7th July 2005

Wireless Security

AirTight Networks

www.airtightnetworks.net

www.asi.com.au

Presenters: Maree Lowe

Michael Schipp

Agenda

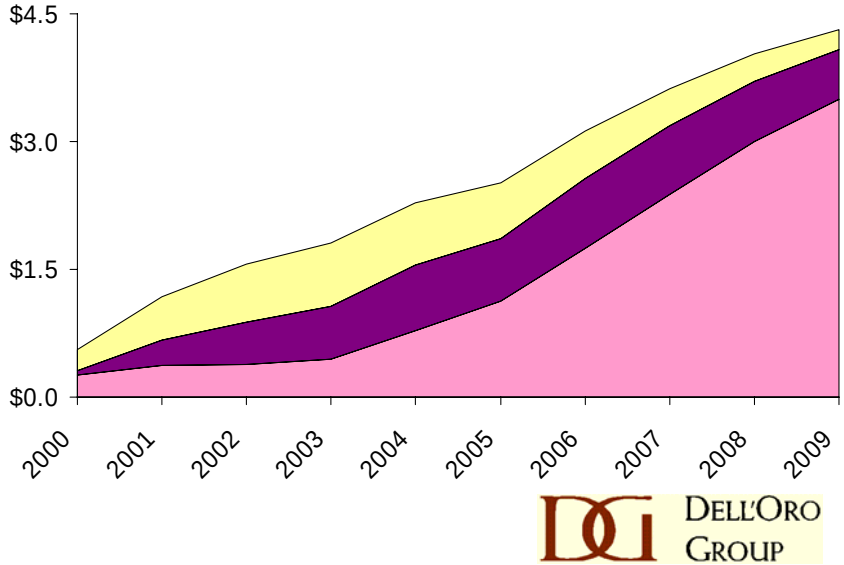
- Wi-Fi Security Evolution
- The Need for Enterprise-Class Wireless IPS
- Introducing SpectraGuard Enterprise 3.0
- AirTight Network Product Advantages
- Summary

Wireless LAN Eras

	1990s	2000s	2010s
Stage	Pioneering	Mainstream	Ubiquitous
Spectrum	900 MHz → 2.4 GHz	2.4 GHz + 5 GHz	2.4 GHz + 5 GHz + ?
Standards	Proprietary → 802.11	802.11 a / b / g "Wi-Fi"	802.11 a / b / g + ?
Markets	Retail Logistics Health Care	Home Networking Enterprise Mobility Hot Spots Education	?
Suppliers	Proxim Aironet Symbol NCR / AT&T / Lucent	Cisco Proxim Symbol Netgear (80+ others) Intel 3Com Allied Telesyn D- Link Linksys	?
Barriers	Price Performance Standards	Security Reliability Management	?

WiFi Market Evolution

- Wi-Fi growth accelerating in the enterprise
- 66% CAGR for embedded Wi-Fi Clients
  - Laptops
  - Mobile Phones
  - VoIP over Wi-Fi
- Exponential growth in wireless threats and network breaches
  - 50% of all network breaches start with Wi-Fi

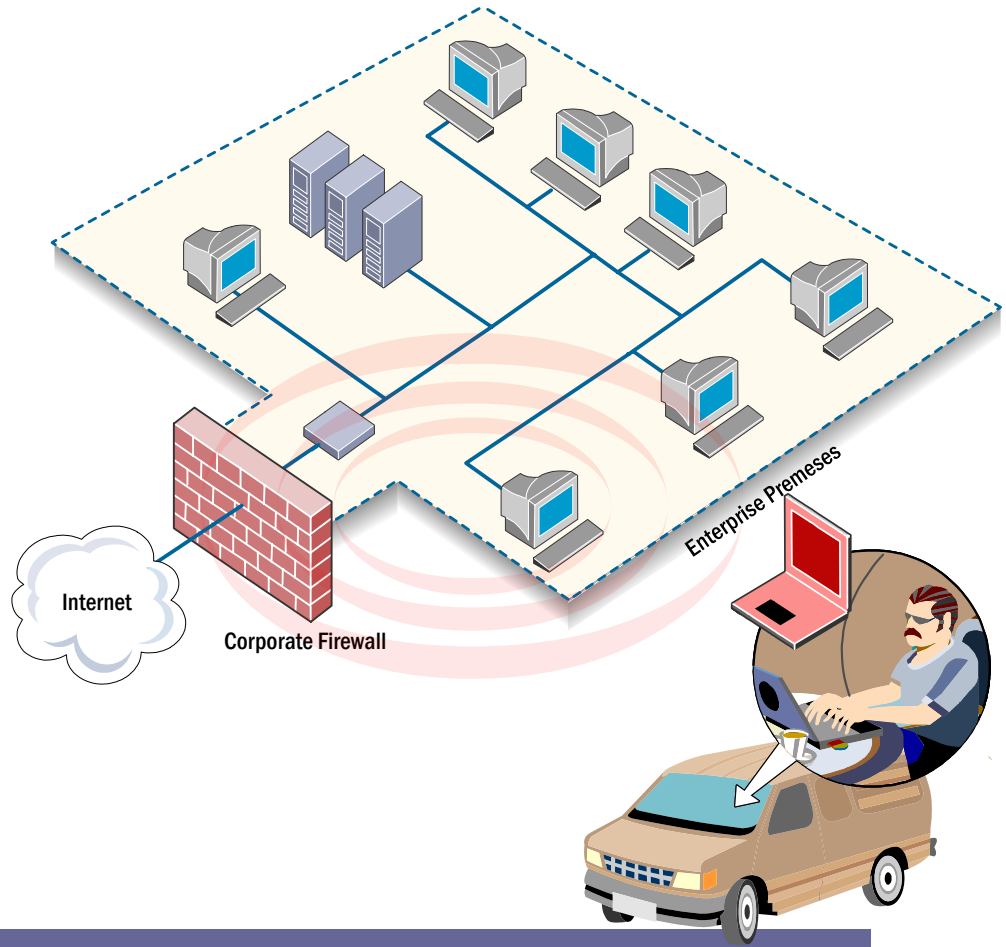


"Nearly one out of every two recorded digital attacks are now taking place via the wireless route as opposed to one out of every ten, at the start of 2004."
mi2g Intelligence Unit

Why do you need Wireless IDS /IPS on your Wired and WiFi network?

