
aws
IoT in the connected home
Building smart products
with AWS IoT

Introduction

IoT is impacting every industry, but the one area that affects almost everyone's day-to-day is in the home. Global demand from consumers for connected home devices is growing. Consumers expect to easily connect, control, and gain insights from everyday items—from coffeepots and light switches to thermostats and security systems—and they are increasingly turning to artificial intelligence (AI) assistants to control other devices in their home and automate simple, monotonous tasks. Beyond simply providing convenience, consumers also expect their connected home devices to improve their quality of life through additional security, comfort, and cost savings.

As the use of connected devices continues to grow, more and more data is being pushed to the cloud, where the latest IoT and machine learning technologies are enabling new innovations in connected home applications. The cloud also enables a whole ecosystem of connected home device manufacturers, service providers, and application developers to easily connect their products at scale, take action on the data they collect, and create a new class of connected home applications that interact with the physical world.

Device manufacturers use IoT technologies in the cloud, and on devices, to help them create connected home products that add or unlock new sources of revenue, better understand how consumers use their products, identify opportunities for product improvement, and create better experiences for their consumers.

Challenges

Connecting and gathering data from large fleets of connected home products requires development effort to deploy and manage devices at scale; collect, filter, and process the deluge of data coming from millions of these devices; address privacy and security challenges; and quickly scale while maintaining low development and deployment costs.

Managing and maintaining large device fleets

Connected home manufacturers deploy, manage, and monitor hundreds of thousands to millions of devices, and then collect, store, and analyze data from these devices. Developing custom software and provisioning infrastructure that can scale up and down to support a high volume of simultaneous connections between cloud services, mobile apps, and an array of devices can be difficult and time consuming.

Additionally, there are circumstances when relying exclusively on the cloud isn't optimal due to latency requirements or intermittent connectivity that makes a roundtrip to the cloud unfeasible.

Aside from technology and software considerations, device manufacturers must also evaluate and select the right hardware vendors from a large ecosystem and then integrate various vendor-specific technologies, which can be time-consuming and complex.

Adding connectivity and intelligence to devices, both deployed and new, as well as on the device and in the cloud, is often not a core competency for device manufacturers.

Translating device data into customer value

Device manufacturers are always looking for ways to make everyday products smarter for consumers and provide better, data-driven offerings that weren't possible prior to IoT. In many cases, device manufacturers want to implement machine learning models to enable devices to become smarter over time. In other cases, device manufacturers want to add innovative functionality to connected devices such as AI assistants and automated reordering of items such as coffee beans or laundry detergent.

Adding these capabilities starts with collecting and making sense of a massive amount of device data. However, IoT data is highly unstructured and difficult to analyze with traditional analytics and business intelligence tools that are designed to process structured data. IoT devices often record noisy processes such as temperature, motion, or sound. The data from these devices can frequently have significant gaps, corrupted messages, and false readings that make analysis unreliable. Deploying and scaling their backend IoT analytics infrastructure to deal with this noisy data take time and resources that are better used focusing on building the best solution for customers.

Managing rising privacy concerns as data spreads into the enterprise

IoT devices in the home produce data that is transmitted, processed, and then stored in databases connected to enterprise systems, such as customer relationship management (CRM) platforms. Consumers are extremely sensitive to potential data and privacy breaches, so manufacturers seek out solutions that help them to protect data on the device itself, throughout all connection points, and in the cloud. As device manufacturers connect growing numbers of connected home products, it has become increasingly difficult to maintain and enforce privacy best practices. Once a consumer's trust is lost, it can be difficult to regain, and they will often vocally select another brand.

Security vulnerabilities exist across the network

IoT fleets consist of devices that have diverse capabilities and are long-lived and geographically distributed. These connected devices are constantly communicating with each other and the cloud using different wireless communication protocols. While this creates responsive IoT applications, it can also expose IoT security vulnerabilities and create opportunities for malicious actors or accidental data leaks. These characteristics, coupled with the growing number of devices, raise questions about how to address security risks posed by IoT devices. To further amplify security risks, many devices have a low level of compute, memory, and storage capabilities, which limits opportunities for implementing security on devices.

