



# Mobile Data Security Essentials for Your Changing, Growing Workforce

**White Paper**

**February 2007**

CREDANT Technologies  
Security Solutions  
White Paper



## YOUR DYNAMIC MOBILE ENVIRONMENT

As the number and diversity of mobile users, device types and access locations continues to increase, the ability to manage and control data security has become mandatory – it’s no longer a question of “whether” to protect data, it’s a question of “how”. How does an organization best protect sensitive information stored on mobile devices (laptops, notebooks, desktops, PDAs, smartphones, or removable media)? How does that organization achieve productivity and competitive advantage, while ensuring their data remains secure regardless of the type of user (employees, affiliates, and even customers), the type of computing device or removable storage device, or the remote access location (a home, a hotel in Chicago, or a coffee shop in Beijing)?

Most of today’s data-at-rest security solutions are based on older encryption technologies that were never designed to work in today’s sophisticated environments, so as a result, they:

- complicate existing processes within the IT department
- create support challenges for the Helpdesk
- expose data during routine IT recovery, repair and maintenance
- impede end-user acceptance of security technology
- cannot meet a number of emerging key data security requirements

Implementing mobile security today requires enterprise-scale security for *all* mobile devices, not just laptop hard drives. It also must consistently enforce mobile data security rules – easily and painlessly - to ensure that the user experience and productivity is not compromised. Furthermore, mobile data security policies should be as simple or as complex as the enterprise environment needs them to be. After all, no two organizations - their infrastructure, workforce or processes – are alike.

In short, **to ensure data security in today’s dynamic environment the security must be controlled and managed in a consistent manner across all mobile platforms, across all users, and across all locations.** An organization requires a solution that is flexible yet treats mobile data protection as integral part of an enterprise's overall security processes.

This white paper outlines four key requirements for implementing an effective and flexible, enterprise-class mobile security solution to secure your mobile data and devices. An organization needs a single enterprise solution for all mobile devices and data—a mobile security solution that is simple, yet powerful and flexible, and that meets the strategic objectives in addressing mobile data security.





## FOUR REQUIREMENTS FOR AN EFFECTIVE MOBILE DATA SOLUTION

Mobile security is not a static process. Device types, users, and locations are diverse and change frequently. An enterprise's mobile security infrastructure must be able to easily accommodate this dynamic change and growth in an ongoing manner. *Data security is about ensuring that every part of the security chain—people, processes, operations, enforcement, and management—work together to provide a complete solution with no weak links.*

1. First, make sure your security solution enables you to constantly identify and control new device usage.
2. Next, make sure it can automatically and consistently enforce security policy and data protection.
3. Then, consider the importance of ongoing security administration—ensure that your security solution uses a single console to manage all device types.
4. Finally, make sure you can quickly and reliably support your end users when things go wrong. The solution should be able to reset passwords, recover encrypted data, etc. with little or no change to your existing support infrastructure and with little to no end user impact.

### THE MOBILE DATA SECURITY LIFECYCLE



-  Monitor for un-protected devices; control the synchronization of data; enforce with preset IT policies
-  Encrypt sensitive data, while providing user authentication, controlled port access and application restrictions
-  Centralize security policy management from a single console for all mobile devices. Audit to ensure that data security rules are enforced across all mobile devices.
-  Minimize complexity of policy enforcement by leveraging existing IT infrastructure; effectively support mobile users while enforcing data controls for lost or stolen devices and minimizing impact of ongoing maintenance and data recovery.

The following sections discuss key considerations and functional requirements for each element and explain how CREDANT Mobile Guardian best meets these needs.

## **1. YOUR SECURITY SOLUTION SHOULD ENABLE YOU TO CONSTANTLY IDENTIFY AND CONTROL NEW DEVICE USAGE**

When implementing mobile security, make sure your solution is able to:

- ☑ detect, audit and control *all* mobile end points as they come onto your network – including unsanctioned and user owned end points.
- ☑ generate detailed reports of mobile end point usage in your environment through a single console.
- ☑ detect, audit, and control synchronization software and 3rd party applications on the desktop such as ActiveSync, HotSync, PC Suite, mail redirectors, and more.
- ☑ support easy, comprehensive mobile security deployment by first detecting mobile end point usage and then automatically enforcing protection selectively across the environment.

