White Paper

Cisco Fog Computing Solutions: Unleash the Power of the Internet of Things

Connect things. Analyze and act on the data they produce in milliseconds. Then send the right data to the cloud for big-data analytics and storage.

Benefits

Only Cisco Fog computing solutions provide the following benefits:

- **Data privacy:** When necessary, analyze sensitive data within the building instead of sending it to a remote data center. Cisco Fog Data Services applies your policy to determine the best place for analysis.
- **Comprehensive security:** Protect fog nodes using the same Cisco physical security and cybersecurity solutions you use to protect other IT assets. These solutions provide the capabilities you need before, during, and after an attack.
- **Business agility:** Gain business insights more quickly by hosting applications closer to your IoT devices and analyzing data closer to the source.
- **Rapid innovation:** Create and deploy new applications more quickly by using our infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) offerings. Or skip development altogether by taking advantage of industry-specific fog applications from our ecosystem partners.
- **Lower operational expense:** Simplify management using Cisco Prime or the Cisco Industrial Operations Kit. Conserve network bandwidth by analyzing data on fog nodes, when appropriate, instead of sending data to the cloud for analysis.

The Internet of Things (IoT) speeds up awareness and response to events. It's transforming whole industries, including manufacturing, oil and gas, utilities, transportation, public safety, and local government.

But the IoT requires a new kind of infrastructure. The cloud by itself can't connect and analyze data from thousands and millions of different kinds of things spread out over large areas. Capturing the power of the IoT requires a solution that can:

- Connect new kinds of things to your network. Some of them might be in harsh environments. Others might communicate using industrial protocols, not IP.
- Secure the things that produce data. And secure the data as it travels from the network edge to the cloud. This requires a combination of physical security and cybersecurity.
- Handle an unprecedented volume, variety, and velocity of data. Billions of previously unconnected devices are generating more than two exabytes of data each day. Sending all of it to the cloud for analysis and storage is not practical. Plus, in the time it takes to send data to the cloud for analysis, the opportunity to act on it might be gone.

Cisco® Fog computing solutions meet all of these requirements. They're part of the Cisco IoT System, a comprehensive set of products for deploying, accelerating value, and innovating with the Internet of Things. Cisco Fog computing solutions include everything you need to:

- Connect any kind of IoT device.
- Secure your IoT devices and protect the data they produce as it travels between the network edge and the cloud.
- Quickly develop and deploy fog applications.
- Direct data to the best place for analysis: fog nodes or your data center cloud platform. The decision depends on how time-sensitive the decision is as well as data-privacy requirements.
- Automate provisioning and simplify management of large numbers of fog nodes spread out over large areas.

Cisco Fog Computing Solution Components

Get everything you need to build a Fog computing solution from the Cisco IoT System. It includes products from Cisco and our partners for:

- Network connectivity
- Physical and cybersecurity
- Fog application development and hosting
- Data analytics
- Management and automation

Network Connectivity

Choose from a wide variety of fog nodes to connect your IoT devices. Options include Cisco routers, switches, wireless access points, and video surveillance cameras, and Cisco Unified Computing System (UCS) servers.

All Cisco fog nodes have converged compute, networking, and storage, which simplifies management and reduces power and space requirements. You can develop and enhance IoT applications in the cloud, and then deploy them to run in the cloud and in the fog. The same application can run on different kinds of fog nodes without modifications.

Integrated Physical Security and Cybersecurity

IoT data needs to be protected on fog nodes as well as in transit from fog nodes to the cloud. To control physical access to fog nodes deployed in remote areas, such as utility field substations or alongside roadways and railways, use Cisco video surveillance and access control solutions.

Protect data as it travels between fog nodes and the cloud by using Cisco cybersecurity solutions. They provide protection before, during, and after attacks. For example, detect anomalous activity using Cisco NetFlow, Cisco TrustSec, and Cisco Identity Services Engine (ISE). Prevent breaches using Cisco Advanced Malware Protection. Respond to anomalous activity by automatically enforcing security policy. With Cisco Intrusion Prevention System (IPS), the security policy can take into account the target of the threat. In IT environments, the response to a threat might be to quarantine or shut a system. In an operational technology (OT) environment, the response to the same threat might be to alert system operators who have the knowledge to decide on the best action.

