Vormetric Encryption Architecture Overview

Protecting Enterprise Data at Rest with Encryption, Access Controls and Auditing

Vormetric, Inc.
888.267.3732
sales@vormetric.com
www.vormetric.com

Abstract

Data security threats and related incidents, such as breaches, can be harmful to any organization. Private and confidential information is sought after for profit, business advantage, malicious use, and both industrial and government espionage. Data breaches can negatively impact organizations in a variety of ways including increased costs, loss of brand reputation and revenue, inability to conduct business, and/or loss of 'secrets.' In order to protect private and confidential information, security teams are increasingly using encryption to significantly improve their defense-in-depth controls around these data assets and comply with regulations such as PCI DSS, HITECH Act, UK Data Protection Act, South Korea's Personal Information Protection Act (PIPA), and more.

The most proven line of defense against data breaches is to protect the data itself with encryption. A comprehensive encryption strategy includes the ability to protect both structured and unstructured data stores that can include database and file server files, documents, image scans, voice, and logs across a heterogeneous IT infrastructure. To gain maximum benefit from their encryption programs, security-conscious enterprises are leveraging intelligent encryption that uses access controls to ensure data is only decrypted for authorized requests.

Vormetric Encryption, part of the Vormetric Data Security portfolio of products, is a comprehensive solution for key management, encryption, and access control for data at rest across distributed systems– all of which can be managed from a centralized data security console. Vormetric Encryption is a proven high-performance solution that transparently integrates into Linux, UNIX, and Windows operating systems to protect data in physical, virtual, and cloud environments.

The Real Risks to Enterprise Data

The main drivers for using encryption and access controls to protect sensitive data include compliance mandates (such as PCI DSS, HIPAA HITECH Act, GLBA, UK Data Protection Act), the rapidly growing number of domestic and international data protection legislative acts, along with executive mandates to protect sensitive enterprise data.

> **"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

Additionally, as organizations shift from physical to virtual environments and subsequently leverage infrastructure in the cloud, the security of their data is an even greater concern. Virtualization drastically increases the portability of operating environments. Subsequently, sensitive information and intellectual property in the form of digital data can be accessed more easily than ever before by unauthorized individuals and malicious insiders.

Making Encryption Successful

While passing audits and minimizing risk are the primary goals for implementing encryption, selecting the right encryption solution for enterprise files shares, databases, and storage systems requires specific focus on performance, extensibility, key management, and low administrative overhead.

In today's exploding regulatory environment, selecting encryption solutions that meet immediate needs – but also extend to the needs of the future – will lower management complexity, operational costs, and afford greater agility in meeting encryption-related audit points and expanding data security needs. Selecting a comprehensive solution that protects data across operating systems, databases, applications, and multiple storage architectures, including DAS (Direct Attached Storage), NAS (Network Attached Storage) and SAN (Storage Area Network), helps eliminate the need for point encryption solutions and the administrative burden they incur.

Key management is arguably the most important aspect of encrypting on a broad scale. Key storage, transmission, and handling directly control the security of the system and the availability of data. Ensuring that key management is centralized, secure, and as robust as possible will avoid future audit points, streamline operations, and ensure that both information security and information management objectives are simultaneously met.

The Vormetric Encryption Solution

Vormetric Encryption is a comprehensive solution for key management and encryption of data at rest. Vormetric offers strong data security controls through policy-based access controls, separation of duties, and auditing capabilities, which can be maintained from a centralized management console.

