



High performance. Delivered.

**Security Considerations in Mobile Computing
Solutions**

**Presented by Stephen Roberts and Nisha Sharma
August 6, 2007**

Contents

- Introduction
- Background
- Benefits and Risks
- Addressing the Risks
- Conclusion
- Contacts



Although using mobile technology has become a standard part of work life, it is inherently insecure; governments need to understand it, acknowledge the risks and manage them

What is the problem?

- The power of mobility is growing every month in terms of devices, features, performance, and value, but it is insecure, and your employees are using it

Why does it need to be addressed?

- The insecurity stems from technical vulnerabilities and people's behaviors

What are other people doing about it?

- Employing security measures such as VPN, Encryption, Firewalls, Anti Virus, Configuration and Device Management

How can Accenture solve the problem?

- Our solution is complete; we use powerful security technologies combined with policies and processes that are designed to protect the data and encourage the desired behaviors



Imagine the consequences... if this employee lost that handheld with all of your private data on it...

Contents

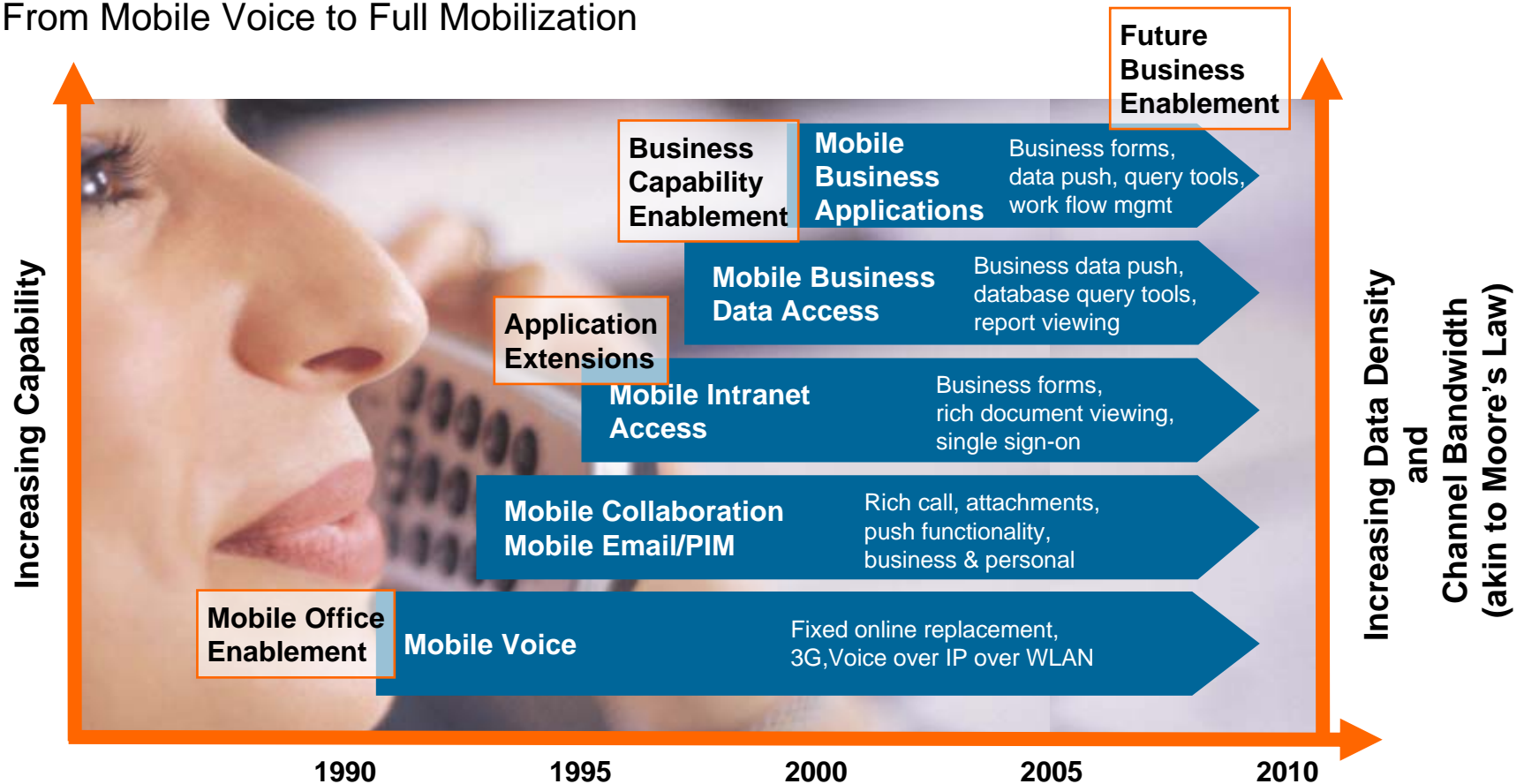
- Introduction
- **Background**
- Benefits and Risks
- Addressing the Risks
- Conclusion
- Contacts



