# FROST & SULLIVAN

# Global Mobile VPN Products Market

*Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker*

**September 2011**

Market Engineering

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# RESEARCH TEAM

## *Martha Vasquez*

Industry Analyst, Network Security

> (001) 210-247-3864
> Martha.Vasquez@frost.com

## *Jennifer Bates*

Director of Consulting & Network Security

> (001) 940-455-7475
> Jennifer.Bates@frost.com

## *Alpa Shah*

Vice President of Research, ICT

> 001) 650-475-4556
> Alpa_Shah@frost.com

FROST & SULLIVAN

2

FROST *&* SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# CONTENTS

FROST *&* SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

3

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Executive Summary

Wireless Internet connectivity has become ubiquitous during the last five years. Driven primarily by lower cost access and integrated connectivity in devices, such as laptops, tablets, and smartphones, wireless Internet has become a viable option for remote employees.

As a result, many businesses and government entities have built remote Internet capabilities into their operating fabrics.

Employees are utilizing mobile devices to perform transactions directly at customer worksites. Protecting these transactions and providing secure connectivity back to the central office is a critical concern.

While many mobile security technologies exist, mobile virtual private network (VPN) technology allows organizations to enhance productivity and operate more effectively and efficiently by providing secure and persistent connections for remote workers.

The mobile VPN products market is an emerging market. The Mobile VPN market is gaining traction because of the explosive growth of mobile devices and the increasingly stringent regulatory requirements facing organizations.

In 2010, the global mobile VPN products market was valued at $160 million in revenue, with a compound annual growth rate (CAGR) of 18.4 percent. The North American region represents the highest percentage of the global market, at 79 percent and $126.9 million in total revenue.

In 2010, the top two vertical markets for mobile VPN products were the telecommunications segment and the government segment. Both of these verticals have a large number of remote employees with access to sensitive information and large field service teams.

The mobile VPN market is forecasted to show solid growth throughout the forecast period. The market consists of a wide variety of vendors ranging from dedicated software vendors, such as NetMotion Wireless and Columbitech, to large vendors that offer a breadth of networking products, such as Cisco and Juniper.

**F R O S T** *&* **S U L L I V A N**

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Market Overview

A mobile VPN is a VPN with specific features designed to provide secure connectivity and persistence over wireless networks. While other technologies, such as mobile Internet protocol (IP), IPSec, or Secure Sockets Layer (SSL) VPNs, provide similar functionality, mobile VPNs unify persistence and security features into a single product built for wireless coverage.
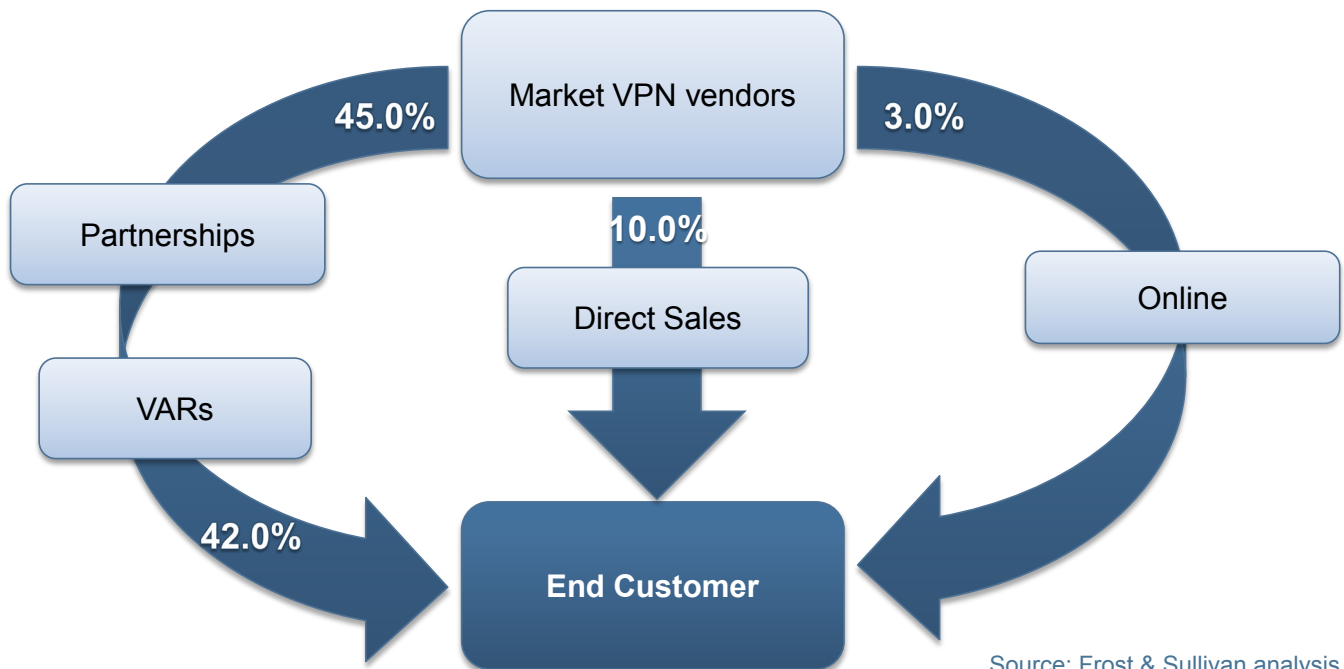
A mobile VPN allows devices to work across a variety of public or private networks, wired or wireless. These networks include wired local area networks (LAN), Wi-Fi networks, hotspots, and many varieties of wireless wide area networks (WANs) provided by different wireless carriers and satellite networks.