## **2. YOUR SECURITY SOLUTION SHOULD AUTOMATICALLY AND CONSISTENTLY ENFORCE SECURITY POLICY AND DATA PROTECTION TRANSPARENT TO THE END USER**

Strong access controls, authentication and encryption must be consistently enforced across all mobile end points to protect sensitive information, meet regulatory/audit requirements, and more importantly, limit your risk of a data breach should mobile data or devices be lost, stolen or attacked.

Your mobile security solution should:

- ☑ seamlessly and automatically encrypt sensitive data across all mobile end points and external media from a single management console.
- ☑ enforce centrally-defined policies that control what is encrypted and how the encryption keys are generated, managed and escrowed.
- ☑ guard against unauthorized access in a multi-user operating system and that data recovery is fast and reliable.
- ☑ prevent end users from controlling, changing or removing security enforcement reliance on the end user to take action.
- ☑ require no second PIN/password at system startup and be interoperable with 3rd party authentication processes. Your solution should support whichever hardware tokens, smartcards, and/or biometric devices your security policy requires.
- ☑ control the use of specific device applications and communication ports.



- ☑ enforce over-the-air and local fail safe protections to suspend access or wipe data.
- ☑ ensure easy recovery of encrypted data if a user forgets their password or leaves the company.
- ☑ provide real-time status of mobile data protection in your environment.
- ☑ ensure enforced data security (policy deployment and updates, authentication, etc.) without interfering with user productivity; provide innovative user friendly features

### **3. USE A SINGLE CONSOLE TO MANAGE ALL DEVICE TYPES**

To minimize complexity and reduce the level of effort required to address mobile security, it is important to implement an enterprise-wide solution that leverages existing infrastructure investments while centralizing administration into one management console.

Your mobile security platform should:

- ☑ Provide a single management console for mobile security administration, control, audit, and reporting with full platform support across mobile and external storage device types to control and automatically enforce and update security policies across all mobile end points



- ☑ Inherit roles (groups) and users from existing LDAP directories (such as Microsoft Active Directory), eliminating the need to re-enter and separately maintain this information
- ☑ Provide separate administrative roles (from help desk to security admin) to control administrator privileges

- ☑ Deliver detailed mobile end point reporting and auditing information
- ☑ Ability to generate detailed reports of mobile end point usage (including synchronization software), protection, and security status



#### **4. QUICKLY AND RELIABLY SUPPORT END USERS AND RECOVER ENCRYPTED DATA WITH LITTLE OR NO IMPACT TO YOUR EXISTING SUPPORT INFRASTRUCTURE OR TO THE END USER**

It is easy to overlook the impact of ongoing support, maintenance and data recovery when choosing the right mobile security solution. Many solutions are deceptively simple in their approach to securing data, and it's not until the time comes to support it that the limitations become all too obvious and dangerous.

Make sure that your mobile security solution:

- ☑ works within the established maintenance and recovery processes used by your IT department and that they do not require the process or recovery time to be changed or lengthened.
- ☑ provides key generation and escrow features which allow immediate, full data recovery with no gaps. Many solutions require keys to be generated on the target device and then escrow them back to a central server. What happens if the escrow process is delayed or fails altogether and the user needs to recover them? Keys should be escrowed *before* the first bit of data is encrypted – without requiring any action by the end user.
- ☑ protects against internal threats—unauthorized access in a multi-user operating system; separates access to encrypted data from access to the operating system.
- ☑ allows self-service password reset and over-the-phone password reset capability; PIN/password recovery requires no network connection.
- ☑ allows the users of handheld devices to make and receive calls without the user having to unlock the device. It should be flexible enough though to require authentication if the user wants to make an outgoing call from the confidential company 'Global Address List'.
- ☑ allows operating system upgrades, hot fixes, and the application of patches without being concerned whether the operating system is encrypted, using "fake" logins, and or/resulting data corruption issues.
- ☑ provides data recovery options that work with your existing IT recovery processes and tools.
  - ☑ data recovery that allows security administrators to access encrypted data without any assistance or cooperation from the end user
- ☑ delivers automatic, real-time policy and software updates "in the field" to ensure quick closure of security gaps, continued regulatory compliance, and mobile productivity.
- ☑ balances security with usability.
- ☑ Enables over-the-air deployment and activation.
- ☑ Interoperates with 3<sup>rd</sup> party device management and synchronization providers, such as Altiris, Intellisync, Good, EIM, SMS, etc.

