thalesgroup.com

THALES

Vormetric Data Security Platform Data Sheet

Vormetric Data Security Platform

As security breaches continue to happen with alarming regularity and data protection compliance mandates get more stringent, your organization needs to extend data protection across more environments, systems, applications, processes and users. With the Vormetric Data Security Platform from Thales, you can effectively manage data-at-rest security across your entire organization.

The Vormetric Data Security Platform is composed of an integrated suite of products built on a common, extensible infrastructure with efficient, centralized key and policy management. As a result, your security teams can address your data security policies, compliance mandates and best practices, while reducing administration effort and total cost of ownership.

The platform offers capabilities for protecting and controlling access to databases, files and containers—and can secure assets residing in cloud, virtual, big data and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements, and it prepares your organization to nimbly respond when the next security challenge or compliance requirement arises.

Capabilities

- Transparent encryption for files, databases and containers
- Application-layer encryption
- Tokenization
- Dynamic and static data masking
- FIPS 140-2, Common Criteria certified key management
- Cloud Key Management
- Privileged user access control
- Access audit logging
- Batch data encryption and tokenization

Environment and technology support

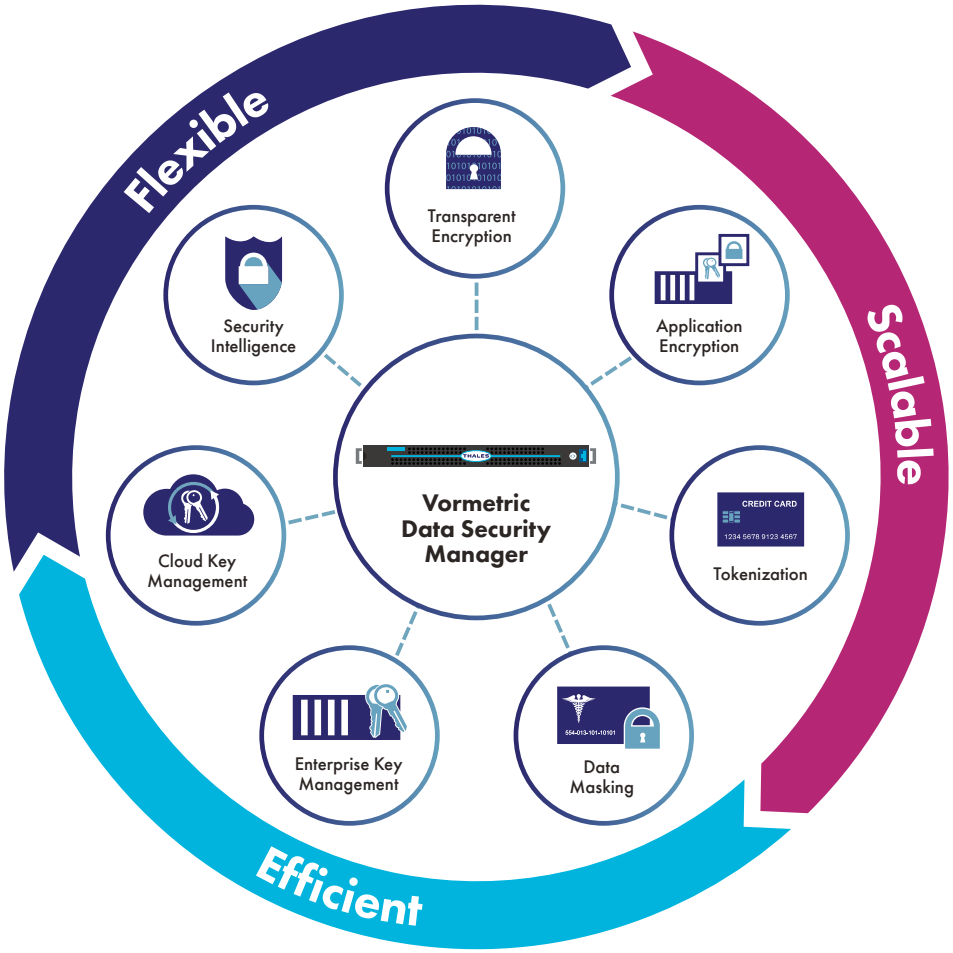
- IaaS, PaaS and SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, Microsoft Office365 and PCF: MySQL databases within Pivotal Cloud Foundry
- OSs: Linux, Windows and Unix
- Big data: Hadoop, NoSQL, SAP HANA and Teradata
- Container: Docker, Red Hat OpenShift
- Database: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase and others
- Any storage environment

Platform advantages

- Centralized data-at-rest security policies
- Manage keys for Vormetric Data Security Platform and third-party encryption products
- Consistent security and compliance across physical, virtual, cloud and big data environments
- Pre-defined SIEM dashboards deliver granular, actionable file-access intelligence
- Flexibility and extensibility enable fast support of additional use cases
- Integrate with supported HSMs and other third party sources for data encryption key
- Use supported HSMs as the secure root of trust for high levels of assurance including FIPS 140-2 Level 3 certification

Compliance

- PCI DSS
- GDPR
- HIPAA/HITECH
- NIST 800-53
- FISMA
- PIPA
- Regional data residency and privacy requirements



Strengthen security and compliance

By leveraging these flexible and scalable solutions, security teams can address a broad set of use cases and protect sensitive data across the organization. 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 General Data Protection Regulation (GDPR),
the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and regional data protection and privacy laws. The Vormetric Data Security Platform equips organizations with powerful tools to combat external threats, guard against insider abuse and establish persistent controls, even when data is stored in the cloud or any external provider's infrastructure.

Maximize staff and resource efficiency

The Vormetric Data Security Platform makes administration simple and efficient, offering an intuitive Web-based interface, a command-line interface (CLI) and application programming interfaces (APIs) including support for REST, Java, .Net, and C. With this solution, you can apply data-at-rest security quickly and consistently, maximizing staff efficiency and productivity. Plus, 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 isolated 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. The centralized management environment for all Vormetric Data Security Platform products. Provides policy control as well as secure generation, management and storage of encryption keys. Includes a Web-based console, CLI, SOAP and REST APIs. Available as FIPS 140-2 and Common Criteria certified virtual and physical appliances.

Vormetric Transparent Encryption. Built around a software agent that runs on a server to protect data-at-rest in files, volumes or databases on-premises, in the cloud, or in hybrid cloud environments. Features hardware accelerated encryption, least-privilege access controls and data access audit logging across data center, cloud and hybrid deployments. Features these extensions and additions:

- **Container Security.** Establishes controls inside of Docker™ and OpenShift™ containers, so you can ensure other containers and processes and even the host OS can't access sensitive data. Provides capabilities you need to apply encryption, access control and data access logging on a per-or within-container basis.
- **Live Data Transformation.** Enables encryption and periodic key rotation of files and databases—even while in use—without disruption to users, applications and business workflows.
- **Vormetric Transparent Encryption for Efficient Storage.** Provides a high degree of security for data stored on storage systems by encrypting data while retaining critical storage efficiencies, such as deduplication and compression. Offers the best data protection possible while maintaining storage efficiency — an industry first solution!
- **Vormetric Transparent Encryption for SAP HANA.** Provides advanced data-at-rest encryption, access control, key management and data access audit logging across SAP HANA implementations and environments

Vormetric Tokenization with Dynamic Data Masking. Vormetric Tokenization makes it easy to add random or format-preserving format-preserving tokenization to protect sensitive fields in databases and policy-based dynamic data masking for display security.

