

Wireless LAN Security

> March 12, 2003

DIGITALNET

AirDefense

Gartner

Agenda

- **Introduction**
Jay Johnson, VP – AirDefense
- **Security on the Run**
John Pescatore, VP – Gartner Research
- **WLANs: Risks & Defenses**
Jay Chaudhry, CEO – AirDefense
- **Wireless LAN Security – A Case Study**
Bob Martin, CIO & VP – DigitalNet Government Solutions
- **Questions & Wrap-up**

Support

- **To send us questions during the sessions:**
Email a **Question** link on the left-hand side of your browser window
- **For Technical Support:**
Email fgo@airdefense.net or call 770-663-8115 x124
- **Archive of this presentation** will be available on www.airdefense.net

Security on the Run



> John Pescatore
Gartner Inc.

DIGITALNET


AirDefense

Gartner

Horror Stories

This part of the presentation is copyrighted by Gartner Research & hence not available for download

Gartner

WLANs: Risks & Defenses



> Jay Chaudhry
Chairman & CEO

DIGITALNET

 AirDefense

Gartner

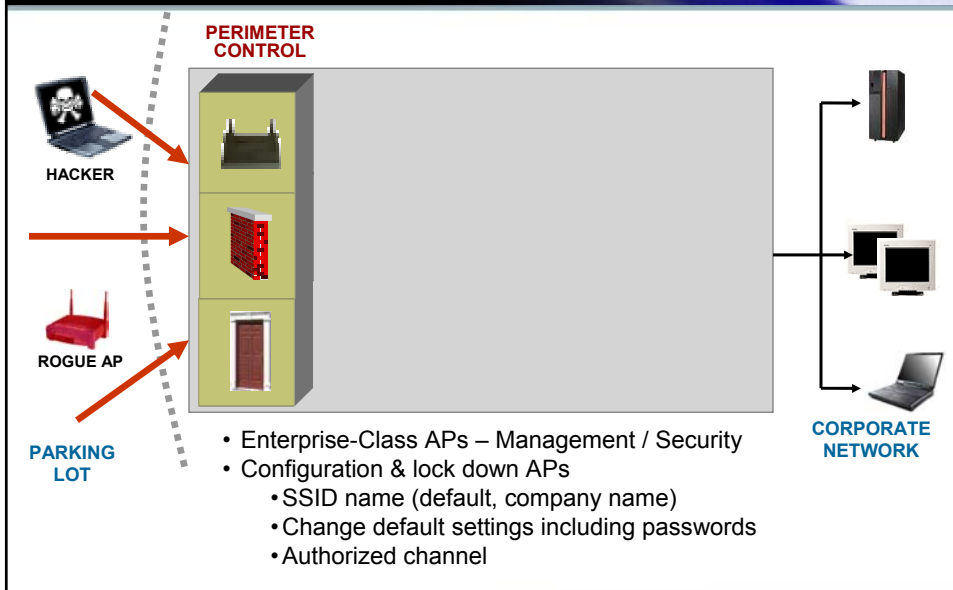
About AirDefense

- Founded in 2001, HQ in Atlanta
- Singular focus on wireless LAN security
- Complements wireless VPNs, encryption and authentication
- Over 40 blue chip customers including govt. organizations
- First-mover, innovative patent-pending technology

