THALES

www.thalesesecurity.com

‹Thales e-security›

Vormetric Data Security Platform Architecture

A technical introduction to the Vormetric Data Security Platform, including select products, use cases and deployment models

White Paper

Contents

Executive Summary

As security teams struggle to contend with more frequent, costly, and sophisticated attacks, data-at-rest encryption becomes an increasingly critical safeguard. This white paper offers an overview of the different encryption approaches available today. The paper then provides an introduction to the Vormetric Data Security Platform and shows how it uniquely addresses the requirements for data-at-rest encryption across a modern enterprise environment. The paper offers details on the platform's architecture, and reveals how this architecture helps maximize the security of sensitive assets, while minimizing total cost of ownership. Thales also offers detailed architecture white papers for many of the products covered in this document.

Introduction

Today's enterprise security teams have a lot on their plates and a lot on their minds. The attacks they are supposed to guard against are getting more sophisticated, persistent, and, worst of all, effective. Insider threats continue to be the Achilles heel of many security organizations. According to the 2017 Thales Data Threat Report[1], 88% feel at least somewhat vulnerable to data threats. The report also proves those concerns are well founded: 42% of organizations experienced a data breach at some point.

Further, the financial ramifications of these breaches continue to grow. Consider just a few statistics from the most recent "Cost of Data Breach Study" by the Ponemon Institute[2]:

- The average total cost of a data breach was $3.8 million, a figure that increased 23% since 2013.
- The average cost paid per compromised record grew more than six percent, and now stands at $154 per record.

Making challenges even more daunting is the fact that the IT landscape continues to undergo fundamental and fast change. As businesses grow increasingly reliant on virtualized environments, cloud services, and big data analytics, the security risks and requirements change substantially.

While security teams strive to contend with these changes and stay in front of escalating threats, they are increasingly focusing on leveraging encryption to protect sensitive data where it resides in abundance: stored files and databases. However, while demand for data-at-rest encryption is increasing, so too is the pressure to boost efficiency and agility. Quite simply, security teams need to support these increasing demands and respond more quickly, without spending a lot more or hiring a lot more staff.

As they implement plans for balancing all these competing demands, security leadership needs to intelligently evaluate the options available, and select the approaches and solutions that are best aligned with their technical, security, and business objectives. The following section offers an overview of the different data-at-rest encryption approaches that security organizations can employ.

1 — 2017 Thales Data Threat Report features polling and analysis by 451 Research. Find the report here: http://dtr.thalesesecurity.com

2 — Ponemon Institute, Cost of Data Breach Study: Global Analysis, www.ibm.com/security/data-breach

Data-At-Rest Encryption

APPROACHES AND ALTERNATIVES

Encryption is the process of encoding sensitive data so that only authorized parties can read it. There are four levels in the technology stack in which encryption is typically employed: full-disk or media, files, databases, and applications.

In general, when encryption is employed lower in the stack, it is less likely to interfere with operations in the layers above. For example, if the encryption occurs in the disk level, there is very little risk of any impact on the file, database, or application layers. The file, database, and application layers can access decrypted data and will function the same as before. However, with this simplicity comes very little protection. Once the media is booted with the encryption key, all the data is in the clear and at full exposure to insider and external threats.

On the other hand, if encryption or tokenization occurs in the application layer, data is encrypted right at the source, before it leaves the application or e-commerce server. While this approach offers significantly increased security as it protects from any access that is not using the authorized applications, it is typically more complex, costly, and time consuming to implement because application developers need to modify every application that will require access to the encrypted data.

Following are more details on the advantages and disadvantages of encryption at each level in the technology stack.

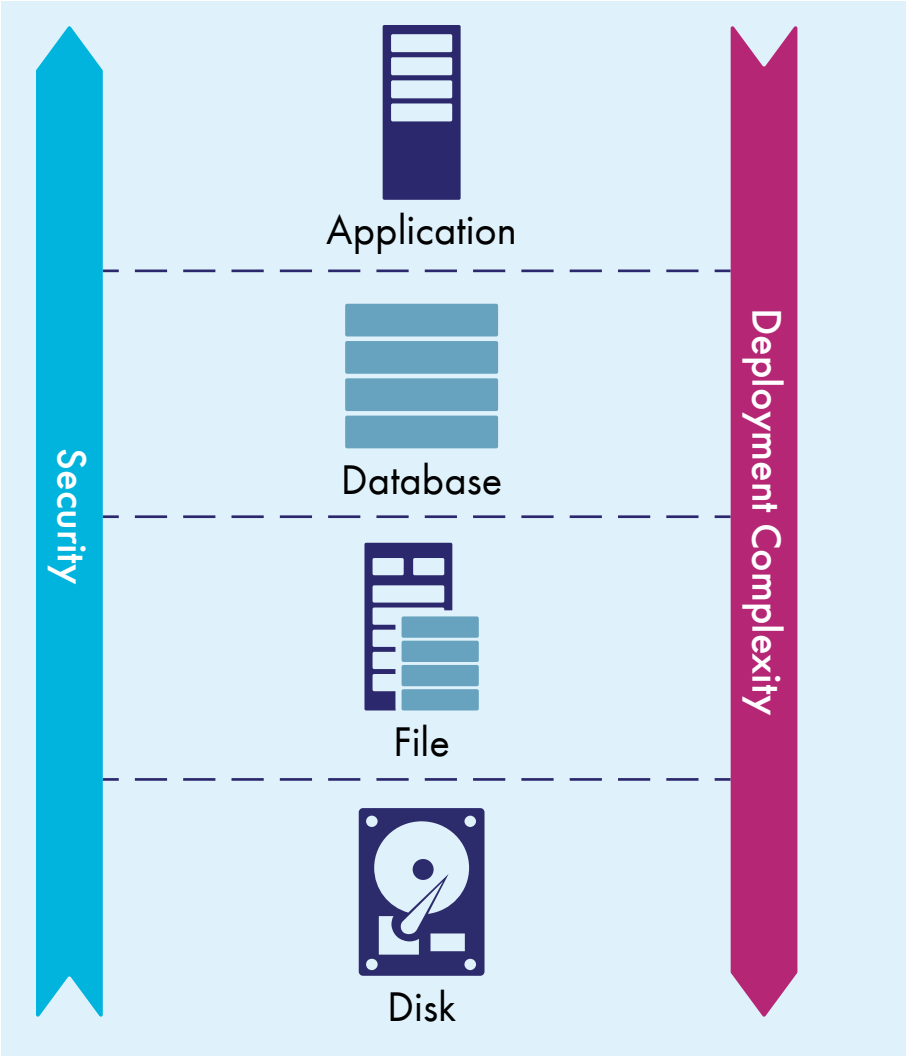

Fig. 1 – Security increases when implemented higher in the stack. However, deployment is less complex lower in the stack.

FULL-DISK ENCRYPTION

One approach to data-at-rest security is to employ full-disk encryption (FDE) or self-encrypting drives (SED). These approaches encrypt all information as it is written to the disk and decrypt it as it is read off the disk.

