THE TOLLY GROUP

The authoritative, unbiased source for IT certification, research and testing

WHITE PAPER

February 2006

A white paper commissioned by AirTight Networks, Inc.

Document #206103

Evaluating Wireless Intrusion Prevention Systems

Comparison of Products from AirTight Networks, AirMagnet and Aruba Networks Reveals Robust Capabilities of AirTight SpectraGuard Enterprise

TOLLY Up to Spec CERTIFIED

Statement of Licensing Info and Acceptable Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors can occur.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

Tolly Group Services

With more than 17 years experience validating leading-edge Information Technology products and services; The Tolly Group has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy.

Our "Up-to-Spec" service provides the custom testing complement to the "standard", granular tests offered in "Tolly Verified". See our "Up-to-Spec" Home Page.

Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

This document was authored by:

Charles Bruno,
Executive Editor
The Tolly Group

Table of Contents

Evaluating Wireless Intrusion Prevention Systems

Keeping Threats in Check

An effective WIPS must do three things well:

1. Detect & automatically classify wireless devices & events - to figure out which are threats and which are not
2. Prevent multiple wireless threats simultaneously while continuing to scan for new threats
3. Accurately locate threats on a floor map - so they can be eliminated quickly

All enterprises face a new category of security threats created by wireless networking - whether or not they choose to install a wireless LAN. Every laptop computer today ships from the factory with built-in wireless capabilities. When these laptops are turned on, they automatically start looking for a wireless signal, and, if they find one, they'll start networking.

They may network with the authorized corporate network, or a neighbor's network across the street, or a "honeypot" AP deliberately placed by a hacker to steal their information, or even with another laptop computer if there's no WLAN in the area. In any of these scenarios, the enterprise network and security managers must protect the user's data, the laptop, and the network.

In addition, wireless APs are now so small and so inexpensive that rogue APs are now a common phenomenom and a commonly understood threat. The majority of rogues are not attached to the network for malicious purposes, but they open holes in the network perimeter nonetheless. And, there are rogues that are placed for illegal purposes, and these have to be found and eliminated quickly.

In all of these cases, network managers must have the tools, and the processes, in place to deal with the litany of wireless threats.

The primary tool being deployed in this security campaign across enterprises is the wireless intrusion prevention system (WIPS).

Products under test:

- AirTight Networks SpectraGuard Enterprise Ver. 4.0
- AirMagnet, Inc. AirMagnet Enterprise Ver. 6.1.0
- Aruba Networks Aruba Mobility Controller Ver. 2.4.1.0

Unlike wired security devices, WIPS monitor the airwaves to detect wireless threats. Users need to understand that not all WIPS are equally effective at classification, prevention, and location of wireless threats.

Moreover, while competitive WIPS solutions may indeed offer many of the same security provisions, the degree and depth of those capabilities varies markedly. Given the mission-critical nature of the data and traffic traversing the corporate airwaves, it is imperative for network managers to understand the difference in protection afforded by various WIPS solutions.

For instance, while the vast majority of WIPS offerings suggest they can identify rogue APs and protect against them, the reality is that these products do so to very different degrees. While several systems may all identify a rogue AP, they may have vastly different success rates at so-called wireless blocking, where the WIPS instructs clients to cease communicating with the rogue AP(s).

Test Highlights - SpectraGuard Enterprise

- Detects 100% of the security threats launched against it, while AirMagnet Enterprise missed 25% and Aruba Mobility Controller missed 30%
- Prevents 100% of the threats, while AirMagnet Enterprise prevented half of them, and Aruba prevented only one-third
- Effectively prevents multiple threats simultaneously from a single sensor, while the competitive devices did not
- Continues to scan for new wireless threats even while preventing active threats, while the other systems did not
- Creates zero false alarms, unlike AirMagnet Enterprise which threw off as many false alarms as threats detected
- Locates wireless threats with a high degree of accuracy - within 4 meters in test scenarios, while the Aruba Mobility Controller did not converge on a location, and AirMagnet Enterprise was 12 to 40 meters off.

Evaluating WIPS

AirTight Networks, Inc. commissioned The Tolly Group to evaluate SpectraGuard Enterprise, a multi-faceted WIPS designed to protect enterprise network infrastructures from wireless attacks. In addition to its WIPS functionality, SpectraGuard Enterprise also provides visibility into the RF medium, such as the 802.11a/b/g networks tested, and simplifies monitoring and troubleshooting of WLANs.

The Tolly Group assessed the capability of SpectraGuard Enterprise to detect and block a range of wireless threats - from dealing with rogue APs, to detection and prevention of access point (AP) MAC address spoofing, to detection and prevention of Denial of Service (DoS) attacks, and several others described below.

Tolly Group engineers measured the effectiveness of SpectraGuard Enterprise against two other products: AirMagnet Inc.'s AirMagnet Enterprise and Aruba Networks Aruba Mobility Controller. Tests were conducted at AirTight Networks facilities in Mountain View, CA during December 2005 and were audited by Tolly Group personnel.

Tests show that SpectraGuard Enterprise detected all 24 of the threats launched against the networks and also blocked unauthorized traffic and prevented threats from inflicting network damage in all 24 scenarios. Competing devices were not nearly as effective, detecting about 30% fewer threats, and preventing only about half of the threats from operating in the network. (See Figure 1.)

Competitive Interaction

The AirMagnet and Aruba products discussed in this white paper were acquired through normal product distribution channels. All products were configured for the test by AirTight engineers and the configurations were verified by Tolly Group personnel.

The Tolly Group invited officials from AirMagnet and Aruba Networks to participate in the testing, as specified by The Tolly Group's Fair Testing Charter. Both companies declined the invitation in November 2005.