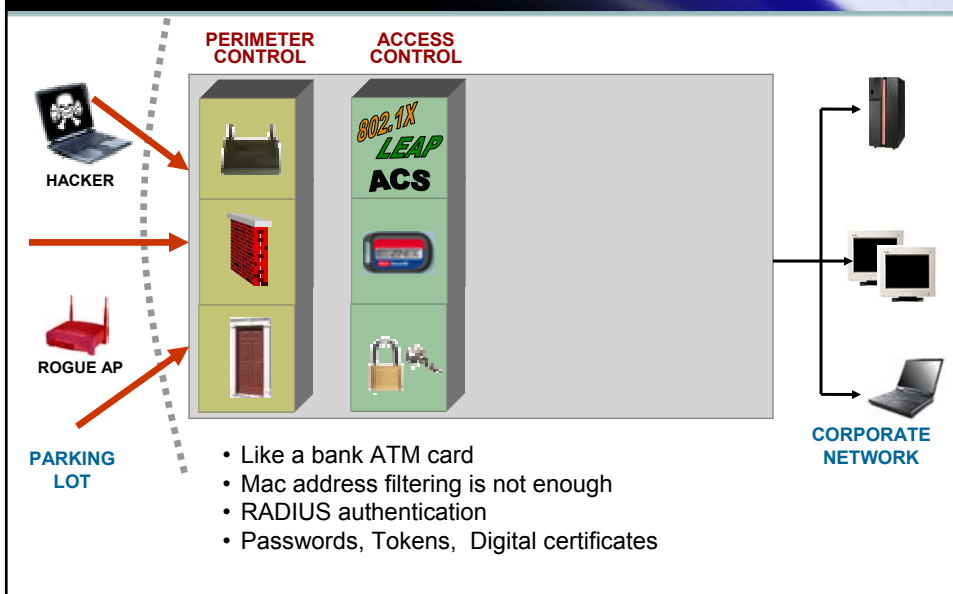


Layered Security Approach

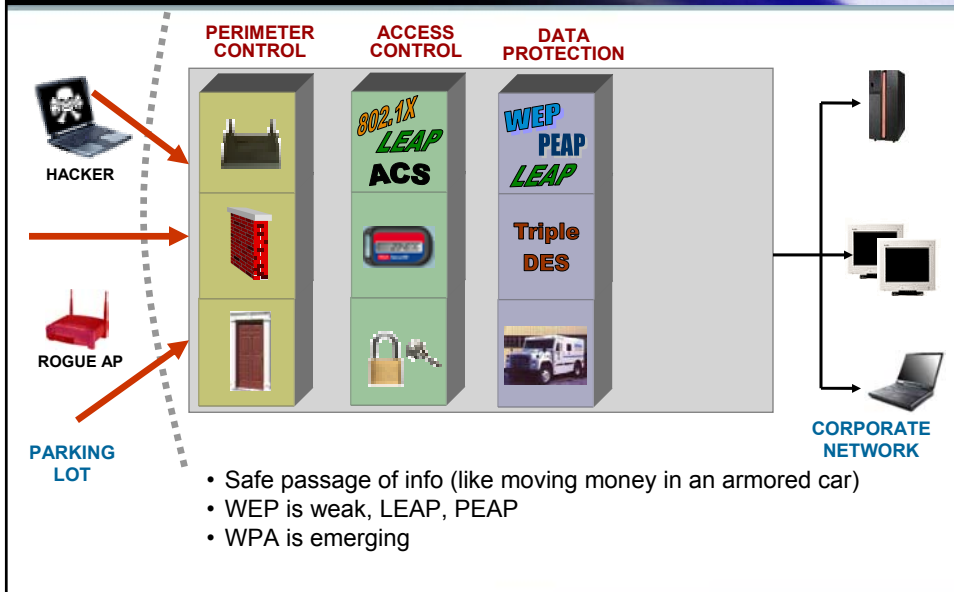
Layered Approach to Security Protect Your Perimeter



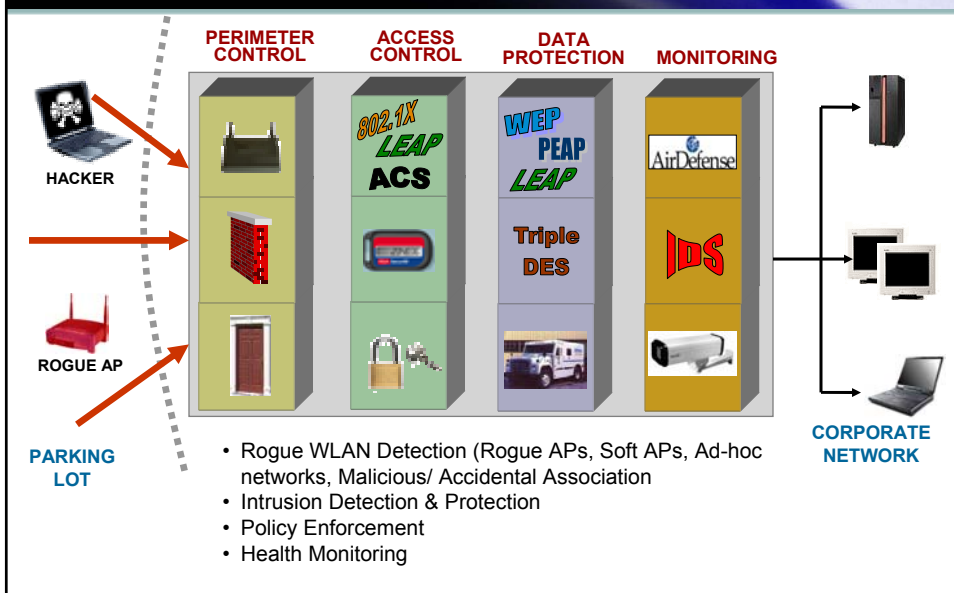
Layered Approach to Security Who has Access (Authentication)?



