PRESIDIO FEDERAL

CASE STUDY

WHAT IS IoT?

The “Internet of Things” (IoT) encompasses billions of “smart” objects including sensors, industrial and utility components, cars, trucks, and machines using wireless technology to connect to the Internet, transforming the way we work, communicate, and consume products and services. Simply put, IoT is a network of physical objects that contain embedded technology to communicate and sense or interact with the environment.

The IoT incorporates technologies such as machine learning, machine-to-machine communication, sensor data, big data, and more. Operational technology (OT) is a specific category of hardware and software whose purpose is to monitor and control the performance of physical devices. Currently, 62% of federal agencies are using IOT Technology and 92% of federal agencies are using OT Technologies.

The Cisco IoT portfolio includes two security-specific products:

- Cyber Vision, a deep packet inspection software product
- ISA-3000, an industrial firewall with all the firepower features plus additional support for industrial protocols and ruggedized housing

62% of federal agencies
are using IOT Technology

92% of federal agencies
are using OT Technologies

WHY IS IOT IMPORTANT TO FEDERAL AGENCIES?

IoT is important for agencies because they each will have machines that make up their network environment requiring continuous management to fulfill their mission. With IoT connecting devices to the internet, offsite management and monitoring is now possible.

Our team recently assisted a Department of Homeland Security (DHS) agency with utilizing IoT/OT to meet sustainability and critical infrastructure cybersecurity objectives. By building a network that was air gapped from their internal network an agency can give external network managers the access the access they need without going on-prem.

THE CHALLENGE:

A DHS agency needed to provide secure internet access to their employees in their East Coast offices. Due to security reasons, the agency did not want to risk using their existing internal network yet wanted to be federally compliant. Our job was to ensure they could leverage this new wireless network for employees.

We also pointed out the future possibilities of using IOT including creating separate wireless networks globally, integrating other IoT solutions, and enabling remote monitoring or cradle point devices or wireless gateways.

SOLUTION:

After considering multiple manufacturers' products, our team designed and implemented a scalable multi-site wireless Cisco Meraki network that is isolated from the DHS internal networks. This network consists of two sites, each with a Cisco Meraki MX-85 firewall, Cisco Meraki MS-355 switches, and Cisco Meraki MR-44 WiFi6-capable access points. Our administer training provided the agency with the knowledge to self-manage the project onsite or to use Presidio Federal as their managed services provider.

BENEFITS AND A LOOK TO THE FUTURE:

Our team proudly exceeded the DHS agencies expectations by enhancing the original design of the network as a "guest network" to an "employee network" with authentication via a self-registration portal. Within two weeks our delivery team had the wireless network up and running in the primary building getting 450 MGPS download speeds. The project was completed on time and under the recommended hours. Now, subsequent buildings will have lower implementation costs due to existing cloud configuration templates.

Our solution can be scaled from a single firewall, switch, and access point to a fully separate multi-site, multi-floor network. For the DHS agency, the multi-site, multi-floor implementation cost was $238,000 and it took our delivery team about 1 month to implement. By making this change to going wireless and focusing on a "wireless first" approach, government agencies can save significantly by reducing the overall cable plant costs.

DHS was well positioned for future innovation opportunities given their isolated network. With this distinguished advantage, the agency can use tools such as sensors, monitors, and cameras. By leveraging AI, agencies can conduct trend analysis and do user tracking of traffic within their store fronts or commissaries, as well as enable automation and machine learning capabilities. Now, thousands of users can receive access to their networks vs. the hundreds that were the case prior to this implementation.

ABOUT PRESIDIO FEDERAL

Presidio Federal, is a purpose-built and mission-driven IT services and solutions provider dedicated to serving the federal government. We leverage our wealth of experience and deep relationships across our partner ecosystem, creating an environment of active collaboration and real-time responsiveness.

The company develops and delivers the most advanced technologies through expert knowledge centers in automation, augmentation, cloud, cybersecurity, digital infrastructure, and collaboration. Presidio Government Solutions is a wholly owned subsidiary of Presidio Networked Solutions.