

VORMETRIC WHITEPAPER

Securing Sensitive Agency Information (SAI) and Personally Identifiable Information (PII)

**Employing CoreGuard to track, manage, protect,
and erase SAI and PII.**



VORMETRIC

Table of Contents

Introduction	3
Tracking SAI and PII	3
Managing and Protecting SAI and PII	3
SAI and PII Protection Summary	5
Erasure of SAI and PII	6
CoreGuard™ Information Protection System	6
CoreGuard Architecture	6
CoreGuard Features	7
Context-Aware Access Control	7
Host and Application Integrity Protection	7
Audit, Alert and Reporting	8
Data at Rest Encryption	8
Enterprise-Class Design	8
Transparent Integration	9
Conclusion	9

Introduction

Vormetric's CoreGuard solution for data security enables the tracking, managing, protecting, and erasure of Sensitive Agency Information, particularly Sensitive Agency Information (SAI) and Personally Identifiable Information (PII), extracted from controlled IT environments such as data stores and databases. CoreGuard's least privileged access control enforcement significantly reduces and limits the potential for unauthorized or malicious release of SAI and PII and provides secure logging and audit data to identify the potential sources of SAI and PII data leakage or loss. The patented CoreGuard approach of providing policy based decryption enables SAI and PII data protection as well as data access management control to further reduce all forms risk to stored data. And, CoreGuard's centralized key management services can be utilized to perform virtual data shredding.

Tracking SAI and PII

Organizations have long relied on corporate policies and threats (implied and specific) of disciplinary action to keep both directly and indirectly authorized computer system users from unintentionally or intentionally disclosing sensitive data. In many cases, authorized users have figured out that there is very little chance of the organization detecting the source of an unauthorized data loss, so policies have very little value as a deterrent. This lack of accountability can lead to a lax attitude concerning proper handling of sensitive data which can result in disclosure of information, whether intentional or not.

The use of technology to implement critical deterrence and detection functionality is required to limit the risk of unauthorized access, misuse and destruction of sensitive data. The implementation of auditing, logging, alerts and notification services are the most proven methods of deterrence and detection at the data access level. The technology employed to instantiate these highly recommended services must be highly secure, robust and full featured to deliver an effective and unalterable means of deterrence and detection.

CoreGuard maintains a detailed audit trail of all attempts, successful or not, to access protected resources. This audit trail details who, what, where, when and how of the access attempt which is typically enough data to pinpoint the insider making the access request. It also provides information on the file operation being attempted (read, write, delete, change permissions, etc.) which can be used to identify, track and monitor potential avenues for inappropriate dissemination of sensitive information.

CoreGuard stores the audit logs on the Security Server Appliance (SSA) so that IT administrators can not use their administrative privilege to alter the log information to hide their activities. Only security personnel with access to the SSA can manipulate the CoreGuard audit logs. The SSA can be configured to send out alerts to Syslog, SNMP or email in response to specific events such as an unauthorized access attempt to files on a specific host.

The CoreGuard solution can be deployed on both Agency Enterprise Servers and Agency Desktops with support for the Windows, Linux, Solaris, HP-UX and AIX operating platforms.

Managing and Protecting SAI and PII

Encryption has become an important proactive security control used to prevent the risks associated with the loss, exploitation, and theft of sensitive data – both SAI and PII. This control is particularly important with respect to preventing the use of the compromised data to commit fraud, theft or espionage. The process of encrypting data renders it unusable, protecting SAI and PII from intentional or un-intentional exposure.

One of the best ways to manage proliferation of SAI and PII within the enterprise is to tightly control access to the data while it is at rest. Vormetric's CoreGuard controls access to data at rest using a

combination of policy-based user access control, encryption and detailed audit logging to restrict access to sensitive data, thus keeping it from proliferating within the enterprise thus lowering the risk and effort required to monitor, track and manage data in motion.

CoreGuard uniquely protects data stores and information repositories where SAI and PII reside on both heterogeneous servers and desktops encompassing both local internal disk, direct attach storage (DAS), network attached storage (NAS), storage area networks (SAN), as well as tape back up data sets. Regardless of where data resides – in databases, database logs, database archives, database dump files, file servers, email servers, print servers, print logs, etc. as well as web and application servers and their logs – CoreGuard protects all file system based data.

Encryption alone, however, is not enough to prevent and protect against all the risks to sensitive data. Vormetric's CoreGuard provides several tools to protect against the un-intentional or unauthorized use of SAI or PII.

CoreGuard's high-speed data encryption prevents users from bypassing the policy based user access controls. Files can be encrypted using AES-128 or AES-256 symmetric key encryption algorithms to prevent unauthorized access. The use of encryption forces users to gain access to protected data via CoreGuard, especially with built-in separation of duties for security administration which central manages the encryption key repository.

