AIRDEFENSE SOLUTIONS

PROTECT YOUR WIRELESS NETWORK AND YOUR CRITICAL DATA

SECURITY AND COMPLIANCE

THE CHALLENGE: SECURE THE OPEN AIR

Wirelesss communication lets you take your business wherever your customers, your products and your vendors are. It connects you to your mobile work force. It gives you the flexibility to compete aggressively. When they are not tied down with wires, your people can be free to be more productive, more responsive and more effective.

That freedom, of course, comes with some risk. Your business data is an asset just as precious as cash and just as important to safeguard. It includes not only your own proprietary and financial information, but financial and personal data about your customers, your vendors and your partners.

The more enterprises turn to wireless LANs and Wi-Fi to meet critical business needs, the more hackers spring up, specializing in ever more innovative ways to hijack your communications and profit at your expense. But they are not the only threat – an innocent outsider who accidentally connects to one of your access points or an employee who brings in an insecure new device can expose you just as seriously. Even the most casual security breach can earn you the unwanted attention of increasingly concerned legislators and regulators.

What can you do to keep your data assets safe when they are literally flying through the air? You can take charge. You can be proactive. You can use tools designed to meet the unique challenges of wireless network security, developed by a globally recognized 80+ year leader in mobility technology – Motorola.

THE SOLUTION: PROACTIVELY PROTECT YOUR NETWORK

A threat to your network security is a threat to your mission. The AirDefense Security and Compliance solution is designed to help resolve security problems before they affect your business. So you can reduce downtime, mitigate risks and conduct your mission-critical business with confidence.

The AirDefense Security and Compliance solution watches over your systems, alerting your IT staff to vulnerabilities so you can take action before they can be exploited. Automatic monitoring gives you the ability to instantly disconnect a rogue device or lock out an attacker, without disrupting routine business communication. You can not only ensure your compliance with security mandates, you can demonstrate it, using either our pre-designed audit reports for the most common regulatory bodies or your own easily customized reports.

Most important, you can protect your organization's network from the substantial risks associated with a security breach. And that means your reputation, your productivity and your bottom line will be protected, too.

SECURITY

The AirDefense Security and Compliance solution includes the most advanced 24x7 wireless monitoring tools, allowing your IT staff to identify network attacks and vulnerabilities, and to instantly terminate the connection to any rogue device. The system uses collaborative intelligence with secure sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g/n) wireless traffic in real time. As a key layer of security, Motorola AirDefense complements VPNs, encryption and authentication.

With the AirDefense Security and Compliance solution, you get complete protection against wireless threats, together with policy and compliance monitoring, in a system that can scale to meet the needs of even the largest global organizations.

LOCK OUT INTRUDERS

One of the most challenging wireless security threats is a malicious intruder – this could be anyone looking to find a weakness in your network before you do. The AirDefense Security and Compliance solution is your 24x7 security force, guarding against wireless intruders. It constantly watches your network's daily activity, analyzing existing and day-zero threats in real time against historical data. Using the industry's most extensive event library, with more than 200 security and performance events, this next-generation wireless protection platform automatically identifies and reports wireless attacks, unusual traffic patterns or other suspicious activity, Sophisticated detection engines minimize false alarms, so only meaningful events come to the attention of your staff.

MEETING COMPLIANCE STANDARDS FOR HEALTHCARE

Health Insurance Portability and Accountability Act (HIPAA): Healthcare organizations must maintain the sanctity of patient data by complying with HIPAA regulations. Security management must be supported through constant verification and enforcement of security policies, provide intrusion alarms, audit trail information, event reporting capability and continuous vulnerability assessment.

MEETING COMPLIANCE STANDARDS FOR RETAIL

Payment Card Industry Data Security Standard (PCI DSS): Retailers are subject to mandates of the Payment Card Industry (PCI). PCI DSS requires that card holder environments change wireless defaults (passwords, SSIDs, WEP keys, etc.), analyze and identify all wireless devices, restrict physical access to wireless devices, log wireless activity and define wireless usage policies.

DISABLE ROGUE DEVICES

Unauthorized devices can behave like a master key to your offices – a single rogue access point can give an attacker full access to your internal network, bypassing traditional wired network security controls. The AirDefense Security and Compliance solution can identifiy and automatically disconnect any rogue device. By analyzing wireless traffic, the system prioritizes the level of threat that a potential rogue poses, so your administrators can deal with the most serious dangers first. While less sophisticated intrusion prevention systems might disable a neighboring access point by mistake, the AirDefense solution is accurate and reliable, protecting you against both unwanted intrusion on your network and unwarranted intrusion on someone else's.

INVESTIGATE AND ANALYZE

Often, the real impact of a security threat is revealed not in a single significant event, but in a series of small ones – like a burglar quietly walking around your building, checking whether all the windows are locked. When it comes time for forensic investigation of network security, the AirDefense Security and Compliance solution makes the detective work easier.

