WHITE PAPER
Internet of Things

Developing Solutions for the Internet of Things

Intel® products, solutions, and services are enabling secure and seamless solutions for the Internet of Things (IoT).

Introduction

The world is undergoing a dramatic transformation, rapidly transitioning from isolated systems to ubiquitous Internet-enabled 'things' capable of generating data that can be analyzed to extract valuable information. Commonly referred to as the Internet of Things (IoT), this new reality will enrich everyday life, increase business productivity, improve government efficiency, and the list goes on.

Intel is working with a large community of solution providers to develop IoT solutions for a wide range of organizations and businesses, including industrial, retail, automotive, energy, and healthcare industries. The solutions generate actionable information by running analytic software and services on data that moves between devices and the cloud in a manner that is always secure, manageable, and user-friendly.

Powering Business Transformation

Whether connecting a consumer wearable device, vehicle, or factory controller to the Internet, everyone wants it to be quick and seamless. This paper describes how Intel® products and technologies are helping make this a reality by providing fundamental building blocks for a robust ecosystem that is developing end-to-end IoT solutions.

Building Blocks for Thing to Cloud Innovation

The IoT vision is to create opportunities to transform businesses, people's lives, and the world in countless ways by enabling billions of systems across the globe to share and analyze data over the cloud. With these capabilities, IoT solutions can improve medical outcomes, create better products faster, lower development cost, make shopping more enjoyable, or optimize energy generation and consumption. Moving forward, nearly every device will need built-in, secure, interconnected intelligence. Similarly, the supporting network and cloud infrastructure must be enhanced to better protect data, manage devices, and perform data analytics.

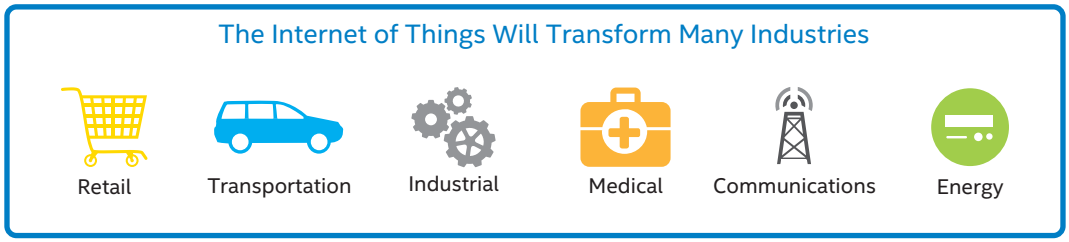

Table of Contents

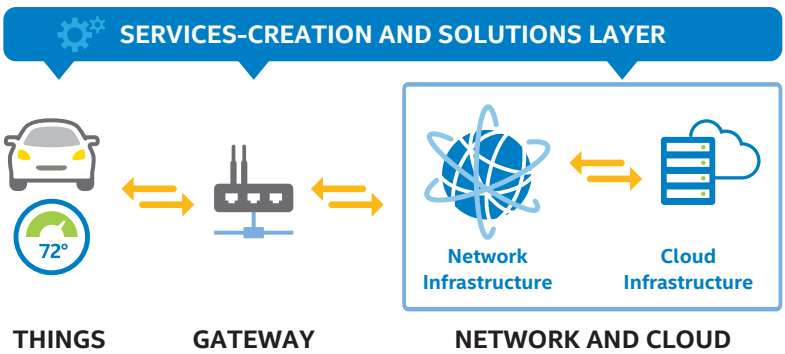

Figure 1. IoT Solutions Join Together a Wide Variety of Systems

IoT architecture can be simplistically represented by four categories of interconnected systems: things, gateways, network and cloud, and services-creation and solutions layers, as depicted in Figure 1. With extensive expertise spanning all these areas, Intel has a unique perspective on what is required to ensure reliable and secure bi-directional communication amongst these systems:

Things

Today there are billions of things found in commercial and industrial settings, in the home, and in the hands of mobile users. Already, cars, device sensors, wearables, and mobile phones are connecting directly through broadband wireless networks and accessing the Internet. An IoT solution requires things to either be intelligent so they can filter and manage data locally, or connect to gateways that provide this functionality.

Examples:

- **Mobile:** smart phones, tablets, GPS systems, wearables
- **Home:** security alarms, energy consumption monitors, lighting switches, thermostats
- **Industrial:** smart buildings, factory automation, energy grids, fleets

Gateways

A major barrier to realizing the full promise of IoT is that around 85 percent[1] of existing things were not designed to connect to the Internet and cannot share data with the cloud. Addressing this issue, gateways for mobile, home, and industrial act as intermediaries between legacy things and the cloud, providing the needed connectivity, security, and manageability.

Network and Cloud

Network Infrastructure: The Internet is a global system of interconnected IP networks that link computer systems together. This network infrastructure, comprising routers, aggregators, gateways, repeaters, and other devices that control data traffic flow, also connects to telecom and cable networks (e.g., 3G, 4G/LTE) operated by service providers.

Data Center / Cloud Infrastructure: Data centers and cloud infrastructure contain large pools of virtualized servers and storage that are networked together. Supporting IoT, this infrastructure runs applications that analyze data from devices and sensors in order to generate actionable information used for services and decision making.

Services-Creation and Solutions Layers

Getting to market faster and realizing the full value of IoT hinges on orchestrating the assembly and analysis of data from legacy systems and existing business assets. Helping provide this capability, Intel brought together industry-recognized leaders in application programming interface (API) management software, including:

- **Mashery*:** Pioneer of API management with a massive API developer community and marketplace
- **Aepona*:** Leading provider of API and monetization solutions for service providers

IoT Value Chain

As explained in the previous section, IoT touches a wide variety of systems, requiring the IoT ecosystem to deliver a broad assortment of capabilities, shown by the value chain in Figure 2. The circles contain relatively standard components, starting with *ingredients*, such as processors, modules, operating systems, and security software. Original design manufacturers (ODMs) use these components to build *boards* that end up in *devices* delivered by original equipment manufacturers (OEMs).

