

VORMETRIC BUSINESS BRIEF

# **Regulatory Governance and Information Security**

**A technical response to the Bloor Research paper “New regulations are putting CEOs behind bars: what new international regulations mean for your business”**



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.

## Introduction

As discussed in the Bloor Research paper “New regulations are putting CEOs behind bars: what new international regulations mean for your business,” there are several new and forthcoming rules and regulations bringing pressure on organisations to ensure that measurable and demonstrable processes and procedures are in place for securing sensitive information. The challenge is to put into place good business practices and controls which do not hinder business operations but still control the flow of information.

As with most required business controls, a balance between process and technology is needed, as no single measure will satisfy all criteria. In a complex environment constantly shifting between compliance and business risk, the need to have a flexible, adaptable solution is paramount; otherwise, organisations will be confronted by a rigid and expensive operation that can quickly become outdated.

Consequently, organisations are well advised to think beyond the ‘current’ compliance issue and adopt a flexible approach to business controls and audit. This should address known areas of concern as well as other requirements which will become necessary in the future. While measures chosen based on their expediency may be the quickest route to short-term compliance, a solution that is successful over the long term will allow for adaptability in addressing all anticipated control requirements, providing a much more attractive return on investment.

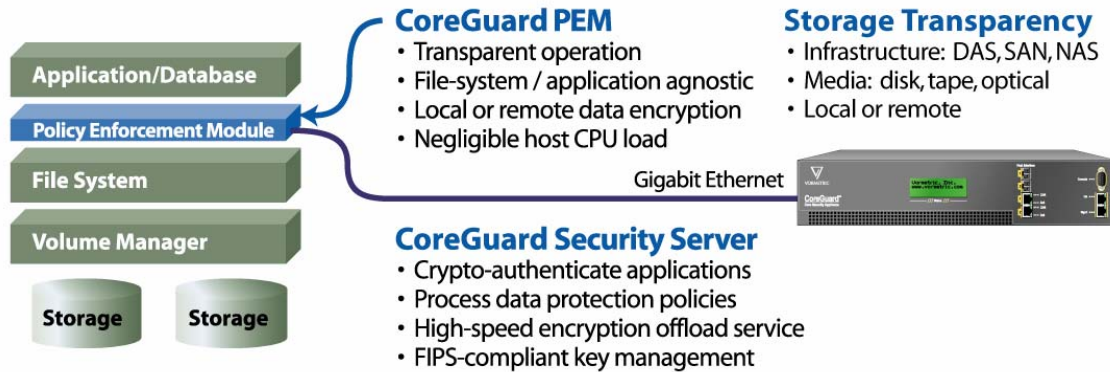
## About CoreGuard

Vormetric's CoreGuard Data Security System is the industry's first comprehensive information protection solution that ensures system and data integrity by directly protecting the host servers and stored data at the core of the enterprise IT environment. The CoreGuard System integrates selective encryption of stored data, context-aware data access controls, host and application protection, and fine-grain audit, alert and reporting. By utilising some or all of these features, organisations can put in place technical controls to meet the challenges of regulatory compliance as outlined by Bloor Research.

Before directly addressing some of the issues raised in the Bloor paper and offering Vormetric's solution, it is important to first understand the architecture of the CoreGuard System.

## COREGUARD SOLUTION OVERVIEW

The CoreGuard Data Security System consists of thin software clients, the Policy Enforcement Modules (PEMs), which are loaded onto hosts that serve as protected access points for enterprise information, and a Security Server appliance cluster that communicates with the PEMs via a network connection. The CoreGuard architecture enables local enforcement of data security policies via the PEM, with centralised policy management on the Security Server appliances that defines who or what has authorised access to protected data. This architecture provides for a scalable and extensible security system that can be deployed locally or across an extended enterprise environment.



This innovative architecture combining the lightweight PEM modules with the powerful Security Server appliance cluster provides local enforcement of enterprise security policies across an extended network, along with a highly manageable, extensible, and scalable information protection solution. But above all else it is flexible and can change to meet the challenges presented by compliance or regulatory issues today as well as tomorrow.

## Issues raised in the Bloor paper

### ISSUE: PROTECTING SENSITIVE DATA

In the early stages of any data classification process, while it may be obvious that some information is highly sensitive, the true sensitivity of other data may not be apparent until a data review process has been put in place. Therefore any data security technology adopted must enable data to be moved, added to or reclassified without major changes to the infrastructure or processes around it.

#### CoreGuard response

The CoreGuard System uses an innovative architecture that provides both flexibility and extensibility while remaining non-disruptive to business operations. This architecture—separation of ‘policy enforcement’ from ‘policy processing’—permits centralised management of security policies with distributed enforcement across an extended enterprise for consistent application of enterprise information protection policies. This permits easy implementation of new or updated data security policies by the security organisation—even at remote locations—based on data classification requirements that may change over time due to a re-evaluated risk assessment, a dynamic threat environment, or a reappraisal of data sensitivity.

Moreover, CoreGuard’s file-level operation enables transparency to the operating environment, including host servers, applications, databases, file systems, and storage infrastructures. This high level of transparency allows for reclassified or moved data to be easily secured simply by loading PEMs onto the hosts functioning as access points to the data and configuring new data security policies on the Security Server appliance, without making any changes to the IT infrastructure elements listed above.

Finally, the ability to apply CoreGuard security policies to all data types, such as databases, flat files, media files, shared folders and directories, ensures that new and appended files are still secured based on policy definitions.

