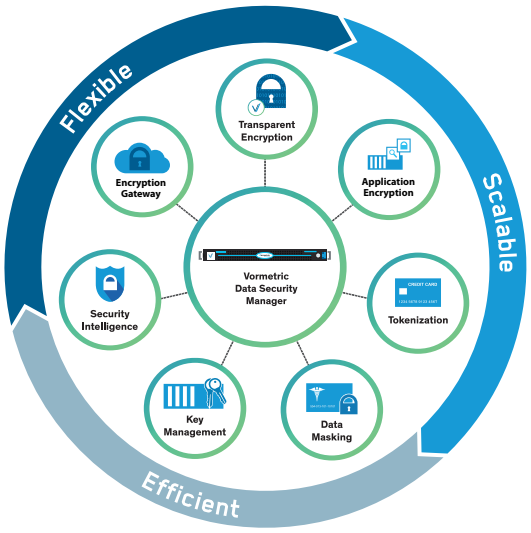
Vormetric Data Security Platform

The Vormetric Data Security Platform efficiently manages data-at-rest security across your entire organization. Built on an extensible infrastructure, the Vormetric Data Security Platform is composed of several products that can be deployed individually, while offering efficient, centralized key management. As a result, your security teams can broaden and strengthen their coverage while streamlining their efforts.

The Vormetric Data Security Platform delivers capabilities for transparent file-level encryption, application-layer encryption, tokenization, dynamic data masking, cloud encryption gateway, integrated key management, privileged user access control, and security intelligence. Through the platform's centralized key management and flexible implementation, you can address security policies and compliance mandates across databases, files, and big data nodes—whether assets are located in the cloud, virtualized environments, or traditional infrastructures. With this platform's comprehensive, unified capabilities, you can efficiently scale to address your expanding security and compliance requirements, while significantly reducing total cost of ownership (TCO).



STRENGTHEN SECURITY AND COMPLIANCE

Vormetric offers a flexible and scalable set of solutions that can meet a broad set of use cases, so security teams can protect sensitive data across the organization. The platform provides capabilities for encrypting and tokenizing data, controlling access, and creating granular security intelligence logs. The platform delivers the comprehensive capabilities that enable you to address the demands of a range of security and privacy mandates, including the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and regional data protection and privacy laws. With these capabilities, organizations can effectively combat advanced persistent threats (APTs), guard against insider abuse, and establish persistent controls, even when data is stored in an external provider's infrastructure.

CAPABILITIES

- Transparent file encryption
- Application encryption
- Tokenization
- Dynamic data masking
- Cloud encryption gateway
- Key management and vaulting
- Privileged user access control
- Access audit logging

ENVIRONMENTS

- IaaS, PaaS, and SaaS
- Linux, Windows, and UNIX
- Hadoop, MongoDB, NoSQL, and Teradata
- SAP HANA
- Docker containers
- Oracle, IBM DB2, Microsoft SQL Server, MySQL, Sybase, NoSQL, etc.
- Any storage environment

Best Encryption Solution

MAXIMIZE STAFF AND RESOURCE EFFICIENCY

The Vormetric Data Security Platform makes administration simple and efficient, offering an intuitive Web-based interface, as well as an application programming interface (API) and command-line interface (CLI). With the solution, data-at-rest security can be applied quickly and consistently, maximizing staff efficiency and productivity. Furthermore, this high-performance solution enables efficient use of virtual and physical server resources, reducing the load on the service delivery infrastructure.

REDUCE TOTAL COST OF OWNERSHIP

The Vormetric Data Security Platform makes it simpler and less costly to protect data at rest. The platform enables your IT and security organizations to quickly safeguard data across your organization in a uniform and repeatable way. Instead of having to use a multitude of point products scattered across your organization, you can take a consistent and centralized approach with the Vormetric Data Security Platform.

PLATFORM PRODUCTS

The Vormetric Data Security Platform features these products:

Vormetric Data Security Manager. Offers centralized management of keys and policies for the entire suite of products available within the Vormetric Data Security Platform. Available as a virtual or FIPS 140-2 physical appliance.

Vormetric Transparent Encryption. Features a software agent that runs in the file system to provide high-performance encryption and least-privileged access controls for files, directories, and volumes. Enables encryption of both structured databases and unstructured files.

