

Sprint[®]



Mobile Security

Presented by Barry Tishgart
Director, Product Marketing

September 20, 2006



Agenda

- > The Demand for Mobility
- > Security: The #1 Barrier to Wireless Adoption
- > Mobile Security Threats
- > Customer Challenges
- > The Solution: Sprint Mobile Security
 - Data Protection
 - Threat Prevention
 - Compliance
- > Customer Benefits
- > Case Scenario
- > Integrated Security Policy
- > The Sprint Mobile Security Advantage

The Demand for Mobility

As analyst reports prove, the demand for mobility is growing dramatically:

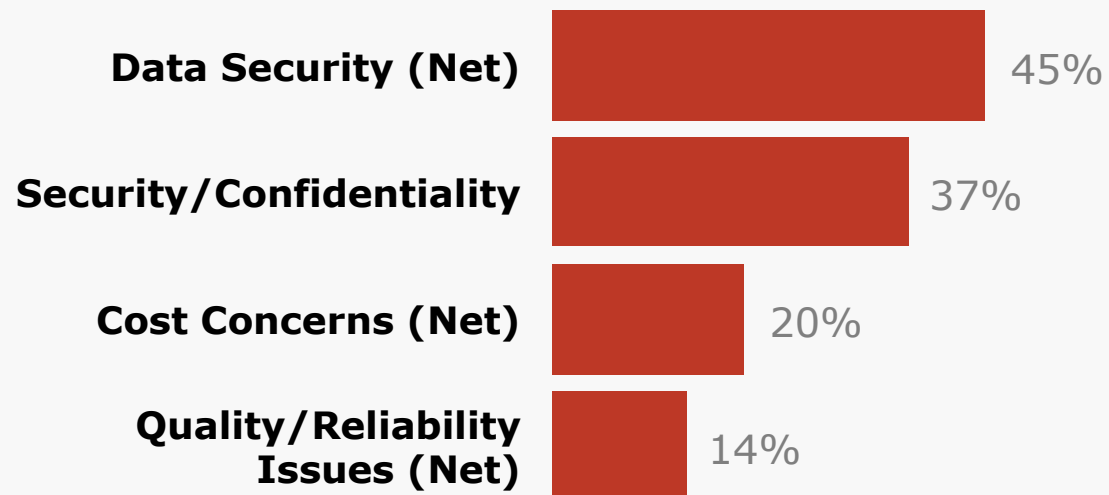
- > “The corporate market for wireless data services is expected to grow by more than 266% in four years”¹
- > “The U.S. wireless data market as a whole is expected to reach \$4.494 billion by 2007”¹
- > “By 2007, 65% of enterprises will deploy wireless applications to their mobile workforce”
- > “The number one management struggle for more than 75% of enterprises is mobile technology”

