Secure Enterprise Mobility℠:
Challenges and Solutions

Sprint

Together with Nextel

Executive Summary

The steadily increasing power of wireless-enabled computing devices has reached a point where productivity options for the mobile professional are abundant and rival what can be accomplished in the traditional office environment. Handheld wireless devices today have processing and storage capabilities analogous to laptop computers of just a few years past and include multiple network connectivity options for ubiquitous access to information. Use of these devices can increase productivity, reduce costs, decrease time to market, increase customer satisfaction, improve employee retention, and enhance revenue.

However, with this ability to make nearly all corporate data available to the handheld user, new security concerns arise. Mobile devices are new endpoints in an IT network infrastructure that is threatened by viruses, spyware, spam, hacker attacks, denial-of-service attacks, insider attacks, and other threats. Wary of the consequences of allowing un-secured data to reach the network edge, enterprises have been reluctant to adopt the breadth of wireless productivity options available to them.

In a complex and dynamic marketplace, enterprises require a comprehensive, integrated solution for secure, policy-compliant access to the breadth of corporate resources from mobile devices. Yet most of the security marketplace is fragmented, with a large number of vendors offering point solutions, each of which only address a portion of the overall security problem. This confused, fragmented model has continued in the mobile security world. This document provides more information on the challenges and opportunities of the mobile enterprise, suggests best practices for addressing mobile enterprise security, summarizes the mobile security solution provider marketplace, and describes the Sprint Secure Enterprise Mobility℠ solution.

Table of Contents

	Page
Growth in Mobile Device and Network Adoption	1
The Benefits of Mobility	1
The Security Challenges that Mobility Poses	1
The Current State of Wireless Security	2
Unanswered Questions	3
How to Address this Challenge: Best Practices	3
The Marketplace: Who Offers Potential Solutions?	5
The Sprint Solution	5
Conclusion	6
For More Information	7
References	8

Growth in Mobile Device and Network Adoption

Mobile communications are becoming an accepted part of life. By 2000, 55 percent of the U.S. population had a mobile phone [1]. Worldwide, one analyst predicts that there will be about 2 billion cell phone subscriptions on the planet by the end of 2005, cementing "the mobile phone's position as the most rapidly-growing and widely-accepted technology of all time [2]." Not surprisingly, enterprise adoption of mobility has risen dramatically as well. The portion of employees that are considered to be "mobile" has increased from 35 percent in 2003 to 38 percent in 2004, and 40 percent in 2005. Today, approximately 50 million U.S. workers are mobile [3]. This rise in enterprise mobility has occurred so quickly that in mid-2005, "35 percent of executives ... were unaware their companies use wireless (access) [4]."

Mobile employees are using handheld devices, such as PDAs, Smartphones, converged devices and Blackberries, as well as laptop computers, for a range of business applications. In addition to email and messaging, these applications could include sales force management, fleet management, work order and dispatch, and procurement as well as a range of medical, financial, transportation, distribution, and other applications. These devices communicate via cradle synchronization, wired networks, Wi-Fi, Bluetooth, wide area wireless networks, and others, enabling employees to access sensitive information that is internal to the enterprise from the outside. At the same time, the storage capability of these devices has risen dramatically, enabling them to store large amounts of corporate information. Many of these devices now also include built-in cameras and microphones, enabling them to take photographs and record conversations [5].

The Benefits of Mobility

The benefits of enterprise mobility are significant, pervasive, and comprehensive. Benefits of mobility can include productivity gains, reduced operating costs, decreased cycle times, increased customer and employee loyalty, competitive differentiation, and revenue growth via the offering of new products and services. In a May 2005 research report, Aberdeen found that "Companies that utilize work order optimization and mobile field service solutions have seen such performance gains as a 28 percent increase in work orders completed per day per technician, an 11 percent jump in first-call resolution rates, and a 16 percent reduction in work orders completed late [6]."

