
ADVANCES IN ENDPOINT DATA SECURITY:

New Technology to Meet Security, Operations and Compliance Needs

Date: February 19, 2008



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.

© 2008 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.

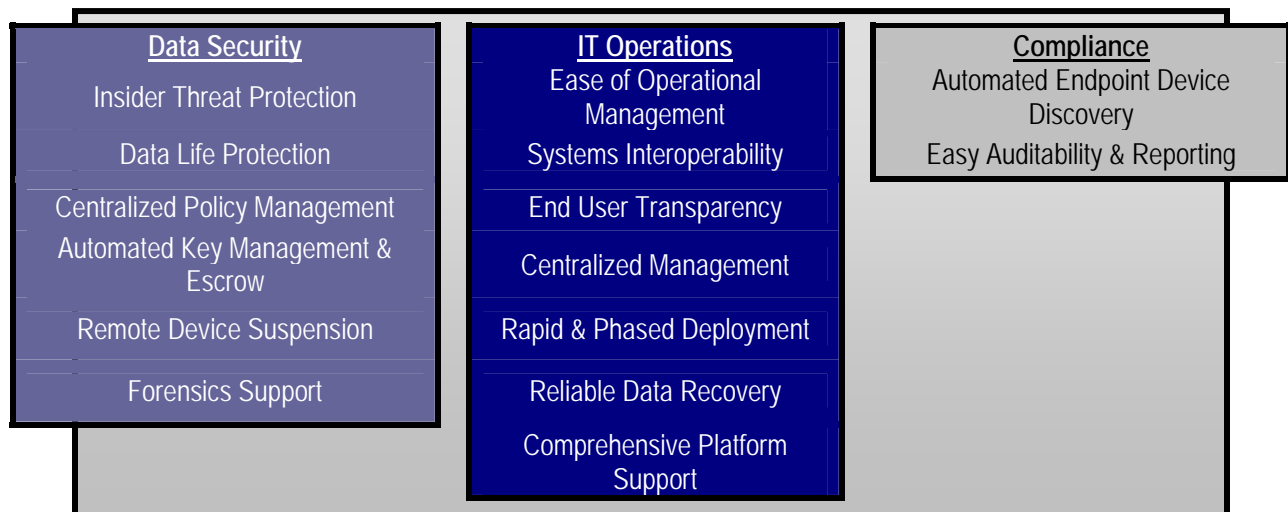
Endpoint Data Protection is about Protecting What Matters Most... ... Your Data

Data security has evolved beyond simply securing “bits on disks.” To ensure data protection in today’s dynamic IT environment, leading analysts recommend that security protects what matters most – the data. This requires a solution with a single, integrated security architecture and a data-centric, policy-based encryption approach that can be consistently enforced wherever the data resides – across heterogeneous endpoint device types, operating system platforms, and end users. The paradigm must shift from Full *Disk* Encryption to Full *Data* Encryption.

