

Extreme AirDefense

Highlights

- 24x7x365WLAN network monitoring for protection against wireless attacks
- Industry leading threat detection library
- Centralized aggregation and correlation of sensor data; minimizing false positives
- Centralized management in large deployments requiring multiple appliances
- Real-time detection of rogue devices with Automatic rogue termination for rapid response to attacks, protecting your network until the device can be physically removed
- Locate rogue devices on a floorplan
- Policy enforcement with instant notification and response based on policy violations
- Advanced forensics providing increased visibility to forensic investigations, including location forensics; determine where the device has been
- Anomalous behavior detection monitors wireless traffic to serve as an early warning indicator
- Built-in reporting for compliance monitoring (e.g. PCI_DSS, SOX, GLBA etc.) or create custom reports with Report-Builder
- Liveview provides 25+ summary graphical visualizations, packet capture and decode for analysis of the live network and real-time traffic
- Spectrum Analysis to monitor and troubleshoot even elusive, intermittent interference sources
- Wireless Vulnerability Assessment to remotely test for vulnerabilities from the perspective of a wireless hacker
- Bluetooth monitoring to detect presence of unexpected BT 2.0 devices to identify potential phishing attacks based on BLE 4.0 tags
- Enhanced detection of devices using EAP-TLS security using Secure Authentication of Equals (SAE).
- Detection of devices using Opportunistic Wireless Encryption (OWE)



A Comprehensive Wireless Intrusion Prevention System

Wireless connectivity provides unique opportunities to communicate in new and powerful ways, but it also brings its own set of vulnerabilities, complexities and management challenges. To get the best out of your wireless network without risking security of your users and business, you need the right set of tools.

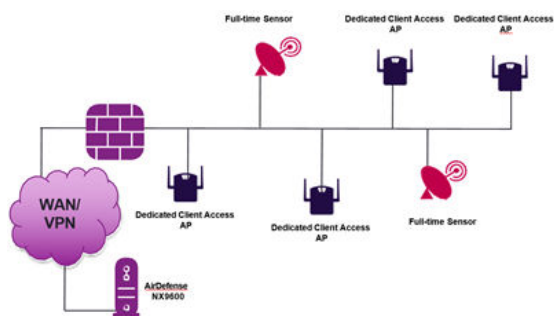
Extreme AirDefense® simplifies the protection, monitoring and compliance of your Wireless LAN networks. Extreme AirDefense continuously safeguards the network from external threats 24x7x365 and notifies IT staff when attacks occur, enabling an immediate response. It also enables compliance with regulations such as PCI-DSS, Sarbanes-Oxley, HIPAA, and GLBA.

Flexible

The Extreme AirDefense system is deployed as a set of access points serving as sensors to monitor the airwaves together with a security appliance. The appliance can be deployed either as a hardware appliance or a virtual appliance. Sensors can be deployed as either dedicated sensors or in radio-share mode. Dedicated sensors offer higher security through increased visibility. There are two deployment options for dedicated sensing (1) the entire access point can be dedicated as a sensor or (2) In a dual radio or tri-radio access point, one radio of the access point can be dedicated as a sensor, with the remaining radios serving user data traffic. In radio-share mode, the access point allocates a time slice for sensing function while utilizing the remaining time for serving data traffic. Extreme access points operating as sensors support 802.11a/b/g/n/ac/ax standards to scan both the 2.4GHz and 5GHz bands and are capable of listening to multiple MIMO streams.

Highly Scalable Architecture

With the explosion of end-user devices and the exponential increase in number of IoT devices, it is critical that wireless security systems keep up with this massive growth in the number of devices on the airwaves. The Extreme AirDefense appliance has a highly scalable architecture that scales across multiple cores in a multi-core server and multiple servers, while providing a single graphical console to manage the entire system. Packet analysis is divided between the sensors and the appliance forwarding only essential security information to the appliance to minimize the bandwidth requirements for the sensor-to-appliance communication. The appliance performs extensive traffic and event co-relation spanning across multiple sensors resulting in an accurate, efficient and secure monitoring system that can scale across thousands of sensors and hundreds of thousands of client devices.



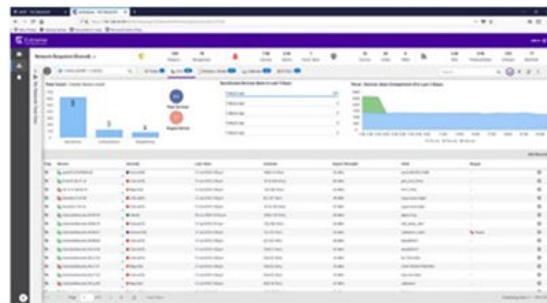
Plug and Play Operation

AirDefense was designed for ease of use with true plug- and-play operation: traffic can be monitored within minutes of installation, complete with the tools to quickly interpret information for fast response to Wireless LAN threats.