Advantages

This is the simplest method of deploying encryption. This approach is transparent to applications, databases, and users. In addition, performance is typically high because the encryption is done in hardware.

Disadvantages

The disadvantage of this approach is that it addresses a very limited set of threats, only offering data protection if the physical drive is stolen. Once the drive is booted and the encryption key is accepted, all the data on that drive is available to any user who can gain access to the system.

FDE makes sense for laptops, which are highly susceptible to loss or theft. However, these encryption approaches aren't suitable for the most common risks faced in data center and cloud environments. FDE doesn't offer any safeguards against advanced persistent threats (APTs), malicious insiders, or external attackers. For example, if an attacker was able to gain access to an application through an authorized user's credentials, FDE wouldn't prevent the attacker from decrypting the data. A recent Aberdeen Research study[3] shows that FDE would fail to address over 80% of data breach incidents in which servers were compromised. In addition, FDE leaves a very limited audit trail. This approach doesn't enable administrators to report on what files have been accessed, but only whether the drive was booted and authenticated with the encryption key.

3 — Aberdeen Research, "Selecting Encryption for 'Data At Rest' In Back-End Systems: What Risks are you Trying to Address," Derek Brink, http://enterprise-encryption.vormetric.com/Report-Aberdeen-Group-Selecting-Encryption-for-Data-at-Rest.html

FILE SYSTEM ENCRYPTION

File-system level approaches offer security controls by employing software agents that are installed within the operating system. The agents intercept all read and write calls to disks and then apply policies to determine if the data should be encrypted or decrypted.

Advantages

By employing encryption at the file level, organizations can establish strong controls that guard against abuse by privileged users. In addition to encryption, advanced file system solutions may offer controls that enable the application of policies governing access and file system functions according to such criteria as users, groups, process, and so on. For example, policies can be instituted that restrict privileged users, such as root-level administrators, from viewing data, while still enabling them to perform typical administrative functions. Some file system solutions can also offer very granular file access logs that can be used for security intelligence and compliance reporting.

One of the key advantages of these file-system approaches is that they are transparent to users and applications, meaning organizations don't have to rewrite applications or change associated business processes.

Limitations

There are some threats that file encryption doesn't guard against. For example, if a security team encrypts database files, the data would still be vulnerable to a malicious database administrator or SQL injection attack. Therefore, a compensating control like database activity monitoring (DAM) may also be required.

Before selecting a solution, it is very important to evaluate technology support. Solutions can be limited in the operating systems they can run on and the databases and file types they can encrypt. In organizations in which a range of technologies are employed, selecting a solution that has the broadest technology support will be important in establishing an enterprise-wide encryption strategy.

DATABASE ENCRYPTION

While approaches vary depending on the nature of the solution, at a high level, by implementing these approaches, security teams can encrypt a specific subset of data within the database, such as a column, or the entire database file. There are many options for implementing database encryption. Several database vendors now offer encryption capabilities for their products. For example, customers running specific versions of Oracle or Microsoft SQL Server databases can leverage functionality called Transparent Database Encryption (TDE). In addition, several security vendors offer encryption products that can support multiple database offerings.

Advantages

Through these approaches, organizations can employ safeguards in databases, which are critical repositories. When instituting effective solutions, they can establish strong safeguards against a range of threats, including malicious insiders—even in some cases a malicious database administrator.

Limitations

The downside to implementing encryption capabilities available from the database vendors is that encryption policies, cryptographic keys, and other efforts will only apply to that one vendor's databases. While this may be fine, for example, in an organization that is only running Oracle databases, if an organization has a heterogeneous mix of applications and databases, administering a number of these vendor-specific solutions can be excessively time consuming, with keys and policies managed in a disparate fashion.

Further, these approaches will lack centralized administration across different technologies, which can lead to security risks and compliance gaps. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires the separation of administrative duties, so no single administrator has complete control over sensitive assets and services. As a result, an organization may need to have controls in place to ensure that one set of administrators manages cryptographic keys while another group handles database administration. To establish these controls, an organization running TDE would also need to implement a separate solution for managing keys.

APPLICATION ENCRYPTION

When employing this approach, organizations leverage application logic and application programming interfaces (APIs) to govern the encryption and decryption of data. Often, application encryption solutions use a collection of software libraries and languages, such as Java or .NET, in order to enable the encryption of specific types of application data.

Advantages

In general, the advantage to these solutions is that they typically protect very specific subsets of data, such as fields in a database. In addition, the protection spans multiple layers, from the application to the disk, and so can guard against a range of threats. This solution will work with any database vendor.

Limitations

The downside is that, compared to file, database, and disk encryption, these approaches need to be integrated with the application, and so require development efforts and resources. In addition, using encryption may change the column sizes, potentially necessitating database schema changes. If data format preservation is required, tokenization or solutions like format-preserving encryption can be integrated with the application.

Vormetric Data Security Platform
Solution Introduction

The Vormetric Data Security Platform efficiently manages data-at-rest security across your entire organization. Built on an extensible architecture, Vormetric Data Security Platform products can be deployed individually, while sharing, key and policy management. With this platform's comprehensive, unified capabilities, you can efficiently scale to address your expanding security and compliance requirements, while significantly reducing total cost of ownership.

The Vormetric Data Security Platform delivers capabilities for transparent file-level encryption, application-layer encryption, tokenization, dynamic data masking, cloud encryption gateway, integrated key management, privileged user access control, and security intelligence.

With the solution, you can address security policies and compliance mandates across databases, files, and big data nodes—whether assets are located in cloud, virtualized, or traditional environments.

STRENGTHEN SECURITY AND COMPLIANCE

The Vormetric Data Security Platform provides capabilities for encrypting and tokenizing data, controlling access, and creating granular data access audit logs. With these capabilities, organizations can more effectively combat hackers, advanced persistent threats (APTs), and insider abuse.

In addition, the platform delivers the comprehensive capabilities that enable you to address the demands of a range of security and privacy mandates, including the PCI DSS, the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and regional data protection, residency, and privacy regulations such as the European General Data Protection Regulation (GDPR) and Japanese Act on the Protection of Personal Information (APPI).

MAXIMIZE STAFF AND RESOURCE EFFICIENCY

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

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

APPLY STRONG CONTROLS WHERE YOU NEED THEM

With the Vormetric Data Security Platform, your organization can establish strong, data-centric controls wherever you need, whether your sensitive assets reside in:

- The cloud, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) environments, as well as private and hybrid cloud environments.
- Servers running Linux, Windows, and Unix.
- Virtualized environments, including VMware, Microsoft Hyper-V, OpenStack, and KVM (Kernel-based Virtual Machine).
- Big data environments based on Hadoop or NoSQL, including Hortonworks, MongoDB, Cloudera, DataStax, Couchbase, IBM BigInsights, Teradata, and more.
- Databases, including IBM DB2, Microsoft SQL Server, MySQL, NoSQL, Oracle, and Sybase.
- Any storage environment, including direct attached storage (DAS), network attached storage (NAS), storage area networks (SAN), and tape.