Full Data Encryption Requirements

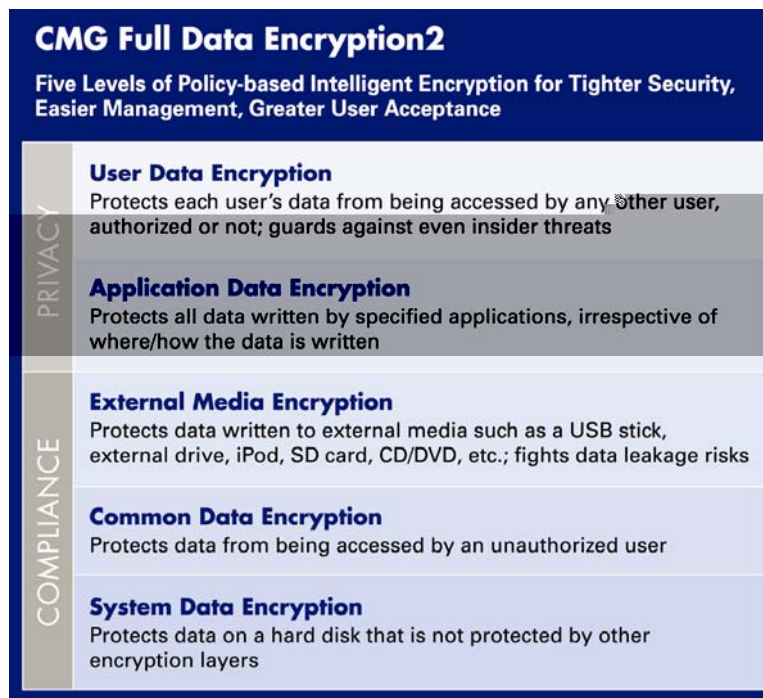
First generation encryption products such as Full Disk Encryption were designed over 15 years ago to protect primarily Windows-based endpoint devices. Unfortunately, this focus on the device means they were architected as stand-alone, platform-specific point products. There is no centralized console to consistently enforce or manage security across the various types of endpoint devices. From a data encryption perspective, these first generation products work by encrypting the entire hard drive, including the operating system and all application files. While this “encrypt everything” approach may, on the surface, seem like the easiest and most comprehensive approach to data security, it is not the best methodology in the long run due to lack of protection against insider threat and significant manageability, recovery, and usability issues.

Companies today need a Full Data Encryption solution that simultaneously meets their security, IT operations, and compliance needs:



Full Data Encryption Requirements

Only CREDANT Mobile Guardian (CMG) offers the single-system security architecture, single management console, and transparent end user interface you need in a scalable, yet easily deployed and managed solution. CREDANT's policy-based Intelligent Encryption technology is the only approach that provides multiple layers of security to deliver next generation CMG Full Data Encryption2.



CMG Full Data Encryption2

CMG protects corporate data no matter where it is stored. CMG's newest layer of Intelligent Encryption, System Data Encryption (SDE) for laptops, provides a foundation that enables greater security than Full Disk Encryption (FDE) and does not have the increased cost or operational, security, and data recovery problems inherent with first generation technologies. CMG goes further than any other offering on the market in maintaining the inherent portability and productivity benefits of mobile devices, while ensuring the confidentiality and full, easy recovery of corporate data.

DATA SECURITY

Corporate data is at risk from every direction. Encryption protects against external threats but what about threats from inside the organization? According to the 2007 CSI/FBI Computer Crime and Security Survey, 64% of the firms surveyed had measurable losses due to inside data leakage¹. To protect against data leakage – especially internal exposure – you must control who gets access to specific types of data. In addition, you must enforce endpoint data access controls, authorized application usage, and balance security implementation with usability. The question is, how?

The classical answer is through the access controls that are built into the operating system. The problem with that answer is that access control lists (ACL's) have been notoriously hard to manage. Full Data

Encryption2 provides a simpler approach to solving this problem by only allowing the user with access to the encryption key to view the data.

Insider Threat Protection

How do you protect information from insider threats in a multi-user or shared computer environment?

First generation technology products encrypt the entire hard disk using a single encryption key: there is no way to protect one user's data from any other authorized user accessing the same hard drive. For instance, when IT technicians perform routine maintenance on the CFO's laptop, they must decrypt the entire disk before they can begin to diagnose problems or make changes. Both are authorized users, however, the CFO may not want the technician to have access to confidential financial data stored on the laptop. Likewise, there is no way to support multiple levels of administrator privilege. Because everything on the disk must be decrypted before IT's work can begin, any technician, irrespective of their level of privilege in the company's security hierarchy, would potentially have access to all the data on every FDE "protected" machine in the company. Another example is found in a hospital where multiple doctors and nurses use the same FDE "protected" computer to access many patients' information. In this case, doctors and nurses should only have access to data about their own patients.

CREDANT Mobile Guardian provides stronger security because it protects against unauthorized data access from internal and external threats. How do we do this?

