KEY MANAGEMENT

SIMPLIFY IT OPERATIONS, SECURE AND CONTROL ACCESS TO DATA ACROSS THE ENTERPRISE

Controlling and maintaining encryption keys is an essential part of any enterprise encryption and key management strategy. Silos of encryption without centralized key management can become a security administrator’s nightmare, consuming time, budgets and putting data at risk of accidental compromise.

Our increasingly interconnected online world has been the most significant driving force in the evolution of key management systems. The connection of public and private sources has provided much easier access to the organization’s network and data to those who need it – notably employees, customers, prospects, and partners. But it has also opened the door to intentional or accidental misuse by hackers or even malicious internal users. These attacks can have dire consequences for the enterprises under siege, resulting in substantial loss of revenue, massive fines, and degraded customer trust.

Most IT organizations have gradually adopted disparate systems with different ways of managing encryption keys over many years. It may be a security breach event, the burden of managing disparate encryption systems, the trauma of a lost encryption key that renders data inaccessible, or an industry compliance regulation that forces them to turn to key management as a requirement for improving data security.

Without a centralized system of encryption key management, security administrators are faced with a costly, inefficient, and often impossible task. A typical enterprise has accumulated many different databases over time from separate vendors. This heterogeneous world means that an enterprise looking to secure databases, such as Oracle and SQL Server with native Transparent Data Encryption (TDE), has to factor in the increased costs and administrative resources required for managing multiple, incompatible encryption solutions. In addition, each separate encryption system requires specialized training to learn the unique processes that are specific to that system.

VORMETRIC KEY MANAGEMENT

Vormetric Key Management provides a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise. It simplifies the management and administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.

KEY ATTRIBUTES VORMETRIC KEY MANAGEMENT

- **Simplify key management** — Consolidate enterprise encryption key management and certificate storage solutions
- **FIPS 140-2 certified** — The Vormetric Data Security Manager is a Hardware Security Module (HSM) and is available with Level 2 and Level 3 certification
- **Reduce downtime** — High availability and proactive notifications of certificate and encryption key expiration reduces application and user downtime
- **Centralize reporting** — Generate consolidated reports for compliance and simplified auditing of encryption key and certificate usage
- **Standard API Support** — Leverage OASIS PKCS#11 and KMIP APIs for programmatic encryption key management and bulk key vaulting
- **Multitenant operations** — Role-based administration for compartmentalized management of data security policies, data encryption keys, and audit logs
- **Transparent Database Encryption (TDE)** — Consolidate encryption key management for Oracle and Microsoft SQL Server
Vormetric Key Management enables organizations to:

**Improve Operational Efficiency** by ensuring that keys are stored securely and always available to authorized encryption services. It also provides the ability to audit and report on all activities relating to keys including key generation, rotation, destruction, key import, and key export.

**Reduce Management Burdens** with Centralized Key Management. VKM simplifies the process of managing cryptographic keys, enabling security teams to gradually consolidate the management of encryption across the enterprise. Centralized key management in a solution conforming to FIPS 140-2.

**Cut Costs with a Unified Solution** by managing heterogeneous encryption keys, including keys generated by Vormetric Encryption, IBM Infosphere Guardium Data Encryption, Oracle TDE, Microsoft SQL Server TDE, and other applications with integrated encryption.

Vormetric Key Management is part of the Vormetric Data Security family of offerings. VKM manages third-party encryption keys, while Vormetric Encryption combines server encryption for data-at-rest with integrated key management. Both Vormetric Key Management and Vormetric Encryption share common management and system infrastructure.

### ELEMENTS OF THE VORMETRIC KEY MANAGEMENT SOLUTION:

- **Vormetric Data Security Manager (DSM)** — a network Hardware Security Module (HSM) appliance that provides centralized key and policy management. It features an intuitive Web-based management console for enterprise-wide administration, policy management and audit of encryption keys. The Vormetric DSM conforms to FIPS 140-2 and provides common management for both Vormetric Key Management and Vormetric Encryption.

- **Vormetric Key Agents** — integrate with Oracle TDE and Microsoft SQL Server TDE and communicate with the Vormetric Data Security Manager to provide lifecycle management for Oracle TDE Master Encryption Keys and Microsoft SQL Server database encryption keys.

- **Vormetric Key Vault** — provides high availability storage and backup of symmetric and asymmetric encryption keys of any strength, and tracks expiration dates. Key Vault is an option available with the Vormetric Data Security Manager.

### ABOUT VORMETRIC

A leader in data security solutions, Vormetric (@Vormetric) protects data-at-rest in physical, virtual, big data and cloud environments. Trusted by businesses and governments for over a decade, the Vormetric Data Security Platform secures the data of more than 1,500 global enterprises—including 17 of the Fortune 30. With Vormetric, a single infrastructure and management environment protects data wherever it resides with file, volume and cloud storage encryption, tokenization with dynamic data masking, field-level application encryption, sophisticated access control policies, third party and integrated encryption key management. For more information, please visit: www.vormetric.com.