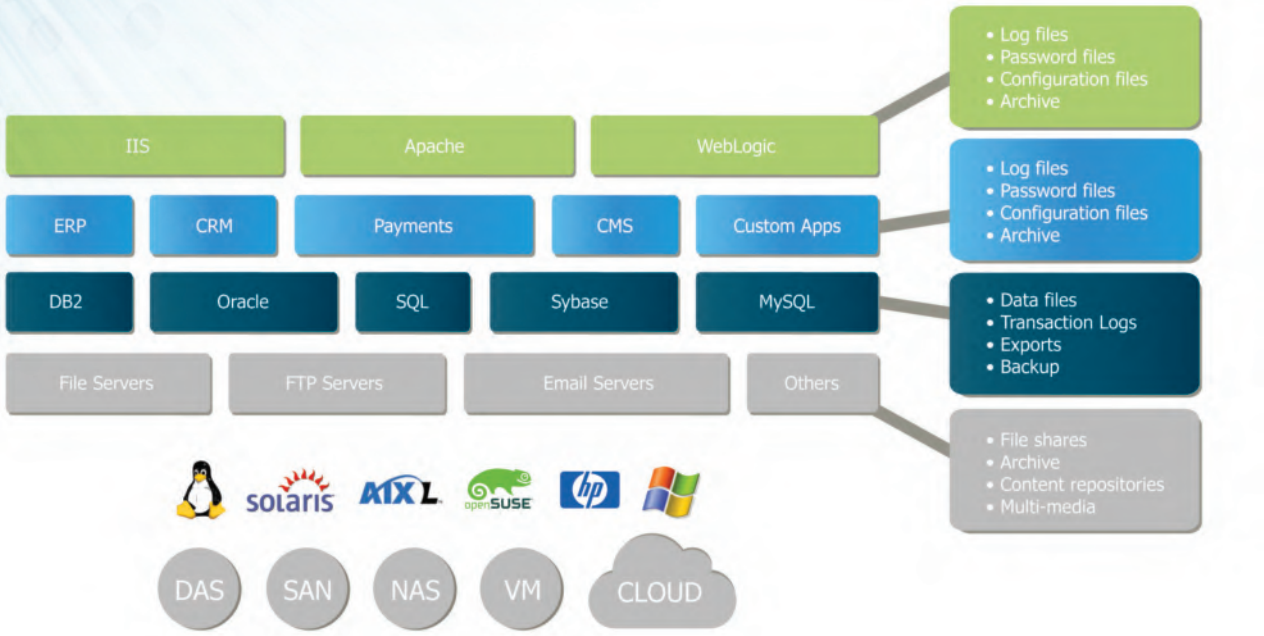

Figure 1: Vormetric offers a broad and flexible approach to encryption that protects data across all leading applications, databases, operating systems, and storage devices.

The Vormetric Encryption solution consists of two major components:

- Vormetric Data Security Manager
- Vormetric Encryption Expert Agents

The flexibility and scalability of the Vormetric Encryption design stems from its separation of the Data Security Manager from the Encryption Expert Agents. The Data Security Manager provides centralized administration of encryption keys and data security policies, while the Encryption Expert Agents provide protection of structured and unstructured data stores that can include database and file server files, folders, documents, image scans, voice recordings, logs, and more.

Vormetric Data Security Manager

Vormetric Data Security Manager integrates key management, data security policy management, and event log collection into a centrally managed cluster that provides high availability and scalability to thousands of Vormetric Encryption Expert Agents. 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. The Data Security Manager stores the data security policies, encryption keys, and audit logs in a hardened appliance that is physically separated from the Encryption Expert Agents. Security teams can enforce strong separation of duties over management of the Vormetric system by requiring the assignment of key and policy management to more than one data security administrator so that no one person has complete control over the security of data.

Vormetric Data Security Manager is accessed from a secure Web-management console and supports multiple Encryption Expert Agents. As a 2U rack-mountable Federal Information Processing Standard (FIPS) 140-2, Level 2 compliant security appliance (FIPS 140-2, Level 3 Key Management with Hardware Security Module), the Data Security Manager functions as the central point for creating, distributing, and managing data encryption keys, policies, and host data security configurations.

