



Detect, Protect, Manage, and Support:

Control Mobile Data and Devices Before They Control Your Organization

White Paper

April, 2006

CREDANT Technologies
Security Solutions
White Paper





Table of Contents

WHY EVEN CONSIDER MOBILE SECURITY?1

HOW TO CONTROL THE SEEMINGLY UNCONTROLLABLE2

 1. DEVELOP WRITTEN POLICIES TO ADDRESS MOBILE DATA/DEVICES 2

 2. DEPLOY INFRASTRUCTURE TO ENSURE POLICY ENFORCEMENT 2

 MOBILE SECURITY LIFE CYCLE PROCESS 3

CREDANT MOBILE DATA SECURITY LIFECYCLE3

 DETECT: TO IDENTIFY DEVICE USAGE, ENFORCE POLICIES AND AUDIT FOR COMPLIANCE..... 3

 PROTECT: TO SAFEGUARD DATA AND LIMIT RISK 4

 MANAGE: TO CENTRALIZE ADMINISTRATION AND ENTERPRISE CONTROL..... 6

 SUPPORT: TO MINIMIZE IMPACT AND ENSURE EASE-OF-USE..... 6

 3. COMMUNICATE MOBILE SECURITY POLICY TO EMPLOYEES..... 9

SUMMARY9

 ABOUT CREDANT TECHNOLOGIES..... 11

 CREDANT MOBILE GUARDIAN PRODUCT SUMMARY 11

 CONTACT US..... 12

WHY EVEN CONSIDER MOBILE SECURITY?

It is no longer an issue of whether to allow employees to be mobile: a mobilized workforce increases the speed of business execution. However, with increased productivity comes increased risk. Why? Because sensitive internal information (such as executive communications, email, data files, corporate directories, and calendars) is being stored on mobile computers and external media storage devices without any way to protect that data if one of these devices gets lost or stolen.

Gartner Group estimates that 90% of mobile and removable media devices have inadequate security to protect against even the most common of situations, such as the next passenger picking up a device left in a taxicab. Independent estimates show that more than 375,000 devices are left on public transport every year in the USA. More troubling is the risk of these devices being used by motivated hackers to penetrate the enterprise. Some of these scenarios may include the hacker accessing stored passwords or other sensitive data on the device, gaining electronic access to the organization through the device's VPN client, or by using stored contact information to initiate a social engineering attack, any or all of which could be catastrophic for you and your customers.

As organizations are faced with increasing legislation such as Gramm-Leach-Bliley, Sarbanes-Oxley, HIPAA, and California Senate Bill 1386, the risks – and costs – of not protecting sensitive internal information stored on mobile or removable media devices can no longer be ignored. A benchmarking study conducted in 2005 by the Ponemon Institute in Tucson, Arizona estimates that 86% of security breaches involve the loss or theft of customer or consumer information. Within the previous 12 months between 23 million and 50 million US adults have received notification stating that their personal information had been lost and the cost of notification is estimated to be \$140/per lost customer record.

In addition to operational costs, a lack of mobile data/device security leads to increased liability, brand damage, monetary fines, negative PR from external exposure, and loss of customer confidence – all of which negatively impact your bottom line. The benchmarking study conducted by the Ponemon Institute estimates that the customer "churn rate" (the rate at which companies lose customers) with companies that lose customer data (and subsequently have to inform the customers of the loss) may be as high as 20% (1 in 5 customers) and growing. (The normal customer "churn rate" hovers at 1-2% per year but varies by industry.) Finally, companies with security breaches face significantly higher marketing and sales expenses in order to retain existing (disillusioned) customers and to continue to attract new customers against a background of very negative publicity.

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 "if", it's a question of "how". To achieve productivity and competitive advantage, organizations must ensure data remains secure regardless of the type of user (employees, affiliates, and even customers), the type of computing device (laptops, notebooks, PDAs, smartphones, or removable media), or the access location (home, a hotel in Chicago, or a coffee shop in Beijing).

To ensure data security in today's dynamic environment, an organization requires a solution that is equally dynamic and that treats mobile data protection as a continuous process.

There are four major elements in this process -- Detect, Protect, Manage, and Support. Combined, they form a comprehensive Mobile Data Security Lifecycle. The key benefit of this lifecycle approach is that it ensures every aspect of data security is controlled and managed across all mobile platforms—it is not specific to any one type of device or user, or to just one aspect of security. The alternative approach is to implement multiple, device-specific 'point' solutions and consoles—a labor intensive and non-scalable approach that limits an organization's ability to easily control, manage, and support data security and recovery.