Layered Approach to Security Protecting Data (Encryption)



Layered Approach to Security Monitoring Traffic in the Air

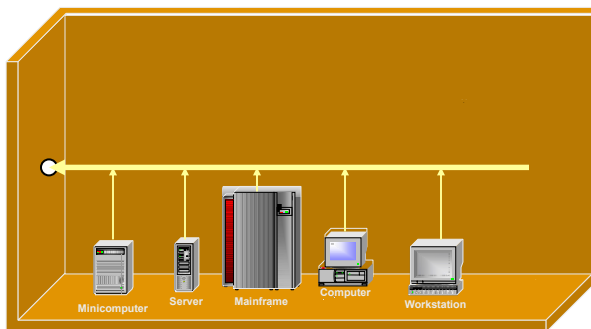




Why Monitor?

Wireless vs. Wired LANs

The walls of the facility provide a solid line of defense against intruders



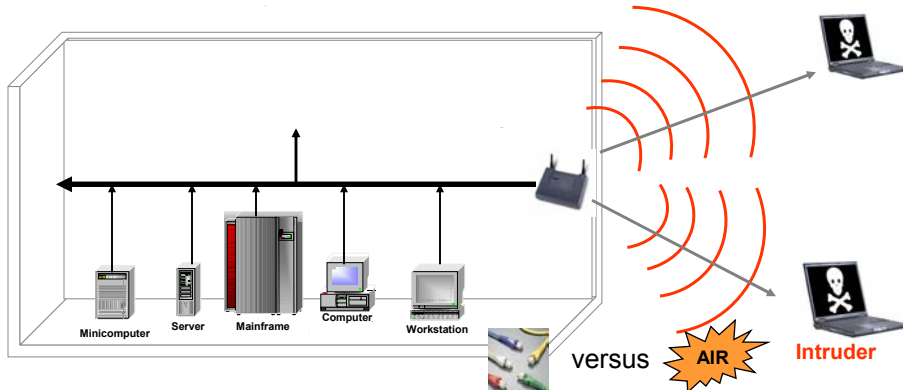
Hacker on Street
or Parking Lot



Wired LAN is extension of Wired LAN

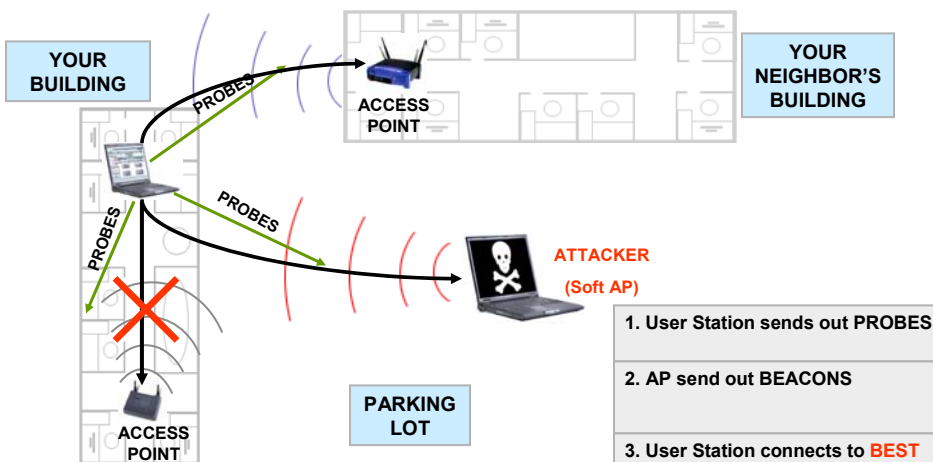
You don't control the medium (air)...

- With a single access point, walls come tumbling down
- Your Ethernet is now in the parking lot!
- New challenges



Accidental Associations

You don't control who you connect to...



