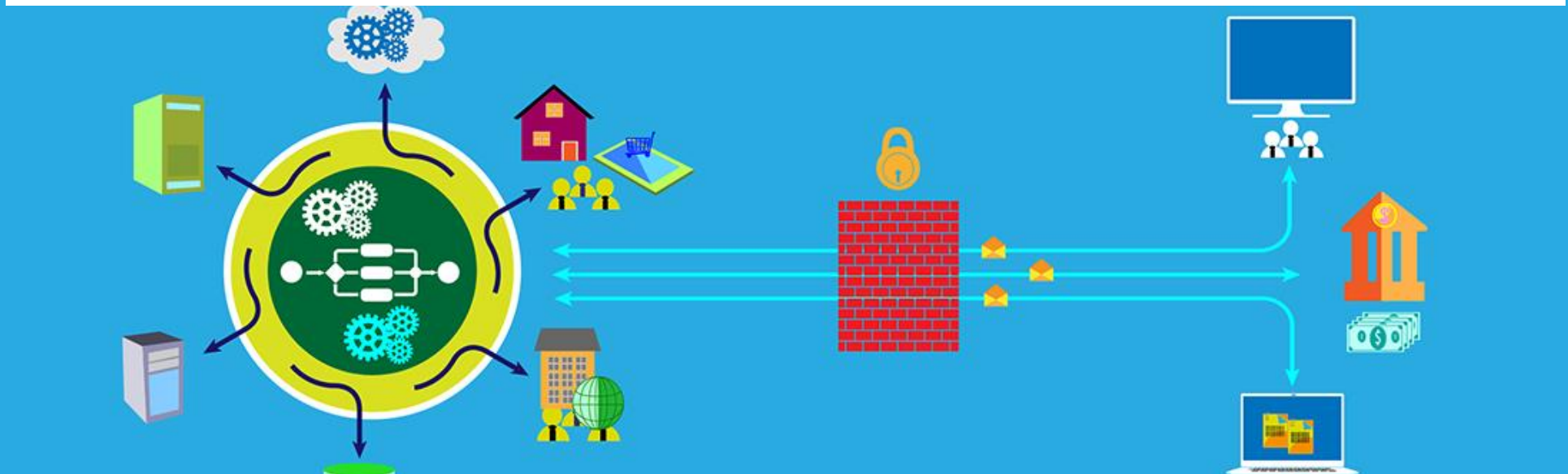
ComputerWeekly.com | TechTarget

E-guide

CW+ Content

How to prepare your network for IoT data challenges



In this e-guide

In this e-guide:

IoT and edge computing are revolutionizing the technology used across industries, and not even the network is safe from an upgrade.

For an IoT deployment to succeed, organisations must prepare their network infrastructure for a flood of data from the furthest reaches of the network to reduce latency and security risks. IT managers must understand how each piece -- including 5G, Wi-Fi, gateways, user interfaces and platforms -- of the IoT network integrates and how business priorities affect network architecture.

Each industry has its own requirements when it comes to security and data analysis. IoT networks expand the attack surface, which could put patient data at risk in the healthcare industry. Manufacturing plants need analysis to predict when machines will break to prevent extensive downtime or putting their workers at risk. A general IoT architecture upgrade will work, but to successfully deploy a network for IoT,

In this e-guide

organisations must tailor their infrastructure for that specific use.

This e-guide outlines how business requirements will affect your IoT network build, takes a deep dive into specific IoT network architecture and explores IoT topology options.

Kristen Gloss, associate site editor

In this e-guide

IoT network architecture shaped by business requirements

Linda Rosencrance, Contributor

In today's world, organisations are still unraveling IoT and designing their IoT network architecture based on current integration points rather than choosing an out-of-the-box network structure.

A successful setup depends on the type of industry or market served by the IoT applications, said Arti Bedi Pullins, founder and CEO of Pundit Consultantz in Chicago, in an email. However, most IoT infrastructure plans involve two or three layers that ultimately relay data -- either in real time or in batches -- and analytical measurements based on the data the sensor or embedded system collects.

IoT gathers and analyzes real data from the physical world and translates it into workable uses based on industry; market; consumer; or even AI, algorithmic and programmatic needs, Bedi Pullins said.

