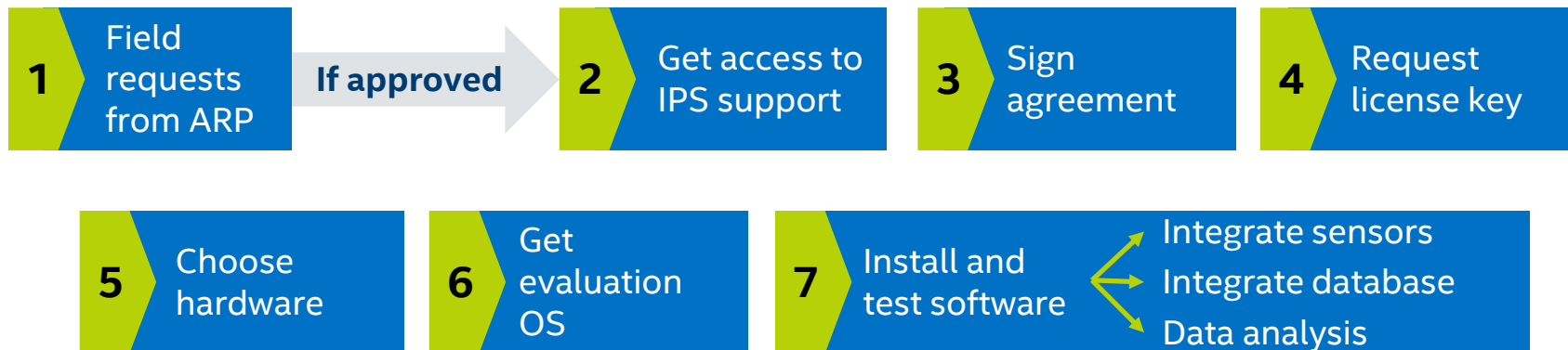
WIND RIVER

Developer Experience

EVALUATION PROCESS OVERVIEW

New customers are able to receive the 3.0 release through the following process.

1 Field requests from ARP

If approved →

2 Get access to IPS support

3 Sign agreement

4 Request license key

5 Choose hardware

6 Get evaluation OS

7 Install and test software →
- Integrate sensors
- Integrate database
- Data analysis

1. HW & SW combination meets my needs
2. The price and support options are right for my company
3. You're ready to build your solution

→ **Proceed to Development**

NOTE: If you have access to view NDA documents on CDI, see detailed information on these steps in our 3.0 Developer Experience
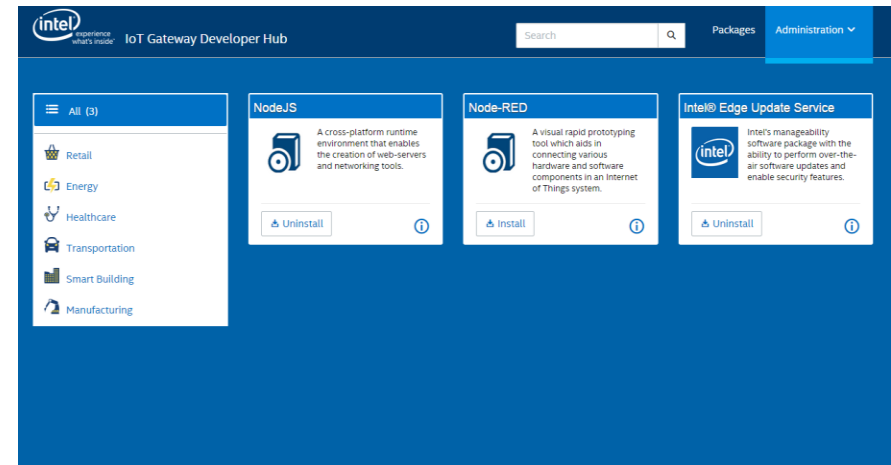
INTEL® IOT COMMERCIAL DEVELOPER KIT

WIND

A new evaluation/development option coming with **3.1 release** in Sept/Oct

- Replaces current development kits

- Intel® Galileo™ 2 + Grove Industrial Sensor Kit* allows evaluation of a complete solution, right out of the box