1. Source: U.S. Business Wireless Subscriber 2004-2008 Forecast, Keith Waryas, IDC 2004

2. Source: MORPACE International, November 2005 Broadband Wireless Optimization & Positioning Study

Security: The #1 Barrier To Wireless Data Adoption

Top Barriers to Business Mobility



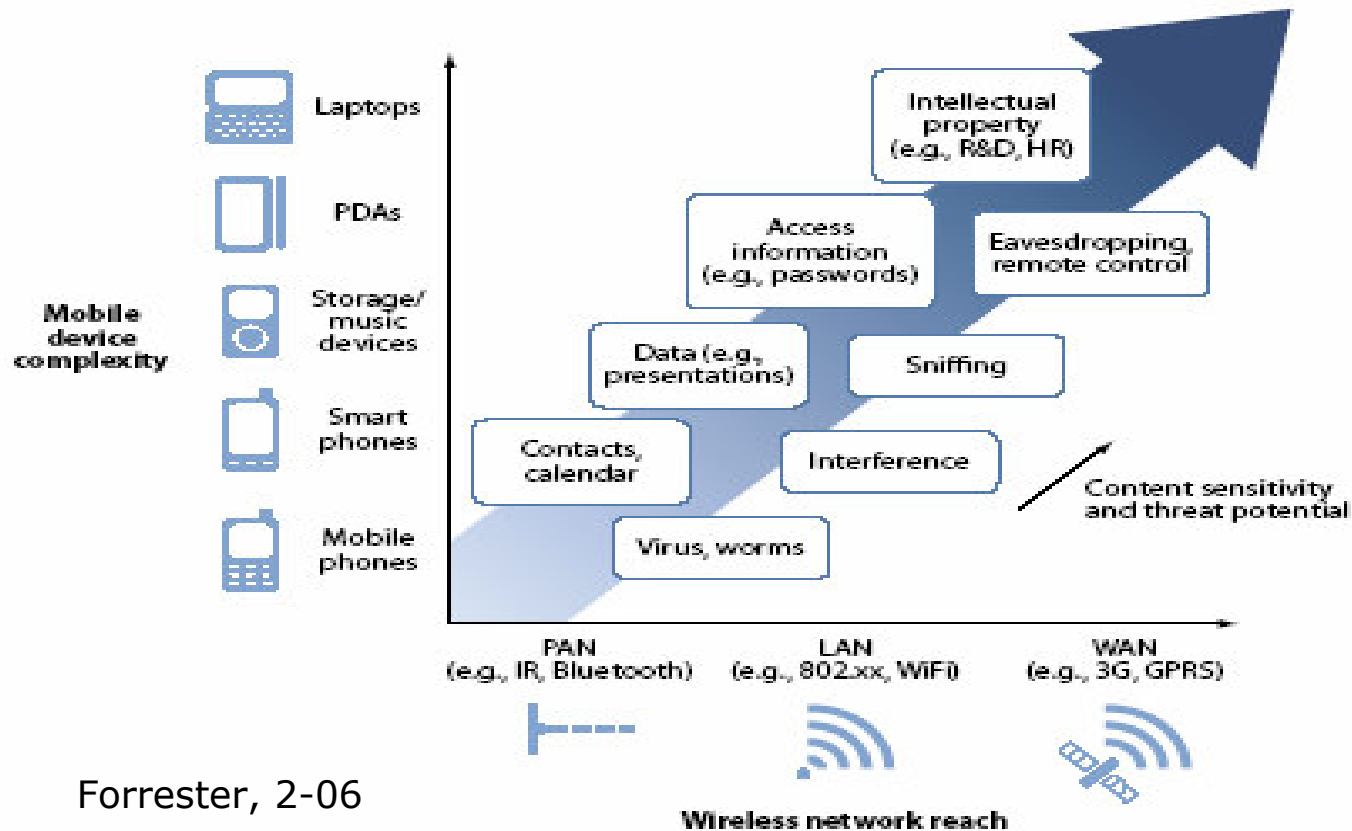
Source: SBS Solution Thrust
Prioritization Study 10/04

“Research indicates that security remains the number-one barrier to deployment of both wireless local-area and wireless wide-area technologies within enterprises.”

— Yankee Group 7/22/05

Why Mobile Security Services will grow

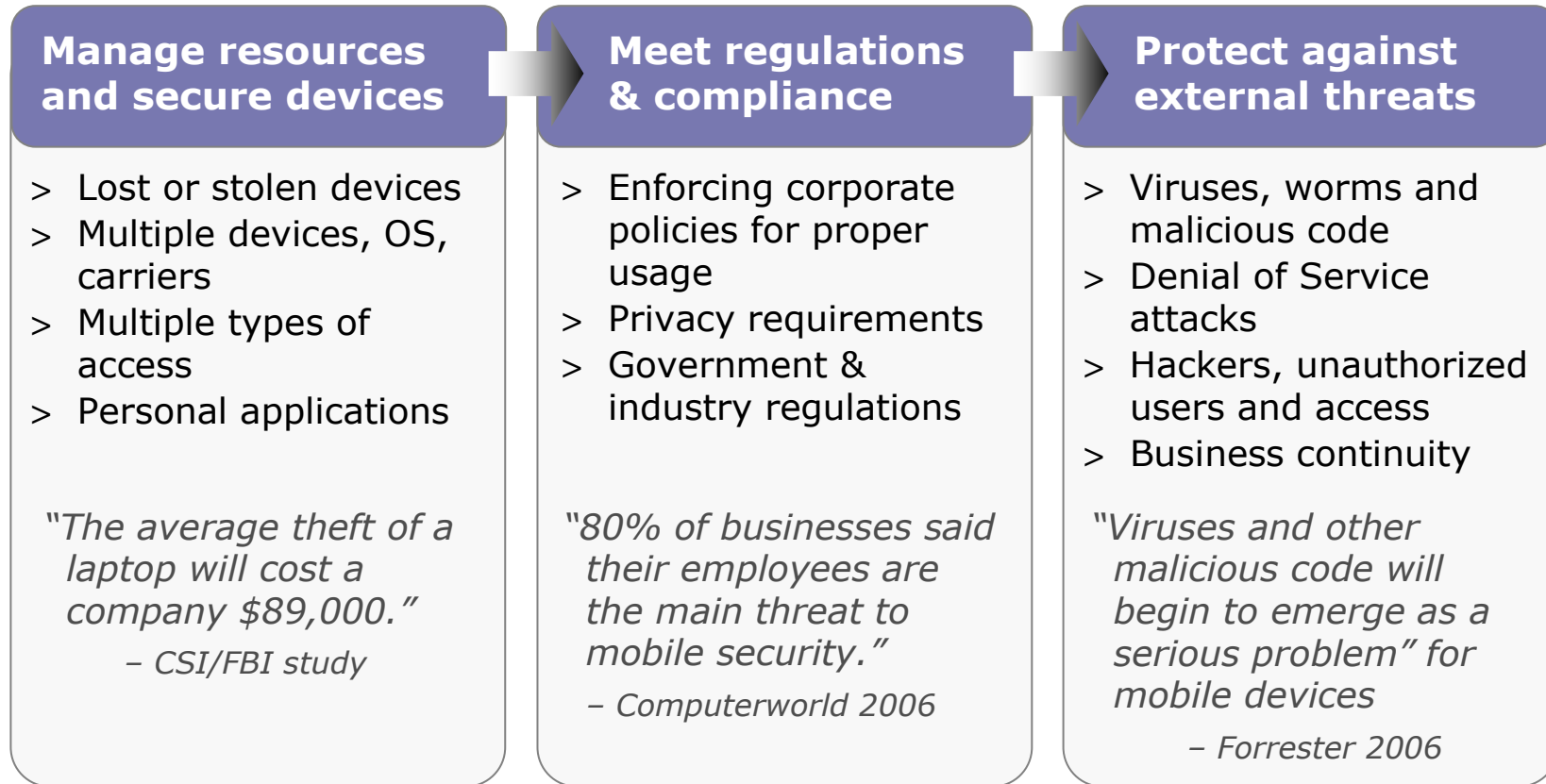
The increase in mobile device complexity increases the potential for security threats.



