A COALFIRE WHITE PAPER

Using Encryption and Access Control for PCI DSS 3.0 Compliance in AWS

Implementing the Vormetric Data Security Platform in a Payment Card Environment running in Amazon Web Service (AWS)

February 17th 2014

Executive Summary

This paper examines the suitability of the Vormetric Data Security Platform for AWS to secure Payment Card Industry (PCI) data in accordance with the PCI Data Security Standard (PCI DSS)[1] 3.0 when used in Amazon Web Services (AWS).

In Coalfire's evaluation and analysis of the Vormetric Data Security Platform and its various security capabilities, we have determined it to be capable of such support, when implemented within the context of a PCI compliant security architecture. In addition, there are no known inhibitors within the product that would prevent an organization from running PCI applications in a compliant manner and there are features that facilitate meeting certain PCI requirements.

Due to the unique business, technical, security and governance requirements that every organization has, this paper does not provide detailed recommendations for how to configure Vormetric products to meet the applicable portions of the PCI DSS.

When implementing solutions that contain sensitive or regulated data within Amazon Web Services (AWS) organizations must be able to secure and control the data in this multitenant infrastructure that is not under their direct control. The Vormetric Data Security Platform delivers a combination of strong encryption, access and privileged user control policies enforcement, and security intelligence to secure and control data in the cloud.

Introduction

Merchants, large and small, face the high risk of data breaches arising from inadequate security controls or insecurely developed and deployed applications, which leak or allow access to sensitive cardholder data. The Payment Card Industry Data Security Standard was developed with the intent of reducing the risk of handling cardholder data and is one of the most rigorous standards established to date.

[1] The PCI DSS is available from the PCI Security Standards Council at http://pcisecuritystandards.org. At the time of this writing the current standard is version 3.0.

Security professionals, service providers, application developers, hardware manufacturers and converged infrastructure vendors are working across a number of security domains to address the data security needs of merchants. Virtualization and cloud computing can create additional challenges in achieving compliance with the DSS, but does not inherently prevent compliance.

This paper is organized as follows:

- **PCI and Cloud Basics:** Provides the background of PCI DSS and its application in virtual/cloud environments.
- **Overview of the Vormetric Data Security Platform:** Overview of the product capabilities and deployment models available in the cloud.
- **Vormetric Data Security Platform Components and associated PCI Scope:** Describes how the platform components support PCI.
- **Applicability of PCI DSS to Vormetric Data Security Platform:** Reviews the primary PCI DSS requirements and how, where applicable, these are addressed by the Vormetric solution.
- **Conclusion:** Summarizes the findings of the evaluation of Vormetric solution and its fitness as a PCI DSS application platform.
- **Appendix:** Controls and Support Matrix provides a cross reference of those PCI DSS sections applicable to the Vormetric Data Security Platform for AWS deployments.

PCI and Cloud Basics

This paper assumes the reader is familiar with PCI DSS (including relevant guidance publications); Card Brand Requirements, supplemental documents from the PCI Security Standards Council, such as the cloud and virtualization guideline documents[2]; and any specific guidance published by their acquiring bank or processor. The PCI DSS applies to all

[2] The Information Supplements: *PCI DSS Cloud Computing Guidelines (version 2.0, February 2013)* and the *PCI DSS Virtualization Guidelines (version 2.0, June 2011)* are available from the PCI Security Council at http://pcisecuritystandards.org.

organizations that store, process, or transmit cardholder data, regardless of volume. This includes merchants, service providers, payment gateways, data centers, and outsourced service providers.

Although this paper specifically addresses PCI compliance, the same basic principles can be applied when implementing systems that comply with other similar regulations, such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and so on.

Use of a PCI DSS compliant CSP does not result in PCI DSS compliance for the client. The client must still ensure they are using the service in a compliant manner, and is also ultimately responsible for the security of their CHD – outsourcing daily management of a subset of PCI DSS requirements does not remove the client's responsibly to ensure CHD is properly secured and that PCI DSS controls are met.