  - Runtime and sensors included

  - Plug and play in about10 minutes

- Easily port to production HW with minimal SW changes

OOBX GUI loaded on Intel® Galileo™ Gen 2

Contents of Kit
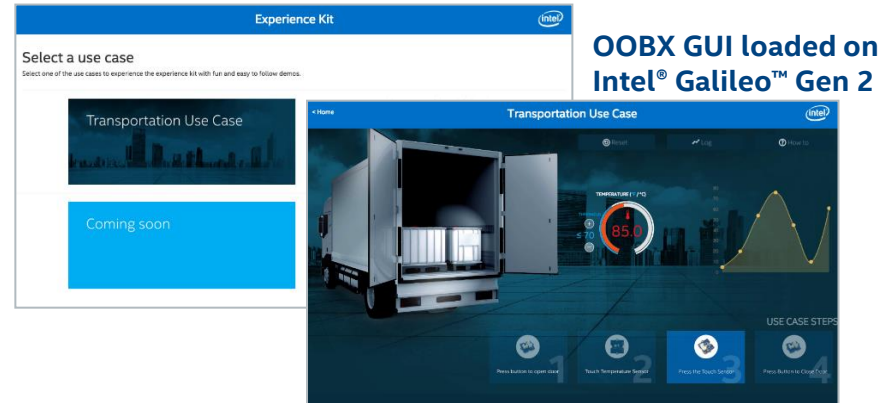
DEVELOPMENT PROCESS OVERVIEW

After evaluation, you may take the following steps

