



Securing the Internet of Things for the US Public Sector

How to build a secure foundation, reduce risk, and implement solutions



The current state of the Internet of Things: benefits and challenges

The adoption of Internet of Things (IoT) technologies by public sector entities can result in many benefits: increased public safety with video surveillance or street lights, traffic management systems to control vehicle flow, Supervisory Control and Data Acquisition (SCADA) for utilities, and enhanced medical experience with connected infusion pumps and monitoring systems that communicate with patient records systems. Providing these and other new capabilities, all while increasing employee productivity, is one of the key reasons we are seeing an explosion of IoT deployment in the public sector.

The basic concept of IoT is to have a sensor that performs a certain function and, based on that function, collects data that can be stored or sent to a controller. The data is collected, correlated, and analyzed so that it can then provide insight and spur an action. Sensors come in many shapes and sizes, and can be as simple as detecting temperature, soil content, or a motion. But they can also be more complex, such as those used in vehicles or medical devices. Complex sensors are usually made up of hardware, an operating system (OS), and an application. They communicate to and send data to a controller that is sitting in a cloud or a data center.

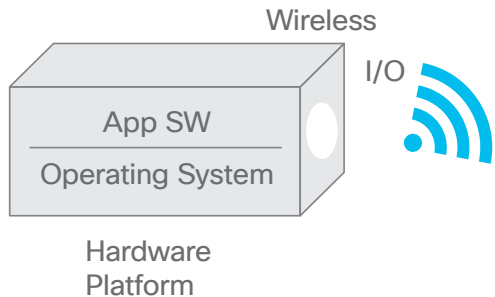


Figure 1. Typical IoT Sensor



To benefit from IoT, agencies and institutions must shift their environment to support this new and exciting approach. The breadth of IoT goes well beyond the traditional carpeted hallways of information technology (IT) departments. To achieve the best user experience, agencies and institutions need to address specific areas of concern, including:

- **Device connectivity:** Wireless technologies are the typical access method for IoT, but wired connectivity (including RS-232, RS-485, Ethernet, and others) is also available.
- **Device placement:** Devices could be placed in areas that are not physically controlled.
- **Device proliferation:** IoT devices could outnumber typical IT devices exponentially.
- **Device vulnerabilities:** Many IoT devices are not made by IT companies.

Based on these concerns, new strategies must be put in place to manage the sheer volume of devices and the infrastructure needed to support them. Additionally, given the types of devices that will be placed in the network and their diverse locations, a clear strategy must be implemented to secure IoT devices and the data that will be extracted from them.

How to build a secure foundation for IoT

For a chief information security officer (CISO), IoT can seem like a nightmare. Unlike traditional office automation, IoT devices can be, and usually are, deployed outside traditional carpeted areas. Combined with the sheer number of devices connected in an IoT environment (and the nascent technology being used to connect the non-IT devices), a complex set of security challenges results, as does the question, “How can we successfully address these security worries?”

At Cisco, our approach is to break up the problem set into four areas, with the goal of thoroughly understanding and addressing the challenges of each.



1. Device connectivity

IoT devices often leverage wireless technologies to connect to a network. Many of these devices will use Wi-Fi, but more will use technologies like 4G, 5G, Bluetooth Low Energy (BLE), and Low-Power Wide-Area Network (LPWAN).

In the public sector, we see sensors providing environmental feeds along sides of roads, video cameras and lights on street corners, and indoor sensors to control access to medical equipment or to schools and other buildings. The wireless technology will be selected based on the wireless availability, the capabilities needed from the wireless technology (long distance vs. short distance), and the power consumption of that wireless technology. Some sensors will have a limited power source with long-term life expectations, and some wireless technologies are adapted to that environment. Plus, the different wireless technologies may have different security capabilities that must be understood and appropriately accommodated.



2. Device placement

Because IoT is about connecting typically unconnected devices to the enterprise network, we should consider that these devices can and will be placed anywhere. Devices could be placed in areas that are not physically controlled. As a result, it may be necessary to physically secure the device to ensure its viability.