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

Vormetric Batch Data Transformation. Makes it fast and easy to mask, tokenize or encrypt sensitive column information in databases. Can be employed before protecting existing sensitive data with Vormetric Tokenization or Vormetric Application Encryption. Delivers static data masking services.

Vormetric Key Management. Provides unified key management to centralize management and secure storage of keys for Vormetric Data Security Platform products, TDE, and KMIP-compliant clients as well as securely storing certificates.

CipherTrust Cloud Key Manager. Manages encryption keys for Salesforce, Microsoft Azure and AWS that addresses enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments – and without the need for enterprises to become cryptographic experts. Available for private cloud or on-premises deployment.

Vormetric Protection for Teradata Database. Makes it fast and efficient to employ robust data-at-rest security capabilities in your Teradata environments. Offers granular protection, enabling encryption of specific fields and columns in Teradata databases.

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

Vormetric Data Security Manager

The Vormetric Data Security Manager (DSM) centralizes management and policy for all Vormetric Data Security Platform products. The DSM enables organizations to efficiently address compliance requirements, regulatory mandates and industry best practices, and to adapt as deployments and requirements evolve. The DSM and the products it manages are integrated with user and group identity management systems such as LDAP, Active Directory, local user databases, Hadoop and container environments—offering best-practice management of security policies and deployments.

Secure, reliable, and FIPS-certified system

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.

Flexible implementation options

The DSM is offered as a FIPS 140-2 Level 1 virtual appliance, as well as two hardware appliances: The V6000, which is FIPS 140-2 Level 2 certified, and the V6100, which is FIPS 140-2 Level 3 certified. The virtual appliance is available in VMware, HyperV, KVM, Amazon Web Services, and Azure compatible formats.

Supported HSMs can also provide a FIPS 140-2 Level 3 root of trust for virtual or v6000 hardware Vormetric Data Security Management appliances.

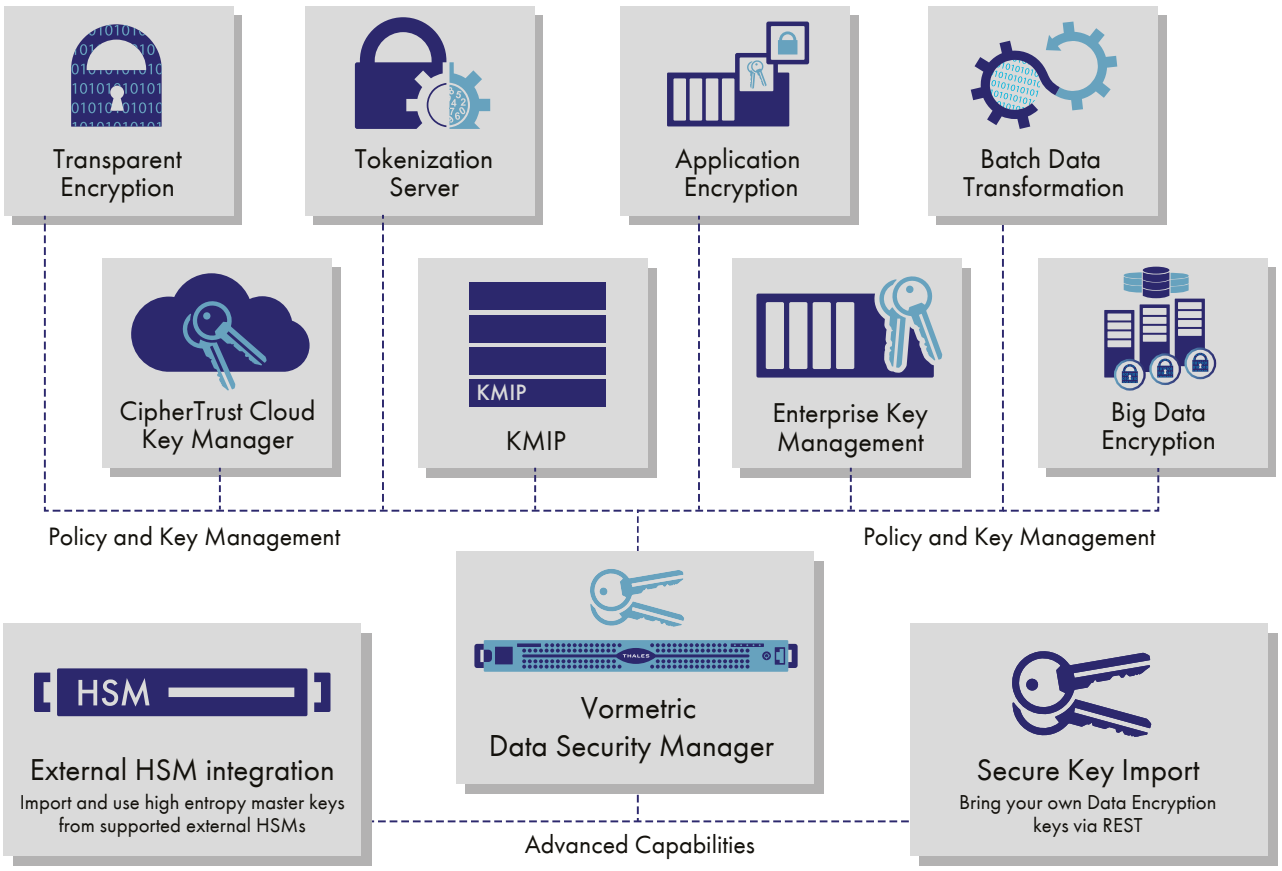
Key features

- Single console for all platform policy and key management
- Multi-tenancy support
- Proven scale to 10,000+ agents
- Clustering for high availability
- Toolkit and programmatic interface
- Easy integration with existing authentication infrastructure
- RESTful API support
- Multi-factor authentication and internal HSM
- Remote Administration

Technical specifications

Platform options:

- FIPS 140-2 Level 1 virtual appliance (FIPS 140-2 Level 3 root of trust available with supported external HSMs)
- FIPS 140-2 Level 2 hardware appliance (FIPS 140-2 Level 3 root of trust available with supported external HSMs)
- FIPS 140-2 Level 3 Hardware appliance (Includes internal HSM)
- The virtual appliance is available in VMware, HyperV, KVM, Amazon Web Services, and Azure compatible formats



Unified management and administration across the hybrid enterprise

The DSM minimizes capital and expense costs by providing central management of heterogeneous encryption keys, including keys generated for Vormetric Data Security Platform products, IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE and KMIP-compliant encryption products. The DSM features an intuitive Web-based console and APIs for managing encryption keys, policies, and auditing across an enterprise. The product also centralizes log collection.