Wireless Intrusion Prevention

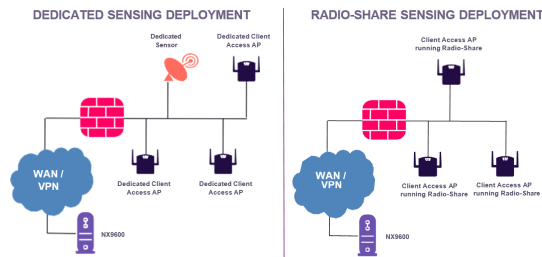
Maximizing the productivity of your wireless assets means maintaining the strongest security posture possible. AirDefense security and compliance functions work seamlessly across your wireless network to detect and neutralize rogue devices, enforce policies, prevent intrusion and ensure regulatory compliance. Automated tools for threat mitigation and policy enforcement give you the confidence of real-time response to risks and the peace of mind of having an effective security posture.

By analyzing existing and day-zero threats in real-time against historical data, the AirDefense Wireless IPS module can accurately detect wireless vulnerabilities and unusual network activity. Context-aware detection, correlation and multidimensional detection engines mean minimal false positive alarms. An extensive threat library and customizable policy settings enable the system to respond automatically to wireless security threats, minimizing security risk to your network.



Rogue Detection and Mitigation

AirDefense supports both dedicated and radio-share sensing modes of operation. In the former, additional access points act as dedicated sensors to perform 24 x 7 scanning. In the radio-share mode, the access point primarily serves data and periodically goes off channel to monitor threats in other channels. In this mode, the access point also performs sensing while serving data on the infrastructure channel. Dedicated sensing offers better visibility of the airwaves. Using sensed data and extensive correlation, the system identifies true rogues that are connected to the wired network, separating them from neighboring access points and minimizing false positives. Once a rogue is identified, the system can employ various techniques to perform rogue containment including air-termination, locating and disabling the port on the access Ethernet switch to which the rogue is connected or using an ACL for the same. AirDefense also supports the termination of rogue clients operating in PMF environment.



Security Policy Management

AirDefense allows the administrator to define security policies that need to be enforced in the network. When the system detects a policy violation, an alarm is generated. The system features an alarm action manager that can be configured to trigger specified actions based on the alarm including sending an email to an administrator, generating a syslog or snmp trap, initiating an automatic remote packet capture, launching spectrum analysis etc.

Locating Rogues

AirDefense sensors can locate rogue access points and clients and indicate their location on a floor plan. This assists IT staff in finding and disconnecting them.

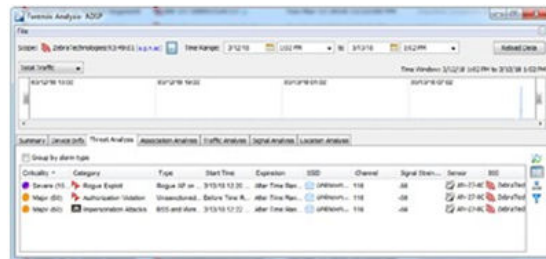
Reporting and Compliance

AirDefense has extensive reporting capabilities in the areas of network security and policy compliance. AirDefense has several built-in reports in the areas of security, infrastructure, inventory, compliance etc. Additionally, it also has a report builder that allows the administrator to create custom reports by choosing fields available in the AirDefense database. The custom report can then be used in the future like a pre-defined report.

This module requires the WIP License.

Advanced Forensics

Forensics is a key aspect of security. In the event of an audit, IT staff need the ability to analyze and extract data of network activity during a time interval of interest which occurred in the past. Items of interest may include identifying which clients connected to a specific access point, communications to a specific destination, amount of data traffic exchanged between devices of interest, time-of-day when those exchanges happened etc. Such analysis assists organizations determine a window of exposure to a target attack and provide factual data to support an audit. The Advanced Forensics Module gives administrators the ability to continuously monitor the wireless environment and provides the data and analysis tools they need to support forensic investigation and network performance troubleshooting.