We must also remember that the primary purpose of the IoT sensor is to collect data and then send it to a controller. As a result, it is just as important to secure the data while on the device and as it is in transit from the device to the controller. This isn't always easy since devices could be located anywhere and are using different wireless technologies. And, unfortunately, it's not too difficult to extract data from unsecure and non-encrypted wireless systems. So that also becomes a critical concern for all IoT systems.



3. Device proliferation

In many public sector IoT use cases, such as public safety and transportation, agencies can be adding thousands (even tens of thousands) of devices to be managed and secured on their network. It's estimated that IoT devices [will number 55 billion by 2025](#), or more than seven times the world's population.

Managing this tsunami of devices creates many challenges – from basic patch management to systems management to data proliferation for connected devices. Because of these needs, the workload placed on an IT department will increase. As a result, we believe managing and securing this new environment will require much more device visibility, network analytics, and automation to reduce the need for human actions within the overall system.



4. Device vulnerabilities

IoT sensors introduce several threat vectors to an enterprise environment. These devices are made up of hardware, an OS, and an application to perform the function of the sensor. Each of these layers introduces a point of concern, especially considering there may be thousands of these sensors. One of the complications of IoT is the numerous operating systems being used by these sensors (including different flavors of Linux, FreeRTOS, WindRiver, Google Brillo, and Arm Mbed OS). Add the fact that many IoT manufacturers are interested in developing a minimal viable product to beat their competition to market, and security issues of support and control become even more evident. Programmable Logic Controllers (PLCs) may also introduce vulnerabilities into the environment.

Besides the numerous operating systems, there are many hardware platforms from the sensor vendors, and most of the systems today are purpose built. The nature of many of these sensors is to communicate back to a controller, a gateway, or another device to upload information and get instructions, which makes for a simple deployment but adds yet another attack vector.

Finally, since many IoT devices are battery operated, many of these systems are designed to consume as few resources as possible. Others are designed for high-capacity processing, implementations such as video analytics, analog-to-digital data processing, fog computing, and so on.



The variety of systems and lack of commonality in this developing field nearly eliminates the ability to create a “standard” security package that is ubiquitous to all systems. One could state that having a variety of sensor models may provide security through obscurity, but one could also argue that it adds complexity to the entire enterprise. The combination of numerous operating systems, unique applications, and short time to market could mean a recipe for disaster if not addressed. The chart below summarizes the security concerns seen in a typical IoT architecture.

Security concerns	Specific threats	Threat vector
Data in motion attack	Unsecure wireless Gateway (GW) vulnerability	Man in the middle DOS attack (initiator) DOS attack (receiver)
Sensor compromise	OS vulnerability Hardware vulnerability App vulnerability	Device offline Bot membership Data corruption Data exfiltration
Data at rest attack	Server attack Application attack Database attack	Data exfiltration Data corruption

Table 1. IoT areas of concern

What can you do to mitigate your risk?

Understand your risk, then develop a plan to protect your IoT domain(s)