DSM specifications

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, BIS certifications
FIPS 140-2 Level 3	V6100 model is equiped with an internal HSM FIPS 140-2 Level 3 root of trust available for V6100 and virtual DSMs via integration with supported HSMs
HSM Remote Administration	V6100 only; requires optional Remote Administration kit

Software Specifications

Administrative Interfaces	Secure Web, CLI, REST
Number of Management Domains	1,000+
API Support	PKCS #11, Microsoft Extensible Key Management (EKM), REST
Security Authentication	Username/Password, RSA multi-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, 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 Virtual Appliance

Number of CPUs	2
RAM (GB)	4
Hard Disk (GB)	100GB
Support Thin Provisioning	Yes

Vormetric Transparent Encryption

Vormetric Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging that helps organizations meet compliance reporting and best practice requirements for protecting data, wherever it resides.

This solution's transparent approach protects structured databases, unstructured files, and linked cloud storage accessible from systems on-premises, across multiple cloud environments, and even within big data and container implementations. Designed to meet data security requirements with minimal disruption, effort, and cost, implementation is seamless – keeping both business and operational processes working without changes even during deployment and roll out.

Meet compliance requirements for encryption and access control

Encryption, access controls and data access logging are basic requirements or recommended best practices for almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/Hitech, GDPR and many others. Vormetric Transparent Encryption delivers the controls required without operational or business process changes.

Scalable encryption

The Vormetric Transparent Encryption agent runs at the file system 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, container and big data environment – regardless of the underlying storage technology. Administrators perform all policy and key administration through the Vormetric DSM.

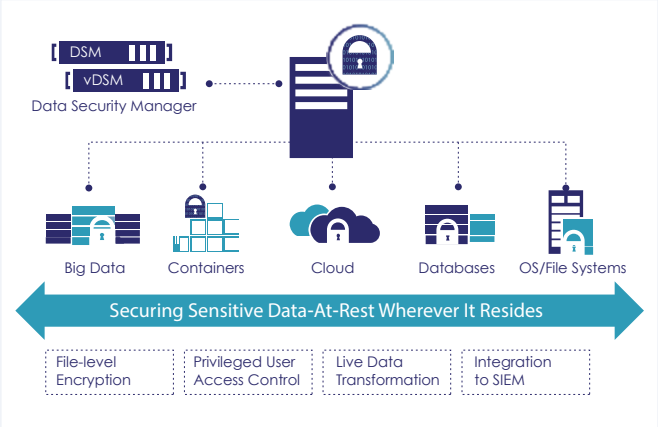
Encryption takes place on the server, eliminating bottlenecks that plague legacy, proxy-based solutions. Performance and scalability are further enhanced by leveraging cryptographic hardware modules that are built into such modern CPUs, such as Intel AES-NI and IBM POWER9.

Key benefits

- Meet compliance and best practice requirements for encryption and access control that scales easily across platforms and environments
- Easy to deploy: no application customization required
- Establish strong safeguards against abuse by privileged insiders

Key features

- Broadest platform support in industry: Windows, Linux and Unix operating systems
- High performance encryption: Uses hardware encryption capabilities built into host CPUs - Intel and AMD AES-NI and POWER9 AES encryption
- Suite B protocol support
- Log all permitted, denied and restricted access attempts from users, applications and processes
- Role-based access policies control who, what, where, when and how data can be accessed
- Enable privileged users to perform their work without access to clear-text data
- Extensions offer added capabilities, including more granular container support, comprehensive data protection while maintaining storage efficiency and zero-downtime data encryption capabilities



Vormetric Transparent Encryption secures data wherever it resides

Granular user access controls

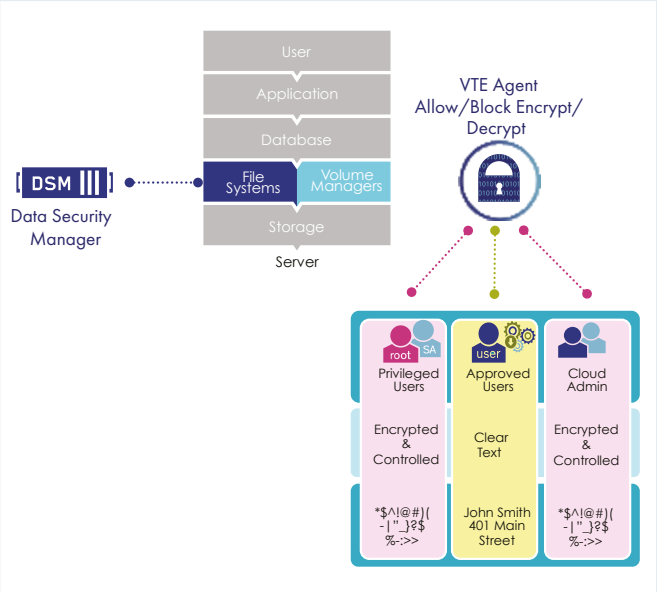
Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.

Non-intrusive and easy to deploy

Vormetric Transparent Encryption agents are deployed on servers at the file system or volume level and include support for Linux, Unix, Windows file systems as well as cloud storage environments like Amazon S3 and Azure Files. Deployment requires no changes to applications, user workflows, business practices or operational procedures.

Protect data on-premises or in-cloud

Keep control of your data by managing encryption keys and access policies from your local data center for both your on-premises and cloud data, even in hybrid environment deployments.



File-level encryption prevents privileged user abuse

Technical specifications

Encryption Algorithms

- AES, 3DES, ARIA

Extension Licenses

- Container Security
- Live Data Transformation
- Efficient Storage

Platform Support

- Microsoft: Windows Server 2019, 2016 and 2012
- Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu, Amazon Linux
- UNIX: IBM AIX*

Database Support

- IBM DB2, Microsoft SQL Server, Microsoft Exchange Data Availability Group (DAG), MySQL, NoSQL, Oracle, Sybase and others

Application Support

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

Big Data Support

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

Encryption Hardware Acceleration

- AMD and Intel AES-NI
- IBM POWER9 cryptographic coprocessor

Agent Certification

- FIPS 140-2 Level 1

Container Support

- Docker, Red Hat OpenShift

Cloud Support

- AWS: EBS, EFS, S3, S3I, S3 Glacier
- AZURE: Disk Storage, Azure Files
- PCF: MySQL databases within Pivotal Cloud Foundry

**IBM AIX only supported by Vormetric Transparent Encryption, version 5.3 agents*

Live Data Transformation

Deployment and management of data-at-rest encryption can present challenges when transforming clear-text to cipher-text, or when rekeying data that has already been encrypted. Traditionally, these efforts either required planned downtime or labor-intensive data cloning and synchronization efforts. Vormetric Transparent Encryption Live Data Transformation Extension eliminates these hurdles, enabling encryption and rekeying with unprecedented uptime and administrative efficiency.