Inability for IoT applications to scale

Due to the changing patterns of connected home device usage, manufacturers need flexible and scalable infrastructure that can expand and contract as the demand fluctuates. This makes it difficult to not only manage device fleets but also to provide a reliable, consistent experience for customers.

Managing cost at every stage of deployment

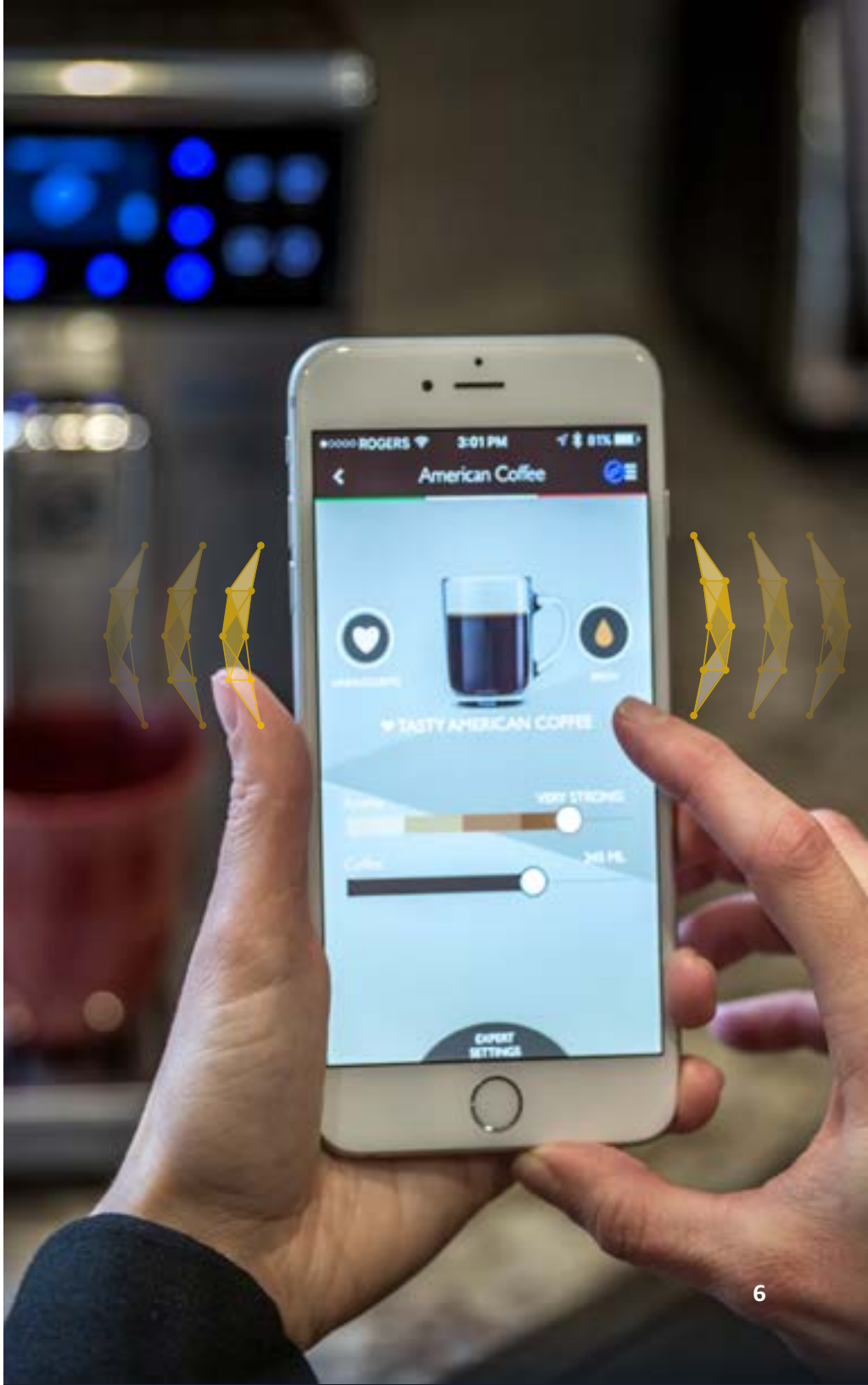
Device manufacturers constantly balance decisions for how to build, manage, and analyze their IoT solutions while attempting to maintain extremely low production, service, and maintenance costs, as end consumers are extremely price sensitive.

