

«Thales eSecurity»

## Vormetric Data Security Platform



## VORMETRIC DATA SECURITY PLATFORM

As devastating security breaches continue to happen with alarming regularity and 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 eSecurity, you can effectively manage 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 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.

### 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 advanced persistent threats (APTs), 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

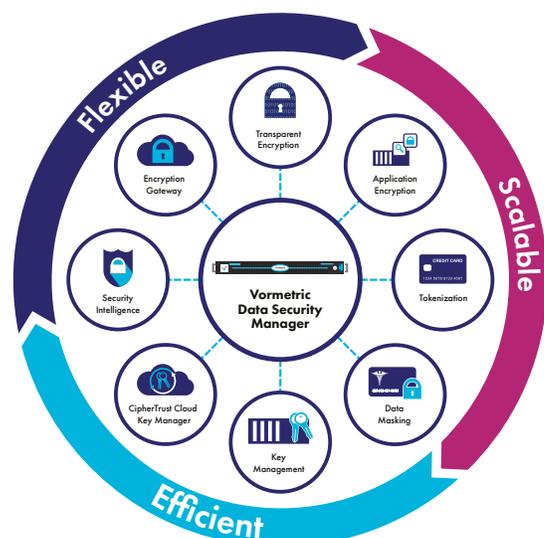
The Vormetric Data Security Platform makes administration simple and efficient, offering an intuitive Web-based interface, a command-line interface (CLI) and application programming interfaces (APIs) including support for REST, SOAP, Java, .Net, and C. With this solution, you can apply data-at-rest security quickly and consistently, maximizing staff efficiency and productivity. The platform also supports orchestration and automation using the Vormetric Orchestrator. Plus, this high-performance solution enables efficient use of virtual and physical server resources, reducing the load on the service delivery infrastructure.

### CAPABILITIES

- Transparent file encryption
- Application-layer encryption
- Tokenization
- Dynamic and static data masking
- Cloud storage encryption
- FIPS 140-2, Common Criteria certified key management
- Key management as a service
- Privileged user access control
- Access audit logging
- Batch data encryption and tokenization
- Orchestration and automation support

### ENVIRONMENT AND TECHNOLOGY SUPPORT

- IaaS, PaaS and SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, Amazon S3 (and compatible API services)
- 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

## COMPLIANCE

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



## 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.** Delivers centralized controls that enable consistent and repeatable management of encryption, access policies and security intelligence for all your structured and unstructured data. Available as FIPS 140-2 and Common Criteria certified virtual and physical appliances.
- **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. Features these two extensions:

- **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-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 Tokenization with Dynamic Data Masking.** Easy to implement 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 NIST-standard AES encryption 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 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 stores certificates.
- **CipherTrust Cloud Key Manager.** Manages encryption keys for Salesforce Shield Platform Encryption, Microsoft Azure KeyVault and AWS Key Management Services 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 as a cloud service offering, or for on-premises deployment.
- **Vormetric Cloud Encryption Gateway.** Enables organizations to safeguard files in such cloud storage environments as Amazon Simple Storage Services (Amazon S3) and other S3-compatible object storage services. Offers capabilities for encryption, on-premises key management and detailed logging.
- **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 Orchestrator.** Automates deployment, configuration, management and monitoring of select Vormetric Data Security Platform products. Offers capabilities that simplify operations, help eliminate errors and speed deployments by automating repetitive tasks.
- **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 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 solution can be integrated with LDAP directory services, so you can establish controls over users and groups and ensure security policies are enforced across the organization. The solution also provides the logs needed to support the strictest compliance requirements.

### 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 can address a range of unique environments and security requirements, and is available in several form factors:

- > Virtual appliance, which is FIPS 140-2 Level 1 certified.
- > V6000 hardware appliance, which is FIPS 140-2 Level 2 certified.
- > V6100 hardware appliance, which is FIPS 140-2 Level 3 certified and is equipped with a Thales nShield Solo hardware security module (HSM) that offers nShield remote access support.

The DSM is also available on the Amazon Web Services (AWS) and Microsoft Azure marketplaces.

### 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 nShield Remote Administration
- > Orchestration and automation support

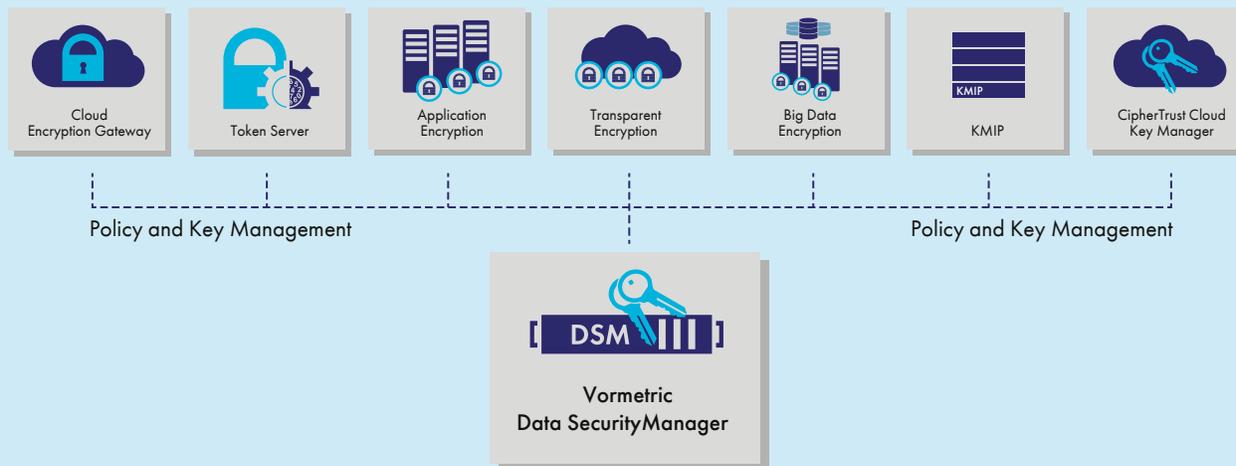
### TECHNICAL SPECIFICATIONS

#### Platform Options

- > FIPS 140-2 Level 1 Virtual Appliance
- > FIPS 140-2 Level 2 Hardware Appliance
- > FIPS 140-2 Level 3 Hardware Appliance
- > AWS and Azure marketplaces



The V6100 DSM offers nShield HSM secure remote administration with multi-factor smart card authentication



## UNIFIED MANAGEMENT AND ADMINISTRATION ACROSS THE HYBRID ENTERPRISE

The DSM minimizes costs by providing central management of heterogeneous encryption keys, including keys generated by 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