1. User Station sends out PROBES
2. AP send out BEACONS
3. User Station connects to **BEST ACCESS POINT** based on signal strength, noise & other factors

Monitoring Complements Encryption & Authentication

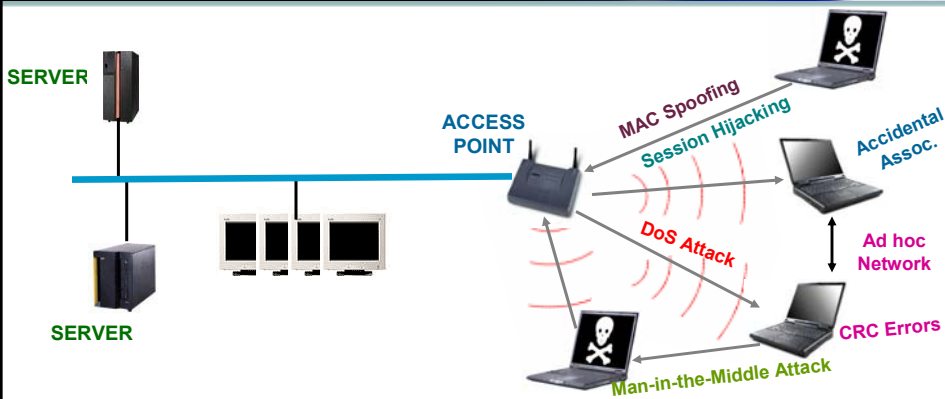
Gartner

*“To truly secure wireless LANs, enterprises **must monitor their airwaves** to detect intruders and threats that can come from unscrupulous hackers and well-meaning employees.*

*Monitoring the airwaves of a wireless LAN is an essential element of security that **should also include advanced encryption and authentication.**”*

Richard Stiennon, Gartner Security Research Director

Monitoring of Wired Network + Airwaves = complete security & operational support



Wired side Monitoring

✓	Traffic Flow	✓
✓	Intrusion	✓
✓	Performance	✓
✓	Problem Diagnostics	✓
✓	Rogue Devices	✓

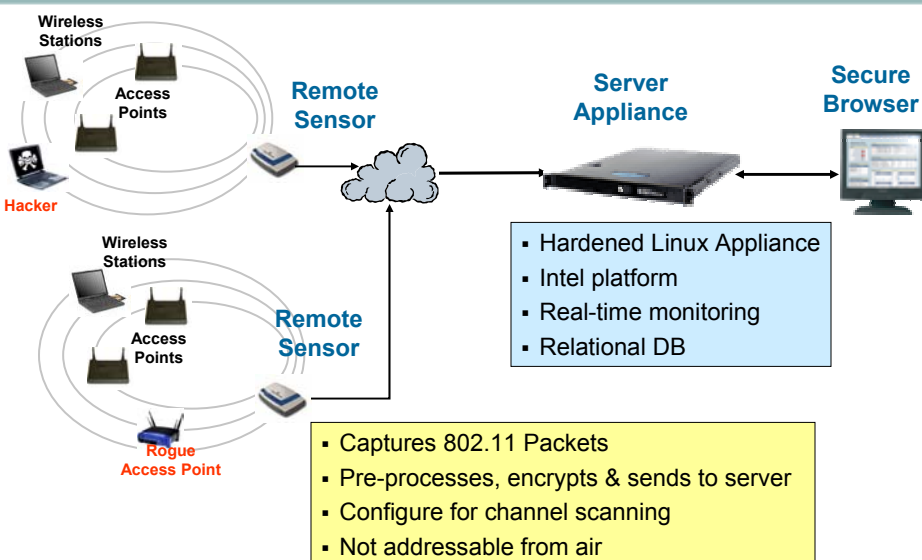
Air Monitoring



AirDefense Solution

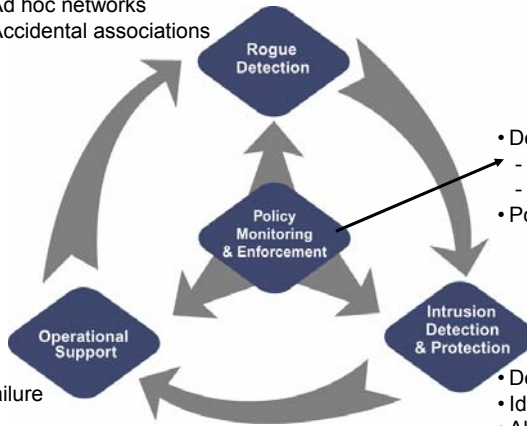
AirDefense Monitors Wireless Traffic

Video camera approach – 24 X 7, Real-time



AirDefense Functionality

- Rogue hardware APs
- Soft APs
- Ad hoc networks
- Accidental associations



- Define & monitor policy
 - Security, Configuration
 - Performance, Usage
- Policy enforcement