A mobile VPN solution may also include additional reporting, management, and control features. Frost & Sullivan also sees many traditional network access control (NAC) vendors partnering with vendors in this space, and some mobile VPN vendors have developed their own NAC solutions.

Frost & Sullivan requires the following features to be present in a mobile VPN solution for inclusion in this study:

- **Session persistence** - Traditional VPN users lose connectivity once they roam into different wireless networks, whereas mobile VPN users do not. The virtual IP address for each mobile VPN client remains the same, even when the IP address changes. The network connection is always on through a persistent IP address.

- **Application persistence** - As mobile VPNs pass through different networks, the application sessions are sustained, even when connectivity is lost. Traditional VPNs lose application sessions, causing data loss and forcing users to restart applications.

- **Network transparency** - When switching networks, the mobile VPN is transparent to the user and does not compromise security or privacy. The application interface remains the same.

- **Bandwidth optimization** - Mobile VPNs use a variety of optimization features to reduce network consumption and to lower bandwidth constraints thus lowering costs for organizations.

## FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker
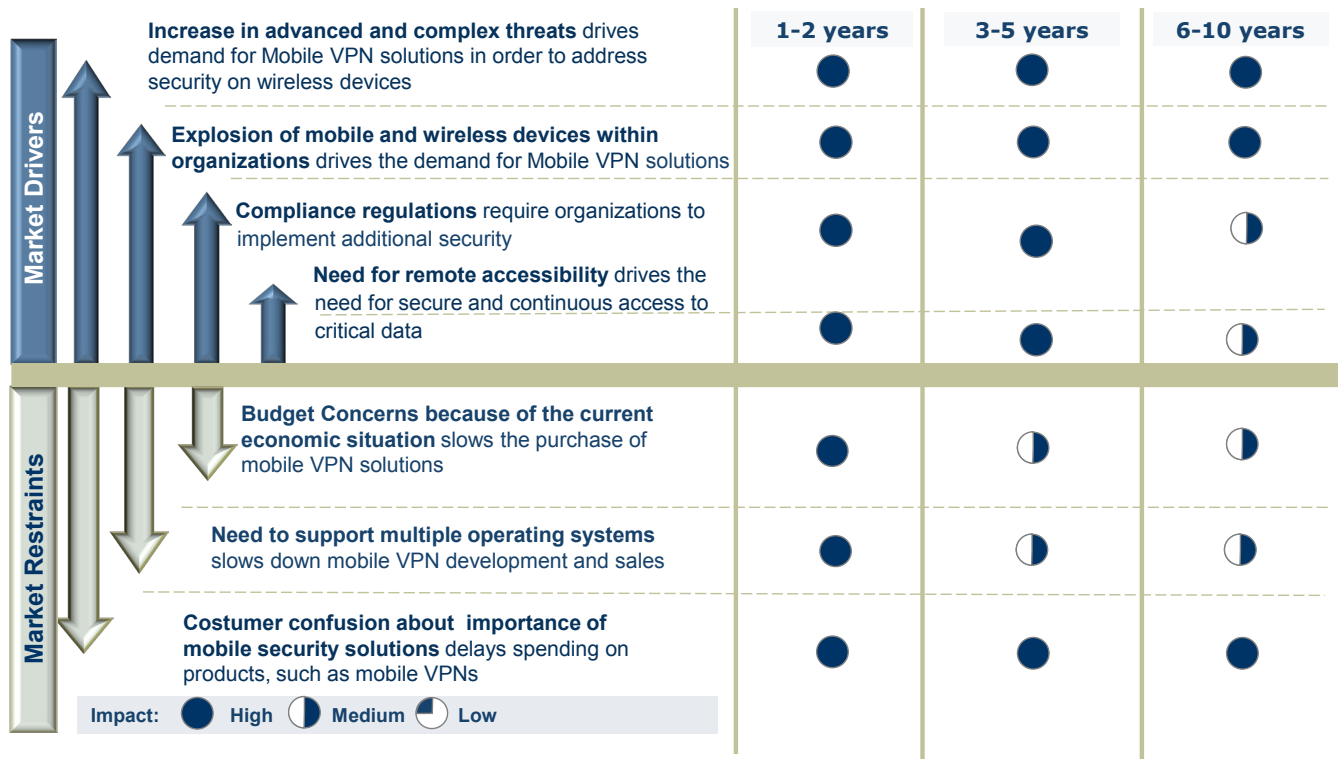
## Distribution Channel Analysis, Global, 2010



Source: Frost & Sullivan analysis.
Key: VARs: value-added resellers

**Key Takeaway: Partnerships and value-added resellers (VARs) are preferred sources of market VPN products because of their ability to provide trusted technical guidance.**

F R O S T & S U L L I V A N

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# External Challenges: Drivers and Restraints

## Key Market Drivers and Restraints

| Market Drivers | 1-2 years | 3-5 years | 6-10 years |
|---|---|---|---|
| **Increase in advanced and complex threats** drives demand for Mobile VPN solutions in order to address security on wireless devices | High | High | High |
| **Explosion of mobile and wireless devices within organizations** drives the demand for Mobile VPN solutions | High | High | High |
| **Compliance regulations** require organizations to implement additional security | High | High | Medium |
| **Need for remote accessibility** drives the need for secure and continuous access to critical data | High | High | Low |

| Market Restraints | 1-2 years | 3-5 years | 6-10 years |
|---|---|---|---|
| **Budget Concerns because of the current economic situation** slows the purchase of mobile VPN solutions | High | Medium | Medium |
| **Need to support multiple operating systems** slows down mobile VPN development and sales | High | Medium | Medium |
| **Costumer confusion about importance of mobile security solutions** delays spending on products, such as mobile VPNs | High | High | High |

Impact: ● High ◐ Medium ◔ Low

Source: Frost & Sullivan analysis.