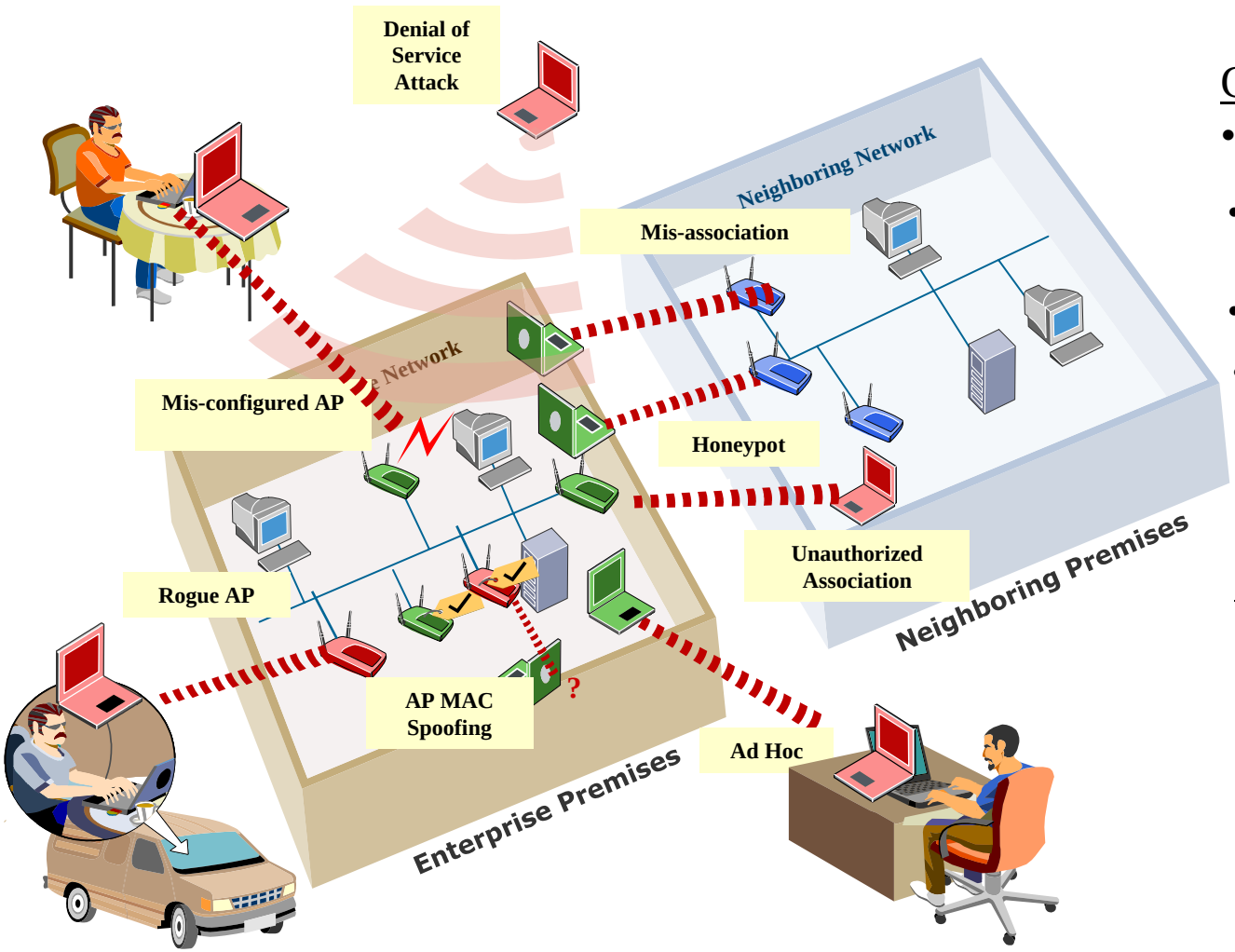
Wireless Threats Exist in Every Network

- A single rogue AP behind the firewall…
- …and your network is at risk
- Even if you do NOT have a wireless LAN



Your Corporate Air Space is an Asset that Must be Monitored, Managed and Protected

Major Wi-Fi Threat Categories



Common

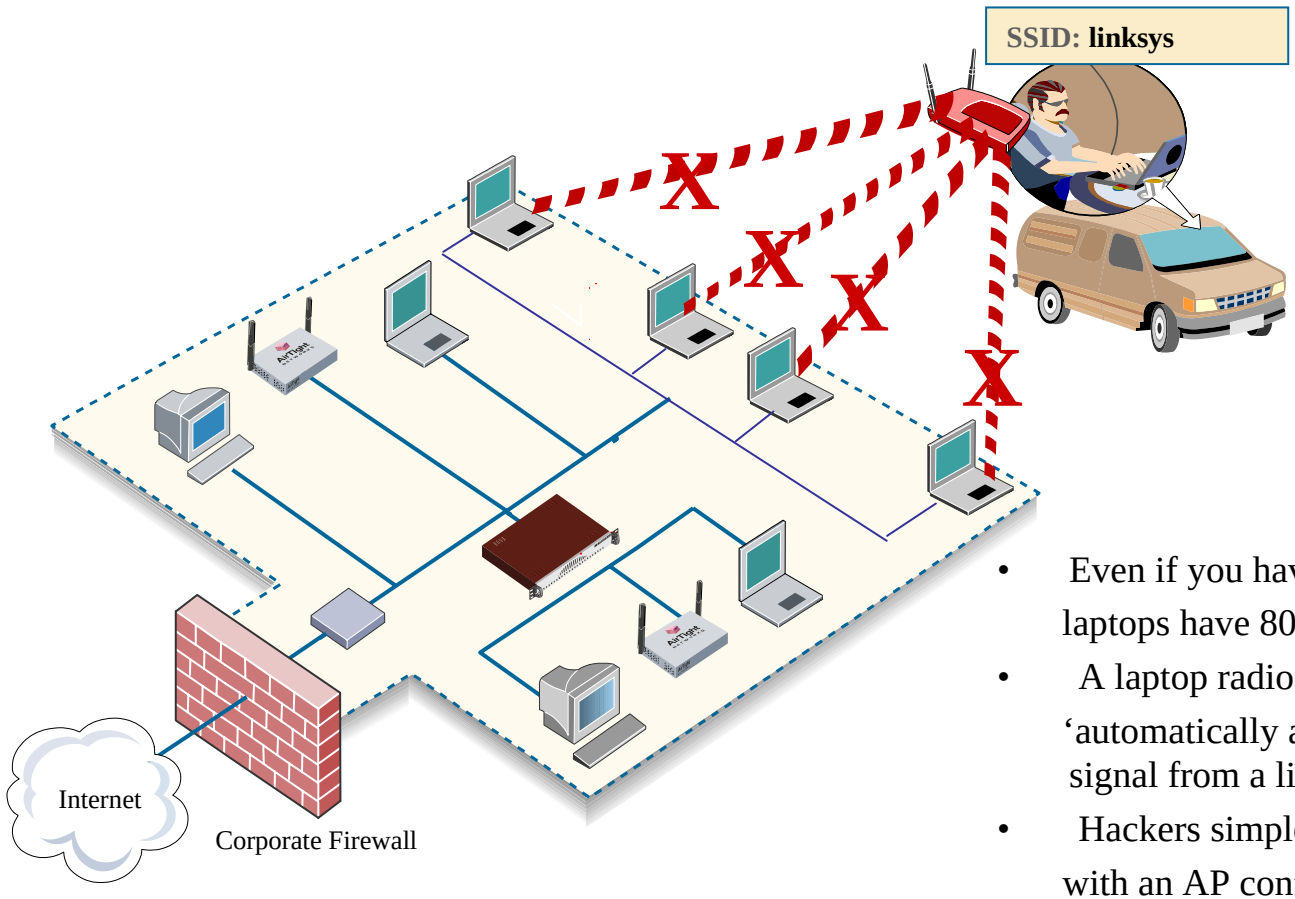
- Rogue Access Points
- Mis-configured Access Points
- Ad hoc connections
- Client mis-associations
- Unauthorized client associations

Malicious

- Honeypot APs
- MAC Spoofing APs
  - Client > Malicious AP
- Denial of Service
  - De-authentication flood
  - Packet storm

Firewalls, VPNs, and 802.11 Security Standards
Do Not Prevent These Wi-Fi Threats on Either Wired or Wireless Networks

Prevent Wi-Fi Threats in a No Wi-Fi Network



Honeypot attack lures in multiple laptops to miss-associate.