<b>Chassis</b>	1U rack-mountable; 17" wide x 20.5" long x 1.75" high (43.18 cm x 52.07cm x 4.5 cm)
<b>Weight</b>	V6000: 21.5 lbs (9.8 kg); V6100: 22 lbs (10 kg)
<b>Memory</b>	16GB
<b>Hard Disk</b>	Dual SAS RAID 1 configured with FIPS tamper-evident seals
<b>Serial Port</b>	1
<b>Ethernet</b>	2x1Gb
<b>IPMI</b>	1x10/100Mb
<b>Power Supplies</b>	2 removable 80+certified (100VAC-240VAC/50-60Hz) 400W
<b>Chassis Intrusion Detection</b>	Yes. Also includes FIPS tamper-evident seal on the top cover.
<b>Maximum BTU</b>	410 BTU max
<b>Operating Temperature</b>	10° to 35° C (50° to 95° F)
<b>Non-Operating Temperature</b>	-40° to 70° C (-40° to 158° F)
<b>Operating Relative Humidity</b>	8% to 90% (non-condensing)
<b>Non-Operating Relative Humidity</b>	5% to 95% (non-condensing)
<b>Safety Agency Approval</b>	FCC, UL, BIS certifications
<b>FIPS 140-2 Level 3 HSM</b>	V6100 model, which is equipped with an nShield Solo HSM
<b>HSM Remote Administration</b>	V6100 only; requires optional nShield Remote Administration kit

### Software Specifications

<b>Administrative Interfaces</b>	Secure Web, CLI, SOAP, REST
<b>Number of Management Domains</b>	1,000+
<b>API Support</b>	PKCS #11, Microsoft Extensible Key Management (EKM), SOAP, REST
<b>Security Authentication</b>	Username/Password, RSA multi-factor authentication (optional)
<b>Cluster Support</b>	Yes
<b>Backup</b>	Manual and scheduled secure backups. M of N key restoration.
<b>Network Management</b>	SNMP, NTP, Syslog-TCP
<b>Syslog Formats</b>	CEF, LEEF, RFC 5424
<b>Certifications and Validations</b>	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

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

## VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption delivers 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, Docker and cloud environments.

This solution's transparent approach enables organizations to implement encryption, without having to make changes to applications, infrastructure or business practices. Unlike other encryption solutions, protection does not end after the encryption key is applied. Vormetric Transparent Encryption continues to log access and enforce policies that protect against unauthorized access by users and processes. With these capabilities, you can ensure continuous protection and control of your data.

### ENABLING SCALABLE ENCRYPTION ACROSS ALL YOUR ENVIRONMENTS

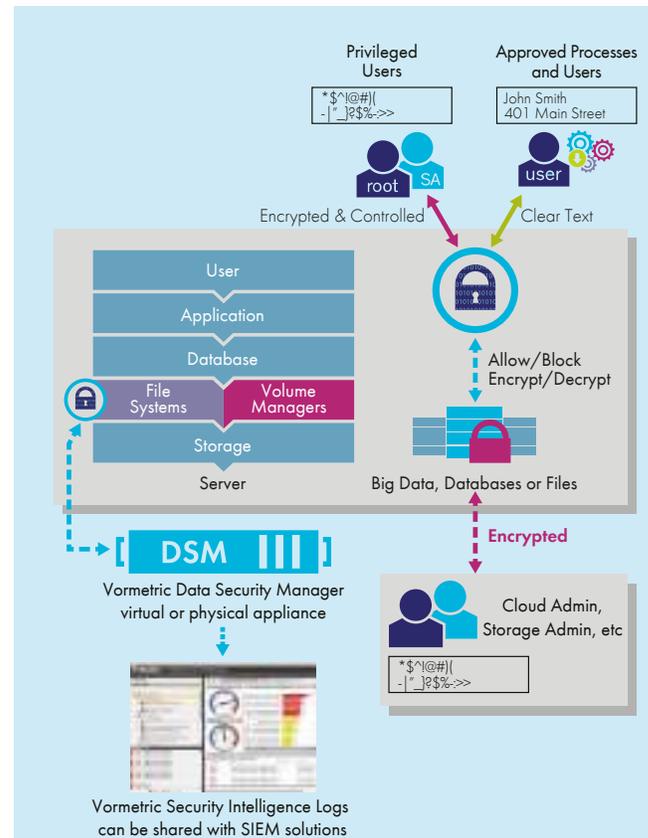
The Vormetric Transparent Encryption agent runs at the file system level or volume level on a server. The agent is available for a broad selection of Windows, Linux and Unix platforms, and can be used in physical, virtual, cloud, container and big data environments—regardless of the underlying storage technology. Administrators perform all policy and key administration through the Vormetric Data Security Manager (DSM).

The solution's agent-based architecture enables encryption to be performed on servers, eliminating bottlenecks that plague legacy, proxy-based solutions, which route all information through fixed nodes on networks. Performance and scalability are further enhanced by leveraging cryptographic hardware modules that are built into such modern CPUs, such as Intel AES-NI, IBM Power8 in-core and Oracle SPARC.

### POWERFUL AND GRANULAR USER ACCESS CONTROLS

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

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



### KEY BENEFITS

- > Scale encryption 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
- > Strong encryption and 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 and zero-downtime data encryption capabilities

## TECHNICAL SPECIFICATIONS

### Extension Licenses

- Container Security
- Live Data Transformation

### Platform Support

- Microsoft: Windows Server 2008 and 2012  
Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu
- UNIX: IBM AIX, HP-UX\*, Solaris\*

### Database Support

- IBM DB2, Microsoft SQL Server, 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 P8 cryptographic coprocessor
- SPARC encryption

### Agent Certification

- FIPS 140-2 Level 1

### Container Support

- Docker, Red Hat OpenShift

\*HP-UX and Solaris only supported by Vormetric Transparent Encryption, release 5.x agents

## CONTAINER SECURITY

Containers are bringing unprecedented benefits to organizations, but this technology also comes with new risks. Vormetric Container Security delivers critical capabilities for encryption, access controls and data access logging, so organizations can establish strong safeguards around data in dynamic container environments.

This solution is a software license for Vormetric Transparent Encryption that enables security teams to establish controls inside of containers. With this extension, encryption, access controls, and data access audit logging can be applied on a per-container basis, both to data inside of containers, and to external storage accessible from containers.

### MEET COMPLIANCE REQUIREMENTS

Today, many security teams have limited controls available for managing and tracking access to data that's held within containers and images. As a result, these teams are finding it difficult to comply with all their relevant internal security policies and regulatory mandates. This extension of Vormetric Transparent Encryption delivers the encryption, data access control and auditing capabilities you need to address compliance requirements and regulatory mandates. You can leverage the solution to protect sensitive data—whether you manage payment cards, healthcare records or other sensitive assets.