- Detect device failure
- Fault diagnosis
- WLAN misuse
- Traffic usage & trends

- Detect impending threats
- Identify attacks
- Alarms / alerts
- Proactive response

AirDefense Positioning Stateless vs. Stateful Technology

Intrusion Protection

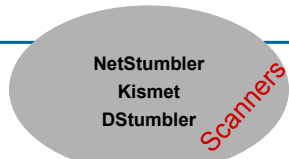


Intrusion Detection

Vulnerability Assessment

Rogue Detection

Traffic Analysis



AirDefense Guard

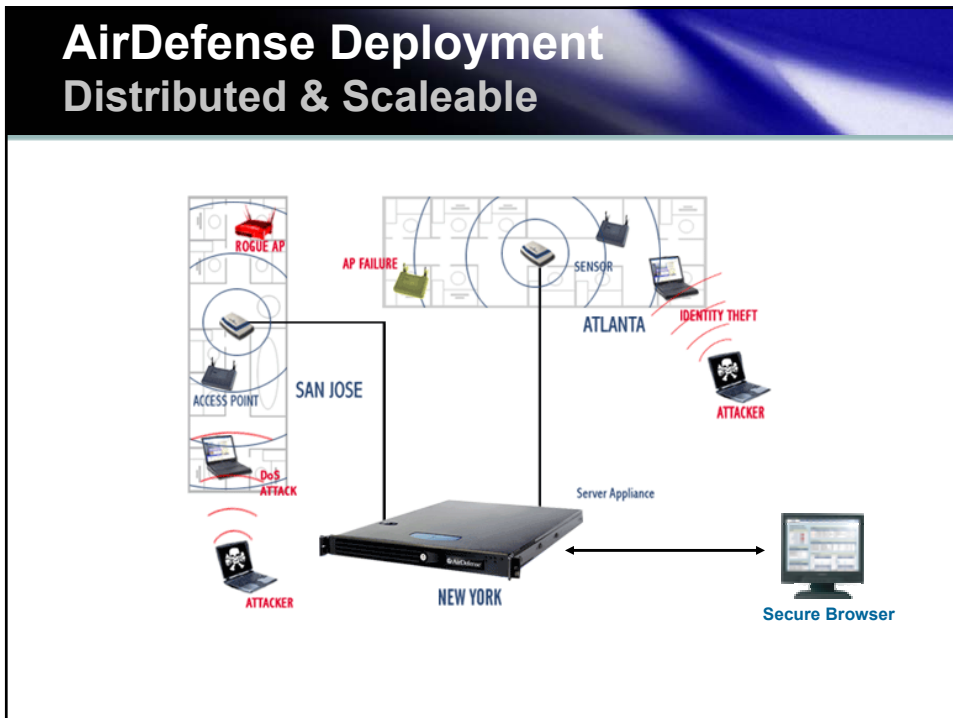
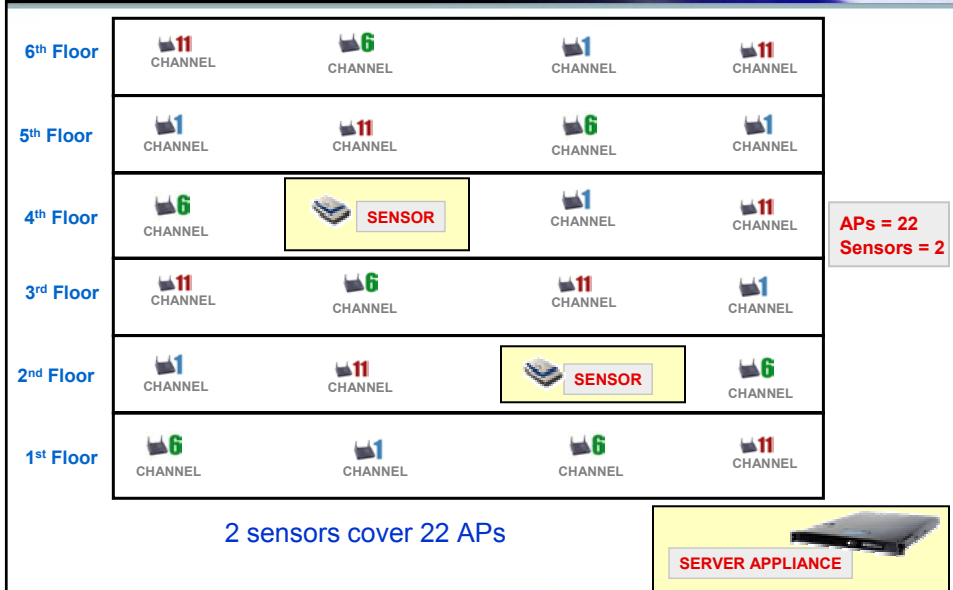
RogueWatch