Tempted by benefits like these, the extent of enterprise mobility is expected to continue to expand rapidly. By 2010, one group predicts that 80 percent of key business processes will involve the exchange of real-time information and mobile workers [7]. With the 3G buildout, as wireless network speed increases, the range of mobile applications deployed is likely to expand during this period as well.

Hence, failing to deploy wireless applications to the mobile workforce is a missed business opportunity. The enterprise that fails to deploy these applications is likely to face competitors that will deploy them, or that have already deployed them. Conversely, deploying wireless applications can be a powerful differentiator.

The Security Challenges that Mobility Poses

However, along with these benefits, new security concerns arise. "Mobile security is one of the fastest growing sectors in the wireless space and it is a priority for everybody, from operators to device manufacturers to silicon vendors to the mobile software and middleware vendors," explains Yankee Group analyst John Jackson [8].

Simply allowing a mobile device to fall into the wrong hands poses problems, as the confidential information stored in the device may be easily retrievable (if not properly protected). One firm recently reported the theft of a laptop computer that contained personal information on approximately 16,500 current and former employees of a major telecommunications firm [9]. One study showed that travelers left 85,000 mobile phones, 4,500 laptops, and 21,000 PDAs in Chicago taxis over a six-month period [10].

But security issues extend considerably beyond misplaced devices. Many of these devices are vulnerable to attack. In 2004, Gartner estimated that "approximately 90 percent of mobile devices lack the protection to ward off attackers [11]."

Another area of mobile security concern is the ubiquitous nature of viruses and malicious code or malware. A key application of mobile devices, including laptops,

is email, and email was the transmission mechanism for 92 percent of viruses in 2004 [12]. One analyst explains that "when you think that there are more mobile devices than computers, you stop to think about the impact that a virus could have [13]." Looking ahead, one analyst predicts that malicious programs will be as much a problem for cell phones in 2006 as they are for computers today. "First it will be a nuisance. The next phase will be crime, like theft or theft of service, and then after that we'll start seeing different types of attacks [14]."

At the same time, the complexity of managing mobile devices is increasing, while high bandwidth networks proliferate. The number of access points to the network, connection methods, and transport methods has grown, adding to the difficulty of managing and protecting these devices inside and outside of the office (see Figure 1). In 1990, network access was typically accomplished via a limited number of access points and methods- either a LAN or dial-up telephone line provided access for a desktop computer. Today, the access locations have grown to also include the home, cafes, convention centers, airports, parks, and many others; connection methods have grown to also include cable modem, DSL, VoIP, WiFi, cellular and others; and, in addition to laptops, access devices now also include tablet PCs, PocketPCs, Personal Digital Assistants (PDAs), and a range of cellular phones. The latter complicates access control, as employees connect their personal mobile devices to corporate networks.

The cost of inadequate mobile security can be significant. A study of the MS Blaster worm, for example, which entered company networks most often through infected laptops, showed remediation costs of $475,000 per company. Larger node-count companies reported losses of up to $4.2 million [15].

Another way to examine the potential costs of inadequate mobile device security is to consider the cost of cybersecurity breaches in general. This is a valid consideration because mobile devices pose yet another endpoint in an enterprise network that already suffers from costly security vulnerabilities. According to the most recent CSI/FBI Computer Crime and Security Survey, the total cost of security breaches from 269 survey respondents that were able to quantify costs was about $141 million or approximately $500,000 per respondent. In this survey, the top five types of losses were due to viruses, denial of service, theft of proprietary information, insider net abuse, and abuse of wireless network [16].

