The Role of Edge Computing in Enterprise IoT

Exploring the power of 5G, LTE, and containers to connect and optimize IoT with less hardware

Overview

Like a rocket ship soaring through space, edge computing is quickly gaining momentum in the networking world, and it isn't expected to slow down anytime soon. An estimated 45% of the world's data will be moved closer to the network edge by 2025, according to a global Internet of Things (IoT) decision-maker survey. By that same year, it's also estimated that 75% of enterprise-generated data will be created outside of centralized data centers or clouds, according to Gartner.

The need for connectivity at the edge of the network touches nearly every industry and every vertical, especially with the rise of bandwidth-intensive technologies such as IoT and artificial intelligence (AI). These types of advanced applications require the power of edge computing and the speed and flexibility of wireless 5G connectivity to operate efficiently. The growing demands of data processing applications have put a strain on traditional cloud computing as more devices are connected to the cloud, causing bandwidth limitations and network congestion on the edge, among a host of other problems.

Edge computing is one way to handle the ever-increasing flow of information, but understanding what it means for business and how it will impact your wide-area network (WAN) is critical. So, let's explore edge computing — why it matters, what it takes to build an effective strategy, and the individual types of technology that come together to make an edge computing solution cost-effective.

The what and why of edge computing with containers

Processing tasks happens more quickly and applications perform better when they run closer to where they are used. Edge computing enables precisely that. Connected devices can process data closer to where it's generated — or at the "edge" — decreasing how much information is sent upstream, thus reducing unnecessary traffic over the network. This increases operational efficiency by improving processing speeds and WAN resiliency and reducing costs associated with data storage, transmission, and local server operations. But what, exactly, defines an edge device?

Edge devices support networking, computing, and limited data storage, meaning they can make autonomous decisions by analyzing information on the fly without returning data to a central data center or the cloud. This could be anything from consumer products such as a mobile phone or fitness watch to an enterprise-class Wireless Wide Area Network (WWAN) router. For example, consider a building with sensors that monitor the temperature of every room. With edge computing on the WWAN router, data can be processed on-site, only sending alerts to building managers when there's a spike or temperature drop outside a desired range. Because only outlier data is sent to managers, cellular data usage, network traffic, and cloud storage are reduced significantly.

Edge computing and innovation through IoT are interlinked — IoT technology is changing how we live, work, and communicate, and edge compute helps make that possible. Whether an organization uses IoT devices to monitor building security, the status of a delivery truck's engine, or stock on retail shelves, the opportunities are seemingly endless.

"The ability to easily deploy containers for edge computing is important because it saves us from having to run a dedicated server on site for such a small payload," said Ian Beason, Product Development Manager, Motor City Wash Works.

Using containers for IoT

The world is experiencing an IoT explosion, with new devices cropping up virtually everywhere — in fixed sites, vehicles, and in the field. This widespread IoT expansion means organizations must consider complementary network architecture models to reduce network bandwidth and the high price tag associated with transferring large amounts of data to and from centralized cloud applications.

Long-term cloud storage and real-time access storage are expensive, especially for enterprises with widespread IoT deployments. With edge computing, companies reduce the amount of back-and-forth data transfer between the edge and the cloud. Intelligent edge processing capabilities allow them to only send necessary data back to headquarters or the cloud, providing huge savings in both cost and bandwidth.
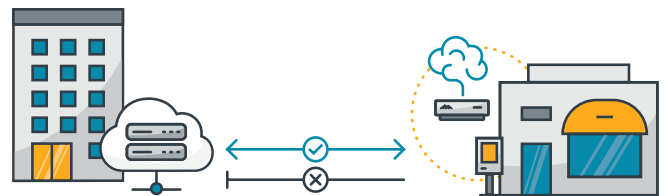
The value of WWAN solutions that support containers

Enterprises need an all-in-one WWAN solution that combines the flexibility and speed of cellular and the power of edge computing to enable today's advanced IoT applications. A wireless edge gateway or router with edge computing capabilities provides better routing, cellular connection, and network performance, all while allowing businesses to manage connectivity and security from anywhere.

Small-footprint edge endpoints are multifunctional, providing more than just connectivity. Purpose-built wireless routers connect through cellular to an existing public or private network and can manage and extend connectivity to other local devices, including through serial port, Ethernet, Bluetooth® wireless technology, or Wi-Fi.

Technologies such as IoT and AI benefit from using a wireless router because they provide sufficient computing power, enabling enterprises to process analytics, run machine learning models, and more at the edge in real time. This built-in computing allows routers to run multiple applications directly on the device, converting it into a secure and agile edge point, ready to connect workers, sites, and devices.