Your 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 your strategic objectives in addressing mobile data security. This white paper takes you step-by-step through best practices for creating a mobile security strategy and for implementing an enterprise-class solution to secure your mobile data and devices. It also outlines the benefits of the CREDANT Mobile Guardian solution for controlling the security of all things mobile in your organization.

HOW TO CONTROL THE SEEMINGLY UNCONTROLLABLE

1. DEVELOP WRITTEN POLICIES TO ADDRESS MOBILE DATA/DEVICES

Begin by creating written policies and procedures that address the security risk of mobile data and devices in their entirety. In setting policy, it is important to first understand how and why mobile/external media storage devices are interacting with your enterprise so you can limit risk with minimal impact to business operations. Make sure your policies specify who can use mobile devices, for what purposes, and which kinds of devices are allowable. Your security policies should also include how (and why) the data and device itself will be protected, including the details of how users authenticate to your enterprise, what information will be encrypted, and what device capabilities (for example, cameras and Bluetooth) are allowable.

Given the plethora of devices, price points and functionality available, the need for an organization to allow users to utilize a variety of different device types is important. However, in order to minimize support costs, we recommend limiting the number and types of devices supported.

You might ask what right the organization has to enforce the use of security on personally-owned devices. *The organization owns the data and therefore owns the responsibility of protecting it. It is their burden of risk, not the individual.* From an organization's perspective, policies should detail how corporate information is to be used, by whom, and how it is to be protected – independent of where the data resides. The corporation has the absolute right to allow employees and business affiliates to access corporate data with mobile devices BUT ONLY if the information will be adequately protected.

2. DEPLOY INFRASTRUCTURE TO ENSURE POLICY ENFORCEMENT

Implementing mobile security requires a holistic approach to managing *all* things mobile. The solution must provide enterprise-scale security for *all* mobile devices including

Windows-based computers such as laptops, notebooks, and tablets; handheld devices such as PDAs and smartphones; and removable media such as USB fobs, CompactFlash cards, and iPods. In addition, it must consistently enforce mobile data security rules – easily and painlessly, to ensure that the user experience is not compromised more than is absolutely necessary





MOBILE SECURITY LIFECYCLE PROCESS

Mobile security is not a static process. Device types, users, and locations are diverse and change frequently. Your mobile security infrastructure must be able to easily accommodate this dynamic change and growth in an ongoing manner. First, make sure your infrastructure enables you to constantly identify and control new device usage. Next, make sure it can automatically and consistently enforce security policy and data protection. Then, consider the importance of ongoing security administration and make sure your infrastructure uses a single console to manage all device types (or risk the burden of managing multiple, point product, device-specific consoles). 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.

In response to these requirements, CREDANT Technologies approaches mobile data security as a continuous, “life cycle” process. We define this life cycle as having four (4) distinct, yet highly integrated elements, each which must be addressed to adequately secure your mobile data. CREDANT Mobile Guardian is the only solution that follows a security management life cycle approach, enabling you to Detect, Protect, Manage, and Support at each step along the way.

CREDANT MOBILE DATA SECURITY LIFECYCLE



-  Reduce risk by monitoring for unprotected mobile devices
-  Eliminate data breach if mobile device is lost or stolen
-  Reduce administration with centralized management
-  Minimize impact of forgotten passwords, 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.

DETECT: To IDENTIFY DEVICE USAGE, ENFORCE POLICIES AND AUDIT FOR COMPLIANCE

The ability to detect mobile and external media storage device usage, enforce security policy adherence, and control synchronization should be mandatory – simply asking

employees to use security software on the device is not sufficient. Every time a device attempts to connect to your organization's network, it must be checked to ensure that security software is installed and that the security policies are up-to-date and being enforced. Specifying that employees must use security software on their mobile devices but not ensuring its use is like having speed limits but no traffic tickets. As one Fortune 35 executive put it, "We had a written security policy, but no capability to enforce or audit it. This was something we had to address!"

When implementing mobile security, make sure that your solution will:

- Automatically detect mobile end points as they come onto your network
- Automatically collect inventory and report on the mobile end points in use
- Automatically collect and detail the synchronization software and other 3rd party applications on the desktop that expose a backdoor for corporate information to flow through (e.g. mail redirectors)
- Allow you to automate the rollout of security software to mobile end points in phases

CREDANT MOBILE GUARDIAN (CMG) from CREDANT Technologies allows you to put your paper security policies for mobile devices into action. CMG Enterprise Edition is the only mobile security product on the market today that can detect *every* approved – and unapproved – mobile and external media storage device to meet security audit requirements. Its features include the ability to *automatically*:

- Detect, audit and control *all* mobile end point usage – including unsanctioned and user owned end points
- Generate detailed reports of mobile end point usage in your environment through a single console or in an exported report
- Detect, audit, and control synchronization software and 3rd party applications on the desktop such as ActiveSync, HotSync, PC Suite, mail redirectors, and more
- Phase your mobile security deployment by first detecting mobile end point usage and then automatically enforcing protection selectively across the environment

PROTECT: To SAFEGUARD DATA AND LIMIT RISK

Strong access controls, authentication and encryption must be consistently enforced across 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.