Encryption without access control, however, will not protect the data. If the ability to decrypt the data is not restricted based on the principle of least privilege, virtually any user can access decrypted data. CoreGuard applies policy-based user access controls to provide intelligent control of the aforementioned encryption. These access control policies govern who, what, where, when and how access is granted as it relates to protected information. Thus the information access request adheres to the principle of least privilege when determining whether or not to decrypt the data.

In addition, both host and application integrity protection are essential to ensuring the proper systems and applications are accessing SAI and PII data sets. CoreGuard can lock down protected hosts to their "gold image", preventing changes that are inconsistent with the security policy from being made to the platform. Unauthorized applications such as worms, Trojans and other forms of malware, are blocked from running and from propagating, protecting information from the introduction of data-directed malware. CoreGuard digitally signs the authorized application images and allows only images with the proper signatures to run in a protected environment.

Furthermore, Separation of Duties is required to ensure a "two man rule" security policy where certain actions (i.e. encryption key and policy changes) can only be implemented if approved by two authorized users thereby establishing "no lone zones" in the security model. CoreGuard's Security Server Appliance (SSA) and the use of a dedicated security administrator instantiates a "no lone zone" security model. Also, by storing user access policies, encryption keys and audit logs on a separate, hardened server appliance, IT administrators are unable to utilize their administrative privilege to bypass the access controls put in place to protect sensitive data. Since symmetric encryption is only as secure as the key management, CoreGuard separates the encryption keys from the data and stores them in a hardware key store. CoreGuard is FIPS 140-2 certified (FIPS certificate #442).

The last key area of managing and protecting SAI and PII is the segregation of duties: separating data access from data viewing. CoreGuard uses a patented method of encryption called MetaClear™ Encryption. MetaClear encrypts the body of the file using the specified symmetric key while leaving the file header in the clear. This allows for IT administrators to perform administrative operations on the file such as backups without requiring the file data to be decrypted. This prevents IT administrators from using their administrative privileges to view data they are only authorized to manage. In this manner, CoreGuard segregates the duties of users who need to manage protected files from users who need to view the contents of protected files.

CoreGuard's Policy Enforcement Module (PEM) performs all encryption of data on the local machine and does not require SAI and PII to be transferred to external devices. For environments where SAI and PII is transferred across the network to a client machine (file servers, NAS, etc.), placing the PEM on the client will result in the data remaining encrypted while being transferred across the network and then decrypted locally.

When deployed in conjunction with a Data-in-Transit/Motion, Data Leakage Detection and Content Filtering solutions such as Vericept, Websense, Vontu and/or Verdasys, the full data lifecycle can be securely managed. Once CoreGuard has granted least privilege access to SAI and PII Data-at-Rest, through their EDGE client solutions, Vericept, Websense, Vontu and Verdasys can control data distribution by authorized users to authorized secure application channels such as secure email or laptop/USB drive encryption solutions like Credant or Pointsec.

SAI and PII Protection Summary

Data Loss Threats	Methods Employed	CoreGuard Mitigation
Privileged Theft The ability to illegally obtain 'trusted' root access privileges.	Password cracking, buffer overflow, local login and privilege escalation.	<ul style="list-style-type: none"> • Encryption • Separation of duties • Audit
Application Tampering The alteration or insertion of executable code for the purpose of running an unauthorized version of the application.	Trojans, worms, unauthorized patches and altered or corrupted code.	<ul style="list-style-type: none"> • Host Integrity • Application Authentication • Audit
Unintended Privilege The use of root access or DBA privileges to access and view information outside of a user's authorized role.	Copying of data, control and user files or tables, transmission of data, viewing of data, and deleting or altering data and access logs.	<ul style="list-style-type: none"> • Encryption • Separation of duties • Audit
Data or Log Tampering The alteration of data or audit logs.	Access to data at rest, including database or file content and audit logs, via (i) the operating system, (ii) in transit to or from storage, or (iii) local access to the storage system.	<ul style="list-style-type: none"> • Encryption • Audit
Storage Media Theft The theft of storage media or hardware from a datacenter or in transit to or from a vaulting facility.	Physical theft.	<ul style="list-style-type: none"> • Encryption
Unauthorized Data Copy Making copies of sensitive data files in order to circumvent access control or disseminate sensitive data.	Copying sensitive data to external media, a different location on the same system or across the wire to another system	<ul style="list-style-type: none"> • Encryption • Separation of Duties • Policy-based Access Control
Unauthorized File Sharing – Enabling file sharing in a manner	Sharing local drives or altering ownership or file	<ul style="list-style-type: none"> • Encryption • Policy-based Access

that enables unauthorized users to view sensitive information	permission rights on a file or directory	Control <ul style="list-style-type: none"> • Audit
Damaging or Corrupting Data - Intentional or unintentional changes to data	Malicious corruption, insider carelessness, malfunctioning application code	<ul style="list-style-type: none"> • Policy-based Access Control

Erasure of SAI and PII

Vormetric's CoreGuard enables electronic file shredding so that data can be securely and permanently deleted from disks. CoreGuard ensures that SAI or PII is written to disk in an encrypted format, and all encryption keys are stored in secure hardware. Through the process of erasing or zeroing out the centralized encryption keys, all copies of SAI and PII data protected by the encryption keys can be securely and permanently deleted regardless of location or storage media.

