

VORMETRIC WHITE PAPER

Six Rules for Encrypting Your Enterprise Data



VORMETRIC

Copyright © 2005 Vormetric, Inc. All rights reserved.

Vormetric, CoreGuard, MetaClear are trademarks or registered trademarks of Vormetric, Inc. in the U.S.A. and certain other countries. Other names and products are trademarks or registered trademarks of their respective holders.

The information in this document is subject to change without notice and must not be construed as a commitment on the part of Vormetric, Inc. Vormetric, Inc. assumes no responsibility for any errors that may appear in this document. No part of this documentation may be reproduced without the express prior written permission of the copyright owner.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.

Executive Summary

Regulatory compliance requirements for protecting personally identifiable information (PII) and risk mitigation strategies for protecting valuable digital information assets have led many enterprises and government agencies to consider encrypting their sensitive stored data. While the encryption algorithms themselves are well standardized, the myriad of technical solutions designed to achieve diverse objectives for securing information leave many security architects unsure which approach is best for their environment.

Determining the optimal approach to stored data encryption requires careful planning and a review of the organization's objectives for encrypting their data. By evaluating the solution's impact on business operations and deploying an appropriate architecture for the encryption operation, the organization can maximize the benefits it derives while minimizing the potential pitfalls that can impede operational processes farther down the line.

This document provides an introduction to planning for stored data encryption by offering six fundamental rules that should be considered prior to deployment. Following these rules will help to maximize the effectiveness of the encryption security layer while avoiding an adverse outcome that can result from unanticipated consequences.

Introduction

A RAPIDLY CHANGING RISK ENVIRONMENT

An increasingly dynamic and technically challenging risk environment has forced security and network administrators to change the way they think about securing their most sensitive information assets. New business models rely on open networks with multiple access points to conduct business in real time, driving down costs and improving response times to revenue generating opportunities. By leveraging the ability to quickly exchange critical information and improve their competitive position, enterprises are introducing new vulnerabilities that can be exploited to gain unauthorized access to sensitive information. Furthermore, the insider threat is now considered by many to represent the greatest risk to enterprise resources.

In addition to changes in the IT infrastructure itself and the way the information is utilized, the threat environment has evolved to represent a greater risk to the assets of the enterprise. Rather than pursuing notoriety through service disruptions or website defacements, attackers are pursuing economic gain, with the objective of stealing information while avoiding detection. A thriving black market for personal information and the opportunity to blackmail large organizations for their intellectual property ensures that a large amount of illegal activity will continue to be directed at stored personal data and digital assets.

PROTECTING SENSITIVE DATA WITH ENCRYPTION

In order to mitigate this increased risk, the use of encryption is increasingly being required or recommended as a best practice for protecting data at rest. Financial services institutions, merchants that accept credit cards, health care services and other companies and government agencies that maintain confidential personal information that could be misused for identity theft are all required to consider the use of encryption to protect their PII from inappropriate use.

Deploying encryption that provides effective protection of data across an enterprise environment, however, is a challenge that requires planning and forethought. Following are six rules that can be applied to any encryption project to help avoid unanticipated barriers and prevent future complications that will burden executives, security administrators and IT administrators alike.

#1: Address the Objective

The success of a security program will ultimately be decided by whether it achieves its objectives for mitigating risk to organizational assets. Often, however, administrators may embark on an aggressive data encryption strategy when other, more easily attained, means may achieve the same result. Taking a step back to evaluate the primary objective can help define whether encryption is the best safeguard, and, if so, what must be included in the scope of the solution.

BENEFITING FROM STORED DATA ENCRYPTION

Strong encryption is sometimes described as the ultimate protection for stored data. While this may be valid for archived media storage, encrypting data in an environment with many vulnerabilities actually provides little mitigation of risks to data at rest. Encrypting active or online backup data should be considered as enforcement of access control, the primary means of enforcing acceptable use policy. The intent of access control is to apply authentication, authorization and audit controls to all data requests before granting access so data can only be used in the appropriate manner. Strong, context-aware access controls enable a more granular authorization of access, such as by data user in conjunction with a particular application or time of day. Without strong access control that can also restrict data viewing by root level administrators, encryption only serves to protect against data extraction from stolen media and side door attacks.