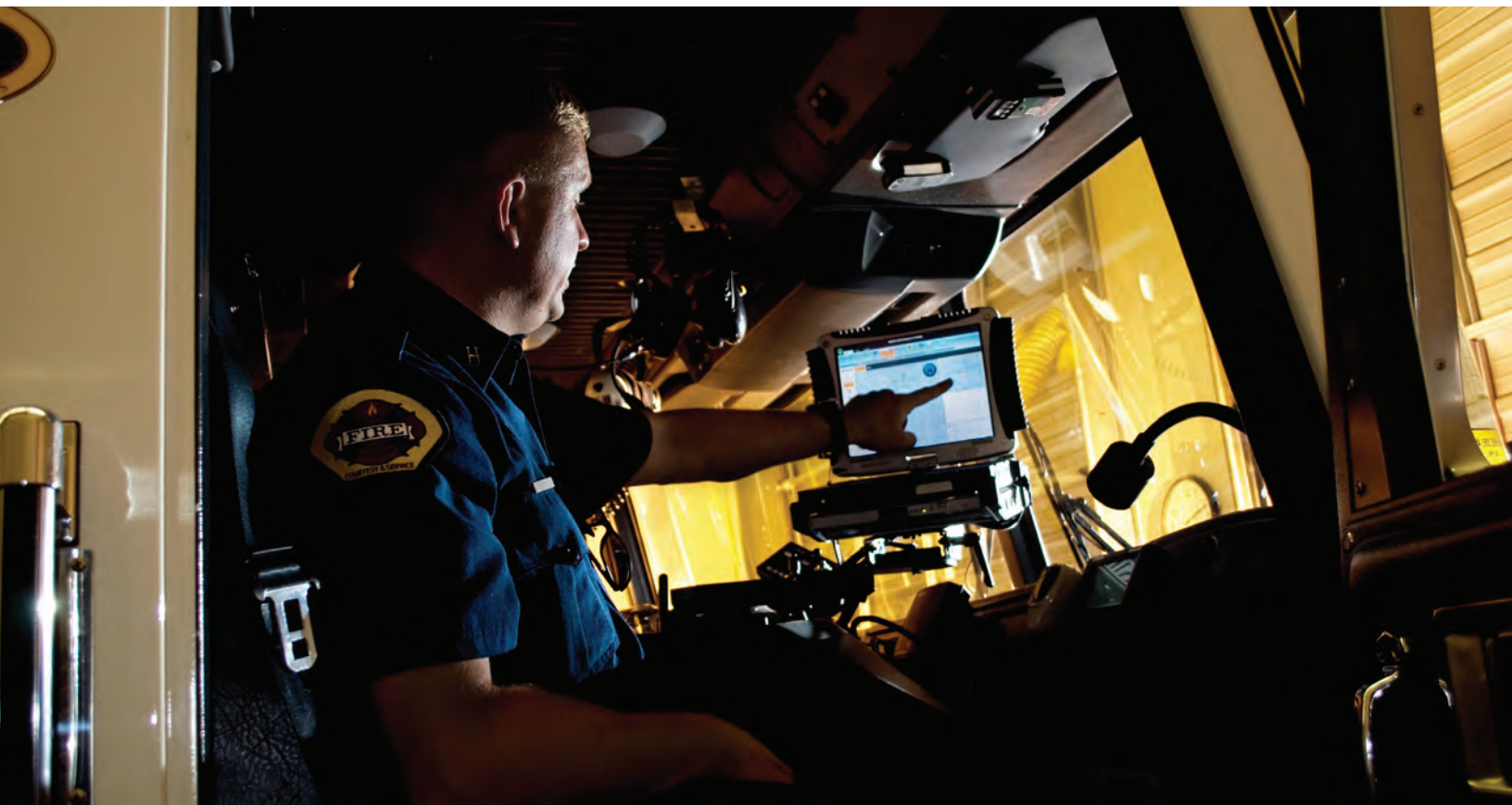
What are the possible consequences of a security incident at your organization? Are you obligated to comply with governmental security initiatives, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Federal Information Processing Standards (FIPS), Family Educational Rights and Privacy Act (FERPA), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), America's Water Infrastructure Act (AWIA), or numerous other standards? Do you maintain critical infrastructure for the public? What would the results be if your organization was the source of a denial-of-service (DOS) attack? How will this affect your brand? What are the penalties – jail or just monetary? You'll likely have more questions than answers, but understanding your risk is paramount in understanding how secure your IoT infrastructure needs to be.

Develop a plan

The Cisco Lifecycle approach – prepare, plan, design, implement, operate, and optimize (PPDIOO) – is a reliable and tested methodology we recommend for reducing security risk in public sector organizations.

- **Prepare:** Develop a business plan, including a technical strategy and security policy
- **Plan:** Understand where you are and where you need to be (gap analysis)
- **Design:** Create a detailed design that addresses your requirements
- **Implement:** Publish security policy and deploy the technology
- **Operate:** Test and maintain the security policy and technology
- **Optimize:** Improve the policy and technology

Note that this is a living lifecycle, and as these technologies are still being developed and updated, you'll continue to refine and improve the process and infrastructure.



