

Seamless Mobile Security for Network Operators

Build a secure foundation for winning new
wireless services revenue.



New wireless services drive revenues. Faced with the dual challenges of increasing revenues and gaining competitive advantage, network operators are now offering wireless data services at an unprecedented rate.

However, today's highly competitive race to market often results in operators rolling out new services and applications without devoting an appropriate amount of time, energy and resources to security issues.

With security and availability being among the top concerns of both business and consumer markets, this oversight allows wireless security vulnerabilities to threaten—and even reverse—gains in revenues and customer loyalty.



Why Should You Care About Wireless Security?

Security risk assessments conducted by Motorola for network operators around the globe reveal widespread security vulnerabilities that could jeopardize operational infrastructure, subscriber data and privacy, and network availability. With security now a leading concern for enterprise customers served by wireless operators, security incidents that become public can negatively impact your reputation, leading directly to brand damage and loss of revenue.

Motorola Wireless Security Services

Motorola's Wireless Security Services include a full range of offerings that provide you with the expertise you need to protect your core infrastructure—and your valued customers—from wireless security threats.

- **Wireless Security Assessment Services**
- **WLAN Security Assessment Services**
- **Cellular Worm Bandwidth Assessment Services**
- **Risk Management Services**
- **Design and Implementation Services**
- **Managed Security Services**
- **Security Policy Services**
- **Incident Response Planning Services**
- **Physical Security Services**

Today, wireless security vulnerabilities threaten network availability and operator revenues



Fraud and identity theft



Disruption of service and network downtime



Regulatory compliance issues



Viruses, worms and other malicious attacks

Made possible largely by the advent of high-speed, IP-enabled networks, applications and devices, wireless data communications present a host of opportunities for you to grow revenues and build customer loyalty. In fact, network operators' revenues from wireless data services are estimated to reach \$50 billion in 2006 and grow to more than \$90 billion in 2008.¹

However, current and next-generation networks, platforms, applications, and devices face mounting wireless security threats. And in an era when it's never been easier for users to switch carriers, extended downtime and frequent security breaches can quickly erode customer loyalty and lead to loss of revenues and market share.

Fraud and Identity Theft

In today's expanding wireless communications environment, your network faces new and persistent threats: attackers seeking to intercept calls, steal customer data and disrupt or disable network operations. Striking from anywhere at any time, these invaders can commit identity fraud and compromise user privacy by carrying out "spoofing," "man-in-the-middle" and other malicious attacks against wireless networks.

Disruption of Service and Network Downtime

Other vulnerabilities, such as insufficient segregation of multiple networks, a lack of comprehensive perimeter security measures, or inadequate security patching and update processes, can result in costly equipment damage as well as widespread outages that negatively impact customer and investor confidence.

Regulatory Compliance Issues

Regulatory compliance issues can complicate your security efforts and impact network availability. Although making enterprise applications and data available to wireless users is becoming a strategic initiative for an increasing number of network operators, doing so can expose critical and confidential data protected by such statutes as the Sarbanes-Oxley Act in the U.S. and emerging regulation for traffic data retention in the European Union.

Viruses, Worms and Other Malicious Attacks

The growing interconnectedness among diverse systems means that today's wireless networks can be brought to a standstill by the same worms, viruses and other attacks that snarl communications, compromise critical data and cause outages on traditional wired networks.

Given their heightened awareness of security issues and incidents, subscribers increasingly see security as a key differentiator when choosing between service providers. Motorola Wireless Security Services help you build a secure and trusted communications environment that serves as the foundation for greater subscriber retention and increased wireless services revenues.

Whether defending against hackers and other cyber-threats, navigating complex regulatory requirements or implementing next-generation networks and technologies, Motorola Wireless Security Services provide an expertly coordinated combination of prevention, monitoring and recovery strategies to help you ensure network security and availability while protecting your vital core infrastructure and the privacy of your customers.

¹ Motorola Network/Industry Research and Analysis

Motorola Wireless Security Services help you build a secure foundation for winning new wireless services revenue

Why Technology Alone Isn't Enough

In recent years, many executives have come to regard security solely as a technology issue. In reality, it is an *environmental* issue that requires a carefully integrated strategy of vigilance involving people, process, policy and technology. Vulnerabilities in any of these four critical security program components represent rich targets for exploitation.