The system stores important information such as channel activity, signal characteristics, device activity and traffic flow – in all, more than 325 data points per wireless device, per connection, per minute, so you can trace back through months of history on a device only recently found to be suspicious. Instead of physically visiting sites, your administrators can investigate remotely, rewinding and reviewing minute-by-minute records of connectivity and communication on your network. So investigations that might once have required hours can be completed in just minutes.

ASSESS VULNERABILITIES

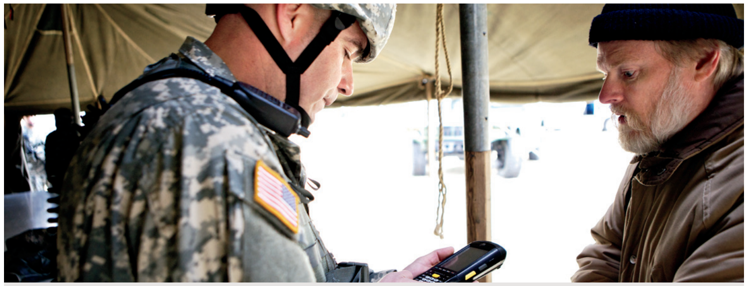
To truly harden your wireless network against malicious attacks, look at it closely through an attacker's eyes. The Wireless Vulnerability Assessment module is a patented testing technology that simulates attacks from a wireless hacker's point-of-view. Its extensive scan features lets you validate firewall and wireless switch policies, while also helping you identify paths of entry to sensitive wired systems that might be exposed through your wireless network.

The assessment technology works remotely and satisfies requirements for regulatory compliance, so you can save the costs of sending personnel or consultants to remote offices and stores to manually conduct required security audits. Configured to run automatically or on demand, the assessments can be customized with blacklists to target networks or devices, validating what should or should not be accessible from the wireless side. By routinely and automatically assessing potential vulnerability, you can proactively fortify the security of all your information assets, wired and wireless, across your entire enterprise.

SECURE LEGACY INFRASTRUCTURE

Wireless security protocols have evolved significantly over time. So some devices in your wireless infrastructure may not offer the same level of protection as the rest of your network. The Motorola AirDefense WEP Cloaking module provides protection for wireless infrastructure secured by legacy encryption protocols.

Motorola AirDefense WEP Cloaking is the first and only patented technology to protect retailers and other organizations using the Wired Equivalent Privacy (WEP) security standard to protect networks from common attempts used to crack encryption keys. Leveraging the Motorola AirDefense Services Platform, the WEP Cloaking module uses the same sensors to continuously protect access points, laptops and portable data terminals, in use by many retailers, from passive and active attempts to crack WEP encryption keys.



MEETING COMPLIANCE STANDARDS FOR FEDERAL AGENCIES

Department of Defense Directive 8100.2: The Department of Defense Directive 8100.2 establishes policy and assigns responsibilities for the use of commercial wireless devices, services and technologies in the DoD Global Information Grid. It spells out policies for deploying secure wireless networks and requires monitoring of those wireless networks for compliance.

REDUCE REGULATORY RISK

No matter how much you have invested in IT security, a single insecure wireless LAN device can compromise your entire network backbone. The potential financial costs and loss of public confidence of such a security breach are bad enough. But in industries subject to legal oversight, any security lapse can also carry significant legal and regulatory ramifications.

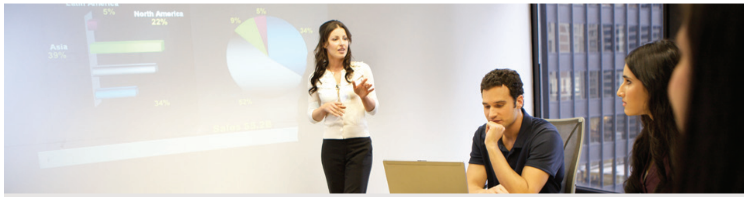
The AirDefense Security and Compliance solution is designed to help you not only meet, but clearly demonstrate, your organization's compliance with the defined policies of regulatory bodies. A straightforward, easy-to-use system helps you define security compliant policies, track your wireless activity, test and audit your wireless network security and routinely report your regulatory compliance.

COMPLIANCE

REPORT EFFICIENTLY

The AirDefense Security and Compliance solution includes built-in reports covering a variety of wireless network activity and compliance requirements from auditors. The system includes regulatory compliance reports for retail establishments, healthcare organizations, financial service providers and government agencies. Your administrators simply print the applicable report to demonstrate the wireless network's compliance.