We are getting more connectivity, more bandwidth and we're using it

Business Mobility Evolution

From Mobile Voice to Full Mobilization



The convergence of great and affordable mobile technology with the enterprise has made these devices and popular but risky to business

- We have developed a pop culture attitude that mobility is a proper way to conduct professional business; this has spawned a generation of workers in the workforce for whom mobility is the norm
- Culturally we're at a point now where employee expectations result in pressures to adopt mobile work styles whether or not enterprise management actually wants them
- These technologies, however, are inherently insecure, as are laptop and other mobility technologies. Where you are, and what device you're using should be less relevant than who you are and the security of the data



The most popular mobile devices are largely based upon consumer technologies, with lower security design expectations. And probably should not be treated as trusted even after the application of security policies, technologies and techniques.

As these trends in remote work and pervasive remote communication continue and grow, the risks will grow commensurately

- The implication is that today any data item can be sent to any device by any user, with or without the knowledge or consent of the enterprise
- These capabilities are improving every day, with new devices and network technologies arriving on the scene

“It does not look like handheld device integration is a passing fad, especially as technologies like Smartphones gain popularity. The initial reaction to ignore handheld device integration into the enterprise will not be an intelligent business decision in the months and years to come.”

Source: Gartner



Contents

- Introduction
- Background
- **Benefits and Risks**
- Addressing the Risks
- Conclusion
- Contacts



Mobility presents a multitude of benefits and risks

Security Business Case

- Increased productivity
- Decreased costs
- Timely response
- Improved Morale
- New Work and Business Processes



- Loss of Sensitive Information, Data, and IP
- Access to your networks and systems
- Liabilities to contract and regulatory penalties
- Lost productivity
- Intelligence leaks



But as the benefits increase, so do the risks

- The means of transmission have gotten more pervasive and faster. Wireless networks of all kinds, from 400-700Kb/Sec EVDO or faster 802.11*
- The devices are smaller, and we're more likely to use them with us in public places
- As costs decrease, capacities and speeds are increasing
- Portable storage has become ubiquitous and commonplace



Risk Management: the market for mobile security software will grow from \$214 million in 2006 to \$957.9 million in 2011, representing a 35% CAGR

Source: IDC



Human behavior, including being unaware of the danger, heightens the risk



Left in D.C./Baltimore Cabs in 6 Months of 2006

- 6,102 Mobile Phones
- 2,260 PDAs
- 339 Laptops

Source: Pointsec

- We keep important work-related files on these devices in case we need to get something done while we're out
- We transmit critical data, user identity information, passwords on networks not well known to us
- Work styles built around shuttling content between office and home on portable media have arisen
- Losses of media or devices with confidential content are not necessarily reported to the CIO/CSO
- It can be difficult to determine how much (or which) content an employee has at home if they are terminated
- Content can be accidentally transferred via "sneaker net"



