Vormetric Data Security Public Sector Use Case Overview

A single, extensible solution that helps public sector organizations to protect critical data, meet compliance and cybersecurity requirements while gaining security intelligence across physical, virtual, cloud and big data environments

As public sector organizations 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 such as citizen information, state secrets, intellectual property and financial data are extremely valuable commodities that are attractive targets requiring data-centric protection. Given permeable perimeter security, sophisticated hackers and advanced persistent threats (APTs), public sector organizations need to reduce their attack surface by securing and controlling access to sensitive data.

Vormetric Data Security protects what matters 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 gather security intelligence to identify any emerging issues in real-time. Vormetric provides data root of trust, allowing only authorized parties can access the data and allowing that trust to be selectively extended to internal and external parties across government infrastructure and cloud infrastructure. Vormetric provides transparent, strong, efficient data protection that is easy to deploy and manage; the Vormetric platform is rapidly deployed because it avoids costly time investments in modifying applications or storage infrastructure. This enables an immediate protection to an environment that can be realized in a matter of weeks across a wide variety of operating systems and storage platforms.

Data Protection

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

- **Big Data and Cross Domain Data Segregation –** Mixing big data repositories for analytics while maintaining security of the underlying data can pose data security challenges. Vormetric can transparently secure and control access to structured and unstructured big data repositories with exceptional performance, enabling data segregation across domains.
- **Data Consolidation Initiatives** – Vormetric Data Security enables governments to merge servers and data repositories across networks (unclassified/classified) to drive further savings in data center consolidation (FDDCI). By using the Vormetric platform organizations can be assured that data is visible and accessible based on credentials.
- **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
- **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 can also store and manage encryption keys for Transparent Data Encryption (TDE) keys from Microsoft SQL Server and Oracle.
- **Unstructured Data Security** – Unlike standard disk encryption that only secures the physical drive, Vormetric Encryption enables public sector organizations to meet requirements to secure, and control access to un-structured 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 government 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. Further ensuring a lower risk profile from government employees, contractors, and outside threats.

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)

Advanced Persistent Threat Challenges

"100% of all data breaches involved stolen credentials."

Mandiant Report (February 2013)
Source: mandiant.com/threatlandscape

- **Commercial/Government Off the Shelf Application Data (SAP, Documentum, Peoplesoft, Sharepoint, etc)** – Vormetric Encryption encrypts and controls access to data for COTS/GOTS applications with a unified platform so that public sector organizations can meet security obligations without disrupting operations.
- **Federal Contractors and Outsourcing** – Systems integrators and contractors handling sensitive data frequently have to demonstrate that sensitive data is protected. Vormetric Data Security encrypts, controls access, and reports on access to meet contractual obligations. This can create a stronger and more secure implementation to meet FOCI and SSA requirements of organizations working with the US government.
- **Crypto-shredding** – Disposing of servers and storage containing sensitive data can be a costly exercise for many public sector organizations. Vormetric Data Security enables public sector organizations to cryptographically shred information, enabling repurposing of storage while avoiding expensive equipment disposal costs. The ability to crypto-shred keys can ensure that forward deployed assets are not accessible if compromised. If they are secured, data can be rapidly and securely be regained with appropriate credentials.
- **Certificate Management** – Expired SSL certificates can cause a disruption in the continuity of operations. Vormetric Vault enables public sector organizations to store, report and alert on certificates and other security materials to maintain application uptime and minimize SSL management costs.

Compliance Mandates and Security Directives

Enhanced compliance requirements, implement new legal frameworks and new data security regulations pose an ongoing challenge to public sector organizations. Vormetric Data Security provides the data protection functionality required to adhere to a variety of 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 ensures citizen information and government credit card data in databases as well as voice files, reports, and images are secured.
- **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** – in addition to US Federal actions under the Presidential Executive Order for CyberSecurity, nations around the globe are instituting data protection laws which mandate encrypting citizen data. This includes the UK Data Protection Act, EU Data Protection Directive and South Korea's Personal Information Protection Act. Vormetric Data Security provides a significant contribution to the meeting of these standards, and initiatives for both structured and unstructured data.

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 straightforward 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