### ESTABLISH GRANULAR, COMPREHENSIVE SECURITY IN CONTAINER ENVIRONMENTS

Vormetric Container Security leverages open APIs and interfaces to enable policy-based encryption, access controls and data access audit logging for information stored within containers or accessed from containers. With this solution, you get rock solid operation, easy deployment and the strong protections you need to safely deploy production applications that use even the most sensitive information.

### EMPLOY STRONG SAFEGUARDS WITH OPTIMAL EFFICIENCY

Vormetric Container Security offers the following advantages:

- **Comprehensive safeguards.** Secure container volumes and protect data from being inappropriately accessed or exported.
- **Granular controls and visibility.** Establish granular access policies based on specific users, processes and resource sets. Create isolation between containers, so only authorized containers can access sensitive information.
- **Flexible, efficient deployment.** Employ controls in containers environments without having to make any changes to applications, containers or infrastructures.

### KEY BENEFITS

- Protect against root/privileged/unauthorized user access within containers
- Protect data against privilege escalation attacks from other containers
- Easily isolate data access between containers
- Meet compliance mandates for data access controls and container level auditing

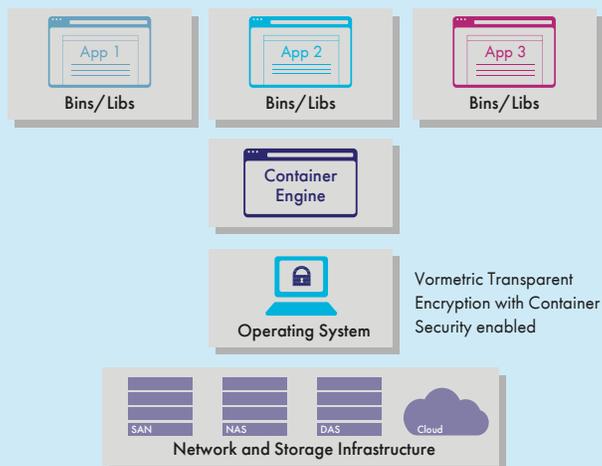
### KEY FEATURES

- Provides encryption, access controls, and data access audit logging, both for Docker and OpenShift hosts and images
- Offers controls that address data stored within containers, as well as data accessible from containers
- Enables granular controls for specific users, processes and resource sets
- Doesn't require any changes to applications, containers or infrastructure
- Uses the same agents and infrastructure set as Vormetric Transparent Encryption

### TECHNICAL SPECIFICATIONS

#### Platform/Environment Support

- Docker and Red Hat OpenShift
- Red Hat Enterprise Linux, 7.x
- Can run on physical systems, VMs and AWS EC2 instances



## 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

- Expand encryption implementations, while minimizing downtime and storage requirements
- 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 2008 and 2012
- Linux: Red Hat Enterprise Linux (RHEL) 6 and 7, SuSE Linux Enterprise Server 11 and 12

#### Cluster Support

- Veritas Cluster Server Active/Passive
- Microsoft Cluster: File Cluster, SQL Server Cluster

#### Database Support

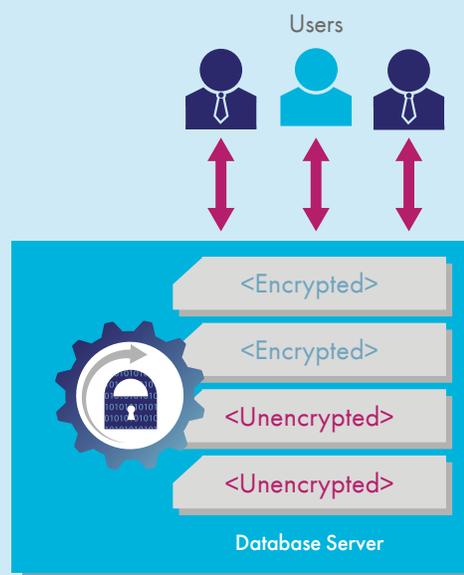
- IBM DB2, IBM Informix, Microsoft SQL Server, Oracle, Sybase and others

#### 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 TOKENIZATION WITH DYNAMIC DATA MASKING

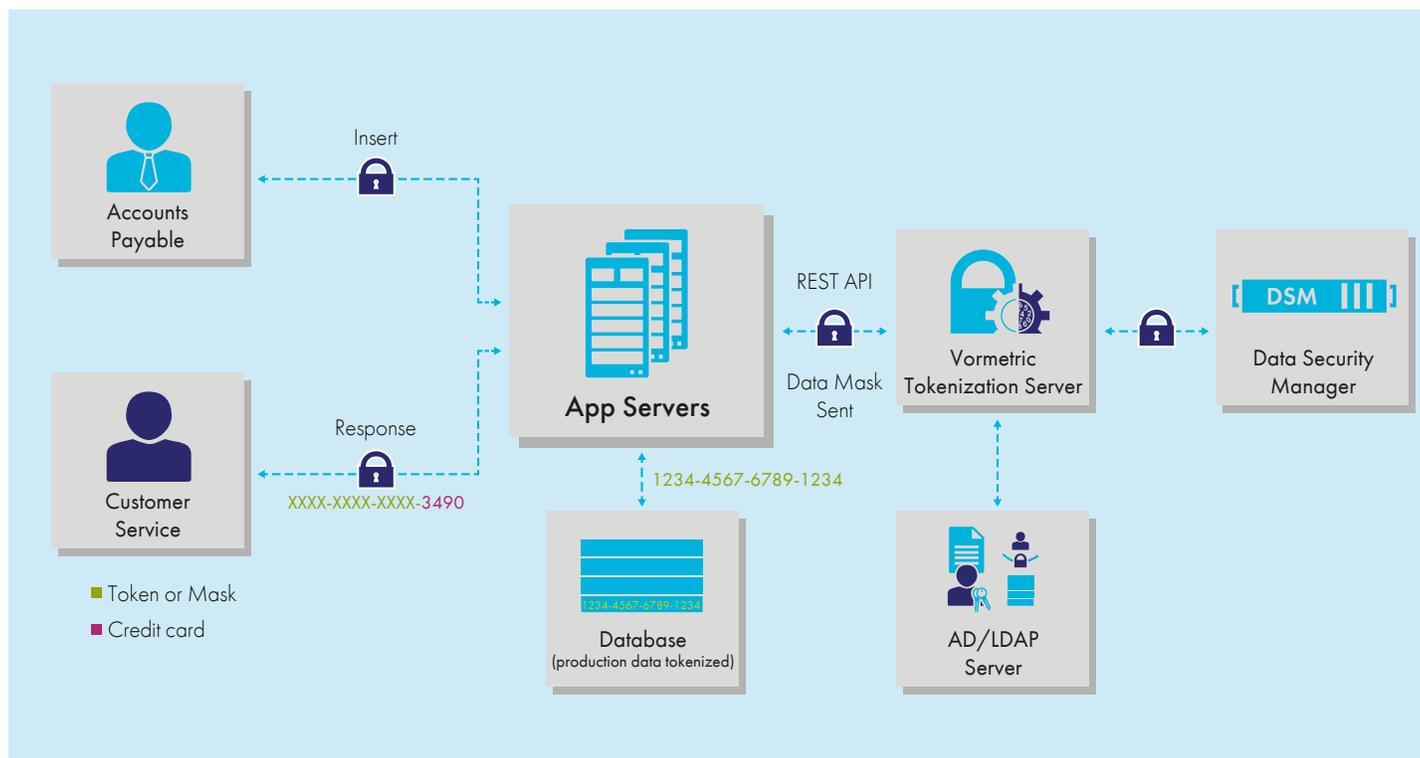
Vormetric Tokenization with Dynamic Data Masking dramatically reduces the cost and effort required to comply with security policies and regulatory mandates like the Payment Card Industry Data Security Standard (PCI DSS). The solution provides database tokenization and dynamic display security. Now, your organization can efficiently address its objectives for securing and anonymizing sensitive assets—whether they reside in the data center, big data environments or the cloud.

