

VORMETRIC WHITE PAPER

# Protecting Enterprise Information

**Requirements for securing information  
assets and personal data against external  
attacks and internal threats**

*“The emphasis has been on the doors, rather than on what they are protecting. We must become less perimeter-centric and more asset-centric...”*

– Greg Shipley, CTO, security consulting firm Neohapsis, in the article “Secure to the Core,”  
Network Computing, January 2003



VORMETRIC

Copyright © 2004 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

In spite of substantial investments by enterprises and governments in IT security and significant technological advancements by security developers, successful attacks on hosts and digital assets continue to grow at an alarming rate. The porous nature of the perimeter is becoming increasingly evident and many attacks are launched from the inside—perimeter security alone cannot solve this problem! Buffer overflow attacks, malicious code insertion, remote application execution and information theft by insiders are but a few of the security concerns that continue to affect organizations.

To address the growing need to protect the integrity of the enterprise information environment—the host servers, applications and stored data residing inside the perimeter—Vormetric has developed the CoreGuard™ Information Protection System. CoreGuard's integrated solution is designed to secure stored information ("data at rest"), enable control over data viewability through the use of encryption, protect host and application integrity, and audit and report on all data access events. At the same time, CoreGuard's file-level approach to information protection is transparent to applications, file systems and storage infrastructures and centrally manageable for easy installation and configuration, while providing distributed, extensible policy enforcement of data security rules throughout a widespread and heterogeneous enterprise IT environment.

This paper examines the need for direct protection of the enterprise information environment and explains how the CoreGuard System represents an innovative and effective solution for securing sensitive information and protecting the hosts and applications that access that information.

## The Problem: An Increasing Rate of Malicious Activity Targeted at Sensitive Information

Enterprises and government agencies alike are experiencing an increasing rate of malicious activity from both external and internal sources directed at sensitive data, as exemplified by the following trends:

- The 'insider threat' is increasingly acknowledged as the critical vulnerability to digital assets, particularly when a large number of administrators are granted 'super user' privilege status in order to perform their job duties.
- Attacks on the IT infrastructure are less often initiated for the challenge and notoriety of the attack and increasingly as criminal activities motivated by economic gain or adversarial damage, and directed at digital assets.
- New vulnerabilities in the IT operating environment are uncovered on a continual basis, resulting in a flood of patch releases that administrators do not have the resources to test and implement in a timely manner.
- A new generation of worms installs back-door access into systems, enabling attackers to upload Trojans that capture transactions in process or allow access to stored information.

At the same time, business operations is driving increased connectivity, 'webifying' applications, opening network access to partners and customers, and outsourcing IT operations—initiatives

that reduce cost and increase productivity and market penetration, but at the cost of increased security risk.

### **Regulatory Legislation and Industry ‘Best Practices’ Standards**

Along with the skyrocketing rate of identity theft has come heightened activity on the part of legislators and regulators to safeguard non-public personal information (NPI) and other sensitive enterprise data. A number of legislative and commercial initiatives are requiring increased attention by executive officers to the privacy and confidentiality of electronic stored data. Information security requirements associated with these measures include:

#### ***California SB 1386 (Civil Code 1798)—“Notification of Risk to Personal Data Act”***

- Agencies and enterprises are required to report suspected breaches of unencrypted personal data to the data owners.
- California Office of Privacy Protection’s ‘best practices’ recommends implementing access control and host protection to prevent the circumvention of data encryption.<sup>1</sup>

#### ***Gramm-Leach-Bliley Act (GLBA)***

- Limit NPI access and viewing privileges only to those with a ‘need to know.’
- Adhere to FTC 16 CFR Part 314 standards for safeguarding customer financial data.

#### ***Health Insurance Portability and Accountability Act (HIPAA)***

- Ensure that only properly authorized individuals can view confidential patient/customer health information.<sup>2</sup>
- Provide long-term information assurance for confidential archived data.

#### ***FDA 21 CFR Part 11***

- Ensure that only authorized individuals can access pharmaceutical electronic files.
- Generate time-stamped audit trails for all accesses to electronic records.

#### ***Sarbanes-Oxley Act of 2002 (SOX)***

- The CEO and CFO must attest to the veracity of financial reports (Section 302) and to the nature and effectiveness of internal controls for information assurance.
- The CEO and CFO provide an assessment of internal controls for financial statements and records (Section 404), also attested to by independent auditors.