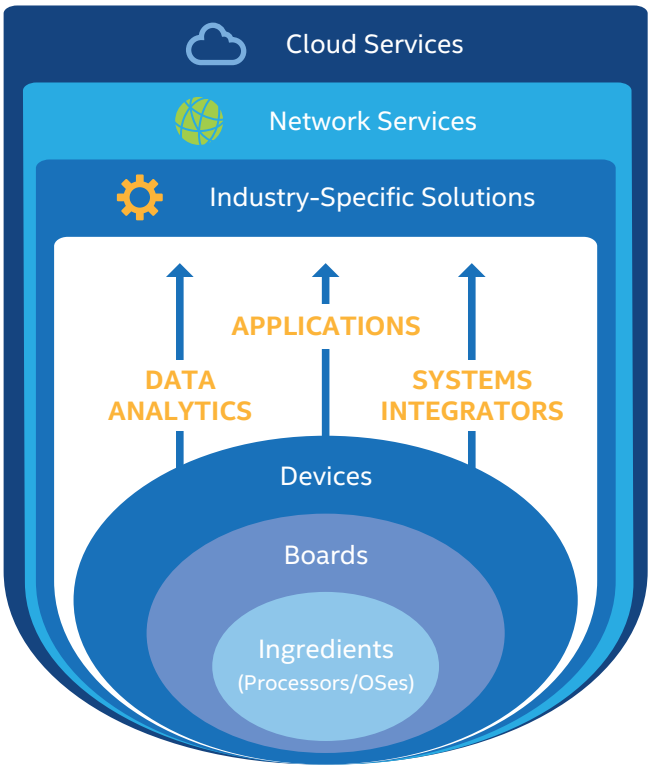

Figure 2. The IoT Value Chain Contains Many Types of Solution Providers

Next, these rather generic products are turned into industry-specific solutions when *systems integrators* incorporate *application and data analytics software*, among other specialty elements. *Network services*, like mobile broadband, provide the connectivity between devices and *cloud services*, which use analytics and application software to turn raw data into useful information.

The Intel product and technology portfolio provides ODMs, OEMs, systems integrators, application developers, and network and cloud service providers with fundamental capabilities for an end-to-end IoT solution, as described in the next four sections.

Explore the Intel ecosystem at every level of the IoT value chain.

Intel Building Blocks for Things

This section describes Intel solutions spanning processors, chipsets, operating systems, security solutions and network connectivity.

Processors and Chipsets

An end-to-end strategy requires making things more intelligent and secure so they can reliably filter and manage data locally. Analytics, encryption, and new application requirements drive the need for high levels of power-optimized performance.

Engineers designing things can choose from four families of Intel® processors based on backwards-compatible architecture that deliver scalable performance (Figure 3), ranging from the energy-efficient Intel® Quark™ SoC X1000 to high-performance Intel® Xeon® processors. Intel computing platforms span a broad range of price-performance points with a common set of code that works across processors.

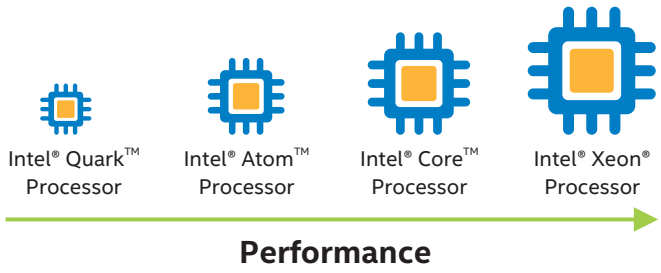

Figure 3. Intel Provides Unique Performance Scalability with Four Processor Families

- Intel Quark SoC X1000 is a family of low-power, system-on-chips (SoCs) that is ideal when lower power and size take priority over higher performance. These 32-bit, single-core Intel® architecture-compatible CPUs operate at speeds up to 400 MHz.
- Intel® Atom™ processor E3800 product family provides low power and thermally-efficient application performance in small form factor devices. The processors feature enhanced media and graphics performance, error correcting code, industrial temperature range, built-in security, and integrated image signal processing.

3

- Intel® Core™ processor product family delivers exceptional compute, graphics, and media performance, along with enhanced security and I/O flexibility. Designed for small form-factor applications, the 4th generation Intel Core processor (U-processor line), shown in Figure 4, uses a multi-chip package (MCP) that integrates a low-power CPU and platform controller hub (PCH) onto a common package substrate.

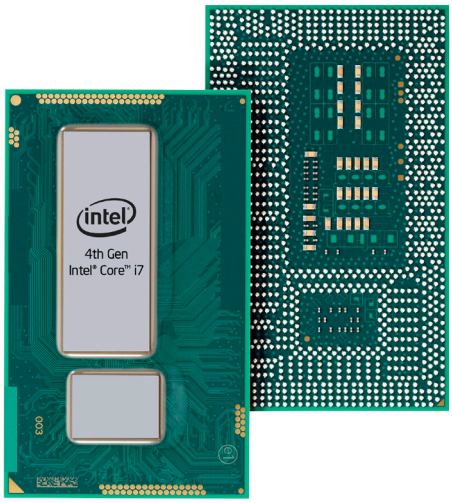

Figure 4. The Small Form Factor 4th Generation Intel® Core™ Processor Integrates CPU and Chipset in One Package

- Intel Xeon processors are designed for compute-intensive applications that demand the highest available performance, combining multi-core performance and exceptional compute density with hardware-based manageability, security, virtualization, and power management.

Operating Systems

Intel processors run a variety of operating systems from the Linux* community, Microsoft*, Google*, and the following offerings from Wind River*:

- *Wind River VxWorks** is the world's leading commercial real-time operating system (RTOS) and has been serving the needs of embedded systems of all shapes and sizes for more than 30 years.
- *Wind River Linux* is the leading commercial embedded Linux platform and the first to bring the advantages of open source without the risks to companies in all industries.
- *Wind River for Android** offers a portfolio of software and testing products to support rapid and high-quality platform and application development for devices running the Android operating system.