# Drivers

## Increase in advanced and complex threats drives demand for Mobile VPN solutions in order to address security on wireless devices

The Internet has become a universal platform for conducting business. As a result, attackers have zeroed in on the Internet for conducting theft and fraud. Mobile devices are not immune from this trend and both consumers and organizations are looking for products to secure transactions conducted on Internet from outside the organization.

Even though mobility allows workers to demonstrate improved productivity, organizations have become increasingly concerned with hackers accessing corporate networks by posing as remote employees. Cybercriminals have shown they can easily take advantage of users connecting through hot spots or through unsecured connections, and organizations have little defense against these kinds of attacks.

Hackers are constantly looking for new vulnerabilities to exploit, and enterprises need to be prepared for these zero-day attacks. Using encrypted sessions and enforcing organizational policies on the mobile endpoint will help to prevent these attacks.

## Explosion of mobile and wireless devices within organizations drives the demand for mobile VPN solutions

Lowered prices and higher speeds for mobile Internet drive mobile devices into the hands of businesses and consumers.

Organizations are leveraging the use of personal mobile devices in the workplace. Today, most employees can access any business application and can connect to their corporate networks from anywhere through mobile applications, such as smartphones, laptops, tablets, and netbooks.

Because more and more work transactions are processed through mobile devices, security is a heighted concern. Mobile VPN technology and other mobile security products will be a crucial component as more mobile devices enter the workplace.

## Compliance regulations require organizations to implement additional security

The instances of data breaches continue to rise, and organizations are required to comply with government regulations that help secure customer data and company financial information.

As mobile devices become more prevalent and more cyber threats specifically targeting mobile devices are discovered, the security for mobile devices must improve.

Regulation and compliance is a strong driver for all information security markets, including the mobile VPN market. Verticals and industries continue to release specific guidance and regulations for

information security. Influential legislation effecting mobile VPN market include: the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Gramm-Leach Bliley Act (GLB) and Sarbanes Oxley (SOX).

## Need for remote accessibility drives the need for secure and continuous access to critical data

For remote employees, the ability to access data at all times is critical. Businesses now expect their employees to be able to log on from any location. The ability to access the Internet through enhanced wireless technologies has allowed for applications to be downloaded onto mobile devices. Employees are using more applications than originally intended. As more applications are available for mobile or wireless devices, enterprises are utilizing these applications to increase efficiency and to enhance productivity.

Furthermore, falling prices for consumer devices and data plans have driven organizations to adopt more mobile devices into the workplace. Because businesses financially benefit from constant employee mobility, keeping connections secure and persistent is a necessity.

# Restraints

**Budget concerns because of the current economic situation slows the purchase of mobile VPN solutions**

Since 2008, the global economy has experienced slow growth, causing many businesses to cut spending. In a majority of organizations, IT has bee hit hard by spending cuts. As a result, sales cycles have slowed, which has slowed growth in the overall information security market and for new security products, specifically.

Starting in 2010, the economy started to recover, but IT administrators remain cautious about spending on new security technologies. Frost & Sullivan believes that the need for mobile device security will outpace the current hesitation and this market will show steady growth through the forecast period.

**Need to support multiple operating systems slows down mobile VPN development and sales**

Mobile devices of the past were Windows laptops and personal digital assistants (PDAs), but the recent mobile-device market explosion has resulted in an array of mobile devices. Employees are no longer limited to Windows devices, but are using Macs, iPhones, Androids, Blackberries, and Symbian devices to connect to corporate networks.

Mobile VPN vendors are now scurrying to offer solutions for these broad-based platforms. This restraint will decrease as mobile VPN vendors offer a larger portfolio for these diverse operating systems. Many mobile VPN vendors have support on the roadmap or in development for these platforms, and this restraint will lessen over the next 18 months as development and product releases catch up with demand.

**Costumer confusion about importance of mobile security solutions delays spending on products, such as mobile VPNs**

Enterprise architects are still discovering more security measures are needed as they adapt to more wireless devices connecting to their networks. These security issues have perplexed information (IT) administrators on how to implement proper security measures for wireless devices.

Many organizations attempting solve mobile security challenges look to traditional VPN solutions, such as SSL or IPSec VPN. Mobile VPN vendors have to educate IT buyers before they can influence their buying decisions.

Despite high adoption by many organizations, many organizations remain reluctant to adopt mobile devices because of the potential security risks associated with allowing remote employees to access corporate networks.

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Forecasts and Trends

## Product and Technology Trends

### Management tools: analytics/policy tools

Businesses today are looking for solutions that offer more than just secure tunnels—they are also looking for better management tools. The increase in multiple devices and remote employees has driven the need for better visibility in managing these devices. In addition, the remote user can now log in to many different networks, making it difficult for IT management to centrally manage these devices. In addition to managing these devices, businesses want to view mobile workers' activities on wireless connections.