Zero-downtime encryption and key rotation

Live Data Transformation delivers these key capabilities:

Zero-downtime encryption deployments. The solution enables administrators to encrypt data without downtime or disruption to users, applications or workflows. While encryption is underway, users and processes continue to interact with databases or file systems as usual.

Seamless, non-disruptive key rotation. Both security best practices and many regulatory mandates require periodic key rotation. Live Data Transformation makes it fast and efficient to address these requirements. With the solution, you can perform key rotation without having to duplicate data or take associated applications off line.

Intelligent resource management. Encrypting large data sets can require significant CPU resources for an extended time. Live Data Transformation provides sophisticated CPU use and I/O rate management capabilities so administrators can balance between the resource demands of encryption and other business operations. For example, an administrator can define a resource management rule specifying that, during business hours, encryption can only consume 10% of system CPU, while on nights and weekends, encryption can consume 70% of CPU.

Versioned backups and archives. With key versioning management, Live Data Transformation offers efficient backup and archive recovery that enable more immediate access. In a data recovery operation, archived encryption keys recovered from the Vormetric Data Security Manager are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys.

Key benefits

- Improve security and data availability with zero downtime encryption deployments
- Reduce costs associated with encryption implementation and maintenance
- Minimize encryption's impact on the user experience
- Leverage non-disruptive key rotation to enhance security and regulatory compliance
- Accelerate recovery of data encrypted with older keys

Technical specifications

Operating System Support

- Microsoft: Windows Server 2019, 2016 and 2012
- Linux: Red Hat Enterprise Linux (RHEL) 6 and 7 and 8, SuSE Linux Enterprise Server 11, 12 and 15

Cluster support

- Microsoft Cluster: File Cluster, SQL Server Cluster

Database support

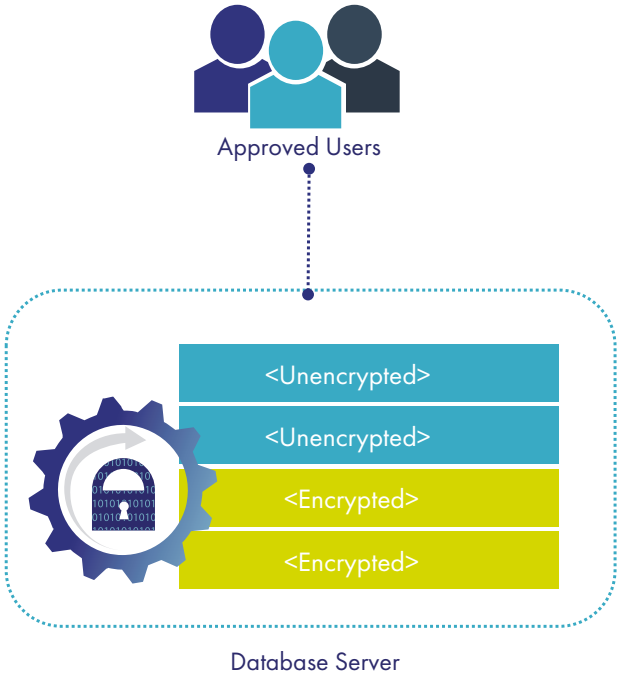
- IBM DB2, IBM Informix, Microsoft SQL Server, Oracle, Sybase and others

Big Data Support

- Cassandra, CouchBase, Hadoop, MongoDB, SAP HANA

Backup/Replication Support

- DB2 backup, NetBackup, NetWorker, NTBackup, Oracle Recovery Manager (RMAN), Windows Server Volume Shadow Copy Service (VSS)

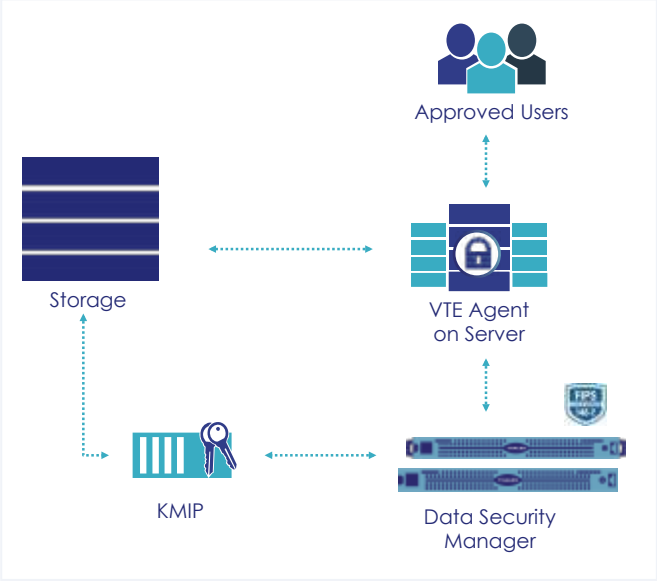


Vormetric Transparent Encryption Extensions and Additions

Vormetric Transparent Encryption for Efficient Storage

With VTE for Efficient Storage, users no longer need to make the choice between data security and storage efficiency. They can have both! The solution provides a high degree of security for data that is ultimately stored on enterprise storage systems by encrypting data while retaining critical storage efficiencies, such as deduplication and compression. VTE for Efficient Storage offers the best data protection possible while maintaining storage efficiency -- an industry first solution!

Using secure key sharing technologies between Vormetric Transparent Encryption and storage arrays, encrypted data from hosts running VTE can now be analyzed by enterprise storage solutions, compressed and deduplicated and then securely stored on the array in encrypted format. It's the best of both worlds.



Vormetric Transparent Encryption for Efficient Storage

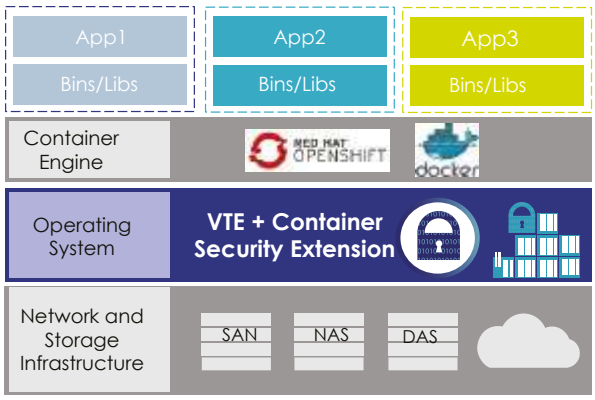
Vormetic Transparent Encryption for SAP HANA

Vormetric Transparent Encryption provides a proven approach to safeguarding SAP HANA data that meets rigorous security, data governance and compliance requirements. The solution can be quickly deployed, requiring no changes to SAP HANA or the underlying database or hardware infrastructure. With the solution, organizations can encrypt SAP HANA data and log volumes, and establish strong governance and separation of duties.