#### ***Basel II Capital Accord***

- Financial institution capital reserves must account for operational risk, as well as credit risk, commencing in 2006.
- IT security risk is the principal driver of operational risk.

#### ***European Union—Directive 95/46/EC***

- Implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, alteration or unauthorized disclosure.

#### ***VISA Cardholder Information Security Program (CISP)***

- Encrypt sensitive stored information (Visa account number and expiration date), restricting access by ‘need to know,’ and track all accesses to data by unique ID.

In addition to legislative penalties and lawsuits by affected individuals, firms that fail to adequately protect sensitive information can be subject to other adverse consequences. A University of

Texas Graduate School of Management study concluded that firms that suffered a public security breach experienced an average loss of 2.1% of their market values within two days surrounding the event, an average loss of \$1.65 billion in market capitalization per incident.<sup>3</sup> Taken together, the increased regulatory oversight, the threat of malicious attacks, and the potential negative consequences of security breaches—particularly those that expose private information—all point toward the need for more effective measures to protect sensitive enterprise information.

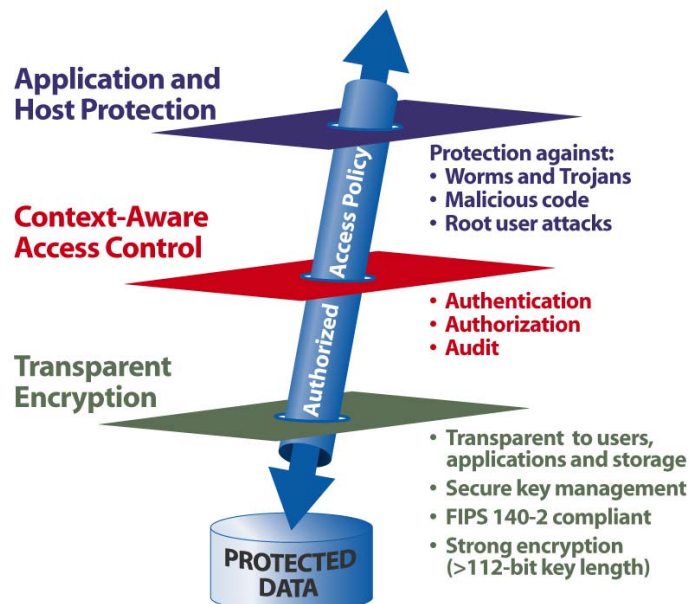
## The Solution: Enterprise Information Protection

Protecting the enterprise information environment—comprised of host servers, applications and stored data—is a task that extends beyond the capabilities of today’s perimeter and point security solutions. Vormetric developed the CoreGuard Information Protection System to provide a comprehensive, multi-layered approach to protecting against exploitable vulnerabilities and the ‘insider threat’ that can compromise sensitive information.

### FUNDAMENTALS OF INFORMATION PROTECTION

A comprehensive, effective solution that protects the entire enterprise information environment requires the use of several integrated technologies and capabilities that protect not just the data at rest, but also the integrity of the applications and host servers that can request access to the data. The solution must ensure application integrity by verifying the authenticity of all applications before they are allowed to run and must ensure host integrity by preventing tampering with the operating system, file system or configuration and .dll files. This is critical because exploiting a compromised application or host is one of the most frequently used methods for unauthorized users to access sensitive information. Attempting to secure stored data with the use of encryption alone may guard against theft of data on the storage media or attacks that bypass the authorized access channel, but leaves the data open to attack by exploitation of many other vulnerabilities. The diagram below illustrates the multiple layers of protection required for effective protection against both external and internal threats.