- ☑ *Multi-layered Intelligent Encryption technology delivers CMG Full Data Encryption2 with critical business controls to ensure data privacy balanced with usability.* CREDANT's multiple layers of defense extend compliance controls to endpoint devices and ensure that data-at-rest is protected at all times. Our unique, policy-based approach is the only one that follows the leading analysts' advice to "protect data, not devices." What's more, CMG is the only solution that can apply encryption at the volume, file-type, application, user, or system level. This gives companies the flexibility to encrypt only what needs to be encrypted or to encrypt everything on the disk (like full disk encryption products but without the operational limitations).
- ☑ *Policy-based data privacy controls prevent data leakage – inside or out.* Only CMG enables companies to define who has access to what data and ensure that only the owner of the data can get access to the data. This is advantageous when many people share one laptop or when company information needs to be kept secure during routine maintenance of the user's device. This is also important for companies that have different security policy requirements by user role or department. CMG even includes five administrator roles to ensure the scalability and flexibility needed to meet existing IT and security procedures while ensuring the integrity of the administration process. What's more, CMG also includes seamless integration with Cisco NAC to help address threats coming from endpoint devices or the network.

Full Disk Encryption



Full Data Encryption2



CMG Full Data Encryption2 for uncompromised operations and tighter security against insider threats

Centralized Policy Management

Endpoint security is more than just encrypting data. Companies must manage security across a wide variety of device types and platforms. They must control how endpoints access corporate networks and data; enforce which applications can or cannot be used on each endpoint device; and decide what type of communication methods are allowed/not allowed.

CREDANT enables administrators to easily control and secure a broad range of mobile device platforms—iPods and USB flash drives; Microsoft Windows-based desktop, tablet and notebook PCs; Windows Mobile devices; Palm-, RIM-, and Symbian-based smart phones, and PDAs—and any sensitive data that resides on them from one console. Authorized administrators simply access CMG through the web interface to see and manage their LDAP and mobile security infrastructures from a single view. They can even create custom reports using a variety of reporting tools already in use by the organization.

With CREDANT, security administrators can automatically detect and discover extensive endpoint inventory data. Once collected, this information can be used to enforce device and data access policies, manage endpoint synchronization, control removable media, and meet auditing and reporting needs.

“Centralized management is recommended for most storage encryption deployments because of its effectiveness and efficiency for policy verification and enforcement, key management, authenticator management, data recovery, and other management tasks. Centralized management can also automate deployment and configuration of storage encryption software to end user devices, distribution and installation of updates, collection and review of logs, and recovery of information from local failures.”

US National Institute of Standards and Technology (NIST), *Guide to Storage Encryption Technologies for End User Devices*, Special Publication 800-111, November, 2007.

CMG makes it easy to manage endpoint security, prove that a specific device is protected, or show when a device last checked in with a valid policy. In just a few clicks, administrators can:

- ☑ *Define a mobile user's current state and determine whether access to handheld devices will be granted.* If a device has been lost, stolen or an employee has left the company, administrators can easily change a user's status to "suspended," or "deactivated." Upon the next attempted synchronization of the device, this policy change will take effect and prevent them from logging into CMG, unlocking the device, or accessing sensitive company information.
- ☑ *Determine whether a CMG protected endpoint device can synchronize with companion PCs that are not protected by CMG.* This ensures that only approved mobile users and CMG enabled devices can synchronize to corporate systems – eliminating the risk associated with inadvertent or malicious synchronization and controlling the flow of sensitive data from your corporate environment.
- ☑ *Enforce policies that specify what applications may or may not be run on each endpoint device.* This dramatically reduces helpdesk calls and the threat of malware and malicious code introduction to the network.
- ☑ *Protect information by restricting the use of communication ports or external removable media devices (including Compact Flash, SD cards or PCMCIA cards).* Based on each user's security policies, CMG supports a disable/enable option to protect against sensitive data being copied to external storage media. CMG also provides control over network access (wired or wireless), as well as the ability to disable/enable infrared ports controlling whether users can beam business cards, applications or documents to one another.