- Even if you have no 802.11 AP's, most laptops have 802.11 cards
- A laptop radio is default configured to 'automatically associate' with the strongest signal from a list of SSID's
- Hackers simple sit outside the building with an AP configured to a common SSID and wait for a number of laptops to connect

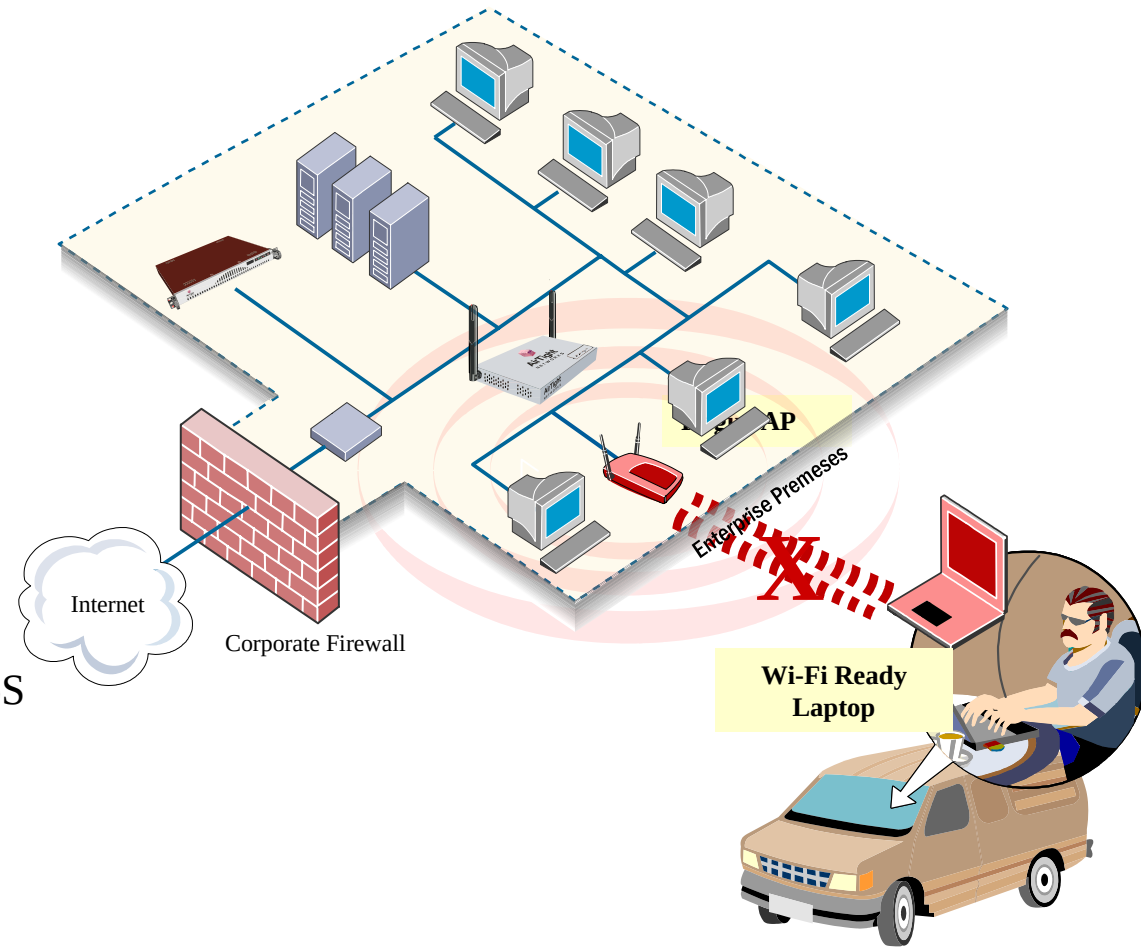
Rogue AP Blocking

Rogue AP is Detected
- Over-the-air detection
- Network connect tested
- Auto-classified

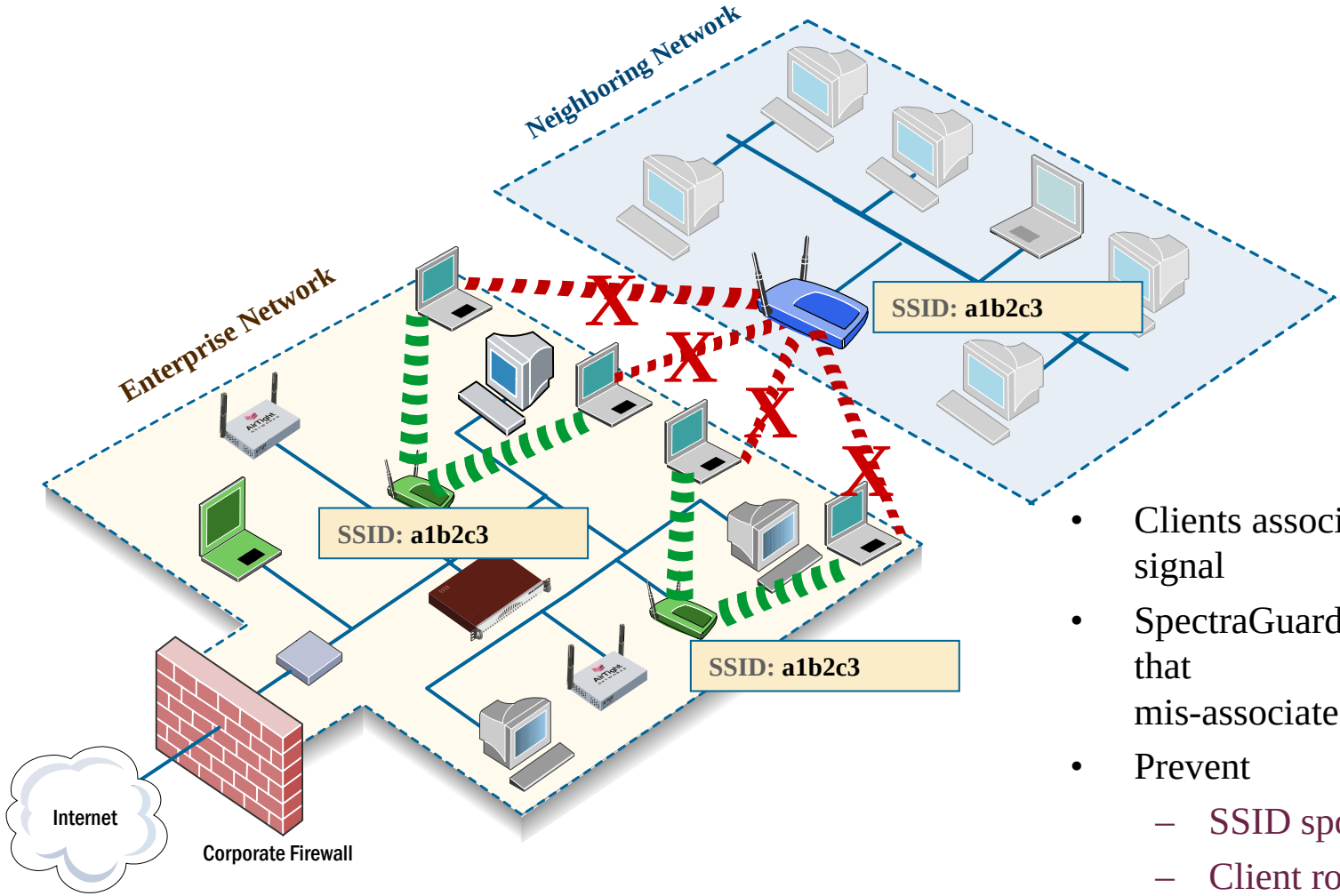
- No False Positives
  - Does not rely on switch