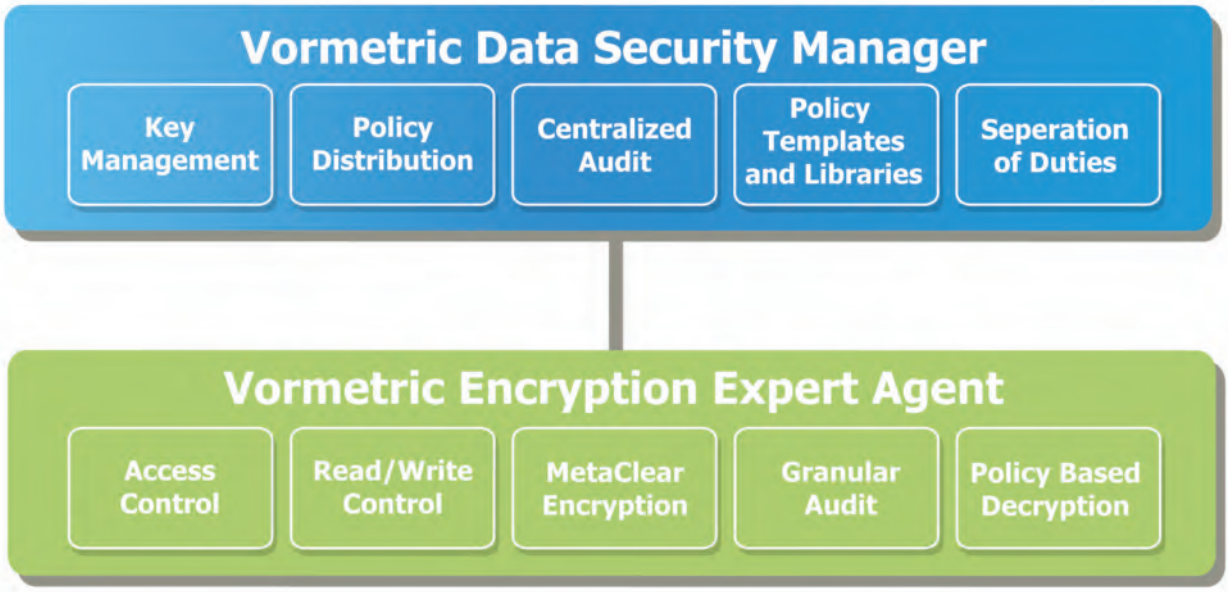

Figure 2: Vormetric Data Security Manager is the central point for creating and managing encryption, keys, and policies, and then distributing them to Vormetric Encryption Expert Agents.

Vormetric Encryption Expert Agents

Vormetric Encryption Expert Agents are software agents that insert above the file system logical volume layers. The agents evaluate any attempt to access the protected data and apply predetermined policies to either grant or deny such attempts. The agents maintain a strong separation of duties on the server by encrypting files and leaving their metadata in the clear so IT administrators can perform their jobs without directly accessing the information. The agents perform the encryption, decryption, and access control work locally on the system that is accessing the data at rest in storage. This enables encryption to be distributed within the data center and out to remote sites, while being centrally managed via the Data Security Manager cluster.

Vormetric Encryption Expert 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. Current OS support includes Microsoft Windows, Linux, Sun Solaris, IBM AIX, and HP-UX.

1. For more on PCI DSS, see Complying with PCI DSS Encryption Rules whitepaper http://enterprise-encryption.vormetric.com/complying-with-pci-dss-encryption-rules.html

> **"Vormetric Encryption gives us a modular ability to effectively encrypt server-based data at rest and manage that protection effectively. Future scalability to apply this solution where additional needs may arise was a significant consideration."**
>
> - Thomas Doughty, CISO, Prudential

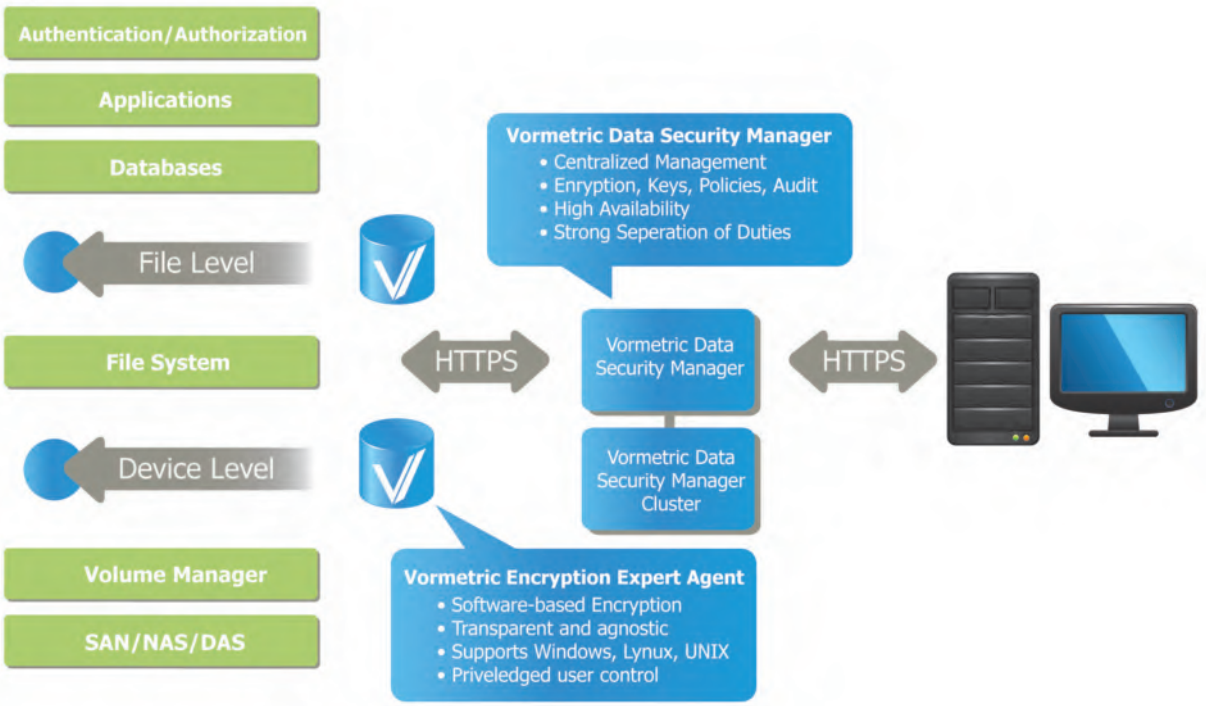

Figure 3: Vormetric Encryption Expert Agents reside between the database, application, or user layer; and file system or volume manager in order to transparently encrypt/decrypt data.