You can explore the functionality of our Intel® IoT Gateway Developer Hub at this stage
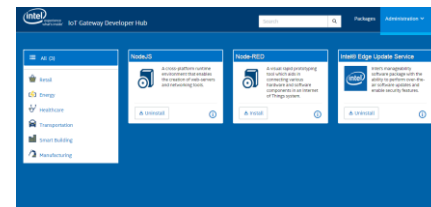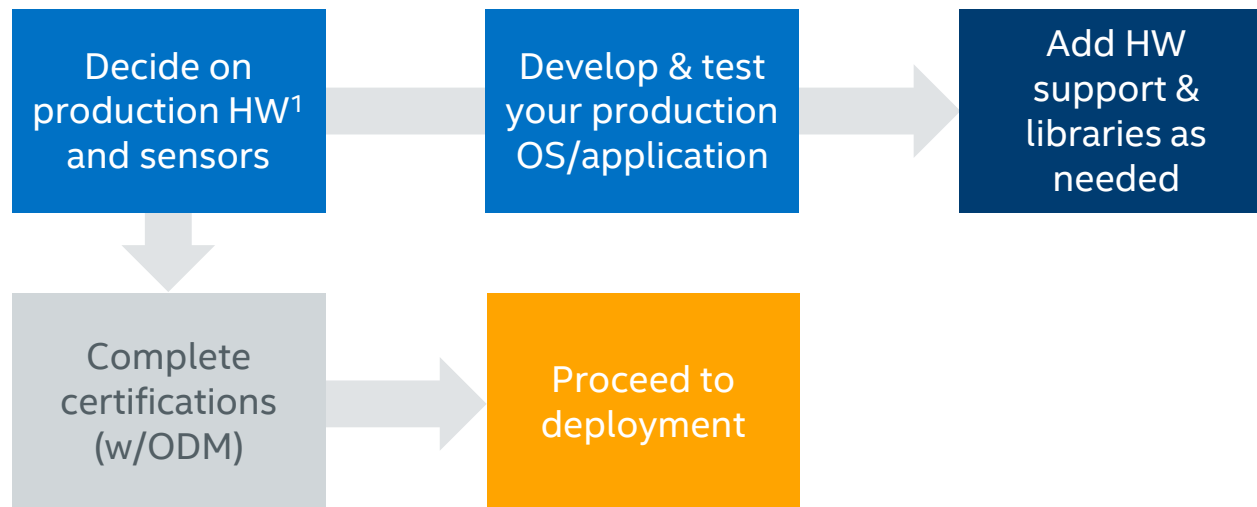
Decide on production HW[1] and sensors → Develop & test your production OS/application → Add HW support & libraries as needed
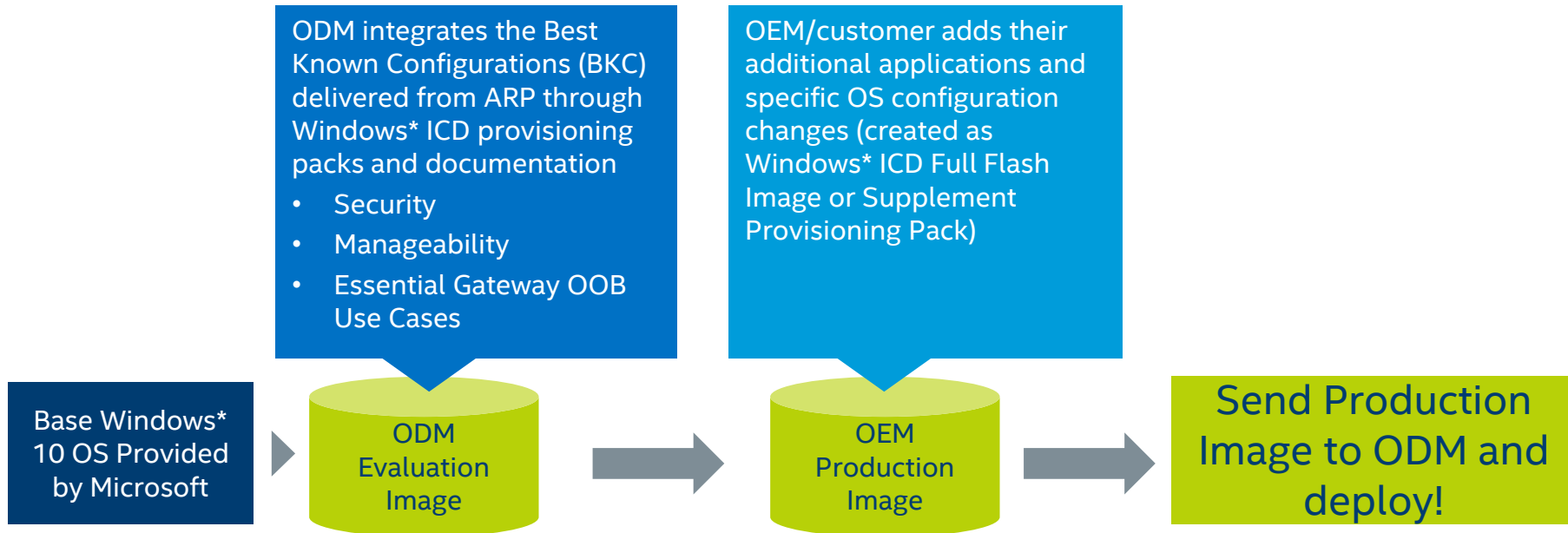