Defeating encryption can also be achieved by hijacking unprotected hosts that serve as access points to sensitive data, which allows attackers to cloak themselves as legitimate data users. Host integrity enforcement is therefore essential to enabling encryption as an effective layer of security. Without this safeguard, vulnerabilities such as root attacks, trojan horse backdoors and unintended use of privileges remain unchecked and afford a means of attack to malicious users.

MEETING REGULATIONS AND INDUSTRY STANDARDS

To address the burgeoning identity theft crisis and protect the privacy of personal data such as health records, legislators and industry leaders have mandated regulations and standards that require the holders of personal information to take measures to prevent unauthorized access and viewing of that data. While not all of these regulations specifically require the use of stored data encryption, many organizations are moving ahead with implementing encryption for their protected information since a judicial interpretation will likely refer to best practice standards that advise the use of encryption in conjunction with other security layers to protect PII.

The following table provides a summary of several regulations that address the need for holders of PII to protect against unauthorized access and viewing.

Regulation	Affected Organizations	Encryption Requirement	Reference Document
Gramm-Leach-Bliley Act (GLBA) of 1999	Financial Service Providers	Review the encryption standards used by the institution for Non-Public Personal Information (NPI). The	Interagency " Examination Procedures to Evaluate Compliance with the

		selection of data to encrypt and the encryption technique and level should be supported by the risk assessment.	Guidelines to Safeguard Customer Information
California SB 1386	Organizations conducting business in California holding specific personal information	No specific requirement for encrypting personal data, but information that was stolen in encrypted format is exempt from data owner notification requirement.	California Office of Privacy Protection (COPP) best practice guidelines, ‘Recommended Practices on Notification of Security Breach Involving Personal Information.’
California AB 1950	Organizations conducting business in California holding specific personal information	Requires the use of safeguards to ensure the security of specific personal information when not in an encrypted or redacted form.	None specific, but relevant best practices can also be found in the COPP document ‘Recommended Practices on Notification of Security Breach Involving Personal Information.’
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Healthcare organizations	Encryption of stored Electronic Protected Health Information (EPHI) is not specifically required. Requires privacy-conscious business practices that protect EPHI from viewing by unauthorized persons including IT administrators.	Refer to HIPAA legislation or multiple best practice guides.
Payment Card Industry (PCI) Data Security Standard (DSS)	All PCI members, merchants and service providers that store, process or transmit cardholder data	The PCI recommends strong encryption for sensitive cardholder information as an approach to rendering sensitive cardholder data unreadable anywhere it is stored. Access to cardholder data must be restricted based on a need to know.	Payment Card Industry Data Security Standard Version 1.0.

ENFORCING SECURITY POLICY

Enterprise security policy increasingly defines ‘appropriate use’ of sensitive information assets that includes separation of duties and restricted access based on a ‘need to know.’ Application of these policies has often relied on some combination of soft controls that define processes and procedures and employee training. Properly deployed, encryption provides a technical safeguard that automates the enforcement of controls by limiting data viewing to authorized groups or individuals. Improperly deployed, however, encryption gives control over content to the data holder—not the organization or data owner. An effective design should include a centrally managed mechanism for defining the application of encryption that enables the data owner, such as business line management, and not the holder of the data, to control data viewing.

MEETING SYSTEM AUDIT REQUIREMENTS

Programs for encrypting stored data are often initiated following comments generated by external or internal auditors pointing to vulnerabilities to sensitive stored data. Encryption may be

recommended as a means of addressing those vulnerabilities. In other cases, the use of encryption allows the organization to avoid using alternative security technologies that are more intrusive and management-intensive. In these situations, policy-based encryption may be easily verified by auditors, reducing the time required for testing and system auditing. For database protection, the use of file-level encryption allows the organizations to avoid code changes to databases or applications while minimizing any negative impact on system performance.

#2: Don't Get in the Way of Operations

A successful encryption deployment means providing a solution that all groups in the organization can live with. Many encryption products either fail a pilot phase or, worse, have to be removed later because of a negative impact on business operations. Since revenue generation or productivity enhancement are, in most cases, the driving force behind IT resources, business line management will often have the final say.