Data encryption requires a balance between ease of use and security. Check that your security agent can enforce centrally-defined policies that control which encryption algorithm is used (this affects time required for encryption), as well as what is encrypted and how the encryption keys are generated, managed and escrowed. Make sure that your solution guards against unauthorized access in a multi-user operating system and that data recovery is fast and reliable. Finally, make sure your solution does not rely on the end user to take action. It should seamlessly and automatically encrypt data regardless of where the data is saved or what the file is named.

To ensure maximum data protection, two-factor authentication should be used to protect confidential information from unauthorized users. Make sure your solution supports whichever hardware tokens, smartcards, and/or biometric devices your security policy requires. To minimize impact to users and IT staff, make sure your solution does not require a second PIN/password at system startup and is interoperable with 3rd party authentication processes. This will help maintain a true single sign-on environment (one userid/one password), reduce help desk calls, and eliminate the need for manual application modification to integrate authentication processes.

Your mobile security solution should be able to:

- Secure all mobile end points and external media devices in your environment from a single management console
- Enforce strong authentication and data encryption when required
- Control the use of specific applications and communication ports
- Ensure all sensitive data is encrypted across all mobile end points and external media devices using intelligent encryption controls
- Prevent end users from controlling, changing, or removing security enforcement
- Enforce remote and local fail safe protections in the event a mobile end point is lost or stolen
- Ensure recovery of encrypted data if a user forgets their password or leaves the company
- Provide real-time status of protection in your environment

CREDANT MOBILE GUARDIAN (CMG) automatically protects data residing on mobile and external storage devices. CMG Enterprise Edition was built from the ground up to meet the needs of the enterprise, giving you the ultimate flexibility in defining and enforcing mobile security initiatives. Its features include:

- Comprehensive and automatic protection for *all* types of mobile and external media devices from a single management console
- Support for strong authentication – including two factor authentication without the need for special SDK's or additional development
- Advanced controls to shut down potentially dangerous applications (e.g. mail redirectors) and disable potentially dangerous device functionality such as cameras, Bluetooth, and/or infrared beaming
- Patent-pending "Intelligent Encryption" that ensures complete, automatic, and transparent data protection for all data using a defense-in-depth approach to encryption
 - ✓ Automatic encryption of all data written or copied to external media
 - ✓ Automatic encrypted data portability to allow roaming of encrypted data within the enterprise or outside using "CREDANT2go"
- Built-in security controls to prevent tampering and removal of security by end user
- Automatic enforcement of security fail-safe actions including local and over-the-air protections to suspend access or wipe data
- Comprehensive key management ensuring secure escrow of encryption keys at the central server for guaranteed encrypted data recovery

- Detailed reports of mobile end point protection including encryption status and login failures

MANAGE: To CENTRALIZE ADMINISTRATION AND ENTERPRISE CONTROL

IT administrators are inundated trying to manage multiple existing systems that do not address end-to-end mobile security requirements. To minimize complexity and reduce the level of effort required to address mobile security, it is important to implement an enterprise-strength solution that leverages existing infrastructure investments while centralizing administration into one management console.

Your mobile security platform should be able to:

- Provide a single management console to control and enforce security across all mobile end points
- Automatically enforce security and provide guaranteed delivery of security policy updates to mobile endpoints
- Leverage user and group definitions in existing LDAP directories for managing mobile security enforcement
- Separate administrative duties to control administrator privileges
- Deliver detailed mobile end point reporting and auditing information

CREDANT MOBILE GUARDIAN simplifies ongoing mobile security management, minimizes administration costs and eliminates security gaps created by point products by providing a comprehensive solution that integrates with existing identity infrastructures so mobile security policies can be applied to already-defined users and groups. This way, there's no additional administrative overhead when a new employee joins the organization, and it's easy to make global, group, or even a user-level policy change. Its features include:

- Single, centralized, web-based management console for mobile security administration, control, audit, and reporting with full platform support across mobile and external storage device types
- Automatic security software installation on mobile end points and transparent updating of security policies during synchronization or over-the-air, eliminating the need for manual provisioning
- Ability to 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
 - ✓ Group-based security policy administration to reduce management complexity
- Ability to assign five separate administrative roles (help desk to security admin) to control administrator access and privileges in the administration console
- Ability to generate detailed reports of mobile end point usage (including synchronization software), protection, and security status

SUPPORT: To MINIMIZE IMPACT AND ENSURE EASE-OF-USE

Ongoing maintenance and data recovery are areas often overlooked by security experts 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. Encrypting the entire hard disk on a laptop (Full Disk Encryption or FDE), for instance, seems like a simple, effective answer to data security. However, consider this: When the CFO's machine is sent off to be upgraded or repaired, the "secure" data (the CFO's data files) on FDE-protected machines is **completely visible to the repair technician.**

Make sure that your 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. For example, a typical break-fix scenario requires approximately 90 minutes of an IT administrator's time to get the problem resolved and the user up and running again. A full disk encryption mobile security solution can increase the recovery time because the entire hard disk may need to be decrypted before the problem is resolved (can take as long as 7 hours) or administrators must utilize special tools and processes to perform recovery.

Time is of the essence in any data recovery process – lost time equals lost productivity. Make sure your encryption key escrow process does not require end users to manually store keys on separate devices (e.g. floppy) or use some out of band process (e.g. copy the encryption keys to a network drive). The problem with these approaches is that recovery of the encryption keys is not guaranteed immediately and is left up to the control of the end user. If the end user loses the recovery device (e.g. floppy) or the encryption keys are never sent back (e.g. employee leaves the company) then recovery of encrypted data may not be possible. Make sure that encryption keys are automatically, securely, and centrally escrowed. They should be available from the second the first bit of data is encrypted – without requiring any action by the end user.

The act of forcing data to be decrypted immediately opens sensitive data to the threat of unauthorized access. At no time during the recovery process should encrypted data be decrypted and exposed. In addition, make sure your solution protects against unauthorized access in a multi-user operating system. As mentioned before, the last thing you need is for a contracted technician performing standard maintenance to gain access to the company's email announcement on the CFO's machine.

Mobile devices enable users to be productive anywhere, anytime, but only if they can access their devices. To minimize help desk costs and maximize user productivity, users must be able to reset their own passwords without requiring a network connection. Make sure your security agent supports self-service password reset and an over-the-phone password reset capability so a user can call the help desk and participate in a secure challenge-response exchange to regain access to the device.

Another important consideration is how the solution works on smartphones—converged cell phone/PDA devices such as the Treos™ from palmOne™ that are becoming increasingly more popular. The desire to strongly protect the information stored on the device must be balanced with the user's desire to be able to easily make and receive phone calls. For instance, a good solution (one that balances security and ease of use) should allow the user to make & receive voice calls without having to unlock the device, but should require authentication if the user wants to make an outgoing call from the confidential company 'Global Address List'.

Your mobile security solution should be able to:

- Balance security with usability
- Allow operating system upgrades, hot fixes, and the application of patches without being concerned whether the operating system is encrypted and or/resulting data corruption issues
- Provide data recovery options that work with your existing IT recovery processes
 - You should not be required to change or lengthen your existing recovery processes for broken machines
 - You should be able to access encrypted data without requiring the employee to be present (e.g. employee has left the company)
- Separate access to encrypted data from access to the operating system (e.g. local administrators should not be able to access the CEO's data when performing routine maintenance tasks)
- Support self service and help desk password recovery
- Enable immediate policy and software updates without "physically" having to touch each device
- Scale up or down to meet your organizations mobile security requirements

CREDANT MOBILE GUARDIAN provides the following features to balance security and end-user acceptance:

- Flexible configuration which can allow users to answer phone calls without having to unlock their device
- Works within the boundaries of the operating system ensuring that new OS upgrades, hot fixes, and patches can be applied using existing processes without compromising security or causing machine instability
- Server-based encryption key generation and escrow with immediate, full data recovery
 - ✓ Data recovery that works with existing IT recovery processes
 - ✓ Data recovery that allows security administrators to access encrypted data absent the end user
- Separation of encrypted data access from file system access – guarantees that local administrators and multiple users on a machine cannot access another users encrypted data
- Self-service PIN/password reset, with no network connection requirement for recovery, minimizing the number of calls to your help desk
- Over-the-phone password reset capability with secure challenge-response
- Automatic, real-time policy and software updates "in the field" to ensure quick closure of security gaps, continued regulatory compliance, and mobile productivity

- ☑ Multiple deployment options to support phased implementation, support goals, and growth objectives
 - ✓ Over-the-air deployment and activation
 - ✓ IT imaged deployment
 - ✓ Interoperability with 3rd party device management and synchronization providers such as Altiris, Intellisync, Good, EIM, SMS etc.

