By 2020, more than 200 billion devices will be connected to the cloud and each other in what is commonly called the Internet of Things (IoT). Connectivity is imperative to realizing the power of the IoT, which can allow gaining insight from data provided by these connected devices.

There’s a large amount of legacy equipment that is not connected, managed, or secured. That leaves a lot of useful data locked away in a massive array of equipment, like HVAC units, vending machines, and much more. Thus, there is a definite need to address interoperability of legacy systems in order to avoid the incredibly large cost of replacing all existing infrastructure with next generation equipment that can securely connect to the Internet.

Today’s industrial devices and other systems are often designed with interconnectivity and the ability to share data. Intel® Gateway Solutions for the Internet of Things (IoT) is a family of platforms that enables companies to seamlessly interconnect industrial infrastructure devices and secure data flow between devices and the cloud. Intel Gateway Solutions for IoT enables customers to securely aggregate, share, and filter data for analysis. It helps ensure federated data generated by devices and systems can travel securely and safely from the edge to the cloud and back—without replacing existing infrastructure. This new availability of previously hidden data can be valuable to a wide range of businesses and organizations:

- Operators, such as building maintenance personnel, can track real-time operations of various systems and optimize them for particular times of day, types of work, etc.
- Managers, such as property owners and business managers, can correlate data across entire holdings and analyze and optimize the cost of systems operations.
- Manufacturers and service agencies can analyze real-time and trended data from systems to optimize them for power efficiency, performance, operational life, and more.
- Governments and researchers can perform larger analyses on data from seemingly disparate but related systems to correlate impacts and effects of these systems on each other.
**Intel® Gateway Solutions for the Internet of Things (IoT)**

The Intel Gateway Solutions for IoT offers companies a key building block to enable the connectivity of legacy industrial devices and next generation intelligent infrastructure to the IoT. It integrates technologies and protocols for networking, embedded control, enterprise-grade security, and easy manageability on which application-specific software can run.

The Intel Gateway Solutions for IoT enables:
- Connectivity up to the cloud and enterprises.
- Connectivity down to sensors and existing controllers embedded in the system.
- Pre-process filtering of selected data for delivery.
- Local decision making, enabling easy connectivity to legacy systems.
- A hardware root of trust, data encryption, and software lockdown for security.
- Local computing for in-device analytics.

**An Integrated, Pre-Validated, and Complete Solution**

The Intel Gateway Solutions for IoT offers a proven solution—pre-validated on industry-leading software—that delivers an application-ready platform. The solution includes:
- Choice of Intel® processors for the development kits: Intel® Quark™ SoC X1000, Intel® Quark™ SoC X1020D and Intel® Atom™ processor E3826
- Wind River* Intelligent Device Platform XT development environment
- McAfee Embedded Control*

The Intel Gateway Solutions for IoT are built on open architecture to ensure interoperability between systems, enable wide application development, and allow easy services deployment. Integrated and validated components allow maximum flexibility and fast application development and deployment to the field.

---

**Figure 1. Addressing Endless Use Cases.**

**Figure 2. Intel® Gateway Solutions for IoT Software Stack.**
Wind River* Intelligent Device Platform XT

Connectivity, manageability, and security are core building blocks to IoT. Intelligent Device Platform XT provides an integrated, pre-validated stack of software, drivers for a wide range of hardware components, libraries, and tools to support these core services. The software enables flexibility for developers to quickly build enterprise-grade intelligent systems for a large number of applications. Intelligent Device Platform XT supports the following:

- **Manageability** – Intelligent Device Platform XT enables long-term secure remote manageability to simplify deployment, maintenance, and management of remote devices. The software supports industry-standard interfaces, including Open Management Alliance Device Management (OMA DM), Technical Report 069 (TR-069), and web-based configuration interfaces.

- **Communications and Connectivity** – To enable connectivity over the widest range of communications technologies, Intelligent Device Platform XT supports both wireless and wired links. The software includes drivers for a number of hardware vendors’ products and software to support Cellular 2G/3G/4G, Bluetooth*, Serial, USB, Virtual Private Network (VPN), Wi-Fi* Access Point, the MQ Telemetry Transport (MQTT) messaging protocol, and ZigBee*.