When we add malefactors, the risk grows further

- Thin client devices, once thought of as inherently more secure, can be compromised at the server by spoofing the user or guessing passwords
- Devices can be hijacked so that the attacker has remote control over the device or intercepted to bug conversations
- Much information is lost or stolen by being overheard or being visually “snooped”, with mobile users conducting business in the airport, on a plane or train, at a café, or on the phone in a public place



Through 2006, 90 percent of mobile devices that contain business data will have insufficient power-on protection and storage encryption to withstand casual-to-moderate hacker attacks

Source: Gartner

In summary, mobility brings data loss risks, whose causes range from ignorance to theft

These risks include:

- Lack of enterprise knowledge of which employees are using remote devices
- Portable storage devices that can allow for large volumes of unprotected data to be carried in a pocket, and potentially lost or stolen.
- Inability to control the passage of data outside the enterprise or audit its whereabouts afterwards
- Loss and leakage of critical data when devices are lost
- Critical data being snooped when employee devices are used in public settings, such as overhearing a phone call, or reading an email over someone's shoulder
- Malware (viruses, worms, spyware, etc.)



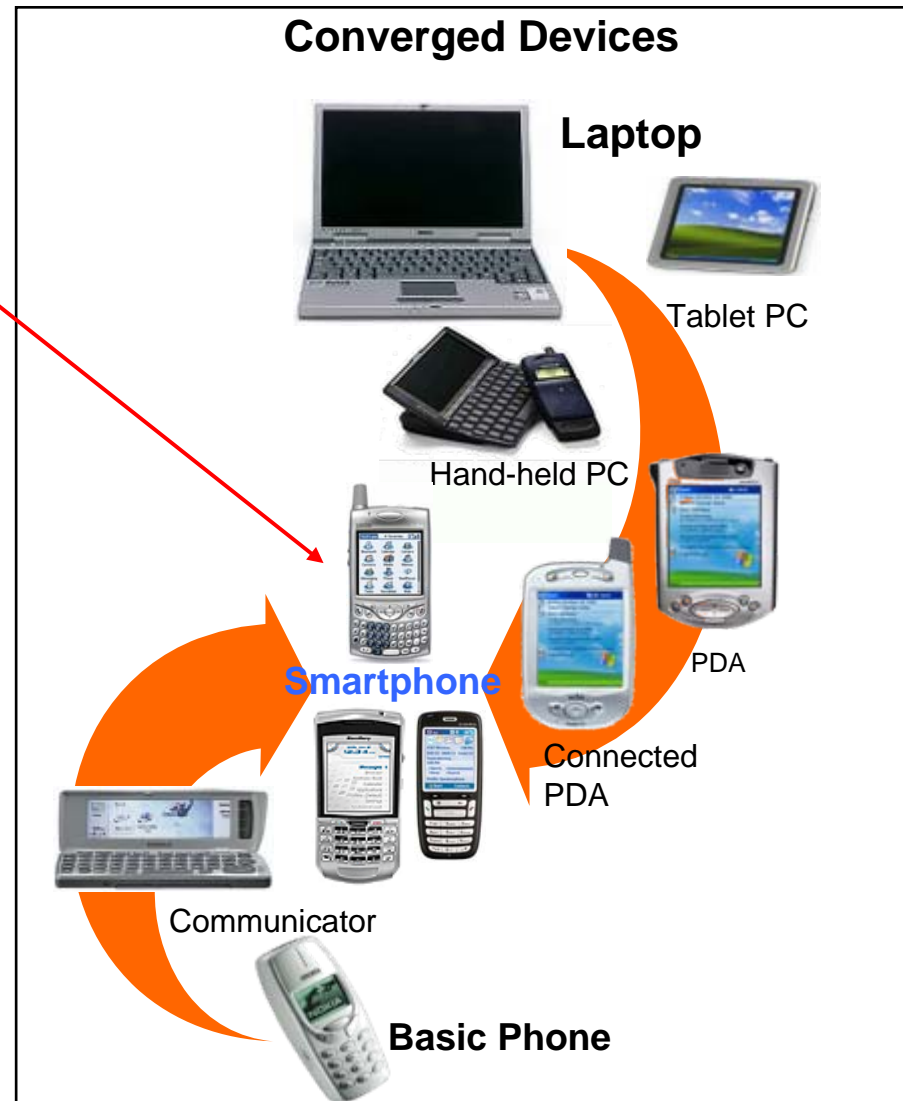
Contents

- Introduction
- Background
- Benefits and Risks
- Addressing the Risks
- Conclusion
- Contact