The architecture combines cloud-based data centers; core services layers; connective layering, such as Ethernet, 5G and 4G; and embedded and sensory-

based learnings, Bedi Pullins said. IoT network architecture includes a few simple layers:

- **Collection.** This is what the device or sensor on the product side collects and measures.
- **Operational.** These are the services and connector mechanics that will sit in the middle to connect and absorb all the calls, creating a gateway.
- **Distribution.** This is the end layer and how the first two layers connect and deliver data and measurements in a meaningful and absorbable way.

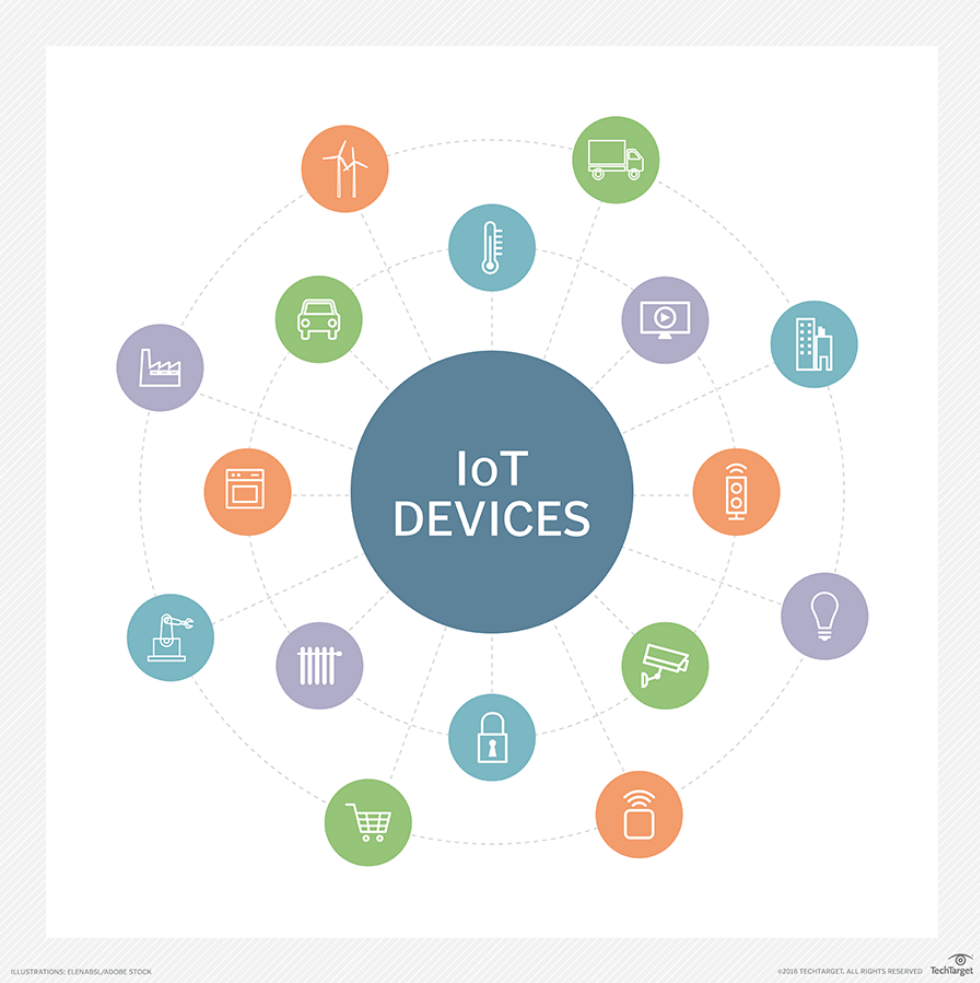
Six IoT network architecture components

People will break up a network architecture framework for IoT into different areas, according to Tim Zimmerman, analyst at Gartner.

"Of course, the first item is going to be the IoT device itself, obviously," he said. "It could be a sensor. It could be an MRI machine in healthcare. It could be a lot of things."

In this e-guide

- IoT network architecture shaped by business requirements
- A comprehensive view of the 4 IoT architecture layers
- IoT architecture layers and design change to address data deluge



The second component is communication -- how a device communicates its data -- Zimmerman said.