Rogue AP Detection and Prevention

In corporate LANs, rogue access points (APs) show up when employees deploy APs without the consent of the IT department.

Without the proper security configuration, users expose their company's network to the outside world. Ethernet jacks are ubiquitous, and it is a simple task to plug in an AP in order to provide wireless connectivity to anyone in the vicinity.

The Tolly Group verified the capability of the tested systems to detect rogue APs connected to the corporate wired network. To correctly identify APs as rogues, they must be both in violation of a company's security policy and connected to the corporate network on the local area network side. Violations can include incorrect SSIDs, lack of active encryption, etc.

Eight different rogue APs, each with varying active services and features, were connected to the wired corporate Ethernet LAN. (See Figure 2, below).

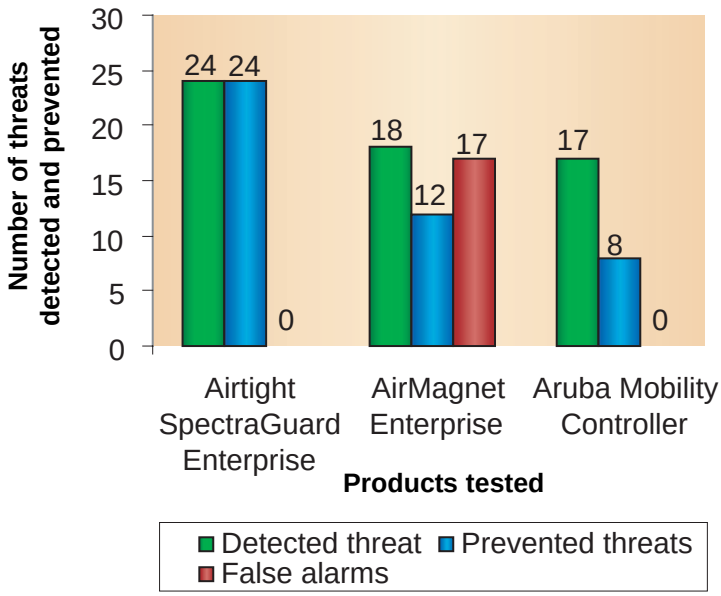
Tests show that AirTight Networks SpectraGuard Enterprise detected all eight rogue APs in less than one minute, and was the only WIPS that was able to identify the subnet to which the rogue AP was attached.

By contrast, AirMagnet Enterprise detected seven of the eight rogue APs but took much longer, even in a simple single switch network. The average detection time was about six minutes, but it ranged from 1 to 12 minutes. AirMagnet Enterprise failed to detect Rogue AP#7 within 15 minutes; that AP had non-adjacent MAC addresses and was WEP enabled.

The Aruba Mobility Controller detected four of the eight rogue APs in less than one minute, but failed to detect the other four.

Source: The Tolly Group, December 2005 *Figure 1*

Efficiency of Wireless Intrusion Prevention Systems at Detecting and Preventing Threats with Minimal False Alarms



Note: Tested devices were exposed to 24 threats.

An Ounce of Prevention

Detecting wireless threats, such as rogue APs, of course, is only half the battle. The other half is isolating these threats, e.g. rogue APs and stopping clients from communicating with them.

Generally speaking, when a WIPS detects a rogue AP, it automatically invokes a protection facility to interact with client devices and instruct them to cease communications with the rogue AP. In effect,

the WIPS attempts to interrupt the session state between the rogue AP and the clients.

Source: The Tolly Group, December 2005 *Figure 2*

Rogue AP Configurations Used in Testing

Rogue AP	Product	Characteristics
RogueAP1	Belkin 802.11g Wireless Print Server (F1UP0001)	Same VLAN, bridge, no encryption
RogueAP2	Belkin 802.11g Wireless Print Server (F1UP0001)	Same VLAN, bridge, WEP
RogueAP3	AirLink Multifunction 802.11 wireless router	Same VLAN, NAT, WEP, MAC adjacency
RogueAP4	Netgear WGR101	Same VLAN, NAT, no encryption, non-MAC adjacency
RogueAP5	Netgear WGR101	Different VLAN, WEP, NAT, MAC adjacency
RogueAP6	D-Link AirPlus G High speed pocket router DWL-G7	Different VLAN, bridge, WEP
RogueAP7	Buffalo AirStation Cable/DSL Router (WZR-G108)	Different VLAN, NAT, WEP, non-Mac adjacency
RogueAP8	Netgear WGT634U	Same VLAN, NAT, no encryption, non-Mac adjacency, DHCP off

The Tolly Group verified the ability of SpectraGuard Enterprise and the other products tested to prevent clients from accessing a corporate network via rogue APs.

Once a rogue is identified, a WIPS should be able to disconnect clients from the rogue AP. A WIPS also should be able to detect and prevent multiple simultaneous security breaches by stopping multiple clients from accessing multiple rogue APs. The Tolly Group also tested these scenarios.

Tests show that SpectraGuard Enterprise successfully detected each of the three different test scenarios (3 clients accessing 1 rogue AP, 3 clients accessing 2 rogue APs, and 4 clients accessing 4 rogue APs on 2 different channels) and subsequently blocked 68% to 87% of PING packets sent between the clients and the rogue APs. (See Figure 3, page 9.) This demonstrates that SpectraGuard Enterprise successfully was able to throttle back communications between the client devices and the rogue APs to the point where it was effectively stopped and thus "logically disconnected" from the rogue AP.

Over-the-air blocking or prevention is required to deal with ad-hoc connections, client mis-association, and other wireless threats. Wired-side blocking or prevention cannot address these threats.