For additional considerations associated with virtualization and cloud computing see the following PCI Security Council Information Supplements:

"PCI DSS Virtualization Guidelines" and "PCI DSS Cloud Computing Guidelines"

PCI, Virtualization and the "Cloud"

The PCI Data Security Standard requires compliance of applications that process cardholder data when those applications are resident in a merchant's Cardholder Data Environment (CDE). The CDE includes all systems and devices 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 store, transmit or process cardholder data from those that do not. This method removes systems that are unrelated to payment card processing from PCI DSS scope.

The introduction of virtualization and cloud computing into cardholder environments can blur the lines of segmentation. This is especially true when hosting both virtual systems that handle cardholder data and those that do not, on the same virtualized platform. However, with attention to the additional risk factors, virtualized environments, including cloud solutions, can be implemented with full compliance, as acknowledged in version 3.0 of the PCI-DSS and the PCI DSS Cloud Computing Guidelines.

When implementing the CDE using virtualization or cloud technologies there are additional risk factors that must be considered and addressed. As noted in the Cloud Computing Guidelines, this is especially true when outsourcing the CDE to a cloud service provider (CSP) for hosting.

This paper does not attempt to address all of the concerns of working within AWS, or any CSP, which are clearly covered in the Guidelines document.

When deploying in AWS or other CSP, 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 AWS while also working with a credit card services provider that is hosted by AWS. The existence of multiple nested relationships – for example where there is a chain of vendors and/or other providers required to delivery of a cloud service – will add complexity to both the service providers and the merchant's PCI DSS assessment process. Coalfire recommends the tools available in the PCI Cloud Guidelines and/or provided by AWS[3] are used to clarify shared responsibilities; while specific questions should be addressed to the client's QSA.

Overview of the Vormetric Data Security Platform

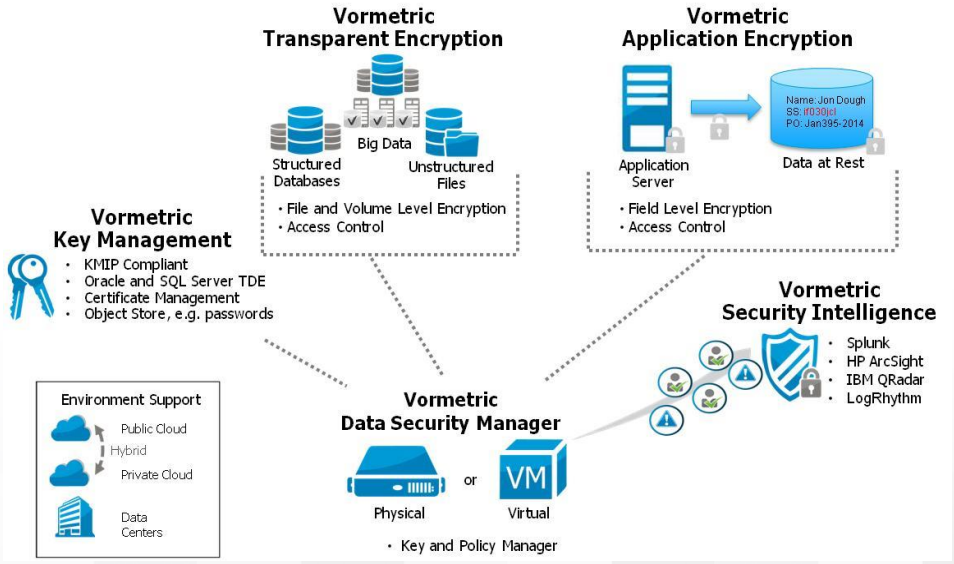

Figure 1: Vormetric Data Security Platform

[3] AWS PCI DSS Level 1 FAQs: http://aws.amazon.com/compliance/pci-dss-level-1-faqs/

This platform is a comprehensive and extensible platform for delivering data-centric security across traditional physical servers, virtual and cloud environments. It offers centralized policy management and data-centric security for a broad range of solutions. A key capability of this platform is Vormetric Transparent Encryption, which uses a software agent that protects structured databases, unstructured data and Big Data through fine-grained access controls, standards-based strong encryption and delivers access visibility through security intelligence logs. The platform also supports standard-based Key Management Interoperability Protocol (KMIP), Transparent Database Encryption (TDE) key management, secure storage for any object, and certificate management.