- Blocked over-the-air
  - 100% accurate
  - Any network / switch

- Better than port blocking
  - Port blocking is not reliable
  - Port blocking may cause DoS

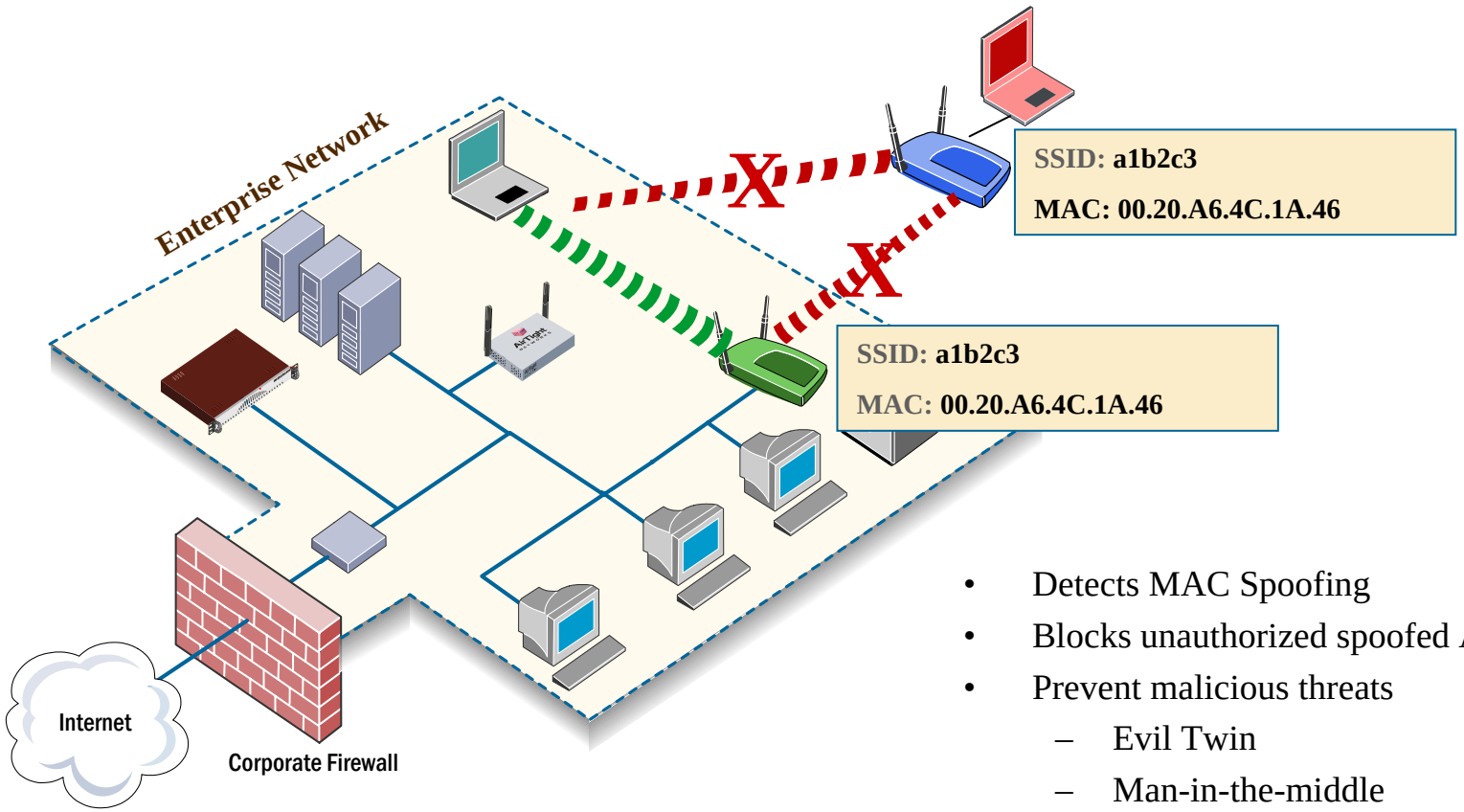


Prevent Client Mis-Association



- Clients associate to strongest signal
- SpectraGuard blocks clients that mis-associate
- Prevent
  - SSID spoofing
  - Client roaming