Application Platform

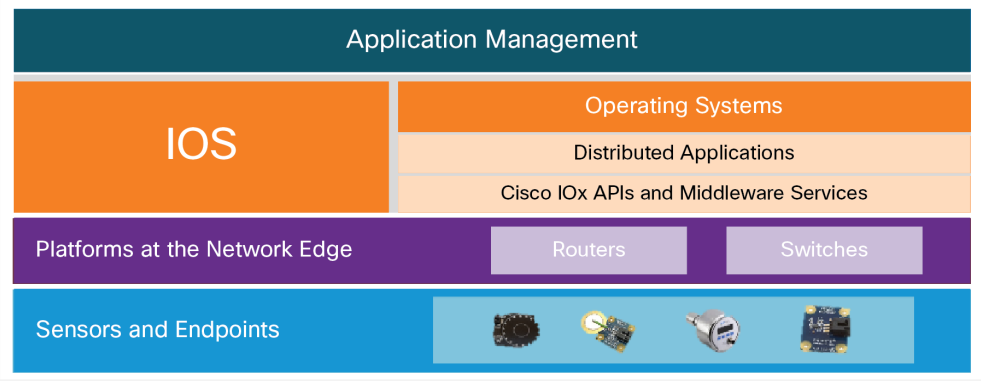
To simplify fog application development, we've replicated the familiar cloud application development model. That's software as a service (SaaS) built on PaaS and IaaS. Here's how it works:

- **IaaS**: Host new or existing applications on fog nodes. Use the Cisco IOx API, which combines the Cisco IOS® operating system and Linux (Figure 1). Cisco IOx currently works with Cisco routers. A manufacturer, for example, could use Cisco IOx to host Rockwell FactoryTalk software on factory-floor routers. Using Cisco IOx APIs, your fog applications can communicate with IoT devices that use any protocol. Fog applications can also send IoT data to the cloud by translating non-standard and proprietary protocols to IP.
- **PaaS: Develop fog applications.** Our first IoT PaaS offering, called Cisco DSX, simplifies fog application development in several ways:
  - Device abstraction: Fog applications need to communicate with many types of IoT devices. Creating a separate application for each vendor's temperature sensor, for example, would be impractical. Cisco DSX saves application developers this effort by providing an abstracted view of IoT devices.
  - Support for multiple development environments. IoT applications that deliver machine as a service (MaaS) are typically developed in various environments and programming languages. With Cisco DSX, fog nodes can support multiple development environments.
  - Simplified management of fog applications. Managing a growing number of fog applications would also be impractical. Cisco DSX simplifies management and automates policy enforcement.
- **SaaS:** Offer MaaS. Using Cisco DSX, a robot vendor, for example, can specify the functions a particular customer can use. The customer pays only for these features. The vendor can later give the customer access to additional features by making a simple software change from headquarters.

How Cisco IOx Works

Cisco IOx hosts applications in a Guest Operating System (GOS) that runs on a hypervisor on a Cisco fog node (Figure 1). Cisco IOx comes with Yocto Linux, but developers can use any operating system.

