Vormetric Data Security for PCI DSS 3.0 Compliance

Payment Card Industry Data Security Standards (PCI DSS) mandate that all organizations that accept, acquire, transmit, process, and/or store cardholder data must take appropriate steps to continuously safeguard all sensitive customer information. PCI DSS has improved the protection of cardholder information, but it can be challenging to gain compliance. Achieving and maintaining compliance can pose a number of significant challenges to enterprise risk managers, information security personnel, and IT operations professionals. To add to the challenge, the PCI DSS version 3.0 became effective on January 1, 2014, although, existing PCI DSS 2.0 compliant vendors have until January 1, 2015 to move to the new standard.

PCI DSS Compliance Challenges

Banks, payment processors, and merchants all rely on increasingly complex, geographically distributed networks, typically containing both structured and unstructured data. Cardholder information may be stored in a variety of different databases and versions, as well as in file server files, documents, images, voice recordings, access logs, and a broad range of other data repositories.

Safeguarding cardholder data in such a wide variety of assets and locations, in a manner compliant with PCI DSS, requires diligent administration and close cooperation between the enterprise's IT teams and the many business units that need access to the data. Finding the right balance between protecting cardholder information, avoiding any disruptions to IT infrastructure, and ensuring uninterrupted access to the information that flows through and across these networks is vital to the security and ongoing operation of the business.

In order to comply with PCI DSS regulations, IT organizations need the ability to manage access control, encryption, key management, and auditing of cardholder data at rest. Attempting to fulfill these requirements with a piecemeal solution would be complicated to operate and costly to implement.

Organizations collecting cardholder information need a comprehensive data security solution that:

- Cost effectively achieve and maintain PCI 3.0 compliance
- Support major SIEM and log collection solutions
- Don't require re-engineering of applications or databases
- Provides strong separation of duties for managing policies
- Maintains a high level of system performance, with no impact to end user processes and doesn't compromise service level agreements (SLA)
- Maintains compliance in cloud and big data environments

Vormetric Meets a Breadth of PCI DSS 3.0 Requirements

The Vormetric Data Security Platform provides data protection products to secure and control enterprise data at rest. Vormetric Transparent Encryption combines encryption, access control, key management and granular logging to protect unstructured files and structured databases on Linux, UNIX, and Windows servers in physical, virtual, cloud and big data environments to meet the requirements outlined in the compliance matrix on the reverse of this brief.

Vormetric Key Features and Benefits:

- Helps address numerous controls in Requirements 3, 7, 8 and 10
- The solution supports Linux, UNIX, Windows servers in physical, virtual, cloud and big data Cardholder Data Environments (CDE)
- Cardholder Data is encrypted, access is controlled and logged
- High performance encryption and high-availability design maintains SLAs
- Quick implementation and easy expansion across CDE helps meet audit deadlines

"Vormetric Data Security is quick and easy to administer, while having negligible impact on performance. It's the perfect solution for meeting PCI DSS requirements."

Daryl Belfry, Director of IT, TAB Bank

PCI DSS Requirement	Compliance Challenges	Vormetric Data Security Solution
Requirement 3: Protect Stored cardholder Data Sub-requirements: 3.2, 3.4.1, 3.5.1, 3.5.2, 3.6	PCI DSS Requirement 3 mandates that all data should be rendered "unreadable – anywhere it is stored", and provides a number of methods how that might be achieved. PCI DSS recognizes the value of strong cryptography coupled with proper key management.	Vormetric Transparent Encryption protects cardholder data by encrypting it at the file/volume level and then by decrypting based on a pre-defined usage policy. This ensures that all data is rendered unreadable anywhere it is stored. Integrated key management makes the process seamless and meets these requirements.
Requirement 7: Restrict Access to Cardholder Data According to Business Need to Know Sub-requirements: 7.1, 7.2	PCI DSS Requirement 7 mandates that only users and resources that must access cardholder data in order to complete their job should have access to systems containing the data. In order to maximize the benefits realized from encryption, organizations are advised to identify a solution that enables the application of security policies on the data itself, as opposed to simply on the systems or applications that access the data. Encryption alone is insufficient to provide the granular control required by the PCI DSS. Encryption is only as strong as the associated key management and access controls.	In accordance with the PCI DSS, Vormetric enforces a least-privilege model, which denies any activity that has not been expressly permitted by policy. This ensures that only users, processes and resources that need access to files or file content have access to it and also has the additional benefit of being able to exclude privileged users (system administrator or root) within the environment from being able to access cardholder data.
Requirement 8: Identify and authenticate access to systems components Sub-requirements: 8.2.1, 8.7	PCI DSS Requirement 8 Assigns a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.	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. 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. - Provide access control to all users with direct access to the database, including administrators and application accounts (8.7)
Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data Sub-requirements: 10.1, 10.2, 10.3, 10.4.1, 10.5, 10.6	PCI DSS Requirement 10 states that all organizations must track and monitor all access to network resources and cardholder data by implementing audit trails on system components, administrators and users. It details out the audit trail entries.	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. It supports all the major syslog formats: RFC5424, CEF, and LEEF

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 1100 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 solution suite protects any file, any database and any application — anywhere it resides — with a high performance, market-leading data firewall that incorporates application transparent encryption, privileged user access controls, automation and security intelligence.

Vormetric Enables PCI DSS Compliance

TAB Bank

- **Business Need:** Encryption of data for banking cardholder information
- **Technology Need:** Protect a mixed environment containing structured and unstructured information.
- **Solution:** Vormetric Encryption for Windows and Linux servers.

RSIEH LLC (Rausch, Sturm, Israel, Enerson & Hornik)

- **Business Need:** Protect all documents containing cardholder information.
- **Technology Need:** Safeguard information used by credit collection application without application changes.
- **Solution:** Vormetric Encryption for Windows servers.

"Vormetric Data Security offered us an easier yet effective method to encrypt our SQL Server databases and comply with PCI DSS encryption and key management requirements."

Troy Larson, Vice President, Information Systems, MetaBank

Vormetric, Inc.
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
South Korea: +82.2.2190.3830
info@vormetric.com
www.vormetric.com