

Seamless Edge-to-Cloud IoT Integration Speeds Time to Market

Solution providers achieve end-to-end integration, deliver actionable customer insights, and gain a competitive advantage with the Intel® IoT Platform and Google Cloud Platform*

A fully integrated edge-to-cloud IoT infrastructure solution can help improve business insights that provide a true competitive advantage.



Executive Summary

Organizations that rely on the Internet of Things (IoT) for critical business processes are looking for ways to merge data silos, reduce security risks, and eliminate duplicate infrastructure. A fully integrated edge-to-cloud IoT infrastructure solution can help improve business insights that provide a true competitive advantage. But implementing such a solution can be complex; organizations need a planned approach to help the transition run smoothly.

Intel and Google have worked together to deliver a standards-based approach to help IoT developers, OEMs, independent software vendors (ISVs), and system integrators (SI) develop seamless solutions. With a joint reference architecture built on the Intel® Internet of Things (Intel® IoT) Platform and the Google Cloud Platform* (GCP*), IoT providers can gain the following capabilities and benefits:

- **Seamless data ingestion.** With a standards-based reference architecture, data is easier to collect and devices are easier to control.
- **End-to-end security.** The architecture is designed to protect device hardware.
- **Easy device onboarding.** New devices can be automatically provisioned to platforms, providing security.
- **Robust scalability.** With Intel and Google technologies, organizations can scale rapidly on demand.
- **Better insights.** GCP's analytics infrastructure with Intel's analytics-at-the-edge capabilities can provide better insights for faster decision making, quicker time-to-market, and the opportunity to provide new services and solutions.

The Intel® IoT Platform and GCP joint reference architecture provides a comprehensive approach for connecting the device layer to the network layer and into the cloud.



Figure 1. The joint Intel and Google reference architecture makes connecting the Internet of Things (IoT) from edge-to-cloud easier, with a focus on security at every layer.

Table of Contents

Executive Summary	1
Introduction	2
Solution Architecture	2
Solution Overview and Benefits	2
Solution Architecture Details	4
Implementation Overview	5
Onboarding Devices	5
Collecting and Integrating Data	5
Managing Devices and Software Updates	5
Summary	6
Appendix A: Logistics and Asset Management Use Case	6

Introduction

The Internet of Things (IoT) is speeding data collection from connected devices and sensors, resulting in an explosion of new devices and sensors that are generating massive volumes of data. This data can help organizations make smarter decisions and bring new products and services to market faster. Gartner Research estimates that by 2020, 25 billion enterprise-owned Internet-connected things across the globe stand to generate up to USD 2 trillion in economic benefit.¹ This presents tremendous opportunities for IoT solution providers, but developing an edge-to-cloud solution can be complex.

The technical challenges of IoT implementations often come from multiple IoT solutions dedicated to a variety of use cases within a single organization. These use cases can include monitoring chemical levels in manufacturing processes, occupancy-dependent lighting in offices, and retail security cameras, or monitoring available parking. Multiple implementations also lead to a lack of interoperability between devices and equipment from different manufacturers. Successful IoT solutions require a deep understanding of infrastructure, security, integration, and interoperability from edge to cloud. Although IoT implementations can be complex, organizations and solution providers can eliminate much of the complexity and meet the growing IoT demand with integrated IoT solutions from Intel and Google.

Solution Architecture

The Intel® Internet of Things (Intel® IoT) Platform and the Google Cloud Platform* (GCP*) each provide capabilities and benefits that help IoT developers, OEMs, independent software vendors (ISVs), and system integrators (SIs) develop industry-standard, seamless solutions.

Solution Overview and Benefits

Together, the Intel IoT and GCP joint reference architecture seamlessly transmits data from sensors, actuators, and other endpoint devices to the Google* cloud. A clearly defined, standard reference architecture that details edge, network, and cloud components provides the following:

- **Seamless data ingestion and device control** for improved interoperability.
- **Robust security** for end-to-end data and device protection.
- **Automated onboarding** for simplified deployment of security-enabled devices.
- **Robust scalability** with cloud-based infrastructure.
- **Customer insights** through GCP's analytics infrastructure.
- **Data monetization** through additional services and applications.

