

VORMETRIC WHITEPAPER

Information Assurance in an Enterprise Hosting Environment

Employing CoreGuard
to Protect Non-Public Information
and Intellectual Property in an
Enterprise Hosting Business



VORMETRIC

Table of Contents

Introduction	3
Assessing Traditional Data Protection Methods	3
CoreGuard™ Information Protection System	4
Advantages for Enterprise Hosting Providers	4
Additional Advantages for Auditing	5
CoreGuard Architecture	5
CoreGuard Features	6
Context-Aware Access Control	6
Host and Application Integrity Protection	7
Audit, Alert and Reporting	7
Data at Rest Encryption	7
MetaClear Encryption	8
Enterprise-Class Design	8
Transparent Integration	9
CoreGuard PEM	9
CoreGuard Security Server Appliance	9
Proven Leadership with Vormetric	10
Summary of Threat Protections	11
Conclusion: Protecting Data Inside and Out with CoreGuard	12

Introduction

Enterprise hosting is a highly attractive strategy in today's complex and agile technology marketplace. Customers are making the decision to focus on their core business rather than dedicating resources to implementing and managing IT infrastructures. The result is an environment where an enterprise hosting company is managing one or more data centers used by multiple corporate or government customers. In this environment, data security is critical in gaining customer trust. Customers must be assured that their data will be protected from all manner of threat, both external and internal. They also need to feel confident that their data is protected from unauthorized access by the systems administrators. This paper will discuss how to protect your customer's sensitive data while still providing administrators the access they require to effectively manage the hosted environment.

Assessing Traditional Data Protection Methods

Traditional methods of providing data security for their clients in a hosted environment include:

Physical Segregation: Taking the customer's servers and putting them inside a cage in the data center on a dedicated network. The customer retains the key and only their administrators have access to the cage(s) and the network connected to the servers. While this provides a level of physical security, the client is still required to manage their servers, thus reducing your value to the client. Additionally, should someone hack into the systems, the digital information contained on them is available for the taking.

Employee Screening and Training: While finding the right employees and training them appropriately is essential, it does not impose any actual controls on the people with access to client's sensitive data.

Corporate Policies: Written policies that define who has access to what client's sensitive data are important, but policies do not provide any actual protection against unauthorized access or information theft.

These traditional methods, which are often carried over from dedicated corporate data center, do not translate well into the enterprise hosting model. The ability to control who has access to sensitive data is critical. In the enterprise hosting business, extending that control across multiple organizations is key. Without this ability, clients are left to either encrypt all data – which often hampers the ability to manage the systems – or trust that administrators (and potentially personnel from other organizations) won't access data they are not authorized to access. One scenario reduces your value to the customer and the other is often a reason to select another vendor and possibly leaves you vulnerable to lawsuits.

Companies that offer enterprise hosting services need a new way to enforce data privacy and protection policies to protect themselves as well as their customers. As part of this data security initiative, companies must:

- Create and maintain policies that control both system administrator as well as customer employee access to data at the hosted site.
- Deploy and enforce their policies on a global scale.
- Prove that the policies are working as expected, and identify anyone who attempts to circumvent the policies.

CoreGuard™ Information Protection System

Vormetric's CoreGuard is the only commercially available product that combines context-aware access controls, high performance encryption of data at rest, and full operational controls including complete audit and logging for all accesses to protected data into a single extensible product. 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 users avoid the cost and on-going maintenance of multiple point solutions and, as a result, benefit from real savings and better administrator productivity. Its policy-based enforcement ensures that enterprise policy is enforced consistently across the enterprise, enabling compliance with regulatory requirements.

Advantages for Enterprise Hosting Providers

By implementing Vormetric's CoreGuard to protect customer data, enterprise hosting providers gain the following advantages:

- **Competitive Edge:** CoreGuard enables you to promote data privacy and protection as a competitive advantage that differentiates your company in your market. If you serve multiple customers that compete against each other, CoreGuard provides demonstrable assurance that any entrusted data will be visible only on a need-to-know basis (i.e. only to the customer and not to the datacenter staff or hackers).
- **Secure Administration:** Vormetric's ground-breaking MetaClear encryption allows management of data without visibility, so your IT administrators can still manage your customer's data; even though they are not able view it.
- **Access Control:** Database administrator access is managed via Vormetric audit logs, providing you with even more control and accountability.
- **On-Demand Scalability:** CoreGuard software installs and scales easily, enabling you to expand the system as your customer base grows.

- **Customer Confidence:** CoreGuard is designed to keep security management and verification in the hands of your customer, boosting customer confidence in the safety of their data, and ultimately strengthening your customer relationship.
- **Improved Resource Allocation:** Vormetric handles data security for you, freeing your resources to concentrate on acquiring new customers and servicing current ones — efforts that generate more revenue — rather than on securing customer data.

Additional Advantages for Auditing

CoreGuard is designed to facilitate audits relating to compliance in the areas of information security and privacy, an advantage that can be leveraged by companies that are outsourcing, as well as outsourcing service providers. CoreGuard is ideal for audits because the system identifies who accessed what data, where, when and how — all the details an auditor needs to know. The tool provides a critical audit trail for data accessed by outsourcing partners, which would otherwise be almost impossible to track. CoreGuard's enforcement of IT governance policies and procedures significantly reduces the amount of recurrent testing required to assure auditors of system and application integrity, and comprehensive audit logs reduce the cost and time required to assess compliance with government regulations. The system is entirely auditable to comply with Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), HIPAA, CA SB 1386, the EU Data Protection Act, Visa's PCI Data Security Standard, and other mandates regarding the handling and protection of information.

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.

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.