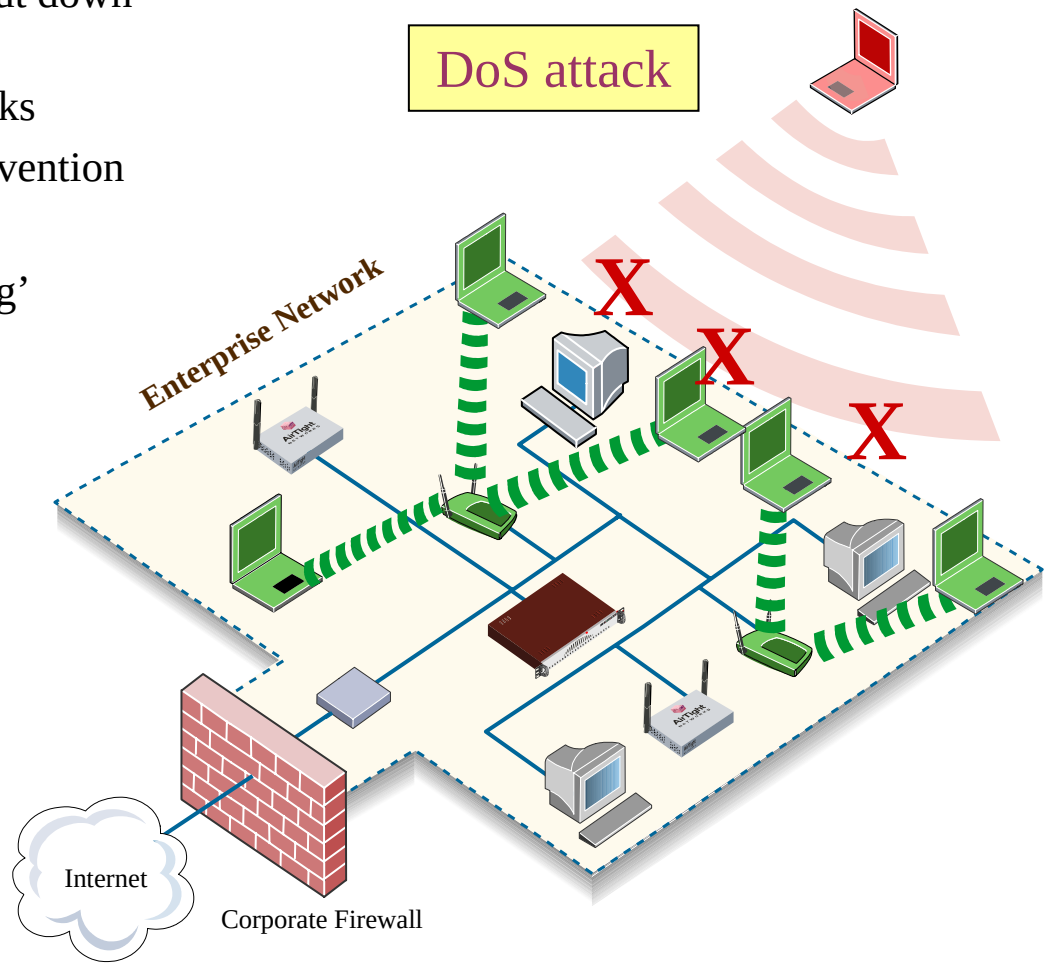
Prevent MAC & Air-Jack Attack



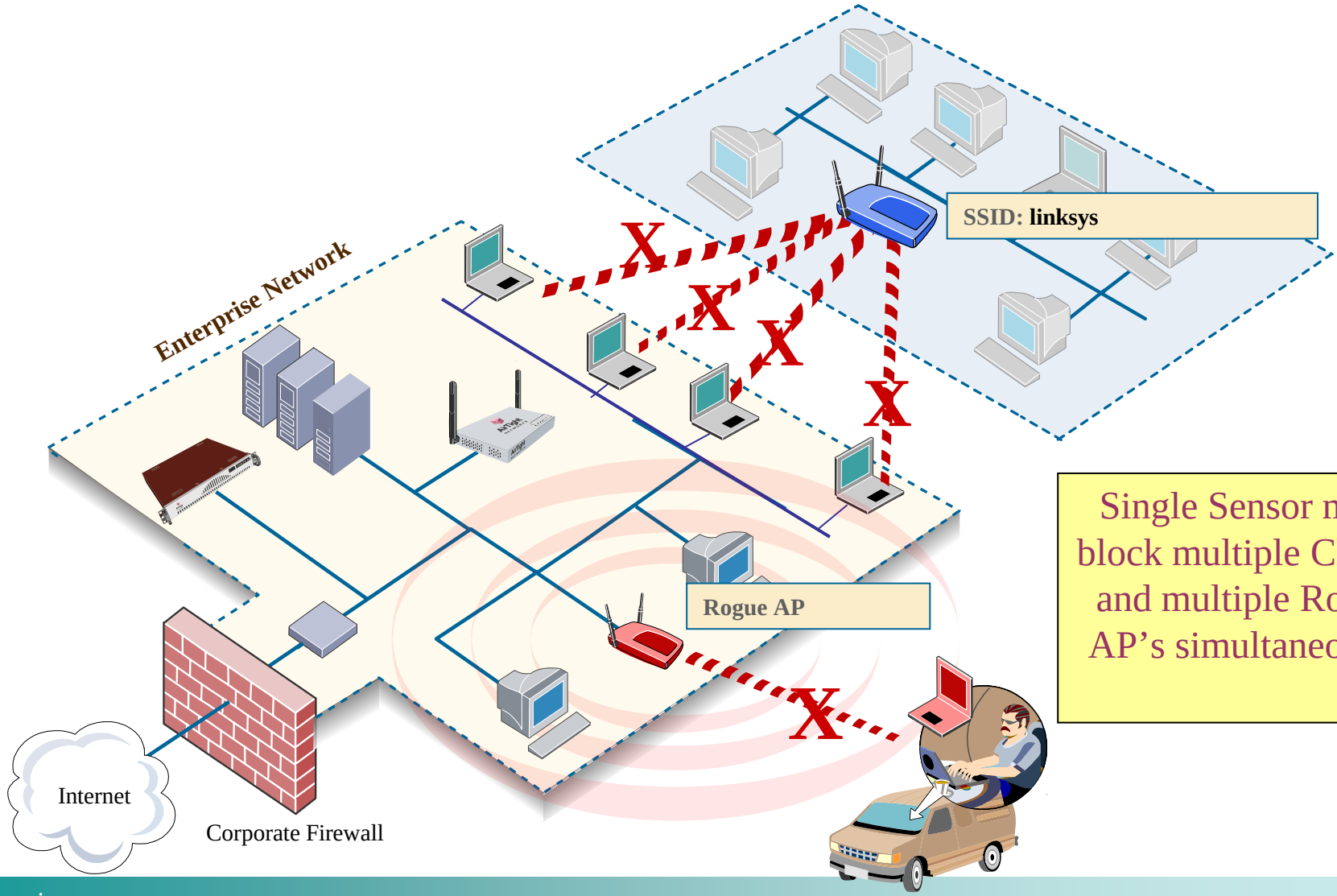
- Detects MAC Spoofing
- Blocks unauthorized spoofed AP's
- Prevent malicious threats
  - Evil Twin
  - Man-in-the-middle

Denial of Service Attack Prevention

- Wi-Fi Denial of Service can shut down your network
- SpectraGuard blocks DoS attacks
  - Exclusive vendor DoS prevention
- Patented
  - 'Virtual Selective Jamming' technique

