thalescpl.com

THALES

Vormetric Transparent Encryption

Advanced data-at-rest encryption, access control and data access audit logging

White Paper

Contents

Introduction

Enterprise digital transformation and increasingly sophisticated IT security threat landscapes are resulting in a fundamentally more dangerous environment for enterprises with sensitive data, even as compliance and regulatory requirements that strictly enforce the requirement for sensitive data protection rise. With attacks adapting on a daily or even hourly basis, even next-generation network and endpoint defenses consistently fail to stop attacks that penetrate enterprises networks, in 2018 more than two-thirds of enterprises had already encountered a data breach1. At the same time, digital transformation is expanding the attack surfaces available to adversaries beyond traditional enterprise boundaries as organizations embrace the business advantages available from these new solutions.

Just as no single attack method is responsible for increased threats to enterprise data, no single digital transformation technology is responsible for increased risks from these new environments – as each technology adopted presents unique data security challenges. However, the number and complexity of these new technologies and the individualized approach required to secure data throughout each environment combine to compound the problem:

- Cloud environments are now the default for workloads and applications with 451 research predicting that by 2019 60% of all workloads will run in cloud environments[1]
- SaaS environment adoption is very high with 61% of organizations using 26 or more SaaS applications in 2018[1]
- In 2018, Big Data, Containers, Mobile Payments, Blockchain, and IoT have all reached 90% adoption or planned implementation levels[2]

Within this environment of increased risks to sensitive enterprise data, a key protection required is the ability to limit access to sensitive information to only those users, groups and processes that require the use of the data – and no more. This need extends across traditional data centers, cloud environments, beneath SaaS implementations and to the data stores of every digitally transformative environment. A system level control that enforces access when it is needed, through only allowed applications, and enforced with encryption, is needed to meet these needs.

Vormetric Transparent Encryption (VTE) enables quick, effective and transparent protection at the system level to meet this need without derailing business processes, user tasks, and administrative workflows. With a single set of data security controls, information stored within physical and virtual systems, big data environments and containers (such as Docker and OpenShift) and linked cloud storage are protected at the file system or volume level across data centers and infrastructure cloud environments. The result is greatly reduced risk, and an enhanced capability to meet compliance and regulatory data security requirements.

[1] https://451research.com/blog/1910-by-2019,-60-of-it-workloads-will-run-in-the-cloud

[2] 2018 Thales Data Threat Report by 451 Research http://dtr.thalesesecurity.com

The Vormetric Data Security Platform from Thales

Vormetric Transparent Encryption is an element of the Vormetric Data Security Platform; a solution that efficiently enables data-at-rest security across entire enterprise infrastructures, regardless of where data is used. Built on a single extensible infrastructure, Vormetric Data Security Platform products can be deployed as needed while sharing a common, scalable, policy control and key management environment. In addition to Vormetric Transparent Encryption, the Vormetric Data Security Platform delivers capabilities for application-layer encryption, tokenization, dynamic data masking, cloud and on-premises key management. These capabilities enable organizations to safeguard and control access to data regardless of where it is stored or used, meeting requirements for compliance, regulatory mandates, data privacy standards and best practices.

Typically, enterprises deploy data security solutions to meet compliance or regulatory requirements, protect their organizations from the consequences of a data breach or to respond to an executive or partner requirement. The Vormetric Data Security Platform is designed to provide a single infrastructure and solution set that enables organizations to meet these needs cost-effectively – without the high overhead, resource usage and complexity that accompanies the deployment of multiple solutions to meet point data security requirements.