Vormetric Data Security Platform

Product Offerings

Following is a brief overview of all the products that make up the Vormetric Data Security Platform:

- **Vormetric Data Security Manager.** Represents the central component of the Vormetric Data Security Platform, enabling the management of multiple Vormetric products. Offers centralized capabilities for storing and managing host encryption keys, data access policies, administrative domains, and administrator profiles.
- **Vormetric Transparent Encryption.** Features an agent that runs in the file system to provide high-performance encryption and least-privileged access controls for files, directories, and volumes. Enables encryption of both structured databases and unstructured files.
- **Vormetric Tokenization with Dynamic Data Masking.** Delivers capabilities for database tokenization and dynamic display security. Enables compliance with PCI DSS and security policies, while minimizing disruption and administrative overhead.
- **Vormetric Application Encryption.** Simplifies the process of adding column-level encryption into existing applications. Reduces complexity for developers by offering documented, standards-based APIs that can be used to perform cryptographic and key management operations.
- **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. Encrypts sensitive data before it is saved to the cloud. Maintains encryption keys on the customer premises, enabling security teams to establish the visibility and control they need around sensitive assets.
- **Vormetric Security Intelligence.** Produces granular logs that provide a detailed, auditable record of file access activities, including root user access. Enables easy integration with security information and event management (SIEM) systems. Delivers pre-packaged dashboards and reports that streamline compliance reporting and accelerate threat detection.
- **Vormetric Key Management.** Gives organizations an efficient, unified way to manage keys for Thales and third-party products.

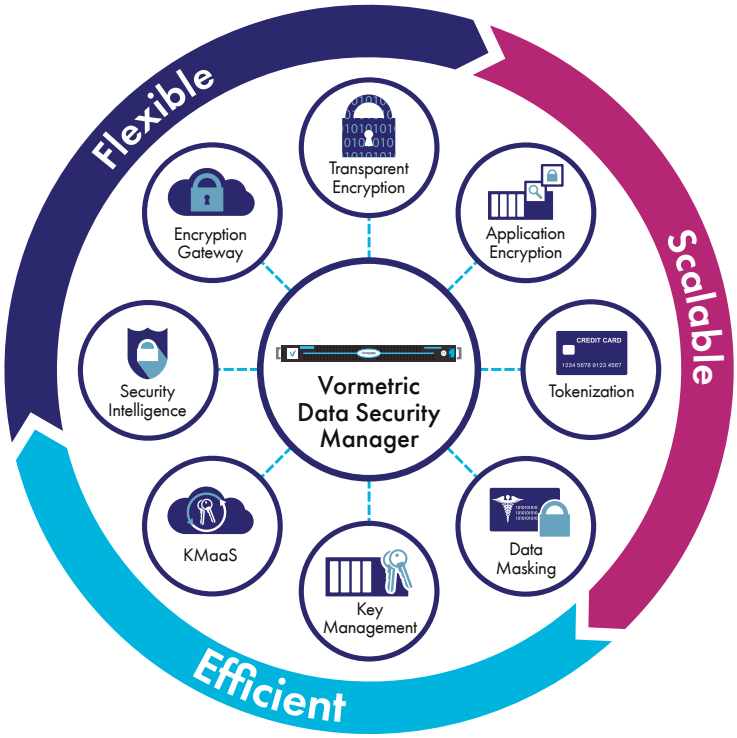

Fig. 2 – The Vormetric Data Security Platform makes it efficient to manage data-at-rest security across your entire organization.

VORMETRIC DATA SECURITY MANAGER

The Vormetric Data Security Manager (DSM) is the core of the Vormetric Data Security Platform. The DSM centrally manages cryptographic keys and polices for the entire suite of products available within the Vormetric Data Security Platform. All implementations of Vormetric Data Security Platform solutions start with the deployment of the DSM.

Centralized Key and Certificate Management

The DSM enables organizations to centrally store and control keys for all Vormetric products from Thales as well as third-party products.

The DSM can centralize and simplify secure key management for third-party products, such as IBM InfoSphere Guardium Data Encryption agents, Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant encryption products. The platform can also securely store and inventory X.509 certificates, symmetric keys, and asymmetric keys.

Fig. 3 – The V6100 hardware appliance is FIPS 140-2 Level 3 certified and is equipped with a Thales nShield Solo hardware security module (HSM).

Flexible Deployment Options

The DSM is flexible and offers support for a number of deployment models, helping customers address a range of business, security, and technical requirements. 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 platform is also available on the Amazon Web Services (AWS) and Microsoft Azure marketplaces.

Both hardware appliances and virtual appliances can be deployed on premises or in the cloud/hosted environments. The DSM supports multiple cloud deployment models, enabling either IT teams or cloud service providers (CSPs) to handle such tasks as system installation and hosting, system administration, and security administration of the DSM. Any of these form factors and deployment models can meet rigorous internal security policies and external regulatory standards.

High Availability

Enterprises must not only protect against data theft, but they must also protect their encryption keys from accidental loss or destruction. Both physical and virtual variations of the DSM offer clustering and failover capabilities that help ensure the security and availability of critical keys and cryptographic processing. In addition, hardware appliances offer redundant system components, including drives and power supplies, to help guard against issues associated with component failure.

> "Vormetric Data Security is quick and easy to administer while having negligible impact on performance; it's the perfect solution for meeting PCI DSS requirements."
>
> *–Daryl Belfry, Director of IT, TAB Bank*

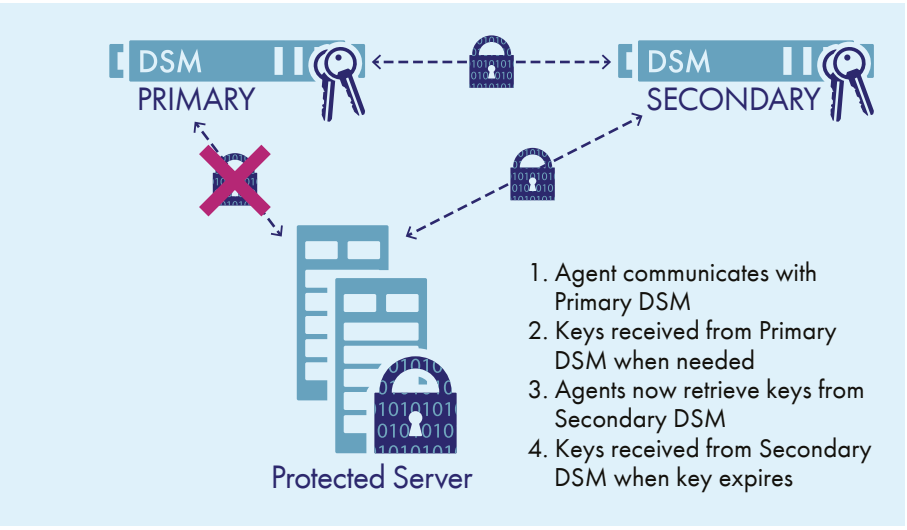

Fig. 4 – The DSM offers clustering support that helps ensure continuous service.

