



Stay Out of the Headlines — The Next Generation of Encryption for Notebooks, Tablets and Desktops

**CREDANT Technologies
Security Solutions
White Paper**



February 2006

Table of Contents

Never Has Information Been More Available and Less Secure	3
What Does CREDANT Mobile Guardian Shield for Windows Protect?	5
How CREDANT Mobile Guardian Shield for Windows Works	8
CREDANT offers Total Data Protection	8
Minimum Overhead, Maximum Protection.....	8
Protecting User and Shared Sensitive Information	8
Protecting Temporary Files.....	9
Protecting the Windows Paging (Swap) File	9
Protecting the Windows Password	9
Protecting Removable Media	9
Recovering Encrypted Data	10
Traditional Approaches to Encryption	11
Comparing and Contrasting Intelligent Encryption, Full Disk Encryption, and File/Folder-Based Encryption.....	13
Conclusion	15
More Information	15
Contact Us	15

Never Has Information Been More Available and Less Secure

In a business world threatened by negligence, regulatory compliance, sabotage, corruption and terrorists, never has corporate data been more available and less secure. The Privacy Rights Clearinghouse's chronology of data breaches lists 118 companies that have reported breaches since February 2005. These data breaches have impacted over 53 million Americans who have had their personal information compromised. Driven initially by California law, the data breaches were reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. More alarming is the fact that 27% of the company's data breaches were the result of a computer, notebook computer or removable storage device being lost or stolen – and the number impacted, 1.2 million Americans, may be grossly underestimated because some companies did not know how much information was stored on the stolen computer.

Gartner estimates that through 2006, 90% of mobile devices that contain business information will have insufficient power-on protection and stored data encryption to withstand casual to moderate hacker attacks¹. CREDANT Mobile Guardian is designed to protect a heterogeneous mobile computing environment comprised of notebooks, tablet PCs, PDAs and smartphones from a wide variety of manufacturers using operating systems such as Windows, Palm, Windows Mobile, RIM Blackberry, Symbian and others. However, by far the most widely used type of mobile device today (and the device which contains the most amount of data) is the Windows Notebook platform. This white paper will focus specifically on securing vital, sensitive information stored on Windows-based notebooks, tablet PCs and desktops.

The requirements for protecting the data at rest on a Windows-based desktop or notebook are quite simple – ensure that only authorized users can gain access to any sensitive information stored on the computer and ensure data is protected when moved to an external storage device. The only way to effectively protect sensitive information is to enforce the use of a strong password and provide a second layer of defense with industry-standard and validated encryption. Encryption scrambles the information making it inaccessible to unauthorized users. Sensitive information needs to be encrypted regardless of where it is stored on the hard drive or removable media such as a USB fob or an iPod. However, you also need to ensure that this encryption is as transparent as possible to the end user to ensure acceptance and discourage work-arounds.

Of course, there is a vast amount of data on a notebook or desktop hard drive that does not have to be protected, because it does not contain sensitive information. The Windows Operating System files and Program files are binary files that do not contain sensitive data. Encrypting these files significantly impacts an organization's every day support and maintenance procedures. Worst case, encrypting these files can have catastrophic consequences, as corruption of an encrypted OS file or program file could cause system instability and possibly prevent the machine from booting or a user from logging in, causing remote or traveling employees to be unproductive or worse, lose all their data.

CREDANT Mobile Guardian Shield for Windows (CMG Shield) takes a revolutionary new approach to protecting information assets against loss, theft, attack and unauthorized use. CREDANT's next generation patent-pending Intelligent Encryption provides four levels of defense that ensures the protection of vital information *no matter where it is stored*. Intelligent Encryption fills the security gaps left by file-based products and the management and recovery issues, data corruption and productivity losses associated with full hard disk encryption.

Protecting sensitive information is critical. The CREDANT solution provides a cost-effective deployment and management infrastructure that greatly eases the burden on IT. Finally,

the CMG Shield is virtually transparent to authorized users while enabling them to always have access to their PC and information without changing the way they work.