Vormetric puts control in the merchant's hands by encrypting the cardholder data and controlling which users and applications can access and view that data. However, the operations environment isn't altered as AWS and your own administrators can continue to manage the cloud environment without changing existing processes, architecture or applications.

The merchant is always the custodian of policies and keys – The Data Security Manager (DSM) can be deployed on the customer premise or in AWS. In either deployment, the cloud provider never has access to the Enterprise's keys and policies.

Vormetric Data Security Platform Components and Associated PCI Scope

The two products leveraged in this PCI solution are the Vormetric Data Security Manager (DSM) and Vormetric Transparent Encryption (VTE). VTE protects virtual servers in the CDE (cardholder data environment) and is managed by the DSM. These components can be deployed in a CDE and meet the applicable requirements of the PCI DSS. The capabilities of the Vormetric solution can assist in satisfying PCI DSS requirements as outlined in the Control and Support Matrix of this document.

Data Security Manager

The Vormetric Data Security Manager integrates key management, data security policy management, and audit log collection. This enables data security administrators to easily manage standards-based encryption across Linux, UNIX, and Windows operating systems in both centralized and geographically distributed environments, including in AWS.

Clustering DSMs provides high availability and scalability to tens-of-thousands of protected servers running across many different operating systems in both centralized and geographically distributed physical, virtual and cloud environments.

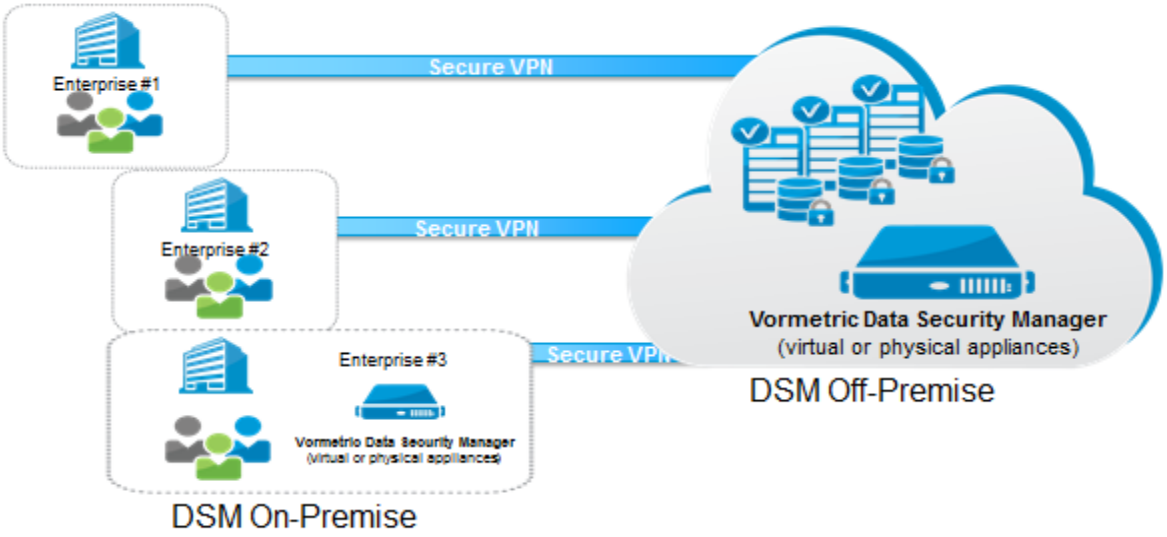

Figure 2: The Vormetric Data Security Manager can be deployed either on-premise or in AWS