Efficient, Powerful Administration

The DSM features a web-based console for managing encryption keys, policies, and auditing across an enterprise. The platform also features command-line, SOAP (Simple Object Access Protocol) and RESTful (Representational State Transfer) APIs.

Robust Separation of Duties

The DSM can enforce strong separation of duties by requiring the assignment of key and policy management to more than one data security administrator. In this manner, no one person has complete control over security activities, encryption keys, or administration. In addition, the DSM supports two-factor authentication for administrative access.

Using the DSM and Vormetric Transparent Encryption together, administrators can create a strong separation of duties between privileged administrators and data owners. Vormetric Transparent Encryption encrypts files, while leaving their metadata in the clear. In this way, IT administrators, such as hypervisor, cloud, storage, and system administrators can perform their system administration tasks, without being able to gain access to the sensitive data residing on those systems.

Also, because these leave metadata in the clear, Vormetric Transparent Encryption doesn't have an impact on management activities like replication, migration, and snapshots. The platform's fine-grained controls can even be used to define whether privileged users can perform such functions as copy, write, or directory listing.

The specific permissions and administrative tasks for each type of DSM administrator are described in the following table.

System Administrator	Top-level administrator who creates domains and administrator accounts, typically assigning at least one administrator to each domain. The system administrator has no visibility into domains or access to protected data.
Domain Administrator	Assigns all administrators, except the original administrator, to domains. The domain administrator assigns roles to security administrators. Domain administrators cannot remove users or domains and they can't access protected data.
Security Administrator	This administrator can perform roles that were assigned by the domain administrator. Each security administra-tor can be assigned different roles, and specific roles can be assigned for each domain. Through the assignment of roles, security administrators can be allowed to handle a range of tasks: > **Audit.** This role grants access to purge and export audit logs. > **Key.** This role enables the creation, modification, and removal of encryption keys. > **Policy.** This role enables administrators to create, modify, and remove policies. > **Host.** This role enables administrators to register hosts, apply access controls to file hierarchies, and modify hosts' audit configurations.

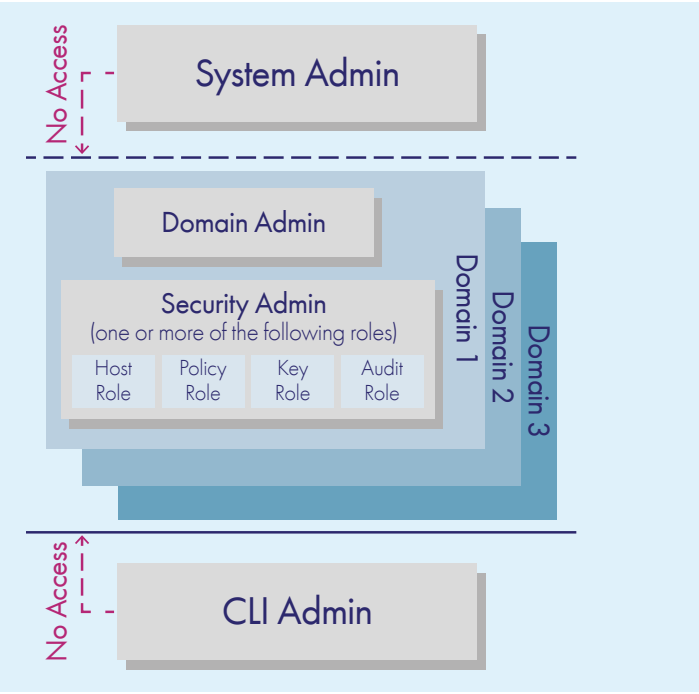

Fig. 5 – DSM management domains enable strong separation of duties between administrators.

The DSM: Key Advantages

By delivering the combination of capabilities outlined above, the DSM offers organizations a range of significant advantages:

> **Consistency.** The DSM provides a central console for managing policies and keys across an enterprise, enabling stronger security controls and more consistent adherence with internal policies and external regulatory mandates.

> **Productivity.** By leveraging a central, unified platform, organizations can significantly boost operational efficiency and staff productivity.

> **Agility.** By leveraging a complete, extensible platform, organizations can more quickly adapt to changing security, compliance, and business requirements.

VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption enables data-at-rest encryption, privileged user access control, and the collection of data access audit logs for structured databases and unstructured files—including those residing in physical, big data, and cloud environments. By leveraging this transparent approach, your organization can implement encryption, without having to make changes to your applications, infrastructure, or business practices.

Continuous Protection and Granular Controls

Unlike other encryption solutions, protection does not end after the encryption key is applied. Vormetric continues to enforce least-privileged user policies to protect against unauthorized access by users and processes, and it continues to log access. With these capabilities, you can ensure continuous protection and control of your data.

The product enforces granular, least-privileged user access policies that protect data from misuse by privileged users and APT attacks. Granular policies can be applied by user (including for administrators with root privileges), process, file type, time of day, and other parameters. Enforcement options are very granular; they can be used to control not only permission to access clear-text data, but which file-system commands are available to a user. The platform logs all permitted, denied, and restricted access attempts from users, applications, and processes. These logs are all captured in the DSM, enabling administrators to get detailed insights and efficiently track security status.

Flexible, Streamlined Implementation

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

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

TOKENIZATION WITH DYNAMIC DATA MASKING

Vormetric Tokenization with Dynamic Data Masking helps your security team address its compliance objectives, while gaining breakthroughs in operational efficiency. The solution provides a single platform that offers database tokenization and dynamic display security. With Vormetric Tokenization, you can meet PCI DSS requirements and secure data in cloud, big data, and data center environments—and do so with minimal disruption and administrative overhead.

By leveraging Vormetric Tokenization, your organization can replace sensitive assets with tokens, so attackers and malicious contractors and employees can't exploit the information to further their agendas.

Dynamic Data Masking

Administrators can establish policies to return an entire field tokenized or dynamically mask parts of a field, enabling role-based display security.

Vormetric Tokenization offers the flexibility to establish varying levels of data redaction. Administrators can establish settings to have an entire field tokenized or may dynamically mask data so that only portions of a field are visible, such as the last four digits of a Social Security Number or credit card.

Vormetric Tokenization can be integrated with your existing LDAP-and Active Directory-based identity directories, so your security teams can efficiently set granular policies for specific users and groups. For example, a user with customer service representative credentials can receive a credit card number with the last four digits visible for customer identification purposes, while a customer service supervisor may be able.

Comprehensive Support for Tokenization Approaches

Vormetric Tokenization supports the following options:

- Format preserving tokenization
- Random and sequential tokens
- Single and multi-use tokens
- Partial tokenization
- Dynamic data masking, alpha-numeric, and custom mask characters

Efficient Implementation

The Vormetric solution employs tokenization at the application layer, and it streamlines all the application development efforts associated with implementing tokenization in an enterprise. With the solution, developers don't have to manually institute identity management or redaction policies. Vormetric Tokenization offers an easy-to-use REST API for integration with the Vormetric Token Server, so your application developers can simply and quickly add tokenization and dynamic data masking to applications.