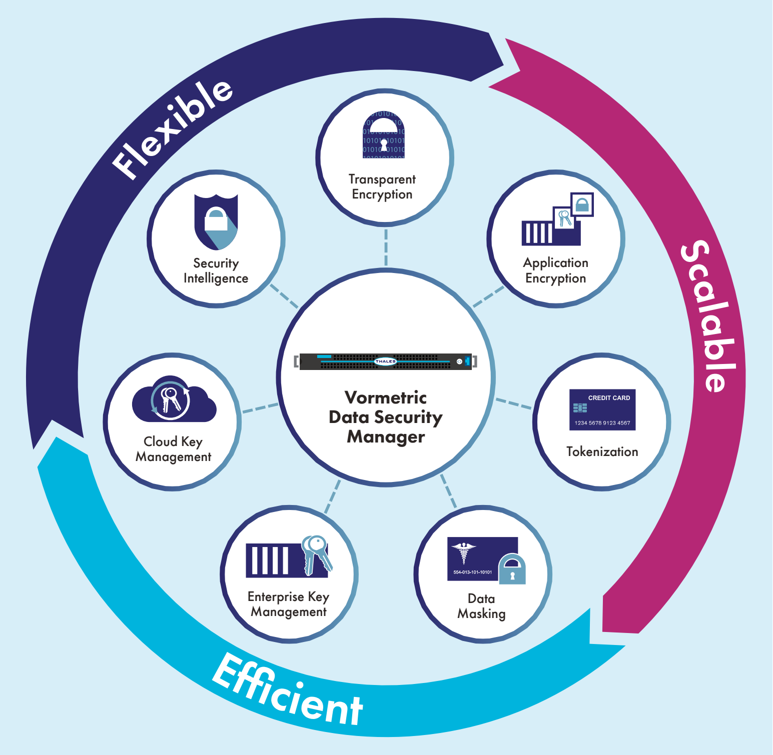

Figure 1. The Vormetric Data Security Platform from Thales Simple one-stop, data-at-rest security

Enables efficient, enterprise-wide administration

With the capabilities offered by the Vormetric Data Security Platform, organizations can choose from a range of technologies and employ the mix that's optimally suited to an organization's specific projects and use cases. At the same time, enterprises gain the cost savings and operational benefits of working with solutions that are centrally and uniformly managed. With the Vormetric Data Security Platform from Thales, organizations can centrally manage keys for Vormetric Transparent Encryption, Vormetric Application Encryption, Vormetric Tokenization with Dynamic Data Masking, other Vormetric products, and third-party devices.

Offers non-disruptive implementation

With the solution's capabilities, organizations 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, organizations can tokenize a credit card field in a database, retaining the tokenized information in a format that is compatible with associated applications. Further, tokens can appear to be real credit card numbers and pass LUHN validation, so tokenization does not break existing validation processes.

Eliminates manual efforts and complexity

RESTful APIs for management and operation of Vormetric Data Security Platform products and enable seamless integration with existing infrastructure. Vormetric Orchestrator provides for automated, integrated deployment, management, and updating of platform products.

Provides investment protection

Customers that have already invested in the Vormetric Data Security Platform can get even more out of their investments. By leveraging existing Vormetric Data Security Manager implementations (required for all Vormetric Data Security Platform products), it is quick and cost-effective to add additional solutions to solve data security problems throughout enterprise infrastructure and cloud environments.

The Vormetric Transparent Encryption Solution

Introduction

With Vormetric Transparent Encryption, organizations can quickly deploy strong controls around their sensitive data-at-rest at the file system or volume level without disruption to users and operational processes. Vormetric Transparent Encryption features encryption, key management, privileged user access control, and the collection of data access audit logs to protect structured databases and unstructured files—in traditional data center servers, virtual environments, linked cloud storage, cloud Infrastructure as a Service (IaaS) implementations, big data deployments, and containers. With optional Live Data Transformation enabled, deployment downtime and maintenance are further reduced by encrypting and re-keying data while it is in use.

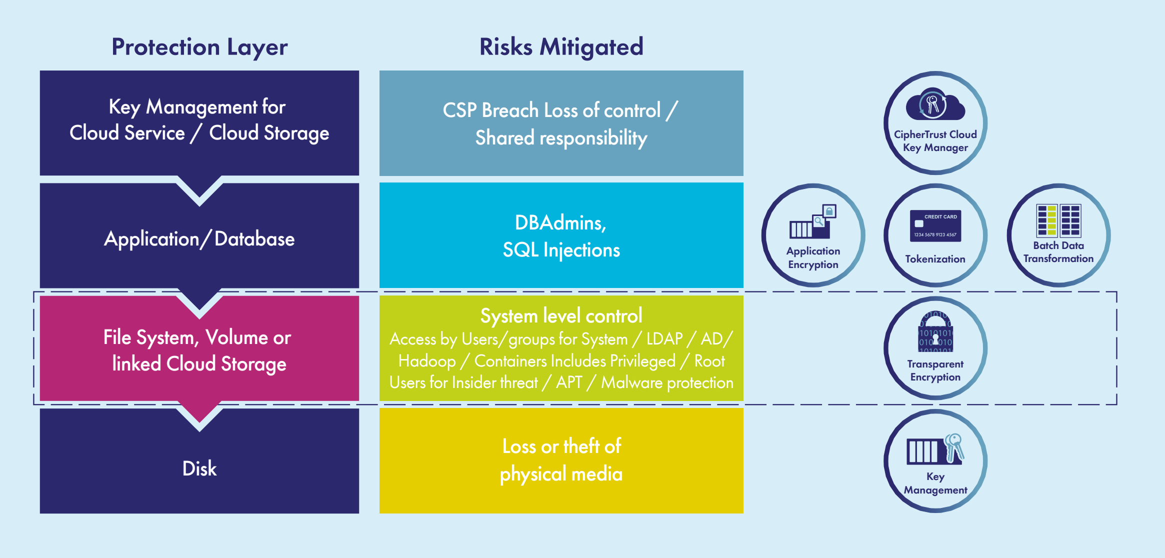
Protection Layer
Risks Mitigated
Key Management for Cloud Service / Cloud Storage
CSP Breach Loss of control / Shared responsibility
CipherTrust Cloud Key Manager
Application/Database
DBAdmins, SQL Injections
Application Encryption
Tokenization
Batch Data Transformation
File System, Volume or linked Cloud Storage
System level control
Access by Users/groups for System / LDAP / AD/ Hadoop / Containers Includes Privileged / Root Users for Insider threat / APT / Malware protection
Transparent Encryption
Disk
Loss or theft of physical media
Key Management