Combining the end user's acceptance of security, the ease of deployment and management for IT, and the use of Intelligent Encryption to effectively secure data, CREDANT enables organizations to enforce security policies to ensure regulatory compliance with CREDANT Mobile Guardian Shield for Windows

CREDANT Mobile Guardian (CMG) Shield for Windows is a component of CMG Enterprise Edition, CREDANT's award-winning enterprise-scale security and management software suite designed to protect all PCs - Windows notebooks, tablets and desktops, as well as smartphones, PDAs and external storage media such as USB drives.

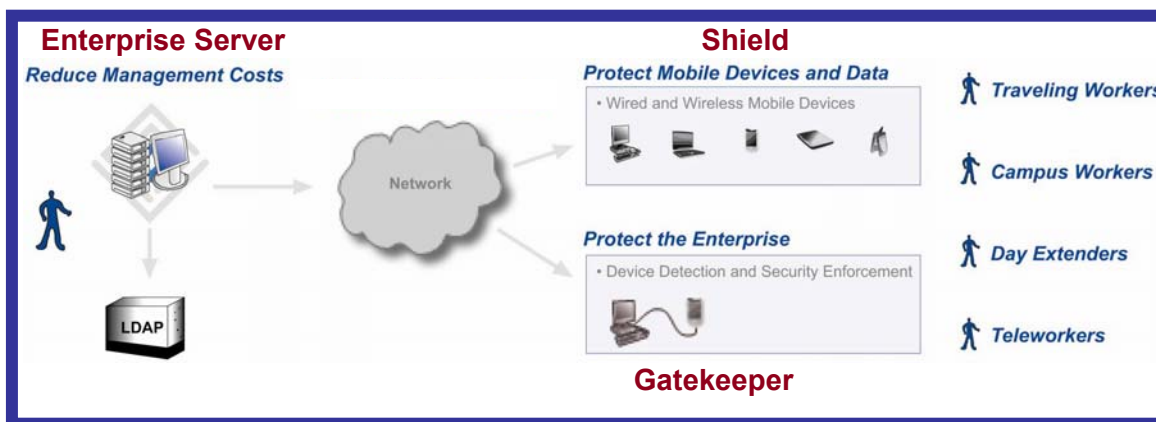


Figure 1 CMG Enterprise Architecture

CMG Shield for Windows, using CREDANT's patent-pending Intelligent Encryption process, is the first solution for notebooks and desktops that ensures sensitive, vital information stored on these computers is protected, no matter where the data is stored. Providing comprehensive security for Windows, CMG Shield is transparent to end users and is the most cost-effective solution to deploy and, more importantly, manage and support long-term by IT departments.

Up until now, organizations have only had two choices – count on a user to store a file in a special folder that ensured it was encrypted or encrypt the entire hard drive. However, full hard disk encryption products are riddled with management, support, and recovery issues, data corruption concerns and productivity losses. CREDANT's Intelligent Encryption reduces overall management, eliminates data corruption, recovery issues and productivity losses associated with full disk encryption, and closes the security gaps created by file/folder-based encryption.

In addition, CMG Shield for Windows has received FIPS 140-2 validation for the CREDANT Cryptographic Kernel under the joint US National Institute for Standards and Technology (NIST) and Canadian Communications Security Establishment (CSE) Cryptographic Module Validation Program. This independent product validation ensures that the product is correctly performing cryptographic operations and that your sensitive information is secure.

CMG Shield allows organizations to:

- **Reduce risk** with enforced, policy-based on-device security, including mandatory access control, stored data encryption, and data destruction capabilities;
- **Minimize recovery and support costs** by not having to decrypt the complete hard drive which can add hours or days to the recovery process;
- **Ensure compliance** with regulations such as HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, California SB1386 and others by ensuring encrypted data stays

protected – even during routine maintenance such as an administrator upgrading existing applications, troubleshooting or simply modifying the local operating system settings;

- **Enable productivity and ease-of-use** with the ability for secure recovery and password reset at all times, whether connected or not;
- **Leverages investment in existing IT infrastructure** by integrating with enterprise directories such as Microsoft Active Directory and providing the ability to control security for diverse mobile devices from a single console.

