



Case Study: Large Defense Contractor in Virginia

Unified Wireless Threat Management

Challenge:

Cost-effective solution to enforce “no wireless devices” policy at secure portion of facility SCIF (Sensitive Compartmented Information Facility)

Solution:

AirPatrol's Wireless Locator System with combined WiFi/Cellular Sensors

Benefits:

- Purchase, deployment and operational cost savings from one single system to detect today and tomorrow's wireless threat vectors

Cell Phones not Allowed at Classified Meetings

This Defense Contractor's business is to support the missions of their customers within the United States Defense and Intelligence community. Classified briefings and classified information processing take place in their facility of meetings rooms, totaling 10,000 square feet. There is a strict policy of no wireless devices whatsoever, including no cell phones, and signs are posted stating it. The Contractor regularly teams up with other systems integrators and Government organizations on large projects, creating fluid and high-people traffic at the facility, so a solution to enforce the policy had to be a practical one.

Cell phones sometimes went off during classified meetings, which became the only way to know if someone had violated the policy.

Combined Cellular and WiFi Detection

The Contractor deployed AirPatrol's Wireless Locator System (WLS) with combined WiFi/Cellular Sensors. They also deployed the optional WLS Connect component, so that Security Personnel could perform historical playback of security data. The solution has a one-of-a-kind combined WiFi and cellular wireless intrusion detection capability.

The Cost-Effective Approach

The Physical Security Team is now enforcing their strict no-wireless device policy, with regular detection and confiscation of unauthorized cell phones. In addition to protecting Top Secret information, WLS also gives confidence to the team that intellectual property within projects is not leaked to the competition. They had been reluctant, due to cost impracticality, to deploy multiple silo'ed systems for the detection of each type of wireless device, especially with future devices coming out which use different parts of the wireless spectrum. With AirPatrol, they purchased, deployed, and managed one system to detect the wireless threat vectors existing today as well as the new ones in the future, which will exist on different parts of the frequency band.

The Physical Security Team has been very pleased with the solution's performance and with the support they received from AirPatrol. On a regular basis, they demonstrate WLS to their peers within the US Government.