REFERENCE ARCHITECTURE

Securing Edge to Cloud IoT Solutions with Intel and Amazon Web Services

The Internet of Things (IoT) is at the heart of a powerful technology revolution. The act of connecting devices and systems to each other so that they can share data, is the seed of new products, services, and experiences. IoT allows companies greater insight into how customers are using and interacting with their products by collecting the valuable data these systems produce.

AWS and Intel are partnering to offer a joint reference platform for IoT architecture that provides a foundation for seamlessly and securely connecting devices, delivering trusted data to the cloud, and delivering value through analytics.

Companies and organizations have been collecting and storing data for years. Now new data analytics technologies enable more productive use of this data by transforming it into information that extract meaning that lead to smarter decision making that drive tangible business outcomes.

However, building an end-to-end IoT solution can be a challenging task for many customers. There are many components to consider: devices and sensors at the edge, communication protocols, cloud infrastructure, business applications that make use of IoT data, and management systems to deploy, monitor and maintain an IoT system. It's important that customers make choices in developing an IoT system that works not just as a prototype, but scales to production level in a secure and manageable way.

The AWS – Intel IoT Platform

The joint Intel-AWS IoT solution begins at the edge, with Intel IoT Gateways and an ecosystem of compatible sensors and devices. These hardware devices include software built with the AWS IoT Device SDK to connect them to AWS IoT and ultimately AWS endpoints. From there, customers and partners can build software to connect any number of devices in the physical world with the full breadth and depth of AWS services to build or integrate any kind of vertical specific IoT application while gaining value through IoT data analytics.

"By using the AWS cloud services, companies are able to build agile solutions that can scale to meet tremendous device growth...while building on top of secure cloud computing infrastructure."

Intel IoT Platform

The Intel IoT Platform includes an end-to-end reference architecture, and a family of products from Intel and its ecosystem, that provides a foundation for seamlessly and securely connecting devices, and delivering trusted data to the cloud.

This solution scales from the development phase of an IoT implementation, into production by leveraging Intel's ecosystem of Original Device Manufacturers (ODMs) that build IoT Gateways and by including device registration and management services from the Wind River Helix Device Cloud (HDC). Customers can quickly develop IoT systems using Intel reference hardware and AWS services. When it is time to go to production, customers can work with ODMs to manufacture the exact hardware that they need for their use case, have them automatically register with AWS IoT on the factory floor, and manage updates, reboots, and configuration changes remotely with HDC.

This document will describe features and capabilities of Intel IoT Gateway hardware, Helix Device Cloud, AWS IoT, and how they can be combined to build complete IoT solutions in the cloud for joint customers.

AWS IoT & AWS

One of the value propositions of an Internet of Things (IoT) strategy is the ability to provide insight into context that was previously invisible to the business. Before a business can develop a strategy for IoT, it needs a platform that meets the foundational principles of an IoT solution.

AWS believes in some basic freedoms that are driving organizational and economic benefits of the cloud into businesses. These freedoms are also why the cloud is proving itself as the primary catalyst to any Internet of Things strategy across commercial, consumer, and industrial solutions. AWS has identified core tenets vital to the success of any IoT platform. These core tenets are agility, scale, cost, and security; which have been shown as essential to the long-term success of any IoT strategy.

The Core Tenets of IoT:

- **Agility** – The freedom to quickly analyze, execute, and build business and technical initiatives in an unfettered fashion
- **Scale** – Seamlessly expand infrastructure regionally or globally to meet operational demands
- **Cost** – Understand and control the costs of operating an IoT platform
- **Security** – Secure communication from device through cloud while maintaining compliance and iterating rapidly

By using the AWS cloud services, companies are able to build agile solutions that can scale to meet tremendous device growth, with an ability to manage cost, while building on top of secure cloud computing infrastructure.

Companies that select a platform that has these freedoms and promotes these core tenets will improve organizational focus on the differentiators of its business and the strategic value of implementing solutions within the Internet of Things.

AWS IoT is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT, your applications can keep track of and communicate with all your devices, all the time, even when they aren't connected.

amazon web services | intel

"With AWS IoT, you can filter, transform, and act upon device data on the fly, based on business rules you define."

With AWS IoT it easy to use AWS services like AWS Lambda, Amazon Kinesis, Amazon S3, Amazon Machine Learning, Amazon DynamoDB, and many others, to build IoT applications that gather, process, analyze, and act on data generated by connected devices, without having to manage any infrastructure.

