Aplura, LLC
5653 Blithaire Garth
Columbia, MD, 21045
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
http://www.aplura.com

Wireless Policy Enforcement

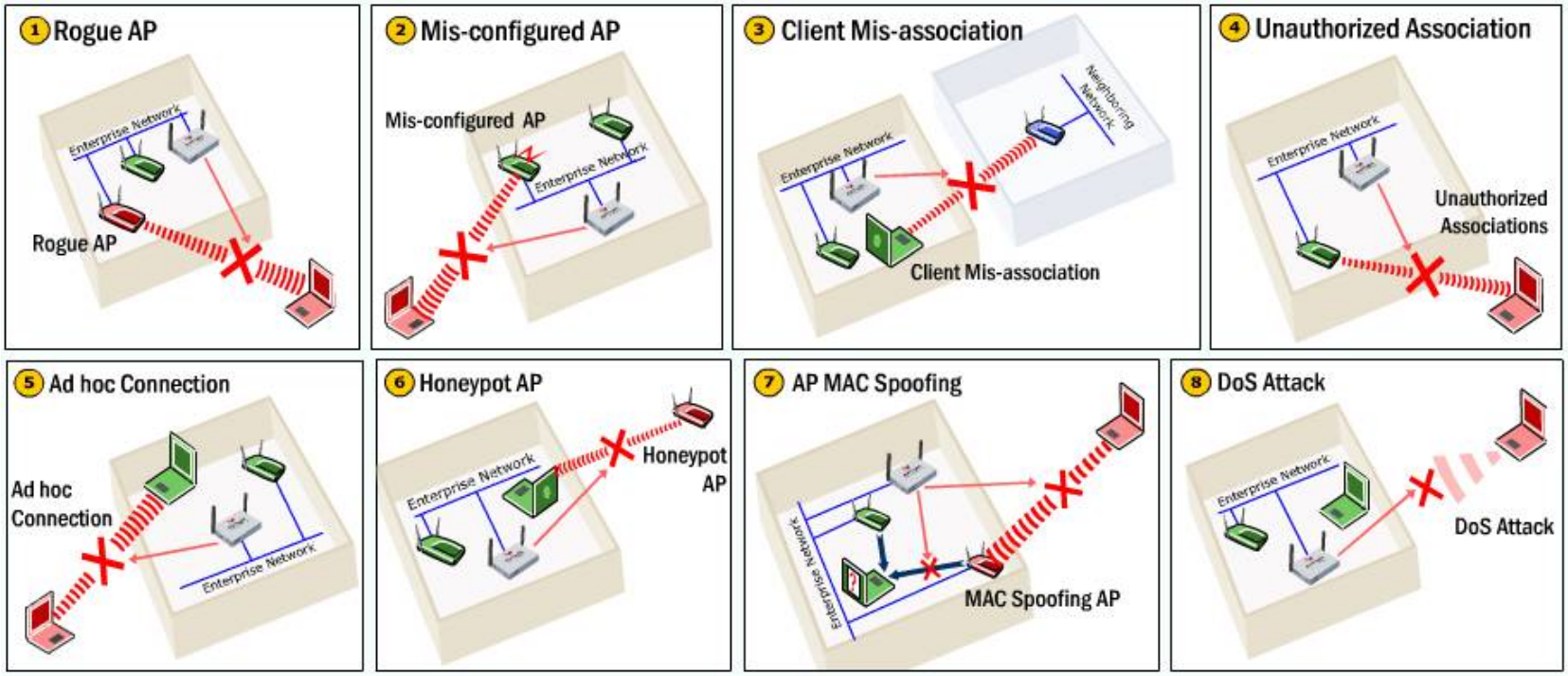
Overview

- Wireless Policy
- Policy Audit: Manual vs. WIPS
- Case Study: 2006
- WIPS Today
- 2008 WIPS Market Survey
- Vendor Comparison
- Conclusion