Government agencies need to stay current and understand new technology

- A “Smartphone” represents a convergence point, where laptop-like power moves downstream and meets high end cell phone size and use case models
- Microsoft Windows Mobile offers scaled down Windows computing functions with Windows application compatibility, and phone features grafted onto it
- Firms like Palm and RIM offer purpose-built devices based on PDA-like platforms
- Nokia and Symbian moved up-market from basic phone products to Communicator and Smartphone products
- All of them are powerful, reliable, useful devices



They need to be aware of what is likely to be brought into the office next week, like this Windows Mobile Smartphone, which rivals the computing power of a 1995-era laptop

- These devices offer a variety of form factors, phone-like and PDA-like, with and without keyboards and cameras
- They offer complementary economic environments, e.g., third party email, office, and connectivity applications
- They have standardized interconnects that support other complementary commercial ecosystems of universally available devices
- This platform leverage has created an economic sector based on mobile technology and a class of consumers who are benefiting from an increase in the performance and capability with each subsequent generation of mobile devices



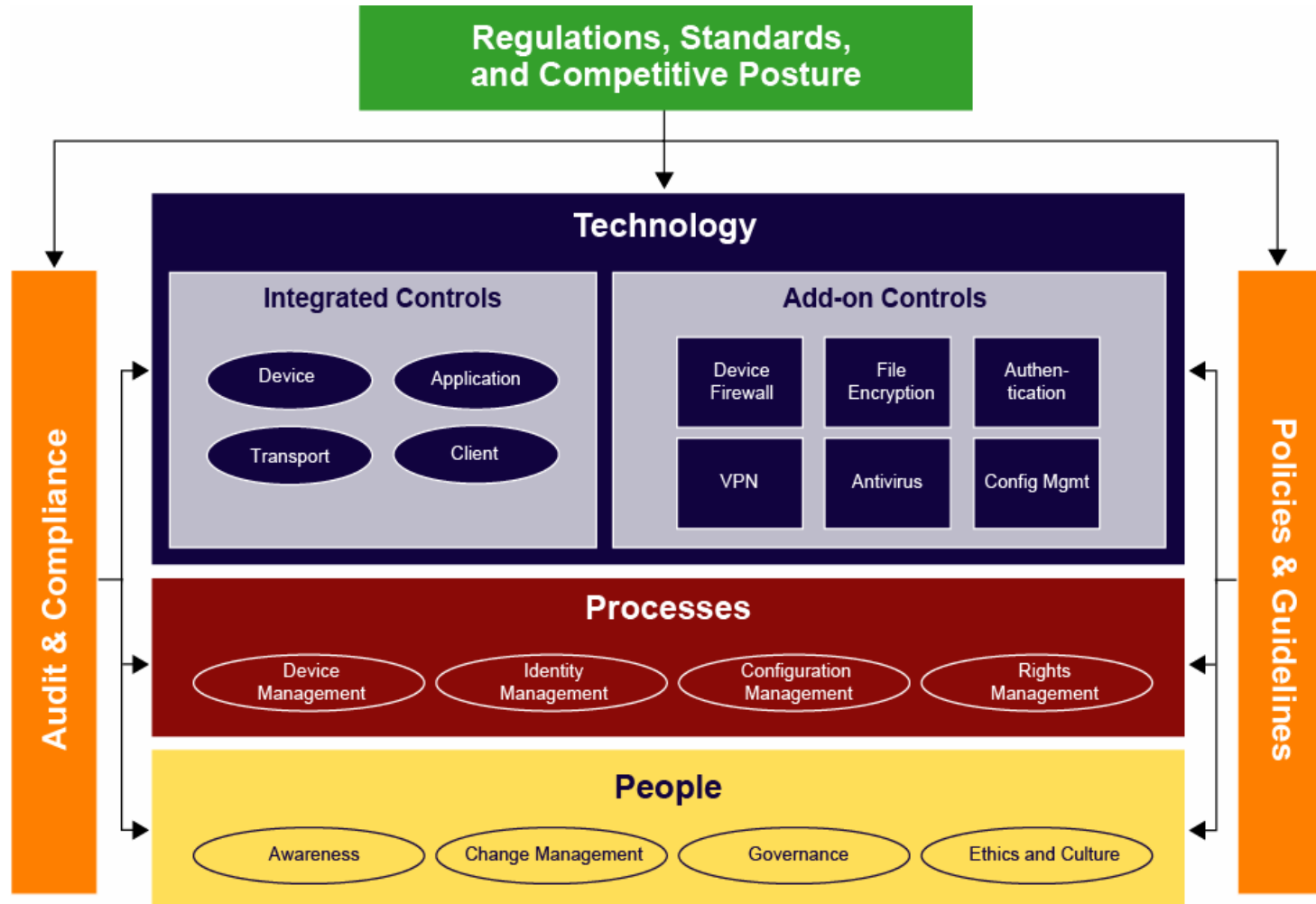
Converged devices surpassed handheld sales globally in 2004. Accelerated growth predicted through 2008