AWS IoT supports HTTP, WebSockets, and MQTT, a lightweight communication protocol specifically designed to tolerate intermittent connections, minimize the code footprint on devices, and reduce network bandwidth requirements. AWS IoT also supports other industry-standard and custom protocols, and devices can communicate with each other even if they are using different protocols.

Authentication and end-to-end encryption throughout all points of connection, help AWS IoT to make sure data is never exchanged between devices and AWS IoT without proven identity. In addition, you can secure access to your devices and applications by applying policies with granular permissions.

With AWS IoT, you can filter, transform, and act upon device data on the fly, based on business rules you define. You can update your rules to implement new device and application features at any time.

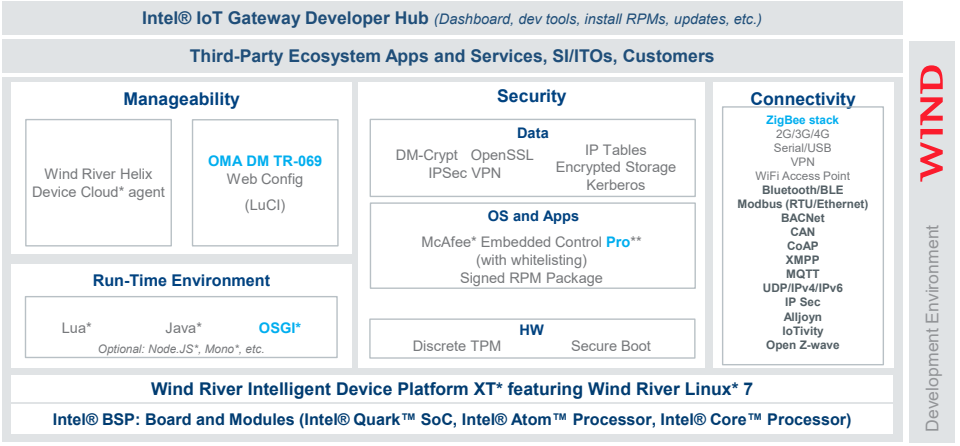
Using Device Shadows, AWS IoT stores the latest state of a device so that it can be read or set at any time, making the device appear to your applications as if it were online all the time. This means that your application can read a device's state even when it is disconnected, and also allows you to set a device state and have it implemented when the device reconnects.

The AWS-Intel Joint Reference Architecture

This section defines the components and integration framework comprising of Intel IoT platform and Amazon Web Services (AWS) IoT reference architectures. It outlines the key components and capabilities of the joint AWS-Intel architecture and how customers can leverage it to build secure end-to-end IoT solutions.

Intel Edge Components

- **Wind River Linux**: is the leading commercial embedded Linux platform hardened for IoT
- **Intel Hardware Security**: Secures the platform at the hardware level with capabilities such as secure boot, Intel Trusted Execution Technology.
- **Intel Processors**: Provides unique performance scalability across Intel Quark SoC, Atom, Core and Xeon processor families.



amazon web services | intel

"AWS IoT leverages an event-driven architecture and works with other AWS Services for application development, storage, analytics and visualization."

- **Wind River Intelligent Device Platform XT**: Simplifies the development, integration, and deployment of IoT gateways with a customizable middleware development environment.
- **McAfee Integrity Control**: Performs monitoring, management, and tight security policy enforcement on edge devices.

Intel Device Management and Security

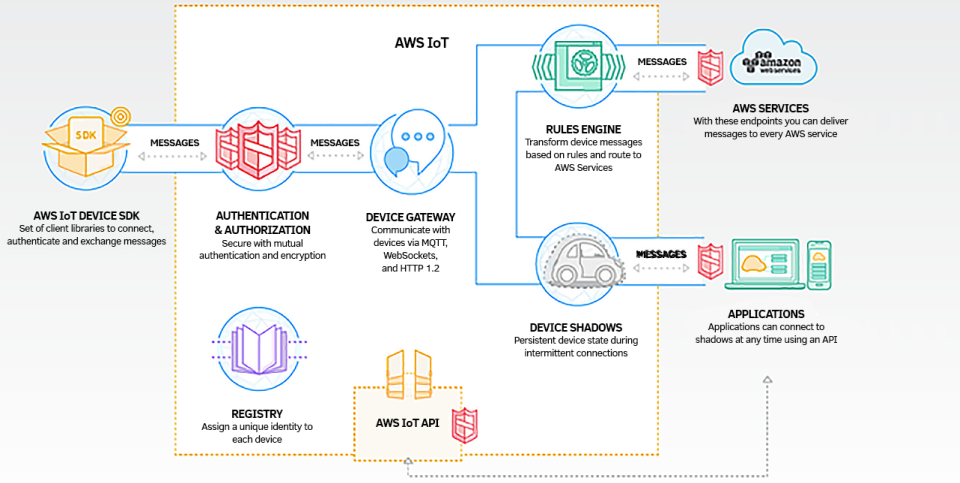
- **Wind River Helix Device Cloud**: Provides device management services (device monitoring, device control, software updates), device registration, device attestation, and secure deployment at scale. Helix Device Cloud leverages McAfee ePolicy Orchestrator to ease administration of distributed devices, automate security policy control, and simplify compliance reporting.