What Does CREDANT Mobile Guardian Shield for Windows Protect?

CMG Shield's Intelligent Encryption protects vital information by combining information about who the user is and what they are allowed to see with information about essential files that need to be protected on notebooks and desktops. Rule-based, CMG Shield encrypts all essential information without encrypting the entire operating system or application files. Unlike file-based solutions, CMG Shield encrypts shared data, user data, temporary files, the Windows Paging file, the Windows Password hash that is stored in the registry, and data stored on removable media.

Rules, specified by the security administrator, govern which folders, files and *types of files* are to be automatically encrypted by CMG Shield on the notebook, tablet PC or desktop. No end-user actions are required to encrypt data. In addition, CREDANT is able to provide total data encryption by ensuring that any file written from any application that the user is running is encrypted no matter where it is saved. This ensures that data is encrypted even if a user accidentally or intentionally saves a file to the Windows OS directory, or if they try to get around the security by renaming files to look like system files. Furthermore, the user cannot disable or bypass the encryption process.

This approach allows the security administrator to establish compliance with privacy regulations such as HIPAA or California Bill SB1386 by encrypting sensitive customer databases and files, without any user action and without encrypting non-private files such as Windows OS or program files

Data files are encrypted and decrypted transparently, on-the-fly as they are accessed by the active user. The data is decrypted by the read process as applications such as Microsoft® Word, Excel, Power Point, Outlook, ACT! or others open and access files. The data is encrypted by the write process as applications modify and store data. This is a completely user-transparent model and does not require any additional user action beyond login. This is also an application-transparent model and does not require any additional application code or integration to function.

Data access and the encryption process are controlled with a CREDANT-enhanced Windows login process. CREDANT provides two modes of the enhanced Windows login process, a full GINA replacement and a GINA-less option.

Enterprises that are looking to implement strong two factor authentication with a PKCS11 smartcard, RSA SecurID for Microsoft Windows, biometric authentication, or another authentication mechanism can use the GINA-less option. This option provides seamless integration with the Windows login process without modifying or associating with the Microsoft GINA. This means that your existing GINA replacements will continue to work with the CMG Shield installed and operating in this mode. Furthermore, end users are not required to login twice using this option. Once the user has successfully authenticated to Windows using the strong authentication, the necessary authentication credentials are automatically passed to the CMG Shield giving the user access to the encrypted data.

Enterprises that do not have a preferred authentication mechanism in house and are looking for a stronger, more secure authentication process than the Windows login can use the

CREDANT GINA replacement option. The login process looks and acts like the standard Windows login procedure, but uses a patent-pending approach to protect the user's Windows password hash and encryption keys until the user successfully logs in. Upon successful login, the active user's encryption keys are unlocked. Encrypted files are then ready to be decrypted on-demand as needed.



Figure 2 GINA Replacement Option

In both modes of enhanced Windows login, only the encryption keys for the active user are unlocked upon successful authentication. Since individual users have individual encryption keys, users are unable to access another user's private information. This allows multiple people to share the same computer securely without sharing passwords and without having access to others' private information.

Both modes provide seamless help desk recovery capabilities in the event that a user has forgotten their password. The GINA-less option follows the normal Windows recovery model. An end user calls the help desk and has the password reset on the domain controller by an administrator. On the next login using the new domain password, the CMG Shield will automatically detect that the user has successfully authenticated to Windows and perform an automated and transparent HTTPS based challenge/response recovery with the CMG Enterprise Server. The end user will not notice this process occurring and within a very short time after login, the end user will have access to all encrypted data.