Edge computing also allows businesses to reduce the amount of IoT-related hardware and on-site computers using routers that support lightweight containers and SDKs. For example, an organization might use virtual containers instead of a physical gateway device to orchestrate data more efficiently at the edge, saving time, money, and space while simplifying management across the entire edge.
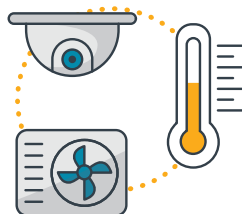
Cellular-enabled solutions with edge computing capabilities connect high-value IoT use cases across various industries, including:

Retail	Facilities management	Smart citites
— Digital signage	— HVAC systems	— EV charging stations
— Kiosks (ATMs, vending machines, and more)	— Video surveillance cameras	— Traffic control cabinets
— Point-of-sale (POS) systems	— Thermostats	— Traffic cameras

The elements of a unified IoT solution

Several different technologies can be pieced together to create a comprehensive IoT solution that leverages edge computing and cellular connectivity. Ideally, all these technologies are folded into one comprehensive solution.
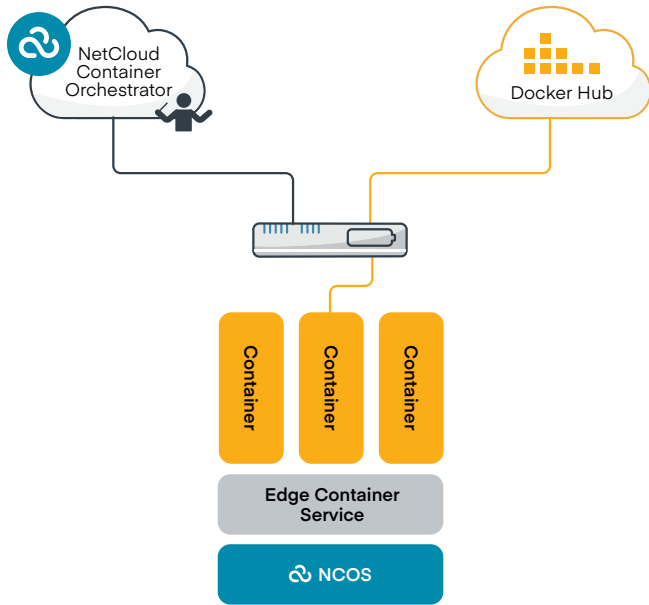
Docker container orchestration

When handling large amounts of data, enterprises can use a Docker container within a router to decentralize services by moving key, lightweight components of their application workloads to the edge environment without impacting the core functionality of the router. These allow organizations to have more technology and solutions running atop the router so that data can be processed on-site but still be cloud managed. This way, users can run applications at the edge to support a wide range of use cases, such as predictive maintenance, edge analytics, and more.

Edge containers are a large part of the edge computing story, so having the ability to monitor them remotely is important. With container orchestration, IT teams are given status updates and alerts that provide better visibility into what's happening within the container. This allows network administrators to start or stop containers running on the endpoint from anywhere.

SDKs

Edge computing can be delivered using a software developer kit (SDK) — a quick solution for companies writing their applications for enterprise routing. An SDK program runs on the router and allows an organization to write apps (typically in Python) and create custom uses to support their edge computing needs, thus reducing expenses and improving the bottom line. Once these apps are written, they can be easily deployed using a cloud-based management tool.

Connectors

Edge connectors allow for easy integration of an enterprise's edge routers or IoT gateways with third-party, industry-standard IoT platforms like Microsoft Azure IoT Central Edge and AWS IoT Greengrass. Organizations can reliably leverage pre-built cloud-to-cloud connections to connect their devices to partner applications for secure orchestration of IoT sensor data and to run edge computing applications on their WWAN routers.
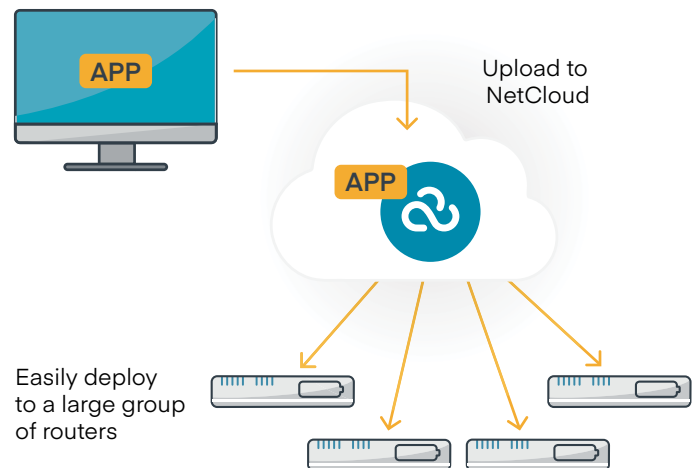
Flexible connectivity

Enterprises can benefit from using wired and cellular connections when managing a large deployment of edge devices across a WAN for better flexibility.

Waiting for wired line installation takes time that many organizations don't have. By deploying an all-in-one wired and wireless router, businesses can utilize 5G or LTE connectivity to connect locations in minutes. Once wired lines are installed, they can still utilize the existing router while transitioning the cellular connection as a redundant WAN source for failover.

Centralized management

Rapid IoT growth requires ample scalability. The most manageable IoT connectivity solutions for edge computing involve cellular routers with a cloud-based platform for monitoring and managing network connectivity and security.

Layered security features

Data security needs vary from business to business, so the ability to customize security features at the edge is critical. IoT devices struggle with typical security methods because they don't have sufficient processing and don't accept agents or updates easily. Therefore, it's important to have data security practices, such as zero trust and secure connectivity, that protect and logically separate the downstream IoT devices.

In edge computing, logical segmentation is important. Segmentation isolates one network from another using software such as containers, which fragments a network into manageable chunks to provide better visibility, easier monitoring, and increased network security.

For example, in many situations, businesses might run POS systems and IoT devices (HVAC or video surveillance) on the same router using containers. With logical segmentation, a hacker cannot gain access to the POS functions and revenue from the IoT device if the two functions are separated on their own network segments.

Learn more at **cradlepoint.com**