The DSM deployment is flexible because it is available as a physical or virtual appliance. The virtual appliance can be deployed on premise or in the cloud. Either deployment model can meet PCI DSS standards. It's important to note that the DSM is the key and policy manager and cardholder/sensitive data is never passed through it. The DSM is available in the following form factors:

- A hardware appliance, 2U rack-mountable, with FIPS 140-2 Level 2 certification
- A hardware appliance, 2U rack-mountable, 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 from a secure web-management console, CLI or through APIs.

Vormetric Transparent Encryption

Vormetric Transparent Encryption (VTE) requires file system agents that are installed above the file system logical volume layers. These agents evaluate any attempt to access the 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 so IT administrators can perform their jobs without directly accessing the information. The agents perform the encryption, decryption, access control, and logging.

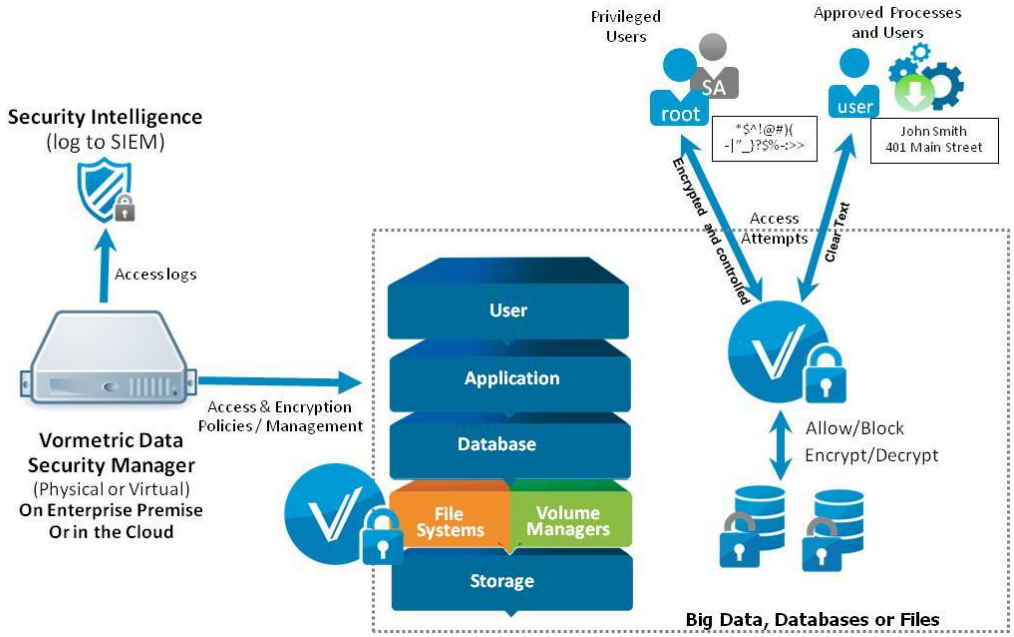

Figure 3: Vormetric enforcing least privilege policies to privileged users

Vormetric 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.

Applicability of the PCI DSS to the Vormetric Data Security Platform

As with any specific solution, there are a specific set of PCI DSS requirements that apply directly to Vormetric. Many of the requirements, such as conducting background checks on employees or implementing secure coding standards for web applications, are non-applicable. Others might apply indirectly, like the requirement to limit ports and protocols to those that are necessary, which would include those ports and protocols necessary to interface between the Vormetric file system agents running on the virtual machines in AWS and the Vormetric Data Security Manager appliance located at the client's site. Some indirect requirements may even be applicable only in certain architectures or implementations; however, certain requirements of the DSS will apply directly to the Vormetric solution regardless of how it's implemented.