Opportunities in the connected home market

Home automation

Home automation opportunities apply to a wide range of connected devices that can be found in the home. This includes white goods like a washer, dryer, oven, or refrigerator; media and entertainment products like a TV or speaker system; and smaller items like a coffeemaker, vacuum, thermostat, switch, or light bulb. These devices can work alone, by directly connecting to the Internet, or together with other devices or hubs for an integrated smart home experience. Consumer experience is critical, with a strong focus on devices being able to quickly connect and achieve an outcome easily.

For example, a consumer who buys a smart coffeemaker will want to be able to set it up and get it connected quickly, likely using an app on their smartphone. They also want to be able to take advantage of that connectivity, like ordering more coffee from Amazon at the click of a button, or even automatically when a sensor detects that coffee beans are about to run out. These devices can also benefit from using voice-enabled AI assistants like Amazon Alexa for an enhanced customer experience.



aws internet of things

Home security & monitoring

Products in the home security and monitoring market include devices such as connected door locks, video doorbells, security cameras, and emergency lighting systems, as well as monitoring systems such as water leak detectors, energy management systems, and connected thermostats.

Consumers expect that their smart cameras and audio sensors will automatically detect threats, then take action, and send alerts to their smartphones. Such devices need to run with low latency and compute data locally as each roundtrip to the cloud could cost valuable time in detecting threats.