#### Multi-Layered Protection for Stored Information Environments:



## REQUIREMENTS FOR INFORMATION PROTECTION

Architecting an effective system for protecting information requires support for six primary design elements. These elements can be broken down into the following components:

- **Host and Application Protection**—protects vital elements of the host so it cannot be compromised and used to acquire access to sensitive data. Unauthorized processes are prevented from running, denying attackers the ability to circumvent the authorized access channel for protected data.
- **Context-Aware Access Control**—allows access to sensitive data only by those authenticated users and applications that are authorized to perform the requested operation, and only on the specifically targeted data and at the specific time the operation is being attempted, including control of system administrator access privileges.
- **Encryption of Stored Data**—protects sensitive data in encrypted form, using standard encryption algorithms, while ‘at rest’ in any network-accessible storage environment.
- **Centralized Management, Distributed Enforcement**—An extensible architecture permits centralized management of multiple information protection policies with remote enforcement across a heterogeneous IT environment, including support for all hosts, data types (e.g., database, flat files, shared folders) and storage infrastructures.
- **Transparent Operation**—integrates seamlessly into data centers, including with existing directory services and storage infrastructures, as well as into existing business operations, security policies and data classification schema.
- **Confidentiality of Data under Management**—separates the ability to access and manage data from the ability to view and process data.

The combination of these elements is essential to providing a comprehensive solution that protects against all vulnerabilities to the information environment, and controls the insider threat.

## Vormetric CoreGuard™: An Innovative Solution for Protecting Enterprise Information

It is not enough to implement a solution that protects enterprise information. Key business and operational requirements must also be met in an effective, integrated way. These factors include:

- Cost-effectiveness
- Manageability
- Performance
- Transparency
- Scalability
- Integration
- Extensibility
- Auditability
- Reporting

Recognizing these requirements, Vormetric developed the CoreGuard Information Protection System, the industry’s first comprehensive solution for enterprise-wide protection of heterogeneous hosts, applications and data at rest. Vormetric’s integrated design eliminates the need to procure and manage multiple point products to secure hosts and data, while its innovative architecture enables separation of duties between IT and security administration.

## CoreGuard Information Protection Prevents Attacks:

<b>Root Attack</b>	Enables the blocking of local root user privileges. Verifies the use of strong authentication services to validate user privileges. Capable of blocking all root access based on user-defined policies.
<b>Worms and Trojans</b>	Verifies the authenticity of application code prior to allowing execution. Prevents worms, unauthorized patches and applications, and altered code from running and propagating, including zero-day exploits.
<b>Buffer Overflow</b>	Prevents the consequences of attacks by denying privileges to unauthorized processes and users.
<b>Unintended Admin Privilege</b>	Controls access to data by root users, DBAs and admins by blocking execution of unauthorized applications and file system operations, and by blocking file system operations against unauthorized data targets.
<b>Unauthorized Data Viewing</b>	Prevents backup administrators, contractors and storage outsourcing partners from viewing data under management, or performing tasks outside authorized time windows, based on data-owner policies.
<b>Audit Log Tampering</b>	Prevents unauthorized access to critical files such as database audit logs that track accesses and modifications to data, preserving the log's evidentiary value and making IT systems more 'auditable.'
<b>Hardware/Media Theft</b>	Encryption of stored data renders theft of hardware and storage media useless for the purpose of information extraction.

The CoreGuard System consists of software Policy Enforcement Modules (PEMs) installed on the hosts that serve as access points to sensitive information, and a Security Server appliance cluster. The PEMs enable enforcement of information protection policies directly on the data access points, including selective encryption of stored data. Policies are composed and managed on the Security Server, which also stores encryption keys. The separation of policy enforcement from policy processing provides flexible mandatory access control, the security model recommended by the NSA as the 'best-practices' approach for data access control.

## Innovative Architecture

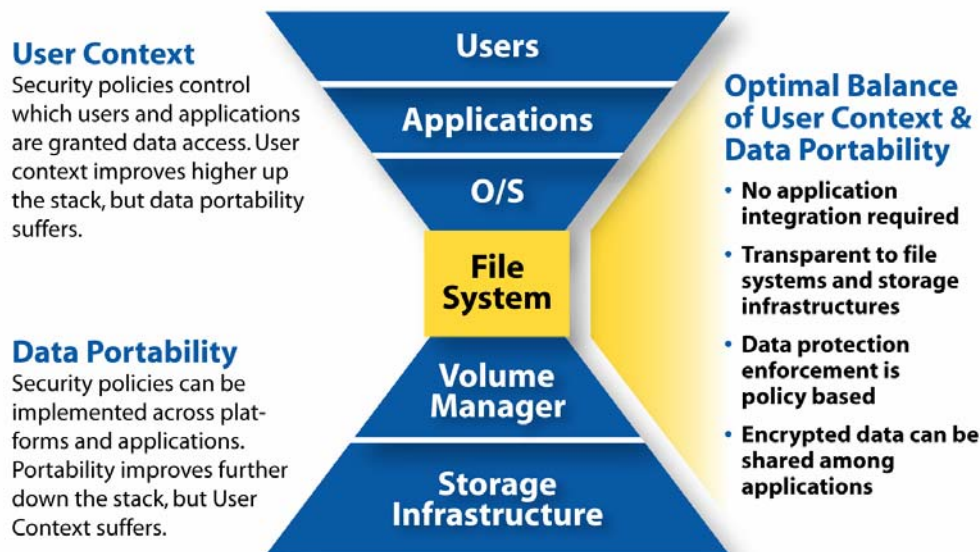
The key to CoreGuard's solution lies in its innovative architecture. The combination of the lightweight PEM and the Security Server appliance provides benefits in manageability, scalability and security. The insertion of the PEM at the file-system level enables granular inspection of all data access attempts and a high degree of transparency for easy installation and manageability.