Vormetric Encryption Advantages

Transparent Implementation

Integrating encryption into an existing IT infrastructure is not normally synonymous with "easy." In fact, most solutions require some type of application or database development changes. Ultimately, these changes can lengthen the deployment cycle by months – even years – and drastically weaken performance.

In contrast, Vormetric Encryption can be implemented quickly without the need to re-architect databases, applications, or files, and without degrading the performance of existing systems. Inserted above the file system logical volume layers, Vormetric Encryption is transparent to users, applications, and databases. No modification to the application or database is required and therefore deployments can be managed in days to weeks. It adds minimal performance overhead and is faster than most native database encryption architectures.

High Performance

The most common question IT organizations have about encryption solutions is, "What is the level of performance degradation?" The level of performance overhead depends on how an encryption solution is architected, how it interacts with existing systems, and the amount of hardware cryptographic acceleration that might be available. For example, column-level encryption adds a linear performance impact – doubling the length of the encrypted column will double the performance degradation.

Vormetric performs encryption and decryption operations at the optimal location of the file system or volume manager. This approach utilizes the I/O profile of high-end applications and databases by only encrypting and decrypting the storage blocks needed by that particular operation. Vormetric Encryption also takes advantage of hardware cryptographic acceleration, such as Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI) and SPARC Niagara Crypto, to speed the encryption and decryption of data.

While most vendors claim the performance impacts of their "transparent" approaches to encryption are in the single digits, Vormetric has been proven to routinely outperform these metrics. Encryption and decryption operations are only performed when disk I/O is executed on sensitive data avoiding any transactional impact of the encryption operations. As a result, Vormetric customers typically report no perceptible impact to the end-user experience when using Vormetric Encryption. Figure 4 shows the results of an online transaction processing (OLTP) benchmark run with Intel® that demonstrated under 2% performance overhead at 70% system utilization.