Wireless Policy

- Should support organization's AUP
- Example Policies:
  - All APs "must be registered and approved"*
  - Only approved clients can connect*
  - VLAN-separation for wireless clients*
  - Disciplinary action for policy violations*
  - Clients must not bridge wired network*

Wireless Attacks



Manual Policy Compliance

- Author and Implement the policy
- Measure/Audit the Policy
  - Not effective/Error prone ”compliance whack-a-mole”
  - Heavy reliance on auditor's skill and equipment
- Enforce the Policy
  - All the same problems as above
- This is neither effective nor scalable

WIPS Overview

- Overlay architecture
- Always on!
- Vendor support (code, updates, plans, howtos)
- Audit wireless policy compliance
- Enforce wireless policy
- WIPS vs. WIDS
- Useful, even with a ”No Wi-fi Policy”

Case Study: Intro

- Fall 2005 - World Wide USG Network
  - 90 sites in >75 countries
  - Slow (high-latent) links
  - No Wi-Fi policy
- ”Best Secured” network in Fed
- CISO ”Detect and stop rogues”
- Small CISO staff

Case Study: Project

- Market Survey
- Research
- Bake Off

Case Study: Solution

- AirTight
  - ”Protect the good, enforce the policy”
  - Accurate classification = less TCO
  - Uses actionable data to audit policy
  - Measure/protect all clients (even off-net)
  - Scalable (built around MSSP model)
  - Prevention Mode

WIPS Today

- Current happenings in WIPS space
  - Acquisitions/mergers
  - New Players in the space
  - New Technology (e.g. 802.11n)
- July 2008 - Customer market survey

2008 WIPS Market Survey

- Define project
- Identify market players
- Evaluate industry posture
- Invite market leaders to present

Market Leadership

Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirDefense			x		
AirMagnet			x		
AirTight				x	
Aruba Networks			x		
Cisco Systems		x			
Network Chemistry				x	
Newbury Networks		x			

Source: Gartner

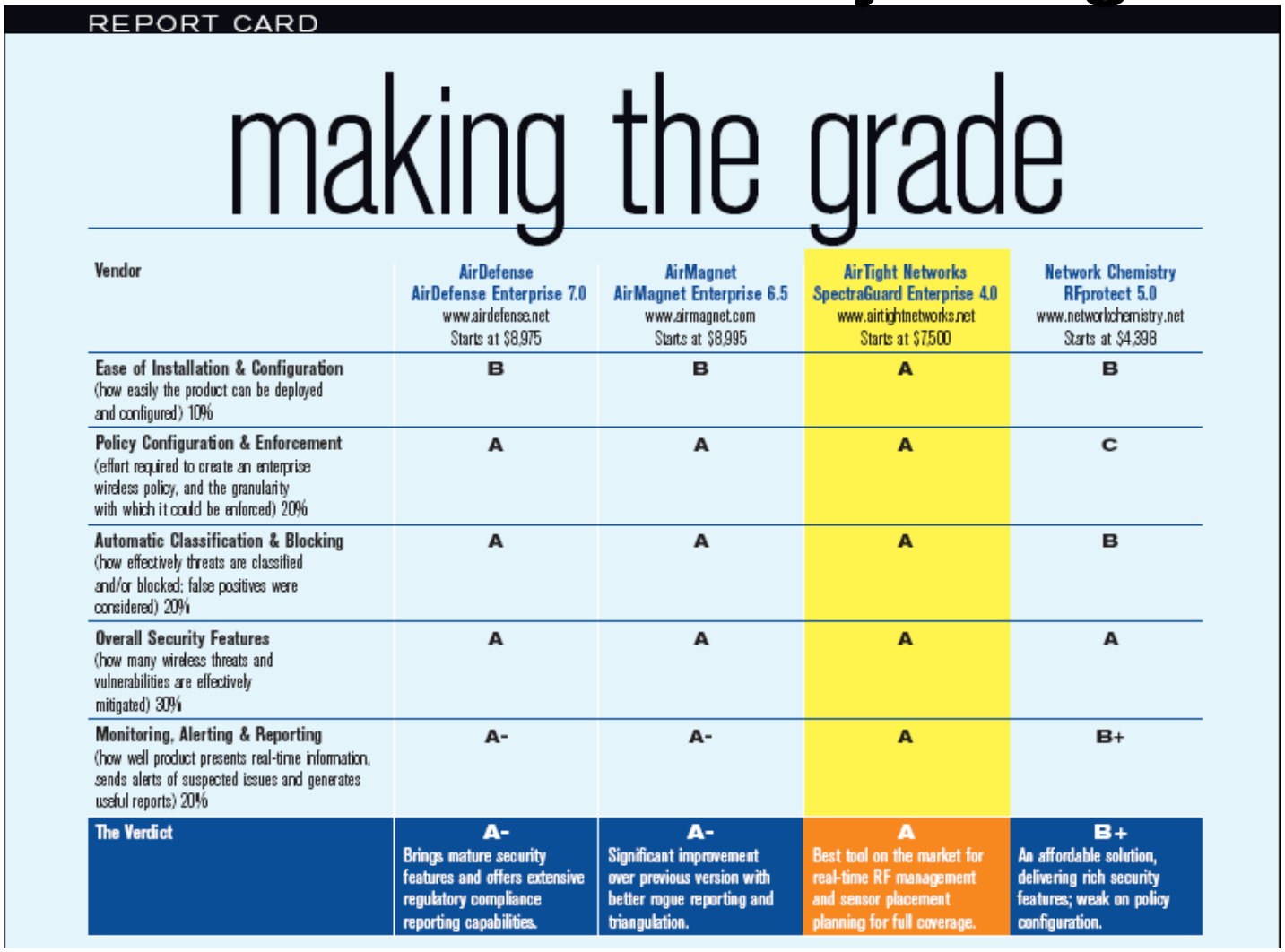
Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirDefense				x	
AirMagnet				x	
AirTight Network				x	
Aruba Network			x		
Cisco		x			