Benefits of the CoreGuard architecture include:

- **Separation of policy enforcement from policy decision making**—The CoreGuard architecture allows the PEM to enforce information protection policies on the hosts and the Security Server to act as the policy decision maker. Storing policies and keys on the FIPS-validated Security Servers ensures they are impervious to attack, while at the same time facilitating the enterprise-wide system management through a centralized interface.
- **Visibility into complete context of data requests**—Installation of the PEM on the host OS at the file-system level allows CoreGuard to inspect the complete context of all access calls for implementation of fine-grain access control.

- **Separation of duties**—CoreGuard's architecture allows system administrator duties to be distinctly separated from security administrator duties, preventing system admins from being able to access or view data unless authorized by security administration.
- **Optimal transparency at the file system level**—CoreGuard is transparent to the applications, database management systems and file management systems that access stored data, providing CoreGuard the ability to enforce information protection policies across multiple applications with no modification required. CoreGuard is also transparent to the data storage infrastructure, working with any combination of DAS, NAS and SAN.
- **Extensibility across heterogeneous environments and applications**—Transparency to file systems, applications and storage infrastructures allows a single CoreGuard cluster to enforce information protection policies addressing diverse security needs covering multiple applications and DBMSs, and heterogeneous network and storage components.
- **Scalable and manageable**—Clusterable Security Servers operate in fail-safe, fully redundant clusters that are internally load-balanced and can support hundreds of PEMs, allowing CoreGuard's performance to scale with the number of protected servers.
- **Limited load on host CPU, negligible performance impact on applications**—CoreGuard supports a combination of local (on the host CPU) or centralized (offloaded to the Security Server appliance) encryption processing. This option permits system architects to tailor system design and performance to their specific needs.
- **Policy updates in Security Server eliminates need for host updates**—Since policies are composed and stored in the Security Server cluster, there is no need to update PEMs on individual hosts in order to implement updated information protection policies.
- **Stable location in the OS**—File system APIs are a very stable part of the OS that are not typically subject to change by patches and updates. Therefore, it is very unlikely that PEMs will need to be modified as updates are made to the host OS.

### File System Level Enforcement:



## CoreGuard PEM

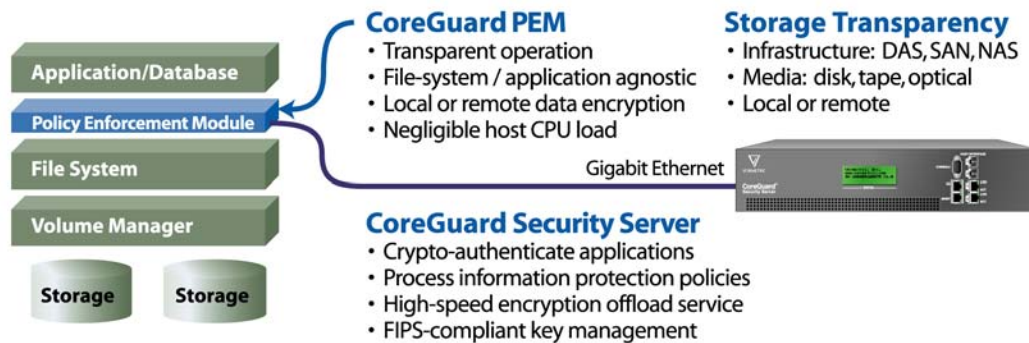
The CoreGuard PEM is an extremely thin software module that installs at the file-system level of the host operating system, but is non-intrusive to operating system functions. Actual encryption of file data can be performed either internal to the host by the PEM or in the Security Server using its high-speed encryption subsystem. CoreGuard PEMs are available for popular operating systems and are transparent to applications, file systems and the storage infrastructure.