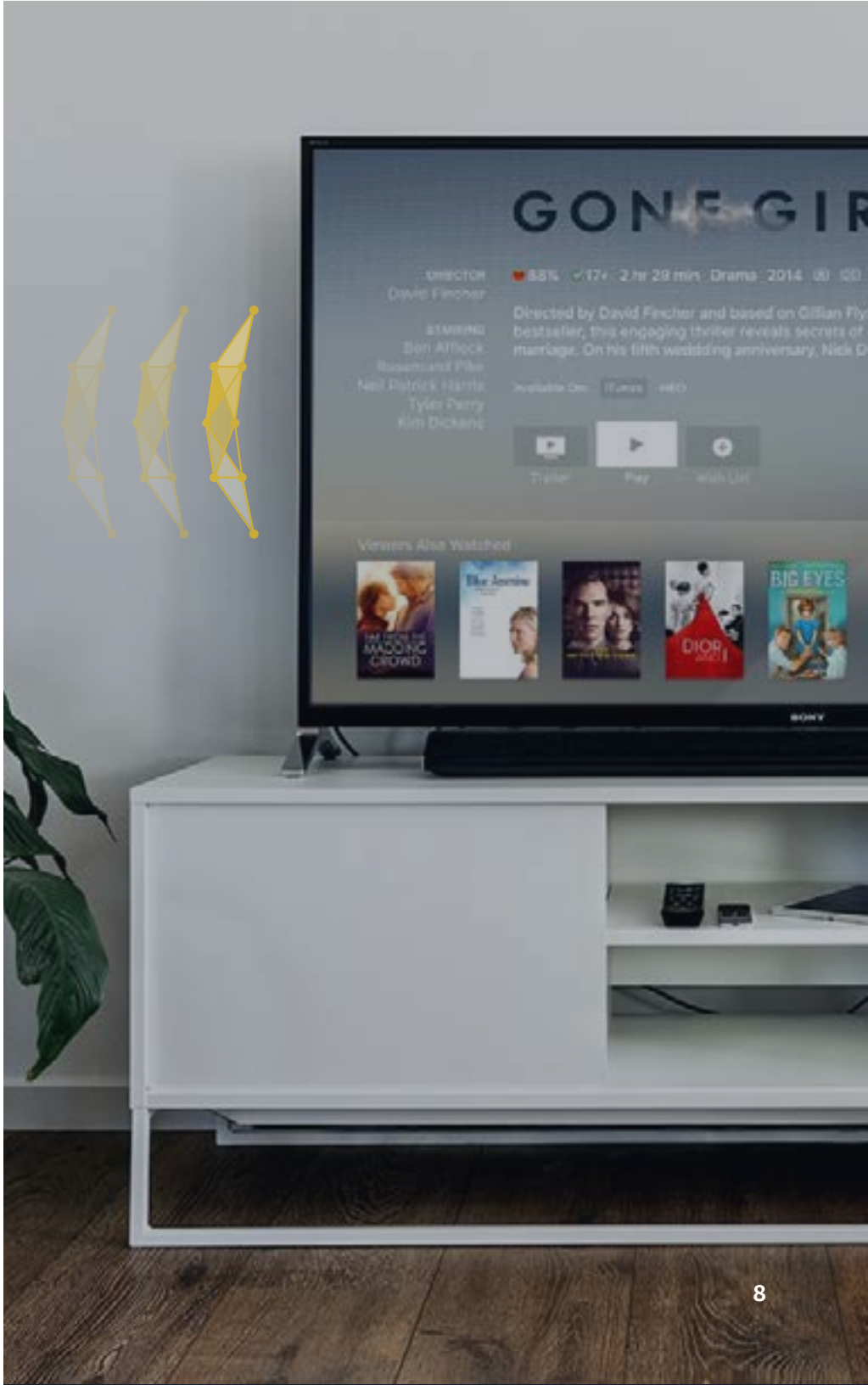
Additionally, devices in the security and monitoring market can use device software to operate locally so that they can act even when the external Wi-Fi connection has been tampered with or lost.

For example, if a burglar cuts the Internet in a home, a home security provider can automate the process of turning on all of the floodlights outside, sounding the internal alarm, and locking the doors. In these situations, IoT devices can perform these tasks locally despite not being connected to the Internet.

Home networking

Network operators and cable providers are looking for new ways in which they can help consumers quickly discover, troubleshoot, and fix their home network issues, including Wi-Fi and Cable TV connectivity. In the past, network operators have been limited with the potential of computing capabilities within those devices. However, with edge computing, they can add new functionality to enhance the overall customer experience.

For example, IoT-enabled set-top boxes can automatically log network diagnostics and send the data to the customer service center proactively, and in turn, they can send a message to the customer to alert when a problem is detected. This level of transparency allows customers to monitor and troubleshoot the network health themselves, through a mobile application.



"Time-to-market is everything for us," says Franz Garsombke, chief technology officer and co-founder of Rachio. "But we're a startup, and we wanted to get our product out there rapidly without investing a lot in our own hardware resources to make that happen. We didn't want to spend all our time maintaining the underlying technology, whether that be device connectivity or servers. For companies wanting to get into the IoT space, tools like AWS IoT enable a faster time-to-market and eliminate the need to spend months and months and hundreds of thousands of dollars building a solution yourself—using AWS, we were able to get our product to market 40% faster than we could if we had to build a highly available infrastructure with load balancing."