As of July 2008

Source: Gartner (July 2008)

Information Security Magazine



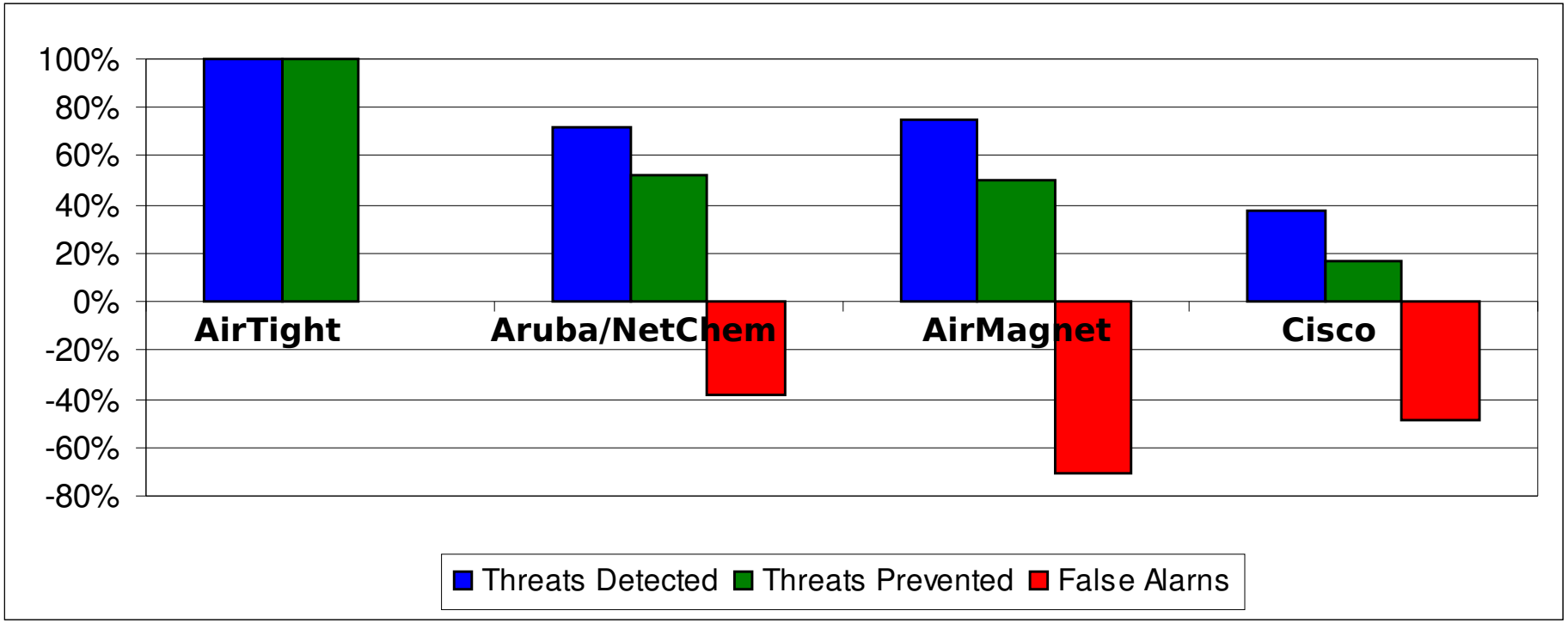
REPORT CARD

making the grade

Vendor	AirDefense AirDefense Enterprise 7.0 www.airdefense.net Starts at $8,975	AirMagnet AirMagnet Enterprise 6.5 www.airmagnet.com Starts at $8,995	AirTight Networks SpectraGuard Enterprise 4.0 www.airtightnetworks.net Starts at $7,500	Network Chemistry RFprotect 5.0 www.networkchemistry.net Starts at $4,398
Ease of Installation & Configuration (how easily the product can be deployed and configured) 10%	B	B	A	B
Policy Configuration & Enforcement (effort required to create an enterprise wireless policy, and the granularity with which it could be enforced) 20%	A	A	A	C
Automatic Classification & Blocking (how effectively threats are classified and/or blocked; false positives were considered) 20%	A	A	A	B
Overall Security Features (how many wireless threats and vulnerabilities are effectively mitigated) 30%	A	A	A	A
Monitoring, Alerting & Reporting (how well product presents real-time information, sends alerts of suspected issues and generates useful reports) 20%	A-	A-	A	B+
The Verdict	**A-** Brings mature security features and offers extensive regulatory compliance reporting capabilities.	**A-** Significant improvement over previous version with better rogue reporting and triangulation.	**A** Best tool on the market for real-time RF management and sensor placement planning for full coverage.	**B+** An affordable solution, delivering rich security features; weak on policy configuration.

Focused Information Security
http://www.aplura.com

WIPS Test Results – Detection/Prevention



Source: Tolly Group

*Air Defense declined to participate in this evaluation

AirTight Differentiators

- Patented “Inside-Out” Detection Method
- Detects and Prevents NAT’d, Encryption and Soft APs
- Zero False Positives
- Does not rely on CAM Table look-ups
- Pre 802.11n and Draft 802.11n Detection and Prevention
- Wireless Policies Enforced per VLAN, SSID, and location
- Multi-VLAN Support
- 3rd Generation WIPS (not WIDS)

AT Differentiators cont'd

- Blocks DoS Attacks
- Multiple Threat Prevention across Multiple Channels
- Auto-Authorization of Clients
- Accurate Location Tracking
- Same Server Manages both Sensors and SAFE Clients
- Ability to Manage over 10,000 Sensors from a Single Console
- Ease of Use

Market Survey Conclusion

- Accurate detection fosters prevention
- Fast reaction-time improves security posture
- AirTight:
  - Accurately detects wireless threats
  - Protects critical resources (clients and APs)
  - Is designed to be “hands off”
  - Is scalable
  - Is priced competitively

Questions?

Presented By:

Sean Wilkerson

CISSP, GSNA, SSP-DRAP

swilkerson@aplura.com