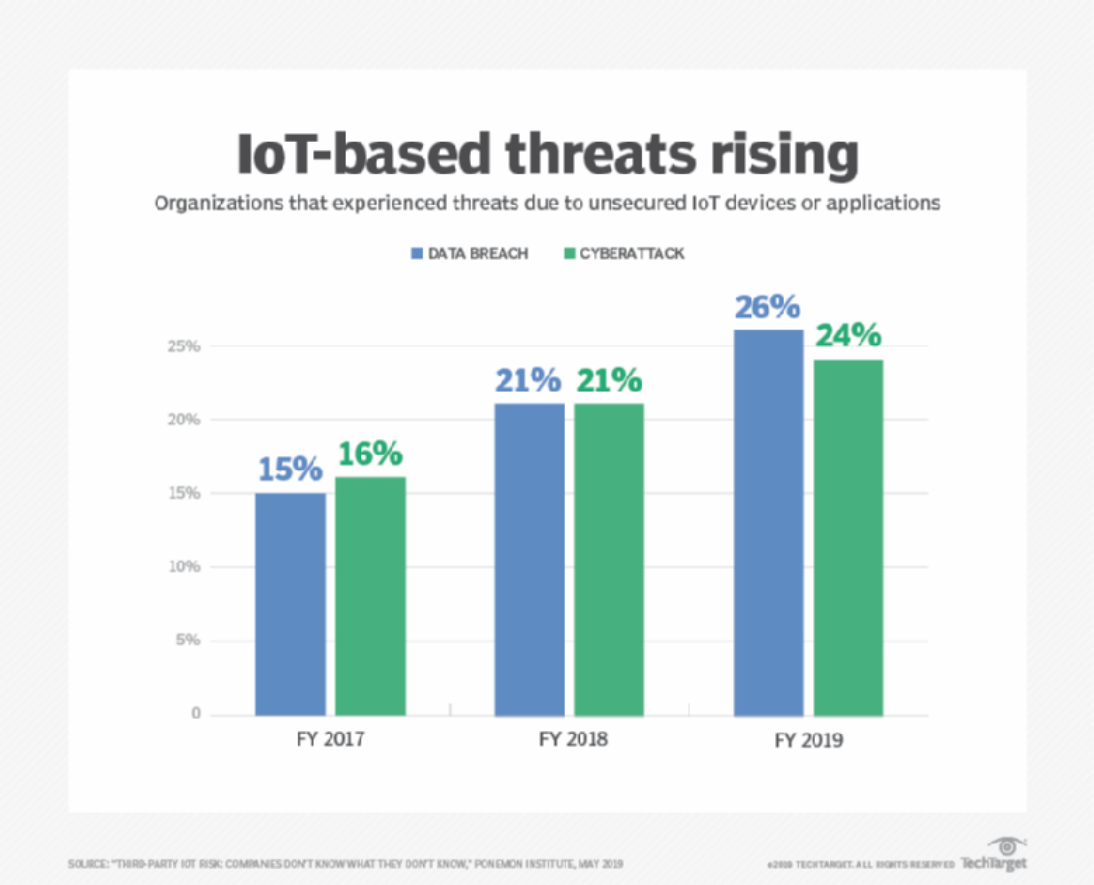
In this e-guide

There are two basic enterprise network architectures that address IoT network communication infrastructure requirements for IT organisations: wide-area communication and cloud application or on-premises communication, according to a Gartner research note co-authored by Zimmerman. Wide-area communication is typically cellular-based, including low-power WAN (LPWAN). Cloud application or on-premises communication consists of many forms of local area wireless, including Wi-Fi and private cellular.

Depending on the business, the communication technology could be a cellular network, such as with autonomous cars, Zimmerman said. In smart cities, for example, sensors on lampposts use LPWAN technology to gather data and communicate with a central control system that makes automated decisions about when they should be turned on and for how long.

The third framework component is security, according to Zimmerman. Security technologies are necessary to protect IoT devices and platforms from breaches. Connected devices that have been in use for many years must communicate safely and securely with newer connected devices.