Snapshot Monitoring

24X7 Real-time Monitoring



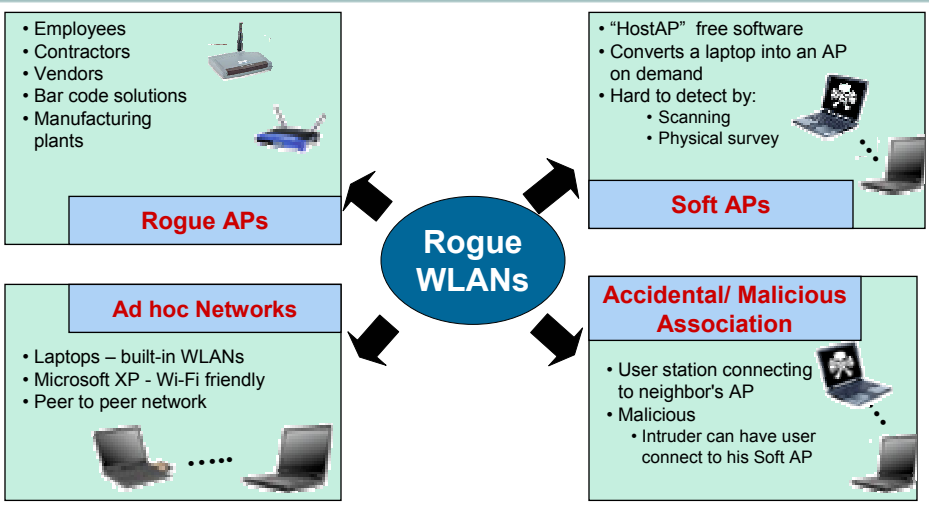
Deployment Example A State Assembly Building