Solutions for securing the IoT environment

The following section discusses some of the solutions and capabilities for securing your infrastructure, part of the design phase of PPDIOO. The plan developed in the first stages of PPDIOO should determine the solutions you need to address the risks most relevant to your environment. Figure 2 at right depicts IoT in several scenarios, including a power grid, water treatment facilities, traffic control, medical equipment used in hospitals, connected vehicles, video cameras, Internet Protocol (IP) lighting, and HVAC systems. There are many ways for an IoT device to connect to the network. Although this diagram shows some specific implementations, all connectivity options are open to every IoT device.

Device authentication, authorization, and accounting (AAA)

The purpose of AAA systems is to ensure sensors on the network are authenticated, authorized, and documented. AAA for onboarding devices is the first line of defense. Basically, never let someone you don't know into your home.

Authentication helps you do this by providing a method to identify devices. Certificate-based authentication (X.509) is a secure and scalable method for IoT devices. Authorization determines what a device can and cannot do on your network, and accounting tracks or logs activity of devices and can provide data that can be used for traffic flow analysis and help plan the network's growth.

The capabilities of AAA have improved with several methods, including;

- **Manufacturer Usage Description (MUD)** - A methodology used to provide a means for IoT devices to signal to the network what sort of access and network functionality they require to function correctly
- **Bootstrapping Remote Secure Key Infrastructures (BRSKI)** - Specifications for automated bootstrapping of a remote secure key infrastructure using vendor-installed X.509 certificates
- **Enrollment over Secure Transport (EST)** - A standard (RFC 7030) designed to improve the provisioning of digital certificates.

The [Identity Services Engine](#) (ISE) is a key component of IoT device onboarding. The ISE server authenticates and authorizes an IoT device onto the network with the help of MUD or BRSKI servers. It functions as one of the decision points through which IoT identification of traffic flows between the IoT device and the IoT controller. The ISE server also provides network visibility with detailed endpoint attribute history.

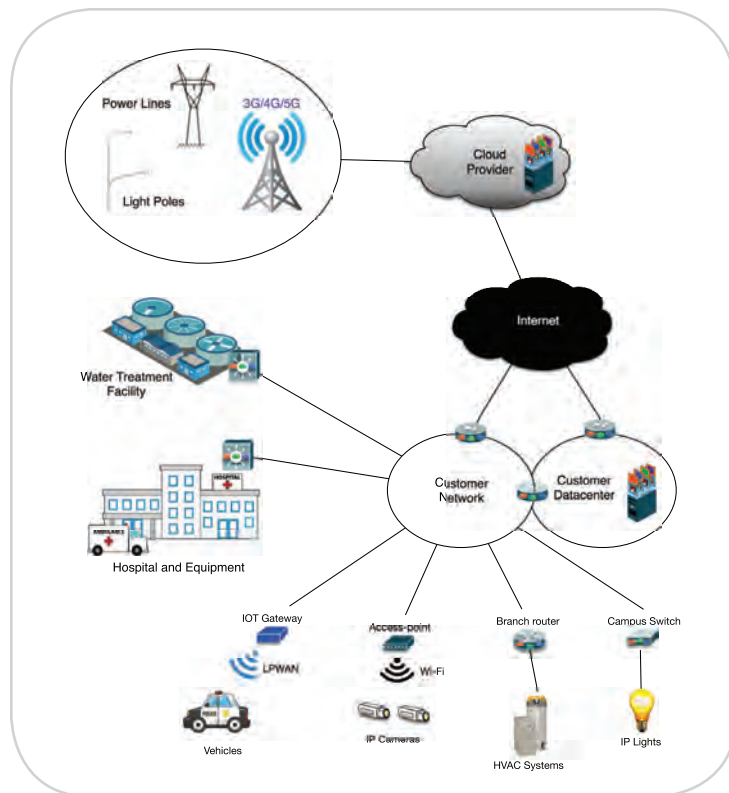


Figure 2. The diversity of the IoT environment

Segmentation

Segmentation is a great way to mitigate the impact of many attacks. Segmentation is a quick and easy way to limit the surface area where the attack can roam, preventing massive propagation of the malware. Being able to logically separate traffic on the same physical infrastructure offers you the capability to initiate unique security policies per segment.