Effective policy for Scott Renegar on Dell Latitude D620 (CT612.Credant.Com)	
Policy Name	Current Settings (Update: 3)
Shield Access Control	
Domain Account Lockout	false
Enable Offline Password Changes	true
Password Attempts Allowed	2
Alpha Characters Required in Answer	true
Authentication Questions	
Mixed Case Required in Answer	false
Number of Characters Required in Answer	4
Numeric Characters Required in Answer	false
Question/Answer Attempts Allowed	3
Question/Answer Expiration Time	30
Question/Answer History Count	5
Question/Answer History Time	90
Question/Answer Reset	false
Special Characters Required in Answer	false
Access Code Attempts Allowed	2
Access Code Failure Action	Apply Cooldown
Access Code Required Message	Authentication Failed. Please contact your system administrator.
Access and Device Code Length	32
Cooldown Time Delay	30

Sample of CMG Security Policy

Automated Key Management & Escrow

Encryption key management and escrow are critical to ensuring a company's ability to fully recover data. First generation technologies that generate encryption keys on the endpoint device require end users to manually escrow the keys. This outdated approach often requires the end user to copy the keys to a floppy or USB drive and then transfer them to an administrator or a central server via some out of band mechanism. The end result: the ability to recover data is placed in the hands of the end user not the company – significantly adding to the complexity of endpoint security administration for IT and security groups. Even more problematic, the keys escrow process does not occur until after the data is encrypted. This means the recovery of encryption keys (and data) is not guaranteed. What happens if an endpoint device is lost or stolen or the end user forgets their password, loses the recovery device, never sends the keys to IT, or leaves the company before the keys are escrowed? How does the company recover the data? It doesn't. The data is lost and the company is at risk.

CREDANT Mobile Guardian automatically creates and securely stores (escrows) encryption keys at the server before any data is encrypted. CREDANT does not require any action by end users to escrow keys. This puts control in the hands of the company rather than the end user by ensuring that the company always has the ability to authenticate and access its encryption keys. With CREDANT, recovery of encrypted data can be performed immediately, from the time the first bit of data is encrypted until the data or machine's end of life. In addition, CMG also includes self-service and administrator assisted device recovery in case of end user authentication failure – even when a device is disconnected from the network.

Remote Device Suspension

First generation full disk encryption products protect data only if a device was properly shut down. If a device is lost or stolen, or an unauthorized user gains access to it after the disk is decrypted, all data contained on the disk is at risk.

With CMG, your security policy decides what happens when devices are lost or stolen or employees leave the company. Administrators can easily suspend access to a device, deny synchronization attempts, delete all data on the device, or change a user's status to "suspended" or "deactivated" to prevent them from logging on and accessing sensitive company information

