ACCELERATE ROOT CAUSE DETERMINATION AND RECOVERY

AIRDEFENSE ADVANCED FORENSICS MODULE

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. For administrators, keeping track of the myriad factors impacting network utilization and availability is difficult without the right tools. The Advanced Forensics Module gives you the ability to continuously monitor your wireless environment and provides the data and analysis tools you need to support forensic investigation and network performance troubleshooting.

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

USE A TOOL DESIGNED FOR WIRELESS

Wireless events tend to be transient by nature making analysis of security and performance issues a difficult undertaking. Without granular historical records, trend analysis is virtually impossible. The AirDefense Advanced Forensics Module gives wireless administrators the ability to rewind and review detailed records of wireless activity in support of forensic investigation or network performance troubleshooting. The Module's unique wireless analysis engine lets you get to historical wireless data for detailed troubleshooting – whenever you need it. Every minute, the system stores 325 data points for every identified wireless device, providing a complete record of WLAN performance and connectivity. This dynamic database of critical device communication and traffic statistics including channel activity, signal characteristics, device activity, and traffic flow, can be used to chart network usage trends, identify anomalies and support capacity planning.

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. 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, assuring better compliance and improving overall security posture.

SIMPLIFY YOUR COMPLIANCE

The Advanced Forensics module also 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**
  Easily identify imbalances, including APs that are intermittently over- or under-utilized.
- **Historical traffic analysis**
  Quickly isolate and identify the issue driving anomalous behaviors, such as connectivity loss when a microwave oven is in operation.
- **Historical channel analysis**
  Determine spare channel capacity to help optimize WLAN frequency planning.
- **Historical location tracking**
  Determine the physical location of a device over time, identifying hot zones where the device typically operates, as well as roaming trajectories for mobile clients.

ADVANCED INFRASTRUCTURE FORENSICS

With ADSP Release 8.1.1, the capabilities of the AirDefense Advanced Forensic module have been extended to include data collection from infrastructure polls. With infrastructure forensics administrators have access to additional information which can be used to ensure the integrity of the wireless network. The forensics module gives administrators access to 115 statistics per poll, sufficient to provide a complete picture of the infrastructure environment yesterday, a week ago or even a month ago.

Powerful visualization tools allow data for a configurable time period to be presented in a way that allows administrators to understand usage patterns, network performance, and long term trends. The data collected in infrastructure forensics is in addition to data collected from sensor forensics but provides complementary information on CPU, memory, and RSSI from the Access Point perspective.

Customers with Air Defense WLAN Management or LiveRF and Advanced Forensics licenses are automatically enabled with Advanced Infrastructure Forensics capability once their upgrade to ADSP 8.1.1 is complete.

HOLISTIC WIRELESS MANAGEMENT

The Advanced Forensics module runs on the Motorola AirDefense Services Platform. The Motorola AirDefense Services Platform offers seamless integration of wireless Security & Compliance Solutions, WLAN Infrastructure Management, and Network Assurance tools that centrally troubleshoot user connectivity issues and optimize WLAN performance. The AirDefense Services Platform is the industry's first comprehensive service oriented platform that can be leveraged by enterprise IT to dramatically reduce TCO and achieve quicker ROI from their WLAN.

Motorola AirDefense solutions reflect our holistic approach to network design, management, security and network assurance. Motorola delivers both an unrivaled indoor/outdoor wireless portfolio and the software tools you need to build and operate a trusted high performance wireless network.

To learn more about how Motorola AirDefense Advanced Forensics solution can cut the time and money you spend to resolve network performance issues, please visit us on the web at motorola.com/wms.

FEATURES

325 data points every minute for every wireless device

Detailed attack and sequence of events leading to a breach

Historic location tracking of wireless devices

Device connectivity and activity logs

SYSTEM REQUIREMENTS FOR MOTOROLA AIRDEFENSE SOLUTIONS

An AirDefense server appliance is required to run the AirDefense Services Platform and all AirDefense modules. The server appliance is a true plug-and-play system with a hardened operating system, optimized database, and application software included.

Current model options include:

- Model 1252
- Model 3652
- Model 4250

Please refer to Motorola AirDefense server appliance sheets for details on specific models.

MOTOROLA