ADDRESSING PCI DSS 3.0 REQUIREMENTS WITH THE VORMETRIC DATA SECURITY PLATFORM

How Solution Capabilities Map to Specific PCI DSS 3.0 Requirements

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

Vormetric, Inc.
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
Singapore: +65 6829 2266
info@vormetric.com
www.vormetric.com

TABLE OF CONTENTS:

In recent years, the requirements detailed within the Payment Card Industry Data Security Standard (PCI DSS) grew substantially—as have the challenges associated with complying with the standard. This paper offers a detailed look at the most recent version of the standard, and it examines the key requirements that Vormetric solutions can help address.

INTRODUCTION

Consumer payment data continues to be a compelling target for criminals, and the defenses enacted to guard these assets continue to be circumvented. In just the last few years alone, it seems virtually every major retail brand, and scores of payment processors and other smaller businesses have been the victims of devastating data breaches.

In an effort to help organizations guard against these types of breaches, the major payment card brands came together to develop a set of rules that would help organizations establish strong defenses around cardholder data. First released over a decade ago, the Payment Card Industry Data Security Standard (PCI DSS) was developed to help merchants, payment processors, and all other regulated entities establish the security controls required to safeguard cardholder data. The most recent release of the standard, PCI DSS 3.0, was published in November 2013, and all regulated organizations were required to align with the new rule by January 1, 2015.

While the need to comply with PCI DSS isn't new, many of the challenges associated with establishing and sustaining compliance are. The increased use of virtualization, cloud computing, and big data have created additional challenges in achieving compliance with PCI DSS. For enterprise risk managers, information security personnel, and IT operations professionals, complying with PCI DSS continues to represent a significant effort.

This paper is intended to help provide some insights into how Vormetric solutions can help support IT and security team's efforts to address PCI DSS requirements. The following sections offer an overview of the Vormetric Data Security Platform. Then, subsequent sections examine the standard's requirements, and outline those rules that this solution can help address.

This document's foundation is based on research and supporting documentation of Coalfire®, a leading PCI-qualified security assessor (QSA) and independent IT audit firm. However, this paper is intended to provide general insights, rather than prescriptive guidance. Every organization's environment, threats, and requirements are different, and security teams need to enlist the services of an external QSA in order to take the most effective steps to establish maximum security of cardholder data, both in the near term and over the long term.

THE VORMETRIC DATA SECURITY PLATFORM

The Vormetric Data Security Platform is a comprehensive and extensible platform for delivering data-at-rest security across traditional physical servers, virtual systems, cloud services, and big data environments. The Vormetric Data Security Platform delivers capabilities for transparent file-level encryption, application-layer encryption, tokenization, dynamic data masking, cloud encryption gateway, integrated key management, privileged user access control, and security intelligence.

With this comprehensive set of capabilities, Vormetric puts control of the primary account number (PAN) and other regulated data in the merchant's hands. With these solutions, security teams can encrypt and tokenize records and retain visibility and control over which users and processes can gain access to the data in the clear.

With these capabilities, Vormetric can help organizations comply with many PCI DSS requirements. Further, it is important to note that Vormetric solutions provide the strong controls that can help organizations address a wide range of other compliance mandates, including the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the UK Data Protection Act, EU Commission Regulation No 611/2013, and many others.

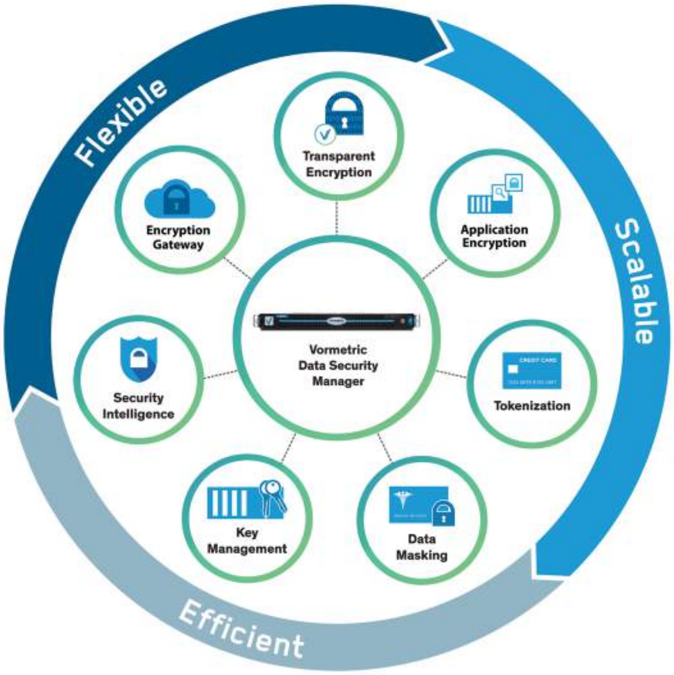

Figure 1: Vormetric Data Security Platform

The Vormetric Data Security Platform features these products:

- **Vormetric Transparent Encryption.** This product features an agent that runs in the file system to provide high-performance encryption and least-privileged access controls for files, directories, and volumes. Vormetric Transparent Encryption offers support for both structured databases and unstructured files.
- **Vormetric Tokenization with Dynamic Data Masking.** This product delivers capabilities for database tokenization and dynamic display security. With these capabilities, organizations can tokenize cardholder data and remove it from PCI DSS audit scope.
- **Vormetric Application Encryption.** Vormetric Application Encryption simplifies the process of adding column-level encryption into existing applications. The product therefore enables organizations to more efficiently encrypt specific columns, for example those holding PANs, within databases.

- **Vormetric Cloud Encryption Gateway.** This product enables organizations to safeguard files in cloud storage environments, including Amazon Simple Storage Service (Amazon S3) and Box. With the solution, organizations can encrypt sensitive files, including those that contain cardholder data, before they are saved to the cloud. The solution maintains encryption keys on the customer premises, enabling security teams to establish the visibility and control they need around sensitive assets.
- **Vormetric Security intelligence.** Vormetric offers granular logs that provide a detailed, auditable record of file access activities, including root user access. The product enables easy integration with security information and event management (SIEM) systems to streamline compliance reporting and accelerate threat detection.

POWERED BY VORMETRIC DATA SECURITY MANAGER

All the products above can be centrally controlled through the Vormetric Data Security Manager (DSM). The DSM controls policies and key management for Vormetric products and provides a unified solution to manage keys for third-party platforms, such as IBM InfoSphere Guardium Data Encryption, Oracle Transparent Data Encryption (TDE), Microsoft SQL Server TDE, and KMIP-compliant encryption products.

This product offers flexible deployment, enabling customers to choose from a virtual appliance and as a physical system that has been FIPS 140-2 certified. The virtual appliance can be deployed on premises or in the cloud. Either deployment model can meet PCI DSS standards. It's important to note that the DSM is only the key and policy manager and cardholder data and other sensitive assets are never passed through it.

The DSM is available in the following form factors:

- A hardware appliance, with FIPS 140-2 Level 2 certification.
- A hardware appliance, with integrated HSM, FIPS 140-2 Level 3 certification.
- A hardened virtual appliance, which can run on-premise or in the cloud.
- As a service through AWS Marketplace.

In support of PCI DSS requirements, the DSM can enforce strong separation of duties by requiring the assignment of key and policy management to more than one data security administrator. In this manner, no one person has complete control over the security of data. The DSM is accessed through a secure Web-management console, command-line interface (CLI), or APIs.

VORMETRIC TOKENIZATION WITH DYNAMIC DATA MASKING

The Vormetric Data Security Platform features tokenization capabilities that can dramatically reduce the costs and effort associated with complying with security policies and PCI DSS. With Vormetric Tokenization with Dynamic Data Masking, organizations can efficiently address objectives for securing sensitive assets and cardholder records—whether they reside in the data center, big data environments, or the cloud.

Vormetric Tokenization makes it easy to use format-preserving tokenization to protect sensitive fields in databases. By leveraging Vormetric Tokenization, you can reduce the size of the cardholder data environment (CDE) by exchanging cardholder data, like the primary account number (PAN), with a format-preserving token. The result is that databases, networks, and other systems that once held cardholder data can be removed from PCI DSS scope. By reducing the number of systems that need to be audited through self-assessment or a QSA, organizations can significantly reduce compliance costs and efforts.

The solution features the Vormetric Token Server, which is a virtual appliance for tokenizing records and managing access to tokens and clear-text data. With Vormetric Token Server, applications use REST APIs to send requests for the creation and management of tokens, which streamlines the process of implementing and managing tokenization. In addition, the product eliminates the complexity of adding policy-based dynamic data masking to applications.

VORMETRIC ENCRYPTION PRODUCTS

It isn't always possible to remove cardholder data from PCI scope using tokenization. Sometimes this data is in an unstructured file, such as an Excel spreadsheet, PDF document or an mp3 audio file. There are other times you may not be able to tokenize the data within the database. Vormetric offers several different encryption solutions that can be employed in the CDE in order to comply with PCI DSS requirements.

VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption enables data-at-rest encryption, privileged user access control, and the collection of security intelligence logs for structured databases and unstructured files—including those residing in physical, big data, and cloud environments.

Vormetric Transparent Encryption employs file system agents that are installed above the file system's logical volume layers. These agents perform encryption, decryption, access control, and logging. The solution's agents evaluate any attempt to access protected data and apply policies defined on the DSM to either grant or deny such attempts. The agents maintain a strong separation of duties on the server by encrypting files, while leaving their metadata in the clear. As a result, IT administrators can perform their jobs without directly accessing the information.