Figure 2. Vormetric Data Security Platform – Risks and Protection Layers for Transparent Encryption

Advanced capabilities

- Zero-downtime data transformation. Add the Live Data Transformation option to alleviate the downtime required for initial encryption and scheduled rekeying operations. With this option, once the Vormetric Transparent Encryption agent is installed on the server, applications and services continue to operate as usual during encryption and rekeying of data.
- Container support. Vormetric Container Security extends policy driven Vormetric Transparent Encryption file level encryption, access controls and data access audit logging to container environments. The solution enables file level encryption and access controls for container user roles, and data stored within, or accessed by, container images.
- Automated deployment and maintenance. Vormetric Orchestrator can be used to automate deployment, configuration, management and monitoring for Vormetric Transparent Encryption deployments, helping simplify operations, eliminate errors and speed deployments.
- Advanced access controls for big data (Hadoop). When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.
- SAP HANA reviewed and qualified. SAP has reviewed and qualified Vormetric Transparent Encryption as suitable for use in SAP solution environments.

Key features:

- **Continuous protection.** Continuously enforces policies that protect against unauthorized access by users and processes, as well as creating detailed data access audit logs of all activities.
- **Granular controls.** Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop, and containers. Controls also include access by process, file type, time of day, and other parameters.
- **Security intelligence.** Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance and forensic reporting requirements but also enable data security analytics with popular security information and event management (SIEM) systems. Includes pre-built displays of key indicators for selected SIEMs.

- **Non-intrusive.** Vormetric Transparent Encryption agents are deployed on servers at the file system or volume level and support both local disks as well as cloud storage environments like Amazon S3 and Azure Files, enabling encryption and access control without requiring changes to applications, infrastructure, systems management tasks or business practices.
- **Strong encryption.** Vormetric Transparent Encryption only employs strong, standards-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The agent is FIPS 140-2 Level 1 validated.
- **Broad storage support.** Supports Windows, Linux, and UNIX local and network file systems, as well as Amazon S3 and Azure Files storage options from on-premises or in cloud environments.
- **System support.** 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. Agents can be located locally on premises as well as across multiple cloud environments.
- **Hardware accelerated encryption.** Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs (Intel AES-NI, AMD AES-NI, and IBM Power8 encryption), delivering encryption with optimal performance even in virtual and cloud environments.

Solution components

Vormetric Transparent Encryption (VTE) minimum solution components consist of two Vormetric products, VTE agents, and Vormetric Data Security Management (DSM) appliances. Beyond the minimum component set are optional elements that extend the functionality available from the solution.

Minimum solution components:

- Vormetric Transparent Encryption agents
- Vormetric Data Security Manager physical or virtual appliances

Optional components:

- **Security Intelligence log usage.** Collect data access audit logs from the Vormetric Data Security Manager appliances using SIEM systems, use pre-configured dashboards to identify unauthorized access attempts to protected data.
- **Live Data Transformation.** Enabled with an additional license. Perform initial encryption and data re-keying without taking applications using data stores offline.
- **Container support.** Enabled with an additional license. Extends VTE encryption, access controls and data access audit logging to data stored within containers or in linked underlying storage environments.