- **Security** – Intelligent Device Platform XT provides strong support for secure image, secure data, and secure management, helping protect the device and data from boot to operations and management. The software supports comprehensive device protection, from a hardware root of trust through boot and software loading, and offers a wide array of protocols and services, including secure boot, whitelisting with McAfee Embedded Control, secure storage, and more.

- **Runtime Environments** – Intelligent Device Platform XT supports applications written in a variety of environments, including Lua*, Java*, and OSGi*, to enable portable, scalable, and reusable application development for solutions based on the Intel Gateway Solutions for IoT platform.

Intelligent Device Platform XT provides the foundation for fast development of intelligent system solutions on industry-standards using a proven software stack.

McAfee Embedded Control*

Integrated with the Intel Gateway Solutions for IoT platform, McAfee Embedded Control maintains system integrity by allowing only authorized code to run (application whitelisting) and only authorized changes to be made (change control). It simultaneously protects embedded system integrity and automates the enforcement of software change control policies.

**Application Whitelisting**
The software automatically creates a dynamic whitelist of the allowed code on the platform. Once the whitelist is created and enabled, the system is locked down to the known good baseline; no program or code outside the authorized set can run, and no unauthorized changes can be made. McAfee Embedded Control shields applications and related binaries at the kernel level—protecting files on disk or in memory, helping prevent malware and zero-day exploits, and minimize the need to patch the environment.

**Change Control**
McAfee Embedded Control only allows policy-based changes that are expected and authorized. The software monitors files and prevents unexpected changes while logging any attempts. It provides complete visibility and accountability through the automated, continuous collection of audit data. Using the data collected by McAfee Embedded Control, one can verify that no changes have been made to critical system files, directories, or registries, and then report these findings to regulatory officials to help meet compliance requirements.

**Endless Potential for Industry and Business**

Designed to securely connect edge devices to the cloud, the Intel Gateway Solutions for IoT is ideal for a vast array of applications including, building automation, industrial automation, and smart city infrastructure, and much more. By capturing and analyzing data...
from new sources, it gives management, service businesses, product manufacturers, and their ecosystems new opportunities for accelerating business innovation, understanding the behavior and uses of their existing products, and a foundation for designing new products for the marketplace.

Intel Gateway Solutions for IoT
Key Benefits
- Delivers an integrated, pre-validated, and flexible open-compute gateway platform, including foundational hardware, software, and security building blocks to allow fast solution development and deployment.
- Enables building scalable solutions with standards-based interfaces to securely connect and aggregate data from the edge to the cloud.
- Enables business innovation on proven technologies across compute, communications, manageability, and security.

<table>
<thead>
<tr>
<th>TARGET MARKETS</th>
<th>DK50 SERIES</th>
<th>DK100 SERIES</th>
<th>DK200 SERIES</th>
<th>DK300 SERIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers, Enthusiasts</td>
<td>Intel® Quark™ SoC X1000</td>
<td>Wind River Linux® (Host), Wind River® Intelligent Device Platform XT, Wind River Workbench, McAfee Embedded Control*</td>
<td>Intel® Quark™ SoC X1020D</td>
<td>Intel® Atom® Processor E3826</td>
</tr>
<tr>
<td>Industrial, Energy</td>
<td>Wind River Linux® (Host), Wind River® Intelligent Device Platform XT, Wind River Workbench, McAfee Embedded Control*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SOFTWARE
- Non-production, 6 Month SW License includes, Wind River Linux® (Host), Wind River® Intelligent Device Platform XT, Wind River Workbench, McAfee Embedded Control*

SECURITY*
- Open SSL* Library, McAfee Embedded Control*

MANAGEABILITY AND PROVISIONING
- OMA DM, TR-069, Web-based configuration interfaces

COMMUNICATIONS AND CONNECTIVITY
- Serial, USB, VPN, MQTT

RUNTIME ENVIRONMENTS
- Java, OSGi

I/O
- Ethernet* 10/100, USB 2.0 host & device, RS-232, full PCIe* mini card slot, UART 5V/3.3V, SPI for Arduino shield, 12C, 14 digital I/O pins, 12-bit 8 channel ADC

MEMORY AND STORAGE
- 512KB SRAM; 256MB DDR3, on-board microSD card

For more information, visit intel.com/iotgates

Figure 3:

Table adapted from page 3 of the document.