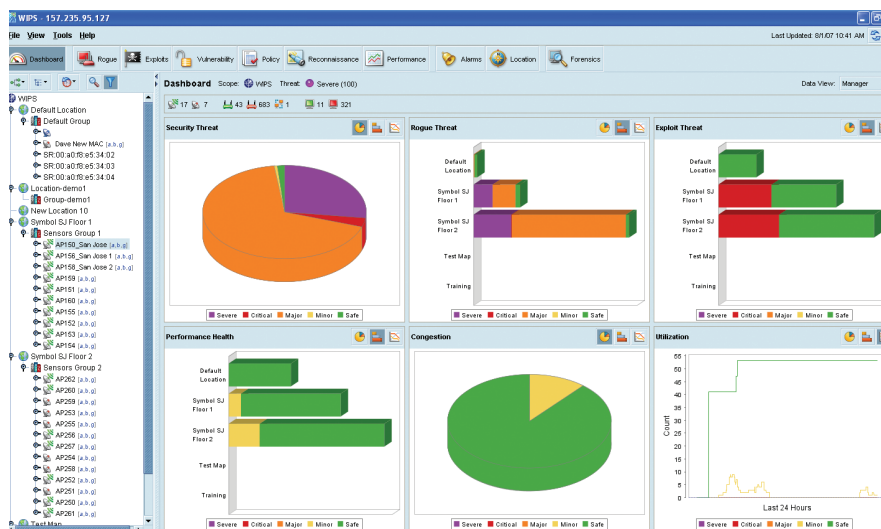




Wireless Intrusion Protection System

Wireless LAN security



FEATURES

24x7 dedicated sensors

Real-time identification of hackers, attacks and system weak spots

Historical database

By storing and managing more than 270 data points per connection per wireless device per minute the product provides a highly accurate assessment of wireless threats including anomalies and zero-day attacks. Allows viewing of events months later to improve network security posture and assist in forensic investigations

Forensic support

Pertinent historical data supports advanced forensics such as time of attack/breach, entry point used, length of exposure, systems compromised, device activity logs and transfers of data

Multiple detection technologies

Provides accurate and comprehensive detection by applying multiple detection technologies including signature analysis, protocol abuse and anomalous behavior in conjunction with correlation across multiple sensors

Secure your wireless network around the clock

With built-in forensic support and industry standard reports for PCI, HIPAA, Sarbanes-Oxley, GLBA, FDIC and DOD, Motorola's Wireless Intrusion Protection System (IPS) provides powerful tools for standards compliance, as well as around-the-clock 802.11a/b/g wireless network security in a distributed environment. It allows administrators to identify and accurately locate attacks, rogue devices, and network vulnerabilities in real time and permits both wired and wireless lockdown of wireless device connections. Tightly integrated when used as an optional component of Motorola's RF Management Suite, it shares a common interface, allowing the network administrator to access all administrative functions through a single control panel.

Integrated policy enforcement provides instant notification and response based on policy violations, while the vulnerability assessment feature identifies network weaknesses, such as misconfigured devices and weak encryption implementations.

See intruders and shut them down — wherever they are

Triangulation-based locationing capabilities enable IT staff to quickly and accurately pinpoint the location of any device on the network and initiate security measures to neutralize threats. Additionally, Motorola's dual-radio sensor technology eliminates blind spots and greatly increases the reliability of the Wireless IPS System. In other systems, blind spots occur due to the brief lapse in time when scanning

occurs on other channels. Motorola's ability to scan 802.11b/g and 802.11a channels simultaneously, as well as the capability for multiple sensors to participate in the termination of a wireless connection, virtually eliminates this vulnerability and increases your overall level of security.

High performance without the high price

Traditional intrusion protection systems rely on a distributed architecture with fat sensors that increase costs, or a centralized architecture where sensors forward all unprocessed data to the server resulting in high bandwidth utilization. The unique architecture of Motorola's Wireless IPS provides the best of both worlds, splitting data analysis between sensor and server. Monitoring data is filtered by intelligent sensors, which identify and forward only essential security information to the server. Bandwidth requirements are minimized, providing scalability for distributed environments. The analysis of events is highly accurate due to the aggregation and correlation of critical information collected by the sensors, which is encrypted and securely transferred to the server. The result is a highly accurate, efficient and secure monitoring system.

Motorola's unique cost-effective architecture also provides flexible deployment options, allowing administrators the flexibility to deploy Motorola AP300s as dedicated sensors to monitor network traffic or as access ports to carry 802.11a/b/g network traffic for Motorola's Wireless Switches.

SPECIFICATION SHEET

WIRELESS INTRUSION PROTECTION SYSTEM
Wireless LAN security

Location-based security

Provides location of unauthorized devices and activities using Motorola WLAN infrastructure

Industry standard reports for compliance

Provides built-in reports for PCI, HIPAA, Sarbanes-Oxley, GLBA, FDIC and DOD, as well as forensic support to determine compliance level after the fact, should a security event occur.

True plug-and-play operation

Auto-classification allows for a quick policy-based authorization of APs and devices. Network traffic can be monitored within minutes of installation, complete with the tools to quickly interpret information for fast response to Wireless LAN threats.

Centralized detection engine

Eliminates the need to upgrade sensors individually — a single server upgrade provides new functionality and protection against the latest attacks and new threats.

Report builder

Allows customized reports to suit your specific needs

Services for a more successful mobility solution

Motorola offers a full suite of services, delivered through a four-phase methodology that includes complete planning and assessment, analysis and design, mobility implementation and ongoing

support for the seamless deployment, management and continued support of your mobility solution.

For more information about Motorola's Wireless IPS or other Motorola Enterprise WLAN products, visit motorola.com/EnterpriseWLAN

Wireless IPS Specifications

Server Engine Specifications

Recommended Systems:	IBM: IBM System x3550 – 7978AC1 Intel XEON processor 5050, 3.00GHz, 667MHz FSB, 2x2MB L2 Cache, Dual Core, 4.0GB ECC DDR2 FBDIMM 667MHz; Storage - 3.5" SATA Simple Swap enabled system; NO INTERNAL RAID; 80GB 7200 RPM 3.5" Simple Swap SATA HDD; CD-RW/DVD Combo V Ultrabay Enhanced; Dual Integrated 10/100/1000 Mbps Ethernet (standard)
	Hewlett Packard: HP ProLiant DL140 G3 Non-Hot Plug SATA Server; Dual Core Intel Xeon 5160 (3.0GHz, 1333 FSB); HP 4.0 GB Fully Buffered DIMM memory; HP 80GB SATA Non-Hot Plug Hard Drive; Integrated Broadcom 5721 NICs; HP 361040-B21 DVD Option Kit

Views:	Summary Dashboard, Rogue, Exploits, Vulnerability, Alarms, Policy, Reporting, Reconnaissance, Performance, Location, Notification, Admin, LockDown, Access Control List
--------	---

Detection Expertise:	Rogue device detection; AP configuration; security configuration; theft of service attacks; denial of service attacks; probe attacks; network topology; worm attacks; AP and client malfunction; operational performance; system diagnostics
----------------------	--

Notifications:	e-mail (SMTP), send to syslog, SNMP trap
----------------	--

Client Specifications

Client:	Installable GUI application, on Windows or Linux
Recommended System:	1.5 GHz processor or faster, 1GB RAM, 100MB available disk space

Sensor Hardware and WIPS Licenses

APs (for Sensors):	WSAP-5100-100-WWW - 802.11a/b/g AP300 with external antenna connectors WSAP-5110-100-WWW - 802.11a/b/g AP300 with embedded antenna
Sensor Licenses:	SW-WIPS-LIC-001-WWW – single sensor SW-WIPS-LIC-010-WWW – 10 sensors SW-WIPS-LIC-100-WWW – 100 sensors
Server Licenses:	SW-WIPS-SRV-100-WWW - Primary SW-WIPS-SRV-R-WWW - Redundant



MOTOROLA

motorola.com

Part number SS-WIPS. Printed in USA 09/07. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Symbol is a registered trademark of Symbol Technologies, Inc. All other product or service names are the property of their respective owners. ©Motorola, Inc. 2007. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.