This joint reference architecture discusses:

- **Intel IoT Platform.** This illustrates the edge components, hardware security, and processors, as well as device provisioning, monitoring, and control.
- **Google Cloud Platform (GCP).** This illustrates the cloud services, including data ingestion, flow, storage, and analytics.

The joint reference architecture is followed by an implementation overview, as well as a logistics and asset management use case example in [Appendix A: Logistics and Asset Management Use Case](#).

Intel Internet of Things (Intel IoT) Platform

The Intel IoT Platform (Figure 2) includes a family of Intel® products. This ecosystem provides a foundation for easily connecting devices and delivering trusted data to the cloud. The benefits include:

- **A broad array of devices.** Intel's ecosystem of original device manufacturers (ODMs) offers a wide range of devices and sensors built on Intel® technology.
- **Security-focused solutions.** Intel technology is designed for increased security at every layer, and includes seamless device preconfiguration capabilities.
- **Enhanced registration and management.** With Wind River Helix Device Cloud*, device management and updates are seamlessly controlled from a central point in the cloud.

Google Cloud Platform (GCP)

GCP provides a security-enabled, cost-effective, and high-performance infrastructure in the cloud hosted through Google's globally distributed data centers (Figure 3). Managed services provide access to this infrastructure for an overall solution. The benefits include:

- **Fully managed services.** Google manages the setup and maintenance of the overall private infrastructure so customers can focus on building solutions.
- **Integrated development experience.** GCP provides a wide range of services for an integrated, end-to-end developer experience.
- **Full control of the environment.** Developers have full control of their computing environment, from data ingestion to presentation, through APIs in multiple languages.
- **Broad scale and reach.** GCP offers outstanding scale and reach, resulting in a computing and data platform that is uniquely positioned to address the challenges of IoT.

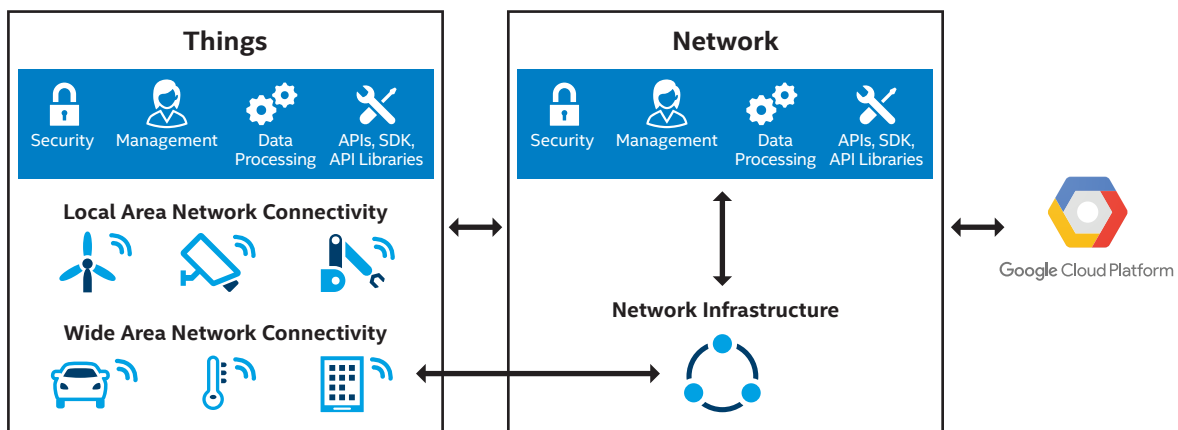


Figure 2. The Intel® IoT Platform connects a wide variety of devices to the cloud, using security-focused hardware and software solutions.