### STREAMLINED TOKENIZATION AND DYNAMIC DATA MASKING

Vormetric Tokenization makes it easy to use format-preserving tokenization to protect sensitive fields in databases and to add policy-based dynamic data masking to applications. The solution delivers the following advantages:

➤ **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 only receive 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.

- **Non-disruptive implementation.** With the solution's format-preserving tokenization capabilities, you can restrict access to sensitive assets without changing the existing database schema. The solution's REST API implementation makes it fast, simple and efficient for application developers to institute sophisticated tokenization capabilities.
- **Batch data transformation.** With this optional utility, you can tokenize high volumes of sensitive records without lengthy maintenance windows and downtime. You can mask sensitive columns in production databases and in copies of databases before they are sent to third-party developers and big data environments.



## KEY BENEFITS

- Reduce PCI DSS compliance effort and scope by minimizing servers requiring audit and control
- 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

## KEY FEATURES

- Virtual appliance enables fast increase and decrease in capacity
- Deploys in AWS, Microsoft Azure, virtualized and physical environments
- Optional batch data transformation utility streamlines large-scale tokenization
- Granular, policy-based dynamic data masking

## TECHNICAL SPECIFICATIONS

### Tokenization capabilities:

- Format Preserving FF1
- Cryptographic tokens (alpha/numeric)
- Random tokens (numbers only)
- Single and multi-use tokens
- Date tokenization

### Dynamic data masking capabilities:

- Policy based
- Alpha/numeric support
- Customize mask character

### Validation support:

- Luhn check

### Virtual appliance:

- Open Virtualization Format (.ovf)
- International Organization for Standardization (.iso)
- Amazon Machine Image (.ami)
- Microsoft Azure Marketplace

### System requirements:

- Minimum hardware: 4 CPU cores, 16 - 24 GB RAM
- Minimum disk: 80GB

### Application integration:

- REST APIs

### Authentication integration:

- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)

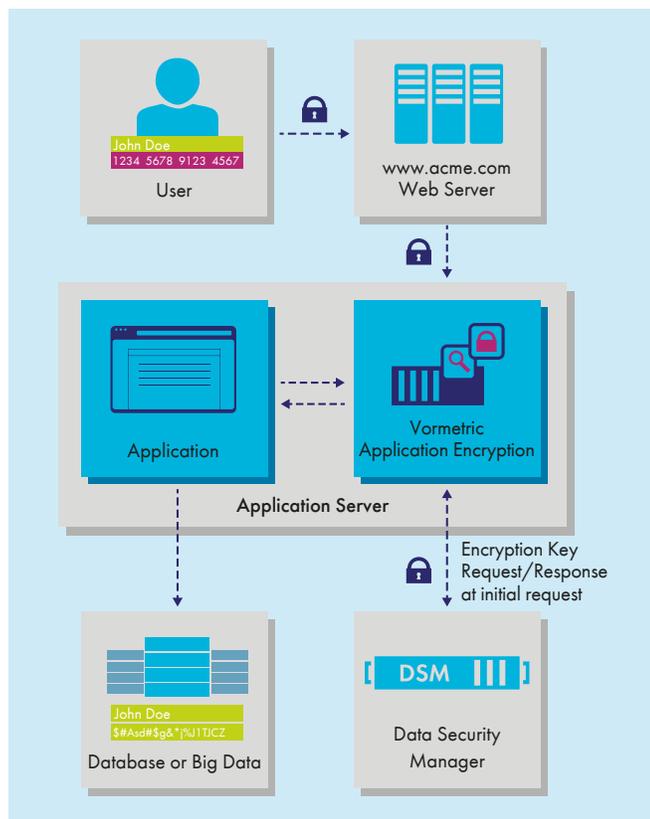
### Performance:

- 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 offers key management and encryption services for data, files, columns in databases, big data environments, and platform-as-a-service (PaaS) environments. 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 in-house encryption and key management services combined with an enterprise-grade secure key store.



### REDUCE APPLICATION-LAYER ENCRYPTION COMPLEXITY AND COSTS

Vormetric Application Encryption simplifies the process of adding encryption capabilities to existing applications. Developers link application code written in C, C# on .NET, or Java to the Vormetric Application Encryption library. The library executes all key management, encryption, decryption, and hash operations. A wide range of encryption mechanisms are supported including but not limited to AES-CBC and format-preserving encryption (FPE – FF1). Automated Key Versioning simplifies code design while complying with best practices around key life cycles. All keys are stored in the FIPS 140-2-compliant Vormetric Data Security Manager.

### ADDRESS COMPLIANCE MANDATES IN THE CLOUD AND BIG DATA ENVIRONMENTS

With the solution, you can address policies and compliance mandates that require encryption of specific fields at the application layer. The solution can encrypt sensitive data before it is stored in databases, big data repositories or PaaS environments.

### LEVERAGE THE VORMETRIC BATCH DATA TRANSFORMATION UTILITY

By leveraging Vormetric Batch Data Transformation, your organization can encrypt large data sets without lengthy maintenance windows and downtime—and without changing applications, networking configurations or storage architectures.