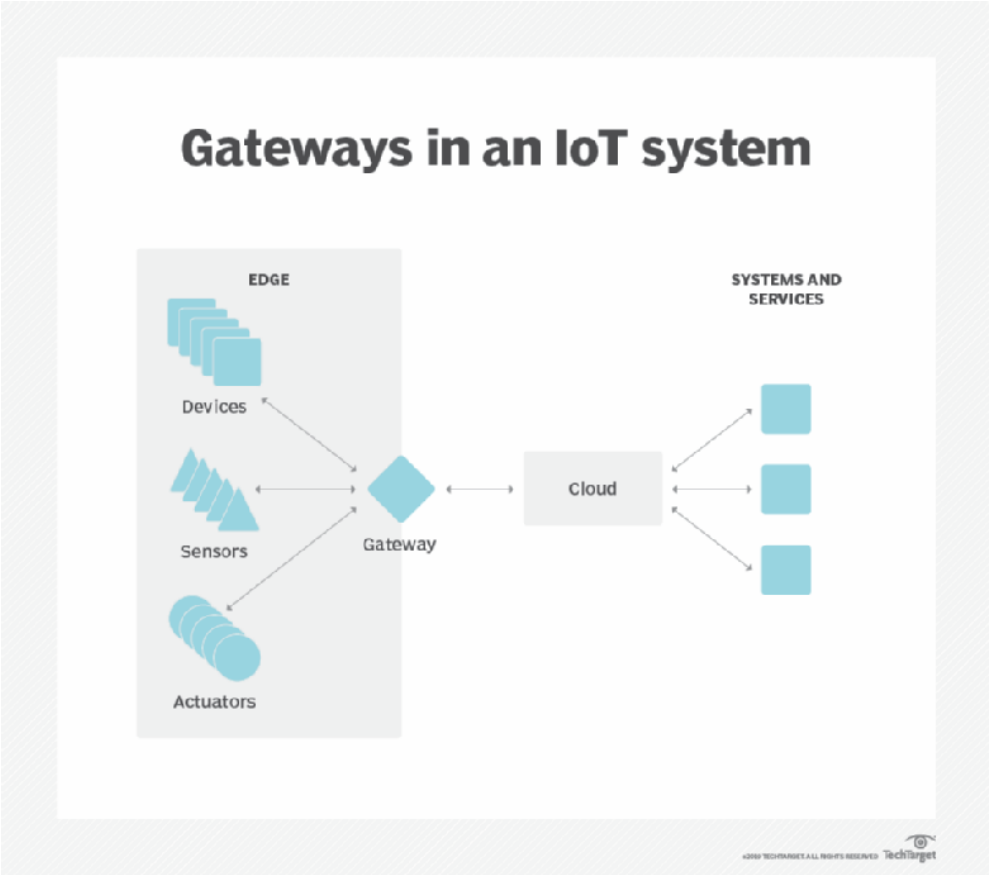
In this e-guide



"[There are] devices that are now coming onto the network that, historically, we probably never would have thought about," Zimmerman said. "From an IT standpoint, this includes things such as your HVAC, your video camera, building

automation. There are [a number of ways] that people actually try to secure these things."

The fourth IoT network architecture component is the gateway, he said. Gateways can house the application logic, store data and communicate with the internet for the things that are connected to it, according to Gartner.



Patrick Filkins, an analyst at IDC, said the primary function of an IoT network gateway is to perform protocol conversion.

"That means you may have a sensor that connects to the gateway using some sort of networking protocol, Wi-Fi, Zigbee, Bluetooth, even wired," Filkins said. "And it will take that local area connection and convert it to a much more efficient, longer wide area network backhaul connection that could have fiber optic. It could have cellular."

The fifth component is the IoT platform, which is an aggregation point for one or multiple different sites or products, Zimmerman said.

"This is where a lot of the data is collected. It tends to be where some of the upper-layer logic resides that may communicate to the gateway, but [it] also may provide direction to the applications," he said.

The final component is the application, which is kind of the user interface, according to Zimmerman. The application component uses collected data to enable users to monitor and control their cars or smart homes, for example.

Business requirements determine component arrangements

"So, there are different ways, depending on the [business] applications, that these things get stretched," Zimmerman said. "All the components exist, but where they reside may differ just a little bit depending on what the outcome needs to be. When I work with clients, it's important to understand what the

business outcome is that they're trying to achieve and then look for all the components that may affect some of the decision-making capabilities within the framework."

In healthcare, consumer-based health data collected directly from physician-based sensors embedded within a stethoscope, glove or patient beds can interface with the operational side of the health system to deliver meaningful information, Bedi Pullins said.

However, the level of personally identifiable information and patient-level data security will be structured completely differently than for autonomous vehicles, she added.

Zimmerman said that before building or adding to existing systems there are certain questions an organization should answer regarding its proposed IoT network architecture. What kind of communication will be used? What is the distance that will be covered? Where will the sensor be located? How often will you communicate with the sensor? What kind of sensor is it? What kind of security does it have? Do you have a security policy?