Source: IDC

By 2009, converged devices such as Smartphones will ship in higher volumes than corporate PCs

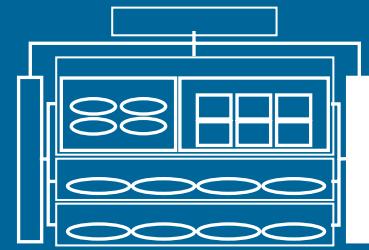
Source: Gartner

Our Mobile Security Solution Architecture takes all of these elements into account



This Mobile Security Architecture represents an ideal end-state based upon the trends in today's evolving technologies. These components exist today but are not entirely mature in all cases for all device classes.

Mobile Security Solution Architecture: Policies & Guidelines



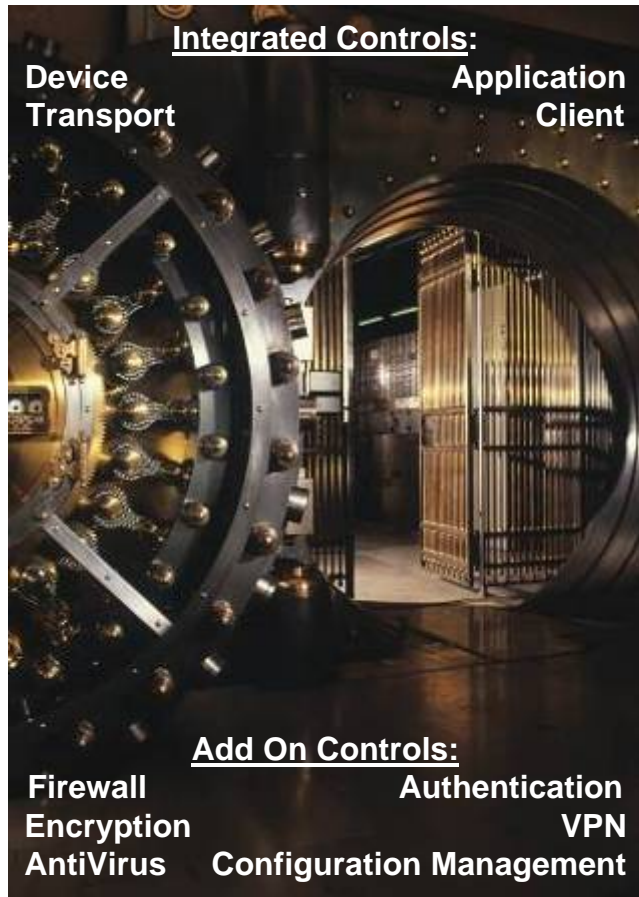
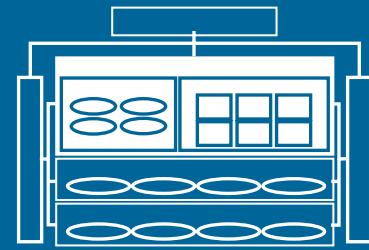
Policy may be one the most important and underestimated components in the solution. It is the manifestation of management intent. The ramifications of policy are complex, and policy creation and validation is a difficult and worthwhile task.