Efficient Scalability and Agility

Vormetric Tokenization delivers the high performance needed to address the operational demands of the most processing-intensive environments. The Vormetric Token Server runs on virtual machines and can be quickly and efficiently scaled up and scaled down to accommodate changing workloads.

VORMETRIC TOKENIZATION: KEY ADVANTAGES

- **Enables efficient, enterprise-wide administration.** With the capabilities offered by the Vormetric Data Security Platform, you can choose from a range of technologies and employ the mix that's optimally suited to your specific projects and use cases. At the same time, you gain the cost savings and operational benefits of working with solutions that can be centrally and uniformly managed. With the DSM, your organization can centrally manage keys for Vormetric Tokenization, as well as for Vormetric Transparent Encryption and Vormetric Application Encryption.
- **Offers non-disruptive implementation.** With the solution's format-preserving tokenization capabilities, you can restrict access to sensitive assets, yet at the same time, format the protected data in a way that reduces the operational impact typically associated with encryption and other obfuscation techniques. For example, your organization can tokenize a credit card field in a database, yet keep the tokenized information in a format that is compatible with associated applications. Further, you can create tokens that appear to be real credit card numbers, so tokenization does not break existing validation processes.
- **Reduces PCI DSS compliance effort and scope.** By leveraging Vormetric Tokenization, you can minimize the repositories and processes that can gain access to payment data in the clear, so your organization can significantly reduce its PCI DSS compliance costs and efforts.
- **Supports adoption of cloud, big data, and outsourced models.** Vormetric Tokenization enables organizations to more fully leverage cloud services, big data models, and outsourced environments, while retaining required security controls. For example, you can migrate tokenized data into a public cloud, and ensure sensitive assets won't be exposed to unauthorized individuals, even administrators, in the cloud provider's environment.
- **Establishes broad safeguards around sensitive assets.** Unlike other dynamic data masking tools, the Vormetric solution tokenizes sensitive fields in the production database. As a result, your organization can establish comprehensive safeguards around sensitive assets across the organization, and help protect against cyber attacks from criminals and nation-states, as well as from insider abuse.

VORMETRIC CLOUD ENCRYPTION GATEWAY

With the Vormetric Cloud Encryption Gateway, organizations can safeguard files in such cloud storage environments as Amazon Simple Storage Services (Amazon S3) and other S3-compatible object storage services. The solution encrypts sensitive data before it is saved to the cloud storage environment and maintains the encryption keys on the customer premises, enabling security teams to establish the visibility and control they need to protect sensitive assets from a range of threats.

Like other Vormetric encryption offerings, the solution relies on the DSM for key and policy management. As a result, you never have to relinquish control of cryptographic keys to your cloud provider and data never leaves your premises unencrypted or unaccounted for.

With the Vormetric Cloud Encryption Gateway, organizations can leverage a strong set of capabilities:

- **Robust, persistent controls.** When the solution is implemented, sensitive data may be copied, shared, and distributed in an array of environments, but security teams can manage keys and policies on their premises, so they retain localized visibility and control.
- **Detailed visibility and auditability.** The Vormetric Cloud Encryption Gateway gives you detailed visibility into data access, access attempts, and more. In the event of a breach or audit, administrators and investigators can access detailed forensics data.
- **Agile performance.** Through its virtualized appliance architecture, the Vormetric Cloud Encryption Gateway offers elastic scaling that enables IT teams to efficiently accommodate changing performance and scalability demands.
- **Intelligent risk detection.** The Vormetric Cloud Encryption Gateway can automatically scan cloud environments and discover unencrypted files that violate security policies. As a result, security teams can effectively mitigate the exposure associated with having users circumvent policies.
- **Transparent, efficient implementation.** IT teams don't need to modify applications or workflows when deploying the solution. In addition, the solution enables security teams to leverage their Lightweight Directory Access Protocol (LDAP) implementations, and, in Amazon S3 environments, Active Directory implementations, to more efficiently manage user and group access policies.
- **Flexible service extensibility.** The solution is built on an extensible architecture that will enable Vormetric and its partners to deliver support for a range of cloud storage environments and SaaS solutions.

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

Key Advantages

Through implementing Vormetric Cloud Encryption Gateway, organizations can realize a range of advantages:

- Encrypt files in Amazon S3, while retaining local control of keys and policies.
- Automatically detect unencrypted files in cloud storage environments and encrypt them.
- Guard against unauthorized access from government subpoena and cloud provider's privileged user accounts.
- Leverage cloud environments more broadly, while strengthening security and compliance controls.
- Boost operational efficiency through centralized controls over encryption keys and policies for a range of environments.

VORMETRIC APPLICATION ENCRYPTION

Vormetric Application Encryption enables customers to encrypt a specific field or column in a database, big data node, or PaaS implementation.

Flexible, Efficient Implementation

Vormetric Application Encryption eliminates the time, complexity, and risk of developing and implementing an in-house encryption and key management solution. 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. Developers can use libraries for Java, .NET, Python, and C to facilitate communication between applications and the Vormetric Application Encryption agent. This agent encrypts data and returns the resulting cipher text to the application.

Robust, Centralized Key Management

Enterprises must not only protect against data theft, but they must also protect their encryption keys from theft, misplacement, or accidental destruction. To facilitate these safeguards, the Vormetric Application Encryption library supports enterprise key management through the DSM. Like other Vormetric Data Security Platform products, all keys that are created and used by the Vormetric Application Encryption library reside in the DSM. This gives Thales customers a unified platform for encryption and centralized key management.

Strong Safeguards

Vormetric Application Encryption delivers the controls needed to address security policies and compliance mandates, both for data on premises and in PaaS environments. With the solution, you can stop malicious DBAs, cloud administrators, hackers and, in cloud environments, even authorities with subpoenas from accessing valuable data.

VORMETRIC SECURITY INTELLIGENCE

With Vormetric Security Intelligence, organizations can harness the extensive logging capabilities of Vormetric Transparent Encryption. Vormetric Security Intelligence delivers detailed security event logs that are easy to integrate with SIEM systems, so you can efficiently detect risks and quickly produce compliance and security reports.

Detailed Data and Powerful Insights

These logs produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into activities pertaining to sensitive data access. Logging occurs at the file system level, helping eliminate the threat of an unauthorized user gaining stealthy access to sensitive data. These logs can inform administrators of unusual or improper data access and accelerate the detection of insider threats, hackers, and APTs.

Detailed logs can be reviewed to specify when users and processes accessed data, under which policies, and if access requests were allowed or denied. The logs will even expose when a privileged user leverages a command like “switch user” to imitate another user.

Broad SIEM Platform Integration

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

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

Vormetric Security Intelligence offers proven integration and pre-built dashboards with a range of SIEM platforms, including FireEye Threat Prevention Platform, HP ArcSight, IBM Security QRadar SIEM, Informatica Secure@Source, McAfee ESM, LogRhythm Security Intelligence Platform, SolarWinds, and Splunk.

Efficiently Deliver Compliance Reporting

In order to adhere to many compliance mandates and regulations, organizations must prove that data protection is in place and operational. Vormetric Security Intelligence delivers the detailed data needed to prove to an auditor that encryption, key management, and access policies are working effectively.