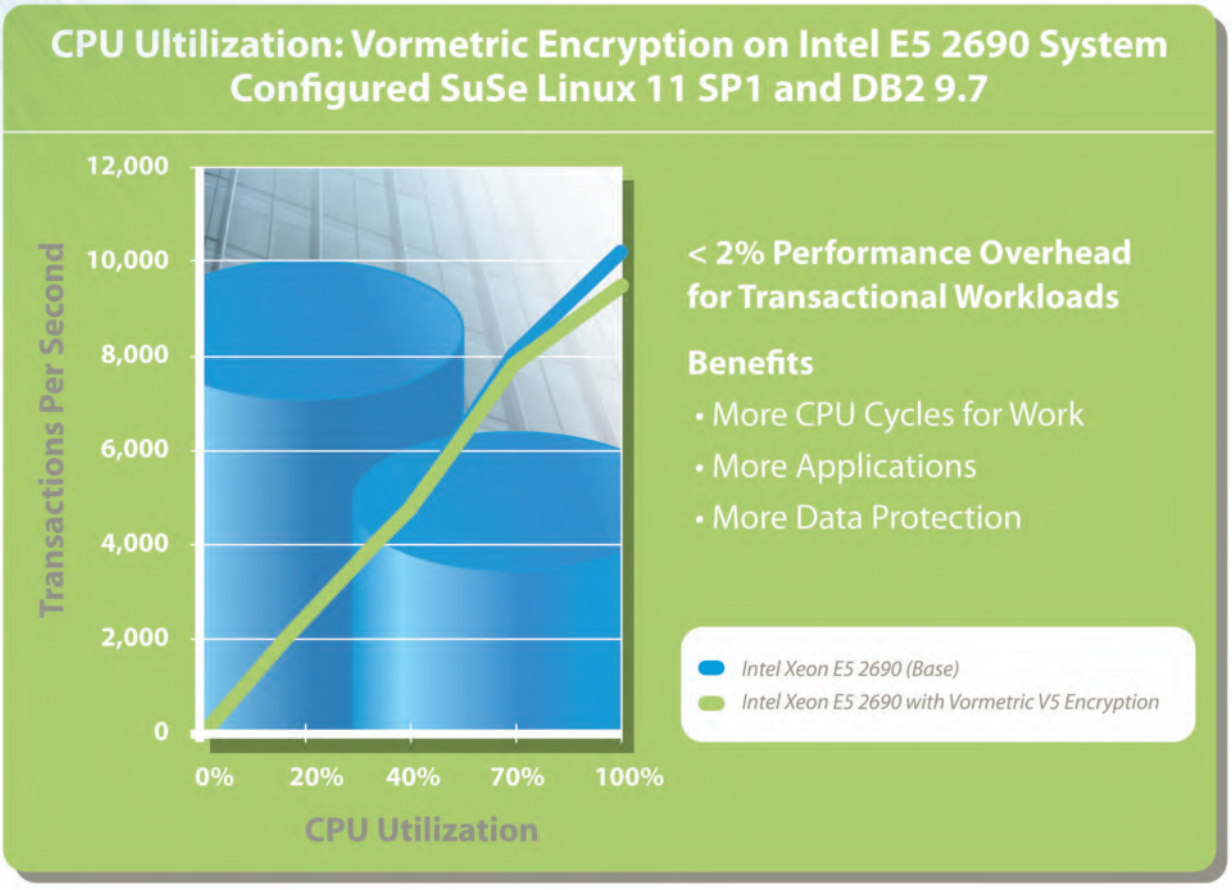

Figure 4: Vormetric Online Transaction Processing (OLTP) performance using the TPoX benchmark.

Centralized Key and Policy Management

Vormetric Encryption provides integrated key and policy management to deliver a secure, easy to administer, and centrally managed solution. This enables organizations to establish consistent and common best practices for managing the protection of both structured and unstructured data accessed by Linux, UNIX, and Windows systems.

Unlike native encryption point solutions (i.e., database vendor encryption) that create policy, key management, and separation of duties issues, Vormetric offers an enterprise-class, secure, and centralized key management system that easily extends throughout diverse IT environments. Employing multiple point solutions for encryption increases the complexity of managing and securing encryption keys, particularly in order to comply with industry and government regulations. Vormetric Key Management is drastically simplified through a single point for all enterprise systems and also provides granular administrative control and auditing.
(Please see the Vormetric Key Management white paper for more information.)

Vormetric Encryption shares common infrastructure with Vormetric Key Management, a solution to manage third-party encryption keys, including keys for Oracle Transparent Data Encryption (TDE) and Microsoft SQL

Server TDE (also described in the Vormetric Key Management white paper). This enables enterprises to achieve an improved return on investment by having fewer security solutions providing greater coverage and a standard security posture.

Strong Separation of Duties

There are two ways Vormetric Encryption provides a strong separation of duties so that no one person has complete control over the security of data. First is with the Vormetric Data Security Manager, where a strong separation of security duties is provided with role-based administration and separate domains. The second way is with Vormetric Encryption Expert Agents, where strong access controls around the data itself provide a separation between security and IT administration.

Role-Based Administration and Domains

Vormetric Data Security Manager provides robust role separation to allow organizations to securely leverage the Data Security Manager infrastructure. Security administration can be broken down into responsibilities, so that one person might administer the creation of data encryption keys while a different person would administer the hosts and policies applied to that key (Figure 5).

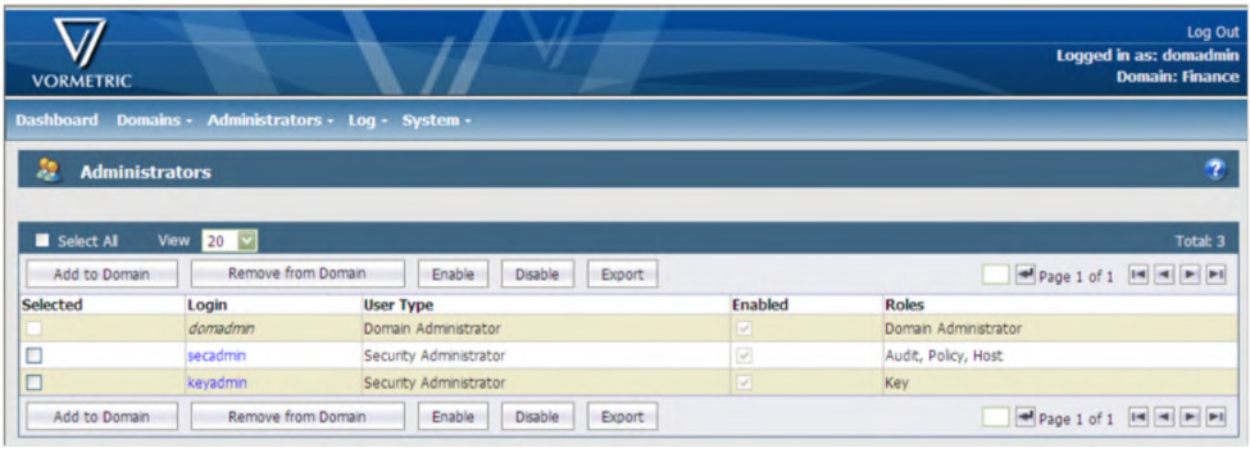

Figure 5: Strong separation of duties enables separation of security roles, so that one person can administer keys while a different person would administer hosts and policies.