The GINA-replacement option offers a self-service password reset capability to ensure that users can always gain access to their device, even if they have forgotten their Windows password and aren't connected to the network. The user merely answers the question they selected during the initialization process and are then allowed to reset their Windows password, without calling the help desk OR having a network connection. In the event that this fails the user can call the help desk for an over-the-phone password recovery using a secure challenge/response recovery mechanism shown in Figure 3 on the next page. The use of this challenge/response procedure ensures that users are always productive by enabling them to immediately regain access to their PC while traveling, without requiring them to connect to the Windows domain controller.



Figure 3 GINA Replacement Help Desk Recovery

In summary, CMG Shield protects Windows password and removable media, all sensitive information stored on a mobile PC such as a notebook or tablet, or on a desktop PC. CMG Shield provides flexible authentication mechanisms allow enterprises to use strong two factor authentication products, existing GINA replacements, or leverage the CMG Shield GINA replacement for added protection. CMG Shield is transparent to end users, is cost-effectively deployed and managed by IT, and provides comprehensive security to protect sensitive information at all times.

How CREDANT Mobile Guardian Shield for Windows Works

CMG Shield for Windows uses patent-pending Intelligent Encryption that enables a security administrator to easily define rules that govern the application of encryption on a machine. The product is extremely flexible: the process can be as simple as defining entire drives or partitions, or as detailed as your environment dictates. Intelligent Encryption applies a defense in depth approach to encryption. The four levels of defense include:

- **Volume and removable media encryption** automatically encrypts data written to any fixed disk or removable media attached to the machine. Encryption of the operating system is not required guaranteeing faster recovery time, less impact on performance, and no integration is required to support strong authentication.
- **File type encryption** automatically encrypts all new and previously created files of a specified type (or multiple types) regardless of where they are stored on the hard drive. This ensures protection of legacy data, temporary and swap files.
- **Application data encryption** automatically enforces encryption of any data written by applications to protect against user error or malicious renaming of a file type that would leave data exposed. This patent pending approach requires no modification to the application and is transparent to both the application and the user.
- **User level encryption** automatically enforces encryption of user specific data ensuring that local administrators and other users with machine access cannot access any other users' sensitive data.

CREDANT offers Total Data Protection

The defense-in-depth approach described above provides a significant number of company and user benefits. It provides the protection necessary to secure corporate data, but offers the flexibility and ease-of-use that cannot be matched by older, first generation encryption products. Key benefits include:

Minimum Overhead, Maximum Protection

CMG Shield for Windows provides a single security policy which defines any/all of the four levels of encryption, and allows all the data files created or owned by a user to be encrypted automatically, wherever the data files are saved on the disk, and whatever their name. This approach means that only the data that needs to be secured is encrypted – no unnecessary encryption of system or program files to slow down system performance. Furthermore, there is no ability for a malicious end user to bypass the encryption process by saving the file into a certain folder, changing the file name, or changing the file extension.

Protecting User and Shared Sensitive Information

Both user information and shared information can be encrypted by CMG Shield for Windows. Shared data can be encrypted and shared between multiple users on a machine or encrypted for an individual user. The CMG Shield utilizes two separate encryption keys to accomplish this, a common encryption key and user encryption key. The application of the encryption keys are determined by simple security policy settings that are defined in the administration console (e.g. Encrypt 'My Documents' – applies user encryption key).

In addition, unlike full disk encryption products, this option allows a number of users to share the device, but with each user having their own private data files which only they can read. This is especially important when the machine needs to be serviced because of a disk fault – technicians are able to read all data on the disk with full disk encryption products. This is not so with CREDANT's user and common encryption capabilities – Helpdesk

personnel can use standard tools to diagnose and fix faults, but your CFO's data always stays secure.

Protecting Temporary Files

Many applications create temporary files during routine file operations. These files are typically stored in undisclosed locations on the hard disk. The CMG Shield provides security policies that enforce the encryption of temporary files and temporary internet files that are saved to disk. Once the CMG Shield is installed it seeks out these files and automatically encrypts and protects the contents. Any future temporary files are automatically encrypted as well ensuring complete protection.

Protecting the Windows Paging (Swap) File

CMG Shield for Windows protects the Windows Paging or Swap file to ensure that any sensitive information that is contained in the file is protected.

