



ATHENS AIRPORT SECURES WIRELESS NETWORK

Customer Description

Built for the Olympics in 2004, Athens Airport is one of the most modern airports in the world. An investment costing 2.2 billion Euros, the new airport was built to replace its congested predecessor and offers passengers a modern, spacious and state-of-the-art environment. The new terminal building and satellite buildings cover an area of 180,000 square meters.

Problem

The airport's terminal building contains over thirty five modern shops, a business centre, twelve restaurants and bars as well as a fully equipped business centre, eight business-class lounges and six car rental companies. The airport employs over 14,000 people catering to the 16 million plus passengers each year. One of the airport's main assets is its wireless internet access for passengers and staff alike.

Securing this complex wireless environment is critical as today's business travellers, especially frequent flyers, insist upon direct communication with their homes and offices while travelling. Anywhere anytime access has become a buzz term of the IT industry, however it must be safe for an airport to allow wireless network access to their passengers. It must also be safe enough for the passengers themselves to use wireless hotspots at the airport.

Picking up email on the go while also remotely accessing corporate data is essential for the majority of business travellers. Airports not enabling wireless internet access could potentially lose passenger traffic - an airport that does not correctly secure their wireless access could potentially be vulnerable to all types of hacker attacks.

At an airport the very movement of people is a good reason to supply a wireless network infrastructure. In most airports, as was the situation at Athens, there is a multiplicity of wireless networks for everything from the baggage handling hall to the point-of-sale card readers in the shops," said Vassilis Kontothanassis, Athens Airport ICTS Coordinator. "All of these networks are at risk if they are not secured. As wireless technology is exploding in popularity, these are completely new challenges to IT security. The ability to maintain the confidentiality and integrity of data is essential for all enterprises, but is particularly important for airports as huge number of credit card transactions take place everyday over wireless networks at airports. Also, a Denial of Service attack on an airport network could effectively close an airport down." Vassilis Kontothanassis is responsible for managing the wireless infrastructure and ensuring its security. He sees his role as enabling access anywhere at anytime to all staff and passengers with wireless devices. "Ensuring our staff have secure access from anywhere within the airport is essential."



"Ensuring our staff have secure access from anywhere at the airport is essential"

Solution

As part of the Airport's implementation of a secure wireless network, AirDefense conducted a site survey using AirDefense Survey™ to measure and assess the state of the RF environment. The infrastructure at Athens Airport is based on a Cisco network and a site survey enabling the IT team to plan the location of the AirDefense overlay network while optimizing its performance. The overlay network was mapped using AirDefense Architect™ which helps to accurately and productively design Wi-Fi networks (802.11) before the actual deployment of access points, sensors and other wireless devices. The solution had to offer guaranteed security and a foundation upon which more installations could be rolled out. It had to cover the whole of the terminal building including the baggage handling area. The solution had to have the ability to detect rogue access points and automatically prevent them from operating within the airspace of the airport. The IT team decided to utilize AirDefense Enterprise as they insisted upon having only the most powerful Wireless Intrusion Prevention System (IPS) available.

"We were keen to work with an organisation that demonstrated it could work in a complex wireless environment and give us peace of mind about security," stated Kontothanassis. The proposed system was designed to provide the Airport with a system which could be quickly and easily expanded as the number of wireless installations increased when and where necessary. It is an overlay network to the Cisco infrastructure with a number of AirDefense wireless sensors deployed on each level of the terminal building. AirDefense's Enterprise was installed to constantly monitor and ensure the security of the data over the Airport's network.

CASE STUDY | Wireless Security



Wireless now and in the future

Since the AirDefense solution was implemented, Vassillis Kontothanassis and his team have been able to detect when and where people are using wireless equipment and devices throughout the airport. They have also been successful in stopping unauthorised attempts to attach to closed segments of the network. In addition, the system also provides moment to moment details of traffic and potential threats which are presented as graphs, enabling the network team to identify and plan for future wireless installations.

The airport's growth in passenger numbers as well as the satisfaction of those passengers' experiences is paramount to Athens's future as a major European hub. The wireless network is of primary importance to the marketing exercise that the airport has undergone in selling itself to passengers and without said protection against malicious attacks, the very operation of the airport could be effected.



"We have to protect the airport network against potential threats. AirDefense enables us to do this."

The particular risks of a wireless infrastructure for an airport are multiple but the two main threats stand as:

- 1) Due to the air being a shared medium, it lacks the physical control of its wired counterpart. Any wireless device can "see" all the traffic of other wireless devices in the network. Sensitive information that is transmitted between wireless devices can be intercepted and disclosed if not protected by strong encryption.
- 2) Airports often integrate wireless technology into their wired network so by connecting through the wireless network one can often bypass the traditional wired-side security. Rogue or insecure Access Points can compromise network security, making them popular targets for hackers. Even if an airport has no sanctioned Wireless LANs, Wi-Fi enabled laptops and PDAs can open backdoors into the corporate network and render existing security measures useless.

"At an Athens airport we have thousands of people in our terminal building at any one time and although the vast majority will be law-abiding each and everyone could be a threat and we have to protect against threats that we don't even know are out there. The AirDefense solution enables us to do this."

About AirDefense, Inc.

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection. AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe. Founded in 2001, AirDefense is based in Alpharetta, GA, and serves hundreds of government agencies and blue chip corporations.

