

ADVANCED FORENSICS

Wireless events are by their nature transient. This presents an enormous problem for administrators researching security and performance issues. Without granular historical records of activity, research is virtually impossible. AirDefense Enterprise provides administrators with the ability to rewind and review detailed records of wireless activity that can assist in a forensic investigation or wireless network performance troubleshooting.

Detailed Forensic Analysis and Remote Troubleshooting

Administrators can choose to view the activity of a suspect device over a period of months and drill down to minute-by-minute detail of wireless activity. It allows organizations to view events months later to improve network security posture, assist in forensic investigations and ensure policy compliance. These records can make the difference between an administrator who can prove an attacker's repeated attempt to break into the wireless network and know where the attack was launched from versus an administrator that is simply unable to prove that a wireless attacker even connected to the network.

The system's unique wireless analysis engine enables organizations to extract pertinent historical data at any time for detailed troubleshooting. By storing and managing 325 data points every minute for each wireless device, Advanced Forensics provides more visibility into wireless LAN performance and specific wireless device activity. AirDefense stores critical device communication and traffic information such as channel activity, signal characteristics, device activity and traffic flow. Trends in network usage can easily be visualized to assist in performance troubleshooting such as identification of abnormal usage and capacity planning.

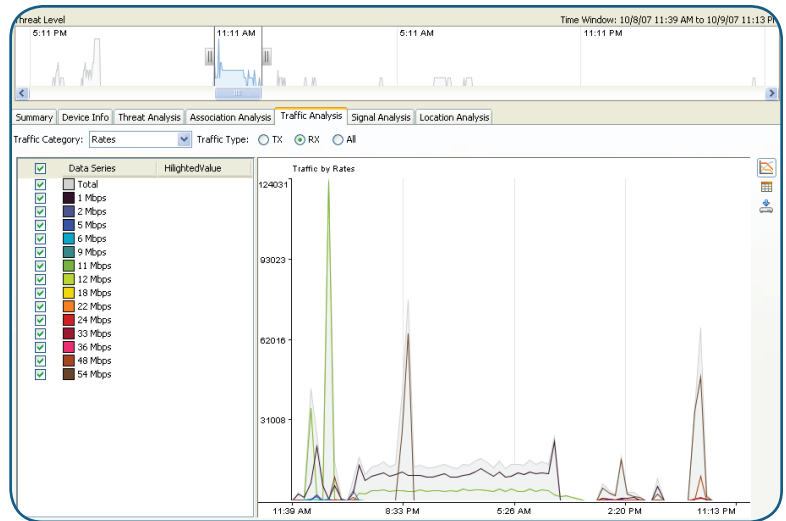
Additionally, AirDefense Enterprise maintains the highly accurate historical data required by many regulations such as HIPAA, GLBA, Sarbanes-Oxley (SOX), Payment Card Industry (PCI) data security standards such as VISA CISP and the Department of Defense.

Features include:

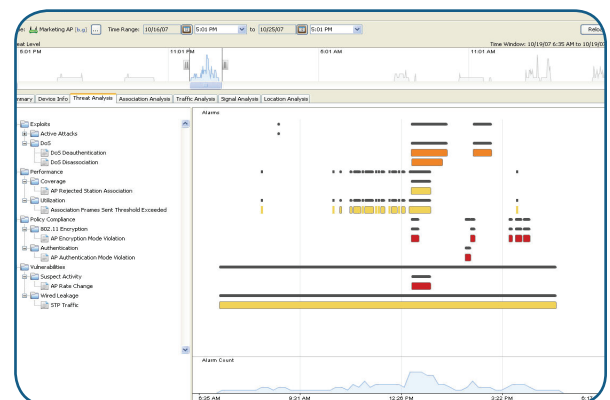
- 325 data points every minute for every wireless device
- Time of attack and sequence of events leading to breach
- Historic location tracking of wireless devices
- Device connectivity and activity logs

Benefits:

- Provides accurate record of wireless threats over time for forensic analysis and policy compliance
- Detailed wireless traffic data enables quick troubleshooting of wireless LAN issues
- Allows trend analysis for network performance and capacity planning.



Advanced Forensics - Traffic Analysis



Advanced Forensics - Sequence of Attack