CoreGuard™ Information Protection System

Mitigating the intentional or unintentional loss of SAI and PII requires a combination of tracking, managing and protecting, and data retention management. CoreGuard™ by Vormetric provides the tools required to deter, prevent and detect unauthorized access to sensitive data. CoreGuard is the only solution to integrate multiple controls into a single, extensible product to protect data privacy. CoreGuard controls (including encryption) are transparent, flexible, and centrally managed. Specific to encryption, our approach and architecture relieves the burdens and hurdles associated with encrypting data such as key management, key escrow, unacceptable performance degradation, and costly application and infrastructure changes. CoreGuard combines high-speed data encryption with policy-based user access controls to prevent users from accessing data without proper authorization. CoreGuard further provides a critical audit trail identifying who accessed (or attempted to access) what data, where, when and how.

CoreGuard Architecture

CoreGuard is comprised of two distinct components. These are the CoreGuard Security Server and the CoreGuard Policy Enforcement Module or PEM. The CoreGuard Security Server is responsible for policy creation of data access and privacy rules, key management of encrypted data and audit logging. A single security server can manage hundred's of host systems with differing OS types. The CoreGuard Policy Enforcement Module, which resides on your host computer, is responsible for data encryption, file system integrity and separation of policy enforcement from policy creation and management.

CoreGuard Features

Context-Aware Access Control

A data encryption product that lacks an effective method of enforcing authentication or access control can easily be spoofed into surrendering decrypted data to an unauthorized user, application or host. CoreGuard employs a five-factor system that requires the context of each data access attempt be validated by a data owner-definable policy. Through this validation process, CoreGuard enforces flexible and fine-grain mandatory access control. The five factors that make up this Context-Aware Access Control system can be described as who, what, where, when and how.

Context Attribute	Purpose
Who (Subject)	<ul style="list-style-type: none"> • Ensure that the Process User ID (PUID) has been authenticated AND • Authenticate the Application being invoked AND • Verify that PUID is authorized to invoke the Application.
What (Operation)	<ul style="list-style-type: none"> • Identify file system Operations available to Subject (e.g., read, write, copy, delete, rename, append) for the target Object
Where (Object)	<ul style="list-style-type: none"> • Identify specific protected data (e.g., file name(s), directory, wildcard) that can be accessed by Subject
When	<ul style="list-style-type: none"> • Verify time window that the Subject is authorized to use for window-sensitive Operations (e.g., backup, contract employees)
How	<ul style="list-style-type: none"> • Manage: Grants access to clear-text metadata, but encrypted file data OR • View: Grants access to clear-text metadata and clear-text file data for data viewing privileges.

By requiring validation of all five context criteria, all attempts to access data by unauthorized means are blocked. Users with root privileges, non-production applications, patches or operating/file-system calls, zero-day worms and Trojans can all be blocked with an unmatched degree of certainty.

Host and Application Integrity Protection

In the majority of attempts at compromising stored information, the initial point of attack is likely to be directed at the most accessible point of vulnerability-the host server. CoreGuard protects information from attack via compromised hosts by blocking all unauthorized processes from running and enforcing a 'gold image' of protected host servers. By verifying the cryptographic fingerprints of both protected applications and resource files, CoreGuard can not only stop zero-day worms and Trojans from accessing, tampering or deleting protected files, but also prevents the execution of malicious code or unauthorized applications introduced by internal users.

The deterministic nature of the CoreGuard policy definition format provides accuracy in detecting and blocking attempts, intentional or unintentional, to run malicious or unauthorized applications on protected