By comparison, AirMagnet Enterprise only blocked from 21% to 41% of the PING packets and the Aruba Mobility Controller blocked from 32% to 42% of the PING packets - both in effect allowing the clients to communicate freely with the rogue APs, even though the systems claimed they were preventing this communication.

Test results underscore that AirTight's Rogue AP prevention performance consistently outperformed AirMagnet Enterprise and Aruba Mobility Controller for all the scenarios tested. Tests also show that only SpectraGuard Enterprise delivers the ability to detect consistently and prevent rogue AP sessions. The test criteria were set to require 65% blockage of any connection to be deemed "effective" prevention.

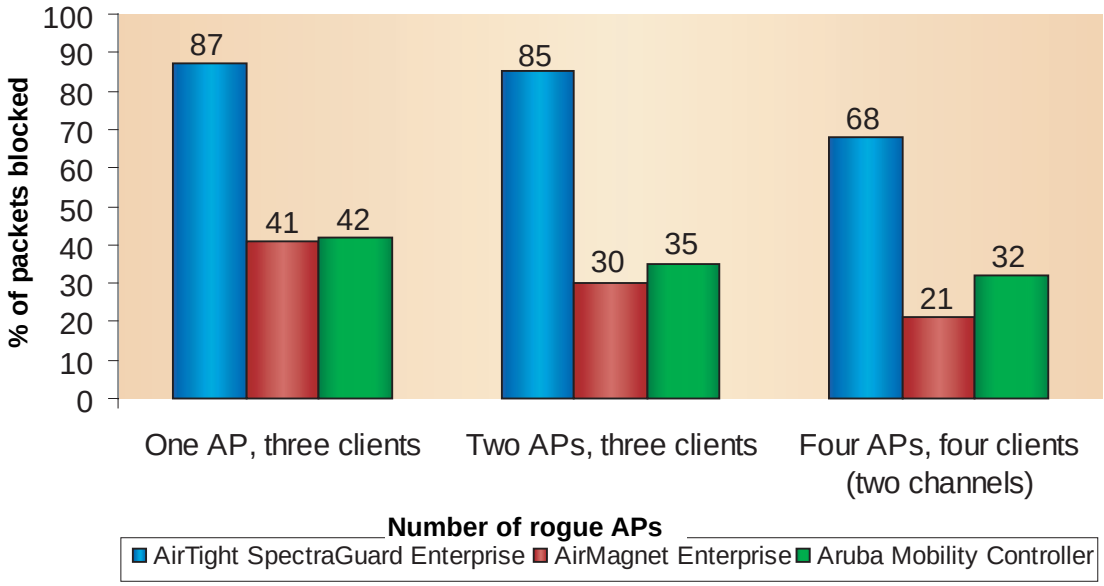
Client Mis-association

Because WLAN signals can travel through walls, it is possible for a corporate WLAN user to connect - or "associate" - deliberately or accidentally with an AP "outside" of the corporate network. (This can happen very easily if said AP is not protected by WEP or another method.) Corporate clients using these systems inadvertently can be exposing password and other company information to outside hackers as they communicate to Web resources over this "open" LAN.

Legitimate clients should be authorized automatically when they connect to a corporate LAN through a wireless connection. They then should be prevented from associating with an unsecured non-corporate AP, either accidentally or deliberately. The Tolly Group examined the capability of the DUTs to detect corporate clients sending traffic through external APs.

Source: The Tolly Group, December 2005 *Figure 3*

Multi-Threat Prevention: Average Percentage Reduction in 'PING' Traffic Sent Between Authorized Clients and Rogue APs



In the test, engineers first verified so-called "client auto-classification," where a new client attempts to join the wireless network and establish communications with an AP. The WIPS must auto-classify the device as an authorized or unauthorized user and take the appropriate action(s).

Auto-Classification

In the test scenario, engineers powered up CorporateAP1 and CorporateAP2, representing two authorized APs on the network. Next they powered up four unknown, uncategorized clients which attempted to join the wireless LAN and communciate with the APs. (These clients represented new employees or newly issued PCs.)

An 'unauthorized client' is a client that has not been authorized for activity on the corporate network. An unauthorized client may attempt to gain access to resources connected to the corporate LAN through the rogue AP. (In wireless jargon, this is called "associating" with the rogue AP.)

For the test, engineers used three Centrino-based, IEEE 802.11 b/g

Source: The Tolly Group, December 2005 *Figure 4*

Wireless Threat Detection and Classification				
	Test Scenarios	**AirTight SpectraGuard Enterprise**	**AirMagnet Enterprise**	**Aruba Mobility Controller**
Classification	**Rogue APs**			
	Rogue AP Auto-classification	YES	NO	YES
	External AP Auto-classification	YES	**NO***	**YES****
	WLAN client auto-classification	YES	NO	YES
Threat Detection	**Rogue APs**			
	Single Rogue AP detection (8 different APs)	8 out of 8	7 out of 8	4 out of 8
	Multiple threat detection (4 clients) - 1 rogue AP	YES	YES	NO
	Multiple threat detection (4 clients) - 2 rogue APs	YES	NO	YES
	Multiple threat detection (4 clients) - 4 rogue APs	YES	NO	YES
	Client misassociation	3 out of 3	2 out of 3	3 out of 3
	Adhoc networks	4 out of 4	4 out of 4	4 out of 4
	AP MAC address spoofing			
	Local AP MAC address spoofing	YES	YES	YES
	Remote AP MAC address spoofing	YES	NO	NO
	Honeypot attack	YES	YES	YES
	Misconfigured AP			
	Security misconfiguration	YES	YES	YES
	Network misconfiguration	YES	NO	NO
	DoS attack	YES	YES	YES
Total threat detection		**24 out of 24**	**18 out of 24**	**17 out of 24**

** AirMagnet classified three APs among all the external APs in the test networks as wired or rogue APs. AirMagnet's auto-classification support falls short of enterprise requirements because it does not automatically classify all of the rougue APs, external APs and clients.*
*** While the Aruba Mobility Controller did auto-classify the rogue APs it found, it missed 4 of the 8 rogues present.*

clients and one Cisco Systems IEEE 802.11 a/b/g client. (See Figures 4 and 5.)