## SUMMARY

The initial setup of your mobile data security solution should not require any action from the end user—it should be automatic, enforceable, and provide immediate feedback on the progress of the installation and subsequent protection of data. Once the setup is complete, your security solution should still not require (or allow) any ongoing action from the end user, but rather it must be as invisible as possible and when it isn't, it should be easy-to-use, without impacting end user productivity.

Mobile data security must be a strategic, company-wide initiative that allows audit and enforcement of multiple security policies across multiple device types, i.e. laptop, TabletPC, PDA, smartphone, removable media. The solution must address all elements of mobile data security, while enabling user productivity anywhere, at anytime, and with minimal risk and low total cost of ownership for the organization

- 1) **Detect & Enforce:** automatically identify devices and data usage; control the synchronization of data directly to rogue mobile devices from PCs or over-the-air synchronization of email from Microsoft Exchange Server; enforce with preset IT policies
- 2) **Encrypt & Protect:** ensure that sensitive data is securely encrypted, while providing user authentication, controlled port access and application restrictions
- 3) **Manage & Audit:** centralize security policy management from a single console for desktops, Notebook PCs, handhelds and USB flash drives. Audit trail ensures that company data security rules are being enforced across all mobile devices
- 4) **Support Existing Operations:** minimize complexity of security policy enforcement by leveraging existing IT infrastructure; effectively support mobile users while enforcing data controls for lost or stolen devices while minimizing impact of ongoing maintenance and data recovery.

## ABOUT CREDANT TECHNOLOGIES

CREDANT<sup>®</sup> Technologies<sup>®</sup> is the market leader in mobile data protection solutions. CREDANT's secure mobility solutions preserve customer brand and reduce the cost of compliance, enabling business processes to quickly and safely "go mobile." CREDANT Mobile Guardian is the only centrally managed mobile data protection solution that provides strong authentication, intelligent encryption, usage controls, and key management that guarantees data recovery. By aligning security to the type of user, device and location, CREDANT ensures the audit and enforcement of security policies across all mobile end-points. Strategic partners and customers include leaders in finance, government, healthcare, manufacturing, retail, technology, and services. CREDANT was selected by Red Herring as one of the top 100 privately held companies and top 100 Innovators for 2004, and was named Ernst & Young Entrepreneur Of The Year<sup>®</sup> 2005. Austin Ventures, Menlo Ventures, Crescendo Ventures, Intel Capital and Cisco Systems are investors in CREDANT Technologies. For more information, visit [www.credant.com](http://www.credant.com).

## **CREDANT MOBILE GUARDIAN**

CREDANT Mobile Guardian (CMG) Enterprise Edition is an award-winning, integrated and easily deployable mobile security and management software platform that enables organizations to easily secure and manage disparate mobile and wireless devices from a single management console. CREDANT select OEM partners such as Hewlett Packard.

CREDANT Mobile Guardian is the only solution to combine integrated, centralized enterprise management capabilities with strong mobile data security across the broadest range of mobile device platforms– all in a single package that is easy to deploy and manage, and easily accepted by end users. With CMG, companies can cost-effectively secure and support an enterprise-scale mobile workforce while improving employee productivity, with the peace of mind that their organization’s sensitive information is secure.

## **CONTACT US**

For more information on how CREDANT can help meet your mobile security and management needs, please contact us:

1-866-CREDANT (273-3268) or 972-458-5400

[www.credant.com](http://www.credant.com)

[info@CREDANT.com](mailto:info@CREDANT.com)

###

Disclaimer: This white paper is not intended to take the place of informed legal counsel. The information and recommendations contained herein are for informational purposes only, and should be expanded upon by trusted legal sources. For specific advice about formulating an information security policy that is compliant with current laws and regulations, or for further information about complying with information security laws, it is recommended that you seek professional counsel.

Copyright © 2007 CREDANT Technologies, Inc. All rights reserved. CREDANT, CREDANT Technologies, the Be mobile Be secure tagline, and the CREDANT logo are registered trademarks of CREDANT Technologies, Inc. All other trademarks used herein are the property of their respective owners and are used for identification purposes only.

Mobile Essentials\_WP\_0207