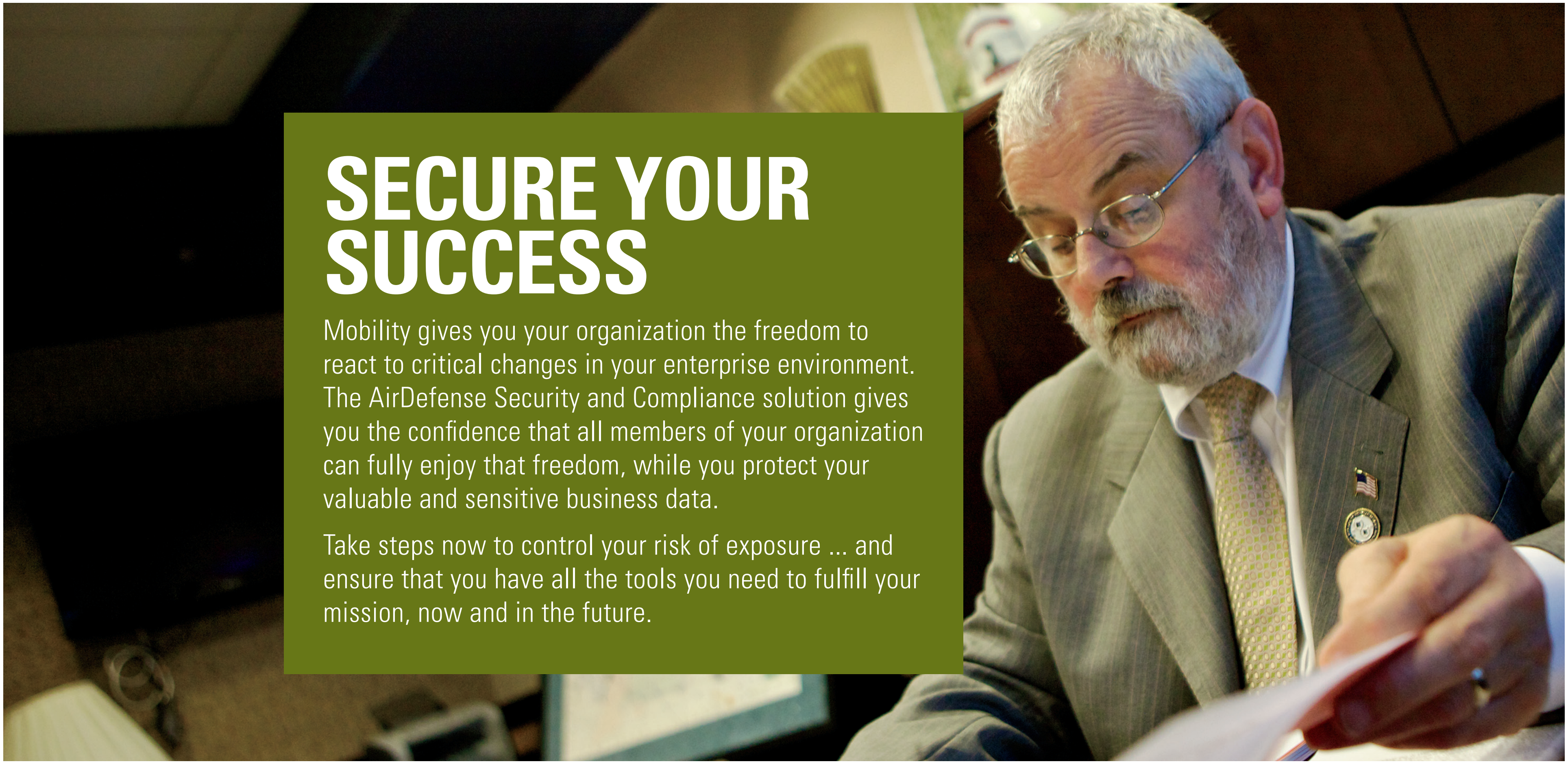
Using an easy-to-understand interface, you can also build your own highly customized reports within minutes, using graphs to provide a quick snapshot of important metrics. In addition to running reports in real time, you can schedule detailed reports to run overnight so they are complete and ready for review at your convenience.



MEETING COMPLIANCE STANDARDS FOR THE ENTERPRISE

GLBA – Safeguards Rule: The GLBA – Safeguards Rule has been defined for banking and financial institutions to insure the security and confidentiality of customer information, protect against anticipated threats to the security or integrity of such information and protect against unauthorized access to such information that could result in substantial harm to customers.

Sarbanes-Oxley Act (SOX): The Sarbanes-Oxley Act Section 404 requires all publicly traded firms to file an internal control statement attesting to management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company. The IT department must document, test, monitor and report the effectiveness of internal control processes.



SECURE YOUR SUCCESS

Mobility gives you your organization the freedom to react to critical changes in your enterprise environment. The AirDefense Security and Compliance solution gives you the confidence that all members of your organization can fully enjoy that freedom, while you protect your valuable and sensitive business data.

Take steps now to control your risk of exposure ... and ensure that you have all the tools you need to fulfill your mission, now and in the future.

To learn how the AirDefense Security and Compliance Solution can help you reduce your exposure to the risks of data compromise, regulatory problems and financial liability, please visit us online at motorola.com/wms or access our global directory at www.motorola.com/enterprisemobility/contactus.

SYSTEM REQUIREMENTS FOR MOTOROLA SOFTWARE 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 see each Motorola AirDefense server appliance specification sheet for model specs.

MOTOROLA