A unique encryption key is generated each time the PC boots, and is used to protect the Paging file for all users. The Paging file is encrypted when not being used by Windows, and is decrypted on the fly when it is being accessed by Windows.

Protecting the Windows Password

Windows stores a hash (a cryptographically manipulation) of the Windows domain password (which is used to login to the domain and to gain access to a disconnected PC) in the registry. There are several generally available programs such as LC 5 (formerly known as LOphtCrack) that take advantage of the stored hash to do a brute force attack of the password by generating passwords, calculating their hash, and comparing them to the hash stored in the registry. If the two hashes match, the attacker knows that he has the correct password. Another type of attack simply resets the password saved in the registry by booting the computer from a floppy disk or CD and running a simple program.

CMG Shield for Windows protects from these types of attack by removing the hash from the registry and storing it in a secure location that is protected by CREDANT encryption.

The user would login to their PC using their Windows password which is checked by CMG Shield for Windows. If they successfully login to their device, then the Windows password hash will be decrypted, placed in the registry only when needed by Windows, and then removed and stored securely in a CREDANT encrypted location.

This approach dramatically improves the security of the Windows password mechanism and ensures that the encrypted information stored on the PC cannot be compromised by using tools to determine (or reset) the Windows password; those tools no longer work because the Windows password hash is only available for a short period of time in the registry WHEN A USER IS ACTUALLY logging in, and is encrypted the rest of the time.

Protecting Removable Media

More and more users are employing USB 'thumb' drives, portable media players (e.g. iPods), and other low-cost data backup devices. This represents a significant security hole in many solutions designed to just protect data at rest on a disk drive. All it takes is one connection of the USB cable and your end users can transfer millions of bytes of sensitive data that can easily be transported in an unprotected state outside of the walls of the enterprise.

CREDANT provides easy to configure security policies to allow administrators to specify exactly what happens to data when it's copied to any kind of removable media. Administrators have the option to set a security policy called "Encrypt

Removable Media” which ensures that all user data written to any removable media will be encrypted. They can also specify a “Scan Removable Media” policy which forces all existing data on removable media to be encrypted upon insertion to a CREDANT protected machine. In addition, any data that is encrypted on removable media will be encrypted with the user’s roaming credentials (encryption key). Controlled by policy this enables companies to contain the use of USB drives within the company while maintaining maximum portability and confidentiality. Roaming Credentials permit encrypted data to be read on any CREDANT protected machine in the enterprise once the end user logs in – an ideal situation for the user who needs to do a PowerPoint presentation on another computer.

For enterprises that are looking to provide their end users with the maximum flexibility in transferring data, CREDANT also provides a built-in encryption option, CREDANT2go (added to the SendTo menu) that allows a user to create self-extracting encrypted archives of one or more files. CREDANT2go produces an executable file that can be run on any Windows machine regardless of whether CREDANT is installed or not – this is especially useful if files need to be sent to other users that are not part of the enterprise, if files need to be archived on a separate system, or if an end user needs to take a file to a home office machine to work.

Recovering Encrypted Data

One of the challenges with any type of data security solution is how to recover data if the encryption keys are lost – the simple answer is that if the keys are lost, then the data is lost too. It is therefore imperative that every precaution is taken to securely protect the keys.

Unlike competitive products, all encryption keys are generated and securely escrowed by the CMG Enterprise Server before being passed down to the device, thereby ensuring that they can never be lost.

Other solutions generate the keys on the device, requiring the end user to manually store them on a separate device (e.g. floppy) or initiate an out of band process to store them centrally (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. stored on a network drive) then recovery of encrypted data may not be possible. From an Enterprise point-of-view, this is a significant and unnecessary risk.

With CREDANT, recovery of encrypted data can always be done, from the time the first bit of data is encrypted until the machine’s end of life. Keys are generated and escrowed on the server, then passed to the device. Recovery is automatically facilitated and does not require decryption and encryption again, and is completely transparent to the end user.