Complete certifications (w/ODM) → Proceed to deployment

NOTE: If you have access to view NDA documents on CDI, see detailed information on these steps in our 3.0 Developer Experience

1. Consider various GEO limitations for the certifications on various ODM hardware.

Intel Confidential   47

INTEL® IOT GATEWAY DEVELOPER HUB

Beta Release: 3.0; Production Release: 3.1

- Microsite GUI to download packages and link to other relevant content for a developer

- Will be included in the evaluation image (for Wind River Flex and Wind River Pro)

- Can pull from Intel, Wind River, and other third-party repositories to install packages

- Allow for add-on opportunities (e.g. McAfee products, partner solutions, etc.)

- Provide ability for agile releases for features installable via packages

DEPLOYMENT PROCESS OVERVIEW
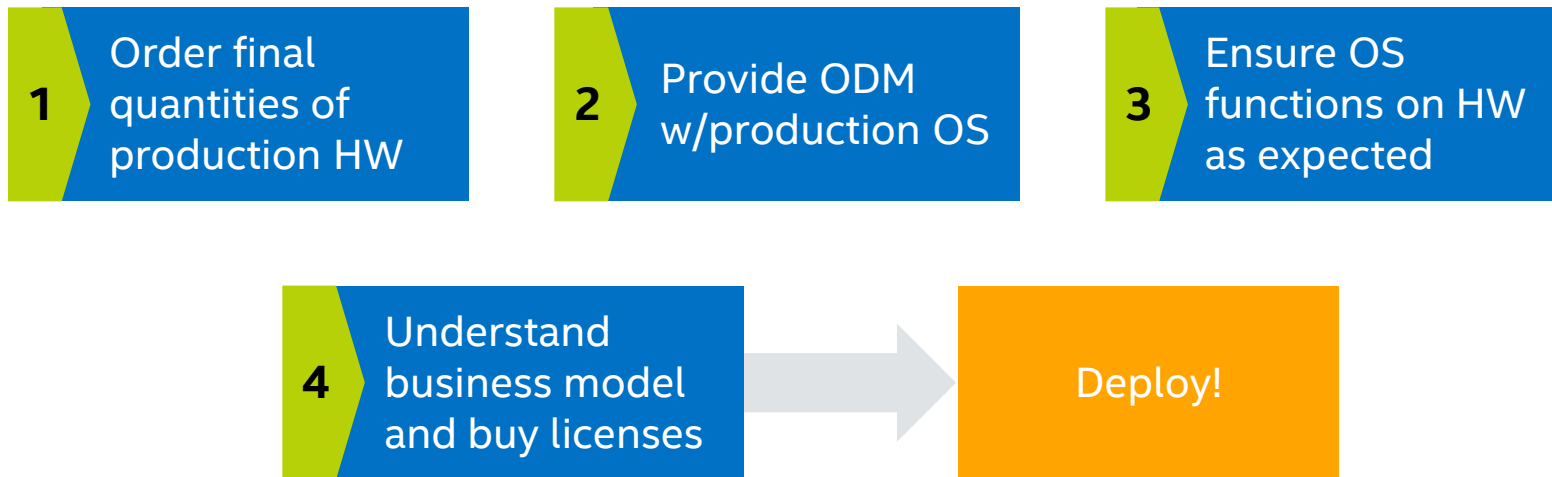
WIND

1 Order final quantities of production HW

2 Provide ODM w/production OS

3 Ensure OS functions on HW as expected

4 Understand business model and buy licenses → Deploy!

NOTE: If you have access to view NDA documents on CDI, see detailed information on these steps in our 3.0 Developer Experience

MICROSOFT

Developer Experience

PATH TO PRODUCTION: MICROSOFT WINDOWS 10*

Microsoft

ODM integrates the Best Known Configurations (BKC) delivered from ARP through Windows* ICD provisioning packs and documentation

- Security
- Manageability
- Essential Gateway OOB Use Cases

OEM/customer adds their additional applications and specific OS configuration changes (created as Windows* ICD Full Flash Image or Supplement Provisioning Pack)

Base Windows* 10 OS Provided by Microsoft

ODM Evaluation Image

OEM Production Image

Send Production Image to ODM and deploy!

CANONICAL

Developer Experience

PATH TO PRODUCTION: CANONICAL

ubuntu

Creating snappy apps is simpler than traditional packaging

Bundle all required files into a single package and add one description file

Packages can be statically linked and may include their own copies of any file(s) they need

Developers can use the exact library versions they want and control when those libraries are updated

Developers may use the core Ubuntu* libraries if preferred

More details: https://developer.ubuntu.com/en/snappy/tutorials/build-snaps/

INTEL® IOT GATEWAY ROADMAPS

INTEL® IOT GATEWAYS: SUPPORTED OS

Shipping	2015		2016				2017
	Q3	Q4	Q1	Q2	Q3	Q4	

Moon Island 2.1, 2.2
- EMS integration
- eMMC support
- Boot optimization
- Connectivity improvements
- LuCI support (MI 2.2)

Moon Island 3.0
- Linux* 7, 3.14 Kernel*
- 64-bit Bay Trail
- UX improvements
- EAL4 cert-ready (retail)
- Initial agent-agnostic OTA manageability APIs (app updates)

Moon Island 3.x (Delivered Qtrly via Packages)

Scalability
- Intel® Core™
- Vertical-specific features
- VxWorks*

User Experience
- WR Helix Cloud OTA OS, SW updates + rollback
- Evaluation OS distribution
- Plug-n-Play sensor kits
- IoT Comm. Dev. program

Security
- Measured boot
- Remote attestation
- Deep packet inspection
- TPM 2.0-enabled

Calypso Island 1.0
- Windows 10* IoT Enterprise & IoT Core
- Base HW enabling
- Validate security & manageability solutions

Calypso Island 1.5
- Audio & video processing enhancements
- Deep packet inspection

Snap Lake 1.0
- Snappy Ubuntu Core*
- Ubuntu 15.4-based
- AES-NI-enabled

Snap Lake 2.0
- Snappy Ubuntu Core*
- Ubuntu 16.4-based
- Includes long-term support

In Planning	Pre-POP L3
Development	Shipping

LEFT edge of box indicates Target Production. All products, dates, and figures specified are based on current expectations and are subject to change without notice.