A simple deployment scenario for file system or volume data within a local data center includes a VTE agent deployed to the host systems or virtual machines and two Vormetric Data Security Manager (DSM) appliances. Two appliances are required for clustering and failover capabilities that enable solution uptime.

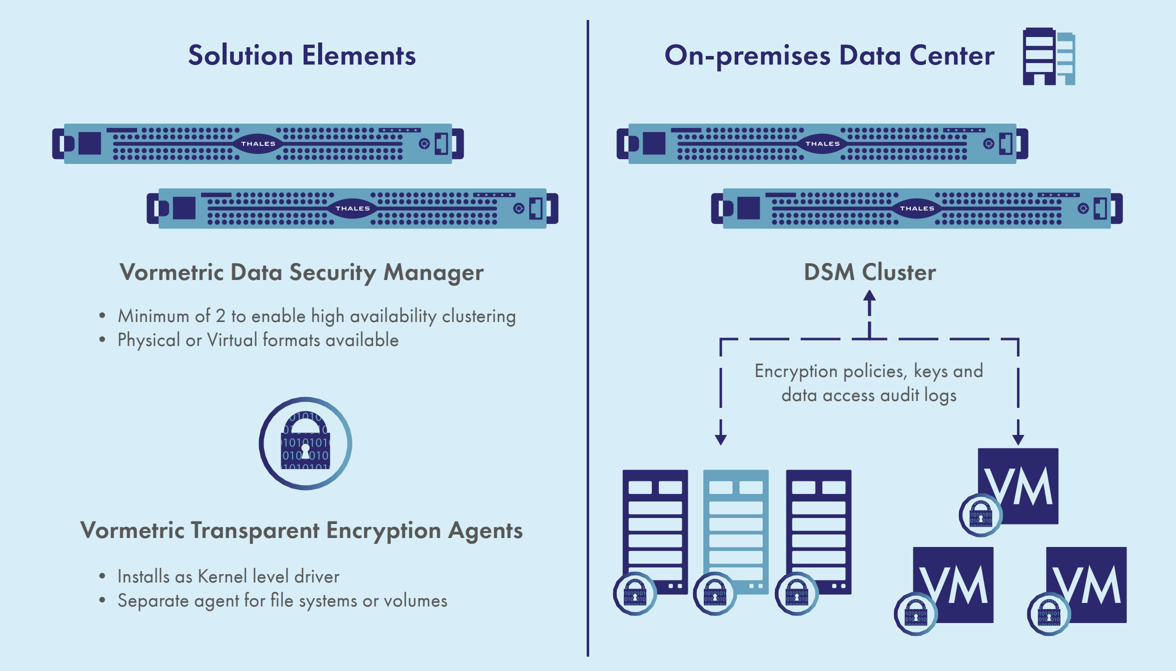
Solution Elements
THALES
THALES
Vormetric Data Security Manager
• Minimum of 2 to enable high availability clustering
• Physical or Virtual formats available
Vormetric Transparent Encryption Agents
• Installs as Kernel level driver
• Separate agent for file systems or volumes
On-premises Data Center
THALES
THALES
DSM Cluster
Encryption policies, keys and data access audit logs
VM
VM
VM

Figure 3. Basic Solution Architecture – Traditional Data Center

Vormetric Transparent Encryption Agent

Vormetric Transparent Encryption agents are kernel level drivers that sit above file systems or volumes in the OS stack. Agents perform encryption, decryption, policy-based access control, and data access audit logging.

Policies administered by agents employ logic and fine-grained access control settings configured at the Data Security Manager (DSM) to evaluate attempts to access protected data, and then either grant or deny access. Controls include who is enabled to access data, what and where information is available to them, when access can be performed, and what processes are allowed to access plaintext, copy encrypted files or even view file system metadata.

This fine-grained policy control enables operation that lets administrators and system level users perform their work (such as system backups, updates, and hardware maintenance), without having access to decrypted sensitive information.

All activities are logged. Logs are available from the local system or the DSM and are integrated with leading SIEM systems. See the section of this white paper on Security Intelligence for further detail.

Application uptime for the solutions whose data VTE protects is supported with an easily available failover capability – simply deploy agents at the primary and failover locations and keep encrypted data stores in sync with standard processes. When top level application failover is required, enable the same policy used at the primary location at the failover location. Result – sensitive information is continuously protected, and business operations continue with standard failover operation.