#### KEY BENEFITS

- > Eliminate the time, complexity and risk of building an in-house encryption solution
- > Centralize control of application-layer encryption and file system encryption
- > Secure sensitive data across a broad range of platforms and on-premises and PaaS environments
- > Stop malicious DBAs, cloud administrators, hackers and authorities with subpoenas from accessing valuable data
- > Streamline large-scale encryption migrations with Vormetric Batch Data Transformation utility

#### TECHNICAL SPECIFICATIONS

##### Supported environments:

- > Microsoft .NET 2.0 and higher
- > Java 7 and 8
- > C

##### Integration standard:

- > OASIS PKCS#11 APIs

##### Encryption:

- > AES
- > Format preserving encryption FF1

##### Operating systems:

- > Linux
- > Windows 2008 and 2012

##### Performance:

- > 400,000 credit card size encryption transactions per second (e.g. single thread, 32 core, 16GB, C)

##### Key administration:

- > Vormetric Data Security Manager

##### Character support:

- > ASCII
- > Unicode

##### Certification:

- > FIPS 140-2 Level 1

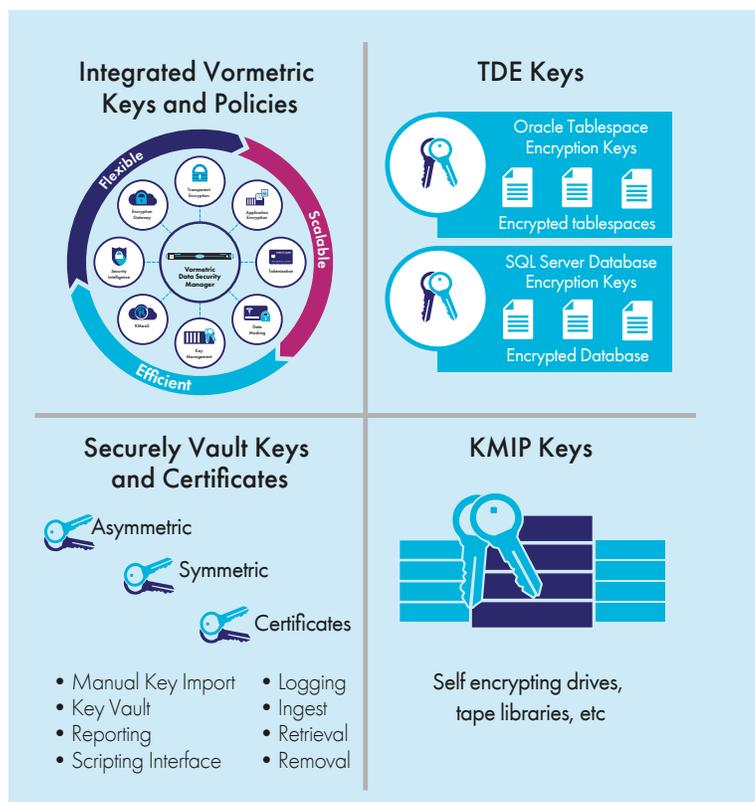
## VORMETRIC KEY MANAGEMENT

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. By consolidating key management, this product 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 devices employed. This growing number of key management systems 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 Data Security Platform solutions as well as keys and certificates from third-party products. In addition, Vormetric Key Management as a Service for cloud 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 offers all the reliability and availability capabilities of the Vormetric Data Security Manager (DSM). The DSM is offered as a virtual appliance and via two hardware appliances: The V6000 and the V6100. The V6100 is a FIPS 140-2 Level 3-certified appliance that is equipped with a Thales nShield Solo hardware security module (HSM). The platform is also available on Amazon Web Services and Microsoft Azure marketplaces.

#### KEY BENEFITS

- > Operational efficiency
- > Continuously available, secure storage and inventory of certificates and encryption keys
- > Alerts offer proactive notifications of expiring certificates and keys
- > 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

##### 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

Data-at-rest encryption capabilities offered by public cloud providers fall short of the needs of security- and compliance-conscious organizations concerned with providers' controlling the infrastructure and encryption that host their data, with little control and visibility on by whom and how their data is being accessed. To help alleviate these concerns, many leading providers offer "Bring Your Own Key" (BYOK) capabilities to enable customer control of the keys used for encrypting their data.

Leveraging cloud provider key control API's, the CipherTrust Cloud Key Manager gives customers lifecycle control of encryption keys with centralized management and visibility.

### COMPREHENSIVE KEY MANAGEMENT

Already created thousands of keys at your cloud provider? CipherTrust Cloud Key Manager will synchronize its database with keys created at the cloud provider. Key attributes, such as creation and expiration rules as well as key usage options are all maintained securely.

CipherTrust Cloud Key Manager offers multiple capabilities in support of enhanced IT efficiency:

- > Federated login to each cloud provider provides the simplest mechanism for granting user access to key data. Cloud service login is authenticated and authorized by the service provider.
- > Centralized Key Management gives you access to each supported cloud provider from a single web tab, with cloud provider-specific key terminology and semantics instantly presented.

### ON-PREMISES OR IN THE CLOUD: YOU DECIDE

CipherTrust Cloud Key Manager offers deployment models that fit your needs:

- > **CipherTrust Cloud Key Manager** as a service eliminates the need to architect, deploy and maintain a high-availability cloud key management solution on premises, with key storage in a FIPS 140-2 Level-1 certified virtual appliance.
- > **CipherTrust Cloud Key Manager** on-premises allows highly regulated organizations to store encryption keys on site, with key storage in Vormetric Data Security Manager (DSM) appliances offering up to FIPS 140-2 Level 3 certification.

### KEY BENEFITS

- > Leverage the value of "Bring Your Own Key" services with full-lifecycle cloud encryption key 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

### KEY FEATURES

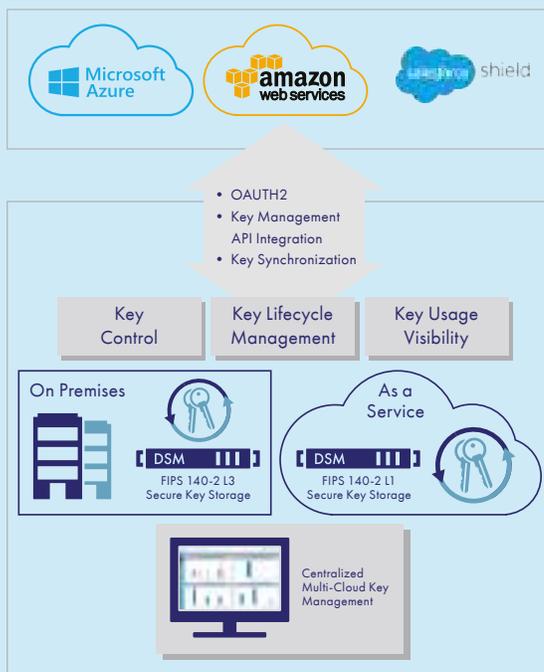
- > Separate key storage from data repositories
- > Comprehensive, granular logs of encryption key and certificate management activities
- > Push-button creation and modification of keys and policies
- > Easy-to-use portal for key lifecycle management