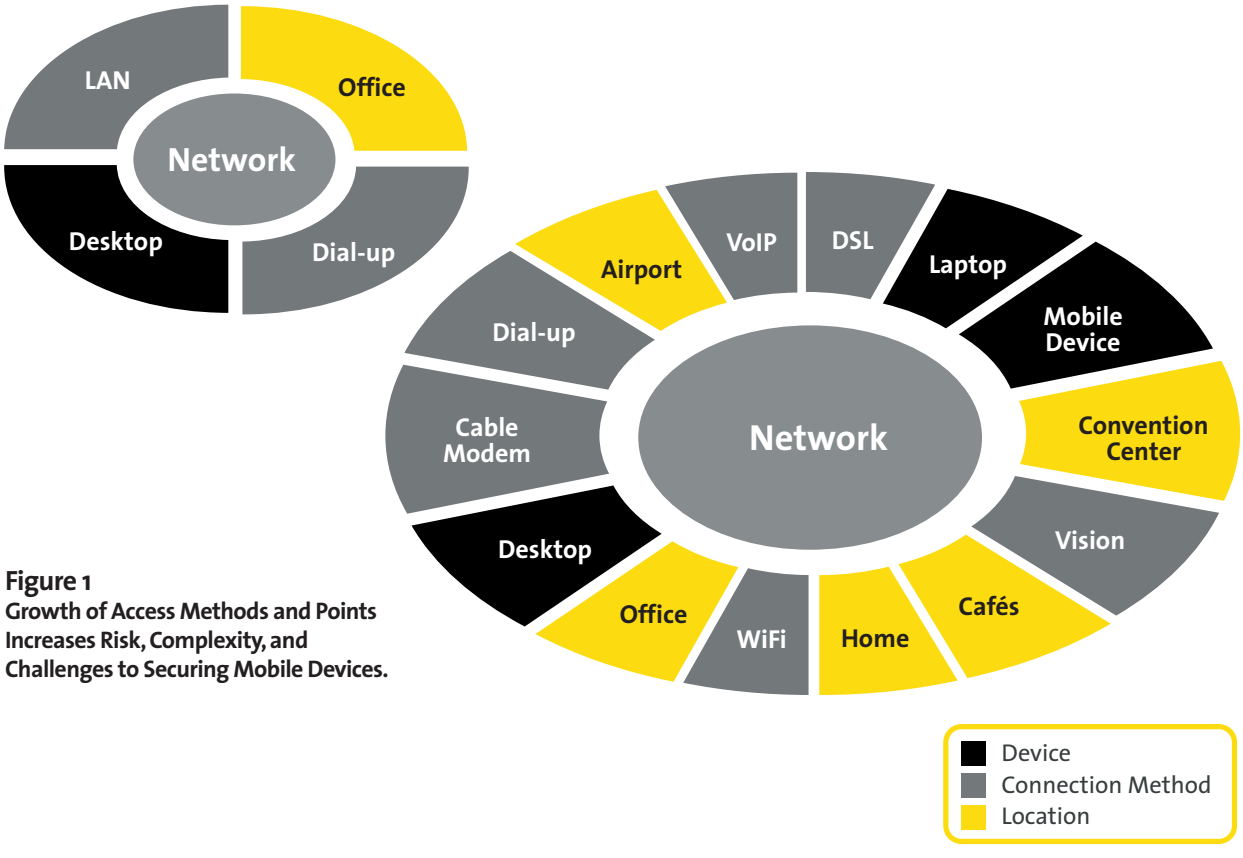

Figure 1
Growth of Access Methods and Points Increases Risk, Complexity, and Challenges to Securing Mobile Devices.