"Because there are so many ways you can connect the dots, these are all the precursor types of questions that you really have to answer upfront," he said. "While all the components of the framework will exist, the complete solution -- the way you connect the dots -- is going to be different depending on the answers."

In this e-guide

A comprehensive view of the 4 IoT architecture layers

Johna Johnson, President and Senior Founding Partner

If your company is like many organisations, it's actively engaged in or considering launching one or more IoT initiatives. It has a goal, a strategy and a desired outcome -- whether to drive revenue, cut costs or optimize business processes. And it may have already selected technologies and suppliers.

But does it have an IoT architecture? And is that architecture specific to this project or a customized version of a more general IoT framework?

You might be wondering why either of those matter -- two reasons. First, organisations with an IoT architecture are significantly more successful than those without. Successful companies -- those that rank in the top third of all companies when it comes to saving money, driving new revenue or improving business processes via IoT -- are 34% more likely to have an IoT architecture than less successful firms.

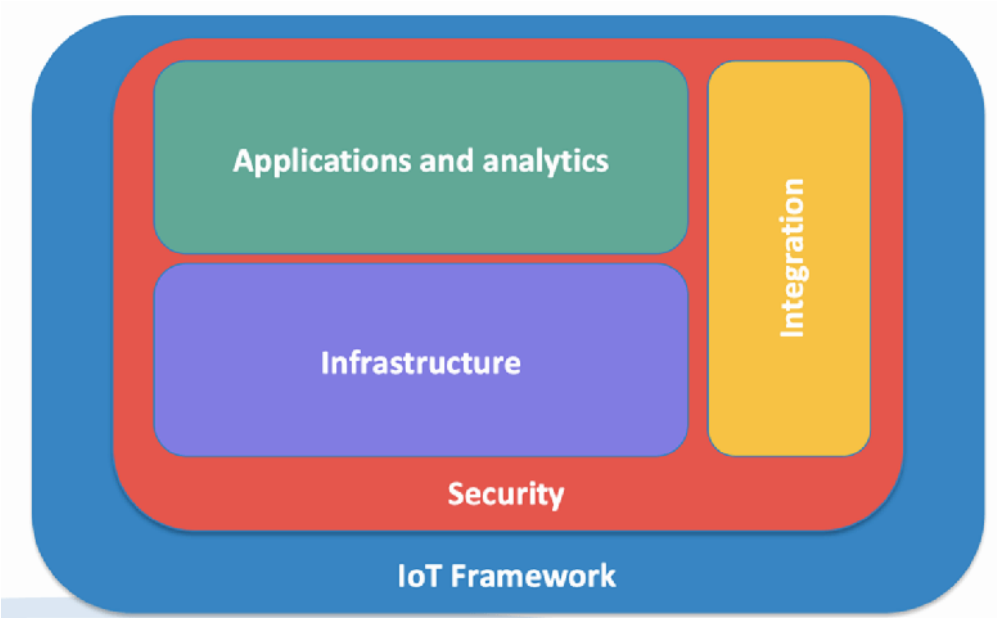
But that's not just any architecture, which brings us to the second reason it's important. Successful companies are more likely to adhere to an architecture

that includes both a general-purpose IoT framework and a specific, customized version for the specific IoT project.

Why both? IoT isn't a stand-alone initiative; it's an extension of IT to the physical world. That means it needs the same strategy and planning that any technology initiative requires, including a plan for how it will integrate into your organization's existing systems and infrastructure.

The four IoT architecture layers

At a high level, an IoT architecture comprises four components: applications and analytics, integration, security and infrastructure (see Figure 1).



The **applications and analytics component** is the piece that processes and displays the information collected via IoT. It includes analytics tools, AI and machine learning, and visualization capabilities. Technologies for this component range from traditional analytics and visualization packages, such as R, IBM SPSS and SAS, to specialized IoT tools and dashboards from cloud providers, such as Amazon, Google, Microsoft, Oracle and IBM, as well as application suite vendors, including SAP, Salesforce and others.