### SUPPORTED ENVIRONMENTS

- > Salesforce: Salesforce Platform Encryption
- > Microsoft Azure: Azure Key Vault
- > Amazon: AWS Key Management Service

### KEY MANAGEMENT SECURITY LEVELS

- > FIPS 140-2 Level 3 on-premises service
- > FIPS 140-2 Level 1 cloud service



## VORMETRIC CLOUD ENCRYPTION GATEWAY

The Vormetric Cloud Encryption Gateway enables you to safeguard files in cloud storage environments such as Amazon Simple Storage Service (Amazon S3) and other S3-compatible object storage services. The Cloud Encryption Gateway encrypts sensitive data before it is saved to the cloud storage environment and gives you control over encryption keys. The solution delivers the visibility and control you need to protect sensitive assets from a range of threats. The Cloud Encryption Gateway relies on the Vormetric Data Security Manager for key and policy management.

### ESTABLISH STRONG CONTROLS OVER DATA STORED IN THE CLOUD

The Vormetric Cloud Encryption Gateway is delivered as a virtual appliance that can be deployed in the cloud or in your data center. Either way, your security team always has complete control over encryption keys. The Cloud Encryption Gateway offers 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.
- **Strong key management.** Enables you to maintain granular, auditable control over policies and keys at all times.
- **Detailed visibility and auditability.** Delivers audit logs that provide granular visibility into file access, offering invaluable support for compliance reporting and forensics efforts.
- **Intelligent risk detection.** Monitors Amazon S3 and other cloud storage environments compatible with the S3 APIs. Discovers unencrypted files that violate security policies and automatically encrypts them.

### KEY FEATURES

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

### TECHNICAL SPECIFICATIONS

#### Open Virtualization Format Virtual Machine

- Min. hardware 4 CPU cores, 4GB RAM
- Min. disk 100GB

#### Amazon Machine Image (AMI)

- m4.xlarge with 4vCPUs 16GB
- 100GB EBS
- High Network Performance

#### Supported Services

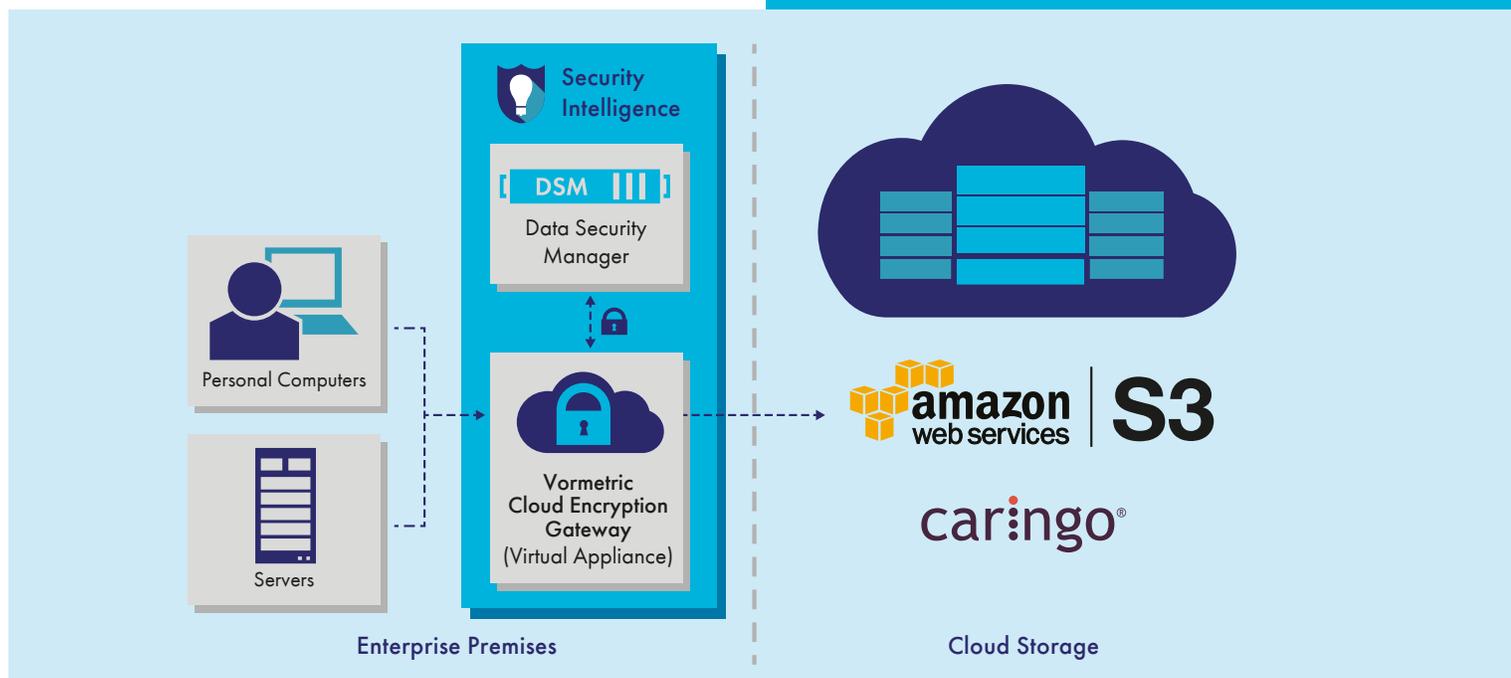
- Amazon S3
- Caringo Object Storage
- Key Management as a Service (KMaaS)