AirTight's SpectraGuard Enterprise and Aruba Mobility Controller were able to properly auto-classify all of the clients. AirMagnet Enterprise did not classify clients automatically and required administrators to authorize clients manually.

Preventing Client Mis-association

Aruba was unable to block client mis-associations, allowing laptops to log onto external networks

In this portion of the test, engineers sought to determine the effectiveness of the WIPS at preventing clients from associating to an unsecure, non-corporate AP, either accidentally or deliberately.

For the misassociation portion of the test, engineers powered up an external AP representing a neighboring company's AP and then associated the three authorized Centrino 802.11 b/g clients with the unauthorized external AP. Engineers examined the DUTs to determine if they properly detected the misassociation. On the prevention side,

Source: The Tolly Group, December 2005 *Figure 5*

Wireless Threat Prevention			
Threat types	**AirTight SpectraGuard Enterprise**	**AirMagnet Enterprise**	**Aruba Mobility Controller**
Rogue APs			
Single Rogue AP (8 different Rogue APs)	8 out of 8	7 out of 8	4 out of 8
Multiple threat detection (4 clients) - 1 rogues AP	YES	NO	NO
Multiple threat detection (4 clients) - 2 rogue APs	YES	NO	NO
Multiple threat detection (4 clients) - 4 rogue APs	YES	NO	NO
Client misassociation	3 out of 3	2 out of 3	0 out of 3
Ad-hoc networks	4 out of 4	0 out of 4	2 out of 4
AP MAC address spoofing			
Local AP MAC address spoofing	YES	YES	NO
Remote AP MAC address spoofing	YES	NO	NO
Honeypot attack	YES	YES	YES
Misconfigured AP			
Security misconfiguration	YES	YES	YES
Network misconfiguration	YES	NO	NO
DoS attack	YES	NO	NO
Total threat prevention	**24 out of 24**	**12 out of 24**	**8 out of 24**

Note: Products "passed" a threat prevention test if they were able to block 65% or more of 'PING' test traffic between an authorized client and a rogue AP.

engineers examined the extent to which the DUTs enabled wireless blocking with the external AP and the resulting frame loss from PING traffic between the clients and the external AP or the neighboring AP.

AirTight's SpectraGuard Enterprise detected and prevented 3 of 3 Centrino (IEEE 802.11 b/g) clients that were simultaneously transmitting traffic through an unauthorized external AP. This demonstrates that SpectraGuard Enterprise can recognize multiple new clients attempting to gain access to the external AP. (See Figures 4 and 5.)

The Aruba Mobility Controller also detected 3 of 3 clients transmitting traffic to an unauthorized external AP. However, only SpectraGuard Enterprise blocked 100% of the traffic between the clients and the external AP. The Aruba Mobility Controller blocked only 26% of the PING packets - an indication that it allowed the vast majority of packets to flow between the clients and the external AP.

AirMagnet only detected 2 of 3 client mis-associations, allowing the third client to communicate freely with an external network, violating security policy.

The AirMagnet Enterprise only detected 2 out of 3 clients communicating with the external APs. While it did prevent traffic on the two clients it detected, it missed the third client entirely, allowing it to communicate freely with the external network. This means that AirMagnet Enterprise's failure to detect all the client mis-associations means that it cannot comprehensively prevent client mis-association.

Ad-hoc Networks

In wireless networks, sometimes clients attempt to form an ad-hoc network with other clients using their wireless capabilities, without going through any AP. WIPS should be able to detect and block the formation of such "ad-hoc" networks from forming, when they involve any authorized client.

For this test, engineers authorized one client PC and did not authorize a second PC. They created matching ad-hoc profiles in each PC and established ad-hoc networks between the PCs with PING traffic flowing between them. Engineers first examined whether the DUTs identified and classified the ad-hoc traffic as a threat. Then, they tested to see if the WIPS could prevent the ad-hoc traffic by instructing the authorized client to throttle back communications with the unauthorized client. This is typically called wireless blocking. The WIPS blocks the traffic to an unauthorized client(s) by preventing authorized clients from communicating with the unauthorized devices.

AirMagnet Enterprise was able to detect but not prevent instances of ad-hoc networking.

Engineers verified the blocking by measuring the amount of frame loss to and from the unauthorized client.

Each of the three products successfully detected four out of four unauthorized client attempts to form ad-hoc networks with legitimate clients. The AirTight system blocked an average of 92% of the traffic from the four different ad hoc networks; however, the AirMagnet and Aruba did not block this traffic effectively by recording 0% and 53% of prevention rate respectively. The test results show that AirMagnet has virtually no control over the ad hoc networks.

AP MAC Spoofing

All WLAN AP equipment is shipped from the factory with MAC address(es) installed for its wireless interface.

Standard tools can allow a hacker to "spoof" these MAC addresses to mask himself/herself as an authorized AP thereby getting clients to associate to him - enabling him to eavesdrop on their credentials and information. This is the first step in creating a "man-in-the-middle" attack or an "evil twin" attack.