Franz Garsombke
CTO and Co-founder, Rachio

Read the case study »

With AWS IoT, you can easily, quickly, and securely build differentiated connected home products at scale

AWS makes it easy for customers such as LG, VIZIO, iRobot, Comcast, and Rachio to build IoT applications that collect, process, analyze, and act on data generated by connected home devices without having to manage any infrastructure. These customers rely on AWS IoT to overcome the top challenges facing device manufacturers and build solutions that deliver value to both their businesses and consumers.

Complete end-to-end solutions

AWS IoT is a set of fully managed services that make it easy to deploy and manage a complete connected home IoT solution.

Built-in connectivity for microcontrollers

You can cut back on development time with Amazon FreeRTOS, an IoT operating system for microcontrollers, which provides connectivity libraries in a tiny memory footprint and is based on the familiar FreeRTOS kernel. With a broad and growing set of qualified hardware, you can easily scale across product lines and build in connectivity to AWS Cloud services such as AWS IoT Core or local connectivity to an edge device running AWS IoT Greengrass.

Reliable and persistent communication

AWS IoT Core lets you easily and securely connect devices to the cloud and enable them to interact with other cloud applications and devices. AWS IoT Core 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 provides scalable, low-latent, bi-directional communication from device to cloud. AWS IoT Core is present in multiple regions worldwide, allowing you a global footprint and minimal downtime.

Device management

Using AWS IoT Device Management, you can onboard, organize, and monitor your devices and create a real-time, searchable fleet index of all of your connected devices to remotely manage your devices at scale. You can also push bug fixes and firmware updates over the air with a few clicks. Plus, the device certificates for routers and set-top boxes managed with AWS IoT Device Management will never expire.

Building IoT applications in the cloud

With AWS IoT Things Graph, you can visually connect different devices, such as sensors and actuators, and web services from different vendors that speak different protocols to build IoT applications. AWS IoT Things Graph allows you to build IoT applications quickly, easily create sophisticated workflows, and easily package and deploy IoT applications to AWS IoT Greengrass-enabled devices, such as cameras or cable set-top boxes, in just a few clicks.

"Customers are demanding easier ways to interact with a growing number of products and technologies throughout the home—Cloud connectivity provides Roomba customers with even more convenience and control, so they can use their phones to manage their Roomba, wherever and whenever it's convenient... The AWS Cloud offered an essential combination of scalability, global availability, and breadth of services."

Ben Kehoe
Cloud Robotics Research Scientist, iRobot

Read the case study »

Offline communication

With AWS IoT Greengrass, connected devices can run AWS Lambda functions, keep device data in sync, and communicate with other devices securely—even when not connected to the Internet. Once the device reconnects, AWS IoT Greengrass synchronizes the data on the device with AWS IoT Core, providing seamless functionality regardless of connectivity.

Local communication

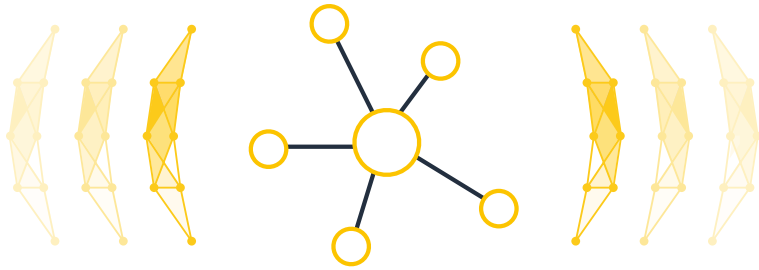
AWS IoT Greengrass devices can act locally on the data they generate so they can respond quickly to local events while still using the cloud for management, analytics, and durable storage. This cuts down on the time and cost it takes for data to make a roundtrip to the cloud. Devices running Amazon FreeRTOS can easily connect to devices running AWS IoT Greengrass, allowing for near real-time local communication.

Spotting events across deployments

AWS IoT Events is a fully managed service that makes it easy to detect and respond to events from IoT sensors and applications. Using IoT Events, it's simple to detect events across thousands of IoT sensors sending different telemetry data, such as temperatures in a freezer or motion detectors using movement signals to activate lights and security cameras. AWS IoT Events automatically triggers alerts and actions in response to events based on the logic you define to resolve issues quickly, reduce maintenance costs, and increase operational efficiency.