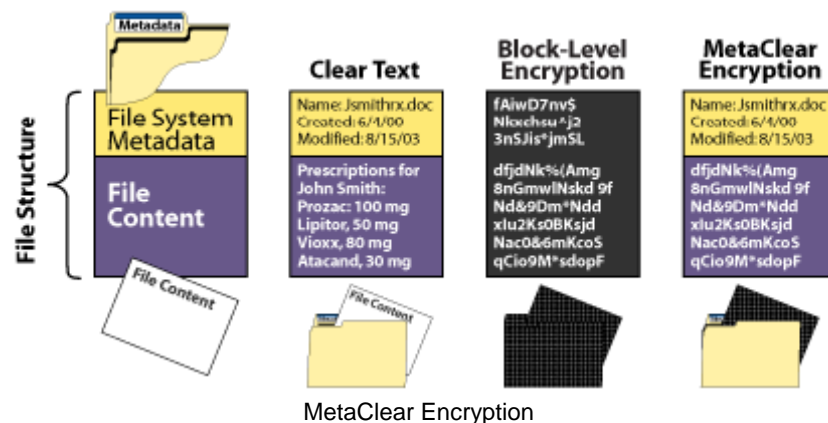
hosts. This accuracy eliminates the challenges faced by other host protection schemes such as Host Intrusion Detection Systems (HIDS) and Host Intrusion Prevention Systems (HIPS) that are susceptible to false alarms or evasion, and avoids the distraction of extensive event logs and the vulnerability to denial of service attacks based on false positive events and alerts.

Audit, Alert and Reporting

Assuring data integrity in compliance with regulatory legislation and system audit guidelines requires logging and forensic reporting of all data access activity. CoreGuard audits not just access requests from authorized access points, but also all requests that attempt to circumvent authorized access channels, and notifies security administrators of policy violations in real time. CoreGuard records all context attributes of the request, enabling complete traceability of host intrusion and data access events to the application and user level, and providing an extensive access log for detailed forensic analysis.

Data at Rest Encryption

Encryption of data at rest provides a means of enforcing access control functionality by defeating attempts to access clear text data that bypass authorized access channels, including the acquisition of information by physical theft of storage media or hardware. The file system-aware CoreGuard encryption engine extends this capability, separating the encryption of file content from the file system metadata, which is kept in the clear. By leaving the metadata in the clear, data management applications can perform their functions without the need to expose the file content in the clear for management operations and without the need for decryption and subsequent re-encryption. This technology, known as MetaClear™ encryption, enables the separation of access to file data from the ability to view such data. By decoupling access to data from the viewing of data, MetaClear enables the enforcement of 'least privilege' security policies by permitting data management without data viewing, resolving the conflict between the need to secure data at rest and the need to manage that data.



Enterprise-Class Design

To ensure that the needs of the most demanding IT environments are met, the CoreGuard System has been designed to support the most stringent, enterprise-class standards.

- **Security Policy Correlation** —Enables enforcement of enterprise security policies defining the appropriate use of data.
- **Extensibility** —Supports distributed enforcement of centralized policies across a widespread, heterogeneous enterprise.
- **Scalability** —Cluster Ready, load-balanced appliances scale linearly in performance. Each appliance supports hundreds of PEMs

- **Availability** —Non-stop availability through fully redundant cluster architecture.
- **Manageability** —Centralized interface minimizes points of management. Configuration changes can be pushed out to host PEMs for quick and easy policy updates.
- **Impervious to Attack** —Split network and security administration domains enforce separation of duties. Administrative auditing logs all configuration settings and changes to security parameters.

Transparent Integration

CoreGuard is transparent to the surrounding IT environment and has a negligible impact to overall application and database performance. CoreGuard protect hosts and application in two ways: 1) by identifying the specific executable files and related resource libraries that are authorized to run and inserting the cryptographic fingerprints for the authorized resources into a reference database, CoreGuard is able to effectively lock down the host to a 'gold image' and precisely define what processes are allowed to run on any protected system; and 2) CoreGuard prevents any process that cannot be authenticated against the reference database from loading into memory, ensuring host integrity and preventing any unauthorized processes from compromising the host gold image configuration.

Since CoreGuard operates at the file system level, it is transparent to applications running on the target host. As such, there is no formal integration required and no application compatibility issues. The result is that CoreGuard can easily be inserted into an existing environment with minimal disruption.

Conclusion

While most organizations have made significant progress establishing a least privileged access model at the extranet remote access layer and the intranet/extranet presentation layer, the data layer has not been addressed. Vormetric's CoreGuard is uniquely capable of implementing least privileged access at the data layer which significantly reduces data loss by enforcing access and distribution channels for SAI and PII. This also provides clearly identified authorized channels for monitoring SAI and PII data leakage and data loss.

The tracking, managing, protecting, and erasure of Sensitive Agency Information, particularly Sensitive Agency Information (SAI) and Personally Identifiable Information (PII) can not be accomplished by employing a data leakage/loss prevention and content filtering for data-in-transit alone. A multiple purpose data-at-rest solution is required to effectively address both data-in-motion and data-at-rest cohesively. Vormetric's approach to securing stored data through encryption and policy based accessed control with logging and auditing capability is the most effective means of tracking, managing and protecting, as well as the erasure of SAI and PII today.

For more information:

Vormetric Inc
3131 Jay Street
Santa Clara, CA 95054
www.vormetric.com
+1 408 961 6100
Email: sales@vormetric.com

Copyright © 2007 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.