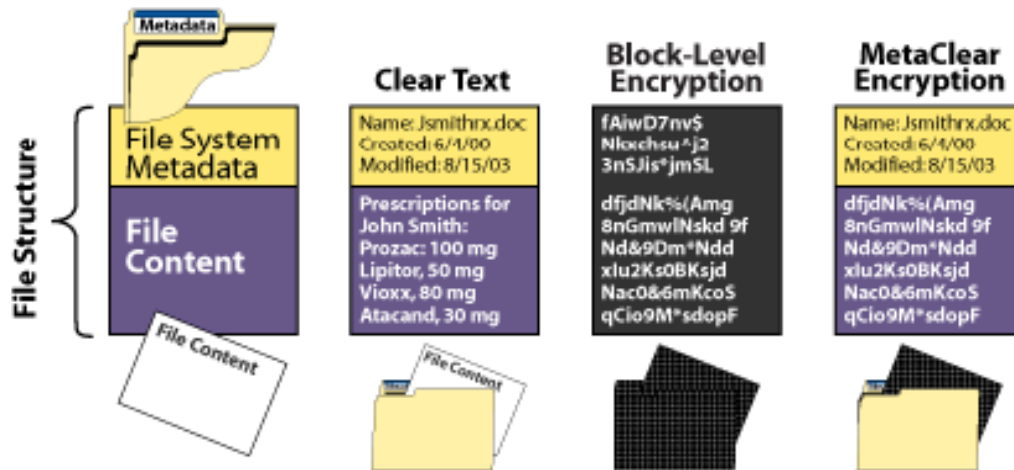
Data at Rest Encryption

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.

MetaClear Encryption



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. With 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
- 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.

The key to CoreGuard's proven and transparent data privacy protection solution lies in its innovative architectural design. The combination of the CoreGuard PEM coupled with the FIPS-validated Security Server Appliance provides tremendous benefit in the manageability, scalability and security of the solution. In addition, the insertion of the PEM at the file system-level enables granular inspection of data access attempts and a high degree of transparency for easy installation and configuration across widespread, heterogeneous networks.

CoreGuard PEM

The CoreGuard PEM, the first of two components in the CoreGuard System, is an extremely thin software module that installs at the file system level of the host operating system. PEMs are the mechanisms to apply any cryptographic key across different systems.

CoreGuard Security Server Appliance

The second component of the CoreGuard System is the CoreGuard Security Server Appliance. The SSA is a scalable, secure appliance that connects to protected hosts and PEMs via the network. A secure protocol between the SSAs and the PEMs permits the rapid and secure delivery of policy decisions to the PEMs as data access requests are made.

Security policies and cryptographic keys are stored and administered within the SSA cluster and cached locally by the PEM in volatile or non-volatile storage based customer configuration. Security policies are used to centrally apply cryptographic keys to data across a variety of systems, applications, etc. as each SSA supports a large number of heterogeneous CoreGuard PEMs. This unique architecture and advanced technologies create a solution that is significantly more effective and easier to manage than alternative solutions.

Proven Leadership with Vormetric

CoreGuard has been proven in real-world installations at many leading corporations in a variety of vertical industries that require protection for sensitive data. Vormetric's impressive customer base includes BMW, BJs Wholesale, EDS, Cadence Design Systems, Synopsys, Bank of Tokyo, Mitsubishi, Ocwen Financial Services, University of Texas Hospital, Planitax, and California Water, to name just a few. Vormetric is the technology leader in the data protection arena, holding 13 patents and FIPS validation on all products. The company is the winner of industry acclamation such as ComputerWorld's 2004 Innovative Technology Award, and serves as a respected partner of industry giants such as IBM, Symantec, HP, Sun and Oracle.

Summary of Threat Protections

Threat Description	CoreGuard Protection
Unauthorized Data Copy	<ul style="list-style-type: none"> • Encryption • Separation of Duties • Policy-based Security • Audit
Lost or stolen media (e.g. backup tape)	<ul style="list-style-type: none"> • Encryption
Unauthorized File Sharing	<ul style="list-style-type: none"> • Encryption
Privileged User Abuse	<ul style="list-style-type: none"> • Encryption • Separation of Duties • Application Authentication • Audit
Malcode Infections (e.g. rogue applications)	<ul style="list-style-type: none"> • Host Integrity • Application Authentication • Audit
Application Attacks (from hackers or insiders)	<ul style="list-style-type: none"> • Host Integrity • Application Authentication • Audit
Modified / Deleted Audit Logs	<ul style="list-style-type: none"> • Separation of Duties Audit
Data Leakage / Unauthorized Access	<ul style="list-style-type: none"> • Policy-based security

Conclusion: Protecting Data Inside and Out with CoreGuard

In this new era where companies are willing to outsource various portions of their operation in order to focus on their core business, enterprise hosting has become an exceptional business opportunity. This opportunity requires a new way of thinking about securing sensitive data and information assets. Locking up the filing cabinet is no longer an adequate strategy. On the other hand, more conventional methods of data encryption consume performance overhead and do not provide a practical option for protecting data in a hosted environment. The best option is to protect digital data with Vormetric's high-speed data encryption and policy-based user access control, allowing global management from a central location. CoreGuard from Vormetric is an economical, powerful and flexible solution that keeps your data safe while giving you the freedom to outsource tasks and share information with partners that need it. With CoreGuard, companies can outsource any tasks with worry-free protection of NPI and IP, so they can concentrate on their core competencies. Outsourcing service providers can also leverage CoreGuard to offer customers value-added protection that will heighten customer confidence and sharpen their competitive edge. All players working within the outsourcing business model can benefit from Vormetric's revolutionary technology and the versatile and reliable CoreGuard data security solution.

For more information:

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

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.