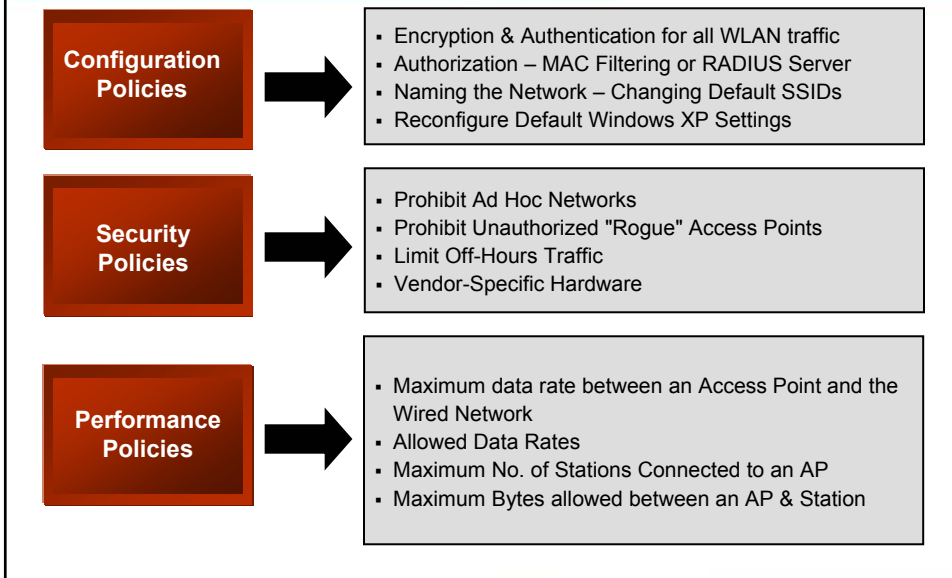
Demonstration

AirDefense Functionality Rogue WLAN Detection

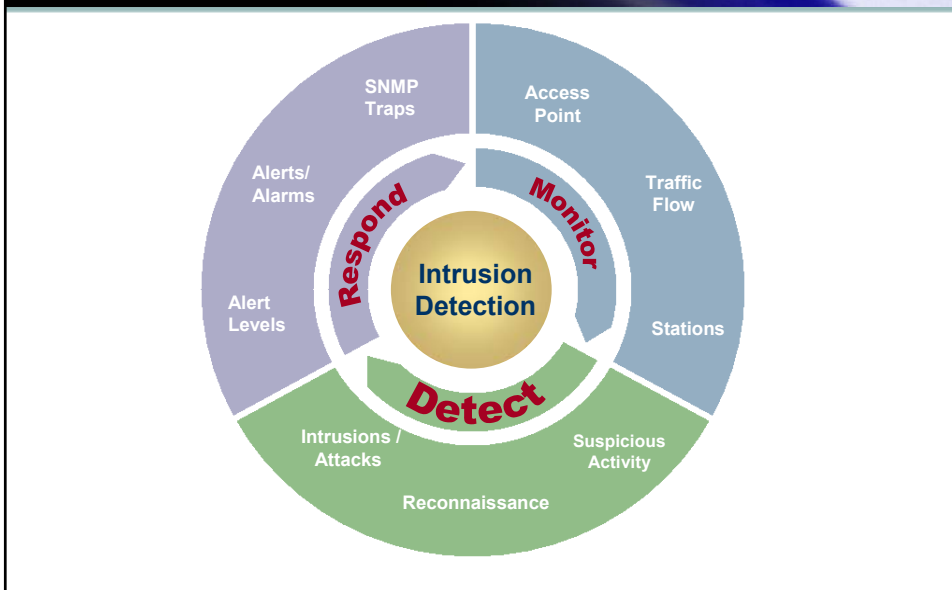


Rogue WLANs are more than rogue APs

AirDefense Functionality Policy Monitoring



AirDefense Functionality Intrusion Detection



AirDefense Functionality

WLAN Health Monitoring

Fault Diagnostics

- APs Malfunctioning
- Failure history
- CRC Errors
- Network misconfiguration

Performance Monitoring

- Too high/low utilization (Too few APs)
- Performance degradation analysis
- Traffic analysis by direction
- Network usage over time

WLAN Misuse

- Bandwidth hogs
- Unauthorized channels
- Unapproved data rates

Wireless LAN Security - A Case Study

- > Bob Martin
VP & CIO
DigitalNet Government Solutions

DigitalNet Government Solutions

- Headquartered in the Dulles Technology Corridor, Northern VA
- Offices in 19 states, with three overseas locations
- More than 1700 technology professionals, approximately 1000 possessing security clearances
- Leading IT provider to the U.S. Federal Government for 30+ years
 - Premier provider of Networked Infrastructure Solutions to Government
 - Information Assurance Consulting Practice since 1978
 - Experience with Civilian, DoD and the Intelligence Community
- World-class advanced technology labs that minimize risk, maximize performance

DIGITALNET

Wireless LANs at DigitalNet

- **Why we deployed WLANs**
 - Employees needed mobility & flexibility while maintaining access to critical information
 - To improve productivity
- **Our Concerns & Challenges**
 - O&M Considerations for Multiple Devices
 - Sensitivity of Data on Lost or Stolen Devices
 - Well publicized inherent lack of security
 - Attacks from hackers or intruders on the corporate network
 - Not knowing if wireless was already deployed without sanctions

DIGITALNET

Our Wireless LAN Deployment

- **Headquarters, Herndon, VA**
 - Sanctioned Wireless LAN
 - Large 5-story building with 2 Access Points on each floor
 - 1 Guest Access Point
 - Total = 9 Access Points
- **5 Remote Locations**
 - No Sanctioned Wireless LAN
 - Ohio, Maryland, Alabama, Illinois, Colorado (2 facilities)
- **Majority Cisco + a few Enterasys Access points**

DIGITALNET

Approach to Deployment & Security

- **Best Practices and Policies**
 - Well Defined and Communicated
 - Supported at the senior management level
 - Organizational culture is your first line of defense
- **Implementation Planning**
 - Understand Business Objectives
 - User's Applications Need
 - User Mobility patterns
- **Layered Security**
 - Containment (Implement and Test Regularly)
 - Authentication/ Authorization
 - Encryption
 - 24x7 Monitoring (Intrusion Detection and Management)



DIGITALNET

Why we Chose to Monitor ?