KEY MANAGEMENT

You can centrally manage keys for all Vormetric Data Security Platform products, and securely store and inventory third-party keys and certificates. The product leverages the DSM to provide, standards-based, FIPS 140-2 validated key management platform that can secure keys for Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant devices. The platform can manage X.509 certificates, symmetric keys, and asymmetric keys. By consolidating key management, this product fosters consistent policy implementation across multiple systems and it reduces training and maintenance costs.

Vormetric Key Management provides powerful and flexible administration capabilities, offering a Web interface, command-line interface, and API. The solution enables administrators to do bulk imports of digital certificates and cryptographic keys.

Vormetric Key Management features extensive audit capabilities that can be used to report on all activities relating to key usage, including key generation, rotation, destruction, import, expiration, and export. The solution can provide alerts that help administrators stay apprised of certificate and key expiration so they can more proactively manage their environments.

Vormetric Key Management delivers all of the significant advantages of the DSM outlined above, including high availability through system redundancy and failover.

Vormetric Data Security Platform Partnerships

Thales e-Security has established an extensive network of technology partnerships, helping ensure our customers can gain maximum flexibility as they seek to pursue their dynamically evolving technology, security, and business requirements.

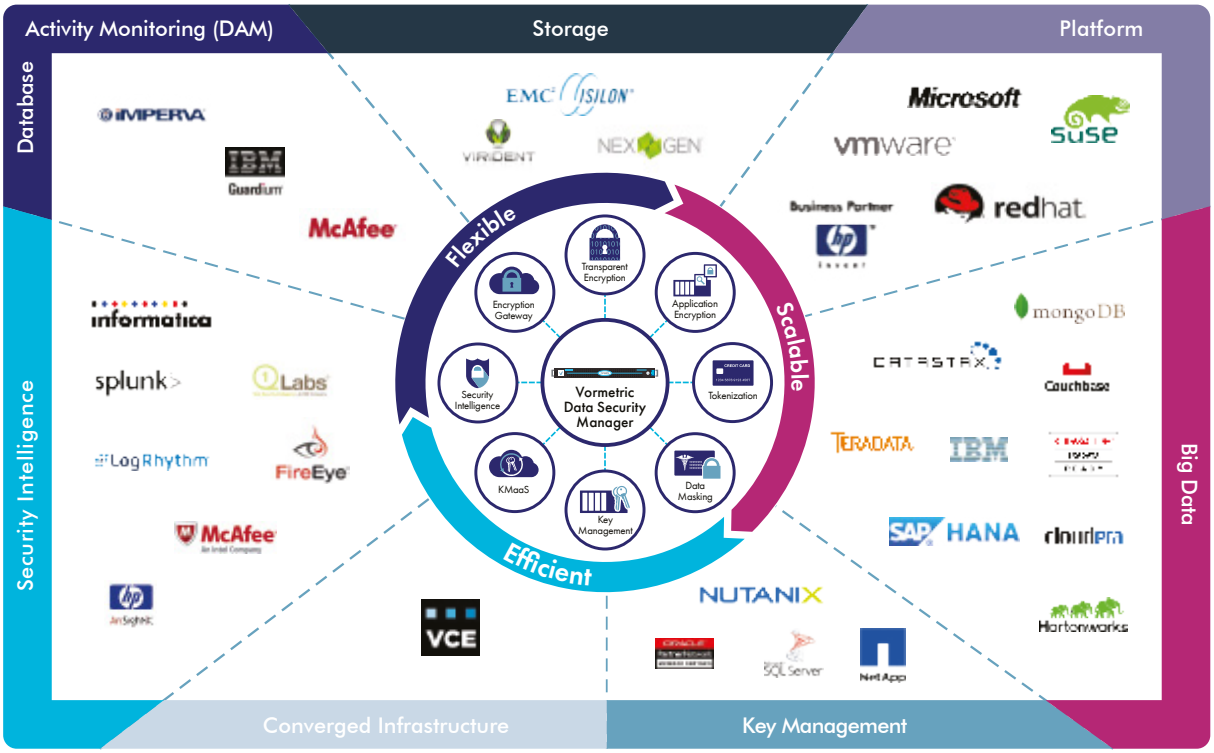

Fig. 6 – Example of the different categories of Vormetric partners and technology integrations.

Vormetric Powering Security-As-A-Service Offerings In The Cloud

Today, Vormetric Data Security Platform technologies are powering data security-as-a-service offerings delivered by a number of cloud providers. Following is a sampling of cloud providers that have partnered with Vormetric to deliver security-as-a-service offerings:

- Amazon Web Services (AWS)
- Armor
- BAE
- BT Security
- CenturyLink
- Cirrity Cloud Partner
- ClearData
- CloudHesive
- Compushare
- Datapipe
- Four Js
- fraXses
- Google Cloud Platform
- Hewlett Packard Enterprise
- HOSTING
- IBM Cloud Managed Services
- Microsoft Azure
- OnRamp
- Oper8
- Peak 10
- Pegasystems
- QTS Realty Trust, Inc.
- Rackspace
- vCloud Air
- Virtustream

For a complete list and more information about the program, be sure to visit the Vormetric Cloud Partner Program[4].

Conclusion

The demands for data-at-rest encryption continue to grow more urgent. Now more than ever, encryption represents a critical means for guarding against data breaches and ensuring compliance with regulatory mandates. With the Vormetric Data Security Platform, organizations can leverage a comprehensive solution that can address a wide range of environments and use cases. Through these advanced capabilities, organizations can address their security mandates, while minimizing costs and administrative efforts. To learn more about the specific products visit the Thales e-Security product pages to find product specific architectural papers, platform data sheets, and other information.

4 — https://www.vormetric.com/partners/cloud-partners

Appendix A: Example Use Cases

The Vormetric Data Security Platform can help organizations address many of their most significant business and technology objectives. Following are some of the most common ways these solutions are being employed.

SECURELY MIGRATING TO CLOUD AND HYBRID-CLOUD ENVIRONMENTS

The Challenge

Today, enterprises are in the midst of a massive shift in the way they manage their business and IT services. In just the past few years, these organizations have gone from IT environments that were hosted in internally managed data centers, to a steadily increasing reliance on virtualization, external service providers and cloud models.

Now a single organization may be reliant upon a combination of cloud-hosted infrastructure, SaaS-based applications, private clouds, virtual private clouds, and a number of other models. Rather than a monolithic move from one approach to another, IT and business leaders are mixing and matching the approaches that make most sense for a given task, so they can best align service models with specific business and technology requirements.

To leverage cloud resources while meeting their security and compliance requirements, enterprise security teams need robust, persistent, and granular controls that can be applied whether data is in their internal data center or at their cloud provider's facilities.

How Thales e-Security Helps

Organizations are increasingly leveraging Vormetric Transparent Encryption as they look to address data-at-rest encryption requirements in their mix of hybrid, internally hosted, and cloud environments. With Vormetric Transparent Encryption, security teams can encrypt data at the file system or volume level within virtual machines (VMs) and then use fine-grained, centrally managed policies to control access to protected data.