AWS IoT Data Ingestion

AWS IoT is a managed service for Internet of Things devices, that currently include an IoT Device SDK, Registry, Device Shadows, Rules Engine and Authentication & Authorization services. AWS IoT leverages an event-driven architecture and works with other AWS Services for application development, storage, analytics and visualization.

AWS IoT currently consists of the following components:

- **Message Broker**—Provides a secure mechanism for things and IoT applications to publish and receive messages from each other. You can use the MQTT protocol to publish and subscribe. You can use the HTTP REST interface to publish.
- **Rules Engine**—Provides message processing and integration with other AWS services. You can use a SQL-based language to select data from message payloads, process the data, and send the data to other services, such as Amazon S3, Amazon DynamoDB, and AWS Lambda. You can also use the message broker to republish messages to other subscribers.
- **Thing Registry**—Sometimes referred to as the Device Registry. Organizes the resources associated with each thing. You register your things and associate up to three custom attributes with each thing. You can also associate certificates and MQTT client IDs with each thing to improve your ability to manage and troubleshoot your things.
- **Thing Shadows Service**—Provides persistent representations of your things in the AWS cloud. You can publish updated state information to a Thing



"The AWS and Intel partnership enables a wide range of solutions that let customers use IoT and data analytics to drive tangible outcomes from connected edge devices, no matter where those devices are located."

Shadow, and your thing can synchronize its state when it connects. Your things can also publish their current state to a Thing Svhadow for use by applications or devices.

- **Thing Shadow**—Sometimes referred to as a Device Shadow. A JSON document used to store and retrieve current state information for a thing (device, app, and so on).
- **Device Gateway**—Enables devices too securely and efficiently communicate with AWS IoT.
- **Security and Identity Service**—Provides shared responsibility for security in the AWS cloud. Your things must keep their credentials safe in order to send data securely to the message broker. The message broker and rules engine use AWS security features to send data securely to devices or other AWS services.

Work Flow and Usage Models

AWS and Intel collaborated to create differentiated IoT architectural framework that helps customers take advantage of the proliferation of intelligent devices and the data explosion to gain business insights and realize operational cost savings. The AWS and Intel partnership enables a wide range of solutions that let customers use IoT and data analytics to drive tangible outcomes from connected edge devices, no matter where those devices are located.