#### Authentication Integration

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

#### Policies

- Encrypt by file type
- Auto key rotation



## 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

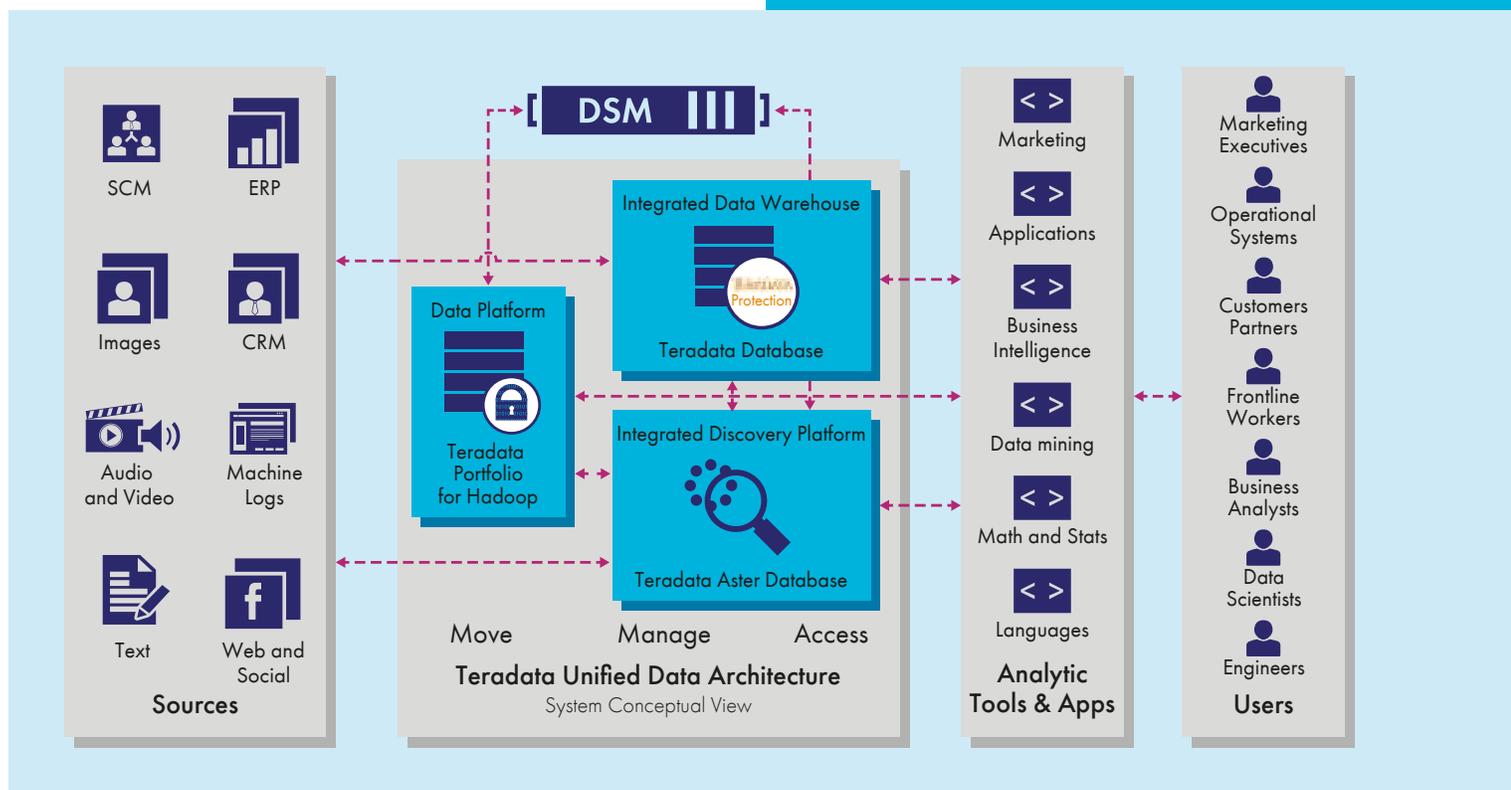
Vormetric Protection for Teradata Database simplifies the process of securing sensitive records, enabling encryption of specific fields and columns in Teradata databases. The solution also offers NIST-approved format-preserving encryption (FPE) capabilities, so you can encrypt sensitive records without 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.

### KEY BENEFITS

- Centralize and streamline your data-at-rest encryption and key management
- Boost security without compromising the value of big data analytics
- Establish protections against cyber attacks and abuse by privileged users
- Deploy rapidly

### KEY FEATURES

- Enforce granular controls so administrators can perform operational tasks, without accessing sensitive data in the clear
- Realize high performance, scaling with the number of Teradata nodes
- Leverage FPE that minimizes storage increase and disruption of encryption
- User-defined functions (UDFs) for encryption and decryption easily integrate into existing SQL code
- Enables customers to use different keys for different columns
- Supports ASCII text and Unicode, enabling flexible language and technology support
- Certified Teradata encryption solution



## 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, other Vormetric Data Security Platform solutions and third-party encryption products. With the DSM, you can manage keys and policies for Vormetric Transparent Encryption, which can be used to protect your Teradata Appliance for Hadoop.

## TECHNICAL SPECIFICATIONS

### Supported platforms:

- Teradata database, versions 14.0, 14.10, 15.0 and 15.10

### Operating systems:

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

### Maximum column widths:

- ASCII: 16KB
- Unicode UDFs: 8KB

## VORMETRIC SECURITY INTELLIGENCE

**Vormetric Security Intelligence delivers detailed, actionable security event logs that provide unprecedented insight into file access activities. With the solution, your organization can leverage immediate alerts that fuel automated escalation and response. These logs are easy to integrate with SIEM systems, so you can efficiently track and investigate suspicious activities and produce compliance and security reports.**

## DELIVERING GRANULAR, ACTIONABLE SECURITY INTELLIGENCE

Traditionally, SIEMs relied on logs from firewalls, IPS, and NetFlow devices. Because this intelligence is captured at the network layer, these systems can generate massive volumes of data, making it challenging for administrators to identify the events that really matter. Further, these systems also leave a commonly exploited blind spot: They don't provide any visibility into data access attempts and events occurring on servers. Vormetric Security Intelligence eliminates this blind spot, delivering targeted, critical insights into file access activities. As a result, the solution helps eliminate the threat of an unauthorized or compromised user account gaining stealthy access to sensitive data.

Vormetric Security Intelligence logs produce an auditable trail of permitted and denied access attempts from users and processes. The solution's detailed logs can be reviewed to specify when users and processes accessed data, under which policies, and if access requests were allowed or denied. These logs can be efficiently shared with your SIEM platform, helping 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.