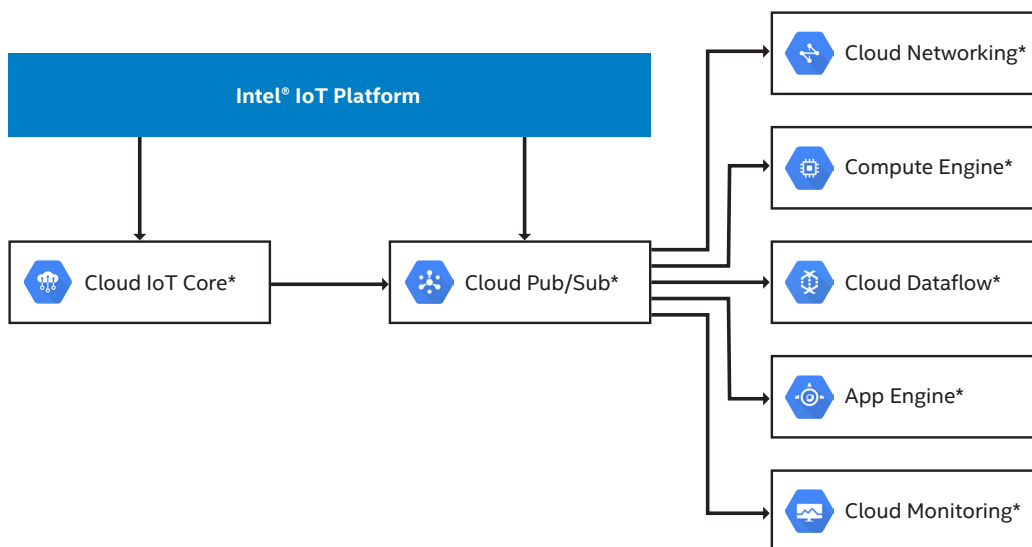


Figure 3. Google Cloud Platform* provides developers with full control of the environment without having to set up and manage the infrastructure.

Solution Architecture Details

The Intel IoT and GCP joint reference architecture (Figure 4) utilizes three primary types of components and solutions: Intel® edge components, such as hardware security and processors; Intel® device and security management, such as device provisioning, monitoring, and control; and GCP cloud services, such as data ingestion, dataflow, storage, and analytics.

Intel IoT Platform Components

Edge components

- **Wind River Linux***. With built-in certifiable security capabilities and portability, Wind River* provides an IoT embedded Linux platform for hardware.
- **Intel® Security Essentials**. Hardware root of trust, capabilities such as secure boot, trusted execution environment (TEE), and Intel® Enhanced Privacy Identifier (Intel® EPID) provide security to the platform at the hardware level.
- **Intel® processors**. Intel® Quark™ system on a chip (SoC) and the Intel® Atom™, Intel® Core™, and Intel® Xeon® processor families provide high performance and scalability.

Device and security management

- **Wind River Helix Device Cloud***. Helix Device Cloud is an IoT portfolio of services and technologies that enable faster time to market; it provides device monitoring, control, software updates, registration, attestation, and security-enabled deployment at scale.
- **Intel® Secure Device Onboarding**. Using the privacy-preserving properties of Intel EPID, an IoT identity standard, onboarding protocols and a rendezvous service, owners can automatically register with their devices in GCP when powered on.

GCP Components

GCP components may vary depending on implementation and are grouped into five primary functions:

Data ingestion

- **Cloud IoT Core***. Cloud IoT Core is a fully managed service that allows you to easily and securely connect, manage, and ingest data from millions of globally dispersed devices. Cloud IoT Core, in combination with other services on Google Cloud Platform, provides a complete solution for collecting, processing, analyzing, and visualizing IoT data in real time to support improved operational efficiency.
- **Cloud Pub/Sub***. Cloud Pub/Sub provides a fully managed, real-time messaging service that allows developers to send and receive messages between independent applications.

- **Cloud Stackdriver Monitoring***. Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud applications.
- **Cloud Stackdriver Logging***. Cloud Logging allows developers to store, search, analyze, and monitor log data and events, as well as to send alerts.