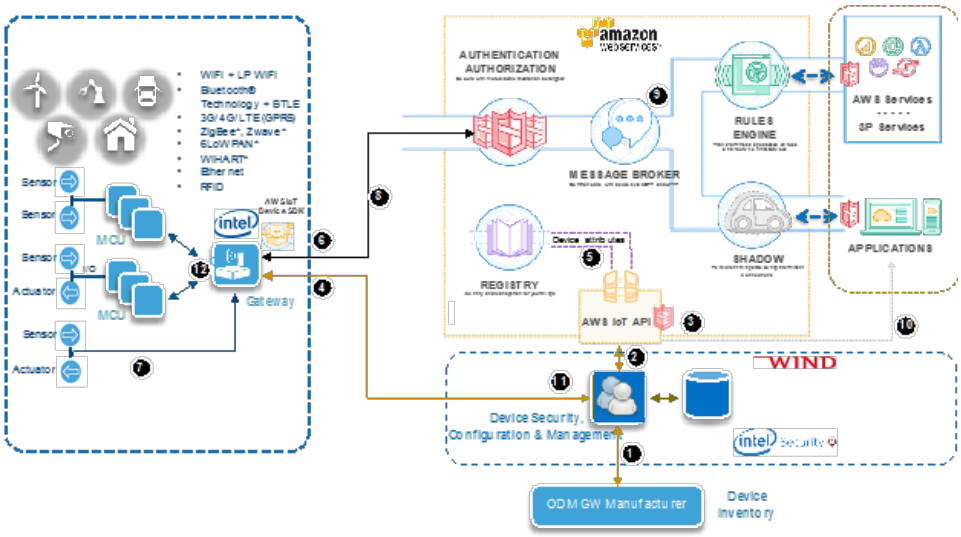
With the tremendous growth of intelligent devices, security is a primary concern for IoT solution deployment that needs to be addressed. Secure Intel hardware and software solutions paired with AWS IoT's mutual authentication security model help customers connect things to the cloud, integrate with existing infrastructure, and securely manage data. Because Intel IoT Gateway comes preconfigured and application-ready, customers can quickly take advantage of IoT solutions to increase efficiency, reduce costs, and solve business problems. Intel IoT Gateway also enables seamless and secure data flow between edge devices and the AWS cloud through pre-integrated, pre-validated hardware and software building blocks. Customers' IoT solutions can then deliver valuable business insights based on data from connected devices at the network edge.

Deployment Experience

Let's walk through a typical IoT deployment scenario: As devices are deployed in the field, it is important to track the device inventory data containing list of gateways (regardless of the ODM manufacturer), their serial number, MAC address and certificates. As part of this architecture, this device inventory data is securely ingested into the Wind River Helix Device Cloud (HDC) at the factory floor of the ODM manufacturer through DXL (Data Exchange Layer) based bulk provisioning APIs. This device inventory is made available to the AWS IoT and other backend CRM applications via secure APIs exposed by HDC, and can be synced up with the help of business logic and workflows on AWS IoT or backend CRM applications such as automatic periodic updates or nightly refresh background jobs. The devices are shipped to customer location(s) and upon powering up at the customer site, the gateway device securely boots up and is attested by HDC, based on hardware root of trust. Upon successful registration, HDC automatically inserts the device certificates into the AWS IoT platform using published APIs. The application on the Intel IoT Gateway establishes a secure data channel using MQTT or WebSockets to AWS IoT using the AWS certificate authentication mechanism. The Intel IoT Gateway gets device configuration from HDC and automatically connects to the sensors and sensor modules. Once the secure data channel is established, applications running on the Gateway get the sensor data and start processing and transmitting data to the AWS IoT platform. All these steps are automated, creating a seamless deployment experience requiring minimal intervention by the customer.

"All these steps are automated, creating a seamless deployment experience requiring minimal intervention by the customer"

The above below depicts key workflows of the IoT solution based on the joint AWS-Intel reference architecture.



Deployment, Registration, Authentication

1. ODM initiates Gateway provisioning by sending device inventory data (list of Gateways, serial number, certs) to Helix Device Cloud (HDC). HDC ingests device inventory data securely through REST APIs.
2. AWS IoT Hub gets device inventory data via HDC APIs.
3. Provisioning Applications takes care of provisioning subscriptions.
4. Once customer powers ON the Gateway, the device securely boots up and HDC attests the Gateway
5. HDC inserts device certificates into AWS device registry via APIs
6. AWS agent authenticates with AWS IoT Hub using device certificates on the GW (Hardware Root of Trust) and establishes secure data path to the cloud

Telemetry, Data Ingestion

7. Business Applications on the device acquires data from connected sensors
8. AWS IoT Client on the Gateway transmits sourced data up to AWS IoT
9. Data messages are routed, processed, stored and made available for enterprise integration

Device Management and SW Updates

10. Application Software Manager pushes the updates to HDC using APIs
11. HDC prepares signed RPM packages and pushes it securely to the Gateway
12. The Intel agent on the Gateway gracefully upgrades the Software

"The AWS and Intel partnership can help customers take advantage of IoT to uncover inefficiencies, reduce risk and cost, seize new opportunities, and increase revenue."

Summary

The Joint AWS and Intel solution provides a compelling architecture for IoT, and provides tools and products for connecting the "unconnected", unlocking the value of data, and visualizing data and monetizing insights. While the Intel IoT Platform provides the foundation for connecting devices, with security and manageability, the AWS IoT Platform enables you to connect devices to AWS Services and other devices, securely process and act upon device data, and enable applications to interact with devices even when they are offline.