Motorola's Wireless Security Services team addresses people, process, policy and technology requirements across a full lifecycle of support services designed to improve wireless network security and help you ensure that wireless networks meet customer expectations for availability, security and privacy.

By providing centralized control over wireless network security and availability efforts, these offerings do more than protect wireless networks; they allow you to achieve your business objectives by providing a secure, trusted communications environment that leads to increased wireless services revenues and customer loyalty.





Wireless Security Assessments

The first step in any wireless security program is a comprehensive security assessment. Motorola's Wireless Security Assessment Services provide a review of all elements in a complete security program, including existing technologies, physical security, incident response procedures and operational security. Tailored to your unique operational requirements, the assessment identifies vulnerabilities and risks, provides detailed recommendations for mitigating risks, and delivers critical insights for protecting core infrastructure and customer data.

- **Identify wireless security vulnerabilities throughout your operations, from subscriber units to applications to networks**
- **Receive detailed risk mitigation recommendations**
- **Protect vital infrastructure and customer data**

" The [wireless security] risks seem to be expanding faster than our ability to deal with them."

– Jay Heiser
Research Vice President, Gartner
Gartner IT Security Summit 2005

A woman with dark hair, wearing a white striped shirt and a dark blazer, is looking down at a light-colored folder she is holding. The background is a blurred outdoor scene with green trees and a building.

WLAN Security Assessments

Motorola's WLAN Security Assessment Services provide an in-depth evaluation to ensure that your WLAN is properly configured and secured according to industry best practices and your unique business requirements. This includes examining existing physical security, incident response procedures and operational security. The findings of a WLAN Security Assessment serve as a roadmap for mitigating the technology and business risks associated with wireless technology, allowing you to address wireless security in a manner that best fits your available budgets and resources.

- **Ensure proper WLAN configuration and security**
- **Prevent unauthorized access and discover rogue access points**
- **Protect organizational assets and customer privacy**

Cellular Worm Bandwidth Assessments

Worms, viruses and other malicious code activity can generate a significant amount of data traffic that consumes precious, revenue-generating bandwidth, especially on the RF interface. Motorola's Cellular Worm Bandwidth Assessment Services provide you with the monitoring and data analysis you need to mitigate the negative impact of malicious code activity on cellular network performance and availability. Services include benchmarking network traffic results against industry averages and providing specific recommendations for reducing vulnerability to worms and viruses.

- **Monitor data traffic to identify wasted bandwidth**
- **Make informed decisions to protect revenue-generating services**
- **Reduce malicious code activity on your network**

Risk Management Services

In the complex, ever-changing world of wireless communications, new threats and vulnerabilities appear daily. Without a thorough, business-focused understanding and prioritization of your network's risks and vulnerabilities, certain threats may be overlooked, exposing customers to theft of critical information or causing downtime that results in financial losses. Other threats may be overprotected, wasting resources and budget. Motorola's Risk Management Services help you understand your unique risks and vulnerabilities, allowing you to invest limited budgets and resources more effectively.

- **Understand and prioritize your specific wireless security risks**
- **Align risk management activities and budgets with business objectives**
- **Protect your investment in next-generation technologies**

Design and Implementation Services

Motorola can provide the security-architecting expertise you need to create dependable, next-generation wireless networking environments. Based on assessment results, Motorola's Design and Implementation Services can help ensure and protect new wireless services revenue by focusing on such critical elements as points of Internet connectivity, firewalls, secure networks, intrusion detection/prevention, VPNs and encryption techniques. From guarding against viruses and worms to ensuring adequate isolation of wired and wireless networks, these services are aimed at building security into your network from the ground up: the most effective way to prevent network downtime.

- **Build a secure foundation for migrating to next-generation technologies and offerings**
- **Protect new wireless services revenues by maximizing network availability, security and performance**
- **Gain centralized control over your wireless networks**



Managed Security Services

To meet subscriber demand for continuous, around-the-clock network availability, Motorola's Managed Security Services provide constant wireless network monitoring in our state-of-the-art network security facility. This service makes highly trained security experts available 24/7, so they can respond to incidents day or night, guide you through the response cycle, and help you understand why an event happened and how to prevent it from recurring. Motorola's Managed Security Services also provide you with security software updates that are tested before they are applied, to avoid adverse affects on your business-critical networks.