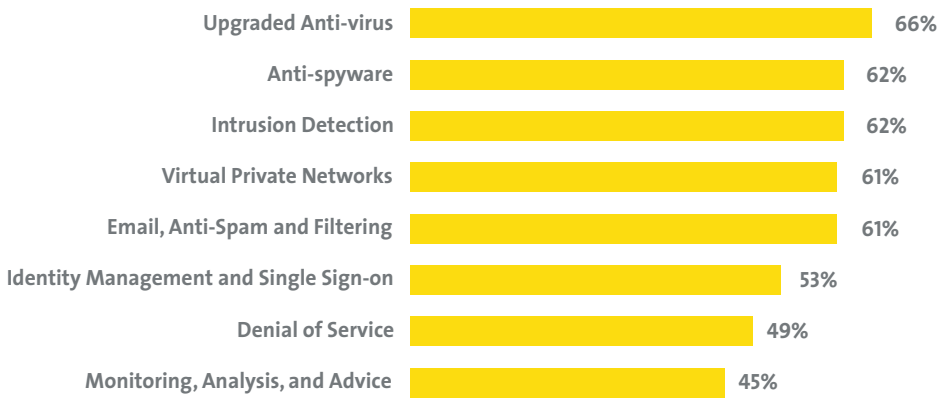

Figure 2
Features of a Mobile Security Solution that Mid and Large Businesses Most Desire [17]

The Current State of Wireless Security

Of those organizations that have established security policies for mobile devices, many strictly limit remote wireless access to corporate resources and applications in an effort to keep information security policy enforced. This restrictive policy contradicts the overall value proposition of mobile productivity. Limiting the use of complex mobile devices to email and other simple applications may effectively comply with security concerns, but curtails the significant mobile productivity gains that can be achieved with full remote corporate access from the handheld.

Many savvy businesses are concerned about wireless security. In a recent survey of 415 companies, 69 percent of respondents were "highly concerned" about wireless security, and 32 percent rated it the highest concern possible [17]. Another way to look at security is to view it as a barrier to deploying mobility. A recent Yankee Group survey found that respondents ranked security as the foremost barrier to deploying wireless LANs and wireless WANs [18].

Unanswered Questions

In light of these challenges and potential costs, there are many questions that CIOs and network administrators can ask themselves within the scope of mobile enterprise security:

- Who has access to corporate data?
- Are all users compliant with corporate security policies?
- What kind of data is exposed in a misplaced or lost Smartphone?
- Who are the mobile users in the enterprise, and are all mobile devices secured?
- Which mobile devices and users are accessing corporate applications?
- Are mobile users accessing via rogue (unsecured) access points?
- Do users have the latest anti-virus applications and up-to-date firewall policies?
- Are mobile users losing productivity due to manual remediation?

For many enterprises, consideration of these security questions raises significant concerns. Gartner predicts that "one of the greatest challenges CIOs will face is the proliferation of wireless devices … the biggest threat to the enterprise will come from the increasing demand for access from new devices owned by employees that cannot be locked down and secured by the enterprise [19]." Adequately addressing these concerns requires a comprehensive solution for secure, policy-compliant access to the breadth of corporate resources from the handheld device.

How to Address this Challenge: Best Practices

Addressing mobile security issues requires both establishment of policies and implementation and enforcement of these policies via a combination of technological solutions. On the policy side, both corporate and regulatory policies are relevant. Corporate policies must address who is permitted to access what information, what actions are permitted and prohibited, and what actions are required. These policies must also define the roles and responsibilities of various stakeholders in the organization, and address not only employees, but also contractors, customers, partners, and others. Relevant regulatory policies include Sarbanes-Oxley, NIST FIPS 140-2, HIPPA, the Gramm-Leach-Billey Act, California Law SB1386, the U.S. Government Information Security Reform Act (GISRA), and others.

Implementation and enforcement of these policies requires a range of technologies. A recent survey of Sprint customers revealed interest in the security areas shown in Figure 2 in any mobile security solution.

Endpoint access control is a key layer of mobile security that has not been fully addressed. Yet, an effective mobile security solution must focus on the end points requiring access. For it is these endpoints (wireless devices, laptops, etc.) that are most susceptible to corruption, and if unsecured, provide an open window into the corporate network. Endpoint threats include unauthorized rogue access points, mobile device theft, misuse of public web applications, abuse of the wireless network, and others. When not connected to the corporate network with their mobile device, mobile workers frequently gain access to the Web from home, public WiFi hotspots, hotels, and other locations, even if such actions disobey established company policies. These actions can expose the corporate network to a range of threats, including viruses, malware, denial of service attacks, unauthorized access, and others.

