

# Pentura Case Study

## BT

### About BT

*BT is one of the world's leading providers of communications solutions serving customers in Europe, the Americas and Asia Pacific. In the UK, BT serves more than 20 million business and residential customers with more than 30 million exchange lines, as well as providing network services to other licensed operators.*

### The Challenge

*To enable secure mobile working for BT Employees*

### The Solution

*AirDefense*

### About Pentura

*Pentura is the UK's first Risk Management Service Provider specialising in understanding key business systems & processes to identify & manage the risk posed to the network infrastructure & sensitive data. Pentura's services & solutions address the risks surrounding the three key factors when considering Information Security; Confidentiality, Integrity and Availability.*

  
**AirDefense**™

  
**Pentura**

#### Contact:

Pentura Limited  
Diddenham Court  
Lambwood Hill  
Grazeley, Reading  
RG7 1JS  
Tel: 01189 768960

BT's employees are highly mobile and needed the flexibility to work securely at multiple locations. "Hot desking" to give employees access to the company's network was tried but was difficult, expensive and impractical. Wireless technology was generally agreed to be the most beneficial solution and with this came they need to establish the best of breed security for the wireless infrastructure.

Employees had laptops and other wireless enabled devices and needed to access email, customer records, and other work applications at multiple locations. The need to do this securely was imperative in the solution BT chose. BT has multiple sites some of which are located in the heart of city centres and many offices could detect more than 30 other Wireless LANs. This meant that a complete site survey had to be carried out at each location to understand what the complexities were and how many wireless networks actually invaded BT's airspace.

At some sites in central London, the initial survey detected that at regular intervals alarms might be raised from the automated bus stop updates. This type of traffic, while not a threat could create multiple security alarms. Other locations in more rural settings provided different problems of distance between buildings and large communal areas. The risks for BT as an organisation and the implications for its management team if the solution they chose was not scalable were immense. The problem of partitioning friendly neighbouring wireless LANs from those that could present a malicious threat was essential. The threats to any wireless deployment are rogue or unauthorised access so the problem for BT was to be able to analyse existing and zero day threats in real-time against historical data to accurately detect all attacks and anomalous behaviour originating inside or outside the organisation. Doing this while providing IT support for over 60,000 workers seamlessly and without increasing IT management time was seen to be essential.

**Requirements** - BT needed a solution that could detect intruders and rogue access points automatically and secure their airwaves cost effectively. It needed a solution that could distinguish between the multiple legitimate neighbouring wireless networks and those that were malicious. In addition it needed to be able to terminate wireless connections between an intruder and an authorised access point and also to terminate authorised devices with rogue access points. Most particularly it required the vendor it chose to be able to enforce the BT security policy to all its mobile workforce without disrupting its business. The solution had to work with the Cisco based network infrastructure.

**Solution** - BT evaluated several Wireless LAN security products before deciding which one to purchase. The evaluation process was exacting. Michael Malcolm RF Manager at BT said "I was a sceptic. I was not going to allow wireless connectivity at BT unless I was convinced that it could be provided securely." The evaluation and testing process was extremely rigorous and thorough. The site surveys were completed using AirDefense Architect which provides complete design and simulation of wireless LANs based on building-specific environments. This product accurately and predicatively helped design the Wireless networks (802.11) before the actual deployment of access points, sensors and other wireless devices. For the deployment BT chose to use AirDefense Enterprise provided through a specialist solutions provider in the UK called Pentura. They have currently deployed sensors in 15 of 21 sites in the UK and plan to roll out the solution across Europe.