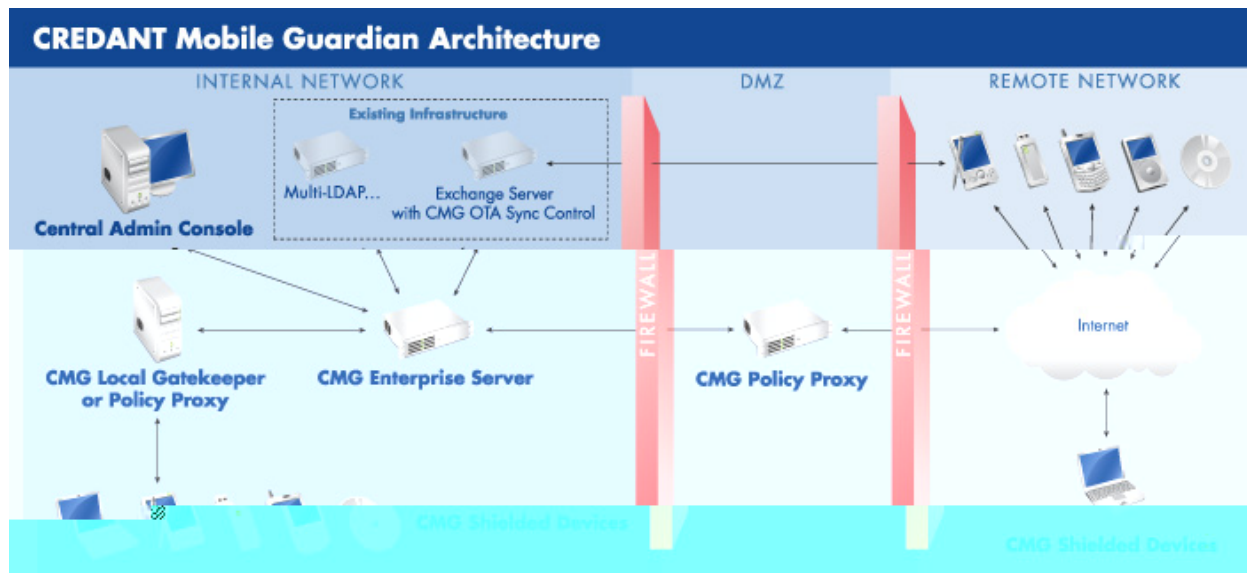
IT OPERATIONS

Another very important consideration when evaluating any encryption solution is the impact it will have on IT desktop support and network operations.

Ease of Operational Management

Since an “all or nothing” approach requires that the entire disk be decrypted and re-encrypted upon each reboot, established IT procedures must be changed to accommodate FDE. This adds lengthy steps to routine deployment, update, and maintenance tasks; increases systems’ complexity; and decreases operational productivity. As one Fortune 100 CIO put it, “Before FDE, a typical break-fix scenario required 90 minutes of an IT administrator’s time to get the problem resolved and the user up and running again. With Full Disk Encryption we discovered that this time increased to 7 hours per machine.” (CREDANT assesses this to be a 78.5% drop in IT productivity and a significant increase in Total Cost of Ownership (TCO).)

CREDANT’s low-impact solution provides endpoint security without decreasing productivity or increasing TCO. Why? CMG does not require organizations to change or add long steps to existing IT maintenance, data recovery or diagnostic processes. With CMG, there is no impact to existing: password reset operations, desktop operations, desktop backup requirements, or disaster recovery. CMG components are highly integrated and interoperate seamlessly using trusted, reliable communication paths. With CMG, administrators can automatically install CMG software on diverse endpoint devices and securely distribute mobile users’ security policies and encryption keys. In addition, CMG enables global, group, or individual user level security policies using read-only integration with existing enterprise LDAP directories to ensure consistency and scalability across the enterprise. You can even upgrade to newer versions of CMG while maintaining your existing policy information and encryption keys.



CREDANT Mobile Guardian Architecture

Systems Interoperability

Because FDE encrypts all operating system files, most FDE products require a proprietary pre-boot authentication process and Master Boot Record (MBR) changes. These modifications can cause serious compatibility issues with other hardware and software products that depend upon industry standard authentication and MBRs. For instance, some FDE products do not integrate well with Windows authentication interfaces and often require custom integration to support multi-factor authentication (MFA) (such as biometrics, smartcards or tokens) and single-sign-on (SSO) initiatives. This adds complexity and opportunity for something to break – not to mention increasing the potential attack surface which must be validated and certified with each version update of each component.

CMG works within the authentication framework provided by Microsoft Windows and the PKCS #11 Cryptographic Token Interface Standard. CMG does not require a proprietary pre-boot authentication process nor does it modify the Master Boot Record (MBR). This enables seamless support of multi-factor authentication technologies including flexible PIN / password parameters, smart cards, biometrics, and RSA SecureID for Microsoft Windows. Because it doesn't change anything, it does not add to the potential attack surface that must be validated and certified with each version update of each component. CREDANT has also achieved FIPS 140-2 Level 1 validation for the CREDANT Cryptographic Kernel (CCK) and for CREDANT's implementation of the AES, 3DES, SHA-1, HMAC-SHA-1, and RNG algorithms across all CREDANT supported platforms.