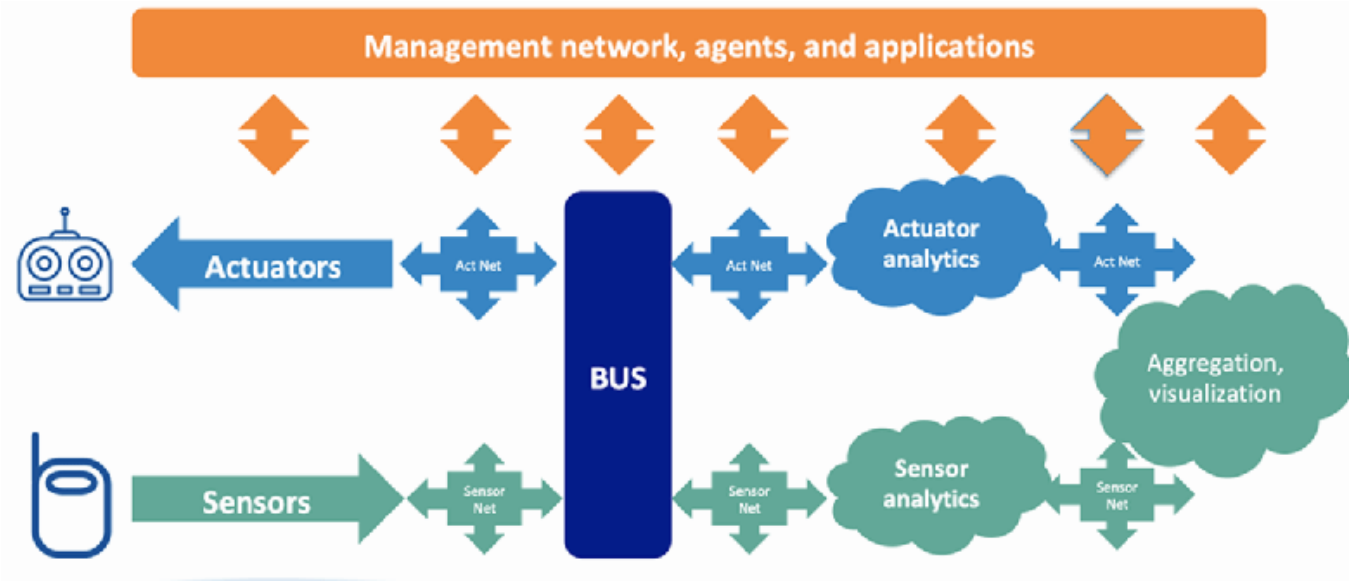
The **integration component** is one that's often overlooked by IoT teams, yet it's crucially important. This is the component that ensures that the applications, tools, security and infrastructure integrate effectively into existing companywide ERP and other management systems. Providers include the aforementioned software and cloud players, as well as a range of open source and middleware providers, such as Oracle Fusion Middleware, LinkSmart, Apache Kafka and DynThings Open Source IoT Platform.

Security is another component that's often overlooked. IoT security includes securing the physical components of the system via firmware and embedded security providers, such as Azure Sphere, LynxOS, Mocana and Spartan. Traditional security vendors, such as Forescout, Symantec and Trend Micro, also offer packages that focus specifically on securing IoT.

Finally, there's the **infrastructure component** (see Figure 2). This includes physical devices -- IoT sensors, which capture information, and actuators, which control the environment. Communicating with, controlling and capturing

In this e-guide

information from the sensors and actuators require a set of networks and platforms. There's the physical network on which the sensors or actuators actually reside; typically, though not always, this is a wireless network, such as Wi-Fi, 4G or 5G. However, data from this network needs to be processed and analyzed, which means it must be transported from the IoT location to the platform, either at the edge or on the cloud, where processing happens. Since the actuator and sensor infrastructure are often different, there may be a different cloud on which the information from the two is combined -- for instance, if a company is monitoring a remote facility via automated cameras, detects a disturbance and wishes to dispatch a drone fleet to that facility. Managing and controlling the IoT infrastructure requires a management layer, complete with agents and applications.



In this e-guide

Do all IoT initiatives require such a complex architecture? No and certainly not at first. However, it's important to recognize that these components will likely become critical downstream, and having an architecture enables IoT architects to plan intelligently for that day and beyond.

Bottom line: Have an IoT architecture for any IoT initiative you're launching. This architecture should make clear how you handle the four components of applications and analytics, integration, security and infrastructure. And your infrastructure architecture should include plans for how you'll design and manage the networks and platforms that you will ultimately require.

In this e-guide

IoT architecture layers and design change to address data deluge

Scott Robinson, Director of business intelligence

IoT architecture layers and topologies are in a state of flux; how IoT grows and what options emerge for new network design will have a tremendous effect on how IoT expands as the world moves forward.

