



## Smart Forensics™ Wireless Forensics at Your Fingertips

Network administrators and incident handlers are faced with the complexity of managing and responding to the growing number of wireless LAN (WLAN) hacking incidents, unauthorized devices and misbehaving end-users. Wireless forensics — the ability to collect and analyze wireless data traffic to decipher what, when and how an incident happened — holds the key to be able to respond swiftly to a security breach or wireless vulnerability.

AirTight Networks' SpectraGuard Enterprise Wireless Intrusion Prevention System (WIPS) provides network administrators with Smart Forensics™ that enables them to drill down into a security incident in just two clicks. Unlike traditional forensics, which often provide raw, unfiltered data for security administrators with wireless expertise to decipher and identify the relevant information, AirTight's Smart Forensics is about doing more with less; powered with AirTight's Active Auto-classification and Live Event architecture, it filters out useless data and presents only relevant and accurate forensics information in an easy to understand and ready-to-use format. Security administrators can make better decisions, faster.

### Key Features

- Two-click forensic drill down
- Configurable forensics time window
- Accurate threat detection and analysis
- Date, time, and duration of incident
- Sequence of events and connectivity logs
- Identification and properties of devices involved
- Physical location tracking of devices: current (if active) and historical (at the time of incident)
- Audit trail of actions taken by the system (e.g., intrusion prevention)
- Audit trail of actions taken by the administrator (e.g., manual quarantine, acknowledgement)

### Key Benefits

- Faster, more accurate analysis
- Faster problem resolution
- Better network security
- No information overload
- No raw data interpretation
- Less wireless expertise required

Forensic audit trail

**Forensic Details**  
Rogue AP is unauthorized AP connected to the enterprise network. Outsiders can access the enterprise network through Rogue AP.

ID	Location	Event Details	Category	Date
69706	Mountain View...	Rogue AP [Netgear_7A:13:CD] is...	Rogue AP	Nov 2, 4:22:00 PM
69709	Mountain View/Ai...	Rogue AP [06:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 4:22:00 PM
69715	Mountain View/Ai...	Rogue AP [0A:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 4:47:00 PM
69711	Mountain View/Ai...	Rogue AP [0A:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 4:35:00 PM
69705	Mountain View/Ai...	Rogue AP [06:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 4:08:00 PM
69704	Mountain View/Ai...	Rogue AP [06:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 4:00:00 PM
69703	Mountain View/Ai...	Rogue AP [06:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 3:41:00 PM
69701	Mountain View/Ai...	Rogue AP [06:06:3C:A3:9F:A8] is a...	Rogue AP	Nov 2, 3:05:00 PM

Event Start Time: Nov 2, 4:21:41 PM    Event End Time: Nov 3, 5:44:04 PM

AP	Client	Association Start Time	Association End Time	Locate
Netgear_7A:13:CD	**	**	**	Locate
Netgear_7A:13:CD	Intel_12:9C:E2	Nov 2, 4:22:00 PM	Nov 2, 4:34:00 PM	Locate
Netgear_7A:13:CD	Intel_12:9C:E2	Nov 2, 5:05:25 PM	Nov 2, 5:34:54 PM	Locate
Netgear_7A:13:CD	Intel_12:9C:E2	Nov 2, 5:37:59 PM	Nov 2, 6:04:08 PM	Locate
Netgear_7A:13:CD	Intel_12:9C:E2	Nov 2, 6:05:03 PM	Nov 2, 6:22:41 PM	Locate
Netgear_7A:13:CD	Intel_12:9C:E2	Nov 3, 9:32:39 AM	Nov 3, 9:43:04 AM	Locate
Netgear_7A:13:CD	Liteon_9F:AC:17	Nov 3, 1:39:50 PM	Nov 3, 1:42:09 PM	Locate

Device details and threat analysis

Current and historical location tracking

## About

### AirTight Networks

AirTight Networks is the global leader in wireless security and compliance products and services, providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers industry's leading wireless intrusion prevention system (WIPS) and the world's only SaaS based wireless security, compliance and Wi-Fi access branded as AirTight Cloud Services™. AirTight's award-winning solutions are used by customers globally in the financial, government, retail and hospitality, manufacturing, transportation, education, health care, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 24 U.S. and international (Australia, Japan and UK) patents granted, and more than 20 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit: [www.airtightnetworks.com](http://www.airtightnetworks.com).

*AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. AirTight Networks, AirTight Networks logo, AirTight Cloud Services and AirTight Secure Wi-Fi are trademarks. All other trademarks are the property of their respective owners.*

## FAQ

Is it necessary to store packet traces and maintain packet level statistics for wireless forensics?

A wireless sensor typically scans across the Wi-Fi channels in 2.4 GHz and 5 GHz spending few milliseconds on a given channel. As a result, the sensor is able to capture only a small subset of packets (typically 10% or less) on any given channel. Maintaining packet level statistics based on partial data capture is error-prone and it can lead to the wrong analysis. AirTight's Smart Forensics limits your analysis to only those devices that are genuine threats to your network.

Is packet-level analysis a must in wireless forensics?

The conventional network forensic approach of data capture, rewind, and replay is simply not effective in a wireless network. Because most wireless intrusion detection and prevention systems (WIDS/WIPS) cannot accurately determine which devices are connected to your network, they capture and store as much data as possible so not to miss the real details. Unfortunately, the captured data is often incomplete or irrelevant, making data analysis difficult if not impossible. AirTight's patented auto-classification techniques accurately classify authorized, unauthorized and neighboring Wi-Fi devices, allowing Smart Forensics to summarize all relevant information without the need for cumbersome packet-level analysis.

Is it necessary to store information about all wireless devices?

Wireless is a shared medium and a wireless sensor scanning the airspace will capture packets from neighboring Wi-Fi networks that have nothing to do with your forensics analysis. Storing large packet traces only makes analysis more difficult to sort out the relevant data from the irrelevant. Furthermore, capturing and maintaining incomplete or irrelevant information from hundreds or thousands of wireless devices will negatively impact the scale and performance of the WIPS. By storing only relevant forensic data, AirTight's SpectraGuard outperforms and outpaces competitive WIPS solutions while providing faster, more efficient forensic analysis.

## The Global Leader in Wireless Security Solutions

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043  
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 [www.airtightnetworks.com](http://www.airtightnetworks.com) [info@airtightnetworks.com](mailto:info@airtightnetworks.com)

© 2011 AirTight Networks, Inc. All rights reserved. AirTight Networks and the AirTight Networks logo are trademarks, and AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. All other trademarks mentioned herein are properties of their respective owners. Specifications are subject to change without notice.