INTEL® IOT GATEWAYS: SUPPORTED SOCS
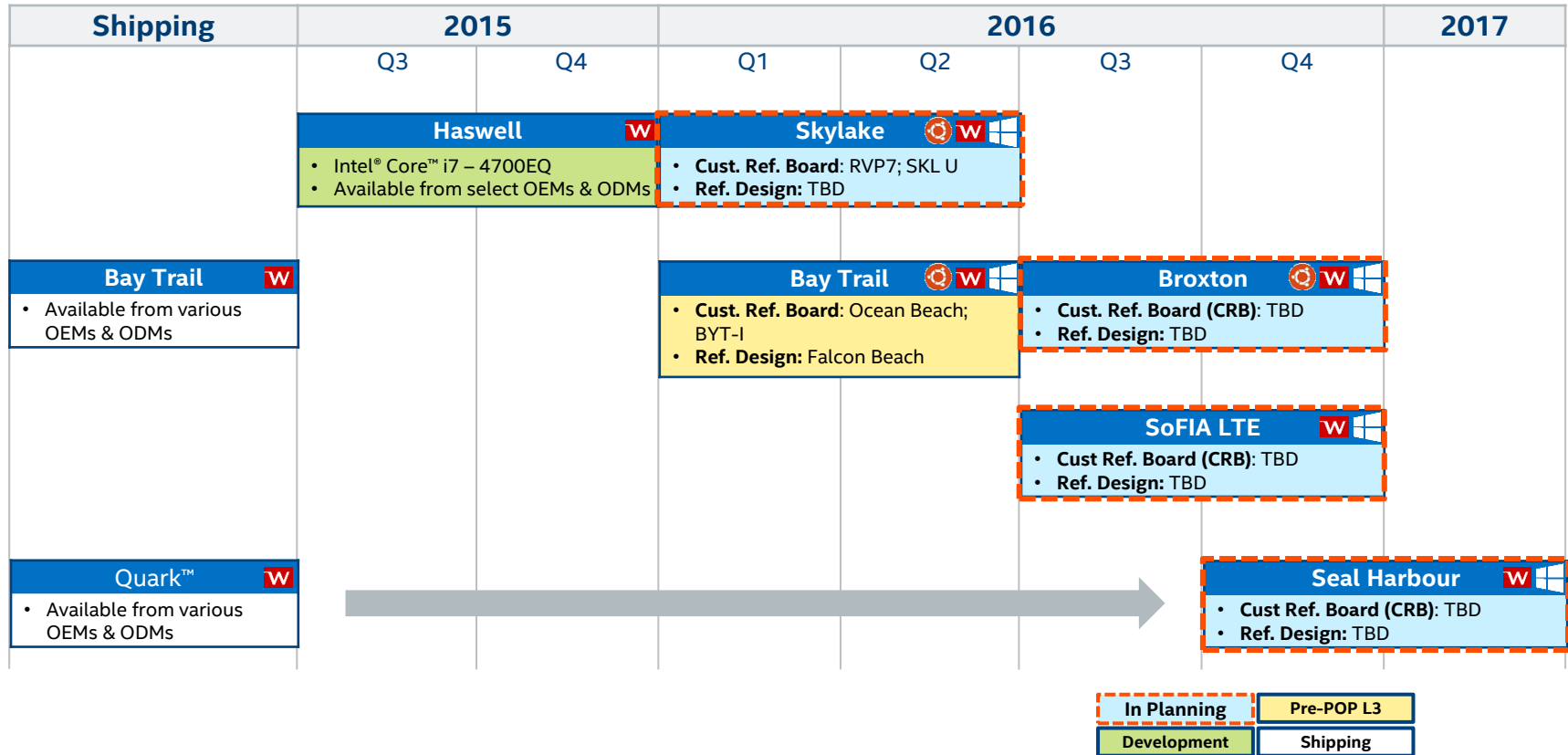
Shipping	2015		2016				2017
	Q3	Q4	Q1	Q2	Q3	Q4	

Haswell W
- Intel® Core™ i7 – 4700EQ
- Available from select OEMs & ODMs

Skylake
- **Cust. Ref. Board**: RVP7; SKL U
- **Ref. Design**: TBD

Bay Trail W
- Available from various OEMs & ODMs

Bay Trail
- **Cust. Ref. Board**: Ocean Beach; BYT-I
- **Ref. Design**: Falcon Beach

