



AirStorm Wireless IDS

Cloud based Wireless LAN Intrusion Detection System

Protect your Wireless Networks

Wireless networks are fantastic for enabling mobility within an organisation. However, they also bring with them inherent security risks as seen in many high profile security breaches.

AirStorm from **RandomStorm** is a Wireless Intrusion Detection System that uses the latest technology and software to identify and alert upon the common risks to Wireless LANs.

AirStorm can be quickly and simply installed into an existing network to provide reports of Wireless activity.

AirStorm can be integrated into the **iStorm** Vulnerability Management Platform (VMP) or the **xStorm** cloud based VMP.

AirStorm helps organisation's achieve compliance with standards such as the Payment Card Industry (PCI) Data Security Standard (DSS).

AirStorm provides the following Wireless Security Technologies as part of its Intrusion Detection capabilities:

- Rogue Access Point Detection
- Non-Compliant Access Point Detection
- Rogue Client Detection
- Wandering Client Detection

About RandomStorm

RandomStorm is the leading Software as a Service (SaaS) provider of proactive security management solutions. Designed for all types of business our simple to use online service and embedded security appliances enable organisations to maintain a high level security posture in line with corporate risk and policy compliance without the need for major infrastructure investment or specialist skills.

Wireless Hardware Inventory

The **AirStorm** solution provides wireless hardware inventory for both Access Point and Wireless Clients.

Detecting rogue APs and rogue clients is dependent upon an accurate wireless hardware inventory that identifies all of the trusted wireless networks for all locations under the organisations control.

AirStorm records hardware information for all trusted networks, trusted Access Points and trusted wireless clients.

Any exceptions to these trusted Access Points are considered rogue, as are any exceptions to these trusted wireless clients.



The hardware inventory also contains connection information that can record when every wireless client connects to the network. This, along with the wireless security logging is in line with compliance requirements such as the PCI DSS.

The combination of the wireless hardware inventory and the wireless intrusion detection technologies provide the framework for implementing a secure wireless network.

Rogue Access Point Detection

A rogue Access Point (AP) is any device that adds an unauthorised Wireless LAN (WLAN) to the organisation's network. A rogue AP is identified as having the same network name (SSID) as the organisation or a different network name with weak or no encryption. Rogue APs can be maliciously placed on the trusted network in order to lure trusted clients to connect or they can be connected by an uneducated employee.

AirStorm alerts via the centralised alerting console when a rogue AP is detected ensuring that the organisation can react against this access point in order to remove the rogue AP from the network. Sophisticated filtering technology prevents false positives to ensure that only real threats are identified and alerted on.

Non-Compliant Access Point Detection

A non-compliant AP is an access point that is configured and allowed on your WLAN that does not meet the minimum security requirements for strong encryption.

AirStorm alerts via the centralised alerting console when a non-compliant AP is detected. This allows the organisation to remedy the configuration on the trusted AP mitigating the risks associated with misconfiguration of an AP.

Rogue Client Detection

A rogue client is an untrusted client that connects to the organisation's trusted WLAN. This could be a malicious user who has obtained the credentials necessary to access the trusted WLAN or a trusted user accessing the WLAN with untrusted hardware such as an Apple iPhone or other WiFi enabled smartphone.

AirStorm alerts via the centralised alerting console when a rogue client is detected. This allows the organisation to ensure that only trusted clients are connected to the organisation's WLAN.

Wandering Client Detection

A wandering client is a trusted client that connects to an untrusted WLAN. Wandering clients are frequently seen when an organisation enforces strict access control to the Internet and the organisation is in the vicinity of a free public AP. The detection of wandering clients is essential to ensure that trusted clients are not bridging the organisation's network with an untrusted network.

AirStorm alerts via the centralised alerting console when a wandering client is detected. Action can then be taken to ensure the wandering client is removed from the untrusted network and user training can prevent a reoccurrence.

AirStorm Placement

AirStorm consists of Wireless LAN Analysers that passively monitor the wireless network traffic. These AirStorm Analysers are positioned throughout your network so that they can cover the wireless reach of your client computers.

The AirStorm Analysers communicate over a secure channel either internally to an iStorm VMP or externally to the hosted xStorm service on the Internet. This model provides total scalability and a cost effective model for both central site and remote branch office installations. The remote solution is an ideal fit for remote sites with a compliance requirement such as retail outlets.

Free Trial

The free trial will consist of a single AirStorm Analyser that can be configured within an organisations network to communicate securely to a trial xStorm account.

RandomStorm Ltd

4 Cromwell Office Park

York Road

Wetherby

Tel: 0845 643 0995

sales@randomstorm.com

www.randomstorm.com