PLANNING FOR DEPLOYMENT

Installing encryption into a live environment can introduce a high level of risk to business operations. Modifying a live application or database with code changes to enable encryption is, in most cases, an option that will generate howls of protest from system administrators. Adopting an approach that is transparent to applications, databases and storage has a much better chance of acceptance by business managers and the IT organization.

MAINTAINING SYSTEM PERFORMANCE

Encryption that provides excellent security but slows system response times to a crawl will not last long. Even where performance can be scaled with additional investment, the result will be conflict within the organization. Generally speaking, an impact on performance of 10% or less is expected and considered to be acceptable. Measures such as buffering or caching writes to encrypted databases may be used in a pilot test bed to artificially increase performance test results and mask poor system design. These introduce a high level of risk to data integrity in a production environment, however, and should not be considered as part of a valid evaluation.

The choice of encryption algorithm and key length will also have a significant impact on system performance. Given the use of the same algorithm, a shorter key length will have a lower impact on system performance. Selecting the shortest key length that provides an acceptable level of security for the life of the data and an efficient computing algorithm—for most, 128-bit AES—will minimize the additional overhead required to support encryption.

BREAKING DATA MANAGEMENT

The deployment of encryption may inadvertently prevent IT organizations from protecting the data that they are trying to secure by breaking their ability to use management utilities effectively. Backup, snapshot and replication applications that ensure data availability and preservation often need to read file system metadata in order to function properly. By applying encryption to the entire file, as do block-level storage encryption devices located within a Fibre Channel SAN, both the file system metadata and the file content need to be decrypted for the application to read the metadata. This approach defeats the purpose of the security by exposing file content to unauthorised viewing and copying at the backup server and incurs the cost of re-encryption after file system metadata inspection.

SCALABILITY

Scaling system performance is critical to meeting the needs of a growing business. Introducing another variable into the infrastructure that prevents scaling in a predictable manner can bottlenecking the flow of data and prevent the organization from achieving the forecasted returns on its IT investment. Encryption should be implemented in such a way as to leverage the existing, high-performance infrastructure and scale with that infrastructure.

#3: Consider the Encryption Architecture

As discussed earlier, system design is critical to achieving the objectives set forth in defining an encryption project. A mismatched architecture can create operational issues without delivering the security benefit that the encryption was expected to deliver.

POINT OF ENCRYPTION

Where the encryption takes place is a critical factor in achieving the organization's objectives for securing data. While encryption can be performed at nearly any point between the end point and the storage media, there are advantages and disadvantages associated with each in terms of performance, transparency, manageability and scalability, as described below:

Encryption Architecture	Example	Advantages	Disadvantages
End-Point System Encryption	Integrated Operating System Encryption	Transparent to network. May be used to protect mobile data.	May rely on action by end user, so protection is not automatic. End user, not organization, has control over access. Key storage on same system is vulnerable. A negative performance impact may discourage use.
Application-Level	Java Cryptography Extension	Protects data from unauthorized viewing from the application tier down to the data storage level. Transparent to management operations if encrypted backup is desired. May be centrally managed.	Supports Java and XML applications only. May be disruptive to operations, requiring integration into applications and impacting performance. Requires recoding of other applications that access encrypted data to enable key sharing. Application updates may require additional coding changes.
In-line Encryption (Block-level)	Fibre Channel proxy appliances	Easy to install and configure. Protects against extraction of data from storage media. Transparent to applications and users.	Does not protect from vulnerabilities above the appliance at the network level. Cost of scaling can be prohibitive, requiring many appliances. Interferes with operation of data management utilities without first decrypting information.
In-line Encryption (File-System)	Network file system proxy appliances	Easy to install and configure for departmental storage. Protects against extraction of data from media. May enforce user authentication via network services.	Limited protection for vulnerabilities above the level of the appliance. Cost of scaling can be prohibitive, requiring many appliances. No protection against compromised authentication service.