At a minimum, a clear understanding of where cardholder data is stored within AWS, and other facilities, is essential for appropriate installation of Vormetric agents and for administering encryption key and access control policies to restrict access to decrypted cardholder data based upon business-need-to-know.

The PCI DSS is broken into twelve high level requirements, each of which contains multiple sub-requirements and defined testing procedures for compliance. Below is a high level alignment of applicability to the standard. A more detailed treatment can be found in the Appendix at the end of this document.

Build and Maintain a Secure Network

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

While Vormetric must be deployed in accordance with this requirement; there are no specific tenets that apply directly to the Vormetric solution. The PCI requirement for a firewall is typically met by ensuring that all Vormetric Data Security Platform components, as with other application servers, are placed behind a firewall. Placing the system hosting the application servers behind a firewall is standard for N-tier architectures.

For multi-tenant environments, where each customer environment, as well as the hosting infrastructure, is considered untrusted by the others, or meeting requirement 1.1.3 for a firewall between the DMZ and the "internal network zone," this may not be adequate. However, implementation of strong encryption, key-management, and access control capabilities, may potentially allow for shared infrastructure components to be removed from scope for PCI DSS consideration.

Ultimately, the adequacy of any segmentation, and therefore its ability to support compliance with the PCI DSS, relies on the validation of its effectiveness through review and as part of the internal penetration testing.

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

While Vormetric must be deployed in accordance with this requirement; there are no specific tenets that apply directly. The Vormetric Data Security Platform components do not install with vendor-supplied default password and all security parameters are defined during installation. Where software components of the Vormetric Data Security Platform are implemented in a CDE, the user should confirm that it is being installed on servers/systems that are secure and hardened operating systems as required in PCI DSS Requirement 2.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Vormetric directly supports the tenets of this requirement. PCI compliant data encryption and key management functionality are provided by the solution. Vormetric defined encryption at the file or volume level; encrypts cardholder data using industry accepted encryption keys; keys are stored independently from the data; and key custodians are granted access to perform key management activities but do 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, and there are no applicable elements of requirement four that apply either directly or indirectly to the Vormetric solution.

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 anti-virus management solution and there are no applicable elements of requirement five that apply directly or indirectly to the Vormetric solution.

Requirement 6: Develop and maintain secure systems and applications

Vormetric is independent of the cardholder data systems and applications. 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.

Implement Strong Access Control Measures

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

Requirement 7 applies directly to the capabilities of the Vormetric solution in that it enforces access control rules to deliver least privileged access and denies access to protected PAN and other sensitive information to unauthorized users and applications. Systems and Database Administrators, and other privileged users, who have access to the data to perform necessary maintenance/administration activities, are not granted permission to decrypt or access the data.

Procedures for requesting and administering access to encryption keys and decryption activities must be developed to ensure that access is granted based upon job-related requirements (7.2).

In virtualized and cloud implementations of Vormetric, access to the cardholder data is managed by the user in the same manner as in a non-virtualized or internally hosted implementation of Vormetric Data Security Platform. Users retain control of the sensitive information independent of the implementation strategy.

Requirement 8: Identify and authenticate access to systems components

Vormetric is independent of the system and network account and password controls required. Vormetric uses the in-place directory service (e.g. LDAP, Active Directory) to authenticate user IDs. Features in the Vormetric solution can be used to:

- Encrypt credentials stored in application files/databases (8.2.1) should custom build authentication systems be in place.
- Provides programmatic access control to all users with direct access to the database, including administrators and application accounts (8.7)

Requirement 9: Restrict physical access to cardholder data

Physical installation of Vormetric components and the controls around physical protection of media must comply with the DSS, but there are no directly applicable elements to the Vormetric solution. The solution can supplement controls requiring hard drives to be securely wiped prior to disposal or reuse. Encrypted data on such hard drives will be practically impossible to recover without the appropriate access and authorization to the Vormetric Data Security Manager.

Regularly Monitor and Test Networks

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

Vormetric provides logging of access at the File Systems level. All read/write requests to sensitive data is tracked with PCI compliant audit records. User controlled policies allow for monitoring of all access to sensitive data, including access by privileged users. Reporting tools provide the ability to analyze logs generated by the agents and DSM. In addition policy can be set in the DSM to send alerts associated with activities that require special monitoring.

Vormetric audit logs can be stored in the DSM or in an organization's System Information and Event Management (SIEM) system or other log collection solutions.

Requirement 11: Regularly test security systems and processes

While Vormetric does not directly apply to specific tenets of this requirement, applicable scanning and testing requirements could apply to components of the Vormetric solution running in the CDE. Additionally, while not a file integrity management tool (11.5), Vormetric's logging and reporting capabilities can supplement monitoring activities over access to files and volumes containing cardholder data.

Maintain an Information Security Policy

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

Vormetric must be covered by and 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 the Vormetric solution.

Conclusion

While there are additional scoping concerns and risks associated with virtualization and cloud computing, when using AWS or other cloud service provider. It is possible to implement a PCI DSS compliant solution for the encrypting cardholder data and allowing privileged account access to cardholder data files/volumes while prohibiting access to the decrypted information; thus eliminating risk of exposure of sensitive data from privileged users and from common hacker tools that exploit privileged user accounts .

The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of the Vormetric Data Security Platform in the clients CDE and the context in which it is implemented.

Vormetric not only supports the implementation of PCI DSS control requirements; it includes features which can facilitate the users desire to mitigate the risks of implementing their CDE in AWS or other CSP.

References & Resources

1. Cloud Special Interest Group, PCI Security Standards Council. (2013). *Information Supplement: PCI DSS Cloud Computing Guidelines*.
2. Virtualization Special Interest Group, PCI Security Standards Council. (2011). *Information Supplement: PCI DSS Virtualization Guidelines*.
3. AWS PCI DSS Level 1 FAQs: AWS website
4. Amazon Web Services: Risk and Compliance (November 2013)

Appendix: Vormetric Controls and Support Matrix

The following table provides additional details on the specific requirements which must either be met by Vormetric Data Security Platform or which Vormetric features provide support to assist in deploying a PCI compliant environment. The table only lists those requirements that were considered either applicable or supported, and not the entire PCI DSS. Unlisted controls were determined to be inapplicable to Vormetric, specifically, though they may apply to the broader design and management of a cardholder data environment, which includes the implementation of Vormetric Data Security Platform. Merchants, credit card services providers and any other entities covered by the requirements of the PCI DSS should always consult with their own PCI Qualified Security Assessor (QSA) to determine the scope of controls applicable to them.

Table 1: Applicability of PCI DSS 3.0 Controls to Vormetric Security Platform

DSS REQ.	REQUIREMENT DESCRIPTION	COMMENT/EXPLANATION
Requirement 1: *Install and maintain a firewall configuration to protect cardholder data*		
No applicable requirements. If Vormetric is implemented as part of a cardholder data environment, the user should ensure that it is deployed in a network environment that PCI DSS v3 compliant. Whether the Vormetric DSM is implemented in the AWS managed network or in the user-managed network, the network must be compliant with the requirements outlined in PCI DSS Requirement 1. However, the controls surrounding the network and deployment of 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 is implemented as part of a cardholder data environment (CDE), the user should ensure that it is deployed in an environment that PCI DSS v3 compliant. The Vormetric Data Security Manager is a pre-configured and uses a hardened Linux operating system. Where software components of the Vormetric Data Security Platform are implemented in a CDE, the user should confirm that it is being installed on servers/systems that are secure and hardened operating systems as required in PCI DSS Requirement 2. The Vormetric components will not allow implementation with default or weak passwords.		
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.*	Vormetric supports secure storage of sensitive authentication data (SAD) as required by 3.2, for those issuers or others that must store SAD, by using strong cryptography with associated key management for encrypting files or volumes where SAD reside. Vormetric's ability to encrypt structured and unstructured data means that it can protect the data whether it is in flat files or in databases.

		While issues and companies supporting issues, may have a legitimate business need for storing data, merchants, service providers supporting merchants, and acquirers must never store sensitive authentication after the payment transactions authorization is processed.
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 protecting stored data by using strong cryptography with associated key- management for encrypting files or volumes where 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 supports volume level encryption that expands encryption beyond a single file or a database column. Vormetric manages access to the encrypted data independent from the systems operating systems access control. While integrated in the users LDAP or Active Directory for authentication access to decrypted data is based upon rules managed and administered within the Vormetric Data Security Manager. Cryptographic keys are not tied to user accounts, but are contained within the Vormetric system. Vormetric performs the encryption/decryption functions, as opposed to granting authorized and authenticated users access to the key.
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	While the user will need to document key managements procedures, Vormetric supports 3.5, by ensuring that encryption keys are securely stored. Vormetric directly supports 3.5.1 by ensuring cryptographic keys are centrally generated and stored by the Data Security Manager. The actual keys are never visible to anyone, including key custodians or systems administrators.

	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	Vormetric restricts access to keys and key management activities by managing access within the Vormetric Data Security Manager, which decouples access rights from central access managements systems such as Active Directory, thus restricting access by privileged users such as system administrators and root unless explicitly granted within Vormetric's Data Security Manager. 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 Data Security Manager (DSM), which is separate from the location where the data encryption key is used. If the option to cache data encryption keys on the local server is selected, in order to eliminate network latency, the local keys are also encrypted with an AES 256-bit key. Vormetric also offers an HSM option, satisfying 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	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 of the technical requirements associated 3.6. The Vormetric's Data Security Manager (DSM) architecture is designed for strong crypto-key management using a secure web management console providing 3.6 compliance for: **3.6.1** Cryptographic keys are centrally generated by the Data Security Manager 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 Secure cryptographic key storage	**3.6.3** Providing a secure central repository for cryptographic keys and policies. Customers have the option 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, the keys are protected with a wrapper key and are not assessable by any systems user
	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 3.6.6defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4** Crypto-key can changed by key custodians based upon the organization's crypto-period policies. When a key is retired 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.
	3.6.5 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.	**3.6.5** Crypto-key can changed by key custodians when 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 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control	**3.6.6** Manual clear-text cryptographic key management is not required by Vormetric. Custodians can create keys, but key values are not visible to the custodian. DSM protects keys from any one person having access to key material by following a "no knowledge" and configurable split knowledge/dual control policies.
	3.6.7 Prevention of unauthorized substitution of cryptographic keys	**3.6.7** Access control policies defined within the DSM control access to key creation and other key management activities, restricting access to authorized key custodians only. The Data Security Manager 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 the Data Security Manager archive into a new or replacement Data Security Manager.
Requirement 4: *Encrypt transmission of cardholder data across open, public networks*		
No applicable requirements. However the data transmission controls surrounding the payment transaction and other cardholder data transmission controls are entirely dependent upon the user's architecture and are outside of the scope of the paper.		
Requirement 5: *Protect all systems against malware and regularly update anti-virus software or programs*		
The Vormetric 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 compliant cardholder data environment. However, the encrypted cardholder data could be stored on systems that require anti-virus and the Vormetric user 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 is independent of the cardholder data systems and applications. 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.		
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 directly supports 7.1 by adding a layer of access control on top of the native operating system access control. It also can harden the access control defined at the OS layer and prevent root administrators and privileged users from accessing or viewing cardholder data. The solution enables least privileges 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, administrators can identify the files that require backup without providing them 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 ensure privileged users, such as Administrator or Root, are granted access needed for their job responsibilities but restricted from accessing cardholder data unless explicated granted to meet a business need, thereby restricting access based on "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 the cardholder data based on their 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 the user will need to implemented processes for approving requests for access, Vormetric supports 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. With an organization's documented approval process Vormetric policies can be configured to include 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 documented process for granting access to cardholder data is enforced.
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 directly supports 7.2 by setting access control policies that define through policies that authorize users and applications granted access to cardholder data storage on any server or storage device. Only users and applications that are part of authorized policies can access the data in clear text. (Administrators can be given access to the files containing cardholder data, but data is not decrypted for them.). Default policy is to "deny all" without explicit authorization through policies.

Requirement 8: *Identify and authenticate access to systems 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 is independent of the system and network account and password controls required. Vormetric integrates with existing directory service (LDAP, 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 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, an operating system super- user can have a policy preventing file copies and the ability 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 data not be adequately cleaned from media, the data will not be viewable unless the Vormetric Data Security Manager 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 a detailed logging at the File System level. Any read/write and other access requests for sensitive data can be audited and the audit records contain information to track access back to a host machine, directory, file or resource accessed, specific user, user group, policy invoked, application and time.
10.2.	Implement automated audit trails for all system components to reconstruct the following events:	Vormetric provides a detailed auditing at the File System level. Any read/write or other request for sensitive data can be audited and the trails

	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 **10.2.7** Creation and deletion of system-level objects	contain information to track access back to a specific user, application and time, including: - Policies can be constructed to monitor individual access to cardholder data. (10.2.1) - By constructing policies to monitor individual access to cardholder data individuals with root or administrative privileges is logged. Policies can also prevent privileged users from accessing data in the clear without interfering with their ability to perform their day-to-day administrative duties. Both failed and successful attempts to view card data are logged. (10.2.2) - By enabling administrators of the Data Security Manager that are assigned the role of "audit officer" to access audit trails, which are centrally stored. Vormetric recommends that audit/log data be sent to a centralized log server safeguarded by Vormetric. All access and access attempts to Vormetric logs are audited. (10.2.3) - Through configuration to audit all denied access requests. (10.2.4) - By logging 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 a detailed auditing at the File System level, by generating audit entries that include: - Username 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,	The DSM can be configured to synchronize with an NTP server.

	and storing time. - Critical systems have the correct and consistent time	
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 Vormetric Data Security Manager. 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 safe-guarded with the Vormetric solution. - Ensuring log files cannot be modified while they reside on the Vormetric Data Security Manager. Further, customers may use the Vormetric solution to block or monitor changes to log files and other audit trails.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	Vormetric Security Platform generates log reports for monitoring of daily activity.
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.	Vormetric, while not file integrity management software that can be used to alert changes to all operating system and execution files, Vormetric generates audit information for unintended direct access to cardholder data and can be configured to generate alerts thus providing integrity monitoring for cardholder data under its control.
Requirement 12: *Maintain a policy that addresses information security for all personnel*		
No applicable requirements. Along with the rest of the cardholder data environment, a Vormetric deployment must be covered by and 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 1300 customers, including 17 of the Fortune 25 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.

About Coalfire

Coalfire is a leading independent information technology Governance, Risk and Compliance firm that provides IT audit, risk assessment and compliance management solutions. Coalfire has offices in Dallas, Denver, Los Angeles, New York Seattle and Washington, D.C. and completes thousands of projects annually in the retail, financial services, healthcare, government, and utilities industry sectors. Coalfire offers a new generation of cloud-based IT GRC tools under the Navis™ brand that are used to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire's solutions are adapted to requirements under the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley FISMA, and emerging data privacy legislation. Coalfire is a Qualified Security Assessor (QSA) and Payment Application QSA (PA-QSA) firm, and is also a HITRUST CSF Assessor firm. For more information, please visit www.coalfire.com.

Acknowledgments

Coalfire would like to acknowledge Charles Goldberg and Mike Yoder from Vormetric for their support and contributions to this document.