Pipelines

- **Cloud Dataflow***. Cloud Dataflow is a unified programming model that provides managed services for developing and executing a wide range of data processing patterns including extract, transform, load, and batch and continuous computation. Cloud Dataflow frees developers from operational tasks, such as resource management and performance optimization.

Storage

- **Cloud Storage***. GCP provides an object store solution for excellent IoT performance and price.
- **Cloud Datastore***. Cloud Datastore is a NoSQL database that is ideally suited for mobile and web endpoints.
- **Cloud Bigtable***. Cloud Bigtable is designed for workloads that require higher speed and lower latency, such as analytics.

Analytics

- **Cloud Dataflow***. Dataflow provides programming primitives, such as powerful windowing and correctness controls, that can be applied across both batch- and stream-based data sources.
- **BigQuery***. BigQuery is a fully managed, petabyte-scale, low-cost enterprise data warehouse for analytics.
- **Cloud Dataproc***. For Apache Spark* and Apache Hadoop*, Cloud Dataproc is designed for open source data tools for batch processing, querying, streaming, and machine learning.
- **Cloud Datalab***. Cloud Datalab is an interactive tool for exploring, analyzing, and visualizing data with a single click.

Application and presentation

- **App Engine***. App Engine is a platform-as-a-service (PaaS) solution used to develop applications without concern for the underlying infrastructure.
- **Container Engine***. Container Engine is a managed Kubernetes* solution that provides industry-specific solutions, such as fleet management.
- **Compute Engine***. Compute Engine is an infrastructure-as-a-service (IaaS) product that offers VMs on a variety of guest operating systems.

Intel® IoT Platform and Google Cloud Platform*

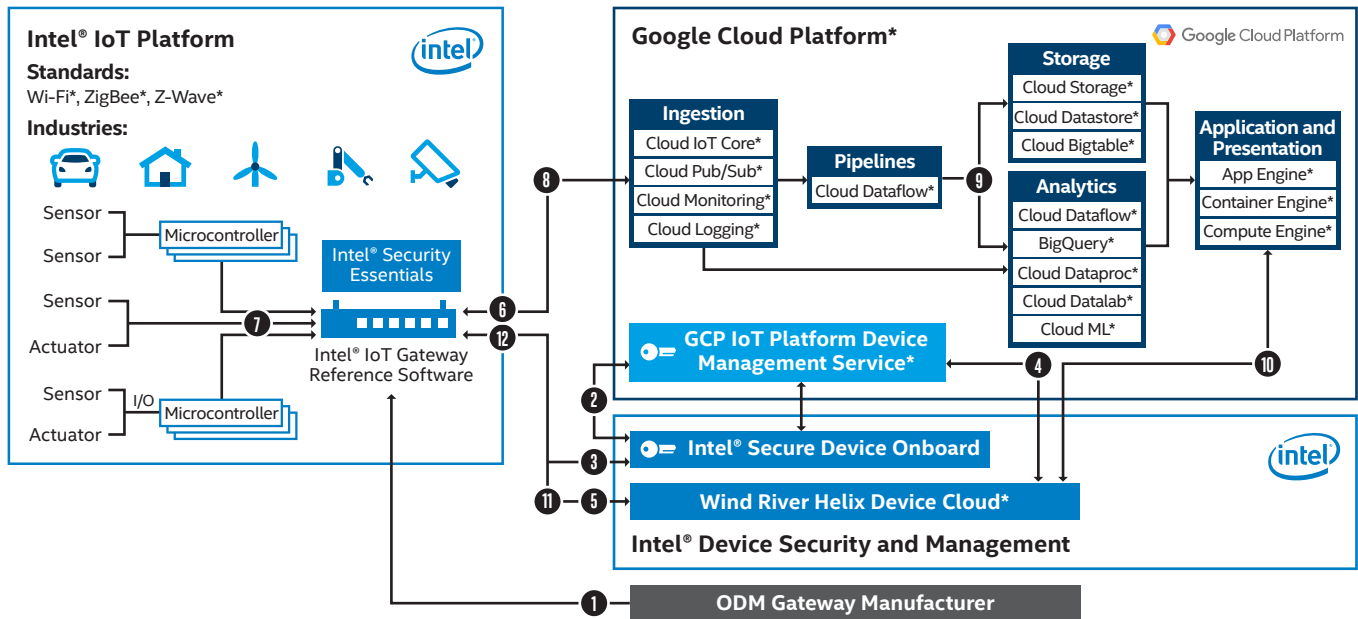


Figure 4. The Intel® IoT Platform and GCP* joint reference architecture details the connections for seamless device onboarding and ownership privacy.