For this test scenario, an external AP copied the corporate AP's MAC address and SSID in order to appear identical. Clients will normally associate with the AP with the stronger signal. Clients may associate initially to the spoofing AP, or even transfer the connection in the middle of a transaction because of a stronger signal.

Only AirTight SpectraGuard Enterprise was able to detect (and prevent) a remote AP MAC spoofing attack.

Engineers first examined the ability of the DUTs to detect and prevent local AP MAC spoofing - that is, when the unauthorized AP resides in the same physical vicinity as the AP it is spoofing - such that it can be "seen" by the same WIPS sensor.

For the Local MAC spoofing test, engineers used a Soekris AP as the corporate AP and a Cisco AP as the spoofing AP. Engineers configured the Soekris AP to have the same MAC address as the Cisco AP and placed these APs close enough to be visiable to the same sensor. Engineers examined whether the DUT identified that two devices used the same MAC address and prevented traffic from an authorized client to pass to the spoofing AP.

All three products successfully detected and blocked the unauthorized AP spoofing a local AP. (See Figures 4 and 5.) However, SpectraGuard Enterprise was more effective at blocking traffic, stopping 97% of the PING traffic to the spoofing AP versus just 87% for AirMagnet and 26% for Aruba products.

For the remote spoofing test, engineers set up the test bed such that one sensor saw only the corporate AP and another sensor saw only the spoofing AP.

When engineers tested remote spoofing - where an unauthorized AP spoofs the MAC address of an AP in another physical location (not visible to the same WIPS sensor), only AirTight's SpectraGuard Enterprise detected and prevented the security incursion.

Honeypot Attacks

One serious lower-layer attack that exploits client weaknesses is the honeypot AP. In the wireless realm, a "honeypot" is an attacker's AP that is set up in close proximity to an enterprise, advertising the SSID of an enterprise AP. The goal of such an attack is to lure authorized clients to associate with the honeypot AP. From that point, a security attack can be mounted, or an attempt can be made to learn the client's authentication credentials. Most client devices have no way of distinguishing between a valid AP and an invalid one - the devices only look for a particular SSID and will associate to the nearest AP advertising that SSID.

In a honeypot AP, the duplicate SSID can be a deliberate deception or the result of poor configuration, as when neighbor networks have been setup with default SSIDs from the same vendor.

Engineers configured CorporateAP2 (as a legitimate AP) and configured another AP as the honeypot by giving it an SSID matching CorporateAP2. Engineers then verified that the DUTs recognized that the honeypot AP utilized a different MAC address, and then consequently verified that the DUTs' prevention policies blocked traffic with the honeypot by witnessing the frame loss of PING traffic between clients and the honeypot AP - such frame loss amounts to wireless blocking, since clients are blocked from communicating with the honeypot AP.

Tests show that all three products successfully detected and prevented honeypot attacks. (See Figures 4 and 5.)

Only AirTight's SpectraGuard Enterprise was found to enforce different WiFi security policies on different VLANs. This enables an enterprise to set different WLAN policies for various functions, different parts of a building, or even multiple sites. Neither of the competitors tested support this.

Misconfigured APs

There are several scenarios where corporate APs may be accidentally misconfigured or mislocated (attached to the wrong subnet). WIPS systems should enforce the company's security policy, alert the network administrator to such events, and prevent authorized clients from con-

necting to a corporate AP that has been misconfigured.

Tests show that all three products were able to detect and prevent a security misconfiguration where encryption on a corporate AP was "inadvertently" turned off. However, only AirTight's SpectraGuard Enterprise was able to detect and stop a network misconfiguration where "Corporate AP1" was placed in VLAN2, which was a violation of the corporate security policy. (See Figures 4 and 5.) This might represent a scenario where an enterprise creates a special VLAN for guest access - and allows APs to be installed on this VLAN, but at the same time prohibits APs on the other VLANs in the building.

One point to consider: AirTight's policies are subnet-specific, while AirMagnet's policies are site-specific - meaning users have more granular control with AirTight's SpectraGuard Enterprise.

Denial-of-Service Attacks

Wireless Denial-of-Service (DoS) attacks attempt to broadly disrupt network wireless connections by sending broadcast "de-authenticate" commands over the air. A broadcast deauthentication will force clients to disconnect from the AP. As wireless Voice over IP becomes more widespread, the threat of this type of disruption becomes more critical.

Only AirTight's SpectraGuard Enterprise was able to stop a wireless DoS attack.

Tests show that all three products tested successfully detected DoS attacks, but only AirTight's SpectraGuard Enterprise blocked the DoS attacks and restore the WLAN connectivity to 65% of its original throughput.

AirMagnet and Aruba do not support this feature and they let the DoS attacks stop 100% of the WLAN test traffic. (See Figures 4 and 5.)

Location Tracking

It is of significant benefit for a WIPS to not just detect a rogue AP or other disturbance, but to pinpoint with accuracy the location of the device so network personnel can unplug it. Such a capability is called location tracking and almost every WIPS claims to offer it to some degree.

Three of the four APs tested were located at the same location, but operated at different power levels.