No proliferating technology -- not telephones, televisions, automobiles, computers, video games or even cellphones -- has ever grown and spread across the landscape as rapidly as IoT. Of course, computers, video games and cellphones are all, by definition, now part of IoT. IoT even absorbed innocuous devices, such as wristwatches, thermostats, video cameras, door locks, and electrical sockets and switches in buildings.

By the end of next year, the number of devices connected to the internet will approach 40 billion. The problem is that much -- if not most -- of that data is bound for clouds. The number of IoT devices grows by billions every year, but the number of cloud platforms or additional servers within existing clouds only increases at less than 1% of that rate. That's a serious traffic problem in the making.

In this e-guide

IoT proliferation doesn't just create unprecedented digital traffic and all the associated problems; it creates entirely new categories of security concerns because it expands the attack surface by an order of magnitude. The growth increases the need for cleaning and validating data before it even reaches the cloud. IoT expansion has opened up opportunities for new application categories that need machine learning and AI beyond the enterprise firewall, and IoT requires new standards for data usage and storage. Put simply, the need for new and better IoT architecture layers and topologies has never been greater.

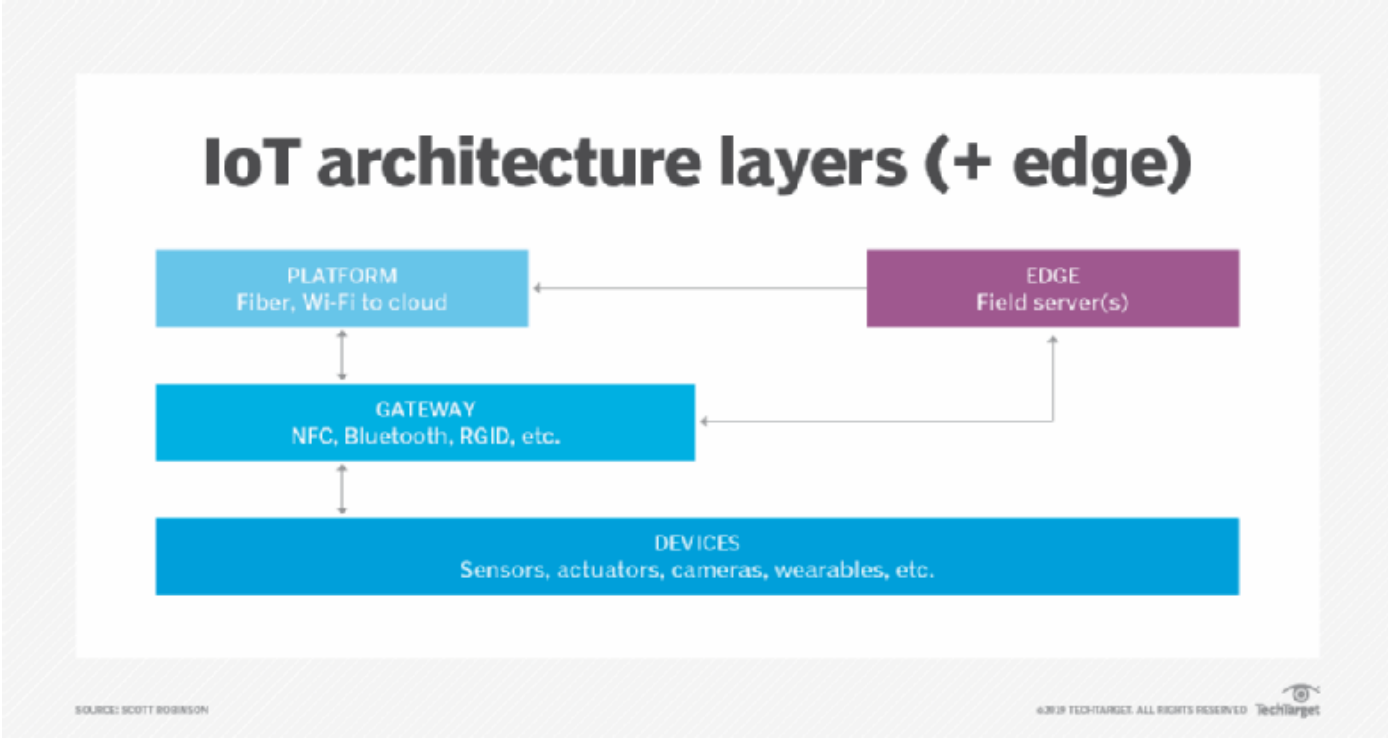
Edge computing addresses IoT architecture layers' needs

The existing IoT architecture is based on a tried-and-true model that is highly scalable and extensible, and it accommodates a broad range of topologies. Even this entrenched model, which consists of three IoT architecture layers, is currently undergoing big changes. The three layers are the following:

1. **Device layer.** This is the client side where all devices, including sensors, switches, actuators and cameras, gather or respond to data live.
2. **Gateway layer**. This layer congregates data from IoT devices and jumps onto the internet or terminates in a data acquisition system. Analog-to-digital conversion of IoT data often happens in this layer.

In this e-guide

3. **Platform layer**. This pathway connects clients and operators, often terminating in a cloud or a data center.



These three layers don't include several resources that IoT needs. Organisations need better tools for local data analysis and routing. IoT generates more data than traditional networks by orders of magnitude; it is

prudent to screen unnecessary data before dumping it in cloud or data center storage. It's also necessary to figure out what data goes where as it's created if the data is going more than one place, rather than sending it to one destination and then moving it again to another.

Many IoT networks require enhanced processing to respond to IoT applications in real time. There isn't time for data to make a round trip to a cloud. Examples include support of driverless vehicles and facial recognition. Local processing resources make this technology practical.

Increasingly, IoT networks become intelligent and respond to activity in the real world. Here, too, there isn't always time for cloud traffic. It's more effective to have machine learning and AI resources embedded in the architecture, especially when the data for machine learning doesn't have a separate use in the cloud.

To meet these needs, a new IoT architecture layer is currently emerging: the edge layer. Sandwiched between the gateway and platform layers, the edge is a new innovation in IoT architecture that provides all of the resources above.

Edge computing is the practice of placing servers in the field -- often beyond the enterprise firewall and certainly beyond the physical server farms that host clouds -- in the proximity of the IoT devices they support. This distributed computing paradigm is not new but represents an innovative answer to IoT problems. Edge nodes can provide in-the-moment data cleansing and routing, as well as real-time turnaround in complex applications with far less latency,

and they make it possible to place machine learning where IoT lives. Nodes can also serve as a bulwark against IoT's expanded attack surface, increasing the security of the gateway layer.

How to choose the right IoT topologies

Within this basic architecture model, an organization can use a number of topologies for distribution and interconnection of IoT elements. It's important to make good choices here because these IoT topologies are specifically engineered to accommodate networks with specific uses. All of them interact with the gateway layer in different ways, and a bad design could limit the network's performance, compromise security or even render some applications impossible. The most versatile topologies are point-to-point, star and mesh.

A point-to-point network has a one-to-one connection between nodes; communication only happens between the two points. This is the simplest and cheapest configuration. The downside is that point-to-point configurations aren't scalable. No redundancy is possible, so there is no graceful degradation. Typically, this is just a simple connection, such as an earpiece to a cellphone or a single device accessing the internet at a single point.

In a star network, many nodes connect to a central hub. The cardinality of the hub is one-to-many. But none of the nodes connect to each other; they only connect to the hub. This configuration tends to have low latency and be consistent. Network tools can easily detect and isolate faults. On the downside,

although reliability is generally high, there is no rerouting if interference occurs. In addition, the hub represents a single point of failure for the entire network. For example, home Wi-Fi has many devices reaching the internet through a single router.

A mesh network includes multiple device, gateway and router nodes. Mesh networks have high scalability and redundancy, as well as exceptional fault tolerance. The downside of mesh configurations is considerable complexity and a high maintenance requirement with increased latency from the multiple hops data packets must make. Mesh networks include industrial automation, large-scale fire monitoring and security, and energy management systems.

To decide which IoT topologies will work best, consider the complexity that can be supported and prioritize latency, fault tolerance, reliability and whether the network needs to scale.

IoT architecture layers and topologies make a well-organized mess

Once an organization decides on an IoT network's architecture and topology, additional questions will arise. What are the best practices involved in managing the network? How does the new network affect the security of the systems it is interacting with? Who owns what?

IoT network administrative standards and best practices have been established, but like IoT architecture itself, they constantly evolve. The truth is there's a

In this e-guide

make-it-up-as-you-go factor in IoT. On the technology side, this method is considered a good thing. Siloed, do-it-all platforms have had their day, and the organic nature of IoT portends a more versatile digital landscape. It calls for greater planning, diligence and innovation than have ever been required before.

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com

© 2019 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.