

VORMETRIC White Paper

Enabling Compliance with the PCI Data Security Standards

Employing Vormetric's CoreGuard to Meet
Encryption and Access Control Requirements
for the Payment Card Industry Data Security
Standards (PCI DSS)



VORMETRIC

Introduction

In 2004, Visa USA, MasterCard International, American Express and Discover, aligned their individual data protection programs to create the Payment Card Industry Data Security Standard (PCI DSS or PCI). This alignment in standards provided an industry-wide framework that complemented each brands' individual security policies— MasterCard's Site Data Protection program (SDP), Visa USA's Cardholder Information Security Program (CISP), American Express' Data Security Operating Policy (DSOP), and Discover's Information Security and Compliance (DISC).

In September 2006 the card brands aligned again to create the Payment Card Industry Security Standards Council (PCI-SSC). The purpose of the Council, as stated on their website, "is to enhance payment account data security by fostering broad adoption of the PCI Security Standards." The Council will have responsibility for the development and maintenance of the standard. The move will also provide the industry with one definitive voice on the compliance issues that are facing the companies obligated to comply. In conjunction with the debut of the PCI-SSC, a new version of the PCI Standard was released. This new iteration, called version 1.1, provides a greater level of granularity on a number of requirements, specifically Requirement 3, which calls for the protection of stored cardholder data.

Compliance with the PCI has become an increasingly prominent concern for companies that process, store or transmit credit card data. While many companies have undertaken arduous and expensive compliance projects, adoption of key technologies that enable compliance has been slow. Encryption, in particular, has been adopted at very slow rates, despite the PCI requirements surrounding the protection of stored data.

Many companies, during the course of their compliance projects, look to point solutions to address many of the requirements. This frequently results in the utilization of resources beyond the initial scope of the project in order to make the various solutions compatible. Encryption provides just such an example. While encryption is an industry best practice, it is only one small portion of the PCI requirements. Many encryption solutions enable compliance only with those requirements that directly pertain to encryption. In selecting a point solution to solve the encryption problem, the company leaves access controls, auditing and logging, and system configurations unaddressed and adds untold complexity to the compliance project.

Vormetric's CoreGuard system is an essential tool for any company that must comply with the PCI. CoreGuard is a cost-effective and easy to manage solution for high-speed data encryption, auditing and logging, application and host integrity, and policy-based user access control. CoreGuard can even protect sensitive data that does not reside in the database environment. It is also easy to install, non-disruptive and transparent to existing applications, business operations and the IT infrastructure.

CoreGuard and the PCI DSS v 1.1

The Payment Card Industry Data Security Standard is a multi-faceted approach to the protection of cardholder data. The Requirements provide a list of mandates designed to increase the overall level of security in the Payment Services Industry. The objective of these requirements is to prompt companies to enact measures that protect cardholder information. While all of the requirements are strict, there are four major categories of requirements that often cause turmoil in the compliance project. They are: Auditing and Logging, Standard Configurations (Application and Host Integrity), Access Controls, and Encryption.

1. Auditing and Logging

There are a number of auditing and logging requirements within the PCI standard. These stringent requirements include:

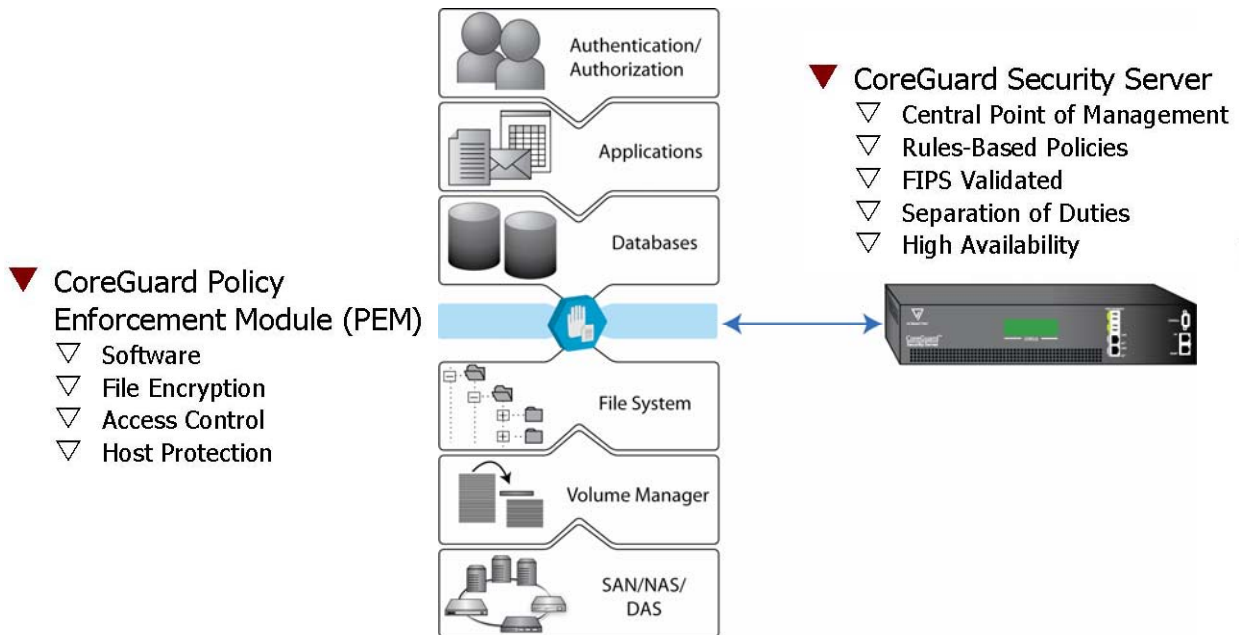
10.2 Implement automated audit trails to reconstruct the following events, for all system components:

- 10.2.1 All individual user accesses to cardholder data**
- 10.2.2 All actions taken by any individual with root or administrative privileges**
- 10.2.3 Access to all audit trails**
- 10.2.4 Invalid logical access attempts**

- 10.2.5 Use of identification and authentication mechanisms
- 10.2.6 Initialization of the audit logs
- 10.2.7 Creation and deletion of system-level objects.
- 10.3 Record at least the following audit trail entries for each
 - 10.3.1 User identification
 - 10.3.2 Type of event
 - 10.3.3 Date and time
 - 10.3.4 Success or failure indication
 - 10.3.5 Origination of event
 - 10.3.6 Identity or name of affected data, system component, or resource.

CoreGuard provides complete auditing capabilities by logging any attempted access to any data by any user. The system not only audits authorized access requests, but also all attempts to circumvent authorized access channels, notifying you of policy violations in real time. CoreGuard records all context attributes of the request – who, what, where, when and how – enabling complete tracking of host intrusion and data access on the application and user level, and providing an extensive access log for detailed analysis. For example, the CoreGuard log would include when the access occurred, who made the request, the application used to make the request, the host where the request occurred, and the file system operation requested.

The Vormetric CoreGuard System



An additional requirement, Requirement 10.5, mandates the protection of the audit trail.

- 10.5 Secure audit trails so they cannot be altered, including the following:
 - 10.5.1 Limit viewing of audit trails to those with a job-related need
 - 10.5.2 Protect audit trail files from unauthorized modifications
 - 10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter

CoreGuard limits access to audit trails only to authorized individuals on a need-to-know basis to control root or administrator access to cardholder data in the same way the system restricts access to the data itself. CoreGuard audit logs are protected from any type of unauthorized modifications, and they can also be integrated with a syslog server and SNMP applications.

CoreGuard's rich auditing capability allows you to review the file IO activity of tests performed on your security systems. Because CoreGuard logs *failed attempts*, you can track and analyze simulated security breach attempts to verify that your data is safe.

2. Data Access Controls

The use of data access controls allows companies to restrict access to sensitive information to only those that need the information in order to perform their job duties. This is an essential protection against internal compromises, as well as against threats originating from outside of the network. The PCI has set forth a number of strict access control requirements. Specifically, Requirement 7 states that companies “restrict access to cardholder data by business need-to-know.” Further requirements surrounding access controls include:

7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

CoreGuard adds a layer of access control on top of your file system’s access control. CoreGuard access control follows a least-privilege model, which means that any activity not expressly authorized will be denied, in accordance with *Requirement 7.2*. CoreGuard context-aware access control protects data by granting access only to authorized users performing authorized operations using the intended application during specified time windows. Using a five-factor system – based on who, what, where, when and how – CoreGuard requires the context of each access attempt to be validated by your own policies. Any attempt at data access that is not authorized according to these well-defined pre-set parameters will be blocked by CoreGuard.

CoreGuard’s “separation of duties” feature further restricts access to data by allowing system administrators and root users to maintain the system and backup data, without being able to view the cardholder data. In the absence of CoreGuard, you would be forced to open full data access to these additional users so they could complete their routine IT administration tasks, and simply trust these sysadmin and root users not to read the data. Even though your IT personnel may be highly trained and trusted professionals, relying on the honor system does not meet the PCI requirements. On the other hand, CoreGuard enables you to comply with the PCI’s data access restriction requirement, and truly restrict access on a need-to-know basis.

In cases when a root or system password is compromised, CoreGuard prevents system administrators or other unauthorized users from decrypting the file and viewing cardholder information. This feature is provided by CoreGuard to enable system administrators to handle and backup sensitive files without being able to view that data. With regard to this particular rule, the feature protects cardholder data in case a default password is not changed, by mistake, leaving the system open to an unauthorized user who has access to the vendor’s default system password. With CoreGuard, even in this worst case scenario, the unauthorized user would still not be able to read the cardholder data.

CoreGuard’s access control features further supports compliance by integrating with your company’s existing ID management system and leveraging those capabilities to determine whether access is authorized based on the unique ID and your security policies.

3. System Configurations

The requirements mandating standardized system configurations are often the most arduous with which to comply. Traditionally, these requirements have been met either by following the NIST guide on server hardening or by purchasing an expensive point solution. Requirement 2.2 directly addresses the system configuration issue:

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example by SysAdmin Audit Network Security (SANS) National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

2.2.1 Implement only one primary function per server (for example., web servers, database servers, and DNS should be implemented on separate servers)

2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices’ specified function).

2.2.3 Configure system security parameters to prevent misuse

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g., unnecessary web servers).

CoreGuard enables implementation and maintenance of secure systems and applications through host protection, by enforcing a “gold image” of protected host servers, defined by you. CoreGuard also provides digital signing of an application to verify it is authentic and has not been altered in any way. Any application that is not recognized or has been modified, would not be allowed to read sensitive data. Verifying that applications and resource files are trusted and authorized, CoreGuard prevents the execution of malicious code or unauthorized applications introduced internally to access protected data, and also prohibits unintended system modifications that could compromise data.

CoreGuard's host protection feature also provides a layer of protection that complements your anti-virus application, preventing any unauthorized code – even an unknown virus – from running on your system. CoreGuard host protection prohibits improper access of cardholder data via compromised hosts by blocking all unauthorized processes – including zero-day worms, Trojans and unapproved patches – from accessing, tampering with or deleting protected files.

4. Encryption

The objective of the PCI is to protect cardholder data. It should come as no surprise, then, that the PCI requires companies to use encryption to protect that data. CoreGuard adheres to the PCI requirements and encrypts data using standard AES 128 bit or 256 bit key lengths. CoreGuard is the easiest way to encrypt cardholder data wherever it may reside: databases, audit and debug logs, flat files, reports, email repositories and backup archives. Encryption can be tied to a user and an application. CoreGuard inserts above the file system layer so it is transparent to users. No modification to the application or database is required. It adds very little performance overhead and is much faster than column level encryption architectures. The PCI states, “*Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.*” The requirement that directly relates to encryption is:

Requirement 3: Protect Stored Data

3.4 Render PAN (Primary Account Number) at a minimum unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- ~ Strong one way hash functions (hashed indexes)
- ~ Truncation
- ~ Index tokens and PADs, (PADs must be securely stored)
- ~ Strong cryptography, with associated key management processes and procedures.

CoreGuard protects stored data by encrypting all cardholder data. CoreGuard ensures only authorized applications and users are able to read the data. This is achieved through policy-based encryption, which means policies set by your security administrators control who can decrypt the data. Encrypting data is important, but it is even more important to control the decryption of data. The advantage of CoreGuard is the combination of access control with encryption, ensuring that only an authorized user running an intended unmodified application can decrypt cardholder data and other sensitive information.

While encrypting data provides the best form of protection, it must be accompanied by secure key management procedures. Requirements 3.5 and 3.6 discuss the manner in which the cryptographic keys are to be managed.

3.5 Protect encryption keys against both disclosure and misuse.

3.5.1 Restrict access to keys to the fewest number of custodians necessary

3.5.2 Store keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key management processes and procedures, including:

3.6.1 Generation of strong keys

3.6.2 Secure key distribution

3.6.3 Secure key storage

3.6.4 Periodic changing of keys

- **As deemed necessary and recommended by the associated application (for example, rekeying); preferably automatically**
- **At least annually**

3.6.5 Destruction of old keys

3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).

3.6.7 Prevention of unauthorized substitution of keys

3.6.8 Replacement of known or suspected compromised keys

3.6.9 Revocation of old or invalid keys (mainly for RSA keys)

CoreGuard provides further protection of stored data by managing secure distribution and storage of decryption keys. The CoreGuard product includes a hardware appliance for key storage and management, and access to this appliance is limited to your authorized security administrators. The keys are maintained on a FIPS -140 certified Security Server. Without the key, unauthorized users are powerless to access cardholder data.

The PCI-SSC has rendered their opinion on CoreGuard's key management processes and their impact on PCI compliance. According to the PCI-SSC, *"the controls outlined...appear consistent with the intent and objectives of the PCI and sufficiently robust to support compliance in cases where companies are unable to meet exact compliance with PCI 3.6.4 and/or 3.6.6."* (For more information or to get the whole opinion for PCI-SSC please speak to a Vormetric sales representative.)

Additional Areas Where CoreGuard Meets the PCI Requirements

6.5.10 – Insecure Configuration Management

Typically, the first target of an intruder is not sensitive data files but the configuration files of the applications that manage the data. The configuration files may contain valuable information to locate the sensitive data, and if the configuration files can be modified, there are many more potential attacks possible. CoreGuard provides an additional layer of access control on configuration files that could prevent even privileged users (root, system administrators) from reading or writing these files. CoreGuard can also encrypt the configuration files and ensure that only the authorized application can open and process them.

8.4 Encrypt all passwords during transmission and storage on all system components.

Applications often need to read a password from a file in order to initiate. For example, when an application server first starts, it may need to log into a database. It is common for the application server to retrieve the database logon from a configuration file or have it hard coded in a startup-script. CoreGuard can easily protect these files by encrypting the script of the configuration file that contains the password, and ensure that only the authenticated application running under the designated OS user can open and decrypt the file containing the password.

11.5 ...alert personnel to unauthorized modification of critical system or content files...

CoreGuard's auditing capability can alert administrators if a critical file is changed (or prevent them from being altered at all – even by system administrators). Critical files can be further protected with encryption to make them unreadable even if the physical media storage is stolen.

Evaluating Other Data Encryption Options

CoreGuard's file level encryption is the broadest encryption solution available, able to address several of the PCI requirements. The PCI standards do not state specifically what type of encryption is required. The rules state only that data must be protected no matter where it is located. Traditional encryption solutions featuring column-level encryption cannot fully meet this requirement, as a great deal of sensitive information often resides outside the database environment. The implementation of a traditional encryption solution leaves a large amount of data unprotected. A brief case study describing the evaluation of Vormetric against other encryption solutions provides an illustration of the effectiveness of CoreGuard in meeting both PCI requirements and business objectives.

As part of an extensive evaluation of data protection solutions, a large Texas-based technology services/IT outsourcing company invited several encryption vendors to deploy their solutions on site and show first hand how they can meet the company's PCI compliance needs. Vormetric was the only vendor that actually had a solution up and protecting data before the end of the two-day evaluation period. In addition, CoreGuard was the only solution that could meet the PCI requirements to encrypt data in storage on internal hard drives and while being transported. The company selected CoreGuard based on this impressive performance, as well as several advantages outlined below.

The following are other options the Texas-based technology services/IT outsourcing company considered before selecting CoreGuard file level encryption:

Column Level Encryption

Column level encryption was not an adequate alternative because the limited performance would not meet the expectations for e-commerce transactions. Additionally, column level encryption would not be able to prevent data theft via host intrusion. Column level encryption would also add an administrative burden because the encryption solution would have to integrate with all applications, and any revisions would require manual updating of all the applications involved.

Storage Level Encryption

Storage level encryption was not an adequate alternative either because it only encrypts data while in storage, but not while it is being transported, making data vulnerable when transmitted across the network. CoreGuard, on the other hand, protects data while in transit within a LAN, as well as when the data is at rest.

In addition, storage level encryption solutions are typically hardware solutions, which are not practical for this company because they needed to distribute the application to multiple locations. The company chose CoreGuard because it is a software solution which facilitates easy remote distribution and implementation.

Disk Level Encryption

Many companies evaluate disk level encryption options in order to meet the objective of Requirement 3.4. Yet, this option may pose a barrier to compliance. PCI v. 1.1 contains specific provisions that must be met when using disk encryption. Requirement 3.4.1 specifically addresses the additional measures that must be taken in order to implement disk-level encryption in a compliant manner. Because of these additional requirements, disk level encryption was also not an adequate choice.

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts) Decryption keys must not be tied to user accounts.

Alternatives to Standard Encryption

In-House Custom Solution

Another option that the company chose not to pursue was the development of a custom in-house encryption solution. This option was not considered due to its resource intensive nature, both in money and manpower.

Compensating Controls

In the past, many companies have chosen to defer encryption in favor of deploying compensating controls. According to the PCI-SSC, a company is deemed to be using compensating controls when it cannot meet "the specific technical specification for a requirement, but has sufficiently mitigated the associated risk". For some, this is a viable alternative depending upon the business or technological constraints they may be facing. In previous years, compensating controls were very loosely defined and no specific mention was made of them in the PCI, or its predecessors. Version 1.1 of the PCI, however, offers very specific requirements for the use of compensating controls. In many respects, these requirements make the use of compensating controls more difficult. In addition, compensating controls will not aid companies in complying with the more than 30 state laws surrounding data breach notifications.

Due to the difficulties of using manual protection methods and the higher associated risks, the company chose to leverage CoreGuard, a proven tool that could meet all their needs at a much lower investment in cost and resources.

Gaining Additional Advantages with CoreGuard

In addition to the fact that CoreGuard was able to address more of the PCI requirements than any other single product, the company also gained the following advantages from Vormetric:

Affordability: CoreGuard is an economical option, costing much less than the other available options. The low cost of CoreGuard is due in part to the fact that four essential capabilities – encryption, access control, host protection and auditing – are delivered within one tool. The company estimated that to implement a selection of alternative applications to handle all the tasks performed by CoreGuard would have cost the company at least 4 times more.

Fast Implementation: The company faced a tight 4-month deadline to implement the solution to meet PCI requirements, so rapid deployment was a key issue for them. They needed a tool that could quickly fit into their environment without requiring a battery of tests. After evaluation of the alternatives, it was clear that only CoreGuard could provide the fast and non-disruptive implementation they needed. After selecting CoreGuard, the product was up and running in 30 days.

Performance: CoreGuard's data encryption process showed the highest performance of any encryption product evaluated. A major problem they found with other encryption solutions, especially column level encryption, is that they consume significant overhead. Low performance is a traditional hindrance to encryption, usually making it an impractical method for securing data that is used in ecommerce transactions. CoreGuard's minimal drag on performance makes the product ideal for protection of cardholder data.

Transparency: CoreGuard's policy-based management and high degree of transparency to the existing applications, business operations and IT infrastructure allow easy and economical deployment, management and scalability across a heterogeneous IT environment. In contrast to alternative data encryption solutions, CoreGuard operates seamlessly across all network, storage and data types and requires no changes to application software.

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 for PCI includes BJ's Wholesale, Sirius Radio, DSW to name just a few. Vormetric is the technology leader in the data protection arena, holding 14 patents and FIPS validation on all products. The company is the winner of industry acclamation such as ComputerWorld's Innovative Technology Award, and serves as a respected partner of industry giants such as IBM, Microsoft, Sun and Oracle.

Conclusion: CoreGuard Enables PCI Compliance

The PCI standards place substantial new data protection burdens on companies, but you can embrace this opportunity to examine the security of your data and install CoreGuard to fill the gaps in your data protection efforts. CoreGuard provides a single affordable tool to meet many of the PCI requirements that are not already covered by the basic security applications you may have in place. By implementing this comprehensive solution, you can add encryption, access control, host protection and auditing to your data protection initiative, and achieve compliance with this critical industry standard.

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.



VORMETRIC