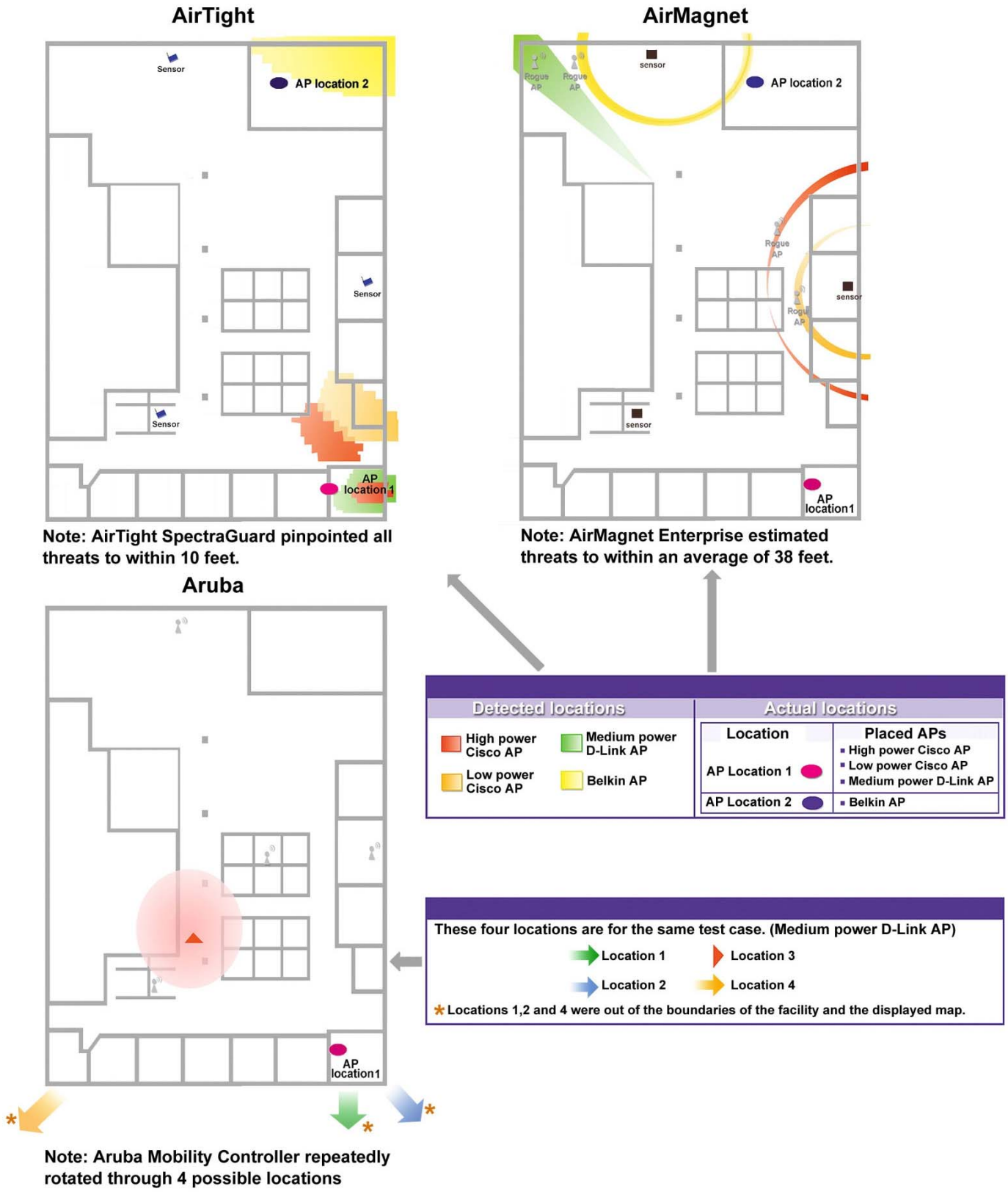
The widely varying predictions of AirMagnet Enterprise and Aruba Mobility Controller on the location of these APs shows inconsistency in their location algorithms.

Engineers measured the accuracy of the location tracking feature of the DUTs in different test scenarios; varying the AP location and transmit power levels. Test results show that AirTight SpectraGuard Enterprise located the APs with a high degree of accuracy, but neither AirMagnet Enterprise nor Aruba Mobility Controller located the APs with much precision.

For every rogue AP tested, AirTight's SpectraGuard Enterprise pinpointed the rogue to within 10 feet. By contrast, AirMagnet Enterprise tracked the rogue location to within an average of 37.5 feet, and Aruba Mobility Controller did not even converge on a single location. Aruba's

Source: The Tolly Group, December 2005 *Figure 6*

Location Tracking Predictions



system kept changing the predicted location of the rogue device - rotating through four possible locations, but never settling on a single prediction.

From a visual rendering of what the products show onscreen via a management interface, AirTight SpectraGuard Enterprise rendered colored shapes to denote the suspected location of rogue APs. (See Figure 6, next page.)

The AirMagnet Enterprise just rendered broad circles around its deployed sensors and the Aruba Mobility Controller never converged by showing a different location in each screen refresh even though nothing in the test bed had moved.

Management Reporting

Many IT organizations must contend with regular compliance reporting requirements imposed by government regulations such as Sarbanes-Oxley, HIPAA, or Gramm-Leach-Bliley.

Pre-defined reports simplify this task. Effective products deliver interactive drill-down features, as well as customizable reporting and flexible delivery frequency.

The Tolly Group examined the three WIPS products tested to determine their support for pre-formatted compliance reports and other report capabilities. (See Figure 7.)

WIPS products also must offer a polished set of troubleshooting capabilities to guide users through trouble spots.

Three of the most common capabilities are remote wireless packet capture, a knowledgebase for root cause analysis and radio frequency (RF) diagnostics that provide RF heat maps to identify trends and issues for radio coverage.

The Tolly Group examined the products tested for their support of these common troubleshooting capabilities. (See Figure 8.)