Vormetric Transparent Encryption Container Security

Vormetric Container Security extends policy driven Vormetric Transparent Encryption file-level encryption, access controls and data access audit logging to Docker and OpenShift container environments. The solution enables file-level encryption and access controls for container users, and data stored within, or accessed by, container images with no changes to container images required.

The solution features the detailed visibility and control needed to comply with compliance, regulatory and best practice requirements. Granular access policies provide privileged user access control within the container environment as well as at the underlying system level. Policies can include who, what, where, when and how sensitive data may be accessed.



Container Level Encryption

Container Security technical specifications

Platform/Environment Support

- Docker and Red Hat OpenShift
- Red Hat Enterprise Linux, 8.x
- Can run on physical systems, VMs and AWS EC2 instances

Vormetric Security Intelligence

Vormetric Security Intelligence delivers detailed, actionable security event logs that provide unprecedented insight into file access activities and that are pre-integrated leading SIEM solutions. Based on the data access audit logging capabilities available from Vormetric Transparent Encryption and the Vormetric Data Security Manager, this information can include all the detail about authorized data access as well as unauthorized access attempts wherever Vormetric Transparent Encryption agents are configured. Information from DSMs also includes actions of security administrators – another item required for compliance audit purposes.

These logs are available in the common formats used by SIEM systems, are centrally collected from the DSM, and prebuilt dashboards with our SIEM partners to make it easy for customers to see immediate value from this information. Dashboards show unauthorized access attempts and can be used to immediately alert on unauthorized access attempts.

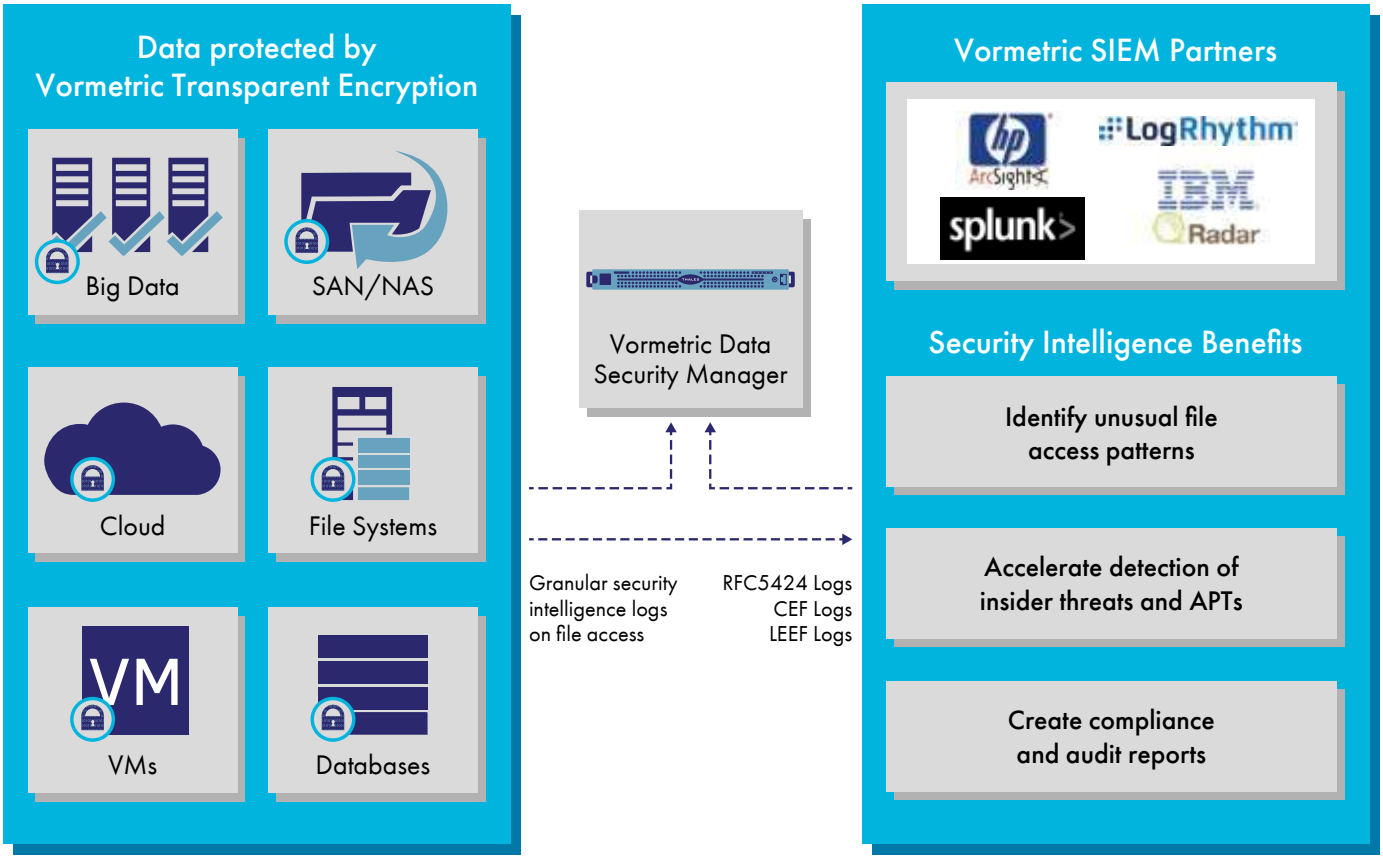
The data sets generated can also be used to create baselines of access patterns by users and applications accessing sensitive data. These baselines can then be used to identify unusual access patterns that may represent a threat.

Key capabilities

- Detect possible malware or malicious insiders making unauthorized access attempts
- Pinpoint unusual patterns of user access to protected data that indicate malware (or a malicious internal user) could be stealing data
- Monitor process access to protected data for anomalous patterns of use that could indicate a process has been co-opted by malware
- Identify attacks on the Vormetric Data Security Management appliance from unauthorized users

SIEM Partner Integrations

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



Vormetric Tokenization with Dynamic Data Masking

Vormetric Tokenization with Dynamic Data Masking reduces the cost and effort required to comply with security policies and regulatory mandates such as the European Union's Global Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS). You can secure and anonymize sensitive assets—whether they reside in the data center, big data environments or the cloud.

Streamlined tokenization

Vormetric Tokenization offers format-preserving or random tokenization to protect sensitive data. Policy-based dynamic data masking protects data in use. A RESTful API in combination with centralized management and services enables the implement tokenization with a single line of code per field. Centralized Tokenization Server management and configuration includes an operational dashboard with convenient tokenization configuration workflows in a graphical user interface.