Easy integration with AWS services

AWS IoT makes it easy to use the broad range of AWS services including AWS Lambda, Amazon Kinesis, Amazon S3, Amazon SageMaker, Amazon DynamoDB, Amazon CloudWatch, AWS CloudTrail, and Amazon QuickSight to build connected home applications that gather, process, analyze, and act on data generated by connected devices, without having to manage any infrastructure. This ensures you can build complete solutions, such as an application that uses AWS IoT to manage security cameras and Amazon Kinesis for machine learning.



Build innovative products quickly

AWS makes it easy to gather and analyze IoT data and then build in innovative functionality based on your learnings. AWS IoT services integrate seamlessly with AWS Machine Learning services, Amazon Alexa, Amazon Dash Replenishment, and many other AWS services to help you differentiate your products, enhance the customer experience, and unlock new sources of revenue.

Device insights

AWS IoT services help you understand how your customers are interacting with your products. AWS IoT Analytics offers the easiest way to run analytics on IoT data and get insights to make better and more accurate decisions for IoT applications. AWS IoT Analytics makes it easy to run and operationalize sophisticated analytics on massive volumes of IoT data, even data coming from noisy and sometimes intermittently connected sources. With AWS IoT Analytics, you don't have to worry about the cost and complexity typically required to build an IoT analytics platform. IoT device data can help inform necessary product improvements, and you can then use AWS IoT to easily push bug fixes and firmware updates with new features over the air with a few clicks. This ensures you can seamlessly deliver a continuously improved experience to your customers without requiring any action on their end.

Easy integration with Amazon Alexa

AWS IoT makes it easy to build in Amazon Alexa functionality into everyday devices so your customers can control them with voice commands. The integration gives you the ability to scale to support fleets of millions of devices with millisecond latency and low connectivity cost. AWS IoT Core also allows you to program your devices to keep them "listening" for long durations, allowing for reliable response from voice-activated commands through Alexa.

"The market for smart devices in the home is flourishing, and AWS IoT services are helping us be part of that development by supporting our Rotimatic flatbread-making robot… We're able to understand our customers better. We can gather data on usage patterns and gauge feedback and satisfaction levels. We can also distinguish the favorite recipe on our Rotimatics. With this kind of information, we can evolve our product with updates—right down to new recipes we send out to the device—that we know will add value to our customers."

Rishi Israni
Co-founder and CEO, Zimplistic

Read the case study »

"Our research and development group is getting information about how our top-of-the-line products are functioning that was impossible to gather before. We have insights into not only how the product is functioning, but also how people are using the product. For example, we gather statistics about motor speed, errors, voltages, and so on, which tell us how well our air-treatment units are operating in the field. We also collect information about users' interactions with our mobile application in order to improve that offering."

Everette Binger
Chief IoT Solutions Architect, Amway

Read the case study »

Machine learning inference

AWS IoT makes machines smarter over time by bringing machine learning and IoT together. AWS IoT Greengrass makes it easy to perform machine learning inference locally on devices, using models that are created, trained, and optimized in the cloud. AWS IoT Greengrass gives you the flexibility to use machine learning models in Amazon SageMaker or to bring your own pre-trained model stored in Amazon S3.

Easily use Amazon Dash Replenishment Service

Amazon Dash Replenishment Service (DRS) allows connected devices to leverage Amazon's retail capabilities to build automatic reordering experiences for your customers. With the easy-to-use APIs, you can take advantage of Amazon's authentication and payment systems, customer service, and fulfillment network to ensure your customers never have that "ran out of it" moment—like a Whirlpool washing machine that orders laundry detergent before your last load.