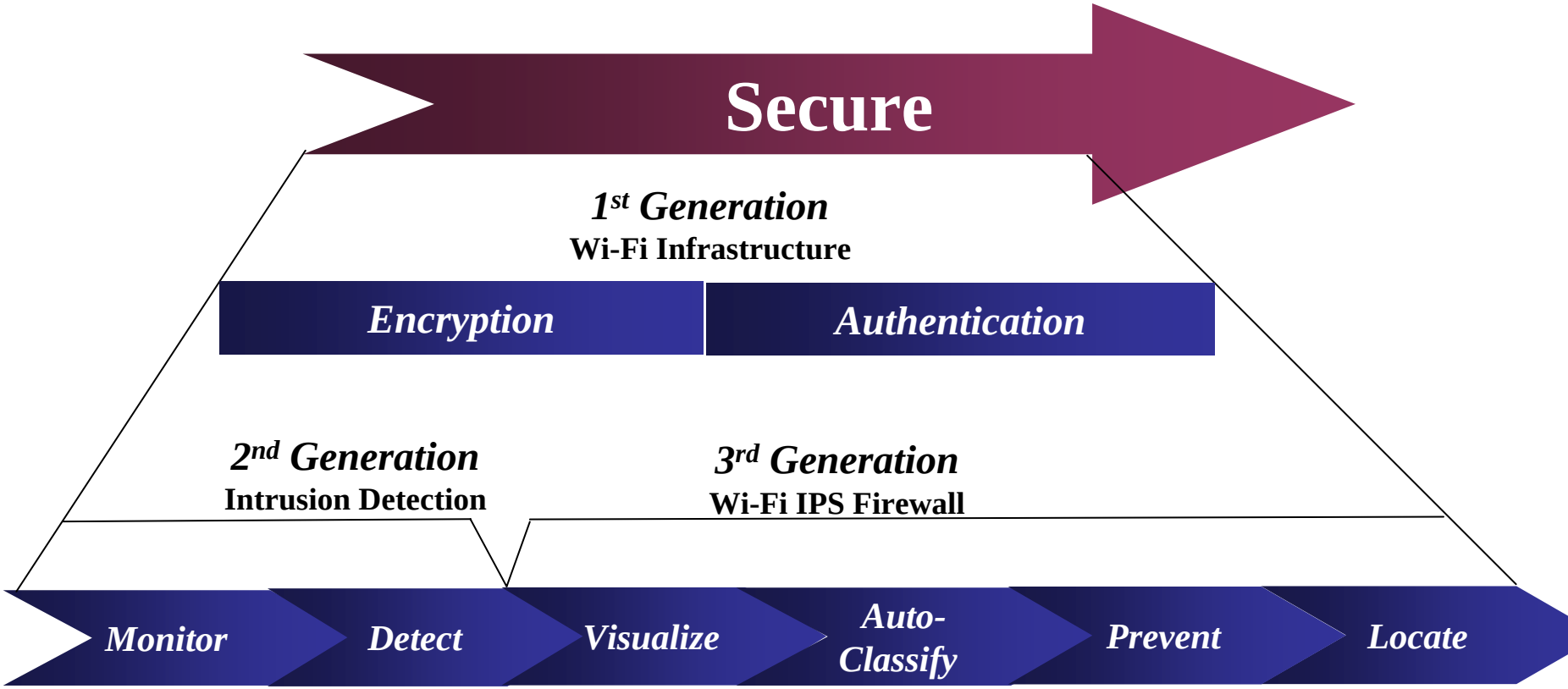


Complete Protection Requires Simultaneous Threat Prevention



Single Sensor must block multiple Clients and multiple Rogue AP's simultaneously

Key Elements of Wi-Fi Security



- 2.4 and 5 GHz
- All channels
- Continuous
- Association
- Activity

- APs and clients
- Alerts/alarms

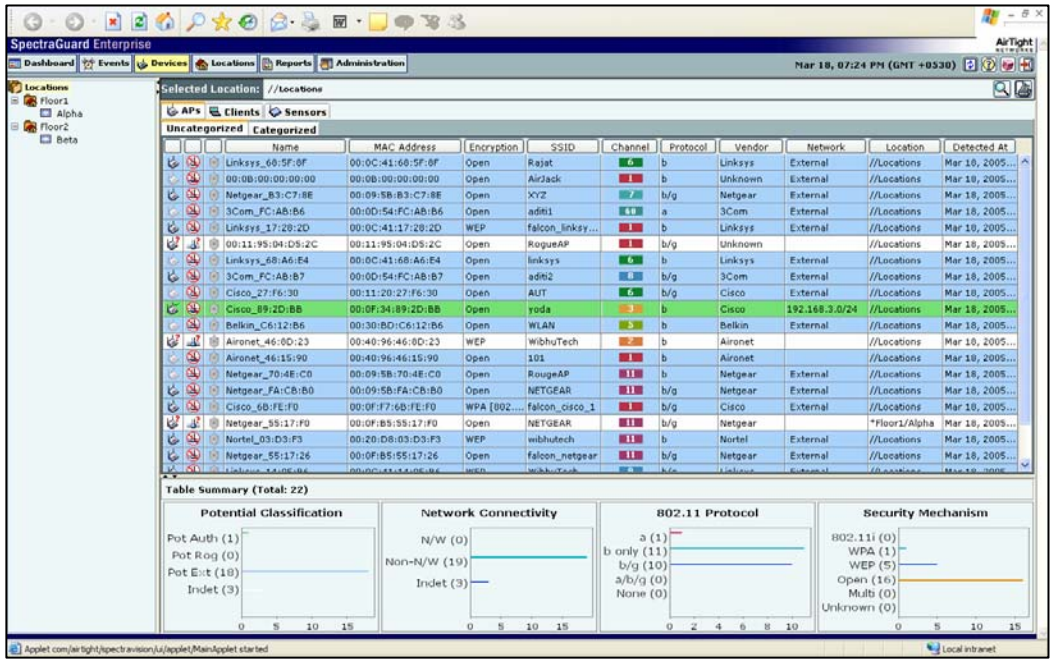
- Live RF maps
- Site specific
- Access points
- Security sensors

- Accurate filtering
- All devices
- All threats

- Block threats
- Automatic
- Non-disruptive

- Plot on floor plan
- Permanent removal

Monitor/Detect



- Scan all bands
  - 2.4 GHz and 5 GHz
- Detect all Wi-Fi activity
  - Access points, soft APs, NATing APs, clients
- Correlate information from multiple sensors
  - Eliminate confusing duplicate reports of the same device

Visualize

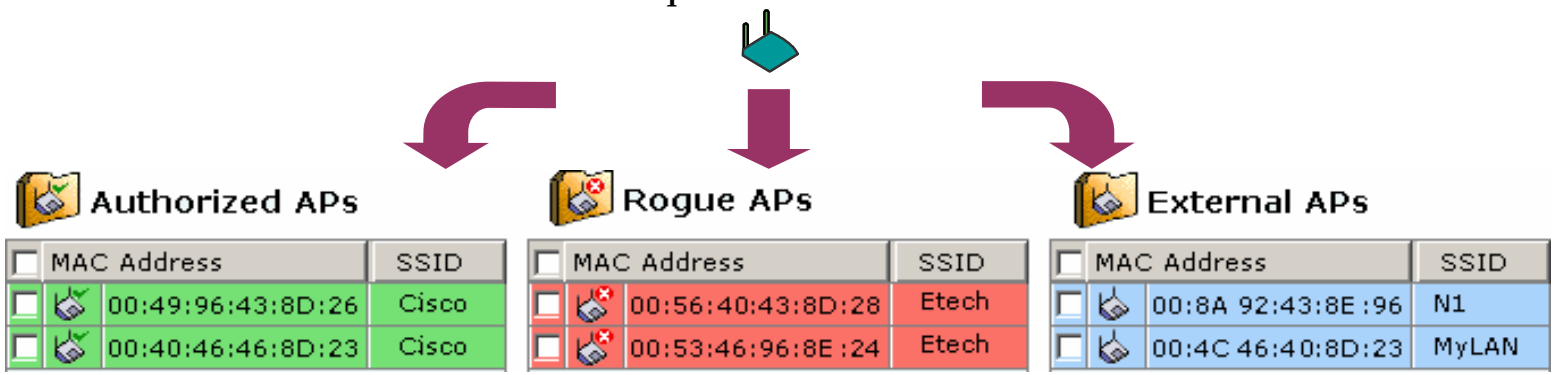
- Make your airwaves visible
- View RF coverage in real time
  - Handhelds only provide a snapshot in time
- Plan for security and Wi-Fi coverage
  - Only integrated solution that ensures proper sensor placement
  - Model detection and prevention levels
- Self-calibrating
  - Site-specific RF characteristics
  - Deployment orientation