Vormetric Transparent Encryption encrypts data at the file system level within cloud instances and then provides fine-grained, centrally managed controls that help ensure that only authorized users and processes can decrypt data. In addition, now customers can leverage data security-as-a-service offerings from a number of leading cloud providers that are powered by Vormetric Transparent Encryption. Be sure to visit the Vormetric Cloud Partner Program page[5] for a complete list of cloud partners.

In addition, if organizations are leveraging cloud storage services like Amazon S3, they can leverage Vormetric Cloud Encryption Gateway to encrypt files before they are stored in these environments. Finally, organizations can use Vormetric Application Encryption and Vormetric Tokenization any time they need to encrypt specific data elements before they are migrated to the cloud.

> "The Vormetric Data Security Platform has put us in the fantastic position of being able to support any encryption deployment model and any data, application, and platform combinations that our clients want to use."
>
> *–Pete Nicoletti, CISO Virtustream Inc.*

5 — https://www.vormetric.com/partners/cloud-partners

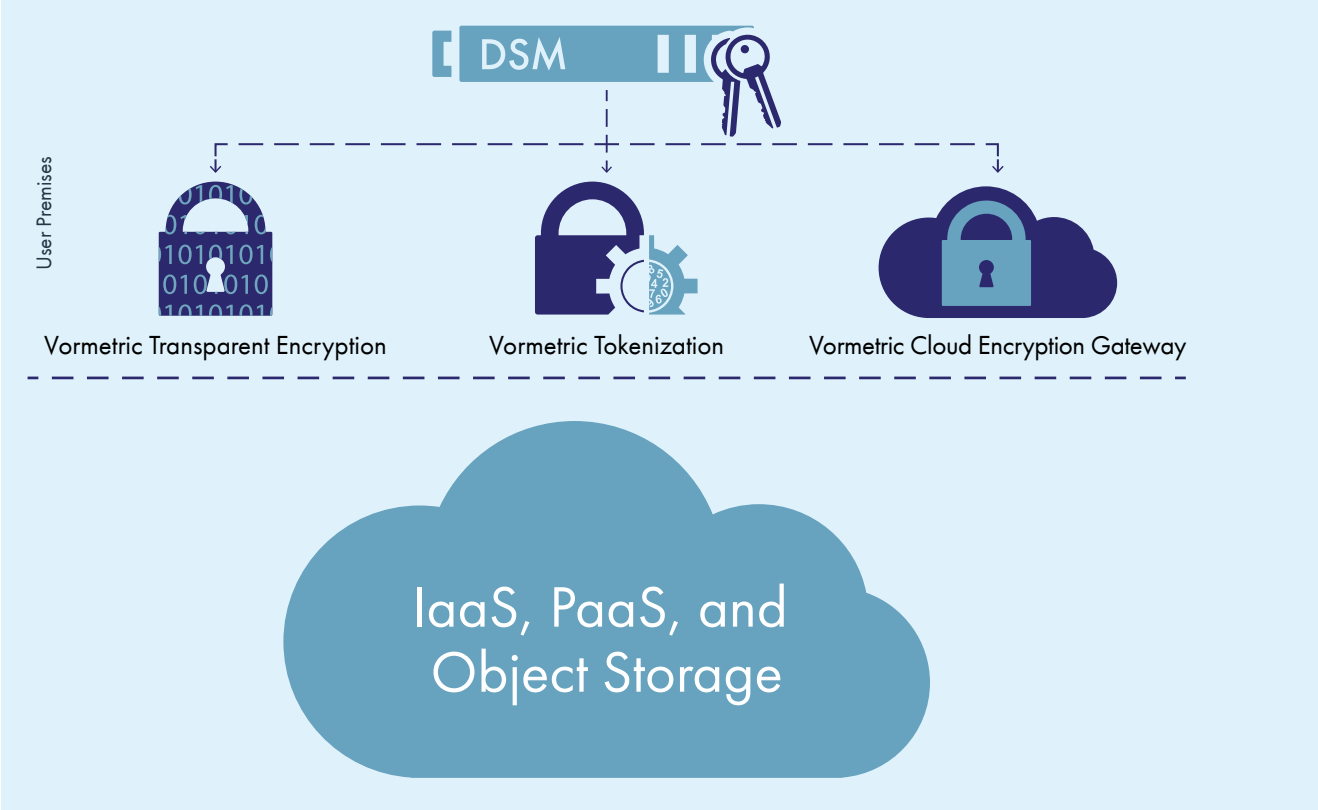

Fig. 7 – The DSM centralizes key management and control of data on-premises and across different cloud environments.

SUSTAINING SECURITY AND COMPLIANCE WHILE LEVERAGING BIG DATA

The Challenge

Today, enterprises are growing increasingly reliant upon big data implementations so their staff can maximize the value of data in furthering a range of objectives, including making more informed plans and decisions, discovering new opportunities for optimization, and delivering breakthrough innovations.

However, given the specific attributes of these implementations, organizations adopting big data can also be exposed to increased risks. Big data implementations consolidate diverse data sets and yield high-value insights, which can make these environments a prized target for malicious insiders and external criminals.

How Vormetric Helps

Vormetric Transparent Encryption is a solution that organizations increasingly leverage to secure the sensitive assets in their big data environments. With the solution, organizations can secure sensitive data in big data environments based on Hadoop or NoSQL, including Hortonworks, MongoDB, Cloudera, DataStax, Couchbase, IBM BigInsights, Teradata, and more.

Vormetric Transparent Encryption can secure the entire big data environment, including the data sources that may be fed into the environment, the big data nodes and the "data lake", and the analytics and reports that get generated. In addition, in cases where organizations may need to encrypt specific data elements before they are migrated into the big data environment, organizations can also use Vormetric Application Encryption and Vormetric Tokenization.