3. COMMUNICATE MOBILE SECURITY POLICY TO EMPLOYEES

Although it may seem obvious, it bears repeating that security is only effective if it is used. Your employees need to understand your security policy, the risks, and why it is important to protect data stored on mobile end points, even if they are their using their own devices. Without mobile user acceptance, you face an uphill battle on implementing an effective security program or worse, potential security breaches because users refuse to follow rules which they either don't understand or which negatively impact their productivity and results.

Once initial setup is completed, your security solution should not require any ongoing action be taken by the end user. It must be invisible as much as possible, and when it isn't, it should be easy-to-use – without impacting end user productivity. In addition, make sure your security solution gives notice to employees attempting to synchronize with your corporate network *before* the security agent is installed so they have the option not to do so if they prefer not to have their personal devices in compliance with your corporate security policy.

CREDANT Mobile Guardian works transparently to end users, ensuring that sensitive data is protected. In addition, CMG notifies users that the security agent will be downloaded to the device upon synchronization, and will only allow them to sync if they choose to continue with the installation.

SUMMARY

Organizations must take control of all mobile devices before the devices and their users take control of the organization—or risk being subject to negative PR, brand damage, regulatory fines, and potential financial losses resulting from rapid decline in customer and investor confidence.

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, Handheld PDA, and Smartphone. The solution also must address all elements of the mobile data security lifecycle (Detect, Protect, Manage and Support), while enabling user productivity anywhere, at anytime, and with minimal risk and low total cost of ownership for the organization

- 1) **Detect:** define the company “rules” for use of mobile data, continuously identify and monitor mobile device and data usage, and audit for compliance--all without impacting productivity.

-
- 2) **Protect:** safeguard data and limit risk of lost, stolen or attacked devices by enforcing access controls, authentication and encryption across mobile end points; minimize impact to users and IT staff by seamlessly and automatically encrypting data “at rest” to meet regulatory and audit requirements.
 - 3) **Manage:** minimize complexity of security policy enforcement by leveraging existing infrastructure, implementing a scalable solution, and centralizing policy administration from a single management console for multiple mobile devices (laptops, PDAs, smartphones and USB flash drives).
 - 4) **Support:** effectively support mobile users while enforcing data controls for lost or stolen devices while minimizing impact of ongoing maintenance and data recovery.

Data security is rapidly becoming the number one concern of companies, customers and legislators. By adopting the methodology outlined above, enterprises can ensure their mobile data remains secure in the event of a security breach. In a single solution, CREDANT Mobile Guardian supports this methodology with the features and functions necessary to secure mobile data across the enterprise.

ABOUT CREDANT TECHNOLOGIES

CREDANT® Technologies 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® 2005. Austin Ventures, Menlo Ventures, Crescendo Ventures, Intel Capital and Cisco Systems are investors in CREDANT Technologies. For more information, visit www.credant.com.

CREDANT MOBILE GUARDIAN PRODUCT SUMMARY

CREDANT Mobile Guardian (CMG) Enterprise Edition is an award-winning, scalable mobile security and management software platform that enables organizations to easily secure and manage disparate mobile and wireless devices from a single management console. While most features described in this document relate to CREDANT Mobile Guardian Enterprise Edition, many of these features also are available in the CMG Group Edition, specifically designed for department-specific initiatives within large organizations and for small- to mid-size enterprises with limited IT resources that must minimize risk while centralizing mobile security policies. CREDANT also offers the CMG Personal Edition for the individual employee through select OEM partners such as Hewlett Packard.

CMG Enterprise and Group Editions consist of the following components that work together to provide this centrally managed security for mobile data:

CREDANT Mobile Guardian Shield - provides robust on-device policy enforcement - access control, strong authentication, intelligent data encryption and user permissions

CREDANT Mobile Guardian Gatekeeper - automates device detection and distribution of Shield client and policies and enforces ongoing compliance to security policies

CREDANT Mobile Guardian Enterprise Server - provides centralized security policy administration, integrates with existing enterprise directories and creates audit logs and reports

CREDANT Mobile Guardian is the only solution to combine enterprise management capabilities with strong mobile data security – all in a package that is easy to deploy and manage, and is easily accepted by end users. With CMG, companies can cost-effectively support a mobile workforce and improve employee productivity, with the peace of mind that their 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

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 © 2006 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.

DetectProtectManageSupport_WP_0406