Regarding support for heat maps, users

Source: The Tolly Group, December 2005 *Figure 7*

Standard Reports Offered and Features of WIPS Products Tested

Types of reports	AirTight SpectraGuard Enterprise	AirMagnet Enterprise	Aruba Mobility Controller
Pre-formatted compliance reports			
SOX (Sarbanes-Oxley Act)	✓	✓	✗
GLBA (Gramm-Leach-Bliley Act)	✓	✓	✗
HIPAA (Healthcare Insurance Portability and Accountability Act)	✓	✓	✗
DoD (Department of Defense)	✓	✓	✗
Other pre-formatted reports			
Device listing	✓	✓	✓
Events listing	✓	✓	✓
Custom reports			
Customizable sections	✓	✓	✗
Customizable database queries	✓	✗	✗

often utilize these to examine the RF coverage of APs deployed in the network, and to spot potential blind spots in coverage that represent potential locations for rogue APs. Appendix A on page 19 contains sample heat maps from AirTight and Aruba; AirMagnet does not offer them.

Summary

As indicated in the beginning of this white paper, every wireless intrusion prevention system must deliver three basic sets of functionality:

- Detecting and automatically classifying wireless threats;
- Preventing multiple simultaneous wireless threats while continuing to scan for new threats
- Accurately locating wireless threats on a floor map.

AirTight Networks' SpectraGuard Enterprise WIPS was the only WIPS tested that delivered on all three counts. SpectraGuard Enterprise clearly outperformed both the AirMagnet Enterprise and the Aruba Mobility Controller on all the measured criteria.

The Tolly Group's hands-on evaluation of the three WIPS offerings also shows that SpectraGuard Enterprise includes incremental capabilities that make it a more versatile approach to wireless security than other products that offer just the basics.

SpectraGuard Enterprise's management reporting, WLAN troubleshooting and RF display/visualization capabilities provide a depth of functionality that is unmatched by the other products tested.

Any network operator considering the purchase of a WIPS should evaluate these advanced services, in addition to marching through the checklist of wireless security threats and how the prospective products are designed to detect and deal with those issues.

In the case of SpectraGuard Enterprise, prospective buyers will find a WIPS that goes well beyond the basics of identifying security threats, to offer a rich set of security capabilities and management tools to help secure wireless deployments in enterprise networks.

Source: The Tolly Group, December 2005 *Figure 8*

Troubleshooting Features of WIPS Products Tested

Types of features	AirTight SpectraGuard Enterprise	AirMagnet Enterprise	Aruba Mobility Controller
Remote wireless packet capture	●	●	●
Knowledgebase for root cause analysis	●	○	○
RF diagnostics using visual RF heat maps	●	○	◐

Key:

● = Feature is supported.

○ = Feature is not supported.

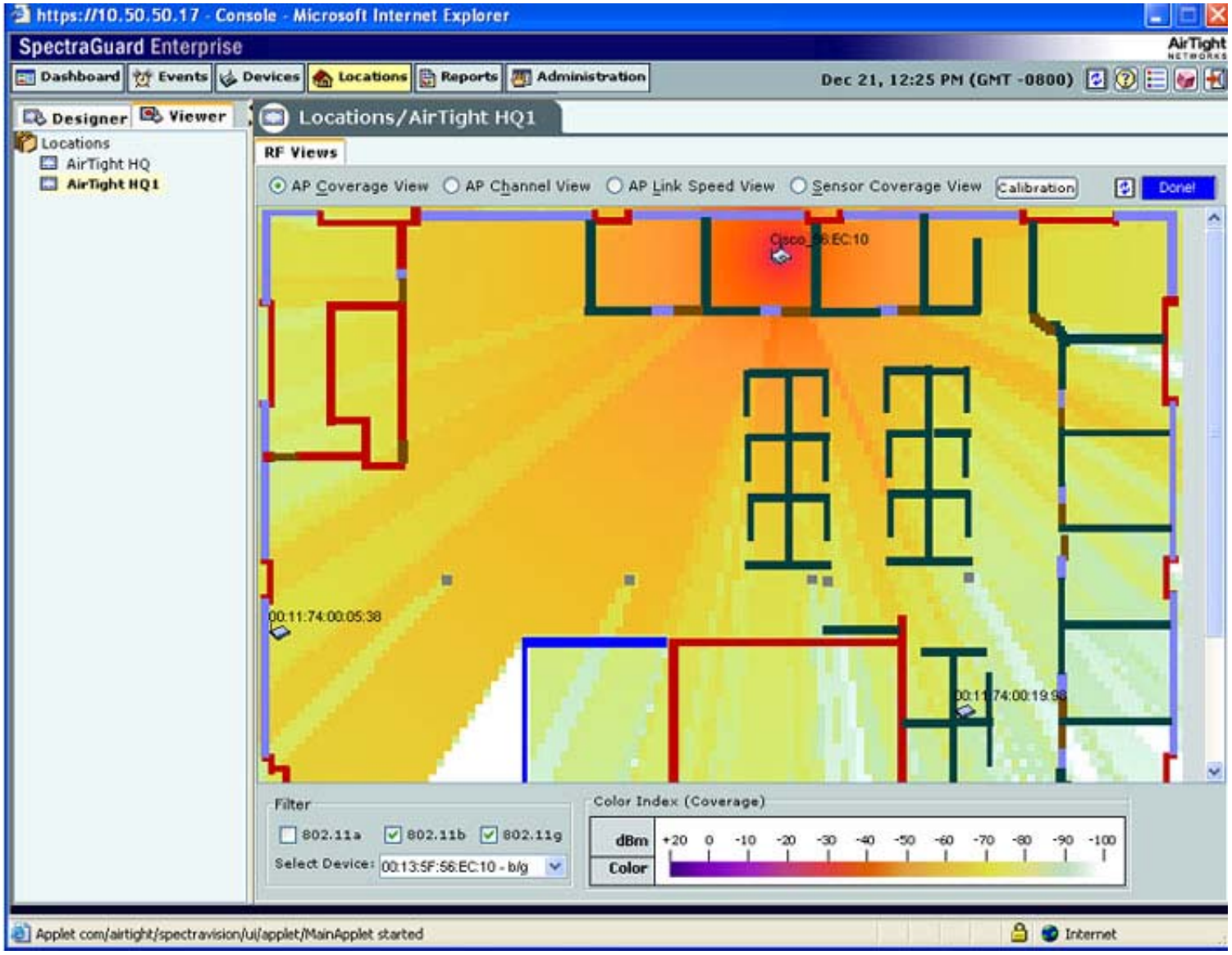
◐ = Feature is partially supported.