Security & privacy customers can trust

Cloud security

AWS IoT makes it easy for you to secure device fleets at scale with built-in device authentication and authorization to keep IoT data and devices protected. AWS IoT provides manufacturers with end-to-end device security with key management, certificate authentication, and data encryption so that IoT devices are secure and are protected from intrusion and data leaks. AWS IoT Core provides the security building blocks for you to securely connect devices to the cloud and to other devices for authentication, authorization, audit logging, and end-to-end encryption. AWS IoT Device Defender continuously audits IoT configurations to ensure adherence to security best practices.

Device security

Amazon FreeRTOS comes with libraries to help secure device data and connections, including support for data encryption and key management, as well as provides a code signing feature for over-the-air updates. AWS IoT Greengrass authenticates and encrypts device data for both local and cloud communications so that data exchanged between devices and the cloud is always protected. With the AWS IoT Device SDK, you can leverage hardware-secured end-to-end encryption for messages sent between AWS IoT Greengrass Core and the AWS Cloud or other local devices. All of this is supported by a world-class team of AWS security experts monitoring systems 24/7 to protect customer content.

"AWS IoT offers leading-edge security capabilities. Messages are encrypted, and the broker adds another level of security—and in general, the policy-based security is a huge advantage of AWS. If one of our devices goes rogue, we don't have to reissue certificates. We can just shut off the policy to that device. It's very simple and effective."

Franz Garsombke
CTO and Co-Founder, Rachio

Read the case study »

AWS IoT helps you manage scale and cost

Managing scale

AWS IoT is built on the most scalable, secure, and proven cloud infrastructure and is designed to support tens of millions of different devices and billions of messages. AWS IoT Device Management makes it easy to securely onboard, organize, monitor, and remotely manage IoT devices at scale. Once you have a scaled IoT deployment, you need tools that can handle monitoring those devices at scale, as well. AWS IoT Events continuously monitors data from multiple IoT sensors and applications, and it integrates with other services, such as AWS IoT Core and AWS IoT Analytics, to enable early detection of anomalies and device malfunction.

Keep development and deployment costs low

As you scale, AWS IoT and our validated hardware partners can help you keep your deployment costs low so that you can provide more value at lower prices to your consumers. AWS IoT enables pay-as-you-go pricing, and there are no minimum fees or mandatory service usage.

Conclusion

There are billions of connected consumer devices in the home, office, cars, and thousands of other places. With the proliferation of these connected devices, connected home device manufacturers increasingly need solutions to connect them, and collect, store, and analyze device data. Built on AWS, which is used by industry-leading device manufacturers around the world, AWS IoT can easily scale as your device fleet grows and your business requirements evolve. Since AWS IoT integrates with AWS Machine Learning services, you can make your devices smarter, even without Internet connectivity. You can easily add Alexa voice functionality and automated replenishment to your connected devices to differentiate your products. Finally, AWS IoT also offers the most comprehensive security features so you can create preventative security policies and respond immediately to potential security issues. For these reasons and more, AWS IoT provides the easiest set of services and solutions to rapidly and securely build differentiated connected home products at scale.

Learn more about AWS IoT

At AWS, our mission is to make sure that you can know the state of every *thing*, for all your devices, and that you can reason on top of that data, so you can solve business problems.

aws internet of things

Device Software

Amazon FreeRTOS

IoT Operating System for Microcontrollers

AWS IoT Greengrass

Secure Local Triggers, Actions, and Data Sync

Connectivity and Control Services

AWS IoT Core

Secure Device Connectivity and Messaging

AWS IoT Device Defender

Fleet Audit and Protection

AWS IoT Device Management

Fleet Onboarding, Management, and Software Updates

Analytics Services

AWS IoT Analytics

IoT Data Analytics and Intelligence

AWS IoT Events

Detect and Respond to Events from IoT Sensors and Applications

AWS IoT Things Graph

Visually Connect Different Devices and Web Services to Build IoT Applications