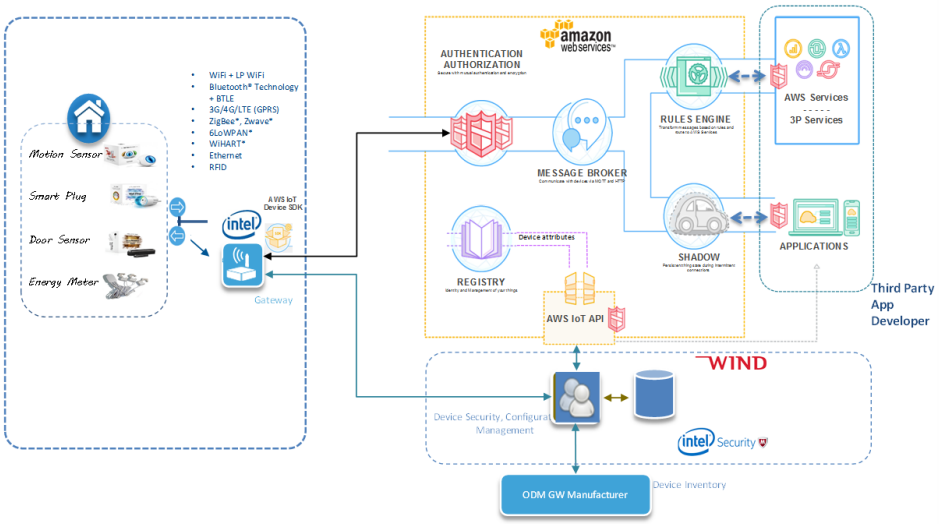
The AWS and Intel partnership can help customers take advantage of IoT to uncover inefficiencies, reduce risk and cost, seize new opportunities, and increase revenue. More than a million businesses worldwide already trust AWS with data and applications. Now, through IoT solutions powered by the Intel and AWS partnership, companies can revolutionize their relationships with customers through new capabilities made possible by real time connected data. For instance, customers can now monitor their assets in real time and predict failures and can proactively dispatch technicians to repair parts before they fail. In Retail, connected data allows retailers the closely monitor their inventory in store and adjust to changes quickly by replenishing SKUs from the warehouse as well as monitor the inventory in transit.

Use Case

Energy Monitoring & Home Safety

AWS and Intel collaborated to develop a Smart Home platform to deliver energy monitoring, home safety and surveillance services. Utility companies that generate and distribute power can offer these services to their end customers leveraging this platform. The Intel IoT Gateway platform connects to multiple sensors such as smart energy meter/clamp, power plugs, door locks, window sensors, IP cameras etc. In addition, the Wind River HDC provides device security and management capabilities. Sensor data is aggregated at the Gateway and sent to the AWS Cloud over IP/Cellular connection. AWS IoT Platform provides data ingestion, storage, analytics capabilities. Smart Home applications for energy monitoring, home safety, and surveillance both on the cloud and gateway device can be provided by a 3rd party application vendor that can develop and launch cloud applications on AWS IoT platform as well device applications on the Intel IoT Gateway.

These services would not only improve customer retention, but also enable new revenue generating opportunities for Utility companies.



Technology Components	Function
Sensors	Door Sensors, Smart Plugs, Energy Meters, IP Camera, Thermostats, Smart Bulbs
Intelligent Gateway	-Seamless connectivity to Sensors (via Zigbee, Zwave, BLE, 802.11) -WAN Connectivity to the Cloud (via 3G, LTE, Ethernet, Wi-Fi) -Filtering and Aggregation of data at the Edge -Home Apps for Energy Monitoring and Management, Home Safety, Home Surveillance (offline mode) -Secure Connection to the Cloud via AWS Device SDK
AWS IoT Platform	Data Ingestion, Storage
Wind River HDC	Device Management, Registration, & Attestation
Cloud Applications	-Customer Apps build on AWS -Dashboard, Visualization, Reports -Energy Monitoring and Management -Home Safety & Surveillance Applications

Technical Appendices

Appendix A: Sensors

To get started, here is a representative list of sensors that are interoperable with the IoT Gateway.