End User Transparency

Companies today must minimize the impact endpoint security has on end users yet simultaneously and transparently control what an end user can do on or with an endpoint device. Unfortunately, an "all or nothing" encryption approach encrypts bits on a disk so end users cannot access anything until the entire disk is completely decrypted – not even non-critical data or applications. This significantly increases the amount of time end users must wait each time the device is powered up or down. This delay may create frustration and invite end users to avoid using endpoint security (by not shutting down their devices) – putting all data on the device at risk.

CREDANT Mobile Guardian's encryption, authorization, and other security policies are silently enforced so there is minimal impact on end users. With CMG, there is no additional end user training, no impact upon initial encryption, no impact on system performance, and no waiting for Operations to recover lost data. CMG's powerful, yet flexible security policies deliver the transparency you need to:

- ☑ *Perform data encryption upon demand.* This means there is no delay in accessing data or any change to how end users work.
- ☑ *Ensure that Bluetooth-enabled devices such as PDAs or smart phones remain "always on" and active.* As long as the trusted Bluetooth headset or car kit remains in proximity, CMG users need only authenticate once to obtain constant connectivity to Bluetooth applications. (Real-time applications such as GPS navigation systems do not require authentication and are always available.) When the trusted Bluetooth device headset is no longer in proximity to the device, CMG can automatically lock the device to ensure the data it contains is secure.

Phased, Rapid Deployment

Whenever new functionality is introduced into an organization, it is an established IT 'Best Practice' to roll-out the functionality in stages as enterprise impact is assessed. For software, that means deploying the application with a minimum feature set enabled (to ensure that the software itself installs and runs correctly), then switching on features over a period of days or weeks, until the full functionality is available to users. An "all or nothing" approach forces companies to install and begin using all endpoint security features simultaneously rather than gradually turning on functionality. Should something go wrong, serious support problems can result due to a longer and more complex roll back process. Just imagine what would happen if an endpoint data encryption product was installed on the executive team's laptops and *after* the disks were encrypted, an unforeseen problem occurred that prevented the executives from accessing or recovering their data. This would quickly escalate into an IT nightmare. Simultaneously, it is also important that an encryption solution be rolled out quickly with minimal end-user impact and without requiring a full-time crew of professional services personnel.

CREDANT Mobile Guardian (CMG) is the only solution built from the ground up using a unified architecture and single administrative console. This means the deployment and ongoing management of a CMG environment is much easier for your IT organization. Why? CREDANT Mobile Guardian works with your existing infrastructure and enables companies to take a phased approach to deploying encryption software. With CMG, if unforeseen issues arise it will be fast and easy to back out any recent changes. Rather than rolling out encryption software to the entire organization and turning on all functionality at the same time, CMG enables companies to install the software in smaller groups and gradually turn on the features once IT is comfortable.

In addition to supporting phased deployments, CMG deploys more rapidly than other solutions. Why? With CMG there is no need to run a disk repair tool or defragmenter prior to installation and encryption (as is the case with FDE). What's more, CMG can encrypt an average laptop in minutes, while the end user is working. Most FDE solutions will take from 4 to 12 hours to encrypt every sector on a 60GB drive, even when there is no data on 90% of the drive. Finally, because CREDANT's removable media encryption is provided with the same client that encrypts the local hard disk(s), USB/iPod/CD encryption can be rolled out at the same time and at a much lower cost than rolling out and managing a separate solution.

Centralized Management

Another consideration is that a distributed architecture requires administrators to manually "touch" multiple consoles to repetitively install encryption software, manage encryption keys, and create or modify security policies on each platform. How do you ensure that endpoint security policies are up-to-date and consistent with those defined in your existing LDAP directories? How do you do this without increasing the workload of already overburdened security staff? The US National Institute of Standards and Technology (NIST) recommends that storage encryption be managed centrally and that organizations consider solutions that use existing system features (such as operating system features) and infrastructure.

CMG's unified architecture and data-centric methodologies provide a single, web-based management interface which decreases the number of platforms each technician must learn and manage. This minimizes errors, reduces training requirements, and lowers costs.