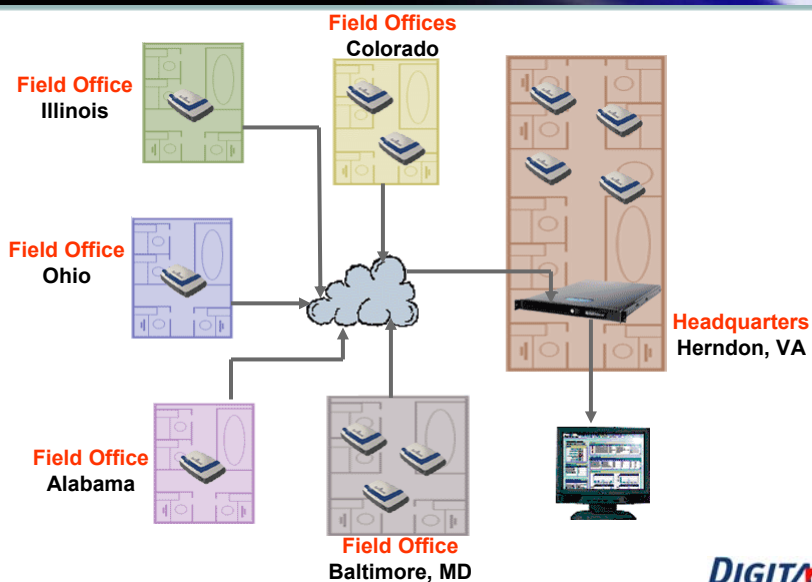
- Two Different Approaches were considered:
 - **Wireless Scanners & Sniffers (NetStumbler)**
 - Not scalable – was very labor and time intensive
 - Lacked central manageability and operations
 - **24x7 real time Monitoring**

We chose 24x7 monitoring because it analyzes WLAN traffic in real time to:

 - Identify rogue wireless LANs
 - Detect intruders and attacks
 - Enforce network security policies
 - Deflect intruders from the network
 - Monitor health of wireless LAN

DIGITALNET

AirDefense Deployment Distributed but Centrally Managed



DIGITALNET

Benefits of deploying AirDefense

- **Ensures Proper Security Configuration**
 - Eliminates Rogue APs, Ad hoc Networks, Soft APs
 - Eliminates Accidental Association Risks
- **Helps Maintain Performance and Reliability**
 - Provides Continuous Survey Verification
 - Monitors Network Performance and Usage
 - Quickly Isolates Interference & Equipment Degradation Problems
- **Detects and Thwarts Malicious Intrusions**
 - Detects and Prevents Scanning, Spoofing, Attacking
 - Provides Immediate Event Alarm/Response

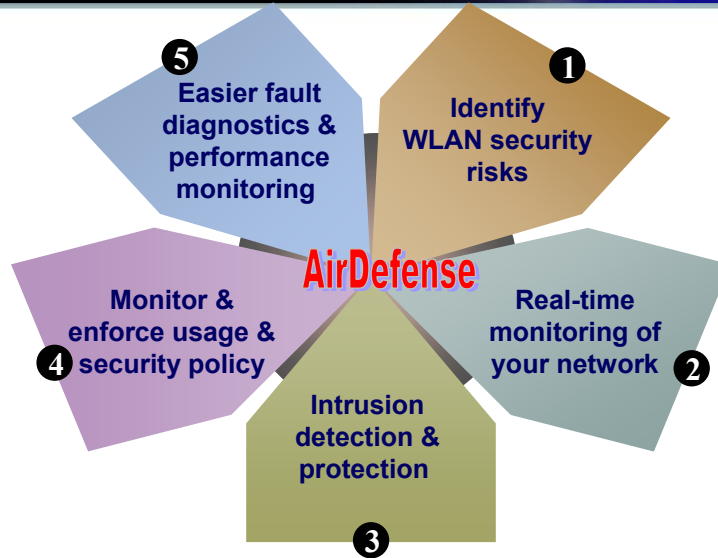
DIGITALNET

Our Journey from Customer To Partner

DIGITALNET

AirDefense Benefits

See, Listen and Protect Your Airwaves



Contact Us

- 1-on-1 demonstration
- Personalized Web demo

info@airdefense.net

770.663.8115 x 126

www.AirDefense.net