Segmentation technologies include macro-segmentation and micro-segmentation methods. A macro-segmentation technology would be multiprotocol label switching (MPLS) or virtual routing and forwarding lite (VRF-Lite). These technologies provide segmentation or separation per VRF instance. This means that devices within the same VRF are allowed to communicate with one another.

Micro-segmentation, on the other hand, offers the capability not only to separate traffic within a VRF, but also between devices. This type of technology is generally better suited for IoT, since most IoT devices don't communicate with one another, doing so only with a central device or controller. This technology is implemented with [Cisco's Software-Defined Access](#) (SD-Access).

Simple, open, and automated security

At Cisco, we take a holistic approach to security by integrating it across your entire network, including endpoints, cloud, Internet, and email. This gives you a more effective security posture, with greater visibility. We do this by delivering security products that are:

- Simple to deploy, scale, manage, and operate
- Open to integrate key event, threat, context, and policy security data
- Automated for rapid threat containment, advanced malware protection, and use of network as a sensor and enforcer

Note that this is a living lifecycle, and as these technologies are still being developed and updated, you'll continue to refine and improve the process and infrastructure.

Secure connectivity

The distributed nature of IoT deployments provides a massive attack surface for adversaries to gain access to an agency or institution. However, many in-motion attacks can be prevented through use of secure wireless connectivity. As seen in Figure 2, there are diverse connectivity options when it comes to IoT. Focusing on the wireless options, which will be the predominant access methodology for IoT, still presents a wide range of technologies, including Wi-Fi, Wi-SUN, Bluetooth, NFC, LoRaWAN, and cellular 4G and 5G. The specific connectivity options depend on the deployment methodology and sensor type, among other things. In order to provide a consistent security posture across so many types of technologies, some security capabilities should be embedded in the radio communications, such as encryption at layer 1, while other capabilities will be delivered from the architecture, such as threat analytics.

Threat analytics

You can't prevent what you can't see. By leveraging threat sensors and threat analytics, we can gain visibility into the IoT environment. Threat analytics falls in the Operate phase of the PPDIOO methodology.

Understanding the normal behavior of an IoT device helps determine when that device is acting inappropriately. Threat analytics provides a view of a normal environment and compares it to the immediate environment. By detecting changes in the behavior of the IoT devices, systems can identify areas of concern that the InfoSec team can analyze. Getting full visibility using Cisco Cyber Vision which provides dynamic asset inventory, real-time monitoring of control networks, and comprehensive threat intelligence helps to provide critical insight to the operation of the IoT system.

Another challenge to monitoring IoT devices is that traffic may be encrypted. This poses an interesting problem, but [Cisco's Encrypted Traffic Analytics](#) (ETA) can help by providing visibility into encrypted traffic. This lets you detect malware within the encrypted communications and is critical to understanding the behavior of traffic for deeper analysis.

[Advanced Malware Protection](#) (AMP) contains three primary components: AMP for Endpoints, AMP for Networks, and AMP for Applications (email and web). Out of the three, AMP for Networks is the most appropriate, since most IoT devices generally don't go to the web or send email. [AMP for Networks](#) provides deep visibility into network-level and network-edge threat activity and blocks malware with integration into [next-generation firewalls](#), the [Meraki MX unified threat management platform](#), and [integrated services routers](#) (ISR).

Threat mitigation

One of the most important aspects of security is stopping an attack before it starts. [Cisco Umbrella](#) can help by delivering security from the cloud. It does this by blocking malicious destinations before a connection can be made.

Data security and integrity

Protecting data in motion and at rest is another critical aspect of IoT security. Incorrect or unavailable data creates false information, and making decisions on poor intelligence is never good.

Protecting data in motion using MACsec (802.1AE) for wired connectivity allows for line-rate encryption. IP Security (IPsec) provides an end-to-end encryption solution, but requires encryption software on the IoT device and head-end or controller. Firewalls and intrusion detection/prevention systems (IDS/IPS) are used to protect the more valuable assets, such as application servers, controllers, and data storage systems.