## CoreGuard Security Server

The Security Server is a scalable, secure appliance that connects to protected hosts and PEMs via a standard gigabit Ethernet LAN connection. A secure protocol between the Security Servers and the PEMs permits the rapid and secure delivery of policy decisions and encryption keys to the PEMs as data access requests are made. Full encryption and authentication of all control messages ensures that there is no possibility of a replay or 'man in the middle' attack between PEMs and Security Servers.

Security policies are stored within the Security Server, thereby eliminating the need to update the host PEMs in order to make policy changes. To ensure that the system is impervious to attack, the Security Server is FIPS140-2 validated. The highly scalable architecture includes a dedicated high-availability link for each Security Server along with integrated load balancing, enabling operation in a 'fail-safe' cluster. Each Security Server can support up to hundreds of heterogeneous CoreGuard PEMs.

## The CoreGuard System:

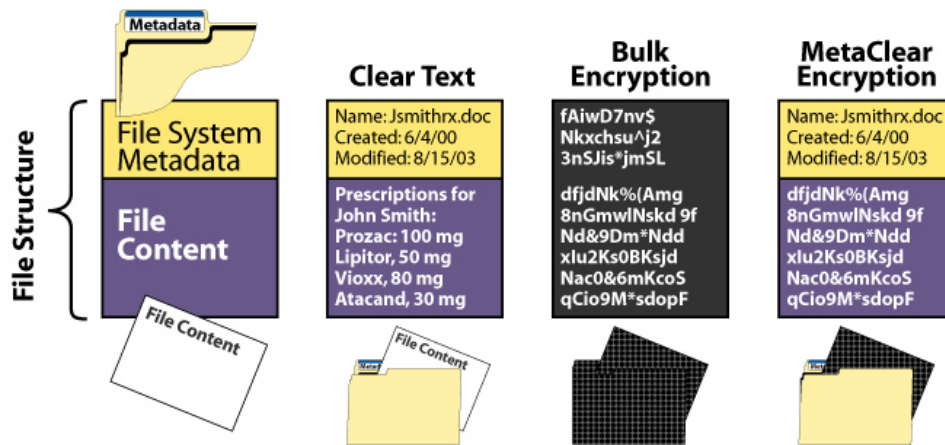


## MetaClear™ Encryption

Using a secure, self-contained key management system and truly random key generation, CoreGuard information protection policies can be defined to strongly encrypt data on a selective, file-by-file basis. The file system intelligence of the CoreGuard encryption engine also enables the encryption of file (or 'payload') data separate from the file system metadata, which is kept in the clear. This technology is known as MetaClear encryption and allows the separation of storage management duties that require access to file data from the right to view such data. MetaClear encryption operates on a page-by-page basis so it can be applied to live database files. CoreGuard supports the industry-standard AES encryption algorithm using either 128-bit or 256-bit key lengths.

While the encryption of stored data is becoming increasingly desirable, and in many cases a regulatory or best-practice requirement, encryption can inhibit the ability to manage data if not applied intelligently. The backup, snapshot and replication applications employed by enterprises to ensure data availability and preservation often require that the file system metadata, the data about the data, be readable in order to perform data management. For example, incremental backup operations require the backup application to inspect the file system metadata of each file to determine whether it has been changed since the last backup. If encryption is applied to the entire file, as do block-level storage encryptors that ignore the file system structure, both the file system metadata and the file content need to be decrypted for the backup application to read the metadata, exposing any sensitive information in the file content to unauthorized viewing at the backup server. Furthermore, this approach incurs the cost of re-encryption of the file after file system metadata inspection as the data is copied to tape. Since it is possible for the decrypted data in the backup server to be replicated to other storage devices, the vulnerability of this exposure to backup administrators, contractors or service providers can carry a significant risk.