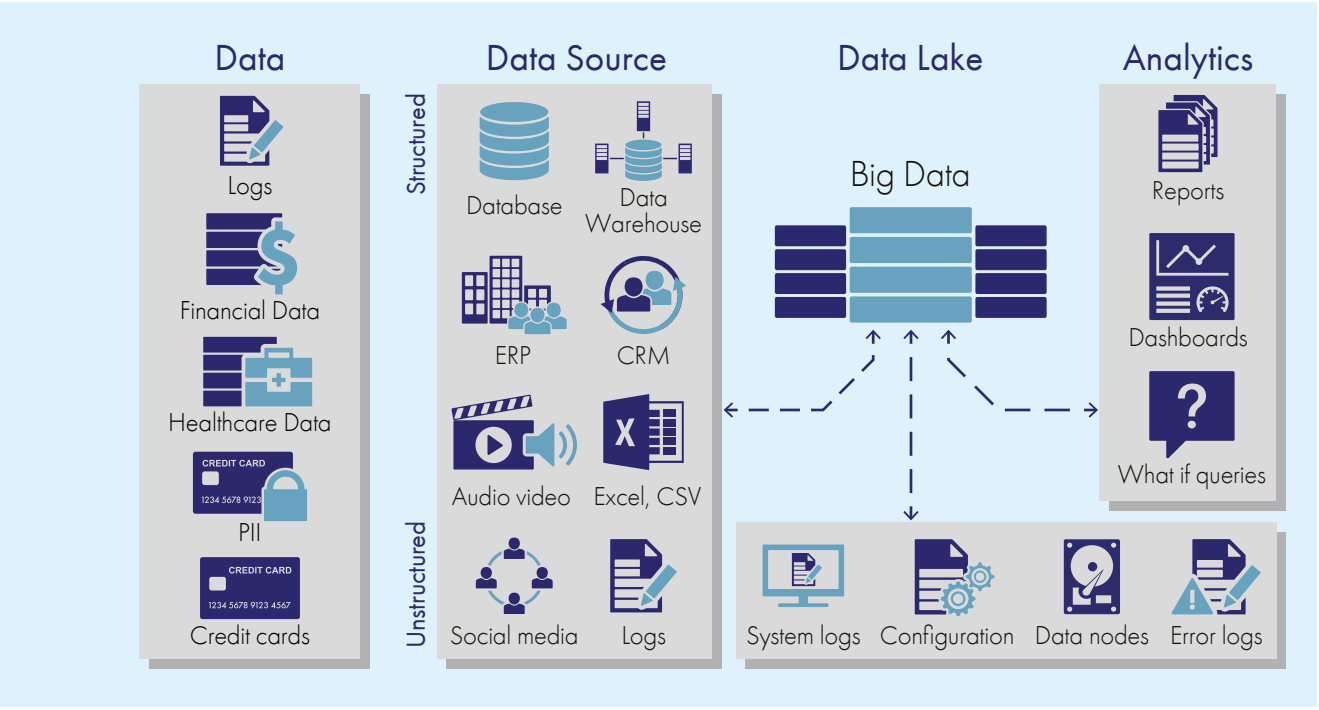

Fig. 8 – Vormetric Transparent Encryption providing end-to-end data encryption, privileged user access control, and key management in a big data environment.

EFFICIENTLY SECURING DATA ACROSS DISTRIBUTED AND MOBILE ENVIRONMENTS

The Challenge

While securing today's evolving data centers can be challenging, many IT organizations also have to contend with the security requirements of a large number of distributed entities. For a large retailer, this can include thousands of globally distributed stores. For banks, this can include branch offices, ATMs, and kiosks. For military organizations, this could include everything from field offices to naval vessels and ground transport vehicles. Especially in recent years, these remote and distributed environments have represented the Achilles heel of many organizations because they are targeted for both cyber attacks and physical theft.

Establishing and sustaining security in these distributed environments can present several significant challenges. For example, they may be more vulnerable to theft or attack and they can be subject to intermittent connectivity. Further, for many organizations, securing these environments also poses significant challenges from a scalability standpoint, as often hundreds of locations need to be supported.

How Thales e-Security Helps

Today, some of the largest retailers, financial institutions, and government agencies rely on Vormetric Transparent Encryption to efficiently secure data in their distributed environments. By leveraging the solution's robust encryption capabilities, organizations can establish the critical safeguards required to ensure that sensitive data remains secure from cyber attacks and even physical theft.

The solution's encryption agents can be remotely deployed and managed, which makes them practical to implement across large numbers of distributed locations. Further, Vormetric Transparent Encryption is optimally suited to the unique requirements of these distributed environments, offering the proven ability to scale to more than 10,000 sites and to deliver high availability, even in environments with unpredictable connectivity. In addition, organizations can leverage Vormetric Application Encryption and Vormetric Tokenization to secure specific data assets before they are transmitted out to these distributed environments.

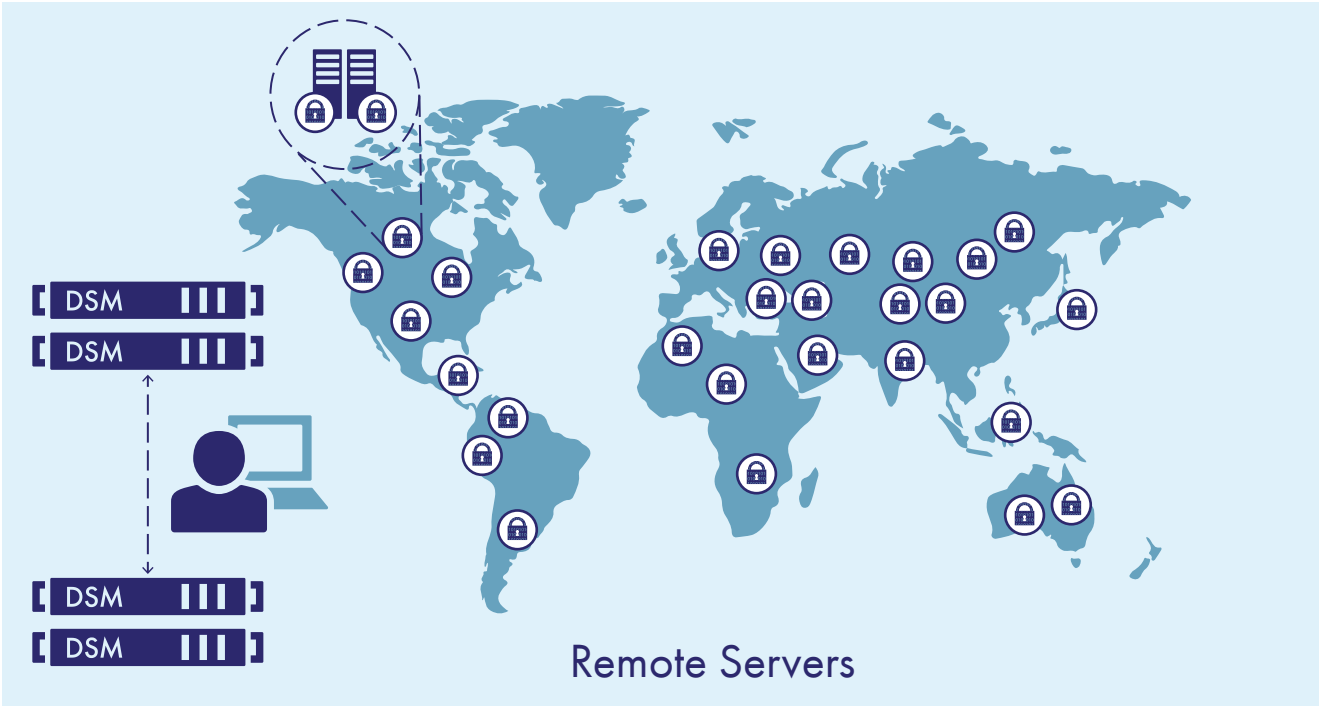

Fig. 9 – Example of a geographically distributed cluster of DSMs providing high availability for thousands of protected servers.

THALES

www.thalesesecurity.com

About Thales e-Security

Thales e-Security 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-premise, 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 e-Security is part of Thales Group.

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, 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