Accenture GACT Security

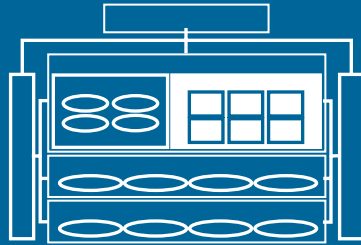
Some Sample Policies and Guidelines

- Allowed Devices Policy
- Appropriate Usage Policy
- Security Password Policy
- Encryption Policy
- Authentication Policy
- Removable Storage Policy
- Lost/Stolen Device Policy
- Employee Termination/Exit Policy
- Secure Application Development Guidelines
- Security Assessment Guidelines

Mobile Security Solution Architecture: Technology: Integrated and Add-on Controls

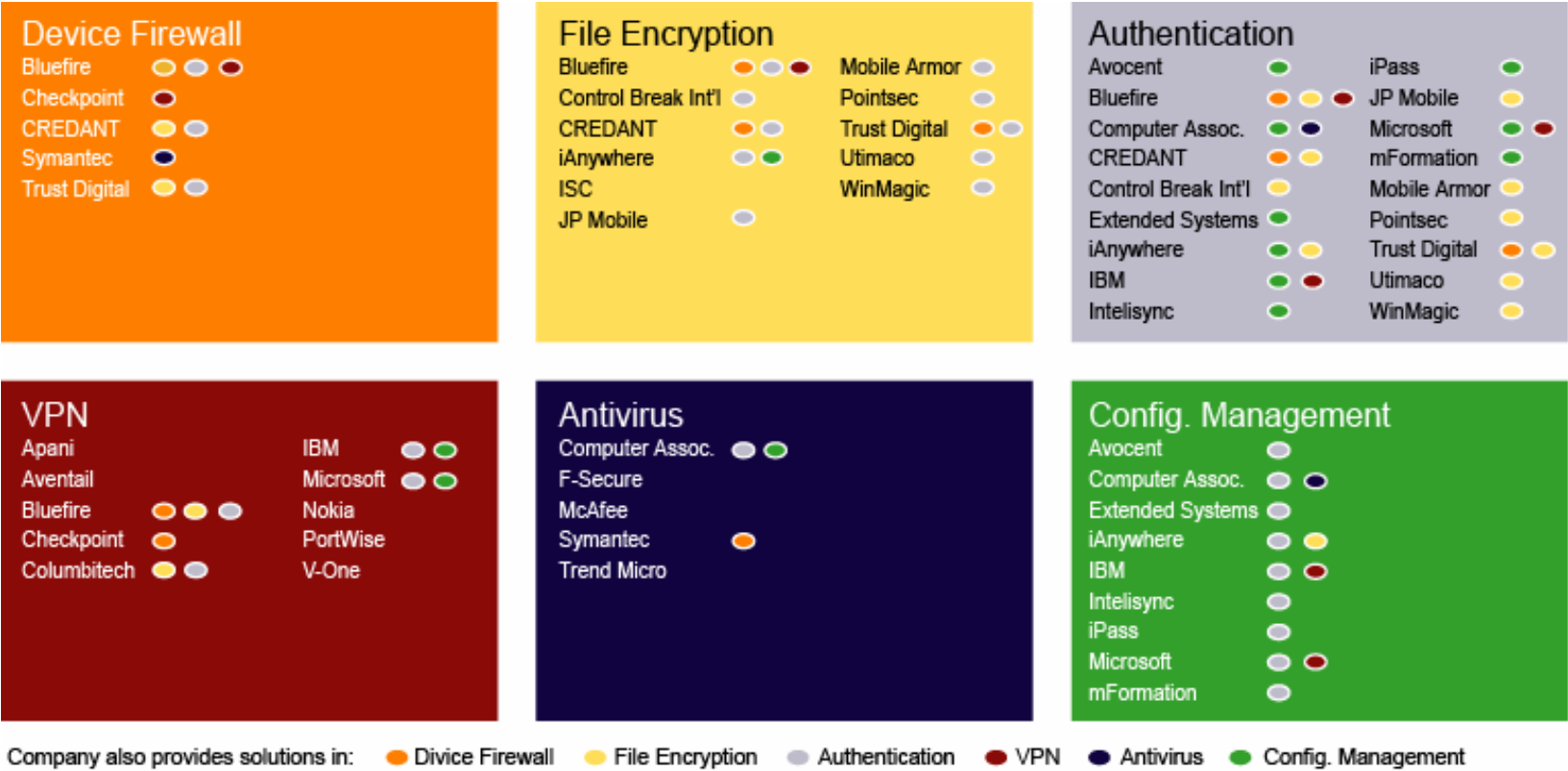


- Certain devices or classes of devices have integrated security controls
 - Power on password or PIN which requires the user authenticate themselves before any access after power up
 - Remote device deactivation which gives central management entities the ability to disable a device in the field
 - Device file system restrictions and privileges
 - Full featured web browser (SSL, Java) which support secure
- Add-on security controls augment the security of certain classes of devices
 - A variety of add-on controls such as file system strong encryption and VPN clients exists for multiple device platforms (Symbian, Palm, Microsoft Windows Mobile Smartphone, others)
 - Not all add-on control vendors support all platforms



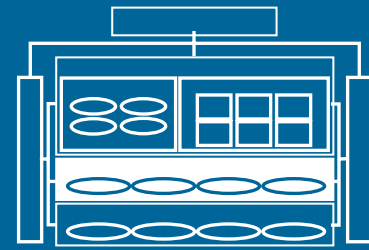
Mobile Security Solution Architecture: Technology: Add-on Controls: Vendor Mapping

There is no one vendor with all of the solution components, and a good overall solution will typically draw from many sources for best-in-class coverage.



