Mobile Device Detection

Government Agency Enhances "No Wireless" Policy Use Case

Summary

Major government agency in Florida implements Sengex's Mobile Device Detection solution to enhance and enforce their "New" no wireless device policy.

Challenge

As part of their security practices, a major government agency's "no wireless devices allowed" policy consisted of a "trust" process in which employees and visitors were required to leave their Personal Electronic Device (PEDs) in storage units located outside building security entrances.

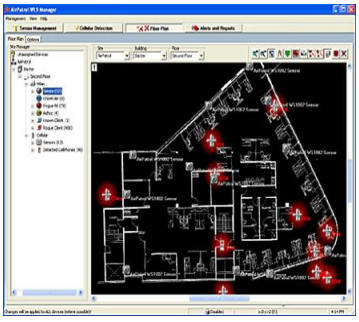
This policy was successful only when visitors and site personnel abided by the requirement; however it was assumed that there were continuous violations, with rogue wireless-enabled devices and cell phones entering the facilities, either intentionally or unintentionally. These PEDs could easily remain undetected via traditional Technical Surveillance Counter Measures (TCSM) sweeps.

These violations would be further compounded in areas designated as Sensitive Compartmented Information Facilities (SCIFs), because the entry of unauthorized devices within these areas could induce risks and threats to national security.

As most organizations grow to provide advanced capabilities to the War Fighter, this organization clearly understood the benefits of a wireless network to their operations. The agency installed a secure wireless network specifically designed to allow agency approved wireless devices to utilize this network. The presence of these wireless access points further enforced the need for a solution that can not only detect unauthorized devices attempting to connect, but in parallel, identify authorized devices as not being a threat to security practices.

Solution

To combat violations, and assure security of the wireless network, the government agency selected Sengex's Mobile Device Detection (MDD) solution provided by AirPatrol's ZoneDefense™ to provide their Special Security Office (SSO) the ability to ensure their visitors and employees were following the updated wireless policies. This eliminated the risk of unintentional or malicious access to sensitive government materials.



When examining available solutions, a key requirement was the need for a highly scalable and intuitive tool that could be implemented across a multi-building campus to provide SSO personnel a centralized system to monitor, track, and be alerted of unauthorized wireless activity across all campus facilities.

Beyond the scalability requirement, another key requirement was to not only detect rogue devices, but also to accurately pinpoint their location, identify the device type (cell or Wi-Fi), and track their movements on a floor plan display. This would enable the SSO to immediately locate the policy violation and rapidly deploy personnel to remove the threat.

A third requirement was that the chosen solution would coexist with their secure wireless network allowing the SSO to distinguish between approved wireless access points and clients, and rogue devices.

The installed system, managed via workstations located within the SSO Director's office, provided a highly detailed view of any wireless activity detected by a network of strategically placed passive sensors located across 19 floors within 8 buildings.

In addition to real time monitoring and alerts, these workstations also provided the SSO organization the ability to view historical activity via the MDD systems recording functionality for forensic investigation.

Once the system was operational, as the SSO suspected, numerous rogue devices were detected operating within the facilities, including inside SCIFs. Security personnel were immediately deployed to discover and remove the numerous offenders. At the same time, campus-wide notification of the system was given, and SSO personnel observed in real time via the MDD's displays a stream of rogue devices being removed from the monitored facilities to the PED storage locations.

With the MDD system installed, the agencies 'no wireless/cell devices' policy has transitioned compliance practices from a position of "visitor/employee trust", to "detection and enforcement", while in parallel enabled secure use of wireless networking technologies within their secure facilities.

Future

Due to the success of the MDD deployment, the agency has decided to expand their coverage footprint to include additional buildings and new buildings under construction. In addition, as a result of the immediate improvement in their wireless security protocols, other government agencies are now considering the deployment of Sengex's MDD solutions to address the same security challenges within their locations.

Contact Sengex to learn more about our Mobile Device Detection solutions and other Sengex offerings

About Sengex

Sengex provides data and wireless security solutions to healthcare, government and commercial organizations, assuring their businesses information is safe from ever evolving cyber threats. Sengex focuses on providing highly innovative data security solutions across all aspects of business operations that meet business's internal and regulatory requirements as they relate to electronic information sharing across the organization or between partners and vendors.

Combining leading edge software technology with real world experience, Sengex delivers innovative security solutions quickly and economically, providing customers the comfort their mission critical data is safe from risk at rest or in transit across public and private networks.