PRESIDIO FEDERAL

cisco Partner

Maximizing the Power of IoT and OT in Federal Agencies

In the ever-evolving landscape of technology, federal agencies continually seek innovative ways to optimize existing tools. Enter the convergence of the Internet of Things (IoT) and operational technology (OT), a pairing that promises not just efficiency but revolutionary remote management capabilities for internet-connected devices.

Let's delve deeper into these terms. IoT, coined in 1999, refers to a network of physical objects embedded with technology, enabling communication and interaction with the environment. This interconnectedness often incorporates artificial intelligence (AI), sensor data, and big data. Currently, 62% of federal agencies utilize IoT for systems control, access management, and asset tracking, according to the Government Accountability Office (GAO).

OT, a subset of IoT, focuses on industrial environments. It's the specialized hardware and software controlling and monitoring devices' physical performance. Think of it as the networks that connect and control everyday machines, such as elevators and heating, ventilation, and air-conditioning systems — things that are increasingly connected to one another and the internet. GAO found that 92% of agencies use OT and that IoT use may increase in the future.

The potential for leveraging these technologies within federal agencies is boundless. With more than 100,000 buildings worldwide, agencies have a near-constant need to manage and track assets they're shipping across the nation or even worldwide. This extends to controlling critical networks like electrical systems and wastewater treatment plants.

WITNESSING IOT AND OT IN ACTION

The tangible impact of IoT and OT integration is already evident. Officials at a Department of Homeland Security (DHS) agency needed to provide secure internet access to workers on the East Coast. To do it, they decided to use IoT to create separate wireless networks, integrate other IoT solutions and enable remote monitoring.

The agency opted for a scalable multi-site wireless network isolated from DHS's internal networks. By air gapping the network, the agency was able to give external managers the access they needed without going on-prem, while still meeting sustainability and critical infrastructure cybersecurity objectives with IoT/OT. Plus, the isolated network lets DHS use AI to conduct trend analysis and track traffic.

NAVIGATING CHALLENGES: CYBERSECURITY AT THE FOREFRONT

Yet, like any technological advancement, IoT and OT bring their challenges. Budgeting, procurement, and securing these systems remain top concerns. With OT, cybersecurity complexities heighten, especially in dispersed or remote industrial networks.

To mitigate risks, agencies must:

- **Bring visibility to the OT environment** by building a list of all industrial assets down to the component level: vendor references, firmware and hardware versions, serial numbers, PLC rack slot configuration, and more. Then, present all of this in a dashboard that provides a single source of truth for all industrial wireless devices and facilitates scalability. Gaining this level of visibility is key to driving network segmentation.
- **Deploy holistic threat-detection techniques,** such as protocol and behavioral analysis and intrusion detection, to protect the agency's industrial network and ensure production integrity, continuity and safety.
- **Use LoRaWAN,** a wireless protocol purpose-built for IoT applications. It uses battery-powered sensors that broadcast to a gateway that sends the data to the servers. The batteries last for years, and the transmissions can go for miles.

The world is more technologically connected than ever, making it easier than ever to manage, monitor and protect the assets, machines, systems and networks that are scattered nationwide and globally.

ABOUT PRESIDIO FEDERAL AND CISCO:

Presidio Federal is a wholly owned subsidiary of Presidio Inc. focused on the federal government market. It serves as a mid-tier integrator to become an easy button for its federal government customers.

Presidio Federal's partnership with Cisco is always evolving in support of the federal government's drive towards digital transformation given today's hybrid work environment and the need to modernize systems. The companies remain ahead of the curve to help their customers eliminate IT complexity, innovate faster with simplified operations, accelerate adoption across the entire IT lifecycle and collaborate effectively across multiple devices. Learn more about the partnership here.