Dynamic data masking. Policies define whether a field is returned fully or partially masked based on user identification controlled by an AD or LDAP server.

For example, the policies could enable customer service representatives to see only the last four digits of credit card numbers, while account receivables staff could access the full credit card number.

Non-disruptive. Format preserving tokenization protects sensitive data without changing the database schema.

Technical specifications

Tokenization capabilities:

- Format-preserving tokens (FF1 or FF3, alphanumeric/numeric) with irreversible option
- Random tokens (alphanumeric/numeric, data length up to 128K)
- Date tokenization
- Both FPE and random tokens can be configured to pass a Luhn check

Dynamic data masking capabilities:

- Policy based, number of left and/or right characters exposed, with customizable mask character

Deployment Form Factors and Options:

- Open Virtualization Format (.OVA) and International Organization for Standardization (.iso)
- Microsoft Hyper-V VHD
- Amazon Machine Image (.ami)
- Microsoft Azure Marketplace
- Google Cloud Platform

System requirements:

- Minimum hardware: 4 CPU cores, 16–32 GB RAM
- Minimum disk: 80GB

Application integration:

- RESTful APIs

Authentication integration:

- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)
- Client Certificate
- OAuth2

Performance:

- More than 1 million credit card size tokenization transactions per second, per token server (using multiple threads and batch (or vector) mode) on a 32-core server (dual-socket Xeon E5-2630v3) with 16 GB RAM

Vormetric Application Encryption

Vormetric Application Encryption delivers key management, signing, and encryption services enabling comprehensive protection of files, database fields, big data selections, or data in infrastructure as a service (IaaS) environments. The solution is FIPS 140-2 Level-1 certified, based on the PKCS#11 standard and fully documented with a range of practical, use-case based extensions to the standard. Vormetric Application Encryption accelerates development of customized data security solutions.

Streamline encryption implementations

Vormetric Application Encryption solution simplifies the process of adding key management and encryption to applications. Developers use RESTful API's, or C-, .NET- or Java-based applications linked with a local PKCS#11 library, to add standards-based secure key management and data encryption services to customized data security solutions.

Secure cloud, database and big data

Address policies and compliance mandates that require you to encrypt specific fields at the application layer, securing sensitive data before it is stored in database, big data, or cloud environments.

Technical specifications

Encryption Algorithms

- AES, 3DES, HMAC-SHA, HMAC MD5, RSA, FPE FF1/FF3

Supported environments:

- RESTful API on any server supporting web services; requires Vormetric Tokenization Server
- Key Services Provider (KSP) for Microsoft Crypto Next Generation (CNG)

OS and Language and/or Binding Support:

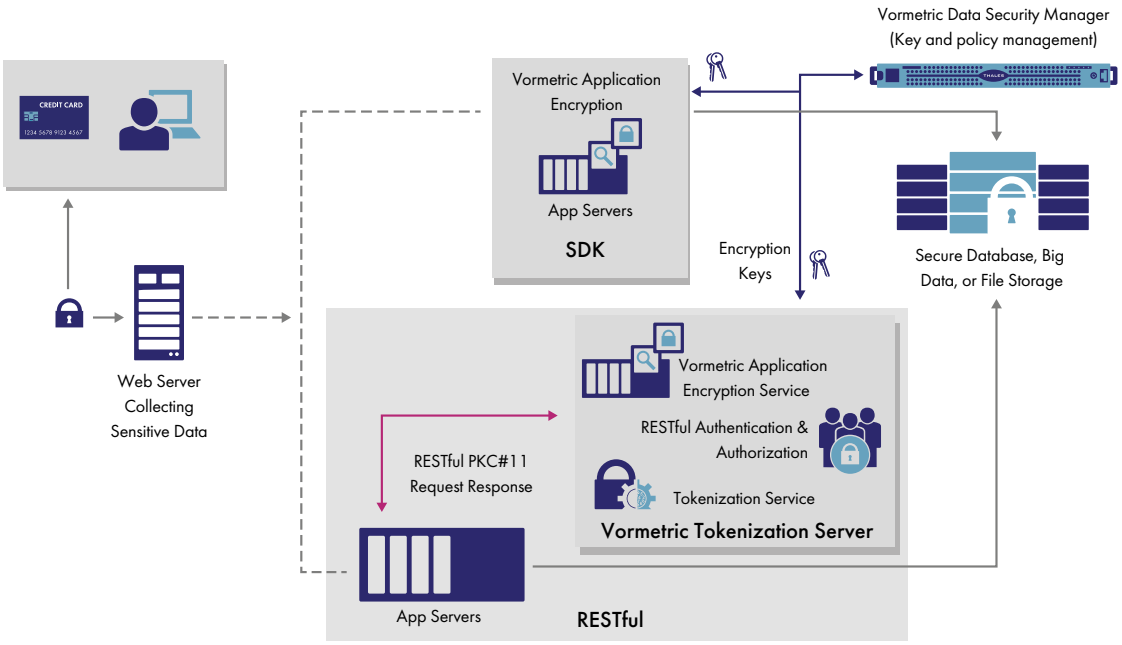
- Windows Server 2008/2012/2016: C, .NET, Oracle/Sun JDK
- Linux: C, Oracle/Sun JDK

Security Layers

- Separation of duties
- Host registration and host-level PIN
- Application-level key access
- RESTful user names and passwords or client certificates
- RESTful key usage and operational controls

Certification:

- FIPS 140-2 Level 1



Vormetric Application Encryption Customer Choice: SDK or RESTful

Vormetric Batch Data Transformation

Vormetric Batch Data Transformation provides static data masking services that enable secure, fast and efficient use of modern digital transformation initiatives such as data warehouses, big data on premises and in the cloud, sharing databases with DevOps, and outsourced data analysis.

Flexible data masking

Vormetric Batch Data Transformation leverages both Vormetric Application Encryption and Vormetric Tokenization with Dynamic Data Masking. Installed on a server already equipped with Vormetric Application Encryption, Batch Data Transformation utilizes Vormetric Application Encryption locally for encryption and key management and communicates with the Vormetric Tokenization Server for tokenization and data masking services.