Capture the Evidence You Need

With Advanced Forensics, administrators can focus on the activity of a suspect device over a period of months and even drill down to review minute-by-minute details of wireless activity. Every minute, the system stores 300+ data points for each identified wireless device, providing extensive data for analysis at a later time. The high level of granular information available for analysis marks the difference between a forensics capability that allows an administrator to detect and resolve a pattern of attack occurring over an extended period versus responding to repeated attacks from the same source as separate and isolated incidents. Such a powerful forensic function enhances your business operation by supporting more efficient network management, improving compliance and overall security posture.

Simplify Your Compliance

The AirDefense Advanced Forensics module maintains the highly accurate historical data required by many regulations such as HIPAA, GLBA, Sarbanes-Oxley (SOX), Payment Card Industry (PCI) data security standards such as VISA CISP and the Department of Defense. So your organization's compliance — and proof of compliance — becomes automatic and routine.

Capabilities include:

- Historical Association Analysis
- Historical Traffic Analysis
- Historical Channel Analysis
- Historical Location Tracking and Roam Trajectories

A Tool for Troubleshooting

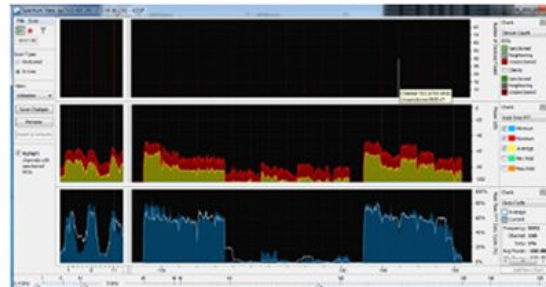
Wireless communication is designed for mobility. Unfortunately, the very feature that makes it so attractive also makes it incredibly challenging to troubleshoot. Users come and go, devices join and leave, interference sources are here one minute and gone the next. Keeping track of the myriad factors impacting network connectivity, utilization and availability is a challenging task. The historical data that kept by the forensics module provides a tool for troubleshooting incidents reported in the past that may not even be active any longer. The system gathers 300+ data points per minute for each identified wireless device including channel activity, signal characteristics, device activity, and traffic flow. This dynamic database can be used to chart network usage trends, identify anomalies and support capacity planning.

Note: This module requires the Advanced Forensics License.

Spectrum Analysis

Wireless networks operate in the same 2.4 GHz and 5 GHz unlicensed spectrum as many devices, such as cordless phones, wireless cameras, and microwave ovens. These devices can cause interference in the WLAN and have an impact on your network performance. Often sources are introduced unknowingly and problems are intermittent, so troubleshooting is difficult and typically must be performed in real time. The Spectrum Analysis module offers a cost-effective solution to resolve these types of interference issues.

The Spectrum Analysis module uses your Extreme WLAN infrastructure (dedicated sensors or access points) to identify and classify possible sources of interference and view the impact to the wireless network. This module generates alerts to network administrators when an interference source is detected. It is a software-only solution that allows you to view the physical layer of your wireless network without requiring specialized hardware. It's easy-to-use graphical interface allows you to monitor and troubleshoot even elusive, intermittent interference sources. The ability to view real-time spectrograms helps identify possible issues and take necessary steps to improve wireless performance right away. Detection is done from a central console, avoiding the need for IT staff to make on-site visits to determine causes of interference.



Note: This module is included with the WIP license with AirDefense 10.1 and higher releases. Requires the Advanced Spectrum Analysis License in prior releases.

Wireless Vulnerability Assessment

The AirDefense Wireless Vulnerability Assessment module uses a patented technology to remotely test wireless security. It allows administrators to automatically log on to an access point and test for vulnerabilities from the perspective of a wireless hacker. Extreme sensors conduct wireless penetration testing, proactively identifying vulnerabilities before they can be exploited, so you can better manage threats and keep your systems secure.

Remote and Automatic

Current practice involves administrators using a combination of traditional vulnerability assessment tools and occasional on-site wireless assessments to identify vulnerabilities. Because of the time and expense associated with manual testing, most organizations usually scan only a small sample of their network locations, potentially missing vulnerabilities. The remote testing capability of the AirDefense Wireless Vulnerability Assessment module eliminates the need for and expense associated with manual testing and on-site visits. Scans can be configured to run either automatically or on demand, allowing you to meet compliance requirements for regulations like PCI DSS while also maintaining a strong network security posture.

Extensive scanning permits validation of firewall and wireless switch policies, while also letting you identify and control potential paths of entry to assets on the wired side of your system. Customizable blacklists even let you target specific networks and devices that should or should not be accessible from your wireless network allowing you to ensure protection of sensitive data.

Note: Requires the Wireless Vulnerability Assessment (WVA) license.