Traditional Approaches to Encryption

In this section, two existing approaches to protecting mobile information will be examined against the requirements previously outlined.

1. Full Disk Encryption (FDE): FDE products ensure that mobile information is secure by encrypting the entire hard drive, including Windows operating system and program files, as well as a variety of pre-Windows boot files. While this approach may, on the surface, seem like the easiest and most secure approach, these solutions can be extremely costly in the long run due to the following limitations:

Reduces End User Productivity

- Encrypting the whole hard drive can result in hard drive failure rates higher than normal, resulting in lost productivity as users must surrender their notebook to IT to have it recovered; several users of full disk encryption products have estimated failure rates in the 8-10% range
- Not compatible with standard Windows features such as Hibernation and Defragmentation
- Modification of the master boot record by third-party software (such as Altiris Backup, TurboTax, Partition Magic, etc.) can cause the full disk encryption program to fail, rendering the hard disk and PC unusable and resulting in the loss of all data
- Requires long initial encryption process which cannot be successfully accomplished by many end users
- Windows System Files and Program Files are encrypted, slowing boot time and affecting application performance

Expensive to Recover and Support

- Requires administrator to manually define users and groups before solution can be deployed due to lack of integration with enterprise directory services such as LDAP or Microsoft Active Directory
- Ghost image recommended before deployment, not just data backup
- Increases support cost and extends "instant recovery time" from minutes to hours and, in many cases, days for "broken" computers because IT has to decrypt the entire disk where as before they could simply use a Windows Recovery disk
- May not be compatible with all versions of BIOS and manufacturers of hard drives/computers
- In-person IT provisioning is usually recommended for full hard disk encryption products, due to issues with the time to encrypt the entire hard drive and potential hardware compatibility issues
- End user training required to ensure successful deployment due to changes in login behavior
- Significant costs associated with end user downtime and time/resources to restore data lost due to increased hard drive failures

Security Limitations

- Many companies have administrators who perform routine maintenance for ongoing support purposes including upgrading existing applications, troubleshooting and reinstalling an existing application, or modifying the local operating system settings. With a full disk encryption product, an administrator needs to have an administrative login for the pre-boot authentication that gives them access to the machine and all

encrypted data on the drive. This means an administrator who is performing routine maintenance will have access to all encrypted data on the drive even though they do not require this access to perform routine maintenance.

Data Loss

- Some data may never be recovered from a corrupted device with full disk encryption.

The successful adoption of security balances deployment, management, support costs and end user acceptance. While considered "secure", the lack of balance in full disk solutions has caused many deployments to fail, resulting in frustration, lack of trust in a solution, unprotected mobile information and significant back-end costs for recoveries.

2. File/Folder Based Encryption: Another alternative is to use a file-based solution that can enforce that the contents of specified folders (such as C:\Secure Folder) are automatically encrypted. These solutions have a number of serious security limitations, including:

Only specific folders/files can be encrypted

- Does not protect sensitive information stored on removable media, in the Paging File, or any files which are not stored in the specified secure folders

User controlled security

- Users must store sensitive information in the specified secure folders, otherwise it is not protected

Microsoft's Encrypting File System, a standard part of Windows 2000 and XP, is a widely available file-based solution which also suffers from these security limitations, as well as from the availability of certain utilities such as LC 5 and EFSCrack which can be used to bypass the Windows password or crack the EFS encryption keys and gain access to the sensitive information.

In summary, neither full disk or file-based encryption meet all the security, management and ease-of-use capabilities required by organizations looking to ensure that their sensitive information is protected at all times.