No RF Coverage

Poor RF Coverage

Auto-Classify

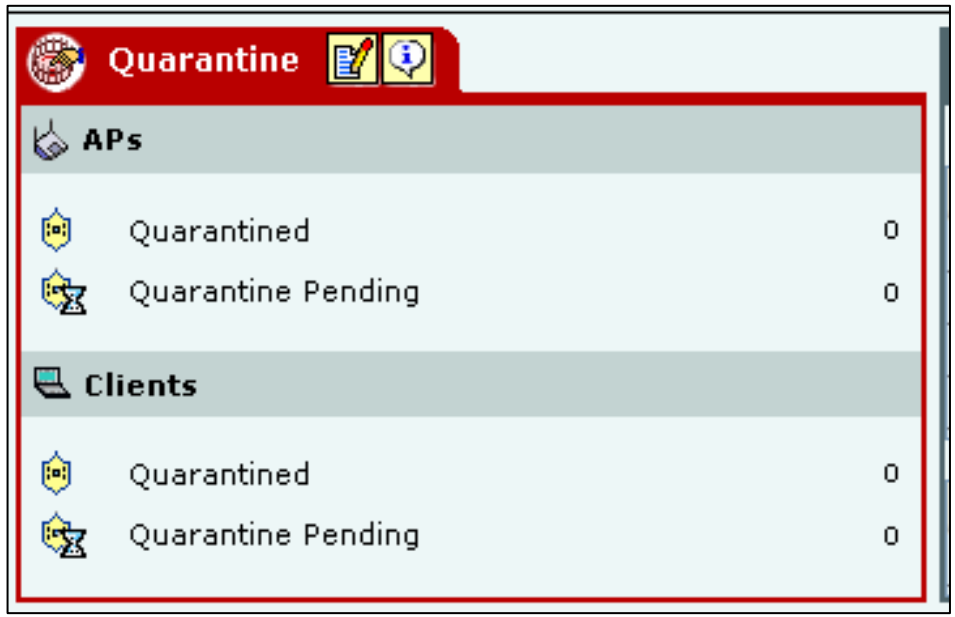
- Comprehensive
  - Access points
    - Authorized, Rogue, External
  - Clients
    - Authorized and unauthorized
- Accurate
  - No false positives/no false negatives
- Instantaneous
  - No manual user intervention required



SpectraGuard Enterprise dashboard automatically classifies Access Points and Clients into appropriate categories.

Prevent

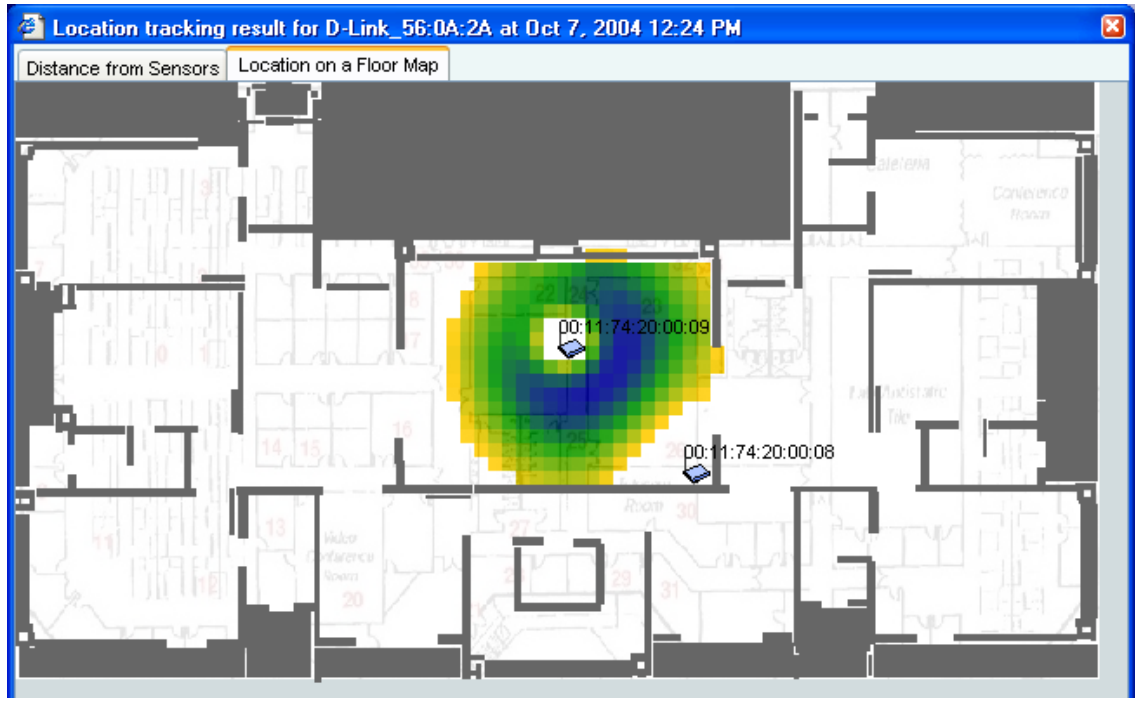
- Over-the-air
  - Ensures non-stop protection
- Instantaneous
  - Based on quarantine policy and accurate auto-classification
  - Doesn't require manual administrator intervention
- No harm policy
  - Won't disrupt your own or neighbor's networks
- Most comprehensive solution
  - All major classes of threats
  - Rogue access points, Evil Twin/Honey Pot APs, MAC spoofing APs, mis-configured APs, rogue clients, client mis-associations, ad hoc networks and DoS attacks



SpectraGuard Enterprise dashboard shows rogue access points that has been quarantined; I.e. automatically blocked to prevent any and all client connections.

Locate

- Precise
  - Locates rogues and other Wi-Fi security threats for physical remediation
  - Pinpoints all AP and client device locations
- Authorized, unauthorized and neighbor
- Immediate
  - One click operation
- Site calibrated
  - Displays location on a floor plan
- One click operation provides graphical probability analysis of location
  - Not just a red ‘X’



SpectraGuard Enterprise integrates a floor plan to show a range of probable locations of rogue APs or clients.

AirTight Solutions

- SpectraGuardEnterprise

  A Comprehensive Wi-Fi IPS Firewall and Performance Management Solution

- SpectraGuard Sentry

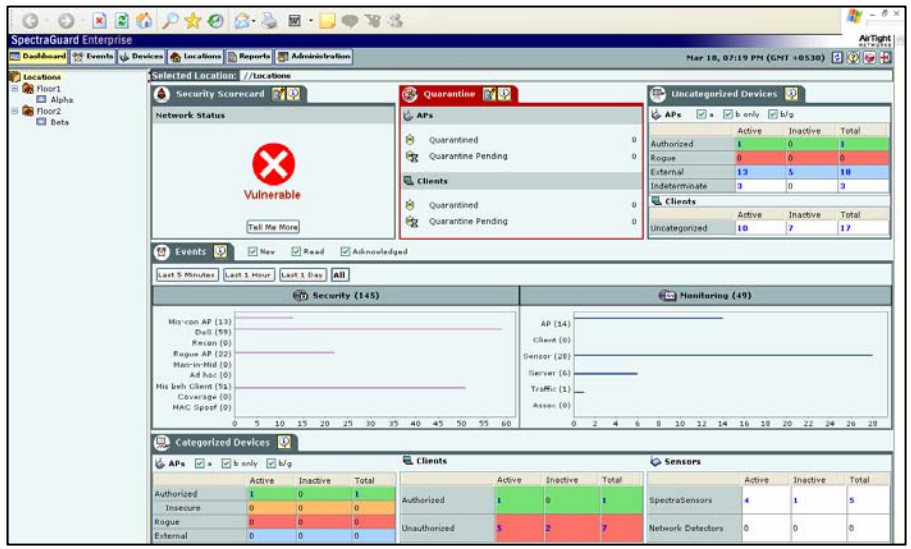
  Affordable Wi-Fi IPS Firewall for Small Businesses