### Network Access Control (NAC)

Companies such as NetMotion Wireless and Birdstep have implemented NAC solutions into their portfolios. The NAC feature allows users to connect to the corporate network only if it complies with security policies. Although this functionality has appeared as important in the past, its adaption has been slow. Control in policies and management is becoming increasingly more important than the NAC feature.

### Increasing number and types of mobile devices and operating systems

As the number of remote workers increases, the multitude of new wireless devices and operating systems is also causing challenges for businesses. In the past few years, the market has experienced an influx in new operating systems besides Windows. Many traditional mobile VPN participants only support Windows and Symbian, and the addition of support for new platforms is a critical competitive factor moving forward.

### Integration/consolidation

Organizations continue to demand a one-stop-shop for security products to reduce complexity and the amount of support contracts. In the information security market, integration and consolidation of vendors continues to rise. Vendors, such as Cisco and Juniper, are partnering with other mobile vendors to increase the value proposition of their solutions. It is likely that pure-play mobile VPN vendors will need to create tighter integration and partnerships with other mobile vendors, or they will be acquired by larger, more comprehensive security providers.

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Legislative Trends

### Payment Card Industry (PCI) Data Security Standard (DSS)

The PCI DSS set a minimum baseline in the marketplace to protect a cardholder's sensitive account and transaction information. On 1 October 2008, PCI DSS 1.2 was implemented. The main purpose for the update was to clarify existing requirements and provide flexibility in the standard's interpretation. Within the mobile VPN market, legislation has stirred the retail market and businesses that have access to remote credit card transactions. The need for encryption and protecting data in motion continues to drive the market for mobile security.

### HIPAA and HITECH

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21, 1996, causing a host of security solutions to be evaluated and implemented by hospitals, doctors, pharmacies, and insurance companies. The Health Information Technology for Economic and Clinical Health Act (HITECH) responds to the criticisms of HIPAA and builds on HIPAA and broadens HIPPA's scope by increasing the rigor for compliance. As the healthcare market adopts wireless technologies, the need for remote access will increase. In addition, organizations will need to secure any mobile or wireless device that is accessing the corporate network to reduce the possibility of threats.
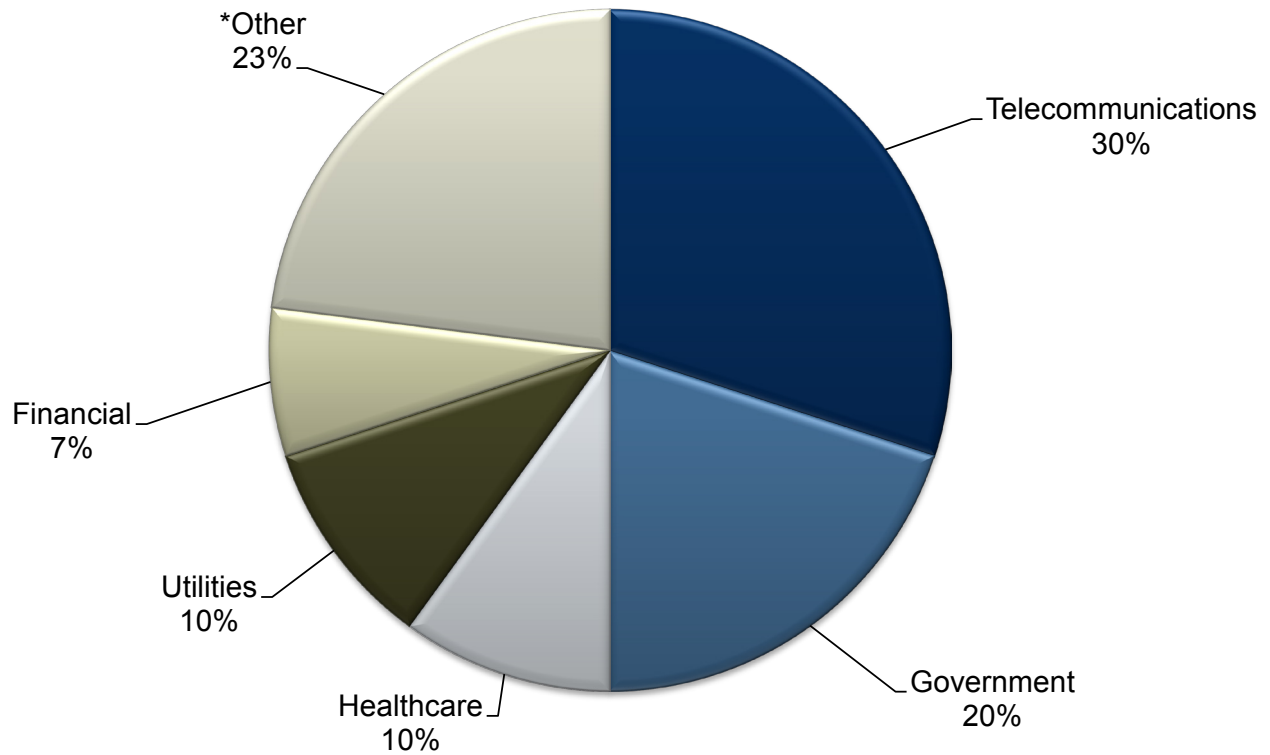
### Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLB) targets the financial markets, banks, securities firms, and insurance companies. This act addresses the privacy of consumer data and its exchange. Given the sensitivity of financial information, the financial sector required little convincing of the need for securing their communications. Financial institutions were early adopters of security technologies because of the size of their networks and budgets and the sensitivity of their data.

### Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) set and enforced standards for corporate financial accountability. Intended to reduce fraud and conflicts of interest, SOX mandates that CEOs, CFOs, and auditing firms attest to the validity of financial records and audits. It establishes management's responsibility for internal control and financial reporting; it also requires organizations to report material changes in financial conditions or operations on a rapid and current basis.

F R O S T & S U L L I V A N

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

## Percent of Revenue Distribution by Total Market
## Sales Breakdown



*Other
23%

Telecommunications
30%

Financial
7%

Utilities
10%

Healthcare
10%

Government
20%

* Other verticles include: Retail, Media, Transportation, Hospitality, Manufacturing, and Entertainment

Note: All figures are rounded. The base year is 2010. Source: Frost & Sullivan analysis.

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Vertical Market Revenue Forecast Discussion

Telecommunications and the government were the largest verticals for mobile VPN products in 2010. The telecommunications vertical represented 30 percent of the global mobile VPN market and generated $48 million in revenue. The government vertical represented 20 percent of the global VPN market by generating $32 million in revenue. The telecommunications vertical includes vendors, such as communication carriers and service providers. Telecommunications companies usually provide services to their own clients; therefore, this market is expected to experience growth through the increasing demand of mobile and wireless devices.

The government vertical remains a leading vertical in information security products. Furthermore, the mobile VPN market is in high demand for public safety, emergency, federal, local, and state agencies. The early adopters for this solution were providers for public safety and emergencies. Devices typically purchased in this sector consist of integrated mobile VPN clients because the demand for seamless security is increasing for this sector.

To remain in compliance, several key security standards are required before approving wireless devices for government employees. The key required security standards include strong authentication, non-repudiation, and secure personal identification devices and network levels. While these stringent requirements are more difficult for vendors to meet, the government is less price sensitive than other verticals.
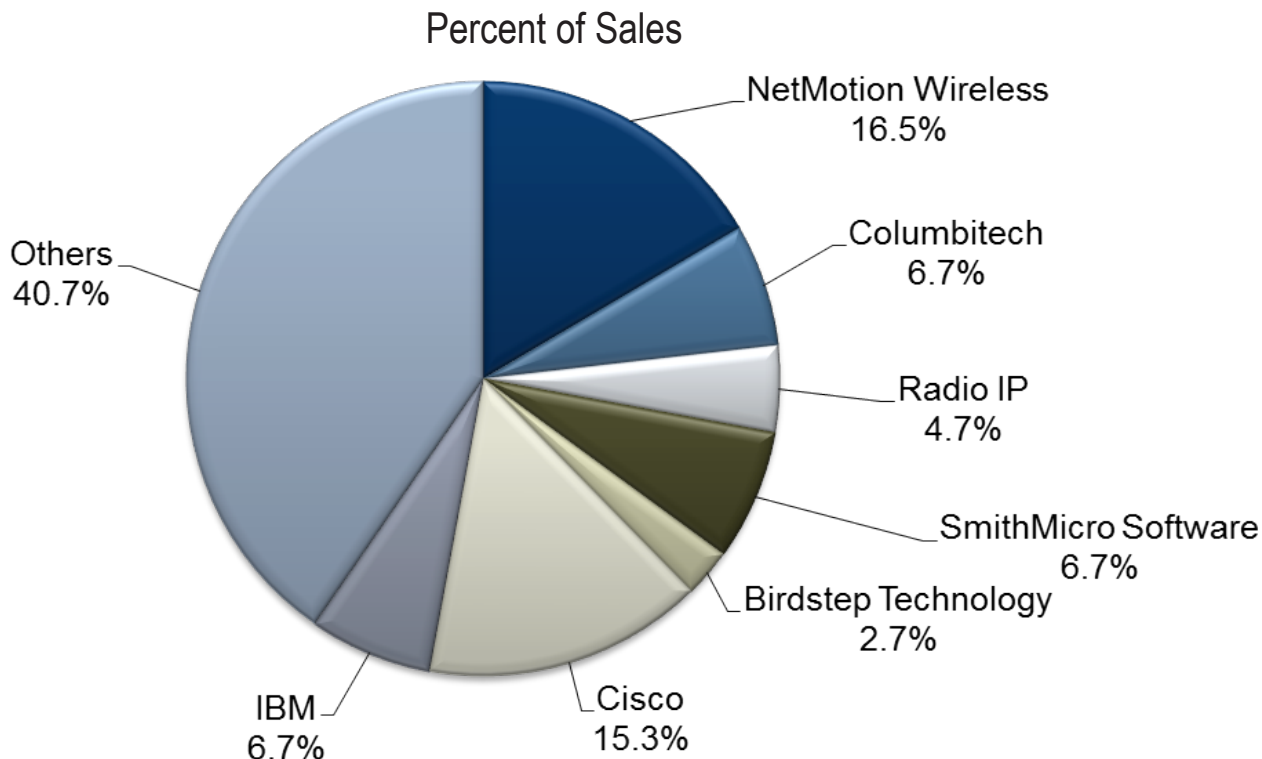
The healthcare vertical generated $16 million in revenue in the total global mobile VPN market. In 2010, this segment represented 10 percent of the global mobile VPN market. The healthcare vertical is made of hospitals and other healthcare facilities.