Figure 1. Cisco IOx Makes It Possible to Offer Fog Infrastructure as a Service



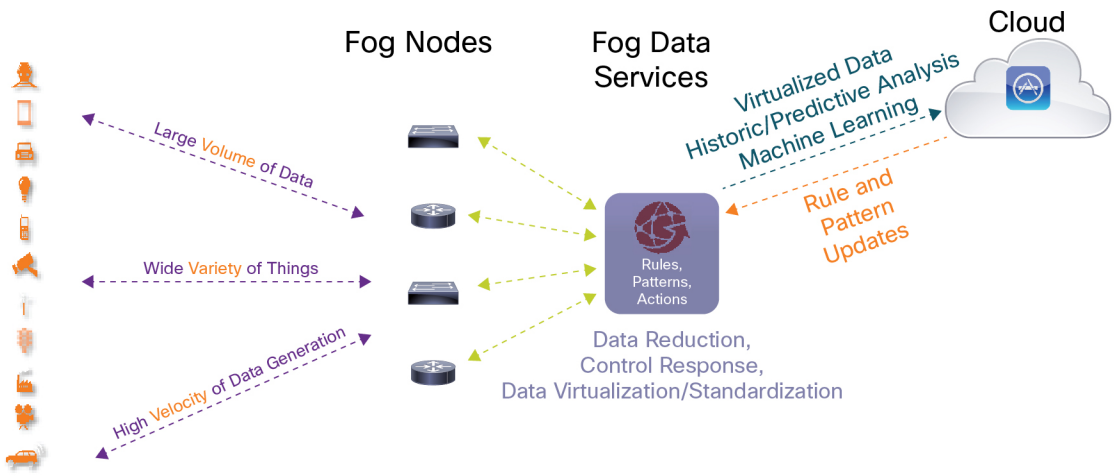
Data Analytics: Cisco Fog Data Services

Manage the volume, variety, and velocity of IoT data by using Cisco Fog Data Services (Table 1). These services direct data to the right place for analysis—cloud or fog—based on your policies (Figure 2). Analyzing IoT data close to where it's collected minimizes latency. It offloads gigabytes of network traffic from the core network. And it keeps sensitive data inside the network. Developers access the Cisco Fog Data Services as REST APIs through Cisco DevNet.

Table 1. Cisco Fog Data Services

Type of Service	What the Service Does
Coordinate what happens in the cloud versus the fog	Applies business rules to decide which data to process locally and which to send to cloud. Dynamically adjusts rules based on pattern recognition, prediction, and anomaly detection
Analyze	Identifies data that requires action, such as a temperature reading above or below a specified threshold
Secure	Makes data anonymous by hiding the source

Figure 2. Fog Data Services Coordinate the Movement of Data from Fog to Cloud



To understand the value of Cisco Fog Data Services, think about high-speed commuter rail systems. Constantly streaming live video over the cellular network would be prohibitively costly. Therefore, most operators store video from onboard video systems on the train, waiting to transmit it until the train arrives at a station with Wi-Fi. If the train derails, however, streaming video over the cellular network becomes worthwhile because passenger safety is at stake. Using Cisco Fog Data Services, the application developers could write a rule stating that if sensors detect hard braking and train tipping, live video should be streamed over the cellular network to the operations center.

Management and Automation

Depending on the industry and application, fog nodes can number in the hundreds, thousands, or tens of thousands. Automate provisioning and simplify management of your fog nodes using Cisco management applications.

Organizations that have field area networks, including utilities and transportation and mining companies, can manage fog nodes using the Cisco Connected Grid Network Management System (CGNMS), which is part of the Cisco Industrial Operations Kit (IOK). Cisco IOK is a one-box solution: a Cisco UCS server with virtualized services, such as virtual router; network management; security; authentication, authorization, and accounting (AAA); zero-touch deployment; a network server; and a self-configuration tool. Virtualized servers and routers reduce upfront deployment and ongoing management costs. And included scripts reduce the time to configure network services from weeks to days.

Manufacturers manage their fog nodes using Cisco Prime Infrastructure. Administrators use a single interface to manage the network, fog nodes, applications, and users.

You can also deploy your own management and automation tools on Cisco fog nodes, using Cisco IOx APIs.