This separation can be taken further with Security Management Domains that combine this role-based administration with the ability to compartmentalize the management for policies, data encryption keys, agent configurations, and audit logs for a particular business group. For example, many enterprises need to compartmentalize data security management of corporate assets between business units and departments into different domains with different groups of security, key, and host administrators, while a smaller business may only have one security administrator for the entire deployment. Data security management can now be both centrally and departmentally administered.

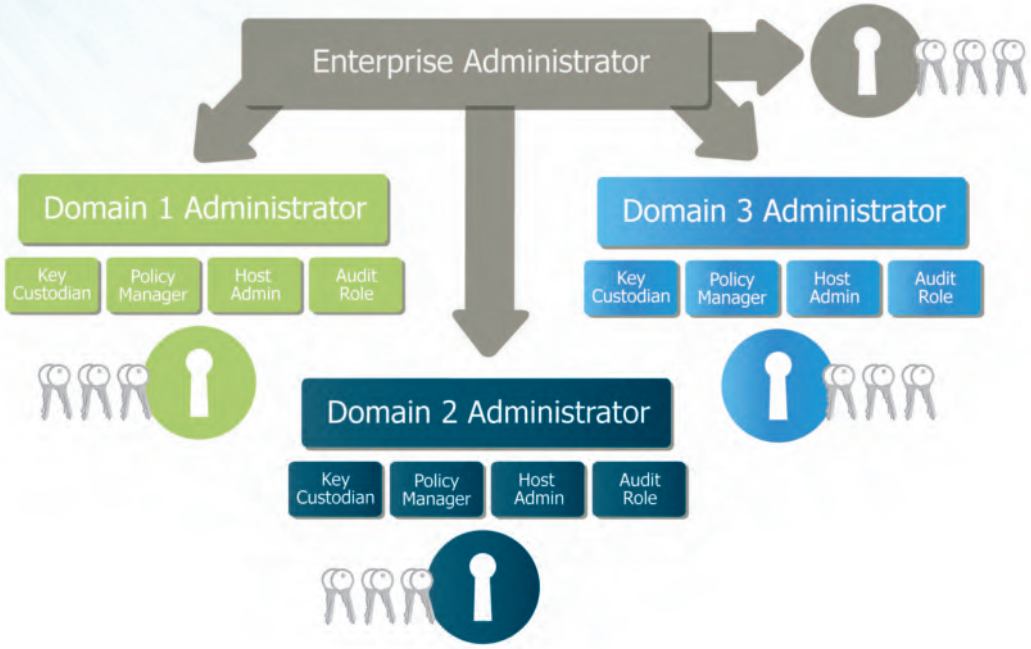

Figure 6: Security Management Domains combine role-based administration of the Vormetric solution with the ability to compartmentalize the management for policies, data encryption keys, agent configurations, and audit logs.

Encryption and Access Control

Vormetric Encryption integrates encryption and access control at the operating system layer to provide separation of duties between data security administrators and server operations. Organizations can apply Vormetric Encryption policies to ensure system administrators and root users can maintain systems and backups without being able to view sensitive data. Vormetric's innovative technology allows management of data without visibility by encrypting file content data but not file system metadata. By leaving the file system metadata in the clear, data management applications and system administrators can perform necessary functions without the need to expose file content during management operations.

With encrypting switch and inline encryption methods, companies are forced to open full data access to system administrators and root users in order to complete their routine IT administration tasks, simply trusting these users not to read the data. By leveraging the Vormetric approach, companies no longer have to rely on the "honor system" as part of their data protection initiatives.

Vormetric Encryption access control follows a least-privilege model, which means that any attempt at data access that is not specifically authorized according to well-defined, pre-set parameters will be blocked. This added layer of optional access controls plus encryption enables organizations to protect against a broader set of data security threats than any other encryption solution.