Intel has a vibrant ecosystem of 3rd party partners, who are members are of the Intel IoT Solutions Alliance, and provide hundreds of sensors that are interoperable with the IoT Gateway. Intel has developed a strategy of providing a robust number of sensors that are applicable to a variety of use cases and business solutions; the strategy has been developed leveraging sensors that have been directly validated by Intel and through leveraging Intel's partner ecosystem to pull through the sensors that they have validated by leveraging their middleware solutions.

Sensor Type	Part Number	Protocol	Vertical	Interface
Occupancy and daylight harvesting	Aura Interior	BACNet	Smart Building	RS485
Energy Meter	Veris E50H5	BACNet	Smart Building	RS485
Modbus 3 Phase Energy Meter	Veris H8035-0100-2	Modbus RTU	Smart Building	RS485
Wall Mount Temp	Veris HWXPHTX	Modbus RTU	Smart Building	RS485
Humidity	Veris HD2XMSTA1	Wire	Smart Building	GPIO
Temp	Comet T0310	Modbus RTU	Industrial	RS232
Temp/Humidity	Comet T3311	Modbus RTU	Industrial	RS232
Temp/Humidity	Omega RH-USB	Basic Serial	Industrial	USB
Open Z-Wave	Various (400+ devices)	Z-Wave	Smart Home	USB or RS232
Interface to Phillips Hue Bridge	Hue Bulbs and Lamps	ZigBee	Smart Home	IP

Appendix B: IoT Gateways

Here is a representative list of IoT Gateways manufactured by Intel's ODM ecosystem. For a broader list of IoT Gateways, please refer to the Intel IoT Solutions Alliance.

	Aaeon® AIOT - X1000	SuperMicro SYS-E100-9Q	Advantech® UTX-3115	Dell® IoT Gateway
				
CPU	Intel®Quark ™SoC X1000	Intel®Quark ™SoC X1021	Intel®Atom™E3826	Intel®AtomE3825
I/O – LAN WAN PAN	- 2x Ethernet^ 10/100 - Opt WiFi, CAN, Bluetooth^ - Optional ZigBee*† or RFID	- 2x Ethernet^ 10/100 - Support for WiFi, Bluetooth, GPS, Cellular - ZigBee*†	- 2x Gbe LAN - Optional WiFi - Optional 3GTelit HE910-G	Ggabit Ethernet, 802.11n, Bluetooth
I/O – Ports	- 4x USB 2.0 Host, 1x USB Client - 1x RS-232/422/485 - 1x RS-422/485 header - 1x DIO (16 bit) - ADC (8 pin, 12 bit) - 2x SPI - 1x I2C - Trusted Platform Module 1.2	- 2x USB 2.0 ports (1 Device & 1 Host) - 1x RS-232 via DB9 - 1x RS-485 via screw terminal interface - 1x Analog input 8 channel 12 bit - 1x DIO - Trusted Platform Module 1.2	- 2x USB 2.0 - 1x USB 3.0 - 1x RS-232 (5v/12v) or 1x RS-422/485 - 2x HDMI - 4x Antenna	- 2x USB 2.0 ports - 1x USB 3.0 port - 1x RS-232, 2x RS-485 - 1x RS-422/485 - 1 HDMI - TPM 1.2
I/O – Expansion	1 x Full Size mPCIe* 1 x Half Size mPCIe*	2x Mini-PCIe 1x ZigBee module socket	1 x Full Size mPCIe* w/mSATA Support 1 X Half Size mPCIe*	1 x mPCIe*
Memory and Storage	- 1 GB non-ECC DDR3 - Micro SD slot - ROM: 8MB SPI	- 512MB DDR3 ECC - Micro SD Slot up to 32GB - 8MB SPI Flash	- 1x SODIMM (up to 16GB DDR3L) - 1x 2.5" SATAII (HDD or SSD)	- 2GB RAM - 32GB mSATA SSD
Op Temp	Standard: 0°C~60°C Wide temp: -40°C~85°C	0°C~50°C	-20°C~60°C	0°C~50°C
Power	VDC 5V or 9-24V	12v DC	12v DC	24v AC/DC
Certs	FCC, CE	CE, FCC, UL	CE, FCC, CCC, BSMI, CB, UL, RoHS, PTCRB, GCF	CE, FCC
Dimensions	88.9 x 146 x 101.6mm	135 x 36 x 109mm	138.5 x 36 x116.4 mm	229 x 216 x 64 mm
Segments	Industrial, Retail, Smart Building	Smart Building, Retail, Smart Factory	Industrial, Retail	Industrial, Smart Building