Use Cases

Rails	Real-time intelligence about conditions and events on trains, trackside, at stations, and the operations center helps you: • **Improve passenger safety:** Analyze and correlate data from ruggedized cameras on the trains and at stations. Monitor sensors on wheels and brakes to determine when parts need service before failure causes an accident. Automatically stream video from onboard video surveillance cameras to the operations center if sensors detect a derailed car. • **Thwart cybersecurity attacks on critical operational systems:** Then take automated actions such as suspending operations or transferring control to a failover system. • **Alert drivers to treacherous conditions ahead:** Fog nodes gather sensor data on tracks and trains to detect unsafe conditions. Drivers are automatically alerted so that they can adjust speed to safe levels. Supervisors also receive alerts if the train is operated in an unsafe manner. • **Increase rider satisfaction:** Provide Wi-Fi in rail cars. The access points connect to onboard fog nodes. In addition to providing passenger Wi-Fi, the fog nodes connect with trackside Wi-Fi access nodes to relay real-time information about the various systems on the train.
Manufacturing	• **Increase agility:** Quickly change production lines and introduce new products. Fog nodes can translate instructions from IP to the proprietary industrial protocols used by plant-floor equipment. • **Reduce downtime:** Avoid costly equipment downtime by performing predictive maintenance. Fog nodes collect machine data and report early signs of problems. • **Secure machines and data:** Analyze data from network devices to detect the earliest signs of network attacks that could threaten personnel or plant safety. • **Authorize access to machines:** Before granting access to a machine, verify that the person is who he or she claims to be and is authorized to use that specific machine. • **Continually confirm that safety systems are intact:** Analyze machine data that's transmitted in different formats, in real-time. Shut down compromised equipment automatically, without waiting for a human to respond to an alert.
Utilities	• **Restore power more quickly:** Fog nodes gather data from the power plant, grid, substation, and customer endpoints. They continually analyze the data to identify incipient problems and alert the system operator. • **Detect potential physical security breaches:** Ruggedized cameras at remote field substations detect breaches, and also correlate events across multiple locations. • **Detect potential cybersecurity breaches:** Automated response helps to prevent infections that could jeopardize safety. • **Reduce maintenance costs and increase system reliability:** Fog nodes gather data from critical systems and look for evidence that systems need maintenance. Predictive maintenance helps to prevent outages and can lower costs. Diagnose and solve problems from anywhere. Sensors throughout the system send alerts about power fluctuation, spikes, and other critical events.

Why Cisco?

Everything You Need and a Broad Selection

Only Cisco provides everything you need to develop, host, and manage applications that span from cloud to fog:

- **Network connectivity:** Choose from many different types of fog nodes, including switches, routers, Cisco UCS servers, and video surveillance cameras. Ruggedized versions are available.
- **Security:** Secure your fog nodes and data using your existing Cisco physical security and cybersecurity solutions.

- **Analytics:** Direct data to the right place for analysis, either a fog node or your cloud platform, using Cisco Fog Data Services. The policy can state that latency-sensitive data is to be analyzed on fog nodes.
- **Management and automation:** Simplify deployment and management of large numbers of fog nodes using Cisco Prime or Cisco CGNMS.
- **Application platform:** Get innovative with the Internet of Things by using Cisco IOx APIs and Cisco DSX to very rapidly develop fog applications. The same application can run on any Cisco fog node: switch, router, Cisco UCS server, or video surveillance camera.

IoT Leadership and Investments

Cisco is actively involved in the industry groups developing cloud and fog standards. That means the solutions you get from us reflect the latest thinking and are continually updated to the latest standards. We are also cultivating startups working on promising Fog computing innovations.

IoT Ecosystem Partners

Our growing ecosystem of partners is developing cloud-to-fog applications for industries such as manufacturing, oil and gas, utilities, transportation, public safety, and local government. Using a commercial application can speed up innovation while saving time and development costs.

IoT Services for Your Industry

Gain deeper insights into the IoT data you collect in the cloud with Cisco Connected Analytics software portfolio. Use it to view real-time information, spot trends sooner, and make predictions that give you the lead. Supplement this information by engaging Cisco Services for data virtualization, sophisticated data analytics consulting, and data science services.

Next Steps

Fog computing is here today. It can make your business more agile, faster to respond, and more innovative with IoT. And everything you need is available from one vendor, us.

To learn more about the Cisco IoT System, visit www.cisco.com/go/iot.

For APIs to develop IoT applications, visit Cisco DevNet: https://developer.cisco.com/iot.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-734589-00 05/15