Database-Level Encryption	Column-level encryption add-ons	Prevents viewing of sensitive information by DBAs and others without a need to know.	Requires installation into DBMS. May require reconfiguration of data type and size, requiring modification of all applications that access that data item. Restricted to encryption of non-search key columns. No protection against compromised applications above the DBMS. Use of triggers and views to encrypt columns has a severely negative impact on database performance.
File System Level	Vormetric CoreGuard	Transparent to users, applications, databases, network file systems and data storage. Allows cost-effective scalability and flexibility. Geographically extensible with centralized management.	Requires support for individual operating system platforms.

STORING ENCRYPTION KEYS

Regardless of the strength of the encryption algorithm, access to ciphertext and the appropriate keys translates into the ability to view data. Effective information security requires storing encryption keys away from its access points. By physically separating key storage, a successful attack on a host server does not allow the attacker to recover data in cleartext form. A hardened appliance that serves as a secure access decision point and key repository prevents tampering and ensures that keys are only made available to legitimate and authorized requests.

Moreover, separating the point of decision for requests to decrypt data from protected access points provides separation of duties between security and IT administration. IT administrators can still manage host server applications, while security administrators are restricted to the configuration and management of security devices that grant need to know access to data. Because encryption is often implemented to satisfy auditors that an effective control on access exists, separation of duties between the administrator of the encryption and those whose access is controlled by the encryption is a key requirement.

#4: Integrate with Complementary and Dependent Technologies

As previously discussed, encryption alone provides limited value in respect to securing data from unauthorized viewing. System planning must consider both complementary and dependent technologies in order to ensure an effective solution.

ENFORCING APPROPRIATE USE WITH ACCESS CONTROL

For security objectives that go beyond protecting archived media, access control can be a complementary technology that is enhanced by encryption, or a dependent technology that both influences and is influenced by encryption, depending on the security objective. Strong access controls enable security administrators to define at a granular level what data specific users are

permitted to access, with what applications, and at what times of day. Where access controls may be defeated by circumventing authorized access channels—defined as authorized applications on known access points—to stored data, encryption complements access control by preventing extraction in a useful form. Access control also depends on encryption to provide the ability to control data viewability, a critical requirement for enforcing both ‘separation of duties’ and ‘need to know’ policies and achieving compliance with data privacy regulations.

PROTECTING HOSTS WITH INTEGRITY ENFORCEMENT

Vulnerabilities in host operating systems and applications provide another avenue for attackers to hijack access points to stored information. Once a host OS is compromised via exploitation of vulnerabilities or use of malware, for example, the attacker can gain root level access and run commands to access data. Controlling not only the integrity of the OS and applications, but also that of resource libraries and configuration files, is essential to preventing successful attacks. Application servers should be locked down to their ‘gold image’ to prevent the unauthorized use of organizational resources and the unintentional introduction of vulnerabilities into the system.

#5 Consider the Data Migration Process

A critical part of planning for the deployment of encryption involves migrating the data from cleartext to ciphertext form without disrupting operations. For new system installations, this will not be an issue, but for organizations with terabytes of data, the conversion may take a considerable amount of time, bandwidth and system overhead if running as a background process during live operation. Converting the data during backup windows is a preferable, non-disruptive strategy if this option is available.

#6 Define the Key Management Process

Mitigating the incremental risk introduced by encrypting data requires adhering to a well-defined key management process. Security administrators should be able to export keys, policies and related data to ensure that data recovery is always possible, even in the event of a catastrophe, given that backup data stored at a remote location is also available. The exported keys and associated data can be encrypted, password protected or otherwise secured and archived in an offsite location, such as a lockbox or escrow account to ensure confidentiality and availability.

Rotating keys with newly generated ones provides little benefit in terms of reassuring security as long as the existing keys have not been compromised and any responsible parties with access are still trusted or subject to sound controls. Given that a 128-bit encryption key provides over 339,000,000,000,000,000,000,000,000,000 combinations, taking upwards of thousands of trillions of years to crack, periodic key rotation has the potential for introducing significantly more risk than it mitigates.

CoreGuard Transparent Encryption

For organizations requiring strong encryption to protect their most sensitive data, CoreGuard provides a solution that is highly transparent, non-disruptive, highly extensible and manageable.