Comparing and Contrasting Intelligent Encryption, Full Disk Encryption, and File/Folder-Based Encryption

Management	Intelligent Encryption with CMG Shield for Windows	Full Disk Encryption	File/Folder-Based Encryption
Centralized administration for all mobile platforms	Yes	No	No
Integrates with LDAP/ Microsoft AD so administrators don't have to manually define users/groups	Yes	Some	Some
Will work on all computers regardless of BIOS, hardware, and installed programs	Yes	No	Yes
Works with software deployment tools (e.g. SMS, Marimba, Tivoli, etc.)	Yes	Yes	Yes
Detect and report handheld usage across Windows platforms	Yes	No	No
Enables enterprises to enforce encryption of only sensitive data based on simple encryption settings	Yes, Intelligent Encryption	No, entire hard disk is encrypted	No, only folders and/or files
Support multi-user environment with user and shared encrypted data functionality	Yes	No	Some
Provides a flexible deployment scheme where full data protection can be turned on over time and not all at once	Yes	No	No
Recovery	Intelligent Encryption with CMG Shield for Windows	Full Disk Encryption	File/Folder-Based Encryption
Requires decryption of the entire disk drive to restore the operating system or recover end user data	No	Yes	No
Self-service password recovery	Yes	Some	No
Modifies the Master Boot record making system recovery more complex	No	Yes	No
Secure Key Generation and Escrow	Yes Keys are generated and escrowed on the server, then passed to the device	No Keys are generated on the device and must be manually escrowed	No Keys are generated on the device and must be manually escrowed

Comparing and Contrasting Intelligent Encryption, Full Disk Encryption, and File/Folder-Based Encryption (continued)

Secure	Intelligent Encryption with CMG Shield for Windows	Full Disk Encryption	File/Folder-Based Encryption
Enforces automatic encryption for external storage devices	Yes	Some, but may be a separate product	Some, but may be a separate product
Prevents access to encrypted data during routine maintenance by administrators	Yes	No	Some
Encrypts swap file	Yes	Yes	No
Encrypts Windows password hash preventing brute force attack	Yes	Yes	No
Encrypts temporary files	Yes	Yes	No
Securely overwrites clear text residual	Yes	Yes	No
FIPS 140-2 Validated	Yes	Some	Yes
Supports Two-Factor Authentication	Yes	Some	Some
Control and secure handhelds across Windows platforms	Yes	No	No
Ease of Use	Intelligent Encryption with CMG Shield for Windows	Full Hard Disk Encryption	File/Folder-Based Encryption
Requires minimal end user training	Yes	Yes	No
Requires end user to be encryption aware	No	No	Yes
Requires pre-boot authentication adding an additional password	No	Yes	No
Encryption transparent to end user	Yes	Yes	No

Conclusion

CREDANT Mobile Guardian Shield for Windows protects your brand and ensures regulatory compliance by securing valuable information on notebooks and desktops against loss, theft and unauthorized use. CREDANT's approach to encryption is far superior to the more antiquated solutions on the market today. CREDANT's patent-pending Intelligent Encryption process uses defense-in-depth encryption to enforce the protection of vital information no matter where it is stored, eliminating the data corruption, productivity losses and back-end costs associated with full hard disk encryption and filling the security gaps left by file/folder-based products.

This ensures peace of mind that your data is secure in addition to compliance with privacy regulations such as HIPAA or California SB1386 – all by enforcing the automatic encryption of sensitive data without any user action.

CMG Shield for Windows is an integrated component of CREDANT Mobile Guardian Enterprise Edition which enables organizations to enforce security on all mobile devices and Windows PCs, ensuring that information is protected at all times.

More Information

More information, including data sheets, case studies, analyst reports and additional business and technical white papers are available in the CREDANT Technologies Resource Center (registration required): www.CREDANT.com/login.php

Contact Us

Please contact us for more information about how we can help meet your Windows and mobile device security needs:

CREDANT Technologies

15303 Dallas Parkway, Suite 1420
Addison, Texas 75001

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.

© 2005 CREDANT Technologies, Inc. All rights reserved. CREDANT Technologies, CREDANT, the Be Mobile Be Secure tagline, the CREDANT logo are, or will be, registered trademarks of CREDANT Technologies, Inc. All other trademarks, service marks, and/or product names are the property of their respective owners. Product information is subject to change without notice.

CMGforWindowsWhitePaper0206

ⁱ Gartner Symposium 2004: Wireless Security Presentation