- SpectraGuard Planner

  Wireless LAN Planning for Performance, Coverage and Security

SpectraGuard Enterprise Server

- Wi-Fi IPS Firewall
  - Provides Monitoring, Detection, Visualization, Auto-Classification, Prevention and Location services
- Auto-classification
  - Accurately identifies all classes of Wi-Fi threats including rogue access points, ad hoc networks and denial of service attacks
- Prevention
  - Automatically blocks simultaneous multiple threats
  - While continuing to scan
  - Selectable prevention level
- Location Tracking
  - Probability graph of location
  - APs and clients
- Monitoring and Reporting
  - Realtime coverage maps
  - Wireless statistics
- System Management
  - Web
- Dimensions
  - 1 RU



SpectraGuard Sensor

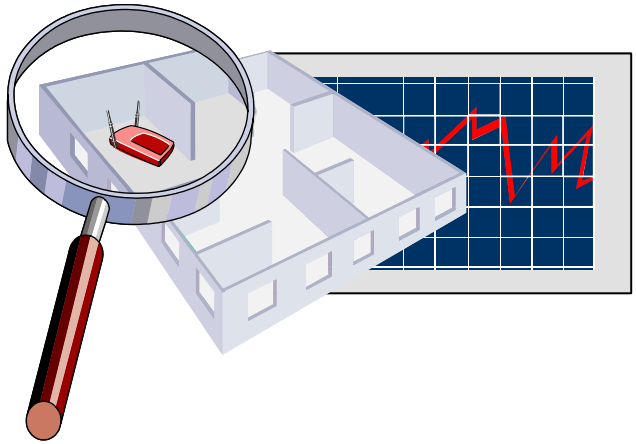
- Dual radio 802.11a and 802.11b/g
- Scans for IEEE 802.11a/b/g devices on all channels
- Simultaneously scans in 2.4 and 5 GHz band
- Devoted to 24 x 7 scanning unlike access points
- Automatically discovered; central configuration from Server
- Limited intelligence - no information in sensor to compromise enterprise if stolen
- Power over Ethernet; plenum rated

SpectraGuard Sentry

- Standalone WIPS Firewall for Wi-Fi Intrusion Detection and Intrusion Prevention
- Browser based management
- Works alongside any Access Point and/or LAN Firewall
- Prevents Rogue AP, Rogue Client, HoneyPot attack, Evil Twin Attack,
- Enables No Wi-Fi policy on Wired Networks
- Simultaneously scans, detects and protects on 802.11 a/b/g
- Protects area between 25,000 to 40,000 square feet

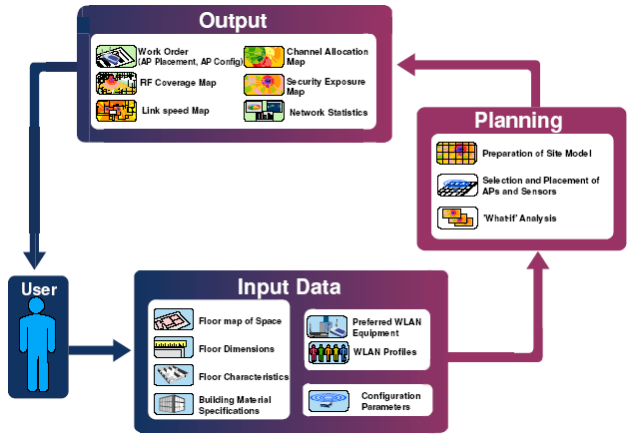
ASI - AirTight Services

- Wireless Vulnerability Assessment



Assess how well your network defends against wireless threats

- Wi-Fi Planning Service



Quick online outsourcing of your Wi-Fi site survey

What Customers think is VIP

"We're still manually classifying Devices and events six months later with our previous IDS system. With AirTight, we completed six months of work in 20 minutes!"

Major Fast Food Retailer

"Over 90% of the alerts from our IDS system were spurious. With AirTight, we aren't bothered with false alarms."

Leading Semiconductor Design Software Developer

"This product is simple - we gave it to our help desk for troubleshooting wireless connectivity issues."

Nation's Largest Auto Wholesaler

Ivy Tech College

Needs:
- Students / Faculty want WiFi
- WiFi is competitive advantage

Issues:
- Students are curious
  - Ad Hoc connection to Faculty PC's
  - Admin Client mis-association to HoneyPot
- Rogue AP's open Admin network
- Evil Twin AP and Web Spoofing
  - Potential identity theft
- Control WiFi within campus
- No free WiFi to neighbors

AirTight Solutions:
- AirTight SpectraGuard WiFi IDS / IPS
  - Detect wireless vulnerabilities
  - Prevent wireless threats
  - Monitor wireless network
- AirTight SpectraGuard Planner
  - Maximize wireless performance
  - Minimize wireless expense
  - Control wireless within campus

"*We require WiFi on campus to remain a competitive college attracting top students and faculty*. SpectraGuard assures our network is reliable and secure from wireless vulnerabilities assuring the integrity of our students and institution."

Ivy Tech, Network Operations Manager.

Adesa

Challenge:

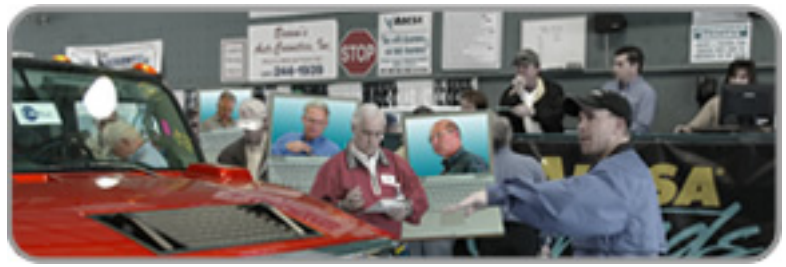
- Desire for wireless LAN access, but not allowed until security concerns answered
- Especially important as PUBLIC Company that needs to ensure Sarbanes Oxley compliance
- Didn't trust built-in security
- Wanted 24 x 7 dedicated security device

AirTight Solution:

- SpectraGuard Enterprise 3.0
- 24 x 7 monitoring

Results:

- Proved wireless can be deployed securely
- Rolling out to corporate headquarters and all 47 branch offices
- Easy enough for help desk to use to allow guests on network



"We've tried to break SpectraGuard, but we can't. It only took us one night to configure. It just works the way it's supposed to. We've proven that it works and now senior management will allow wireless LAN access throughout the corporation."

Chris Roberts, IT Operations Security Supervisor

Thank you

www.asi.com.au