Vormetric Tokenization with Dynamic Data Masking. Delivers capabilities for format preserving tokenization and dynamic display security for databases. Supports PCI DSS compliance requirements and audit scope reduction. Both traditional token vault-based and high-performance vaultless solutions are available.

Vormetric Application Encryption. Streamlines the process of adding encryption into existing applications. Offers standards-based APIs that can be used to perform high-performance cryptographic and key management operations.

Vormetric Cloud Encryption Gateway. Enables organizations to safeguard files in cloud storage environments, including Amazon Simple Storage Service (Amazon S3), Box, and Caringo. Offers capabilities for encryption, on-premises key management, and detailed logging.

Vormetric Key Management. Centralizes management of keys for Vormetric products, IBM InfoSphere Guardium Data Encryption, Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant encryption products. Securely stores and inventories certificates.

Vormetric Security Intelligence. Produces granular logs that provide a detailed, auditable record of file access activities, including root user access. Offers pre-packaged dashboards and reports with security information and event management (SIEM) systems to streamline compliance reporting and speed threat detection.

PLATFORM ADVANTAGES

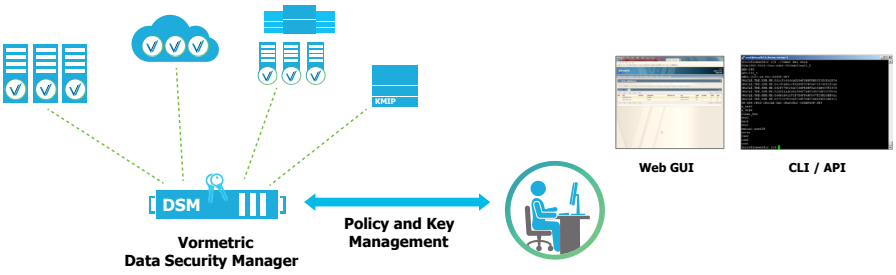
- Centralized data-at-rest security policies
- Manage keys from Vormetric and third-party encryption products
- Consistent security and compliance across physical, virtual, cloud, big data environments
- Actionable granular file-access intelligence with pre-defined SIEM dashboards
- Flexibility and extensibility enable fast support of additional use cases

COMPLIANCE

- PCI DSS 3.0
- HIPAA/HITECH
- NIST 800-53
- FISMA
- PIPA
- GDPR

Vormetric Data Security Manager

The Vormetric Data Security Manager (DSM) offers central controls that enable an IT organization to have a consistent and repeatable method for managing encryption, access policies, and security intelligence for all structured and unstructured data. Once the DSM is in place, you can more quickly adapt to new security mandates, compliance requirements, and emerging threats. The DSM is used for provisioning and managing keys for all Vormetric products. In addition, you can manage keys and certificates for third-party devices. By delivering centralized control of a breadth of data-at-rest security capabilities, the DSM provides low total cost of ownership, efficient deployment, and improved visibility and control.



RELIABLE, FIPS VALIDATED, SECURE SYSTEM DESIGN

To maximize uptime and security, the DSM features redundant components and the ability to cluster appliances for fault tolerance and high availability. Strong separation-of-duties policies can be enforced to ensure that one administrator does not have complete control over data security activities, encryption keys, or administration. In addition, the DSM supports two-factor authentication for administrative access. The DSM is available as a FIPS 140-2 Level 2, FIPS 140-2 Level 3 hardware appliance, and as a virtual appliance.

UNIFIED MANAGEMENT AND ADMINISTRATION ACROSS THE ENTERPRISE

DSM enables enterprises to minimize costs by providing central management of heterogeneous encryption keys, including keys generated by Vormetric products, IBM InfoSphere, Guardium Data Encryption, Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant encryption products. It features an intuitive Web-based console for managing encryption keys, policies, and auditing across an enterprise. The product also centralizes log collection across any number of agents.

Key Benefits

- Single console for all platform policy and key management
- Multi-tenancy support
- Proven scale to 10,000+ agents
- Cluster support for high availability
- Toolkit and programmatic interface
- Easy integration with existing authentication infrastructure
- RESTful API support
- Virtual or physical appliance
- FIPS 140-2 Level 1 Virtual Appliance
- FIPS 140-2 Level 2
- FIPS140-2 Level 3 available

The V6100 DSM offers smart cards for HSM multi-factor administrator authentication

FIPS VALIDATED 140-2 ™

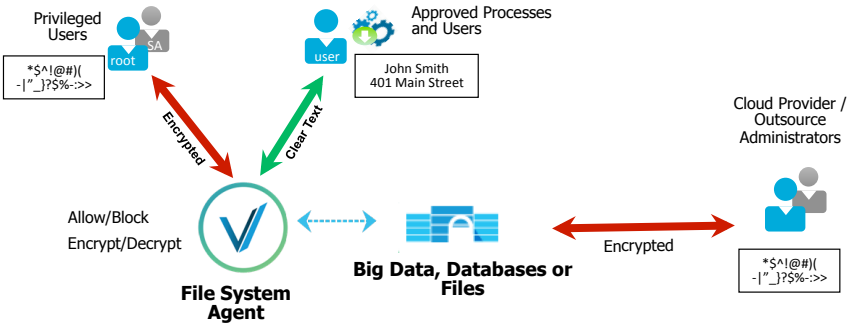
Common Criteria

VORMETRIC V6000 AND V6100 SPECIFICATIONS

Specification	Description
Hardware Specifications	
Chassis	1U rack-mountable; 17" wide x 20.5" long x1.75" high (43.18 cm x 52.07cm x 4.5 cm)
Weight	V6000: 21.5 lbs (9.8 kg); V6100: 22 lbs (10 kg)
Memory	16GB
Hard Disk	Dual SAS RAID 1 configured with FIPS tamper-evident seals
Serial Port	1
Ethernet	2x1Gb
IPMI	1x10/100Mb
Power Supplies	2 removable 80+certified (100VAC-240VAC/50-60Hz) 400W
Chassis Intrusion Detection	Yes. Also includes FIPS tamper-evident seal on the top cover.
Maximum BTU	410 BTU max
Operating Temperature	10° to 35° C (50° to 95° F)
Non-Operating Temperature	-40° to 70° C (-40° to 158° F)
Operating Relative Humidity	8% to 90% (non-condensing)
Non-Operating Relative Humidity	5% to 95% (non-condensing)
Safety Agency Approval	FCC, UL, and BIS certifications
FIPS 140-2 Level 3 HSM	V6100 only
Software Specifications	
Administrative Interfaces	Secure Web, CLI, SOAP, REST
Number of Management Domains	1,000+
API Support	PKCS #11, Microsoft Extensible Key Management (EKM), SOAP, REST
Security Authentication	Username/Password, RSA two-factor authentication (optional)
Cluster Support	Yes
Backup	Manual and scheduled secure backups. M of N key restoration.
Network Management	SNMP, NTP, Syslog-TCP
Syslog Formats	CEF, LEEF and RFC 5424
Certifications and Validations	FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level 3, Common Criteria (ESM PP PM V2.1)
Minimum Virtual Machine Specifications	**Recommendation for Vormetric Data Security Manager Virtual Appliance**
Number of CPUs	2
RAM (GB)	4
Hard Disk (GB)	100GB
Support Thin Provisioning	Yes

Vormetric Transparent Encryption

Vormetric Transparent Encryption offers capabilities for data-at-rest encryption, privileged user access control, and security intelligence log collection. With the solution, you can secure structured databases and unstructured files—including those residing in physical, virtualized, big data, and cloud environments. By leveraging this solution's transparent approach, your organization can implement encryption, without having to make changes to your applications, infrastructure, or business practices. Unlike other encryption solutions, protection does not end after the encryption key is applied. Vormetric continues to enforce policies that protect against unauthorized access by users and processes, and it continues to log access. With these capabilities, you can ensure continuous protection and control of your data.



VORMETRIC TRANSPARENT ENCRYPTION ARCHITECTURE

Vormetric Transparent Encryption is an agent that runs at the file system level or volume level on a server. The agent is available for a broad selection of Windows, Linux, and UNIX platforms, and can be used in physical, virtual, cloud, and big data environments—regardless of the underlying storage technology. All policy and key administration is done through the DSM.

Vormetric Transparent Encryption agents are distributed across the server infrastructure. As a result, the product delivers scalability and eliminates the bottlenecks and latency that plague proxy-based solutions. In addition, you can use hardware-based encryption acceleration products, such as Intel AES-NI and SPARC Niagara Crypto modules, to further enhance encryption performance.

POWERFUL PRIVILEGED USER ACCESS CONTROLS

The agent enforces granular least-privileged user access policies that protect data from misuse by administrators and advanced persistent threat (APT) attacks.

Policies can be applied by user, process, file type, time of day, and other parameters. Enforcement options are very granular; they can be used to control not only permission to access clear-text data, but what file-system commands are available to a user.

Key Benefits

- Broadest platform support in industry: Windows, Linux, and UNIX operating systems
- Easy to deploy; no application customization required
- High performance strong encryption
- Privileged user access control
- Log all permitted, denied, and restricted access attempts from users, applications, and processes
- Granular Hadoop user access controls

Technical Specifications

Platform Support

- Microsoft: Windows Server XP, Vista, 7, 8, 2008, 2012
- Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Oracle Red Hat Compatible Kernel and Ubuntu
- UNIX: IBM AIX, HP-UX, and Solaris

Database Support

- Oracle, DB2, SQL Server, MySQL, Sybase, NoSQL environments, and others

Application Support

- Transparent to all applications and custom applications including SAP, SharePoint, Documentum, and more

Big Data Support

- NoSQL: Couchbase, DataStax, MongoDB
- Hadoop: Cloudera, Hortonworks, IBM
- SAP HANA
- Teradata

Encryption Hardware Acceleration

- Intel and AMD AES-NI
- SPARC encryption
- IBM P8 cryptographic coprocessor

Agent Certification

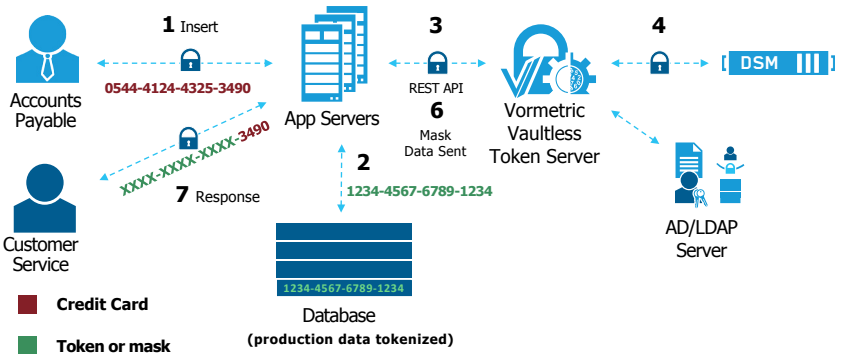
- FIPS 140-2 Level 1

Container Support

- Docker

Vormetric Tokenization with Dynamic Data Masking

Vormetric Tokenization with Dynamic Data Masking products enable application developers to easily tokenize sensitive data using either a traditional vault-based or high-performance vaultless tokenization solution. The solution provides a single platform that offers database tokenization and dynamic display security. With Vormetric Tokenization, you can meet PCI DSS requirements and secure data in cloud, big data, and data center environments—and do so with minimal disruption and administrative overhead.



FAST AND EASY TOKENIZATION

The solution offers a choice between the Vormetric Vaultless Token Server or the Vormetric Token Server. Both products feature a virtual appliance for tokenizing records and managing access to tokens and clear-text data through applications using REST APIs to send requests for the creation and management of tokens. In addition, the product eliminates the complexity of adding support for policy-based dynamic data masking to applications. Vormetric Tokenization delivers the following advantages:

Streamlined application integration. The Vormetric solution employs tokenization at the application layer streamlining all the application development efforts associated with implementing tokenization and dynamic data masking in an enterprise.

Dynamic data masking. Administrators can establish policies to return an entire field tokenized or dynamically mask parts of a field. For example, a security team could establish policies so that a user with customer service representative credentials would receive only a credit card number with the last four digits visible, while a customer service supervisor could access the full credit card number in the clear.

Vaultless Tokenization. Selecting the Vormetric Vaultless Tokenization option delivers the highest performance and removes the requirement for maintaining and synchronizing a token vault database.

Key Benefits

- Remove card holder data from PCI DSS scope with minimal cost and effort
- More fully leverage cloud, big data, and outsourced models—without increased risk
- Establish strong safeguards that protect sensitive assets from cyber attacks and insider abuse

Technical Specifications

Product Choices:
- Vormetric Token Server
- Vormetric Vaultless Token Server

Vormetric Token Server:
- Virtual appliance
- Open Virtualization Format (.ovf)
- Min. hardware: 4 CPU cores, 4G ram
- Min. disk: 5GB

Tokenization capabilities:
- Format preserving tokenization
- Random and sequential tokens
- Single and multi-use tokens
- Partial tokenization

Dynamic data masking capabilities:
- Numeric support
- Customize mask character

Validation support:
- Luhn check

Encryption key management:
- FIPS 140-2 validated platform

Application integration:
- REST APIs
- Bulk APIs for batch jobs

Authentication integration:
- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)

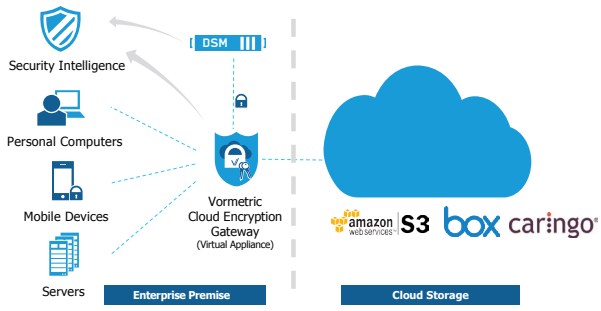
Performance features:
- Virtual appliance enables fast increase and decrease in capacity

Database for vault option:
- Oracle 11gR2 and up

Pricing:
- Per protected server

Vormetric Cloud Encryption Gateway

With the Vormetric Cloud Encryption Gateway, organizations can safeguard files in cloud storage environments, including Amazon Simple Storage Service (Amazon S3), Box, and Caringo. The solution encrypts sensitive data before it is saved to the cloud storage environment. It enables security teams to maintain encryption keys on their premises, so they can get the visibility and control they need to protect sensitive assets from a range of threats. Like other Vormetric encryption offerings, the solution relies on the DSM for key and policy management. As a result, you never have to relinquish control of cryptographic keys to your cloud provider and data never leaves your premises unencrypted or unaccounted for.



EMPLOYS STRONG CONTROLS OVER CLOUD STORAGE DATA

The Vormetric Cloud Encryption Gateway is delivered as a virtual appliance that can be deployed in the cloud or in your data center. The product provides the following advantages:

Transparent, easy implementation. Offers transparent encryption and decryption of files by intercepting traffic as it moves between your users and the cloud.

On-premises key management. Enables customers to maintain local control over policies and keys at all times.

Detailed visibility and auditability. Delivers granular audit logs that track file access to support compliance reporting and forensics.

Intelligent risk detection. Scans Amazon S3 and Box cloud environments, discovers unencrypted files that violate security policies, and automatically encrypts them.

Flexible service extensibility. Offers easy extensibility, featuring Vormetric Security Blades that will enable Vormetric and its partners to deliver support for a growing number of cloud storage environments and SaaS solutions.

Key Benefits

- Transparent deployment
- On-premises key management and encryption
- Stateless architecture enables horizontal, cost-efficient scalability
- Strong cloud storage security and compliance controls

Technical Specifications

Virtual Appliance

- Open Virtualization Format (.ovf) distribution
- Min. hardware: 4 CPU cores, 4G ram
- Min. disk: 100GB

Vormetric Security Blades

- Amazon S3
- Box Enterprise File Synchronization and Sharing (EFSS)
- Caringo Object Storage

Authentication Integration

- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD) — Amazon S3 only

Policies

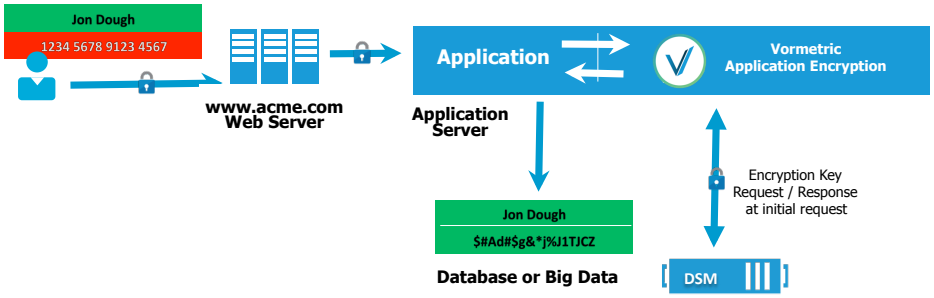
- Encrypt by file type
- Auto key rotation

MongoDB Version

- 2.6.3 or later

Vormetric Application Encryption

With Vormetric Application Encryption, you can do application-layer encryption of a specific file or column in a database, big data node, or platform-as-a-service (PaaS) environment. Vormetric Application Encryption features a library that simplifies the integration of encryption with existing corporate applications. The library provides a set of documented, standards-based APIs that can be used to perform cryptographic and key management operations. Vormetric Application Encryption eliminates the time, complexity, and risk of developing and implementing an in-house encryption and key management solution.



REDUCING APPLICATION-LAYER ENCRYPTION COMPLEXITY AND COSTS

Application-layer encryption is typically used when compliance or regulatory mandates require encryption of specific fields at the application layer, before data is stored. Vormetric Application Encryption reduces the complexity and costs associated with meeting this requirement, simplifying the process of adding encryption capabilities to existing applications. Developers can use libraries for Java, .NET, Python, and C to facilitate communication between applications and the Vormetric Application Encryption agent. This agent encrypts data and returns the resulting cipher text to the application application using either AES or Format Preserving Encryption (FPE). All policy and key management is done through the DSM, simplifying the data security operations environment by reducing the number of management consoles that administrators have to learn and maintain.

PROTECTING DATA IN THE CLOUD

Security professionals often have concerns about moving sensitive data from traditional enterprise applications to PaaS environments. Vormetric Application Encryption enables you to encrypt sensitive data before it leaves the enterprise and is stored in the cloud. By leveraging this approach, you can ensure that cloud administrators, other customers, hackers, and authorities with subpoenas can't access sensitive data, which can help address relevant auditor requirements and security policies.

Key Benefits

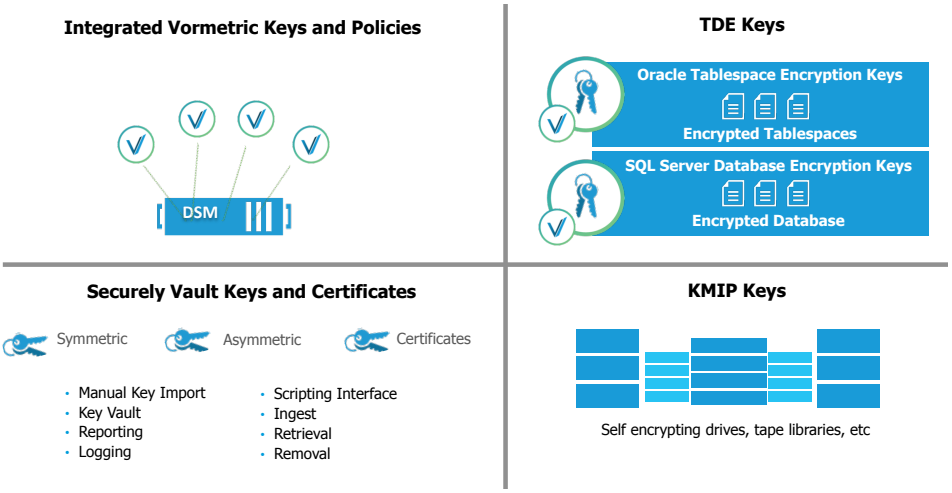
- Leverage proven, Vormetric high performance encryption and key management
- Broad application and platform support
- Centralize control of application-layer encryption and file system encryption
- Stop malicious DBAs, cloud administrators, hackers, and authorities with subpoenas from accessing valuable data

Technical Specifications

- Supported environments: Microsoft.NET 2.0 and higher, JAVA 7 and 8, and C
- Standards: OASIS PKCS#11 APIs
- Encryption: AES, FPE FF3
- Operating systems: Windows 2008 and 2012, and Linux
- Performance: 400,000 credit card size encryption transactions per second (e.g. single thread, 32 core, 16GB, C)
- Policy and key administration: Vormetric Data Security Manager

Vormetric Key Management

With Vormetric Key Management, you can centrally manage keys from all Vormetric products, and securely store and inventory keys and certificates for third-party devices—including IBM InfoSphere Guardium Data Encryption, Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant encryption products. By consolidating key management, this product fosters consistent policy implementation across multiple systems and reduces training and maintenance costs.