## **ISSUE: CONTROLLING ACCESS TO SENSITIVE DATA**

It is well understood that the need to control who can access sensitive data is key to any solution for protecting data. However the issues of allowing functional access to data by processes such as back-ups, system access by database administrators or applications is not so clear. If one considers database administration for example, it is obvious that the 'manager' of the database structure needs access to the data files but do they need the ability to read the content? The answer is no. Likewise should this person have the ability to modify the audit trail of the database? Definitely not! But without adequate controls these problems will remain.

### **CoreGuard response**

CoreGuard enables the enforcement of 'separation-of-duties' policies with respect to the viewing of protected data by system administrators, resolving the conflict between the need to secure data at rest and the need to manage that data. By operating at the file system-level, CoreGuard's MetaClear encryption filters out the file system metadata before encrypting the file content. By leaving the metadata in the clear, system administrators can run data management applications without the need to first decrypt data content, preventing system administrators from being able to view sensitive data unless authorised by the security organisation.

CoreGuard can also be configured to control unauthorised access to critical files such as database audit trails that track accesses and modifications to data. By blocking all access to those audit logs except by authorised users, security organisations are now able to preserve the log's evidentiary value, enforcing two-person controls relevant to data access and making IT systems more 'auditable.'

## **ISSUE: AUDITABILITY FOR SYSTEM AND DATA INTEGRITY**

As systems and processes are deployed there will come a point where their integrity will be challenged. At this stage the organisation will need to demonstrate their processes as well as show documentary evidence of the validity of the data held and accessed, either as proof of ongoing accountability of an audit process or factual evidence of the original content of a file.

### **CoreGuard response**

CoreGuard's comprehensive solution includes protection for hosts and applications that enhances system auditability by enforcing a 'gold image' of protected host servers and enforcing enterprise policies relative to change management. By verifying the cryptographic fingerprints of the authorised applications and resource files running on the hosts, CoreGuard prevents the introduction of unauthorised applications, revision updates and patches by internal or external parties, including 'back door' worms and other types of malware. This same technology can be used to protect other system components such as the host OS, configuration files and application links from being altered in any way.

Furthermore, the CoreGuard policy definition format provides a means of easily confirming the accuracy of internal controls that enforce enterprise security policies for data access and viewing. The *who/what/where/when/how* data security policy parameters implemented by CoreGuard correspond to those typically used to define an organisation's acceptable use policies, allowing for easy verification of controls that dramatically reduces the effort and cost of external auditors.

By ensuring the integrity of the applications and stored data and thereby enhancing the overall system auditability, CoreGuard alleviates the requirement for extensive risk evaluation, the implementation of compensating processes and documentation, and the need for regular system audits to demonstrate system integrity and the effectiveness of security policy enforcement.

### **ISSUE: PROTECTING THE SERVER OPERATING INFRASTRUCTURE**

As part of any risk assessment the question of theft of data by stealing the server or hard drive it resides on is answered by physical measures such as locks and keys. However today there is a greater threat through the compromising of the server in such a way that it gives out the data to the requestor. These forms of attack are rogue applications, which can 'steal' selective information on demand or malicious code that sets out to destroy data. The challenge is not only to protect against known attacks, but to also protect against the unknown. This is important as one should not forget there is always a delay between an Anti Virus or Operating System patch being released to address a new virus and then being loaded on your operational system, during which time your systems and data are vulnerable.

#### **CoreGuard response**

Ensuring system integrity and the appropriate use of enterprise data requires that vulnerable data access points are protected from any unauthorised changes, including the introduction of malicious code. By protecting the integrity of host servers and the applications running on them, CoreGuard prevents system access points from being used as platforms to attack stored data.

Identifying the specific executable files and related resource libraries that are authorised to run on protected hosts allows CoreGuard to create a reference database for those files' cryptographic fingerprints. Any process that cannot be authenticated against this reference database, including zero-day worms, Trojans, unauthorised applications and patches, or altered code, is prevented from running on the protected host. Moreover, the deterministic nature of the CoreGuard data security policies does not rely on signatures or patches to block unauthorised applications from running, so there is no window of vulnerability following the introduction of a new threat. By controlling the processes that can run on protected hosts in combination with the users permitted to access and manage the systems, the organisation can prevent all forms of malware, known and unknown, from accessing, tampering or deleting protected files.

## **Conclusions**

Vormetric's CoreGuard System directly addresses many of the technical control requirements faced by organisations in today's regulatory environment. Its innovative architecture satisfies current requirements for internal controls over the appropriate use of sensitive information and system integrity, while providing the flexibility to address new challenges introduced by business requirements or government regulatory agencies without the need to modify applications or to update the existing IT infrastructure. Its transparency of operation means that data users will not be hampered in conducting their normal business unless they try to access protected data, run an application for which they are not authorised, or launch an unauthorised application. Above all, CoreGuard is extensible and scalable, permitting it to grow with the organisation's needs to protect its valuable data assets.

\* \* \*

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

Vormetric White Paper – [“Securing Enterprise Data”](#)

Vormetric Solution Brief – [“Sarbanes-Oxley: Enforcing Control Objectives for Enterprise Data Environments”](#)

Vormetric White Paper – [“Data Privacy Legislation, Regulations and Standards”](#)

Vormetric Business Brief – [“Reducing Operational and Information Risk”](#)

[CoreGuard Data Security System Datasheet](#)

[CoreGuard FAQ](#)

**Vormetric, Inc.**

Tel: 888.267.3732 (N. America)

+44 (0)870.321 4010 (U.K.)

[www.vormetric.com](http://www.vormetric.com)

[sales@vormetric.com](mailto:sales@vormetric.com)