The healthcare vertical has been a key adopter of SSL VPNs and Virtual Desktop Infrastructure (VDI). Meeting HIPAA compliance has increased the need to secure data on mobile devices—the effort to meet these compliance regulations will create strong traction for this market globally.

Field workers, physicians, and medical staff are being given more access to confidential medical records and other healthcare applications through wireless networks; therefore, the need to protect this data in transit will help spur the growth of the healthcare vertical. Home healthcare and telemedicine is driving the addition of more wireless devices and with required compliance legislations, such as HIPAA and HITech, mobile-device security be at the forefront of deployments.

The utilities vertical is comprised of gas, electric, and energy companies. The utilities segment has adopted mobile VPN solutions in order to provide continuous application sessions and seamless roaming capabilities to field service workers. Field service workers within the utilities vertical are also utilizing this solution to process orders and respond to service inquires more efficiently and effectively.

**FROST & SULLIVAN**

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Market Share and Competitor Analysis

## Percent of Sales



- NetMotion Wireless 16.5%
- Columbitech 6.7%
- Radio IP 4.7%
- SmithMicro Software 6.7%
- Birdstep Technology 2.7%
- Cisco 15.3%
- IBM 6.7%
- Others 40.7%

Other vendors include: Anthasoft, Broadbeam (A Mobileaware Company), Check Point Software, Cryptzone, Fortinet, Good Technology, Juniper Networks, NCP Secure Communications, NetSeal Mobility, RIM, The Green Bow, and WatchGuard

Note: All figures are rounded. The base year is 2010. Source: Frost & Sullivan analysis.

**Key Takeaway: Consolidation and acquisition is expected as Tier I network security companies broaden their mobile security portfolio**

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Market Share Analysis

The top five mobile participants contributed 55.1 percent of total market revenue. NetMotion Wireless leads the competition in 2010 with 16.5 percent of revenue. NetMotion Wireless developed relationships with wireless carriers early in the market, and these relationships have proven to be favorable for the company. In addition to existing partnerships, NetMotion's early market entrance has also enabled the company's success in the mobile VPN market.

Cisco is a top integrator in the market, and its always on approach for remote access has enabled the company to gain a strong market entrance in the enterprise market. Cisco ranked second next to NetMotion with $23 million in revenue for 2010.

Mobile VPN Products Market: Company Market Share
Analysis of Top Participants Global, 2010

| Companies | Revenue (%) |
|---|---|
| NetMotion Wireless | 16.5 |
| Cisco | 15.3 |
| Columbitech | 6.7 |
| SmithMicro Software | 6.7 |
| IBM | 6.7 |
| Radio IP | 4.7 |
| Birdstep  Technology | 2.7 |
| Others | 40.7 |
| **Total** | **100.0** |

\* A list of "Other" companies can be found at link to slide in appendix.
Note: All figures are rounded. The base year is 2010.
Source: Frost & Sullivan analysis.

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Competitive Environment

Competitive Structure, Global, 2010

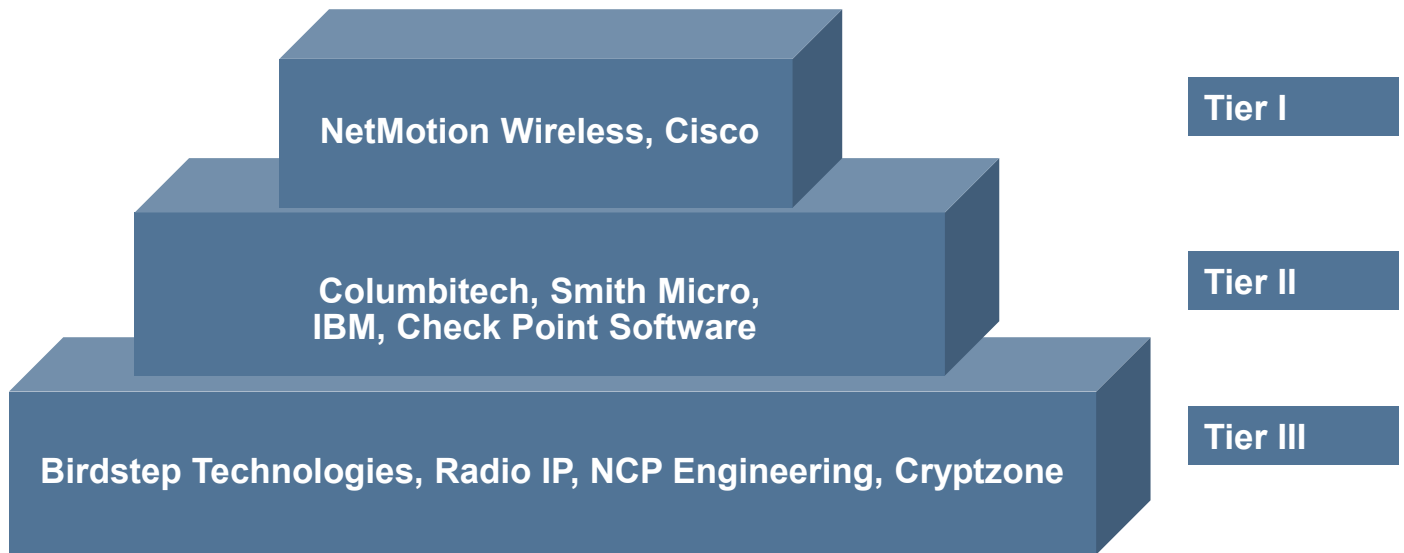| Number of Companies in Market | 19 with revenue greater than $1M USD |
|---|---|
| **Competitive Factors** | Price, performance, partnership relationships, technology, security features, ease of use, easy end-user experience |
| **Key End-User Groups** | Government, healthcare, utility, financial, and retail industries |
| **Major Market Participants** | NetMotion Wireless, Cisco |
| **Market Share of Top 10 Competitors** | 59.3% |
| **Other Notable Market Participants** | Green Bow, MobileAware, Cryptozone, Check Point Software, NCP Engineering |
| **Distribution Structure** | VARs, D Wireless Carriers, integrators, OEMs, and direct sales |
| **Notable Acquisitions and Mergers** | Radio IP purchased ipUnplugged in 2009; Cryptozone acquired Appgate in 2009 |

## Competitor Growth Analysis
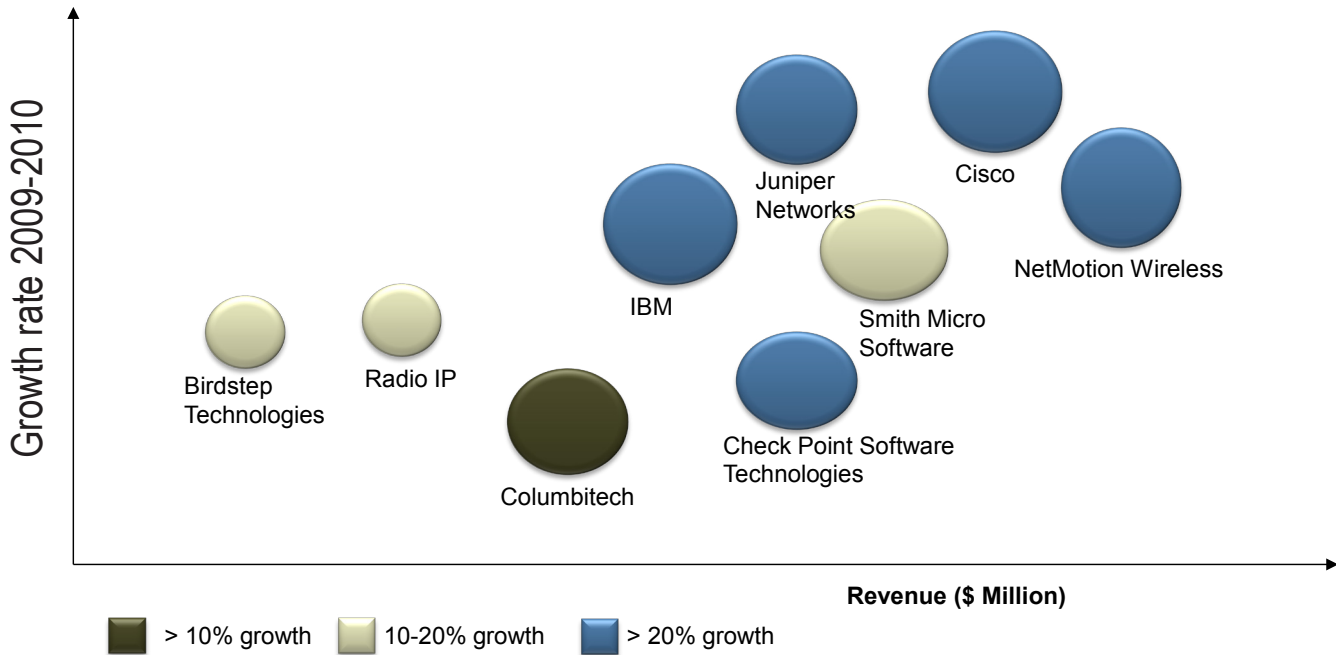


Note: Bubble size represents relative capitalization.
The base year is 2010. Source: Frost & Sullivan analysis.

**Key Takeaway: The highest penetration rates are expected to come from Cisco, Juniper, and NetMotion Wireless**

**FROST & SULLIVAN**

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Tier Analysis



There are three tiers of competitors in the global mobile VPN security market.

- NetMotion Wireless and Cisco were the Tier I market competitors that dominated the market, with a combined share of 42.5 percent in 2010.

- Tier II companies, including Columbitech, IBM, and Check Point Software, were considered challengers or contenders, with a strong presence in the market.

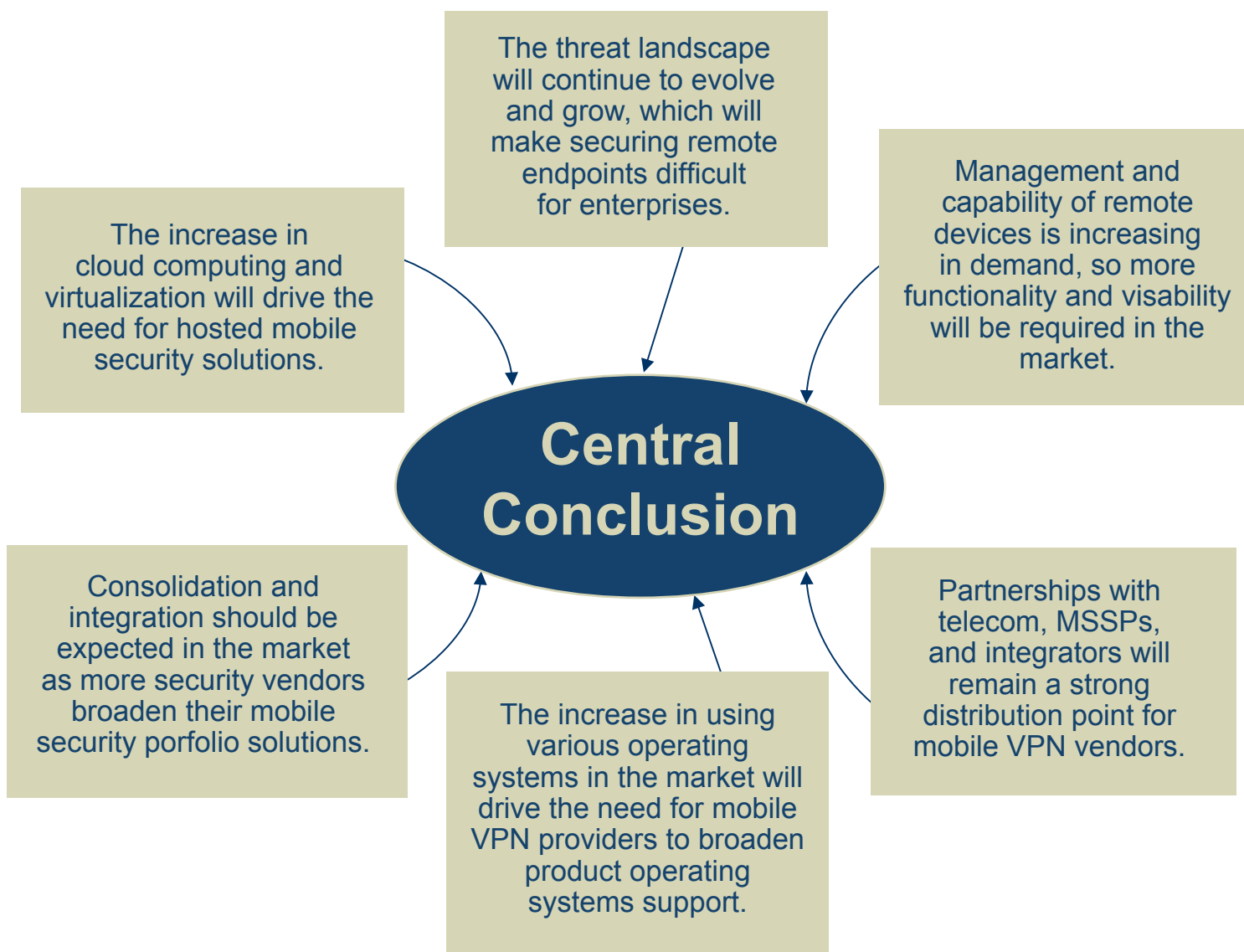- Tier III companies had a smaller presence in the market, primarily niche markets.

FROST & SULLIVAN

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# Competitive Factors and Assessment

Notable Key Partnerships by Vendor, Global, 2010

| Company | Partnerships |
|---------|--------------|
| NetMotion Wireless | AT&T, Verizon Wireless, Microsoft, T-Mobile, Sprint, Sysbase iAnywhere, Sierra Wireless |
| Columbitech | Motorola Symbol, Ericsson, Tella, Verizon Business, HP Invent |
| Birdstep Technology | Nokia, Ericsson, Cisco, Microsoft |
| Radio IP | Bell Canada, Comintel, Rogers, Motorola |
| NCP Engineering | WatchGuard, T-Mobile, Verizon Wireless |
| Smith Micro Software | AT&T, Bell Canada, Sprint, T-Mobile USA, Verizon Wireless, Vodafone |
| MobileAware | AT&T, RIM, Certicom, Motorola, Ericsson, Sprint, Sierra Wireless, Verizon Wireless |

**F R O S T  &  S U L L I V A N**

**Global Mobile VPN Products Market**: Meeting the Wireless Security Challenge with an Emerging VPN for the Remote Worker

# The Last Word

## The Three Big Predictions

1. Consolidation and integration are inevitable in the mobile VPN market.

2. Partnering with integrators, telecom and managed security providers (MSSPs) will enable stronger growth in the mobile VPN market.

3. Support for various platforms for mobile devices will remain crucial as the demand for smartphones and tablets continues to increase.

The threat landscape will continue to evolve and grow, which will make securing remote endpoints difficult for enterprises.

Management and capability of remote devices is increasing in demand, so more functionality and visability will be required in the market.

The increase in cloud computing and virtualization will drive the need for hosted mobile security solutions.

**Central Conclusion**

Consolidation and integration should be expected in the market as more security vendors broaden their mobile security porfolio solutions.

The increase in using various operating systems in the market will drive the need for mobile VPN providers to broaden product operating systems support.

Partnerships with telecom, MSSPs, and integrators will remain a strong distribution point for mobile VPN vendors.

## Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers' acknowledge, when ordering or downloading, is that Frost & Sullivan Research Services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100, Mountain View, CA 94041