Source: The Burton Group: Handheld Device Security Report

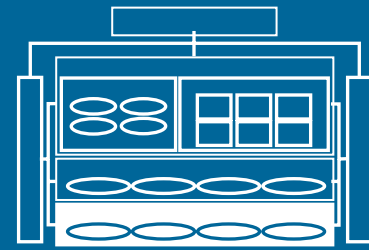
Mobile Security Solution Architecture: Processes



- Alignment of Mobile Workforce Security processes with IT and business processes is critical
- These processes include:
 - Device Management, Configuration Management, Rights Management, Identity Management
- Support of desired and accepted workflows drives utilization
- They should represent the best ways, the approved ways, of accomplishing necessary steps, so that people do not employ work-around processes
- Whenever possible they should be automated and self-service driven to reduce costs and increase satisfaction of customers
- They must have utility to the user community and be documented and publicized



Mobile Security Solution Architecture: People

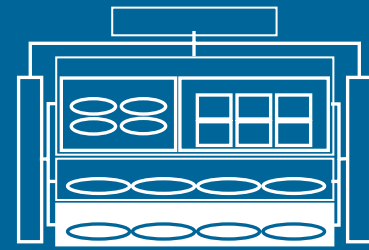


- People are the underlying driver of ad-hoc adoption; any technology and process solution that is going to work must satisfy the people who use it
- **Awareness:** People need to be trained and actively communicated with so they understand what is being done and why, and what they must do to comply and support the effort
- **Change Management:** Things change, and technology progresses; last year's ultra-hip Blackberry may look dated compared with the integrated multimedia and office features of today's Windows Mobile smart phone, and people may adopt the newer device even though you just rolled out the Blackberry. Understand the trends, manage their behaviors, and create satisfying options for early adopters