## ACTIONABLE LOGS THAT FUEL FAST RESPONSE

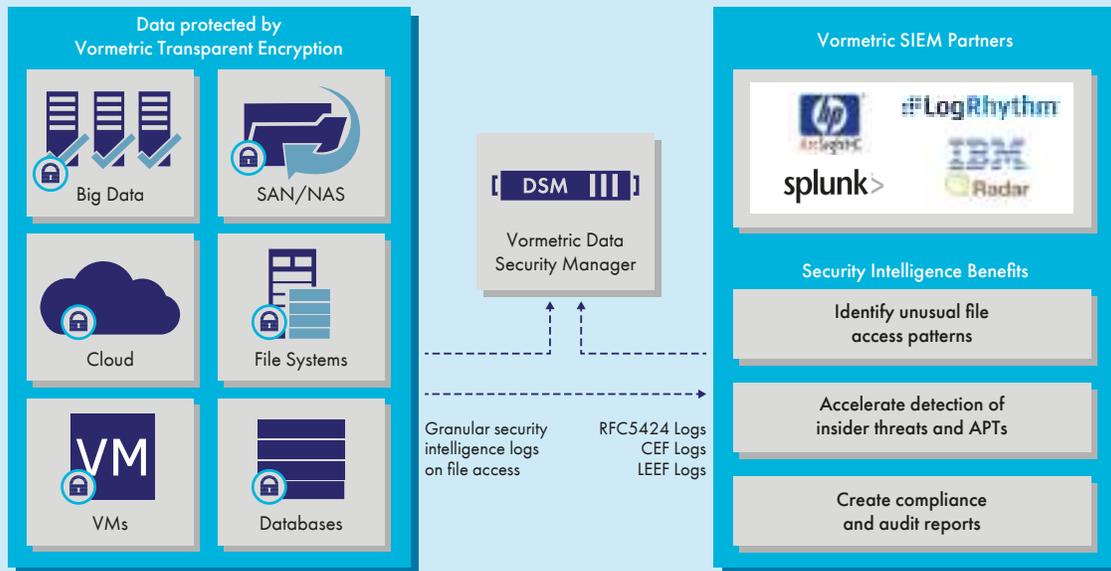
Vormetric Security Intelligence logs provide instantaneous insights that can be fed into your organization's security operations center, including any existing workflows and automated scripts you may have in place. As a result, Vormetric Security Intelligence enables you to ensure risks are identified, communicated, and acted upon in the fastest and most efficient manner.

## STREAMLINING AUDITING AND COMPLIANCE

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. With its detailed visibility and integration capabilities, Vormetric Security Intelligence helps streamline the effort associated with audits and ongoing compliance reporting.



# VORMETRIC SECURITY INTELLIGENCE



## KEY FEATURES

- > Enhanced visibility into sensitive data access
- > Instant alerts can trigger fast, automated response
- > 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

## TECHNICAL SPECIFICATIONS

### SIEM Partner Integration

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



## VORMETRIC ORCHESTRATOR

Vormetric Orchestrator automates deployment, configuration, management and monitoring of Vormetric Data Security Platform products. With these capabilities, organizations can scale their implementations across large enterprise data centers and hybrid cloud environments—while dramatically reducing administrative effort and total cost of ownership.

### AUTOMATION FUELS SCALABLE, EFFICIENT OPERATIONS

For large organizations and cloud service providers, the only certainty is change: changes to operating systems, workloads, databases and network configurations. Vormetric Orchestrator delivers the automation you need to keep pace with such changes. By automating repetitive tasks, the Orchestrator simplifies operations, helps eliminate errors and speeds deployments. The solution reduces the staff resources required to maintain and expand encryption deployments, so your teams can spend more time focusing on more urgent and strategic priorities. Vormetric Orchestrator offers these advantages:

- > **Increased operational efficiency through automation.** The solution delivers automatic deployment and maintenance of Vormetric Data Security Platform products. For example, in the event of a critical operating system patch, it's simple to set up a job that instructs the Orchestrator to automatically update hundreds of servers with a new version of a Vormetric Transparent Encryption agent.
- > **Efficient integration in your environment.** Vormetric Orchestrator features a plug-in architecture enabling fast integration with IT configuration management solutions such as Chef and Ansible.
- > **Flexible deployment options.** Vormetric Orchestrator is delivered as a virtual appliance for mainstream virtualization and public cloud platforms. When installed in your data center, the solution can manage Vormetric Data Security Platform products in remote data centers, private cloud environments and in public clouds.

### KEY BENEFITS

- > Leverage automation to accelerate deployments and boost operational efficiency
- > Scale encryption while reducing total cost of ownership
- > Harness broad environment support to expand encryption

### TECHNICAL SPECIFICATIONS

#### Open Virtualization Format Virtual Appliance Requirements

- > 4 virtual CPUs
- > Minimum memory: 4GB

#### Amazon Machine Image (AMI) requirements

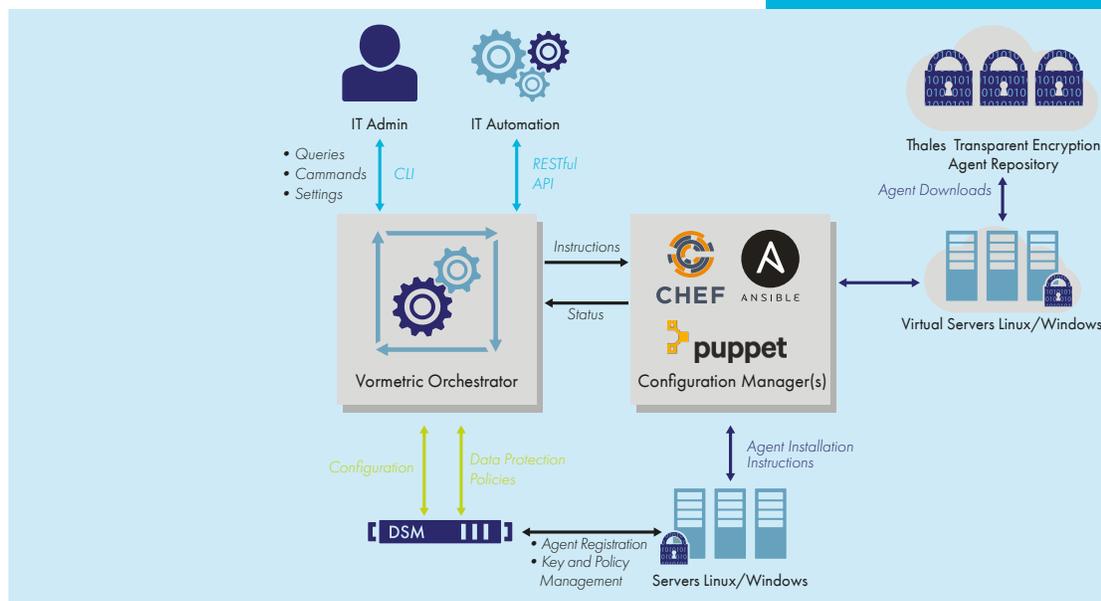
- > 4 Virtual CPUs
- > Minimum Memory 4GB

#### Configuration Manager Support

- > Chef (multiple Chef Servers supported)
- > Ansible
- > Puppet

#### Automation Support

- > Vormetric Transparent Encryption Agents
  - > Agent Installation
  - > Agent Registration Mechanisms
    - > Shared Secret
    - > Fingerprint
  - > Agent Updates
- > Vormetric Data Security Manager Configuration



## About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