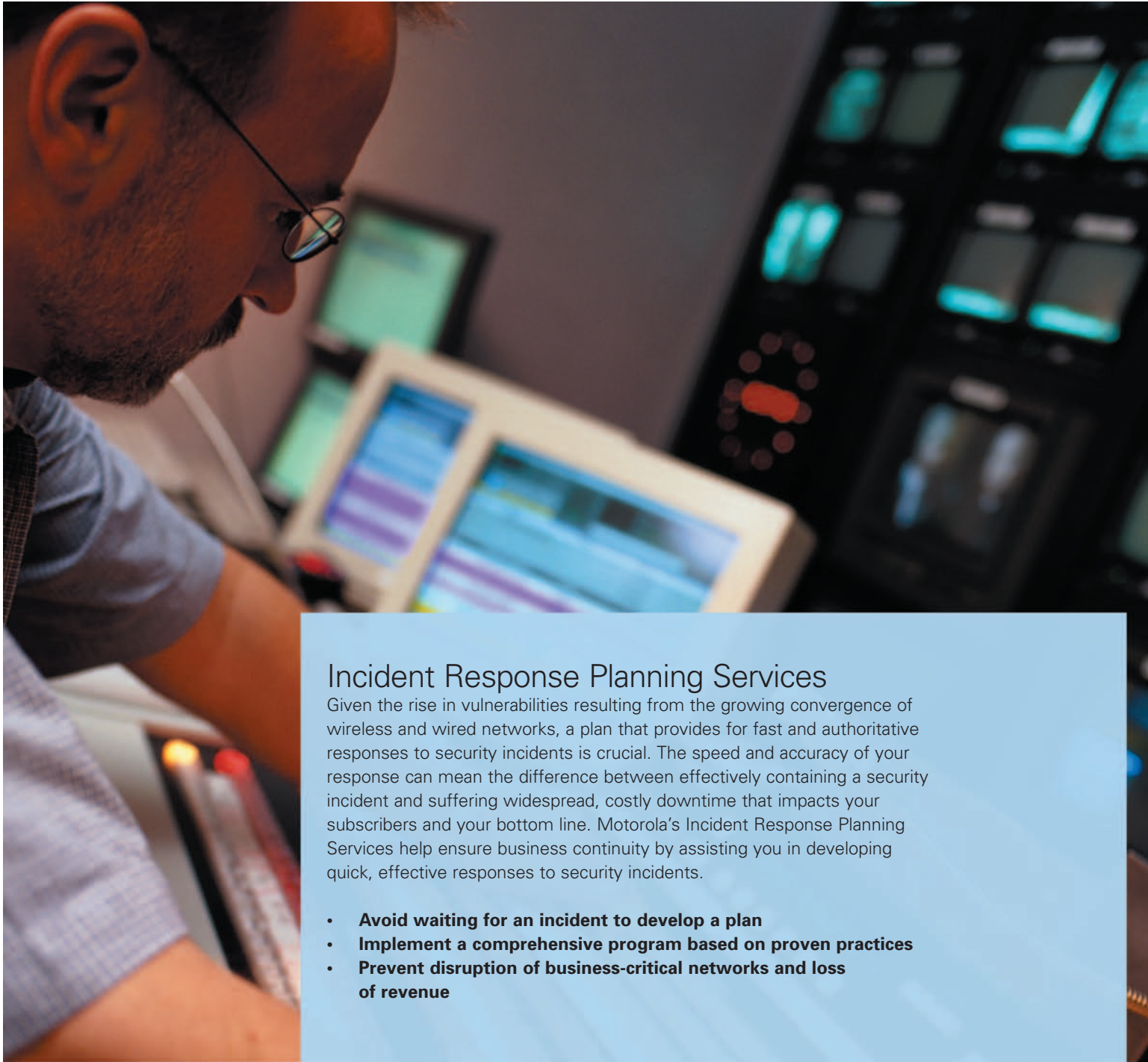
- **Implement 24x7x365 real-time security monitoring**
- **Protect business-critical networks with rapid response to security incidents**
- **Receive the latest, tested software updates and patches**

Security Policy Services

For network operators, the foundation of any successful security program is the ability to effectively communicate risk factors, employee responsibilities and management expectations. A critical component in facilitating this communication is the establishment of formal security policies. Motorola's Security Policy Services arm you with the tools you need to develop and communicate effective, customized security policies for addressing the unique risks and business requirements surrounding your wireless network and ensuring compliance with applicable standards and regulations.