Data security for digital transformation

Transformation options include either encryption or tokenization for files or supported databases.
Use cases include:

- Rapid data rekeying
- Safe database or data extract sharing with big data consumers, DevOps, or third parties
- Preparing data for safe cloud migration
- Preparing a database for tokenization or application-level encryption

Key benefits

- Enables new data uses with flexible security
- Accelerates deployment of Vormetric Tokenization with Dynamic Data Masking or custom applications based on Vormetric Application Encryption
- Leverages and expands existing investments in the Vormetric Data Security Platform

Technical specifications

Data Transformation Options:

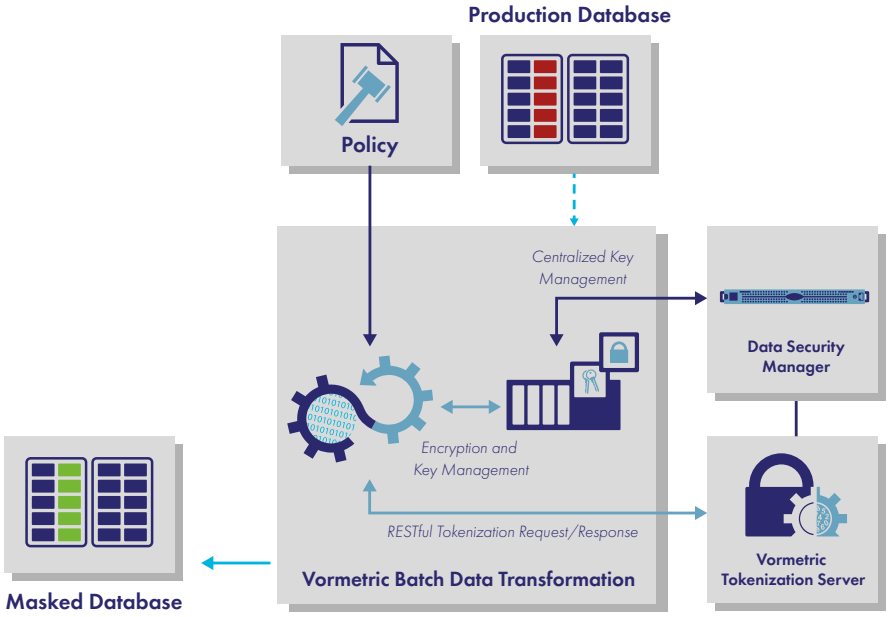
- Tokenization: Format Preserving FF1/FF3, Random Tokenization, Data Encryption: AES, FF1/FF3
- Formatting preserving alpha/numeric

Policy File Options:

- Specific action for each individual column transformation – encrypt, decrypt, tokenize, de-tokenize and re-key
- Easy to apply encryption without the need for application changes
- Flexible key management options – keys in DSM or server, multiple key support

Hardware and Operating System Requirements:

- Processor with 4 cores, 16GB RAM (minimum)
- Java Runtime Environment (JRE)
- Windows
- Linux – RedHat, CentOS, Ubuntu and SUSE



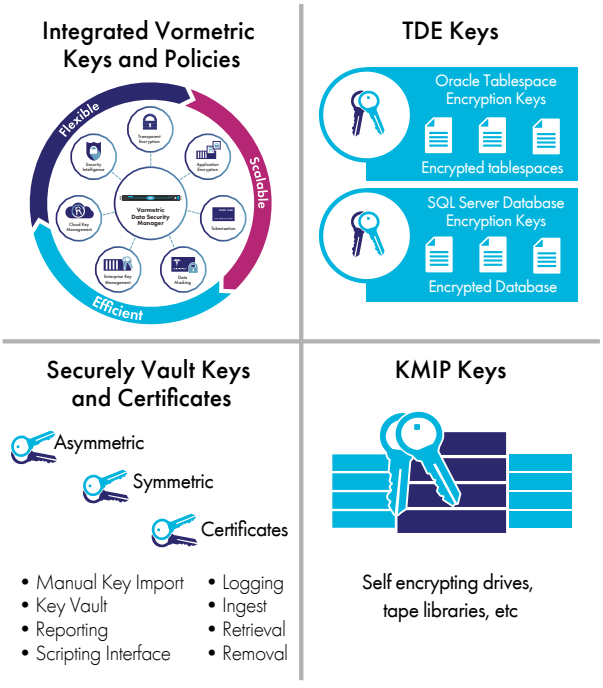
Vormetric Key Management

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

Simplify key management and certificate vaulting

Historically, as the number of applications and devices using encryption proliferated, there was a commensurate increase in the number of key management systems required. This growing number of key management systems made it more complex and costly to maintain highly available encrypted environments. Further, these disparate key management systems risk leaving 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 Data Security Platform solutions as well as keys and certificates from third-party products.



In addition, CipherTrust Cloud Key Manager enables you to leverage the bring-your-own-key services of cloud providers, while establishing full control over keys throughout their lifecycle.

Establish strong, auditable controls

Vormetric Key Management utilizes the Vormetric Data Security Manager (DSM) for key origination and storage. The DSM is offered as a FIPS 140-2 Level 1 certified virtual appliance and two hardware appliances: the DSM V6100 with FIPS 140-2 Level 3 certification equipped with an internal hardware security module, and the DSM V6000 with FIPS 140-2 Level 2 certification. For key management in the cloud, the virtual DSM also available for Amazon Web Services and in the Microsoft Azure Marketplace.

Key benefits

- Secure storage of certificates and keys
- Expiration notifications for certificates and keys
- Reports provide status and 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
- Command line scripts

Key and Certificate Formats for Search, Alerts, and Reports

- Symmetric encryption key algorithms: 3DES, AES128, AES256, ARIA128, ARIA256
- Asymmetric encryption key algorithms: RSA1024, RSA2048, RSA4096
- Digital certificates (X.509): DER, PEM, PKCS#7, PKCS#8, PKCS#12

Third-Party Encryption

- Microsoft SQL TDE, Oracle TDE, IBM Security Guardium Data Encryption, KMIP-clients
- Example partners: Nutanix, Linoma, NetApp, Cisco, MongoDB, DataStax, Huawei

API Support

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

Key Availability and Redundancy

- Secure replication of keys across multiple appliances with automated backups

CipherTrust Cloud Key Manager

Many cloud service providers offer data-at-rest encryption capabilities. Meanwhile, many data protection mandates require that encryption keys be stored and managed remote from the cloud service provider. "Bring Your Own Key" (BYOK) services and API's can fulfill these requirements.

Customer key control

BYOK-based customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them. Leveraging BYOK API's, the CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers full lifecycle control of encryption keys with centralized management and visibility.

Strong encryption key security

Customer key control requires secure key generation and storage. CipherTrust Cloud Key Manager leverages the security of the Vormetric Data Security Manager or supported HSMs to create and store keys.

IT efficiency and compliance tools

The combination of centralized key management for multiple cloud providers in a single browser window, automated key rotation, federated login for supported clouds, and management of native cloud keys offers enhanced IT efficiency. CipherTrust Cloud Key Manager cloud-specific logs and prepackaged reports enable fast compliance reporting.