Implementation Overview

The process of connecting devices, integrating data, and managing software upgrades follows these steps (Figure 4):

Onboarding Devices

1. During manufacturing, the silicon provider embeds Intel EPID credentials in a TEE of the processor. The ODM uses an open source toolkit from Intel to create a global unique identifier, assign a URL for Intel® Secure Device Onboard (Intel® SDO), an automated onboarding service from which the device gets its new owner information. It then generates an ownership proxy that is used to cryptographically verify ownership of the device by GCP.
2. Upon purchase, along with the purchase receipt, an ownership proxy for the device is generated. The owner imports the ownership proxy into GCP, which then signals to Intel SDO.
3. When the device is powered on the first time, it contacts the Intel SDO, which redirects it to the IP address provided by its new designated GCP owner.
4. The GCP trust broker and gateway verify the device through its Intel EPID signature and ownership proxy, and then register the device for management with the GCP and Wind River Helix Device Cloud.

5. The Wind River Helix Device Cloud distributes the device certificate provided by the GCP and configures the pub/sub topic subscriptions on the gateway.
6. The GCP IoT software development kit (SDK) on the gateway authenticates the GCP using the device certificate and establishes a data path to the GCP.

Collecting and Integrating Data

7. Business applications on the gateway acquire data from connected sensors through a number of supported protocols, such as Z-Wave*, ZigBee*, and Bluetooth® technology.
8. The GCP IoT SDK on the gateway transmits sensor data to GCP through MQTT and HTTP messaging protocols.
9. Data messages are routed, processed, stored, and made available for enterprise integration.

Managing Devices and Software Updates

10. Application software managers push updates to the Wind River Helix Device Cloud using APIs.
11. The Wind River Helix Device Cloud prepares signed RPM packages and pushes them to the gateway.
12. The management agent on the gateway of the Intel IoT Platform upgrades the software.

Summary

Intel and Google's end-to-end joint reference architecture for IoT offers a robust, security-enabled, yet simplified solution that gives IoT developers the tools and services to create high-performance solutions. With security-enabled, scalable interoperability, the Intel IoT and GCP joint reference architecture can provide the building blocks for any IoT application in any industry.

The joint reference architecture is reusable, preconfigured, and prevalidated. It can securely connect devices and deliver trusted data with interoperable hardware and software from the edge to the cloud. Each layer is designed with a focus on security and scalable hardware built on Intel technology, and optimized for performance across workloads.

Learn More

You may also find the following resources useful:

- [GCP* Overview](#)
- [GCP* Products](#)
- [Intel® IoT Gateway Technology](#)
- [Intel® IoT Solutions](#)
- [Intel® Secure Device Onboard](#)

Find the solution that is right for your organization. Contact your Intel representative or visit intel.com/securedeviceonboard.

Appendix A: Logistics and Asset Management Use Case

Having visibility to where shipments are at any given time is a significant pain point for supply chain businesses. Market research shows that approximately USD 60 billion worth of cargo is stolen during transit each year.² Additionally, roughly one third of the food produced in the world for human consumption every year gets lost or wasted.³ The ability to trace the journey of a package, such as high-value or perishable goods, in real time can transform how companies manage, track, report, and secure products through logistics (shown in Figure A1). Table A1 illustrates an IoT solution using the Intel® IoT and Google Cloud Platform* (GCP*) joint reference architecture.