Learn more about Wind River operating systems.

Data and Things Security

Organizations are under increasing pressure to protect sensitive data, and prevent device theft and malware attacks. Global regulations protecting personally identifiable information (PII) are becoming more stringent and breaches more costly to organizations that fail to comply. In addition, valuable intellectual property (IP) that creates a competitive advantage is also at risk when data records or devices are stolen or accessed by unauthorized individuals.

The cybercrime community has never been busier, as seen in Figure 5 showing the McAfee* Labs "zoo" grew by 15 percent from the third to fourth quarter of 2014 and now contains more than 196 million unique malware samples.

The potentially large footprint of an end-to-end solution for IoT can increase an organization's exposure to security breaches. Helping to mitigate risk, Intel and its subsidiary, McAfee, offer a wide range of security products that can be deployed on devices, gateways, and network and cloud infrastructure, such as:

- *McAfee Embedded Control* maintains the integrity of devices, gateways, and servers by allowing only authorized code to run and authorized changes to be made. It automatically creates a dynamic whitelist of the "authorized code" on the system. Once the whitelist is created and enabled, the system is locked down to the

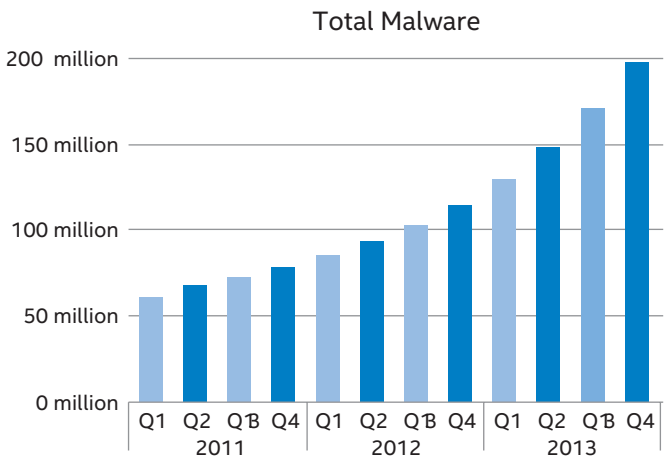

Figure 5. The Amount of Malware Increased More Than Three-Fold in Three Years
Source: McAfee* Labs Threats Report, Fourth Quarter 2013

known good baseline, no program or code outside the authorized set can run. Whitelisting helps to prevent viruses, spyware, worms (like the Stuxnet worm), and other malware from executing illegitimately on IoT systems.

- *McAfee ePolicy Orchestrator* (McAfee ePO*)* is one of the most advanced, extensible, and scalable centralized security management software in the industry. This open platform unifies security management, which may dramatically reduce the cost and complexity of security and compliance administration.
- *McAfee Integrity Control* combines McAfee Embedded Control and the McAfee ePolicy Orchestrator (McAfee ePO) console, enabling the product to provide integrated audit and compliance reports to help satisfy multiple compliance regulations.
- *McAfee Endpoint Encryption* is the cornerstone of data protection since it encrypts data throughout the IoT environment, including devices, gateways, network files and folders, removable media, and USB portable storage devices. The software employs Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)[2] implemented on Intel Core processors, allowing data encryption functions to run up to ten times (parallel mode)[3,4] without slowing down the system (Figure 6).

Learn more about McAfee security products and solutions.

- Intel® Identity Protection Technology (Intel® IPT)[5] helps prevent unauthorized access to data stored in the cloud using strong, hardware-based authentication. This tamper-proof solution operates in isolation from the operating system. It also provides a simple way for web sites and organizations to validate that a user is logging in from a trusted device.

Network Connectivity

The fundamental concept behind IoT is connecting the vast majority of systems in the world to a common network and infrastructure. Intel computing platforms and network interface cards support a wide range of networking interfaces and protocols to provide the necessary connectivity:

- Intel® Ethernet Controller I210 is a low-power, small-footprint, single-port gigabit LAN on motherboard (LOM) network controller with integrated MAC and PHY, making it perfect for small devices.
- Intel® XMM™ platforms are slim modems for 2G/3G/LTE support, enabling high-speed data and voice. They combine cost-optimized ICs, reference designs, and feature-rich software stacks with professional customer support throughout the value chain. Their small size based on a flexible, modular concept allows one design to satisfy various fields of applications, such as mobile phones, mobile computing, or telematics.

  For example, the Intel® XMM™ 7160 cellular platform is a slim modem for LTE smart phones, tablets, and machine-to-machine (M2M) applications. It is an extremely compact solution for LTE/DC-HSPA-connected devices destined for global markets, enabling high-speed data-only solutions as well as voice-capable 4G cellular phones.
- Intel® chipsets support a wide range of I/O interfaces, including Ethernet, USB, RS-232, RS-485, CAN, line out, PCI Express*, and SPI. These interfaces can also connect to modules supporting cellular, Bluetooth*, ZigBee*, Wi-Fi, and other wireless technologies.

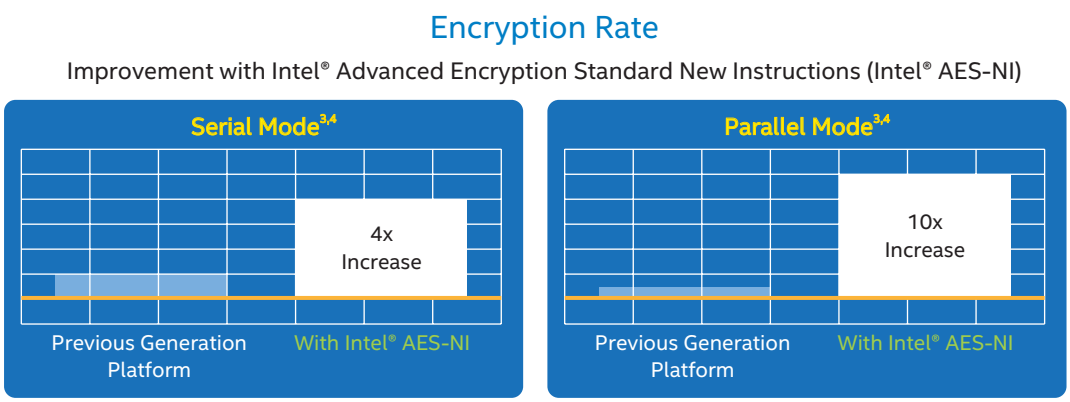

Figure 6. New Intel Instructions Dramatically Speed Up Encryption Rates

5

Intel Solutions for Gateways

Speeding up time to market, Intel® Gateway Solutions for the Internet of Things (Intel® Gateway Solutions for the IoT) helps equipment manufacturers develop, prototype, and deploy application services faster so companies can focus on adding new value-added services. These solutions provide equipment manufacturers with various platforms for developing gateways that securely aggregate, share, and filter data for analysis.

Intel Gateway Solutions for the IoT is built on open architecture to ensure interoperability between systems, facilitate wide application development, and simplify services deployment. Integrated and validated components (Figure 7) allow maximum flexibility, and fast application development and field deployment. The solutions offer complete, validated platforms consisting of hardware and software building blocks, including:

- Choice of Intel processors: Intel Quark SoC X1000, Intel® Quark™ SoC X1020, and Intel® Atom™ processor E3826
- Wind River Intelligent Device Platform development environment
- McAfee Embedded Control security technologies
- Wind River Intelligent Device Platform is a scalable, sustainable, and secure development environment that simplifies the development, integration, and deployment of gateways for IoT. Shown in Figure 8 on the next page, it provides networking stacks that support the protocols used by most IoT systems and enables equipment providers to build high-performance, high-value products that accelerate, analyze, and secure network traffic and applications. The platform is based on Wind River industry-leading operating systems, which are standards-compliant and fully tested, and includes Wind River development tools. The platform provides device security, smart connectivity, rich network options, and device management. Intelligent Device Platform includes ready-to-use components built exclusively for developing machine-to-machine (M2M) applications.

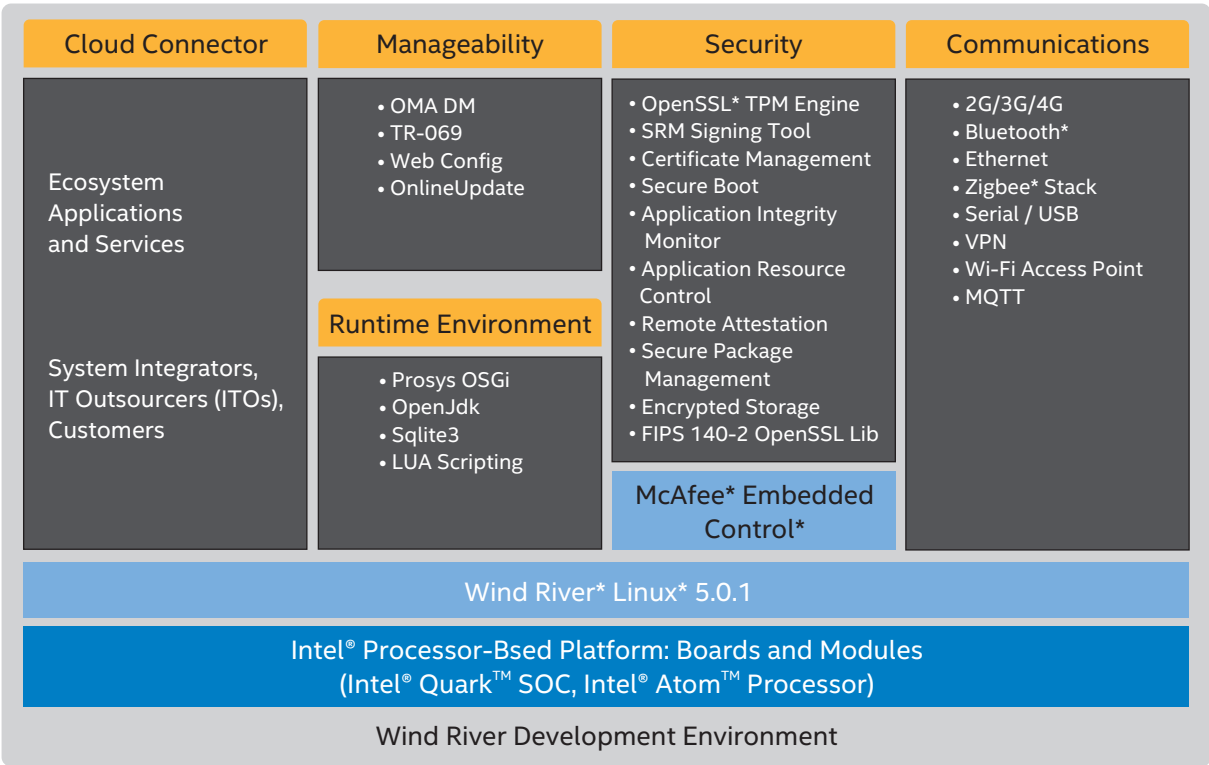

Figure 7. Gateway Software Stack

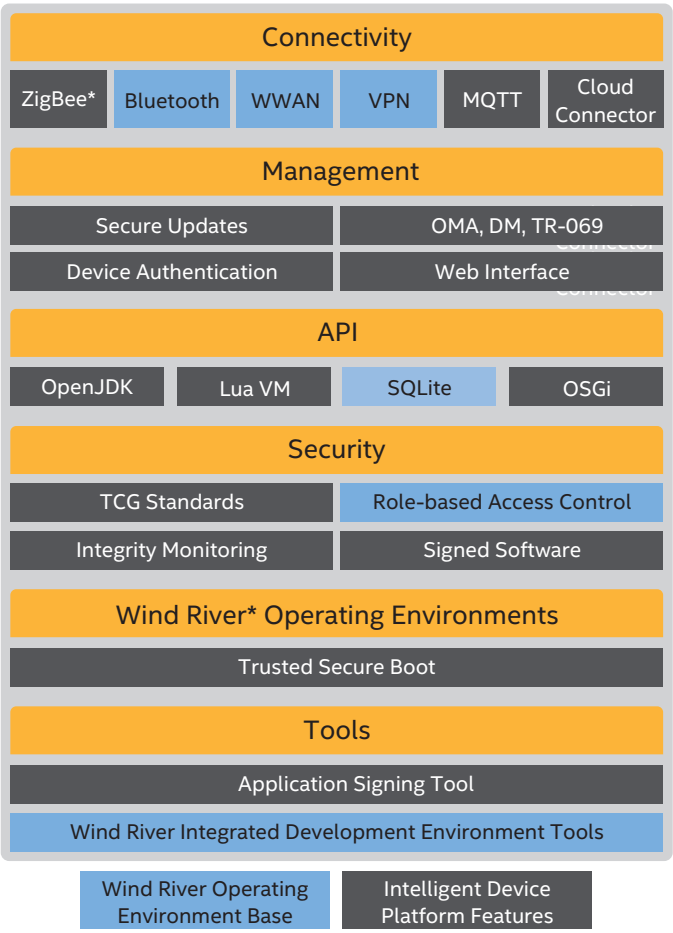

Figure 8. Wind River* Intelligent Device Platform Components

Key Features:

Gateway security: Delivers built-in security features designed to secure the communication channel, the data, and the end device.

Application enablement: Provides Lua, Java, and OSGi application environments to enable portable, scalable, and reusable application development on both resource-constrained and full-featured devices.

Device connectivity: Embraces IoT protocol MQTT for data transportation and native support for Wi-Fi, Bluetooth*, ZigBee, and short-range wireless protocols widely used in IoT devices.

Remote device management: Supports well-established management protocols such as TR-069 and OMA DM.

Intel Solutions for Network and Cloud

With the telecommunications industry transitioning to all-IP networks, equipment manufacturers started to blend the best of communications and computing technologies. Accelerating this trend, software-defined networking (SDN) and network functions virtualization (NFV) are making it easier to consolidate network, cloud, and data center functions onto standard, high-volume servers, switches, and storage.

Intel server technology is extensively used in network and cloud infrastructure to run a wide range of application and analytics workloads on virtualized servers. Connectivity that takes advantage of Intel-based servers, storage, and NICs is becoming increasingly more cost effective and pervasive across both wired and wireless networks. As the telecom industry joins enterprise and cloud industries in deploying all-IP networks, Intel solutions are used in the control and data plane to facilitate localization, security, APIs, and protocols in support of software-defined infrastructure.

At the forefront of developing, securing, and managing network and cloud infrastructure, Intel offers processors, operating systems, development platforms, security solutions, data center management tools, and high-throughput network connectivity.

Computing Platforms and Operating Systems

Computing platforms in the network and cloud are expected to deliver the highest level of performance and availability, and Intel provides technologies and products to make this possible, including:

- Intel® Platform for Communications Infrastructure is designed to simultaneously run diverse workloads (e.g., packet processing, control plane, and application software) to offer an exceptional level of workload consolidation. This software-focused platform features built-in security and compression engines, and accelerated packet processing.
- Carrier Grade Profile for Wind River Linux is the first product to meet the registration requirements of the Linux Foundation's Carrier Grade Linux 5.0 specification built for a Yocto Project* compatible product. This turnkey solution provides essential capabilities for all industries, enabling the next generation of embedded Linux designs that require secure, standards-based, reliable solutions.

7

Development Platforms

Offering easy access to recommended open source and Intel® components, the following development platforms assist developers in prototyping designs, conducting performance evaluations, porting application software, and ultimately delivering production-ready solutions.

- The Intel® Open Network Platform (Intel® ONP) is supported by both Server and Switch Reference Designs, and gives equipment manufacturers a quick development path to high-performance, low-latency switching in either virtualized or hardware-based network appliances. These SDN-compliant designs are flexible and powerful, and support enhanced features critical for today's networking and data center switching environments.

  Intel® Open Network Platform Server Reference Design (Intel® ONP Server Reference Design), diagramed in Figure 9, runs on nearly any Intel Xeon or Intel Core processor-based hardware platform. The KVM hypervisor[6] and Intel® Virtualization Technology (Intel® VT)[7] provide a high-performance and robust virtualization environment.

  A version of Open vSwitch, accelerated by the Intel® Data Plane Development Kit (Intel® DPDK), runs in one or more virtual machines. In addition, optimizations will be provided to facilitate remote management and integration into the orchestration infrastructure. For some workloads, the use of PCI-SIG Single Root I/O Virtualization (SR-IOV) could be used to provide for virtual appliances.

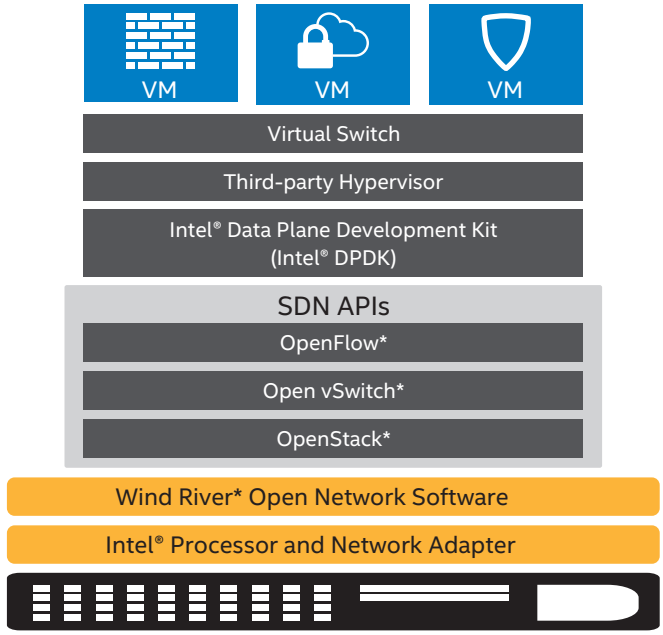

Figure 9. Reference Design

- Wind River Intelligent Network Platform is an integrated and optimized software system that consists of the critical run-time components and life cycle development tools needed to build high-performance, next-generation intelligent network elements. Figure 10 shows the pre-integration of two essential deep packet inspection technologies: IP flow analysis to provide application and content awareness, and regular expression pattern matching to detect malware.

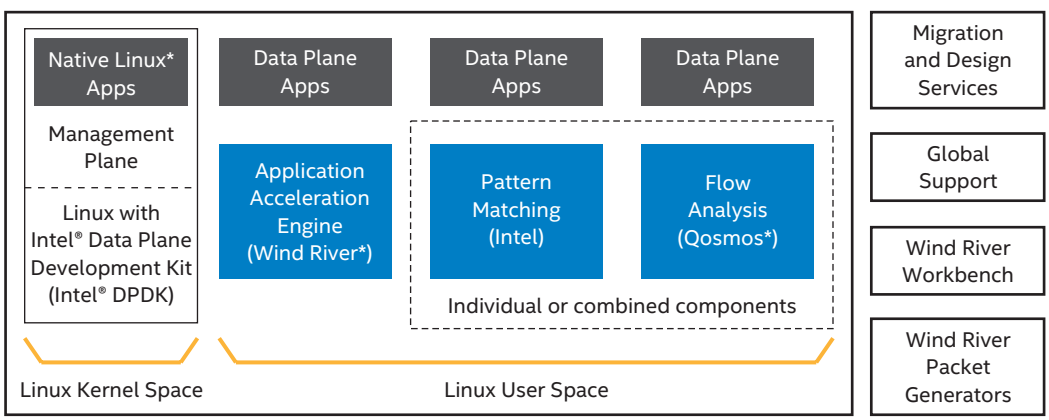

Figure 10. Key Components of Wind River* Intelligent Network Platform

- *Qosmos* ixEngine:* Performing IP flow classification, this set of software libraries and tools enables deep visibility into Layers 4–7 traffic flows, facilitating real-time packet classification, traffic categorization, and communication protocol identification, among other network applications. This information, the product of granular application and data visibility, greatly increases network operators' context awareness, allowing them to better execute security rules and manage traffic. The solution performs pattern matching, flow correlation, and behavior analysis on traffic flows using an application/protocol signature database containing thousands of dynamic protocols, which are regularly updated from live network analysis.
- *HyperScan from Intel:* Executing regular expression pattern matching, this engine scans large amounts of data at high speed searching for malware. The engine accesses a database with hundreds of thousands of static signatures used to detect viruses inside documents, making it ideal for systems requiring intrusion prevention (IPS), antivirus (AV), and unified threat management (UTM). While Hyperscan is a plug-in for ixEngine and for INP, it is also a standalone, high-performance matching engine that supports most industry pattern databases.

  Key Features:

  Consolidated management and data plane: Can lower BOM cost and energy consumption by integrating two workloads that typically require separate computing systems.

  Packet acceleration and throughput: Achieves significant performance gains in IP forwarding, and UDP and TCP termination.[8]

  Application acceleration engine: Provides a comprehensive, optimized network stack designed for the acceleration of Layer 3 and 4 network protocols.

  Deep packet inspection: Identifies traffic flows, communication protocols, and applications.

Network Element Security

- McAfee Network Security Platform uses advanced threat detection techniques to discover and block sophisticated threats in the network, making it ideal for next-generation intrusion prevention, with key features shown in Figure 11. This uniquely intelligent security solution moves beyond mere pattern matching to defend against stealthy attacks with extreme accuracy, while its next-generation hardware platform scales to speeds of over 80 Gbps[9] to meet the needs of demanding networks.

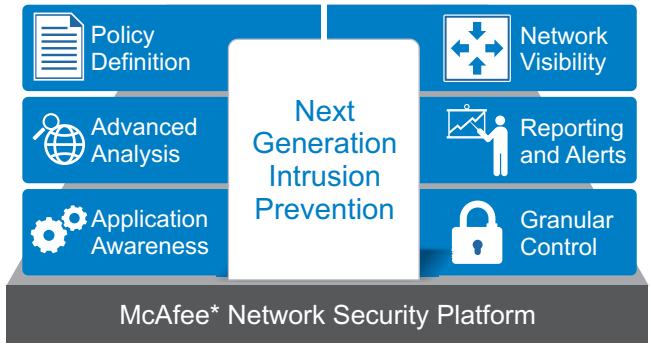

Figure 11. McAfee* Network Security Platform

Data Center Management

- Intel® Datacenter Manager (Intel® DCM) Portfolio provides critical management capabilities for today's data centers. With the Intel DCM Portfolio, IT and facility managers have the tools to improve manageability, increase availability, and reduce costs across key parameters, such as energy usage, monitoring, security, automation, and cloud. This multifunction solution provides key data center capabilities, including:
  - Energy director
  - Virtual keyboard-video-mouse (KVM)
  - Device management API
  - Service-level agreement enforcement
  - Plug-in for the OpenStack*

Network Connectivity

- Intel® 82599 10 Gigabit Ethernet Controller Family is Intel's third-generation 10 GbE controller, which continues to build on the innovative trends set by its predecessor. The Intel 82599 10 Gigabit Ethernet controller is a single-chip, dual-port 10 GbE implementation. It can reduce bill of materials (BOM) cost and design complexity by integrating serial 10 GbE PHYs and provides both simple firmware interface (SFI) and KR interface. The device is designed for high performance and lower memory latency.

Services-Creation and Solutions Layers

In order to fulfill the promise of IoT, data collected by devices and gateways needs to be sent to existing back-end systems, fused with other data sources, and made available to partners, customers, and employees. This can be achieved with application programming interface (API) management.

9

Exposing and Managing Data to Enable New Services

End-to-end IoT solutions need a control layer to not only collect data from things, but also orchestrate key IoT processes and core software modules. This services "platform" layer is the foundation for value-added IoT service creation for vertical industries or for unique IoT business models. The platform must have visibility and interoperability with all other layers of an IoT deployment across hardware, gateways, networks, analytics, and security in order to control all resources.

Management and control must be adaptable to translate information from legacy things and plug in value-added ecosystem components that monetize IoT and track newfound business value. IoT requires flexibility and cannot be based on a single set of standards or implemented entirely from a single vendor's software stack.

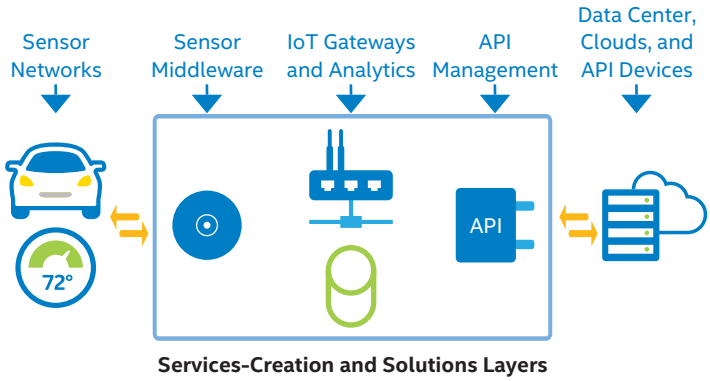

Figure 12. Conceptual Architecture for API Management and IoT

API Management Holds the Key for IoT[10]

Today, a large part of the interoperability, scale, and control for IoT can be achieved through API management. Standards-based design patterns for Web APIs, API management, and a RESTful architecture provide tremendous value in simplifying the task of interoperability across heterogeneous systems handling vast amounts of data. Since APIs have become ubiquitous, IoT deployments spanning a wide range of market segments can benefit from this proven architecture.

APIs lower the barrier to entry for connectedness and enable secure communication from things to applications located just about anywhere – in any cloud, data center, or accessible from API-enabled devices.

Figure 12 shows where sensor middleware and API management for IoT gateway solutions play an important role: they provide data fusion, contextual information, data communication, coordination and synchronization, data and protocol interoperability, privacy and security, and fault tolerance.

A Platform Approach to IoT Management and Control

Intel has assembled interoperable core software and service capabilities as a foundation for IoT based on API management that can help businesses, integrators, and the larger IoT ecosystem jumpstart their IoT deployments. This foundation provides IoT management and control through the implementation of services-creation and vertical solutions layers, as depicted in Figure 13.