Implementation Choices that Match Your Needs

CipherTrust Cloud Key Manager offers several convenient implementation choices to meet your security and deployment needs:

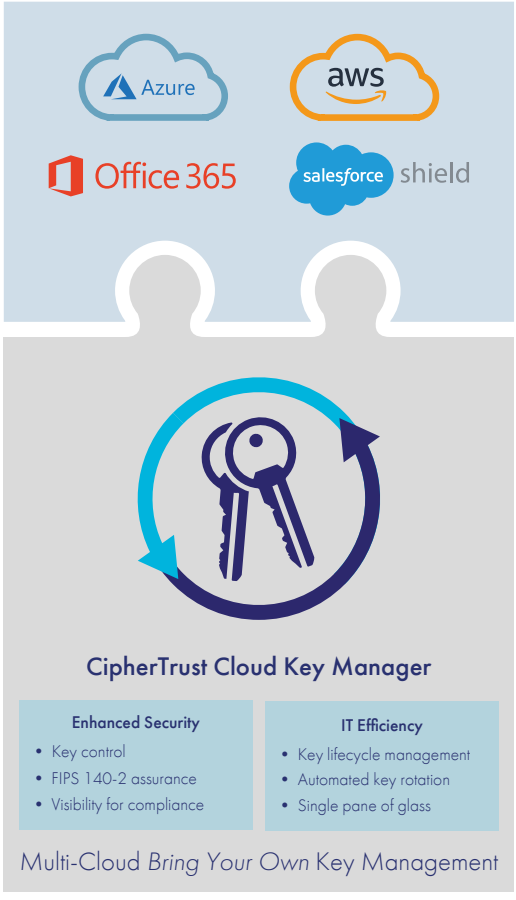
- All-software is available with FIPS 140-2 Level 1-certified key security. Both the CipherTrust Cloud Key Manager Virtual Appliance and virtual Data Security Manager can be instantiated in Amazon Web Services and Microsoft Azure, or deployed in any public or private cloud leveraging VMware.
- Customer that require FIPS 140-2 Level 3 or 2 can deploy or utilize existing Vormetric Data Security Manager appliances or supported HSMs in on-premises or hosted data centers.

Key benefits

- Leverage the value of "Bring Your Own Key" services with full-lifecycle cloud encryption key management. Lifecycle controls include automated key rotation based on basic or "on expiration" schedules, management of cloud-native keys for supported clouds), and full dynamic key meta-data management.
- Comply with the most stringent data protection mandates with up to FIPS 140-2 Level 3 validated key creation and storage
- Gain higher IT efficiency with centralized key management across multiple cloud environments

Supported cloud environments

- IaaS and PaaS: Microsoft Azure, Azure China and Germany National Clouds, Microsoft Azure Stack, Amazon Web Services
- SaaS: Microsoft Office365, Salesforce.com, Salesforce Sandbox



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.

Strengthen security while minimizing disruption and costs

Vormetric Protection for Teradata Database simplifies the process of securing sensitive records, enabling encryption of specific fields and columns in Teradata databases. The solution also offers NIST-approved format-preserving encryption (FPE) capabilities, so you can encrypt sensitive records without altering their format or field schemas. Not only does this minimize the potential impact of encryption on associated applications and workflows, but it helps you avoid the increased storage requirements associated with conventional encryption approaches. And the solution offers dynamic data masking, enabling you to present different levels of decryption and presentation of data to different users. In addition, you can install Vormetric Transparent Encryption Agents on the Teradata Appliance for Hadoop, extending protection from Teradata Database to Teradata big data analytics.

Key benefits

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

Key features

- Realize high performance, scaling with the number of Teradata nodes
- Leverage FPE that minimizes storage increase and disruption of encryption
- User-defined functions (UDF's) for encryption, tokenization, dynamic data masking and decryption easily integrate into existing SQL code
- Encryption with different keys for different columns
- Supports ASCII text and Unicode, enabling flexible language and technology support
- Certified Teradata encryption solution

Technical specifications

Encryption Algorithms

- AES, FPE (FF1, FF3)

Supported platforms:

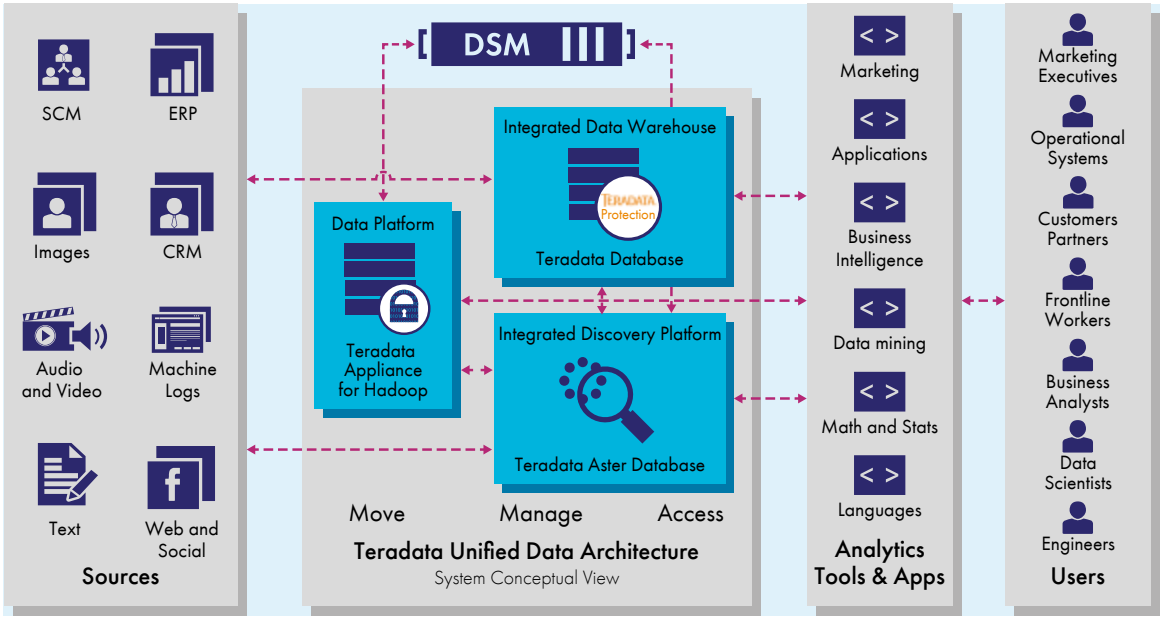
- Teradata database, versions 16.20 and below depending on SLES and product versions

Operating systems:

- SUSE Linux Enterprise Server (SLES), versions 10 or 11

Maximum column widths:

- ASCII: 16KB
- Unicode UDFs: 8KB



Streamline encryption deployment and usage

The solution reduces complexity for developers by offering documented, standards-based application programming interfaces (APIs) and user-defined functions (UDFs) that can be employed to perform cryptographic and key management operations. With the solution, Teradata users can set up their own easily configurable profiles for submitting encryption and decryption requests, including choosing from standard AES encryption and FPE.

Enabling centralized key and policy management

Vormetric Protection for Teradata Database works seamlessly with the Vormetric Data Security Manager (DSM), a hardened, FIPS-certified appliance for administration and key storage. With the DSM, you can centrally manage keys and access policies for Vormetric Protection for Teradata Database and Teradata Appliance for Hadoop, other Vormetric Data Security Platform solutions and third-party encryption products.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <