Vormetric Data Security Use Case Overview

A single, extensible solution that helps organizations to protect data, meet compliance requirements, and gain valuable security intelligence across physical, virtual, cloud and big data environments

As enterprises generate larger amounts of data, they face the growing challenge of protecting and controlling access to accumulated volumes and varieties of sensitive data. Sensitive data like customer information, intellectual property and financial data are extremely valuable commodities that are attractive targets requiring data-centric protection. Given permeable perimeters, sophisticated hackers and advanced persistent threats (APTs), enterprises need to reduce their attack surface by securing and controlling access to sensitive data.

Vormetric Data Security protects what matters is by essentially creating a "data firewall," implementing access policies with fine-grained controls, deploying advanced encryption, key management and vaulting technologies to lock down and change the state of the data, and continuously gathering security intelligence to identify any emerging issues in real-time. Vormetric provides transparent, strong, efficient data protection that is easy to deploy and manage; Vormetric avoids the need to modify applications or storage infrastructure and can be deployed across heterogeneous environments.

Compliance Mandates

Lawmakers and regulators around the world are enhancing existing compliance requirements, implementing new legal frameworks and defining new data security regulations. Vormetric Data Security provides the data protection functionality required to adhere to global compliance regimes.

- **Payment Card Industry Data Security Standard (PCI DSS) –** Vormetric Data Security helps enterprises comply with PCI DSS requirements 3, 7 and 10 that call for the protection of cardholder information. Vormetric Data Security secures cardholder data in databases as well as voice files, reports, and images.
- **HIPAA/HITECH** – Electronic Patient Health Information (ePHI) needs to be secured to maintain compliance with HIPAA/HITECH. Whether unstructured medical imagery or structured database information containing ePHI, Vormetric secures and controls access to ePHI.
- **State Data Breach Notification Laws** – US states have data breach notification laws modeled on California SB 1386 that provides a safe harbor in the event of a breach where the underlying data is encrypted. Vormetric Encryption provides safe harbor and helps businesses avoid the cost and brand damage that comes with breach notification.
- **National Data Protection Laws** – Nations around the globe are instituting data protection laws which mandate encrypting citizen personal information including UK Data Protection Act, EU Data Protection Directive and South Korea's Personal Information Protection Act. Vormetric Data Security secures personal information, be it structured (in databases) or unstructured.
- **Sarbanes-Oxley, GLBA, Basel III** – Vormetric Data Security provides security, access control and reporting so enterprises can demonstrate effective controls over sensitive information.
- **Data Across Borders Compliance** – As enterprises consolidate datacenters and need to ensure that data does not inappropriately cross borders. Vormetric enables them to segregate and control data to meet their legal obligations without modifying applications or storage infrastructure.

Data Protection

Vormetric Data Security provides a single platform that extends across the enterprise to provide data security and operational efficiency in a variety of use cases.

- **Database Security** – Vormetric Data Security protects databases with multiple approaches: Vormetric Encryption can encrypt and control access to databases in any environment – physical, virtual and cloud, while Vormetric Key Management stores and manages encryption keys for Transparent Data Encryption (TDE) for Microsoft SQL Server and Oracle.

Database Audit & Protection Challenges

"The growth in the number of databases and the inherent management complexity of multiple database platforms mean that it is no longer practical for IT leaders to utilize purely native database audit and security functionality."

"Native database security capabilities do not offer sufficient security protection in a rapidly escalating threat and regulatory environment."

"Native database audit and security functions do not inherently extend to other vendor databases. Therefore, enterprises face major problems trying to manage different native database security tools, and, with a lack of any universal functions, will create gaps in security."

Brian Lowans, Gartner, Inc.
"Apply the Nine Critical Capabilities of Database Audit and Protection" (March 2013)

- **SAP Data Protection** – SAP modules frequently contain sensitive information about customers or employees (compensation, health information, etc). Vormetric enables enterprises to meet requirements to secure and control access to such information without modifying SAP or the underlying database.
- **Unstructured Data Security** – Vormetric Encryption enables enterprises to meet requirements to secure and control access to unstructured data (pdf files, CAD diagrams, voice recordings) across a variety of storage environments including NAS, SAN, DAS, and cloud storage.
- **Privileged User Control** – Vormetric Data Security reduces the enterprise risk profile by controlling privileged system users such as root or system administrators, allowing them to do their jobs without having access to protected information.
- **Commercial Off the Shelf Application Data (Documentum, Peoplesoft, Sharepoint, etc) –** Vormetric Encryption encrypts and controls access to data for commercial-off-the-shelf applications so that enterprises can meet security obligations without disrupting operations.
- **Intellectual Property Protection** – Compromised intellectual property can have catastrophic business consequences. Vormetric encrypts and controls access to intellectual property, from design diagrams to databases to reduce the enterprise risk profile.
- **Data Segregation –** Vormetric Data Security enables enterprises and governments to meet data governance mandates by segregating data repositories so that departments or entities can only see data they own and not adjacent data.
- **Outsourcing & Contractual Obligations** – Service providers handling sensitive data frequently have to demonstrate that client data is protected. Vormetric Data Security encrypts, controls access, and reports on access to meet contractual obligations.
- **Legacy Application Encryption** – Home-grown applications face new requirements for data security, but cannot be modified without incurring significant costs. Vormetric Data Security meets security requirements by transparently protecting and controlling access to such sensitive information without requiring application changes.
- **Facilitating Repair & Disposal of Storage Hardware** – Disposing of servers and storage containing sensitive data can be a costly exercise for many enterprises. Vormetric Data Security enables enterprises to cryptographically shred information and avoid expensive equipment disposal costs.
- **Mitigating Advanced Persistent Threat (APT) Risk** – Vormetric Data Security reduces the attack surface by protecting data and controlling access to data targeted by APTs and helps provide security intelligence by communicating unauthorized access attempts and unusual access patterns.
- **Application Encryption** – Vormetric Key Management enables custom applications to take advantage of cryptographic services to secure application data and meet enterprise security requirements.
- **Certificate Management** – Expired SSL certificates can result in downed applications and lost revenues. Vormetric Vault enables enterprises to store, report and alert on certificates and other security materials to maintain application uptime and minimize SSL management costs.

About 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 enterprise customers and government agencies protect what matters — their sensitive data — from both internal and external threats. In a world of Advanced Persistent Threats (APTs), Vormetric's market-leading privileged user access controls and security intelligence are invaluable. The company's scalable solution suite protects any file, any database and any application — anywhere it resides — while maintaining application performance and avoiding key management complexity. Many of the world's largest and most security-conscious organizations and government agencies, including 17 of the Fortune 25, have standardized on Vormetric to protect their sensitive data and provide them with advanced security intelligence.

Core Technologies

Vormetric Data Security can be deployed to address a variety of data protection use cases. The Vormetric Data Security platform provides common management and implementation to with the following capabilities

Data Firewall – The combination of strong encryption, fine-grained access controls and the security intelligence information provided by Vormetric Data Security solutions results in a "virtual" firewall the protects critical data wherever it resides - in physical, virtual and cloud environments.

Granular Access Controls – Detailed control of access control policies for encrypted data by users and processes reduce advanced persistent threats (APTs), as well as preventing root or administrative access – allowing organizations to both meet exacting compliance requirements and to further protect critical information wherever it resides.

Encryption and Key Management – Encryption and management of both structured data (in databases), and unstructured data (in volumes and file systems) across distributed environments – traditional data centers, virtual environments, big data implementations and cloud deployments. Vormetric is transparent to applications, simple and straight-forward to implement, rolls-out quickly and requires minimal management overhead. Vormetric also supports heterogeneous environments with key management for Transparent Data Encryption (TDE) for Oracle and SQL Server databases.

Security Intelligence – Security Information and Event Management (SIEM) compatible log formats capture all access to data and to the Vormetric Data Security environment, providing high value, real-time security intelligence to identify compromised accounts and malicious insiders as well as to find access patterns by processes and users that may represent a threat.

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