Forrester, 2-06

Customer Challenges

Companies are faced with increasing complexity in the mobile environment.



The Solution: Sprint Mobile Security

Sprint is the only carrier to offer a complete security solution that allows customers to protect data, prevent threats and enforce corporate policies across laptops and handheld devices.

Security Management Across Multiple Carriers		
Data Protection	Threat Prevention	Compliance
<p>Authentication Enforce password policies across all devices</p> <p>Data Encryption Protect data with AES or 3DES encryption</p> <p>Mobile VPN Allow users to connect to the corporate network</p>	<p>Mobile Firewall Monitor and Control inbound/outbound access</p> <p>Mobile Anti-Virus Detect and protect against viruses exploiting mobile devices</p>	<p>Policy Management Enforce over 150 user and group policies from a single online portal</p> <p>Remediation Update non-compliance programs automatically</p> <p>Asset Management Manage devices and user profiles online</p>

Premium Customer Care with Online Self-care Portal

Data Protection

Secure devices and corporate data with high speed encryption, integrated authentication and access control

Data Encryption:

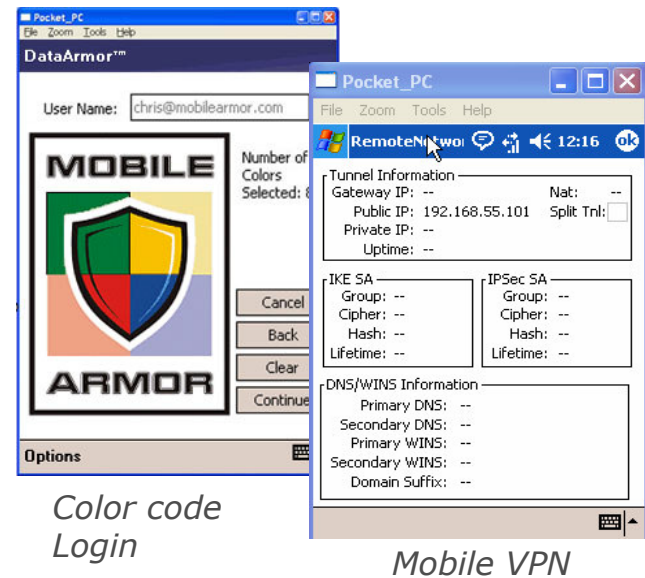
- > Encrypt individual files or an entire device/ memory card with a FIPS 140-2 Certified solution using AES or 3DES Encryption

Authentication:

- > Set password policies with fixed, PIN or color code credentials
- > Create idle time-out policies for devices that have not connected to the network

Mobile VPN:

- > Allow mobile users to access corporate web sites, download files and share data



Color code Login

Mobile VPN

Threat Prevention

Protect mobile devices against threats with device lock & erase, mobile anti-virus and a mobile firewall

Device Lock & Erase:

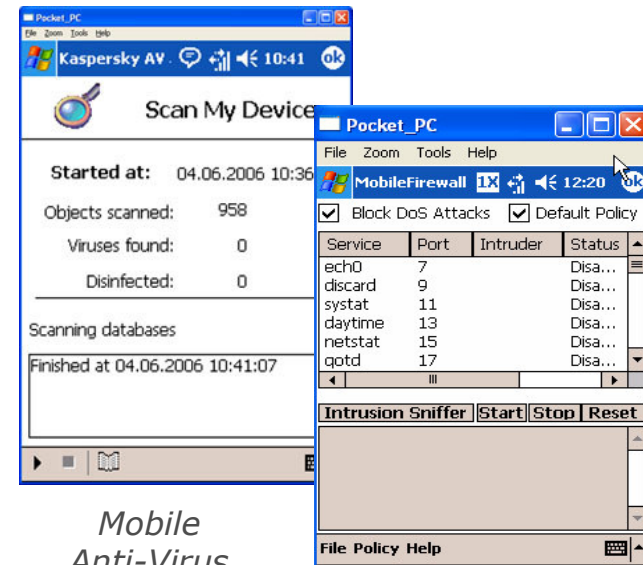
- > Lock devices or delete data on devices that have been lost or stolen

Mobile Anti-Virus:

- > Protect against malicious code, viruses and worms
- > Scan, identify and remove unknown threats

Mobile Firewall:

- > Permit and deny connections based on source/destination, IP ports, and applications
- > Block Denial of Service attacks and alert users of intrusion



Mobile
Anti-Virus

Mobile Firewall

Compliance

Allows IT to enforce a single security policy to all end users;
Over 150 security elements to choose from

Example:

Step 1: Authentication



Am I who I say I am?

- ✓ Do I have the right user id and password?
- ✓ Do I have the right password to view encrypted files?

Step 2: Interrogation

1. Examine device changes (if any)
2. Determine if compliant



Does my device adhere to our security policies?

- ✓ Anti-Virus
- ✓ Data encryption
- ✓ Personal firewall

Step 3: Access Decision

1. No Access
2. Access Granted
3. Remediation or Quarantine



If I am not compliant, what happens?

- ✓ Automatically updates, without user intervention

Customer Benefits

With Sprint Mobile Security, companies can control their mobile enterprise by enforcing corporate compliance and protecting against threats.

- Gain visibility and insight

- Flexible framework to manage policies

- Centralize IT monitoring and reporting

- Easy to procure and deploy

Control

Comply

Protect and Prevent

- Consistency across devices

- Policies meet regulatory requirements

- Minimize risk of security breaches

- Ensure privacy

- Secure corporate data

- Protect against viruses, worms and malicious code

- Defend against fraud and hackers

Case Scenario: Government Agency

A local government agency secured proprietary information on mobile devices for 1000 field employees.

Customer Needs:

- > Needed to provide secure wireless access to end users
- > Required a government-grade certified solution
- > Concerned about unauthorized users and attacks on mobile devices

Solution:

- > Sprint Mobile Security offers a complete package of security services for handheld devices

Benefits:

- > Secured data with AES Data Encryption; Solution is FIPS 140-2 certified
- > Offered secure access to the corporate Intranet with a Mobile VPN client
- > Protected devices from unauthorized users and viruses with a Mobile Anti-Virus and Mobile Firewall



Build an Integrated Security Policy

WHO	<i>Who is authorized to access what data?</i> Identify user-authentication based on access needs and worker profiles.
WHAT	<i>What does your existing infrastructure look like?</i> Choose tools to integrate with apps, network, OS, policies.
WHERE	<i>Where will users be when accessing the network?</i> Understand each access point -- device and network types.
WHEN	<i>Who needs what data when?</i> Determine when users need access to data. Establish an "Access Hierarchy".
WHY	<i>Why invest in mobile security?</i> Sensitive data on devices, rogue access (unprotected or unauthorized), regulatory...
HOW	<i>How do you build a mobile security policy?</i> Start with your remote access and corporate security policies. Extend (not replace!) existing practices to multiple access points.

The Sprint Mobile Security Advantage

Build It Yourself

- Piece together at least 3 commercial off the shelf applications
- Ensure cross carrier compatibility
- Test devices for certification
- Expand help desk to service non-compliant inquiries
- Invest in infrastructure

Sprint Mobile Security

- Tested, pre-integrated, and ready to implement service
- Carrier agnostic service
- Certified to run on multiple devices and OS
- Seamless, consistent user experience
- Zero capital outlay

Q&A

> For more information, please visit www.sprint.com/smms.