Device management: device and data

Managing IoT devices can be a daunting task. Fortunately, there are solutions that will make life much easier. The first is;

- **Industrial Asset Vision** which is an all-in-one solution with three elements. These include, industrial sensors, Cisco Wireless LoRaWAN IXM Gateway, and the Industrial Asset Vision Dashboard.
 - Sensors: There are a variety of sensors that include tracking and monitoring of temperature, occupancy, water leaks, vibration, and so on.
 - LoRaWAN Gateway: Delivers long-range connectivity for both indoor and outdoor environments.
 - Dashboard: Is a cloud-based system providing a single view of location and data from sensors and gateways.
- **Cisco Meraki Cloud Managed Sensor Solution.** It has a similar architecture to Asset Vision, with sensors, Gateways, and a Dashboard, but differs in that communication to the sensors is 2.4 GHz Bluetooth Low Energy or BLE.
- **Cisco Digital Network Architecture (DNA) Center.** It provides a single dashboard for fundamental management of the IoT network infrastructure, supporting design, policy, provision, assurance, and platform automation tasks.



Application security

IoT application programmers should always consider security as an integral part of their programming practices and use effective quality assurance techniques.

The following table shows primary security concerns and related threats, strategy, and risk mitigation, as well as solutions to address each challenge.

Security concerns	Specific threats	Threat strategy	Risk mitigation	Cisco solution
Data in motion attack	Unsecure wireless GW vulnerability	Man in the middle DOS attack (initiator) DOS attack (receiver)	AAA Threat mitigation Encryption	ISE Umbrella IPsec/MACsec
Sensor compromise	OS vulnerability Hardware vulnerability App vulnerability	Device offline Bot membership Data corruption	Dynamic threat intelligence Remote GW and policing AAA Segmentation	NGFW Umbrella SDA Industrial Asset Vision
At rest attack	Server attack Application attack Database attack	Data exfiltration Data corruption	Network behavior analytics Endpoint (server) protection Firewall Application analytics	Stealthwatch AMP for Endpoints NGFW AppDynamics

Table 2. Security concerns and solutions



Summary

The number of IoT devices is growing by leaps and bounds as common, everyday items (even hairbrushes) begin to connect. Developing an IoT system that's completely unhackable may be unachievable. But if we understand the risks and take appropriate actions, we can make it more difficult for these systems to be compromised. And by taking a holistic approach to security, we can significantly improve the overall posture of your IoT network.

Additional resources:

- [Learn more about Cisco and security for IoT](#)
- [Cybersecurity solutions and resources for Government](#)
- [Cybersecurity solutions and resources for K-12 and Higher Education](#)
- [Cybersecurity for the Industrial IoT](#)
- [Critical Infrastructure and Cybersecurity in a New Age](#)



Services as a force multiplier

The IoT, cloud, and new collaboration tools all add value to your network. But they also present a few challenges, such as managing more with less, overcoming talent gaps, and understanding which technologies to implement. At Cisco, we understand this, so we developed a portfolio of IT services to help:

- **Managed Services** that are always on, giving you access to industry-leading technical expertise that helps reduce outages and speed recovery
- **Optimization Services** that help you bridge talent gaps, lower complexity, reduce OpEx, and speed digital transformation
- **Technical Services** to deliver increased operational efficiencies that help lower cost while minimizing risks and disruptions
- **Implementation Services** that let you access our elite resources, including 12,000+ engineers, to increase ROI, speed growth, and lower risks
- **Advisory Services** that provide your team strategic advice, including mapping, so you can speed your network transition while reducing risks and OpEx
- **Training Services** to help develop your talent and keep your network running efficiently.

About the author



Ray Blair is a distinguished architect and has been with Cisco Systems since 1999. He uses his years of experience to align technology solutions with business needs, ensuring customer success. He maintains three CCIE certifications in Routing and Switching, Security, and Service Provider (#7050) and is also a Certified Information Systems Security Professional (CISSP) and a Certified Business Architect (#00298).

Ray is coauthor of four Cisco Press books: *Cisco Secure Firewall Services Module, Tcl Scripting for Cisco IOS, IP Multicast Volume I*, and *IP Multicast Volume II*. He speaks at many industry events and is a Cisco Live Distinguished Speaker.