TRANSPARENCY AND EXTENSIBILITY

CoreGuard's extensible and manageable architecture provides consistent enforcement of security throughout the organization. CoreGuard's separation of policy enforcement at the protected host from policy decision making and key storage at the Security Server appliance provides a high degree of security and enforced separation of duties between system and security administration activities. Centralized control over policy deployment and management provides cost-effective operation and extensible protection wherever data is stored.

By enforcing policies at the file system of the protected hosts, CoreGuard is highly transparent to the existing IT environment. CoreGuard requires no code changes to applications or databases, and operates transparently to network file systems and data storage infrastructures as well.

CoreGuard uses the Advanced Encryption Standard (AES) encryption algorithm, designed to enhance the strength of the data protection while significantly reducing the system overhead required for computation. As a result, CoreGuard enables the use of strong encryption protection with long key lengths while imposing a negligible impact on business operations

METACLEAR ENCRYPTION

The file system intelligence of the CoreGuard system also allows it to encrypt file content separate from the file system metadata, which is kept in the clear. This encryption technology, known as MetaClear, enables the enforcement of policies that control the need to view sensitive data while still permitting access to ciphertext data for management operations.

MetaClear also protects data in process while avoiding disruption to data management operations. By leaving the file system metadata in the clear, storage administrators and data management applications can perform their functions without the need to expose file content in the clear or re-encrypt files following data management operations.

COMPREHENSIVE, INTEGRATED SOLUTION

CoreGuard integrates multiple technologies, including strong, context-aware access control, host integrity protection and detailed audit logging, into a single solution that can be deployed across an enterprise to address multiple data privacy and intellectual property protection requirements. By combining these essential technologies into one, policy-based system, CoreGuard protects high risk vulnerabilities that alternative encryption designs cannot.

KEY MANAGEMENT

CoreGuard enables the safe management of encryption keys by allowing for key, policy and configuration export in encrypted form. Recovery data can be stored on backup media and held in secure, remote facilities in the event of a catastrophic incident.

BENEFITS

CoreGuard's innovative, file system-level approach to encrypting data provides several benefits:

- Preserves the value of intellectual property assets by controlling data access and viewing
- Enhances compliance with strict regulations that address data privacy protection
- Enforces least privilege policy by controlling administrative viewing of sensitive information
- Provides non-disruptive solution by installing transparently to applications and data storage

- Enables separation of duties between IT administration and security administration
- Minimizes support needs by providing a single, manageable solution
- Enables consistent enforcement of company policy across a widespread environment

Summary

The rapidly growing need to protect personal data and digital assets from unauthorized access and viewing has led many organizations to evaluate the use of stored data encryption. As a final layer of protection, encryption enforces the access control function, ensuring that only access requests coming through authorized access channels are granted. Properly deployed with complementary technologies, encryption also enables the separation of data access from data viewing, enforcing a separation of duties between security and IT administration. Ensuring the successful deployment and continual manageability of encryption requires substantial planning and consideration of how to best achieve the organizational objectives.

Vormetric's CoreGuard provides a complete solution for information protection that integrates encryption with access control, host integrity protection and detailed auditing of all access events. CoreGuard is highly transparent, non-intrusive, manageable and scalable across a widespread organization. By providing a solution for multiple security applications, CoreGuard represents a high ROI investment for multiple enterprise information protection needs.

* * *

For more detailed information on the CoreGuard Information Protection System, please refer to the following Vormetric documents and video demonstrations:

Vormetric White Paper: "[Protecting Enterprise Information](#)"

Vormetric Solutions Brief: "[GLBA-Compliant Information Protection for Financial Services](#)"

Vormetric Solutions Brief: "[California SB 1386 & AB 1950: Implementing Effective Encryption Protection for Personal Information Privacy](#)"

Vormetric Success Story: "[Financial Services Institution Success Story for GLBA Compliance](#)"

[CoreGuard Information Protection System Datasheet](#)

[CoreGuard FAQ](#)

CoreGuard Video Demos:

<http://www.demosondemand.com/clients/vormetric/001/page/preview.asp>

Vormetric, Inc.

888.267.3732

www.vormetric.com

sales@vormetric.com



VORMETRIC

www.vormetric.com