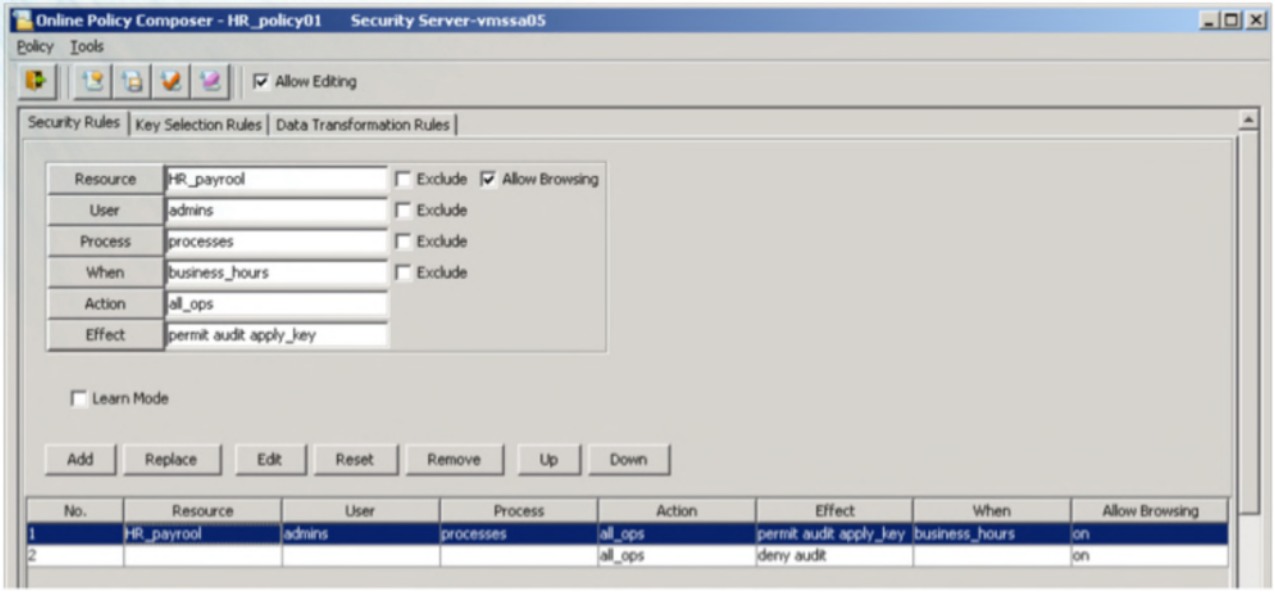

Figure 7: Online Policy Composer provides various layers of protection including who, what, when, where, and how an individual or application may access protected data.

Scalability

With the proliferation of sensitive data, the need to easily scale an encryption solution is paramount. Organizations can easily and rapidly deploy up to thousands of Vormetric Encryption Expert Agents centrally from the Data Security Manager cluster. Data security policies and associated encryption keys are created centrally and then automatically distributed to Encryption Expert agents. Vormetric Encryption is equally suited to meet both centralized (i.e., data center-based), as well as distributed site encryption needs.

Distributed IT Environments

Most organizations today are uncertain as to where all of their sensitive information resides. With typical IT environments, the crown jewels are not likely to be centrally protected in a data center, but scattered throughout the organization in file shares, databases, and storage devices with different access rights and user privileges. Point encryption solutions, such as those provided by database vendors, cannot centrally manage encryption and policies over such a wide area of distributed data. Additionally, inline encryption isn't able to set appropriate access controls in order to keep unauthorized eyes from seeing the sensitive information. In order to scale, hardware encryption soon becomes cost prohibitive, requiring time-consuming configuration and instrumentation.

By contrast, the Vormetric software-based approach works exceptionally well in distributed IT environments where organizations may have thousands of servers geographically distributed throughout the world. Without local security experts and the high costs of implementing physical security controls at each individual site, Vormetric customers can centrally manage and economically deploy encryption and policies to protect both structured and unstructured distributed data.

High Availability

In a business mission-critical IT environment where continuous availability is expected, Vormetric Encryption supports Data Security Manager clustering across Local or Wide Area Networks. This clustering capability ensures high availability, fault tolerance, and load balancing across data centers and/or geographies. Additionally, the data encryption keys, policies, administrator accounts, and agent settings are easily and securely archived offline. These archives are encrypted with a Backup Encryption Key that is split into parts and distributed to a configurable number of custodians. This approach ensures the Vormetric Data Security Manager cluster configuration is archived, but no single administrator can make use of the archive to exploit its contents. (To learn more about this capability, please refer to the Vormetric Key Management white paper.)

Fine-Grained Auditing

The Vormetric Encryption solution provides granular and configurable auditing and reporting of access requests to protected data, as well as changes to the security of that data. The system logs only access requests that require attention or retention (e.g., denied access attempts and certain permitted activity) to ensure security staff is not burdened with superfluous event data.

The Vormetric Encryption Expert Agents securely send and store log records of all context attributes of the request back to the Vormetric Data Security Manager or to third-party log repositories, such as Windows Event Logs or syslogs. This enables centralized tracking of data access at the operating system level, providing an extensive access log for detailed analysis. For example, Vormetric records would include when the access occurred, who made the request, the application used to make the request, the host where the request occurred, the I/O operation requested, and how Vormetric responded (e.g., permit, deny, encrypt, or decrypt).

Vormetric limits access to audit trails on a need-to-know basis, to control root or administrator access to sensitive data, in the same way the system restricts access to the data itself, so Vormetric Data Security Manager audit logs are protected from tampering or any type of unauthorized modifications.

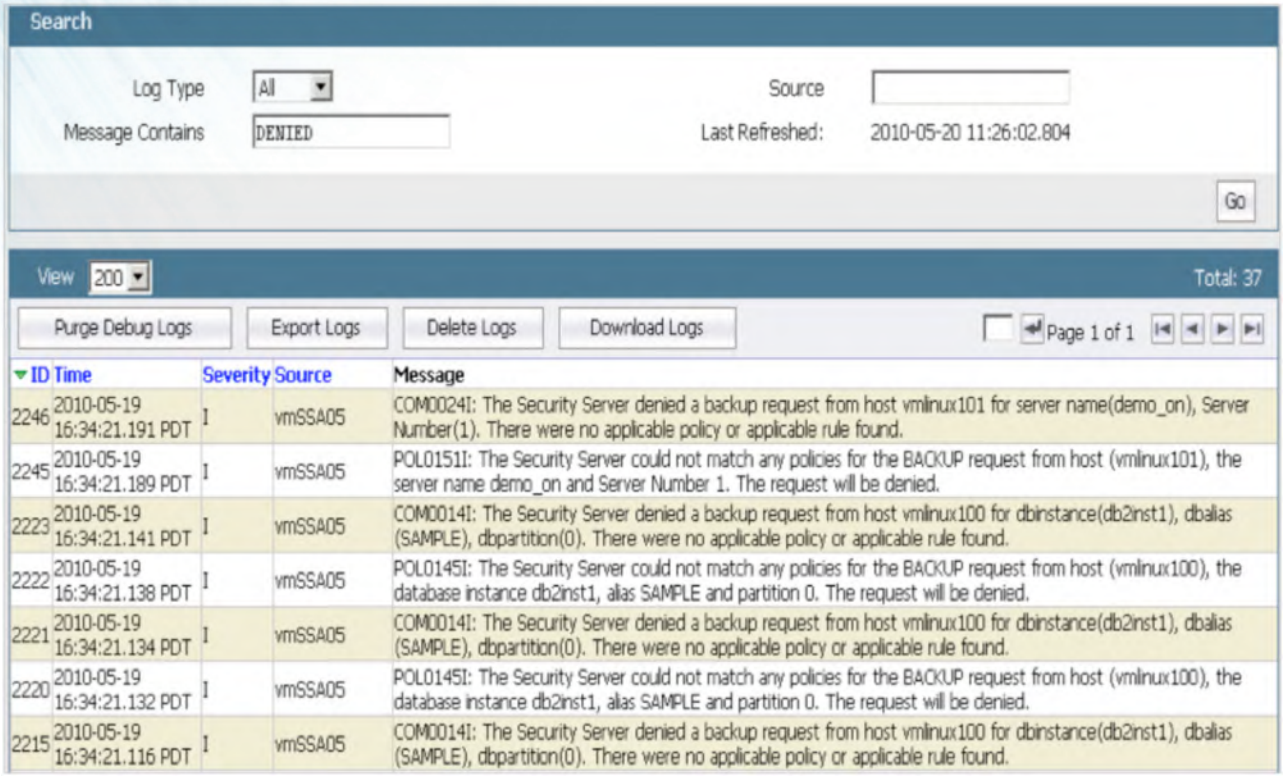

Figure 8: The Vormetric Data Security Management Console displays access logs for detailed analysis.

The system's audit ability aids compliance with industry and government regulatory practices regarding the handling and protection of private and confidential information. Audit logs can be integrated into existing risk management solutions, such as Security Information and Event Management (SIEM) systems. Vormetric's enforcement of IT governance policies and procedures significantly reduces the amount of recurrent testing required to assure auditors of system and application integrity, and comprehensive audit logs reduce the cost and time required to assess compliance with government regulations.

Conclusion

Vormetric Encryption is a proven, simple-to-deploy and manage solution that provides powerful encryption of data across enterprise IT infrastructures – transparently and with minimal performance impact. With high-speed encryption, integrated key management, and context-aware access controls, Vormetric Encryption protects valuable information in order to address industry and government regulations, secure virtual and cloud-based environments, and most importantly, drastically lower the risk of devastating data breaches.