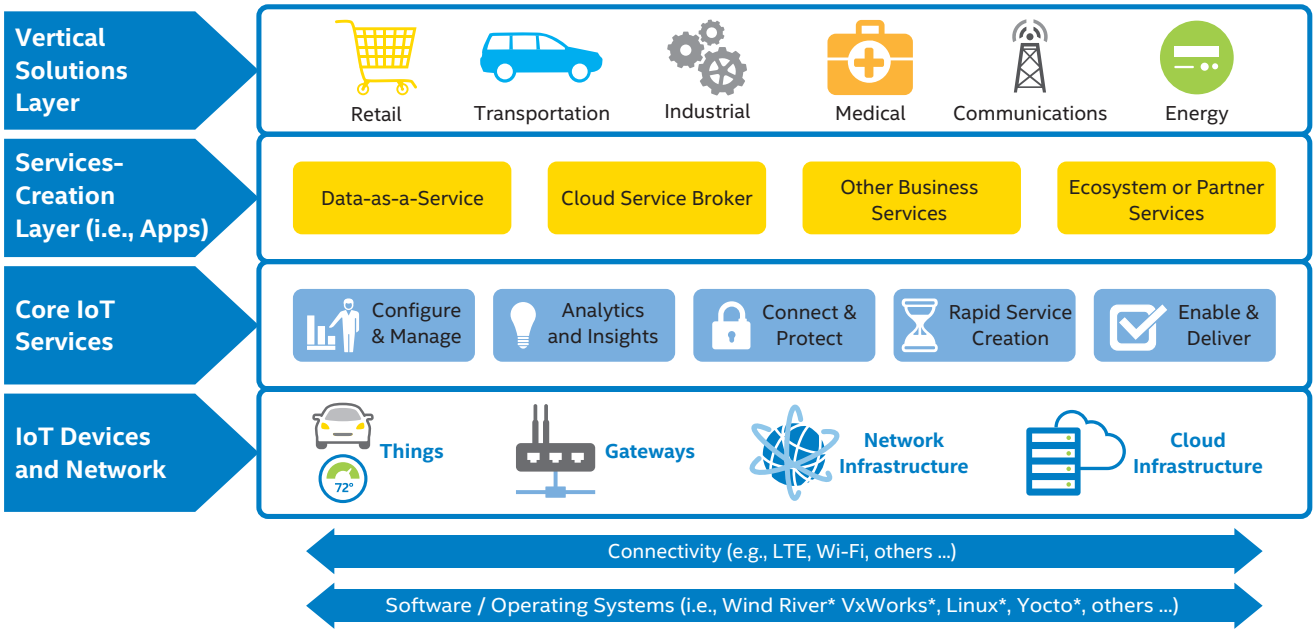

Figure 13. Creating Value-Added IoT Services and Solutions

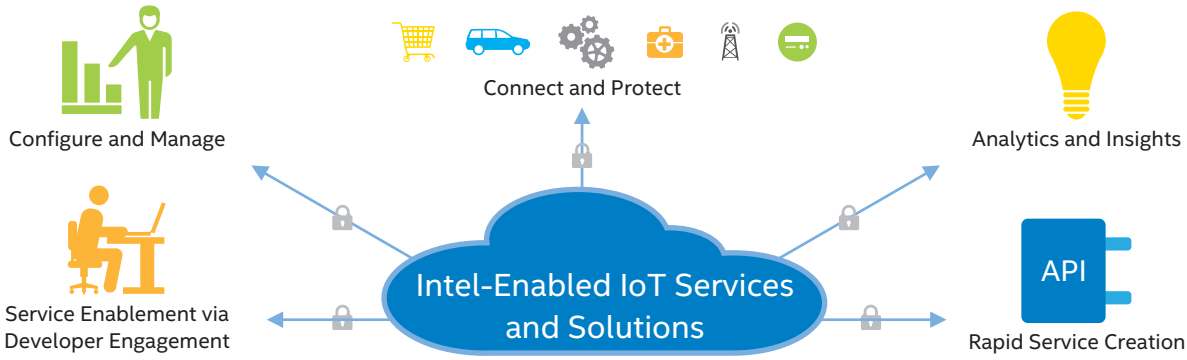

Figure 14. The Foundation for Connected IoT

In order to realize true value for IoT, businesses should focus on the value-added services they can assemble from data derived from IoT and how they can combine this data with their legacy systems and business assets. It is this data mashup that is happening across verticals and where true innovation for IoT is occurring. Any number of unique IoT business strategies and go-to-market business models can be empowered, whether they are internal, external, mobile, or channel partner focused.

Intel is delivering the core IoT software layer to help orchestrate the assembly of finished vertical solutions. This layer supports Intel-enabled IoT services and solutions with the following features:

- Secure end-to-end communications from thing to cloud
- Connected and globally scalable end-to-end solutions
- Remote manageability
- Interoperability across platforms
- Intel® architecture processor-optimized performance
- Intelligent data analytics

This core IoT software layer creates a foundation for connected IoT (Figure 14) by providing the following capabilities:

Connect and Protect – Securely connect and remotely manage things with real-time gateway control using secure APIs to foster interoperability.

Configure and Manage - Remotely manage complete solutions from edge to data center with a consistent user experience.

Data Services and Analytics – Securely transmit, store, and analyze big data using world-class data center technology, while utilizing intelligent algorithms at the edge to optimize performance.

Service Enablement via Developer Engagement – Unlock the power of community innovation for IoT by proactively engaging developers though developer outreach and API portals.

Rapid Service Creation – Quickly and easily enable process integration, mash-up IoT API data with existing systems, and broker APIs with partners, all through API creation and management.

API Management Solutions for IOT

Intel's solutions and services offerings can be mixed and matched to suit specific IoT deployment and usage models.

API Management – Manage and package APIs through a software as a service (SaaS), on-premise portal, as well as enforce traffic from things and analyze API metrics. The solution empowers developers to discover, interact, and test APIs, thereby speeding up IoT application creation.

API Security and Brokerage - Simplify partner and open API programs with mobile-friendly OAuth, API key management, developer on-boarding/access, and a PCI-certified SaaS environment. As needed, apply enterprise-level security mechanisms, such as API, threat protection, identity system integration, and brokering across security domains.

11

Tokenization Broker - Ensure privacy and security of IoT data payloads, like personally identifiable information (PII), with a broker that acts as a proxy between things and back-end data center applications that process IoT data streams.

API Creation and Monetization - Create and publish APIs to partners and end customers that deeply integrate sensor data, business processes, networks, and legacy systems. For payment and settlement, instrument APIs to support various billing, business, and payment network models.

API Go-to-Market Services – Get help from IoT and API experts when developing business cases, partner strategies, and go-to-market plans. Launch APIs to the largest marketplace of 245 thousand active developers and 86 thousand active applications.

The Internet of Things Starts with Intelligence Inside

Emerging end-to-end solutions for IoT will allow individuals, businesses, and governments to collect, analyze, and derive meaning from data in ways that improve people's lives and boost the bottom line for organizations. Helping to make this a reality, Intel's extensive portfolio of open and scalable solutions makes it easier to connect, protect, and manage devices. With expertise in systems across the entire IoT architecture – things, gateways, network and cloud, and services-creation and solutions layers – Intel is accelerating business transformation.

For more information about Intel solutions for IoT, visit **www.intel.com/iot**.

[1] Source: IMS Research.

[2] Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) requires a computer system with an Intel AES-NI-enabled processors, as well as non-Intel® software to execute the instructions in the correct sequence. Intel AES-NI is available on select Intel® Core™ processors. For availability, consult your system manufacturer. For more information, visit **http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni**.

[3] Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

Note: The below disclaimer should be included whenever the general performance disclaimer is used, but should be numbered separately:

Configurations: [describe config + what test used + who did testing]. For more information go to **http://www.intel.com/performance**.

[4] For benchmark test and configuration information, please see the white paper at: **http://software.intel.com/sites/default/files/m/d/4/1/d/8/10TB24_Breakthrough_AES_Performance_with_Intel_AES_New_Instructions.final.secure.pdf**.

[5] No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology (Intel® IPT)–enabled system, including a 2nd or higher generation Intel® Core™ processor, an enabled chipset, firmware, software, and participating web site. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit **http://ipt.intel.com**.

[6] See **www.linux-kvm.org** for more information.

[7] Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM), and for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[8] For performance and test information, see the white paper at **http://www.intel.com/content/www/us/en/communications/communications-packet-processing-brief.html**.

[9] For additional performance information, see the product brief at **http://www.mcafee.com/us/resources/data-sheets/ds-network-security-platform-m-series.pdf**.

[10] Source: **https://blogs.intel.com/application-security/2013/10/08/api-management-for-the-internet-of-things-iot/**.

*Other names and brands may be claimed as the property of others.

Printed in USA 0514/VF/TM/PDF Please Recycle 330562-001US