Appendix A. Heat Map Samples

Heat maps are an administrative tool to help network managers determine holes in radio coverage based on the position of access points. There is no heat map offered in this Appendix for AirMagnet because the company does not offer that capability.

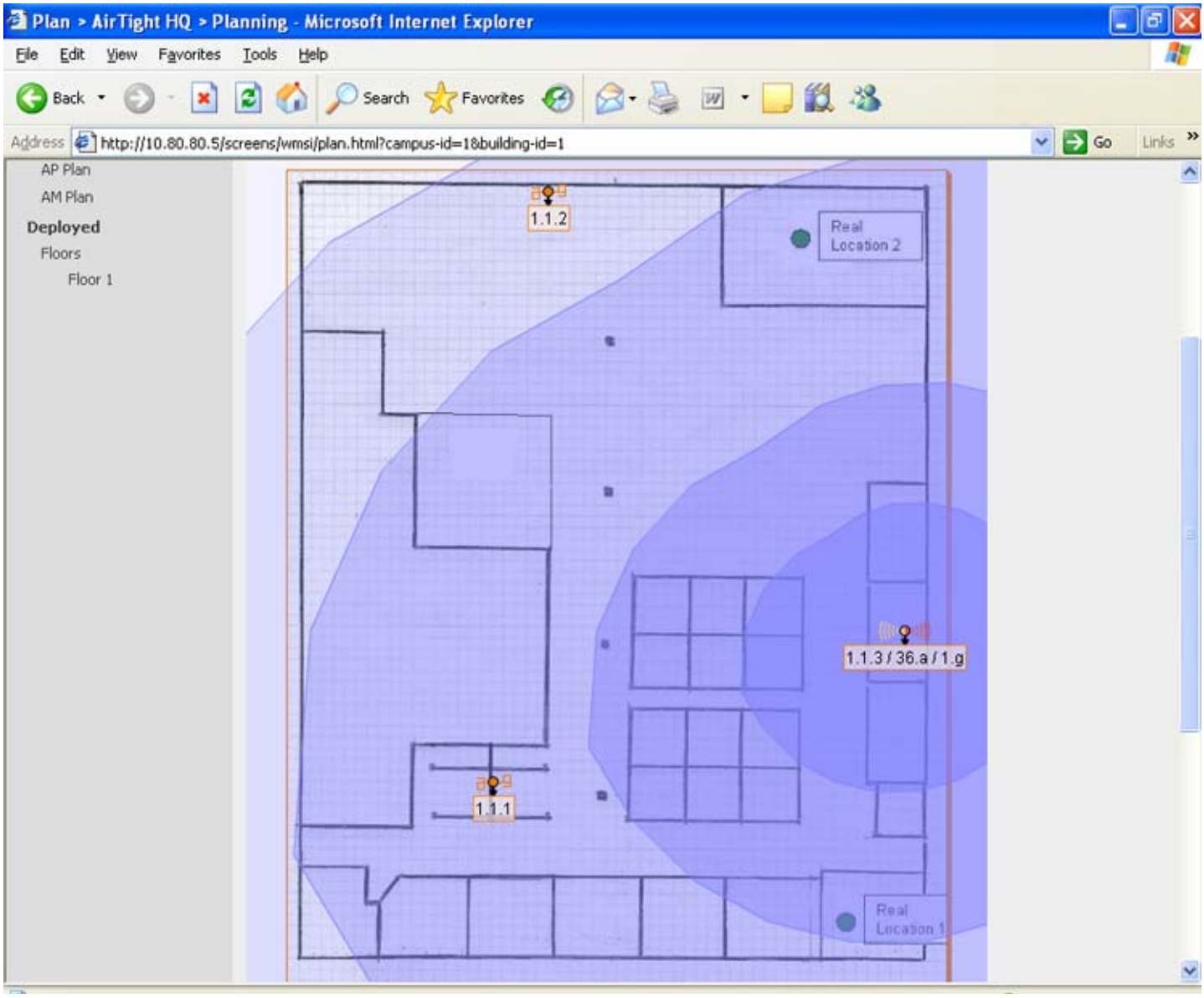
AirTight Heat Map

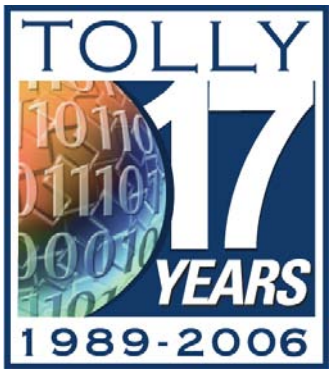
Source: The Tolly Group, December 2005 *Figure 9*



Aruba Heat Map

Source: The Tolly Group, December 2005 *Figure 10*





THE TOLLY GROUP

The Tolly Group, Inc.
3701 FAU Blvd. Suite 100
Boca Raton, FL 33431
Phone: 561.391.5610
Fax: 561.391.5810
http://www.tolly.com
info@tolly.com