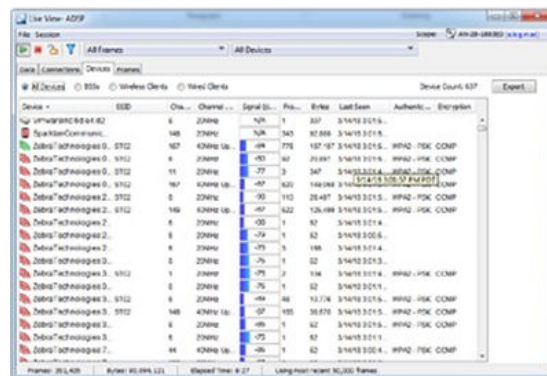
Liveview

The Liveview module in Extreme AirDefense provides a tool to perform analysis on wireless traffic in real-time. Liveview allows the administrator to turn a sensor into a sniffer and capture full layer-2 frames seen on the airwaves. The packet capture can then be viewed on the Liveview UI with the ability to break out individual fields or save as a pcap file to import into other packet analysis tools (e.g. Wireshark). Remote packet capture is supported simultaneously for up to 5 sensors.

Aside from this Liveview provides 25+ summary visualizations derived from the above data on data analysis, device analysis, connection analysis, frame analysis, etc. – providing much more than remote packet capture functionality.

In summary, Liveview provides excellent remote troubleshooting and data analysis capabilities that can be managed from a centralized location, enabling the capability to catch a problem while it is happening, while also eliminating the high operations costs associated with sending a technician onsite.

Note: The Liveview module requires the WIP license.



Bluetooth Monitoring

Extreme AirDefense can perform active monitoring of Bluetooth devices. This feature requires an access point model with built-in Bluetooth hardware. This functionality is useful for detecting bluetooth skimmers that attempt to open up a hole in the network potentially allowing unauthorized access using the Bluetooth protocol. Additionally, Extreme AirDefense can also listen to URL/ UUID advertisements in Google Eddystone or Apple iBeacon enabled tags using the BLE 4.0 protocol. This helps detect tags that can advertise unauthorized URLs opening up an avenue for launching a phishing attack. A white list can be configured to filter allowed URLs (e.g., containing the organization's own domain name), while triggering alerts for potential unauthorized ones. AirDefense offers multiple BLE classification signatures to view, identify, act, and immediately locate unsanctioned and rogue Bluetooth devices that may pose a threat.

Note: This feature is included with the WIP license.

Centralized Management

An AirDefense appliance centralizes management across several thousands of sensors — including sensor configuration and sensor firmware management. While the software architecture on the appliance utilizes multiple engines that are distributed across multiple cores, a central UI interface provides a single pane of glass, hiding the internal distributed nature of the system from the administrator.

For large deployments that need more than one appliance, the AirDefense Centralized Management Console (CMC) module provides aggregated views of the data on multiple appliances and a single point for configuration changes. CMC streamlines the monitoring of security events, automates management, and speeds time-to-resolution of network issues, thereby improving productivity.

Note: This module requires the CMC license for multi-appliance deployments.

Licenses and Specifications

Licenses

Feature	Dedicated Sensor Part Number	Radio-share Sensor Part Number
Wireless Intrusion Prevention (WIP)	AD-SNFL-P-1	AD-FLRS-P-xx
Advanced Forensics	AD-FESN-P-1	AD-FERS-P-1
Wireless Vulnerability Analysis (WVA)	AD-VASN-P-1	Not available.
Centralized Management Console (CMC) (only required for multi-appliance deployments)	AD-CMC-P-1	
Appliance Platform License (only required for primary server/ VM)	SP-SWSV-P-1	

Appliance Specifications

Hardware Appliance	NX-9600-100AD-WR- (supports 2500 dedicated sensor or 3000 radio-share sensors). See NX 9600 specsheet for details
Virtual Appliance Support	Supported with the following hypervisors VMWare EXSi 5.5 or higher Xen 4.1.2 or higher

Client Console Specifications

Recommended System	2 GHz processor or higher, 1 GB RAM or higher, 2 GB disk space or higher with Windows 7 Enterprise or Windows 10 Enterprise
Browsers	Chrome, Firefox, Internet Explorer

Sensor Support Specifications

Access Point Models supported	Cloud IQ Engine Access Points: AP410C and AP460C (Third-radio sensor) WiNG Access Points: AP 7632, AP 7662, AP 7612, AP 8432, AP 8533, AP 7522, AP 7532, AP 7562, AP 505, AP 510, AP 560 ExtremeWireless Access Points: AP 39XX Note: See release notes for features support for each access point model.
-------------------------------	--