Location Visibility with Intel® IoT and GCP* Architecture

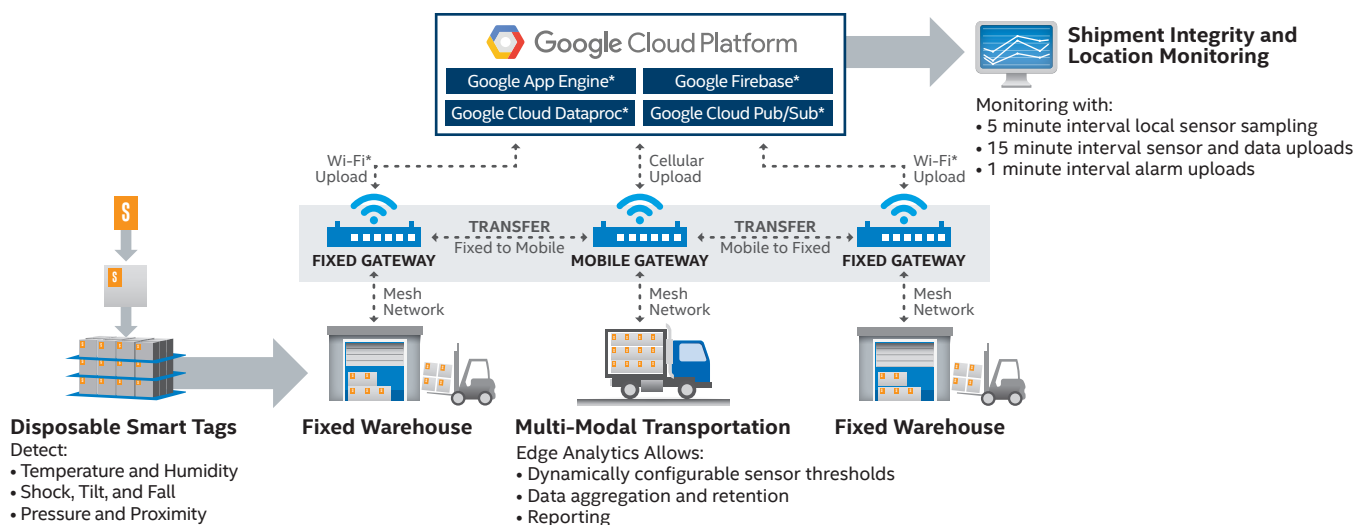


Figure A1. The Intel® IoT Platform and GCP* joint reference architecture provides visibility into the location of goods while in transit, helping transportation businesses reduce lost cargo.

Table A1. Technology Components for the IoT Shipment Visibility Use Case

COMPONENT	DESCRIPTION
Smart Sensors	Multiple battery-operated smart sensors used within a shipment communicate information (temperature, humidity, shock, tilt, fall, pressure, light, proximity) using IEEE 802.15.4 radio to the IoT gateway.
IoT Gateway using Intel® IoT Gateway Technology	Fixed or mobile battery-operated gateways running the Wind River Linux* OS are located on the shipping container, trucks, or pallets.
Wind River Helix Device Cloud*	SaaS-based device management software remotely manages the fixed and mobile IoT gateways.
Intel® Secure Device Onboarding	Cloud-based preconfigured software securely onboards fixed and mobile IoT gateways.
Google Cloud Platform*	Cloud IaaS and PaaS components (e.g., Cloud Pub/Sub*, Cloud Dataflow*, Cloud Storage*, Firebase*, and App Engine*) ingest, process, and analyze data received from the smart sensors through the IoT gateways, using the Pub/Sub messaging protocol.



¹ [gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise](https://www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise)

² aic.gov.au/media_library/publications/tandi_pdf/tandi214.pdf

³ fao.org/save-food/resources/keyfindings/en

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration.

No computer system can be absolutely secure. Check with your system manufacturer or retailer, or learn more at [intel.com](https://www.intel.com).

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

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

© Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Atom, Core, Quark, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

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

1117/JBOS/KC/PDF

Please Recycle

334992-002US