Reliable Data Recovery

To further ensure the ability to reliably and quickly recover data, usage of industry standard operating systems, authentication processes, and recovery tools must not be affected. Unfortunately, first generation technologies result in a dependence on non-industry standard, vendor-proprietary systems to boot endpoint devices. This may negate your IT department's ability to use existing diagnostic tools to identify problems, repair hardware, and/or recover data.

With **CREDANT Mobile Guardian**, data recovery is always ensured. The "System Data Encryption" (SDE) option within our Intelligent Encryption feature enables administrators to set policies that automatically encrypt everything not already encrypted by other options, including operating system and application files. However, unlike FDE-based technologies, SDE does not encrypt the handful of files required for the initial boot process. This enables companies to continue using their existing, industry standard operating systems and avoids the introduction of proprietary pre-boot authentication processes and modified master boot records. With CMG, IT personnel are able to use existing forensic and diagnostic tools to better repair hardware failures and recover corporate data.

Comprehensive Platform Support

Endpoint devices use multiple, diverse operating systems – each with nuances that impact data encryption operations. CREDANT Mobile Guardian supports more endpoint platforms than any other solution available and is optimized to run on each of these platforms to enforce mobile security policies consistently and efficiently across all endpoint devices using a single management console. Currently supported endpoint devices include: Pocket PCs, handhelds, smart phones, iPods and MP3 players and USB storage devices.

COMPLIANCE

Finally, the ability to quickly and easily prove regulatory compliance is the third critical consideration when evaluating any encryption solution. Endpoint inventory management, audit log analysis and compliance reporting require automated endpoint device discovery, a single view of endpoint security across platforms, and seamless integration with existing reporting tools. Unfortunately, first generation point products struggle with gathering endpoint inventory data and require administrators to access multiple consoles and then manually combine inventory data and audit log analysis to create compliance reports.

Automated Endpoint Device Discovery

CREDANT's Inventory Update process is a key aspect of the product's ability to provide Administrators and Auditors with the data necessary to prove compliance. CREDANT Mobile Guardian (CMG) tracks and maintains mobile device inventories so organizations can see how many and what types of devices are connecting to their networks – all from a single console. We also allow you to view inventory on a user or device basis which is additional granularity that some FDE products may not always provide.

Easy Auditing and Reporting

CREDANT Mobile Guardian provides tamperproof audit trails and streamlines inventory management across platforms – dramatically simplifying compliance reporting. CMG's centralized audit logs automatically and securely track administrator activity and system events. Properly authorized administrators can search the audit logs using a variety of criteria, including priority, date, time, user ID and machine name. Mobile device inventory management, policy management, auditing, and reporting are all

done through an ODBC compliant database using a variety of reporting tools already in use by the organization. Should data somehow be lost or stolen, CMG's audit logs and compliance reports help organizations prove that data on any of the CMG managed devices is protected – eliminating the need to go through a costly, time-consuming, and embarrassing public notification process.

Summary

Older generation products such as Full Disk Encryption (FDE) create a false sense of security, and do not provide the architectural flexibility needed to meet emerging endpoint security requirements. CREDANT's policy-based Intelligent Encryption technology is the only approach that provides multiple layers of security to deliver next generation CMG Full Data Encryption².

Only CREDANT Mobile Guardian (CMG) offers the single-system security architecture, single management console, and transparent end user interface you need in a scalable, yet easily deployed and managed solution. Only CREDANT Mobile Guardian (CMG) ensures that your security is consistently and efficiently enforced – regardless of where the data resides. Only CMG provides additional security levels above FDE and does not have the operational and usability impacts that FDE does.

CMG has demonstrated low operational costs, particularly in complex environments. This powerful yet easy-to-use endpoint security solution is the only centrally managed, policy based security management solution that provides Intelligent Encryption using industry standards. Only CREDANT delivers the security, flexibility, compatibility and scalability needed to meet your diverse and evolving enterprise data security requirements.

Contact Us

Please contact us for more information about how we can help meet your end point data protection and 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

ⁱ Computer Security Institute and U.S. Federal Bureau of Investigation, 2007 *CSI/FBI Computer Crime and Security Survey*, 2007.