An agency can select in every possible security technology to protect data... but someone could still buy an insecure device and put it on your network... people's decisions make all the difference in your security posture

Mobile Security Solution Architecture: People

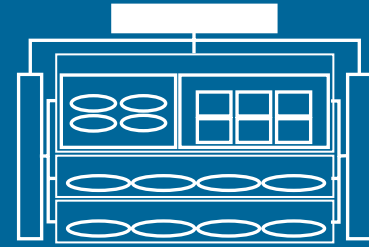


Awareness
Change Management
Governance
Ethics



- **Governance:** When people violate policies, there must be enforcement processes and penalties design to deter violation and encourage adoption
- **Ethics:** People are the core fabric that makes this work, and they must at some level have a strong motivation rooted in the culture not to violate policies covertly and to follow the rules for the right reasons
- Ultimately, people drive our success or failure far more than technology does, and it is up to us to create the right circumstances and environment for success

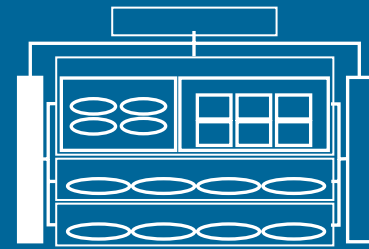
Mobile Security Solution Architecture: Regulations and Standards



- **Regulations** drive Compliance, but even without regulatory pressures, the principals of security and privacy make good sense as foundation elements in a solid mobile security strategy
 - Graham-Leach-Bliley and HIPAA/CMS focus on data privacy, and cause firms to lock down data and enforce security principals that in ways they otherwise might not
- **Standards** can serve as checklists or certification benchmarks, and they drive good security principals into the enterprise, even in firms that are not subject to regulatory pressures
 - ISO 17799, BS 7799 and NIST for example, embody best security practices and distill them down to ten easy to understand categories
 - COSO/COBIT provides standardized tools and security measurement techniques, and further embody best practices



Mobile Security Solution Architecture: Audit & Compliance



- Compliance verification and auditing activities may include Risk Assessments. These assessments, conducted by security professionals, may include:
 - Interviews with managers and individual contributors who have direct knowledge of a process or a technology application
 - Device Spot Checks which test employee compliance to policy and guidelines with respect to the devices they use on a day to day basis
 - Manual Audits which may drill down into detailed system and environmental security aspects
- Gap Analysis output can help the organization plan and execute remediation activities to bring the organization into compliance



Not a one-time event but rather a continual, iterative process of monitoring and improvement.

Contents

- Introduction
- Background
- Benefits and Risks
- Addressing the Risks
- Conclusion
- Contacts



Conclusion

- Using mobile technology has become a standard part of work life and offers many morale, competitive, and productivity benefits
- The convergence of enterprise and entertainment features has made these devices and lifestyle choices popular and made adoption unstoppable
- Mobility brings risks ranging from ignorance to theft; and the worst case result is disastrous for the firm, regardless of the reason the confidential information was exposed
- Developing a security solution to address the risks involves not only technology, but also people, processes and policies
- Even then, Mobility is inherently insecure and should be used with appropriate care. This includes the use of today's corporate-issued laptops, and even the home computers of employees used for telecommuting purposes
- Understand the risks and manage them with technology, policy, process, and a workforce that is conscious of best practices and behaviors

Contents

- Introduction
- Background
- Benefits and Risks
- Addressing the Risks
- Conclusion
- **Contacts**



Contacts

- Stephen Roberts, PMP
 - Accenture, Systems Integration and Technology (SI&T) – Technical Architecture
 - stephen.w.roberts@accenture.com
 - (512) 732-5747

- Nisha Sharma, CISSP
 - Accenture, Systems Integration and Technology (SI&T) – Mobile Computing
 - nisha.sharma@accenture.com
 - (786) 425-7340