**MetaClear Encryption:**



By operating at the file system-level, MetaClear is able to filter out the file system metadata before encrypting the file content. By leaving the file system metadata in the clear, data management applications can perform their functions without the need to expose file content in the clear and without the need for re-encryption.

**Context-Aware Access Control**

One of the key elements of the CoreGuard System is the ability to perform context-aware data access control. The insertion of the CoreGuard PEM at a stable and strategic place in the data access tier enables both visibility into the context for data access requests and enforcement capabilities for fine-grain information protection policies.

### Context-Aware Access Control Policy Criteria:

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

### Host & Application Protection

CoreGuard protects the hosts and applications in order to prevent them from being used as platforms to attack information. CoreGuard does this in two steps: First, by identifying the specific executable files and related resource libraries that are authorized to run on protected hosts, CoreGuard creates a reference database for those files' cryptographic fingerprints. This database ensures that files can be authenticated, enabling security administrators to effectively lock down the host to a 'gold image' and precisely define what processes are allowed to run on any protected system. Second, CoreGuard prevents any process that cannot be authenticated against the reference database from running on the host. This same technology also protects the host OS, config files, DLLs, etc.

CoreGuard's advanced host and application protection capabilities have multiple applications:

- **Application Verification**—ensures that only authorized applications whose cryptographic fingerprints can be authenticated by the CoreGuard System are allowed to run on protected servers, preventing any malware or tampered or malicious code.
- **Change Management**—prevents the installation of unauthorized applications, revisions or patches on protected hosts, enforcing change management policy.
- **Gold Image Verification and Enforcement**—locks down the configuration of a protected server to only those executable files and resources required to support the application or database. Prevents running any additional processes or altered applications that have been tampered.

- **Integrity Protection**—prevents unauthorized or non-authenticated processes from launching, preventing compromise of hosts by all types of malicious code, including zero-day worms and Trojans.
- **Auditability Enhancement**—provides easy verification of the enforcement of internal controls and security processes to auditors, demonstrating compliance with legislative, regulatory and industry standards for information protection and system integrity.

## Summary

Perimeter security can no longer be considered adequate protection for sensitive information due to (i) the increasing porosity of the perimeter required to compete in today's 'real-time' business environment, and (ii) the increasing threat from the growing diversity of 'insiders,' who may also include third-party contractors, vendors, partners and customers. Effectively protecting sensitive data and digital assets requires security enforced from the inside out. Vormetric's CoreGuard Information Protection System provides a comprehensive solution that protects against:

- the consequences of exploitable host vulnerabilities;
- unauthorized applications and processes;
- super users operating outside of their intended mode and purpose; and
- direct attacks on stored data.

By integrating transparent encryption for data at rest and context-aware access control with host and application integrity protection, CoreGuard enables security organizations to confidently protect sensitive information wherever it resides in the enterprise.

\* \* \*

For more detailed information on the CoreGuard System, please refer to the following Vormetric documents:

Vormetric White Paper: "[Data Privacy Legislation, Regulations and Standards](#)"

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

Vormetric Solution Brief: "[California SB 1386 \(AB 700\): Ramifications on Personal Information Privacy Enforcement](#)"

Vormetric Solution Brief: "[Sarbanes-Oxley: Enforcing Control Objectives for Enterprise Information](#)"

Vormetric Technical Brief: "[Defending OS Vulnerabilities in an Oracle Environment](#)"

Vormetric Technical Brief: "[Protecting against Malware](#)"

Vormetric Business Brief: "[Regulatory Governance and Information Security](#)"

[CoreGuard Information Protection System Datasheet](#)

[CoreGuard FAQ](#)

---

<sup>1</sup> California Office of Privacy Protection, "Recommended Practices on Notification of Security Breaches Involving Personal Information," Oct. 10, 2003, < <http://www.privacy.ca.gov/recommendations/secbreach.pdf>>, (11/4/03).

<sup>2</sup> Federal Trade Commission, "Standards for Safeguarding Customer Information," May 23, 2002, <<http://www.ftc.gov/os/2001/07/66fr41162.pdf>>, 2/4/04).

<sup>3</sup> "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan, University of Texas at Dallas School of Management, February 2002.

**Vormetric, Inc.**  
888.267.3732  
[www.vormetric.com](http://www.vormetric.com)  
[sales@vormetric.com](mailto:sales@vormetric.com)