- **Develop, communicate and implement effective security policies and procedures**
- **Measure company-wide observance of stated policies**
- **Avoid costly penalties for non-compliance with applicable laws and regulations**



A man with glasses and a beard is shown in profile, looking down at a computer monitor. He is wearing a light blue button-down shirt. The background is a server room with multiple computer monitors displaying data and server racks with glowing blue lights.

Incident Response Planning Services

Given the rise in vulnerabilities resulting from the growing convergence of wireless and wired networks, a plan that provides for fast and authoritative responses to security incidents is crucial. The speed and accuracy of your response can mean the difference between effectively containing a security incident and suffering widespread, costly downtime that impacts your subscribers and your bottom line. Motorola's Incident Response Planning Services help ensure business continuity by assisting you in developing quick, effective responses to security incidents.

- **Avoid waiting for an incident to develop a plan**
- **Implement a comprehensive program based on proven practices**
- **Prevent disruption of business-critical networks and loss of revenue**

Physical Security Services

From natural disasters to criminals to disgruntled employees, physical security threats to your facilities put vital core infrastructure and confidential customer data at risk. More importantly, physical security vulnerabilities can endanger lives. Motorola's Physical Security Services deploy teams of industry-leading experts with extensive backgrounds in physical security and law enforcement. These teams assess your security procedures, access controls, alarm systems, electronic surveillance measures, and personnel response policies and recommend a course of action to improve your facilities' overall security posture.

- **Uncover physical security vulnerabilities that can put your operations—and people—at risk**
- **Understand your current state of readiness to respond to natural disasters**
- **Improve your facilities' overall security posture**

Building a Secure Foundation for Seamless Mobility

For today's network operators—constantly in search of new revenue sources and market differentiators—seamless mobility means providing customers with the ability to communicate anywhere, anytime across a wide variety of networks, applications and devices.

However, revenue and market gains from wireless services are threatened by a variety of wireless security vulnerabilities that can jeopardize your core infrastructure, cause extended network downtime and erode customer loyalty.

Provide a secure and available communications environment. Mitigate your wireless security vulnerabilities. And build a secure foundation for achieving seamless mobility. Get the expert assistance you need from the Motorola Wireless Security Team.

Motorola: 76 Years of Secure Wireless Communications

Motorola developed its Wireless Security Services based on proven practices established to protect the company's own global operations. Combining deep business savvy with its vast experience in delivering secure wireless communications solutions across multiple industry sectors, Motorola offers end-to-end wireless security expertise that is grounded in our proven, leading-edge wireless expertise and in our strength as a global practitioner providing world-class security to one of the world's most sophisticated network environments.

Motorola's Wireless Security Services team is currently securing the promise of seamless mobility for network, enterprise, government and public safety customers across the globe.

Protect Your Wireless Networks with Motorola Wireless Security Services

Motorola Wireless Security Services leverage the security expertise derived from our long-standing experience as a global leader in wireless, automotive and broadband communications; a reputation built on understanding and accounting for clients' unique business requirements.

Concerned about providing your customers with the highest levels of wireless network availability, security and privacy? Learn more about Motorola Wireless Security Services by contacting your local account representative.

About Motorola Network Services and Applications Management

Motorola's Network Services and Applications Management is a line of business within Motorola Networks that combines innovation, technology and expertise to deliver solutions that are robust, operational and integrated into existing and new service providers' environments. Motorola has taken a practice-based approach and built a complete service portfolio upon key elements of Support, Integration, Applications and Management.



MOTOROLA

Motorola, Inc.

www.motorola.com

MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

1105NetworksGMS