More specifically, a strategic security deployment for end-to-end mobile deployment within organizations must include measures to address three key areas: control, compliance, and cost. With regard to control, IT security must extend corporate policy enforcement to company-owned and individual-owned mobile devices, without affecting productivity or security. Control requirements include:

- Gain visibility and understanding of the enterprise mobile environment
- Establish a flexible framework to set and maintain enterprise and end-user policies
- Implement centralized IT device monitoring and reporting capabilities
- Provide a scalable solution that grows with the demands of the business
- Ensure that the solution is easy to procure and deploy throughout the enterprise

With regard to compliance, companies must ensure that software is current, secure, and auditable. Compliance requirements include:

- Ensure that corporate policies remain consistent from device to device
- Ensure that company policies meet regulatory guidelines
- Minimize the risk of exploits and security breaches
- Ensure the privacy of corporate data from security breaches

Figure 3
No single provider of these types offers the comprehensive, integrated solution that is needed. (Note: this table is current as of 8/15/05. Analysis compares categories as a whole; offers may vary among specific providers.)

Absent ○ ◔ ◑ ◕ ● Strong Offer

Differentiator	Wireless Network Providers	System Integrators	Software Providers	Hardware Providers
Mobile Security Solution Providing Endpoint Access Control for Mobile PCs, Smartphones, and PDAs	◔	◑	◑	◔
Wireless Remediation Services for Mobile PCs, Smartphones, and PDAs	○	◔	◑	○
Flexible Mobile Security Solution Offer with Options: • Personal Firewall • Mobile Anti-virus • On-device Encryption • Email Protection and Message Archiving	◔	◕	◕	◔
Offers Managed Mobile Device Services	○	◑	◔	○
Can Provide Mobile Security for Multiple Operating Systems (PCs, Pocket PCs, and Palm Mobile devices)	◔	◕	◕	◔
Wireline, Cellular, and WiFi Network Service Provider with Proven Security Services	◑	○	○	○
Experienced Support for Laptops, PDAs, and Handheld Computing Devices	◕	●	○	◑

With regard to cost, the solution must balance a company's existing security investment with new solutions that are flexible enough to meet growing business needs. Cost considerations include:

- Increase productivity to increase ROI
- Reduce cost of compliance
- Reduce loss of revenue from fines
- Reduce potential losses from threats which damage the corporate image
- Reduce burdens on help desks
- Consider a single source provider to reduce total cost of ownership (TCO)

The Marketplace: Who Offers Potential Solutions?

A comprehensive, integrated solution for mobile security is needed. However, in today's security marketplace, network threats are generally treated as individual problems, and "point-solution" countermeasures are tailored to address each individual threat. The mobile security market remains fragmented, as different vendors provide point solutions for endpoint encryption, authentication, anti-spam, anti-spyware, anti-virus, and other solutions, each of which needs to be implemented using mobile middleware. This means that current security vendors are limited in their ability to provide integrated and complete mobile security. Unfortunately, this fragmented, reactive approach becomes increasingly complex, inefficient, and expensive as more threats evolve.

Figure 3 shows additional requirements of a comprehensive, integrated mobile security solution. These required attributes include wireless remediation services, flexible offerings, managed service options, ability to offer solutions across operating systems, etc. The figure also estimates the ability of various types of entities to provide such a solution. Wireless network providers, system integrators, software providers, and hardware providers provide various pieces of the puzzle individually, with varying levels of sophistication. Clearly, no single provider offers the comprehensive, integrated solution that is needed.

The Sprint Solution

The Sprint Secure Enterprise Mobility (SSEM) service enables enterprises to extend IT resources to the mobile workforce with a security solution that enables compliance, strengthens control, and reduces costs. SSEM is a managed endpoint access control framework that provides device authentication, interrogation, and remediation services. It enables secure access to corporate resources from mobile-enabled endpoints, such as laptop computers with wireless connection cards and wireless PDA/handheld computing devices. The interrogation process provides a barrier against exploits such as viruses, worms, and other malicious applications. This access control solution provides "end-to-end" security that seamlessly protects the device and the corporate network at the software level, both internally and externally, as data is accessed from various locations.

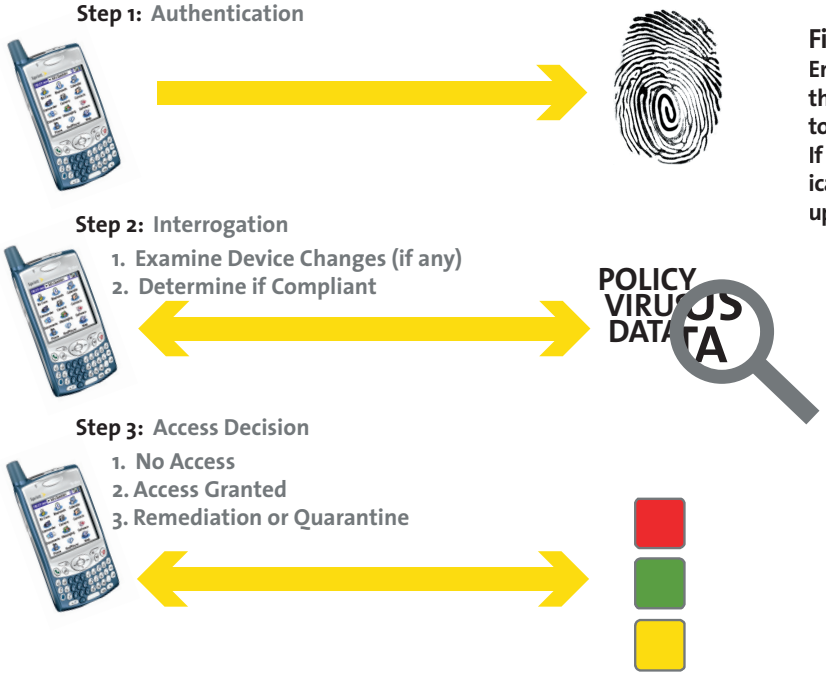

Figure 4
Endpoint access control involves authenticating the user (step 1), then interrogating the device to determine if the user is granted access (step 2). If denied access, the user is redirected to automatically remediate the errors and is granted access upon successful software patch installation (step 3).

Figure 5
The Sprint solution provides a range of services and business benefits.

SSEM Services	Benefits
Mobile Anti-virus	Detects and protects against viruses that target mobile-enabled devices.
Mobile Personal Firewall	Prevents intrusion and ensures end-user access is compliant with corporate security policy.
On Device Encryption	"Locks" files/folders, device memory, hard drives, and removable storage, such as SD cards, flash media, and USB drives.
IP VPN	Ensures security and integrity of data when traversing public networks.
Intrusion Detection	Identifies threats that go unnoticed by firewalls and VPNs by maintaining up-to-the minute intelligence of the access issues that threaten the network.

As shown in Figure 4, "power on" user authentication (step 1) and "on device" encryption prevents local access onto the device, while device authentication helps protect against unauthorized network access. The device interrogation step examines the device to ensure that all software (virus protection, applications, personal firewall, etc.) is properly configured, up-to-date, and compliant with company policy. (This identifies if a user, virus, worm, or other malicious application has altered the security policy on the device.) In step 3, remediation services automatically fix any issues (discovered during interrogation) needed to comply with the security policy and enable the user to gain access. This interrogation and remediation is effective - not just for company-owned laptops and handhelds/PDAs, but for those devices owned by employees, as well.

Endpoint access control enhances the enterprises' ability to:

- Ensure privacy and intellectual property protection
- Defend against hacker activity (e.g., worms, distributed denial-of-service attacks, and viruses)
- Ensure seamless access to business-critical applications and services
- Assure business and financial integrity
- Limit insider abuse
- Protect against industrial espionage
- Enforce corporate security policies to assure regulatory compliance
- Ensure device security and integrity of data when traversing over public networks
- Simplify mobile-enabled device control and management

SSEM offers the following key capabilities:

- *Easy, automated remediation.* Endpoint access control automatically processes and distributes updates and services after authenticating and interrogating each device, providing secure user access and enforcing corporate security policies.

- *Integrated mobile security based on generally available wireline standards today (wireline equivalent).* Sprint is one of the first to offer a complete suite of managed security services for mobile PDAs and smartphones. The security suite also extends to mobile data cards for WiFi, CDMA, EV-DO, and GPRS access.

- *Carrier agnostic service.* Sprint's integrated security suite supports all wireless providers, reaching a broad wireless access user base.

- *Seamless integration into the existing IT infrastructure.* Sprint has done the integration work, enabling SSEM to function as an extension to the existing environment.

- *Over-the-air deployment of security software and applications.* OTA relieves users of time spent manually updating and installing applications on their devices, and ensures that all mobile devices are always compliant with company and regulatory policy.

Sprint also offers optional security features and services, enabling comprehensive security policy enforcement (see Figure 5).

Conclusion

As technology allows the mobile workforce to connect to the enterprise at near wireline speeds, the need to provide increased security for mobile devices will grow to be a business imperative. Mobile-enabled devices are increasingly becoming more powerful and capable of a wide variety of services and features. Today's PDAs and handheld computers have computing abilities analogous to laptop computers of only a few years ago. While mobile computing drives enormous increases in productivity and communication, it also means a greater proliferation of sensitive and mission-critical business information is stored at, or passing through, many different access points. Organizations that are not examining the potential security risks now will lose valuable time in the race to comply with regulations, adopt technology, and avoid the cost of lost productivity, or lost data, due to an attack. Moreover, the customers of enterprise businesses demand that their sensitive data be secure at all times.

Organizations with highly sensitive information must find ways to enforce corporate security policies on all company-owned and individual-owned mobile devices while providing easy remote access to corporate resources. Sound security policy is necessary to take advantage of advanced mobile device capabilities beyond simple email and calendar middleware applications.

As Figure 6 demonstrates, Sprint is the only stakeholder that provides a complete enterprise mobility solution. Sprint Secure Enterprise Mobility is an endpoint access control framework for secure access to corporate resources from mobile-enabled endpoints, such as laptop computers with wireless connection cards and wireless PDA/handheld computing devices. The framework is carrier agnostic and provides seamless integration with existing IT infrastructures. Features include built-in user authentication and device interrogation, which provide a barrier against dangers, such as unauthorized user access, viruses, worms, and other malicious applications, and automated remediation services that fix any security issues that prevent network access.

For More Information

For more information on Sprint Secure Enterprise Mobility, contact your Sprint representative or visit us at www.sprint.com/business or email us at MobileBusiness@sprint.com

Figure 6

This table shows that Sprint is the only stakeholder that provides a complete enterprise mobility solution. (Note: This table is current as of 8/15/05. Analysis compares categories as a whole; offers may vary among specific providers.)

Absent ○ ◔ ◑ ◕ ● Strong Offer

Differentiator	Sprint Solution	Wireless Network Providers	System Integrators	Software Providers	Hardware Providers
Mobile Security Solution Providing Endpoint Access Control for Mobile PCs, Smartphones, and PDAs	●	◔	◑	◑	◔
Wireless Remediation Services for Mobile PCs, Smartphones, and PDAs	●	○	◔	◑	○
Flexible Mobile Security Solution Offer with Options: • Personal Firewall • Mobile Anti-virus • On-device Encryption • Email Protection and Message Archiving	●	◔	◕	◕	◔
Offers Managed Mobile Device Services	●	○	◑	◔	○
Can Provide Mobile Security for Multiple Operating Systems (PCs, Pocket PCs, and Palm Mobile devices)	●	◔	◕	◕	◔
Wireline, Cellular, and WiFi Network Service Provider with Proven Security Services	●	◑	○	○	○
Experienced Support for laptops, PDAs, and Handheld Computing Devices	●	◕	●	○	◑

References

1. "Comparing internet and mobile phone usage: digital divides of usage, adoption, and dropouts," Ronald E. Rice and James E. Katz, Telecommunications Policy 27 (2003) 597-623.
2. Deloitte, "TMT Trends: Predictions, 2005, a focus on the mobile and wireless sector."
3. "Increasing and Improving Productivity with Wireless Technologies," Eugene Signorini, Yankee Group, March 14, 2005.
4. John Stehman, Robert Frances Group, as quoted in article by David Ramel, "Mobile & Wireless World: Compliance regs put bite in wireless security," June 15, 2005, Computerworld, http://www.computerworld.com/printthis/2005/0,4814,102503,00.html
5. Eric Maiwald, "Security for Handheld Devices," v1, 21 October 2004, Burton Group Security and Risk Management Strategies Telebriefing, (www.burtongroup.com).
6. Aberdeen Group report, "Field Service Optimization Report-Part 2 Synchronizing Supply and Demand in Right Time," May 2005.
7. "Hi-Tech Crime, The Impact on UK Business," National Hi-Tech Crime Unit, 2005, http://www.nopworld.com/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf.
8. John Jackson, Yankee Group, as quoted in Susan Rush article for News@2, "Analyst: Mobile Security is a Top Priority," June 16, 2004, http://www.wirelessweek.com/article/CA522095.html.
9. "MCI employee data stolen in laptop theft," Robert McMillan, IDG News Service, May 23, 2005.
10. "Lost Your Cell Phone? Call a Cab! Taxis across the world are hotspots for misplaced electronic devices," Erin Biba, Medill News Service, February 17, 2005, http://pcworld.com/news/article/0,aid,119702,00.asp.
11. "Gartner Says 90 Percent of Mobile Devices Lack Protection to Ward Off Hackers," Gartner press release, March 26, 2004, http://www.gartner.com/press_releases/asset_63930_11.html.
12. ICSA Labs Virus Prevalence Survey 2004, Larry Bridwell, ICSA Labs.
13. Fredrik Lindstrom, senior security consultant at Computing System Innovations, a solution provider in Orlando, Fla, quoted in article by Matt Villano, "New Security Threats Target Cell Phones, Mobile Devices," March 18, 2005, http://www.crn.com/showArticle.jhtml?articleID=159901521&flatPage=true.
14. John Pescatore, Gartner analyst, as quoted in article, "Hackers target cell phones," PhoneContent.com, November 29, 2004, http://www.phonecontent.com/bm/news/gnews/457-1.shtml.
15. "Blaster worm took heavy tool: survey," Sam Varghese, TruSecure/ICSA Labs, September 23, 2003. http://www.smh.com.au/articles/2003/09/23/1064082983214.html.
16. "CSI/FBI 2004 Computer Crime and Security Survey," Computer Security Institute, http://www.issa-sac.org/docs/FBI2004.pdf.
17. Sprint Customer Survey of 415 wireless voice/data decision makers at mid-large size Enterprises (100 employees and over), May 2005.
18. "Creating a Secure Mobile Environment for Business," Yankee Group, 7/22/05.
19. "Gartner Outlines Key Trends for Mobile Technology and Subscriber Evolution" Gartner press release, April 18, 2005, http://www.gartner.com/press_releases/asset_125194_11.html.