SIMPLIFY MANAGEMENT OF KEYS AND VAULTING OF CERTIFICATES

Historically, as the number of applications and devices using encryption proliferated, there was a commensurate increase in the number of key management devices used. This growing number of key management devices made it more complex and costly to maintain highly available encrypted environments. Further, these disparate key management devices often left valuable certificates unprotected, making them easy prey for hackers. Also, if these certificates were left unmanaged, they could unexpectedly expire, which would result in the unplanned downtime of vital services. Vormetric Key Management enables you to expand your capabilities so you can more effectively manage keys for Vormetric's products as well as keys and certificates from third-party products.

SECURE, RELIABLE, AND AUDITABLE

Vormetric Key Management offers all the reliability and availability capabilities of the DSM. The DSM features an optional FIPS 140-2 Level 3 validated hardware security module (HSM). The solution provides extensive audit capabilities that can be used to report on all activities relating to key usage, including key generation, rotation, destruction, import, expiration, and export.

Key Benefits

- Operational efficiency, continuous availability, secure storage, and inventory of certificates and encryption keys
- Alerts offer proactive notifications of certificates and key expiration
- Reports provide status and characteristic information, audit support

Technical Specifications

Manage Security Objects

- X.509 certificates
- Symmetric and asymmetric encryption keys

Administration

- Secure-web, CLI, API
- Bulk import of digital certificates and encryption keys
- Validates on import
- Extracts basic attributes from uploaded certificates and keys for reporting
- Command line scripts
- Retrieval and removal

Supported Key and Certificate Formats for Search, Alerts, and Reports

- Symmetric encryption key algorithms: 3DES, AES128, AES256, ARIA128, and ARIA256
- Asymmetric encryption key algorithms: RSA1024, RSA2048, and RSA4096
- Digital certificates (X.509): PKCS#7, PKCS#8, DER, PEM, PKCS#12
- Third-Party Encryption
- IBM Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE, and KMIP-clients

API Support

- PKCS#11, Microsoft Extensible Key Management (EKM), and OASIS KMIP

Key Availability and Redundancy

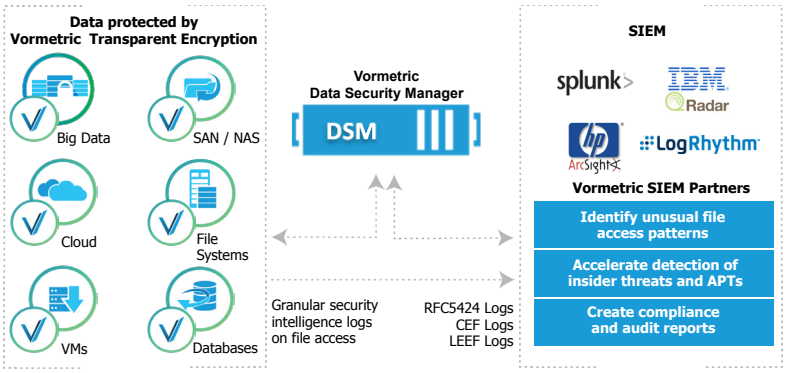
- Secure replication of keys across multiple appliances with automated backups

Common Criteria

FIPS VALIDATED 140-2

Vormetric Security Intelligence

Vormetric Security Intelligence delivers detailed security event logs that are easy to integrate with SIEM systems, so you can efficiently produce compliance and security reports. These logs produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into file access activities. Logging occurs at the file system level, helping eliminate the threat of an unauthorized user gaining stealthy access to sensitive data. These logs can inform administrators of unusual or improper data access and accelerate the detection of insider threats, hackers, and APTs.



PROVIDING SECURITY INTELLIGENCE

Traditionally, SIEMs relied on logs from firewalls, IPS, and NetFlow devices. Because this intelligence is captured at the network layer, these approaches leave a commonly exploited blind spot: They don't provide any visibility into the activity occurring on servers. Vormetric Security Intelligence eliminates this blind spot, helping accelerate the detection of APTs and insider threats.

Vormetric Security Intelligence provides logs that detail which processes and users have accessed protected data. Sharing these logs with a SIEM platform helps uncover anomalous process and user access patterns, which can prompt further investigation. For example, an administrator or process may suddenly access much larger volumes of data than normal, or attempt to do an unauthorized download of files. Such inconsistent usage patterns could point to an APT attack or malicious insider activities.

COMPLIANCE REPORTING

In order to adhere to many compliance mandates and regulations, organizations must prove that data protection is in place and operational. Vormetric Security Intelligence can be used to prove to an auditor that encryption, key management, and access policies are working effectively. The detailed logs can be reviewed to specify when users and processes accessed data, under which policies, and if access requests were allowed or denied. The logs will even expose when a privileged user leverages a command like "switch user" to imitate another user.

Key Benefits

- Enhanced visibility into sensitive data access
- Accelerated APT and insider threat detection
- Export logs in all major log formats: Syslog RFC5424, CEF, and LEEF
- Fast integration with Vormetric SIEM partners
- Consolidated and consistent compliance and audit reporting

SIEM Partner Integration

- FireEye Threat Prevention Platform
- HP ArcSight
- IBM Security QRadar SIEM
- Informatica Secure@Source
- McAfee ESM
- LogRhythm Security Intelligence Platform
- SolarWinds
- Splunk

Vormetric Protection for Teradata Database

By aggregating massive volumes of enterprise data in Teradata environments, businesses can gain unprecedented insights and strategic value. Unfortunately, this very aggregation of data can also present unprecedented risks. Without proper protections, the sensitive assets compiled in these environments can inadvertently be exposed by privileged administrators, or be the target of theft by malicious insiders and external attackers. Now, Vormetric enables your organization to guard against these risks. Vormetric Protection for Teradata Database makes it fast and efficient to employ robust data-at-rest security capabilities in your Teradata environments.

TERADATA®

ROBUST SAFEGUARDS WHERE YOU NEED THEM MOST

With this solution, Vormetric simplifies the process of using column-level encryption in your Teradata database. The product reduces complexity for developers by offering documented, standards-based application programming interfaces (APIs) and user-defined functions (UDFs) that can be used to perform cryptographic and key management operations.

Vormetric Protection for Teradata Database offers granular protection, enabling encryption of specific fields and columns in Teradata databases. This solution uses the Vormetric Data Security Manager, a hardened, FIPS-certified appliance for administration and key storage. The Data Security Manager centrally manages and secures the policies and keys across the Teradata environment. In addition, policy enabled black or white lists deliver granular control of users who are allowed to encrypt or decrypt data in the Teradata Database.

Key Features

- Centralize your data-at-rest encryption and key management
- Enforce granular controls to enable administrators to do operational tasks, without accessing sensitive data in the clear
- High performance, scales with the number of Teradata nodes
- Teradata tested

Key Benefits

- Boost security without compromising the value of big data analytics
- Establish protections against cyber attacks and abuse by privileged users
- Deploy rapidly

Technical Specifications

- Supported platforms
  - o Teradata database, versions 14.0 and 14.10
  - o SUSE Linux Enterprise Server (SLES), versions 10 or 11 sp3
- User-defined functions (UDFs) for easy SQL code integration
- Column widths up to 1024 bytes
- Per column encryption key capable

ABOUT VORMETRIC

Vormetric's comprehensive high-performance data security platform helps companies move confidently and quickly. Our seamless and scalable platform is the most effective way to protect data wherever it resides—any file, database, and application in any server environment. Advanced transparent encryption, powerful access controls, and centralized key management let organizations encrypt everything efficiently, with minimal disruption. Regardless of content, database, or application—whether physical, virtual, or in the cloud—Vormetric Data Security enables confidence, speed, and trust by encrypting the data that builds business. Please visit: **www.vormetric.com** and find us on Twitter **@Vormetric**.

GLOBAL HEADQUARTERS

2545 N. 1ST STREET, SAN JOSE, CA 95131
TEL: +1.888.267.3732
FAX: +1.408.844.8638

EMEA HEADQUARTERS

200 BROOK DRIVE
GREEN PARK, READING, RG2 6UB
UNITED KINGDOM
TEL: +44.118.949.7711
FAX: +44.118.949.7001

APAC HEADQUARTERS

LEVEL 42 SUNTEC TOWER THREE
8 TEMASEK BOULEVARD
SINGAPORE 038988
TEL: +65 6829 2266

WWW.VORMETRIC.COM

02122016