Broxton
- **Cust. Ref. Board (CRB)**: TBD
- **Ref. Design**: TBD

SoFIA LTE W
- **Cust Ref. Board (CRB)**: TBD
- **Ref. Design**: TBD

Quark™ W
- Available from various OEMs & ODMs

Seal Harbour W
- **Cust Ref. Board (CRB)**: TBD
- **Ref. Design**: TBD

In Planning	Pre-POP L3
Development	Shipping

LEFT edge of box indicates Target Production. All products, dates, and figures specified are based on current expectations and are subject to change without notice.

Intel Confidential

56

SUMMARY

A look at what we've covered and where to learn more

INTEL® IOT GATEWAY

- Gateways are the entryway to IoT value—providing insight at the edge, while filtering, aggregating, and sending data to the cloud.

- Intel® IoT Gateways provide essential, integrated security to protect data and devices.

- Intel® IoT Gateways are part of IoT solutions worldwide—increasing ROI and speeding time to insight.

- Intel® IoT Gateways provide developers and the ecosystem with the opportunity to accelerate time to market.

LEARN MORE

General Information:
www.intel.com/IoTgateways

Intel Embedded Design Center:
www.intel.com/gateways

Online Community Subspace:
http://embedded.communities.intel.com/
community/en

GET SUPPORT

Through August 31, 2015 Intel offers Web-based ticket support at no charge

- Submit a ticket with Intel® Premier Support: https://businessportal.intel.com

- For software issues, visit the Intel Knowledge Forum at https://ask.intel.Wind River.com

CASE STUDIES

For more, visit intel.com/iot/blueprints

CASE STUDY

Daikin | HVAC Supplier

Challenge

Daikin needed to integrate HVAC equipment with the building controls for real-time HVAC unit performance, remote diagnostics, and monitoring data.

Solution

Daikin uses Intel® IoT Gateway based on Intel® Atom™ processors to connect its Rebel* rooftop units to the cloud.

Secure data from the cloud

Works with legacy or new equipment

Intelligent gateways get to market sooner

Lower service costs. Focus on innovation and prevention.

Learn more: https://www-ssl.intel.com/content/www/us/en/internet-of-things/customer-stories/daikin-applied-transforms-hvac-systems.html

CASE STUDY

Port of San Diego | Energy Management

Challenge

Cleantech San Diego needed to optimize energy and water usage in commercial buildings.

Solution

Intel® IoT Gateway-based solution monitors HVAC, lighting, and plug-usage reduction.

Energy and cost savings

Reduced greenhouse gas emissions

Energy efficient monitoring. Control greenhouse gas emissions.

CASE STUDY

Malaysian Rice Fields | Irrigation Automation

Challenge

Monitor rice supplies and automate irrigation.

Solution

Abbaco Controls solution with Intel® IoT Gateways provides accurate, near-real-time water level status.

Rice supply self-sufficiency

Minimize manual intervention with automation

Monitoring for fast remote response via smart mobile devices

Increase agricultural sustainability. Automate essential monitoring.

Learn more: http://www.intel.com/content/www/us/en/internet-of-things/videos/abbaco-controls-uses-IoT-for-water-supply-management.html

CASE STUDY

中交兴路
TransWiseway

Chinese Government | Transportation

Challenge

Monitor vehicles and fleet management.

Solution

TransWiseway solution with Intel® IoT Gateways enables nationwide cloud platform for commercial vehicle-trace monitoring.

In-vehicle tablet and infrastructure
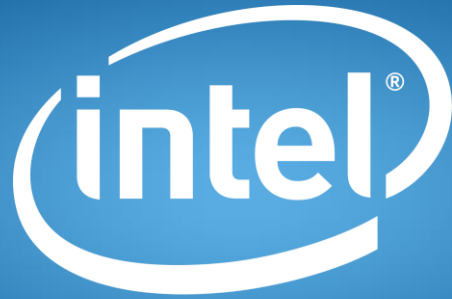
Reduces management costs

Enhanced user experience

Streamline public transportation system. Lower maintenance and management costs.

Learn more: http://www.intel.com/content/www/us/en/internet-of-things/blueprints/IoT-building-intelligent-transport-system-blueprint.html