Vormetric Transparent Encryption agents are installed on each server where data requires protection. The agents are specific to the OS platform and transparent to applications, databases (including Oracle, IBM, Microsoft, Sybase, and MySQL), file systems, networks, and storage architecture. This results in fast and easy deployment.

VORMETRIC APPLICATION ENCRYPTION

Application-layer encryption is typically employed when compliance or regulatory mandates require encryption of specific fields at the application layer, before data is stored. Vormetric Application Encryption reduces the complexity and costs associated with meeting this requirement, simplifying the process of adding encryption capabilities to existing applications.

Vormetric Application Encryption enables application-layer encryption of a specific field or column in a database, big data node, or platform-as-a-service (PaaS) environment. Vormetric Application Encryption provides a set of documented, standards-based APIs that can be used to perform cryptographic and key management operations.

VORMETRIC CLOUD ENCRYPTION GATEWAY

The Vormetric Cloud Encryption Gateway enables organizations to safeguard sensitive data in cloud storage environments. The Vormetric Cloud Encryption Gateway is delivered as a virtual appliance that can be deployed in the cloud or in the customer's data center. The solution encrypts sensitive data before it is saved to the cloud storage environment, enabling security teams to establish the visibility and control they need around sensitive assets. Like other Vormetric encryption offerings, the solution relies on the DSM for key and policy management. As a result, customers can establish PCI DSS-compliant control over cryptographic keys and ensure PAN and other sensitive data never leaves the enterprise premises unencrypted or unaccounted for.

PCI DSS REQUIREMENTS: HIGH LEVEL REVIEW OF THE STANDARD AND HOW VORMETRIC SOLUTIONS CAN APPLY

Complying with the PCI DSS requires the effective implementation and coordination of people, processes, and technologies. While Vormetric solutions can help organizations comply with a number of PCI DSS requirements, neither these solutions, nor any other products, will enable compliance with the entire standard. Many of the requirements pertain to processes and policies, such as conducting background checks on employees or implementing secure coding standards for Web applications. It is also important to recognize that without effective governance, even the most robust technology won't fully address PCI DSS standards, or, more importantly, the organization's ultimate security objectives.

PCI DSS is broken into twelve high-level requirements, each of which contains multiple sub-requirements and defined testing procedures for validating compliance. Below is a listing of each high-level requirement, followed by a summary of how they relate to Vormetric solutions. The appendix at the end of this document offers readers a detailed matrix that specifies how Vormetric solutions address a number of sub-requirements.

BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

While Vormetric products must be deployed in accordance with this requirement; there are no specific tenets of requirement one that the Vormetric solution addresses. Typically, components of Vormetric Data Security Platform that are implemented on premises are deployed in a secure internal network, behind the organization's firewall.

When organizations are storing cardholder data in multi-tenant environments, the environments of other tenants and the hosting infrastructure would be considered untrusted. In these cases, addressing requirement 1.1.4a, which requires "a firewall at each Internet connection and between any DMZ and the internal network zone," (italics added) may not be possible or adequate in securing cardholder data. However, by implementing capabilities like strong encryption, tokenization, key management, and access controls, security organizations can remove shared infrastructure components from PCI DSS audit scope.

Ultimately, the adequacy of any network segmentation, and its ability to support compliance with the PCI DSS, must be validated through such efforts as internal penetration testing.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

While Vormetric solutions must be deployed in accordance with this requirement, there are no specific tenets that apply directly. Vormetric Data Security Platform components do not install with vendor-supplied default passwords; all security parameters are defined during installation. When software components of the Vormetric Data Security Platform are implemented in a CDE, the security team should confirm that they are being installed on servers and operating systems that are secured as mandated by requirement two.

PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

Vormetric solutions directly support the tenets of this requirement. Vormetric offers a range of capabilities—including data encryption, tokenization, privileged user access controls, and key management—that address many of the specific requirements in this section of the standard. Vormetric solutions can encrypt cardholder data at the field, file, or volume level. They can also tokenize and partially mask specific fields in databases. With Vormetric solutions, robust, industry-standard cryptographic keys are used, and they are stored separately from encrypted data. In addition, the solution supports the requirements surrounding split knowledge and dual control of key management. For example, key custodians can be granted access to perform key management activities, but not have direct access to the actual key value.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

The transmission of cardholder data to or from a guest system over a public network must be protected. Focused on data at rest, Vormetric solutions don't directly address the transmission-encryption requirements of this standard. However, by leveraging Vormetric Data Security Platform, organizations can address many of the risks posed by transmitting sensitive data over public networks.

For example, the Vormetric Cloud Encryption Gateway enables organizations to encrypt data on the enterprise premises, before it is sent over networks to Amazon S3 or Box cloud storage. In addition, by leveraging solutions like Vormetric Transparent Encryption and Vormetric Tokenization, organizations can ensure that sensitive assets are secured against unauthorized access, even when databases and files are transmitted across public networks, whether to a remote backup server, a disaster recovery site, or cloud-hosted environment. Because they enable security teams to retain persistent, localized control over cryptographic keys and policies, these solutions enable persistent, auditable control over account information and other sensitive assets.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

If it is determined that anti-virus software is necessary in a given environment, this would have to be addressed in accordance with the customer's overall security framework. There are no applicable elements of requirement five that apply directly or indirectly to Vormetric solutions.

Requirement 6: Develop and maintain secure systems and applications

Vormetric is maintained independent of the databases, applications, and other systems that manage cardholder data. Vormetric provides software updates and patches as necessary. Vormetric customers with current maintenance contracts have access to a support portal from which they can sign up to receive email notifications when software updates are available. As part of their risk assessment policies and procedures, customers should evaluate software updates and ensure that patches are implemented in a timely fashion.

The use of Vormetric should be taken into account when developing software that stores, processes, or transmits cardholder data. However, the controls surrounding the software development life cycle and systems vulnerability management are outside of the scope of the paper.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need to know

Vormetric solutions offer a range of capabilities for addressing requirement seven. With these solutions, security teams can implement least privileged access controls and deny unauthorized access to protected cardholder information. For example, systems administrators, database administrators, and other privileged users may be granted access to perform administration tasks on systems they're responsible for, without being able to decrypt the data on those systems.

Procedures for requesting and administering access to encryption keys and decryption activities must be developed to address the requirement to "enforce privileges assigned to individuals based on job classification and function" (requirement 7.2.2).

When Vormetric solutions are employed to secure cardholder data in virtualized environments and cloud implementations, the security team can manage access in the same fashion as in a non-virtualized or internally hosted implementation. As a result, corporate security teams can retain control of sensitive information, independent of the implementation strategy.

Requirement 8: Identify and authenticate access to system components

Vormetric solutions can work in conjunction with an organization's systems for managing user identities and authentication. These solutions can leverage the identities and privileges established in the corporation's existing directory service, including LDAP (Lightweight Directory Access Protocol) and Microsoft Active Directory. Vormetric solutions can be used to address these requirements:

- Encrypting credentials stored in application files or databases (requirement 8.2.1) when custom-built authentication systems are employed.

- Establishing programmatic access controls for all users with direct access to a database, including administrators and application accounts (requirement 8.7).

Requirement 9: Restrict physical access to cardholder data

The physical location in which Vormetric components and controls are implemented must comply with this standard, however, there are no elements of this standard that apply specifically to Vormetric solutions.

The Vormetric Data Security Platform can support policies requiring hard drives to be securely wiped prior to disposal or reuse. Encrypted data on such hard drives will make that information practically impossible to recover: Someone that somehow gains access to the disposed drive material would also need to gain required authorizations to access the DSM and gain access to the appropriate decryption keys.

When an organization employs Vormetric Tokenization, credit card records can be stored in the token server, where they are protected using encryption and key management techniques that meet PCI DSS requirements.

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

Vormetric Transparent Encryption provides logging of access at the file-system level. This provides PCI-compliant audit records of all read and write requests to encrypted data. Security teams can establish policies that monitor all access to sensitive data, including access by privileged users.

The solution features reporting tools that enable administrators to analyze the logs generated. In addition, the solutions enable administrators to set policies for generating automated alerts whenever activities that require special monitoring are conducted. Vormetric audit logs can be stored within the platform, in an organization's security information and event management (SIEM) system, or in another log collection solution. For more information, including a current list of SIEM partners that provide pre-integrated dashboard or reporting support for Vormetric solutions, please visit the Vormetric Security Intelligence page.

Requirement 11: Regularly test security systems and processes

While Vormetric does not directly address specific tenets of this requirement, applicable scanning and testing requirements could apply to components of the Vormetric solution that are running in the CDE. Additionally, while not a file-integrity monitoring tool, Vormetric solutions can support compliance with requirement 11.5, which requires change-detection mechanisms that "alert personnel to unauthorized modification of critical system files, configuration files, or content files…" Through the solutions' logging and reporting capabilities, administrators can supplement their ability to monitor access to files and volumes that contain cardholder data.

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain a policy that addresses information security for all personnel

Vormetric solutions must be managed in accordance with all of the customer's operational policies and procedures. However, these are operational requirements for the customer and are not directly applicable to these solution's capabilities.

PCI DSS, VIRTUALIZATION, AND THE CLOUD

PCI DSS pertains to all systems in the CDE that store, transmit, or process cardholder data. To reduce the scope of PCI DSS compliance requirements, a merchant can segment their network in order to separate the systems that manage cardholder data from those that do not.

Through this approach, an organization can remove systems that are unrelated to payment card processing from PCI DSS scope. However, the introduction of virtualization and cloud computing into the CDE can blur these lines of segmentation.

When implementing the CDE using virtualization or cloud technologies, there are additional risk factors that must be considered and addressed. This is especially true when a single platform hosts some virtual systems that handle cardholder data and some that do not. In addition, as noted in the PCI DSS Cloud Computing Guidelines, there are additional challenges to address when outsourcing the hosting of the CDE to a cloud service provider (CSP).

However, in spite of these complications, organizations can achieve and sustain full compliance when running some or all of their CDE in virtualized or cloud environments. It should be noted that this paper does not attempt to address all of the concerns of working within a cloud environment, nor is it intended to replace the PCI DSS Cloud Computing Guideline document. However, following are some high-level descriptions of the risks of running in the cloud, and how the Vormetric Data Security Platform can help address them.

CLOUD COMPLIANCE RISKS—AND HOW VORMETRIC CAN HELP

When deploying in a CSP's network, the shared responsibility for implementation, operations, and management of security must be understood and agreed upon by all parties. Nested service provider relationships are not uncommon and could make understanding roles and responsibilities complicated. For instance, the merchant might be hosting with Amazon Web Services (AWS) while also working with a payment processor that hosts some of its operations in AWS.

Today, these types of relationships are growing increasingly commonplace, and they continue to add complexity to both the service provider's and the merchant's PCI DSS assessment process. The Vormetric Data Security Platform provides key capabilities that can help in establishing and supporting clear roles and responsibilities in these scenarios. The solution can help by providing these capabilities:

- Encrypting files on the enterprise premises, before they are saved into cloud storage environments like Amazon S3 and Box.
- Ensuring that the CSP's administrators cannot access cardholder data or other sensitive information.
- Safeguarding against improper disposal or theft of storage resources by ensuring that these incidents won't result in the exposure of any data in clear text.
- Establishing controls so that a failure in multi-tenancy policies or controls will not expose clear text PAN or other sensitive data to other tenants or unauthorized users.
- Enabling data owners to retain continuous custodianship of access policies and keys, even though cardholder data may reside in the CSP's environment.

CONCLUSION

The ability to achieve overall compliance with any regulation or standard will be dependent upon a range of efforts, including the specific design and implementation of the Vormetric Data Security Platform in the CDE. It is advisable to work closely with a QSA early in the design process to facilitate validation. When evaluating solutions to meet an upcoming audit, it is a best practice to consider other common requirements of other current or future regulations and mandates. Selecting a solution that covers many common compliance controls will ultimately not only offer the best long-term value, but also accelerate the completion of the next audit.

It is also important to consider the flexibility of the solution. Any solution you invest in should not only satisfy today's requirements, it should be ready to migrate with you to new environments, such as big data and the cloud. Make sure a solution won't lock you into a specific platform. Select a solution that will support a breadth of platforms to meet new requirements and growth opportunities.

The Vormetric Data Security Platform offers the extensibility to move with you to new environments and platforms, and to meet common compliance requirements around encryption, tokenization, access control, and auditing. The solution centrally manages the data-at-rest security and compliance of all your environments and is ready to expand to new opportunities. That is why over 1,500 customers around the globe trust Vormetric today, including 17 of the Fortune 30.

REFERENCES AND RESOURCES

- Payment Card Industry (PCI) Data Security Standard, 3.0, November 2013
- Cloud Special Interest Group, PCI Security Standards Council. (2013). Information Supplement: Computing Guidelines.
- Virtualization Special Interest Group, PCI Security Standards Council. (2011). Information Supplement: Virtualization Guidelines.
- Using Encryption and Access Control for PCI DSS 3.0 Compliance in AWS, a Coalfire White Paper.

APPENDIX: VORMETRIC CONTROLS AND SUPPORT MATRIX

The following table provides additional details on how specific requirements pertain to the Vormetric Data Security Platform and how the solution supports organizations in establishing a PCI-compliant environment. The table only lists those requirements that were considered either applicable or supported, and not the entire PCI DSS. Merchants, credit card service providers, and any other entities covered by the requirements of the PCI DSS should always consult with their own QSA to determine the scope of controls applicable to them.

Table 1: How Vormetric Security Platform Applies to PCI DSS 3.0 Controls

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
No applicable requirements. If Vormetric solutions are implemented as part of a CDE, administrators should ensure that they are deployed in a network environment that is compliant with PCI DSS 3.0. Whether the solution is deployed on the enterprise premises or in an external cloud provider's environment, the network must be compliant with the requirements outlined in PCI DSS requirement one. However, the controls surrounding the network and deployment of the Vormetric solution are entirely dependent upon the user's architecture and are outside of the scope of the paper.		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
No applicable requirements. If Vormetric solutions are implemented as part of a CDE, the security team should ensure that they are deployed in an environment that is PCI DSS 3.0 compliant. The DSM comes pre-configured and uses a hardened Linux operating system. When software components of the Vormetric Data Security Platform are implemented in a CDE, administrators should confirm that it is being installed on servers and systems that are secure and that have hardened operating systems as required in PCI DSS requirement two. Vormetric components will not allow implementation with default or weak passwords.		

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
Requirement 3: Protect stored cardholder data		
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification AND • The data is stored securely.	While issuers and their service providers may have a legitimate business need for storing this authentication data, merchants, service providers supporting merchants, and acquirers must never store sensitive authentication after the payment transaction's authorization is processed. For organizations that do have a business need to retain sensitive authentication data, Vormetric solutions offer the strong cryptography and key management that support the secure storage of this information as required by **3.2**. Vormetric Transparent Encryption can secure the files and volumes that contain this authentication information, including structured and unstructured data. In addition, with Vormetric Application Encryption, security teams can encrypt specific fields and columns in databases that contain sensitive authentication data. The data can always be tokenized and removed from scope.
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.	With Vormetric Tokenization, administrators can establish policies to return an entire field tokenized or dynamically mask parts of a field. For example, a security team could institute policies so that a user with customer service representative credentials would only receive a credit card number with the first six and last four digits visible, while a customer service supervisor could access the full credit card number in the clear.
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key- management processes and procedures.	Vormetric directly supports **3.4** by offering strong cryptography and associated key management capabilities. With the Vormetric Data Security Platform, organizations can encrypt and tokenize files and fields in which PANs reside. Vormetric's ability to encrypt structured and unstructured data means that it can protect the data whether it is in files or in databases.
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts	While not directly supporting disk encryption, Vormetric Transparent Encryption supports volume-level encryption that expands encryption beyond a single file or a database column. The solution manages access to the encrypted data independent from the system's operating systems access control. Policies governing access to decrypted data are managed and administered within the DSM. This offering can be integrated with an organization's LDAP or Active Directory implementation in order to leverage corporate identities and access policies. Cryptographic keys are not tied to user accounts, but are contained within the DSM. Vormetric performs the encryption and decryption functions, as opposed to granting authorized and authenticated users access to the keys.

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: **3.5.1** Restrict access to cryptographic keys to the fewest number of custodians necessary **3.5.2** Store secret and private keys used to encrypt/ decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method	While the user organization will need to document key management procedures, Vormetric supports requirement **3.5**, by ensuring that encryption keys are securely stored. Vormetric directly supports **3.5.1** by enabling organizations to centrally generate and store cryptographic keys in the DSM. With the solution, the actual keys are never visible to anyone, including key custodians or systems administrators. Vormetric restricts access to keys and key management activities by managing access within the DSM, which decouples access rights from central access management systems such as Active Directory, thus restricting access by privileged users, such as system administrators with root-access privileges, unless explicitly granted within the DSM. Vormetric directly supports the first bullet of **3.5.2** by encrypting the data encryption keys with an AES 256-bit key. This encrypted key is stored securely on the DSM, which is separate from the location in which the data encryption key is used. If an administrator elects to cache data encryption keys on the local server in order to eliminate network latency, local keys can also be encrypted with an AES 256-bit key. Vormetric also offers an HSM deployment option that addresses the second bullet point.
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: **3.6.1** Generation of strong cryptographic keys **3.6.2** Secure cryptographic key distribution **3.6.3** Secure cryptographic key storage **3.6.4** Cryptographic key changes for keys that have reached the end of their crypto-period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as 3.6.6 defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. **3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control **3.6.7** Prevention of unauthorized substitution of cryptographic keys	While the user must document the key-management processes used within their organization and ensure that key custodians understand and acknowledge their responsibilities, Vormetric Data Security Platform supports compliance with the technical requirements associated with **3.6**. The DSM is designed for strong cryptographic key management using a secure Web management console. The solution helps address the following requirements: **3.6.1:** Cryptographic keys are centrally generated by the DSM appliance and are fully compliant with FIPS standards. **3.6.2:** Clear text keys never leave the DSM. When keys are distributed to agents, they are encrypted with a one-time-use AES 256 key and sent over a mutually authenticated TLS connection. **3.6.3:** The DSM provides a secure central repository for cryptographic keys and policies. Customers can choose to cache cryptographic keys on the host server. Vormetric's highly secure agents protect these keys from unauthorized access, even from root administrators. When keys are cached locally, they are protected with a wrapper key and are not accessible by any system user. **3.6.4:** Cryptographic keys can be changed by key custodians based upon the organization's policies for cryptographic periods. When a key is retired by a custodian, it can be permanently deleted. Key change procedures need to specify a process for re-encrypting data with new keys before making old keys obsolete.

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
3.6 Cont.	**3.6.7** Prevention of unauthorized substitution of cryptographic keys	**3.6.5:** Cryptographic keys can be changed by key custodians when a key has been weakened or compromised. When a key is changed by a custodian, it can be permanently deleted. Key change procedures will need to include a process for re-encrypting data with new keys before making old keys obsolete. **3.6.6:** With Vormetric solutions, administrators don't have to do manual management of keys in clear text. Custodians can create keys, but key values are not visible to the custodian. The DSM protects against any one person having access to key material by supporting "no knowledge", configurable split knowledge, and dual control policies. **3.6.7:** Access control policies defined within the DSM govern access to key creation and other key management activities, restricting access to authorized key custodians only. The DSM supports an "m-of-n" sharing scheme for backing up keys. A specific number of shares must be provided in order to restore the encrypted contents of an archive from the DSM into a new or replacement instance.
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	Vormetric solutions are focused on securing data at rest. While Vormetric solutions don't support the encryption of transmissions across networks, they do offer the strong encryption that supports requirement **4.1**. By employing Vormetric solutions, organizations can secure specific files and fields that contain sensitive cardholder data, and ensure that data remains secure, even as that data is transmitted across public networks and into other environments. For example, by employing Vormetric Transparent Encryption, organizations can safeguard sensitive cardholder data residing in files, even as those files are backed up into a remote disaster recovery site. In addition, with Vormetric Cloud Encryption Gateway, organizations can encrypt sensitive files on their premises, before they are transmitted across networks and into cloud storage environments like Amazon S3 and Box.
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs		
The DSM is an appliance with a hardened Linux kernel and is generally not considered "commonly affected by malicious software", particularly when properly deployed away from public traffic in a PCI DSS-compliant CDE. However, the encrypted cardholder data could be stored on systems that require anti-virus, so Vormetric administrators should consult their QSA regarding their architecture and the appropriate technology for protecting against malware.		
Requirement 6: Develop and maintain secure systems and applications		
No applicable requirements. Vormetric provides software updates for new functionality or software patches as necessary. Vormetric customers with maintenance contracts have access to a support portal from which they can sign up to receive email notifications as software updates are available. Customers should evaluate software updates during their vulnerability risk assessment process and ensure that patches are implemented in a timely fashion. The use of Vormetric should be taken into account when developing software that stores, processes, or transmits cardholder data. However, the controls surrounding the software development life cycle and systems vulnerability management are outside of the scope of the paper.		

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
Requirement 7: Restrict access to cardholder data by business need to know		
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Vormetric solutions directly support **7.1** by adding a layer of access control on top of the native operating system access controls. These solutions can also prevent privileged users from accessing or viewing cardholder data that they're not authorized to access. The solution enables least privilege access without interfering with normal administrative operations.
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Vormetric directly supports **7.1.1** by ensuring that cardholder data cannot be viewed by system administrators who do not have a "need to know," while simultaneously ensuring that there is no interruption to data backup and other administrative processes. By leaving metadata in the clear, but encrypting the underlying data, Vormetric solutions enable administrators to identify the files that require backup, without gaining access to the file itself.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Vormetric directly supports **7.1.2** by enforcing policies that enable privileged users, including those with administrator or root privileges, to be granted the access needed for their job responsibilities, while being restricted from accessing cardholder data. In this way, organizations can effectively restrict access based on users' "need to know."
7.1.3	Assign access based on individual personnel's job classification and function.	Vormetric directly supports **7.1.3** by enforcing policies that ensure individuals, applications, and processes are provided least privileged access to cardholder data. Policies can be based on job classification and business responsibilities, thereby restricting access based on "need to know."
7.1.4	Require documented approval by authorized parties specifying required privileges.	While administrators will need to implement processes for approving requests for access, Vormetric solutions support **7.1.4** by providing a granular, policy-based system that restricts access based on individual, role, process, time of day, and location of data. Vormetric solution policies can be configured to be in alignment with an organization's documented approval processes, enabling controls to be enforced around the release of encrypted contents for backup, decryption of contents based on need to know, and control of rights to the data file. Available audit records can be used to monitor granted or changed privileges to ensure compliance with documented access control processes for cardholder data.
7.2	Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following: **7.2.1** Coverage of all system components **7.2.2** Assignment of privileges to individuals based on job classification and function. **7.2.3** Default "deny-all" setting.	Vormetric solutions directly support **7.2** by enabling security teams to enforce policies that authorize users and applications to access cardholder data storage. Only authorized users and applications can access data in clear text. With Vormetric solutions, administrators can be given access to files containing cardholder data, but without gaining the permissions needed to decrypt the file. Default policy is to deny access to all, except those who have explicit authorization.

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
Requirement 8: Identify and authenticate access to systems components		
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase Something you have, such as a token device or smart card • Something you are, such as a biometric.	Through its support for RSA tokens, the DSM can enable the enforcement of two-factor authentication for users attempting to access Vormetric system components.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Vormetric integrates with existing directory services, including LDAP and Active Directory, to authenticate user IDs. All transmission of Vormetric authentication and key material takes place over a mutually authenticated TLS channel.
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	With Vormetric, direct access to data and database queries can be limited to only database administrators. Vormetric Transparent Encryption provides control at the file system level, below the database. When a database is protected with Vormetric, all access to the data in the database must come from the database process. All other sources are denied access. For example, a set of operating system super-users can have a policy that prevents their ability to copy files, while enabling them to view the database contents.
Requirement 9: Restrict physical access to cardholder data		
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	While not directly supporting requirement **9.8.2,** Vormetric supplements other controls introduced to render retired hard drives or removable media unreadable. Should encrypted data not be adequately cleaned from media, the data will not be viewable in clear text unless the DSM is available to authorize the decryption of the data on that media.
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1	Implement audit trails to link all access to system components to each individual user	Vormetric directly supports **10.1** by providing detailed logging at the file system level. Any read, write, or other access requests for sensitive data can be audited. The DSM provides audit records that contain details such as host machine, directory, file, or resource accessed; specific user and user group; policy invoked; application; and time of day.
10.2	Implement automated audit trails for all system components to reconstruct the following events: **10.2.1** All individual user accesses to cardholder data **10.2.2** All actions taken by any individual with root or administrative privileges	Vormetric provides detailed auditing at the file system level. Any read or write access or other request for sensitive data can be audited and the trails contain information to track access back to a specific user, application, and time. The Vormetric Data Security Platform delivers these capabilities: • Policies can be constructed to monitor individual access to cardholder data. **(10.2.1)**

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
10.2 Cont.	**10.2.3** Access to all audit trails **10.2.4** Invalid logical access attempts **10.2.7** Creation and deletion of system-level objects	• The solution enables the monitoring of individual access to cardholder data and the logging of activities of individuals with root or administrative privileges. Policies can also be established that prevent privileged users from accessing data in the clear, while still enabling them to perform their day-to-day administrative duties. Both failed and successful attempts to view card data are logged. **(10.2.2)** • With the solution, DSM administrators can be assigned the role of "audit officer", so they can access audit trails, which are centrally stored. Vormetric recommends that audit/log data be sent to a centralized log server safeguarded by the Vormetric Data Security Platform. All access and access attempts to Vormetric solution logs can be audited. **(10.2.3)** • The solution can be configured to enable the audit of all denied access requests. **(10.2.4)** • The platform enables logging of all key custodian activity. **(10.2.7)**
10.3	Record at least the following audit trail entries for all system components for each event: **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.	Vormetric provides detailed auditing at the file system level, generating audit entries that include: • User-name and group membership. **(10.3.1)** • Type of event. **(10.3.2)** • Date and time. **(10.3.3)** • Success or failure indication. In the case of a permitted action, the event data also includes whether the access was to clear text or to encrypted data. **(10.3.4)** • Origination of the event. **(10.3.5)** • Host and the full path to the file that was the target of the access request. **(10.3.6)**
10.4.1	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. • Critical systems have the correct and consistent time	The DSM can be configured to synchronize with a Network Time Protocol (NTP) server.
10.5	Secure audit trails so they cannot be altered. **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. **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Vormetric secures audit trails generated by: • Ensuring that audit trails cannot be modified while they reside on the DSM. If log and audit files are sent to a centralized log server, this external log repository can be protected and safeguarded with Vormetric Transparent Encryption and access control. **(10.5.2)** • Providing an extensive set of log and audit capabilities to track and monitor access to cardholder data. These files can be sent to a customer's centralized log server or event management solution via syslog. In addition, this external log repository can be protected and safeguarded with the Vormetric Data Security Platform. **(10.5.3)** • Ensuring log files cannot be modified while they reside on the DSM. **(10.5.5)** Further, customers may use the Vormetric solution to block or monitor changes to log files and other audit trails.

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	The Vormetric Data Security Platform generates log reports for monitoring daily activity relating to encrypted assets.
Requirement 11: Regularly test security systems and processes		
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	The Vormetric Data Security Platform is not a file integrity management solution that can be used to alert administrators to unauthorized changes to all operating system and execution files. However, Vormetric Transparent Encryption can provide audit information relating to encrypted file access. For encrypted files that contain cardholder data, the solution can be configured to generate automated alerts any time these files are accessed or modified. In this way, the solution supports the file integrity monitoring requirements detailed in **11.5**.
Requirement 12: Maintain a policy that addresses information security for all personnel		
No applicable requirements. Along with the rest of the CDE, a Vormetric Data Security Platform deployment must be managed in accordance with all of the organization's policies and procedures. However, discussion of these policies and procedures is outside the scope of this paper and Vormetric users should consult with their own QSA regarding their coverage and compliance.		

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps over 1,500 customers, including 17 of the Fortune 30 and many of the world's most security conscious government organizations, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application—anywhere it resides—with a high performance, market-leading data security platform that incorporates application transparent encryption, privileged user access controls, automation and security intelligence.

For more information, please visit: www.vormetric.com.