Minimizing performance impacts is a base requirement of modern encryption systems, and the VTE agent is designed to meet this need. The AES-256 hardware accelerated encryption capabilities available from modern CPUs is used by the agent regardless of the environment. UNIX, Linux and Windows deployments to physical servers, virtual environments, cloud IaaS/PaaS (Pivotal) and even container environments all benefit from the extremely low overhead on encryption and decryption available from hardware acceleration.

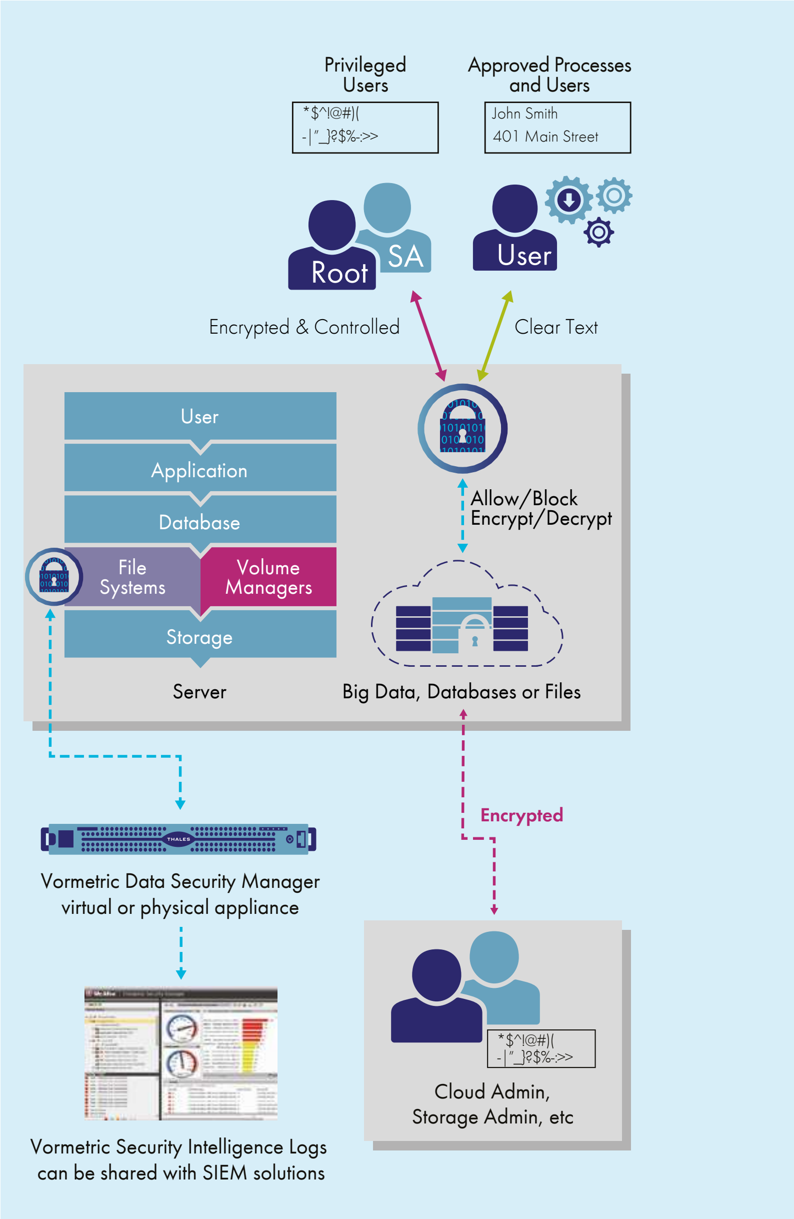

Figure 4. Vormetric Transparent Encryption encrypts, enforces access policies, and logs all file, volume and linked cloud storage access

Environment Support

OS Support

Microsoft: Windows Server 2008, 2012, 2016

Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu

UNIX: IBM AIX

Big Data Support

Hadoop: Cloudera, Hortonworks, IBM

NoSQL: Couchbase, DataStax, MongoDB

SAP HANA

Teradata

Database Support

IBM DB2, Microsoft SQL Server, MySQL, NoSQL, Oracle, Sybase and others

Encryption Hardware Acceleration

AMD and Intel AES-NI

IBM P8 cryptographic coprocessor

Application Support

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

Agent Certification

FIPS 140-2 Level 1

File systems

Supports most standard file systems for each OS – See your Thales sales representative for a complete and current listing.

Amazon AWS – EBS, EFS, and via the AWS Storage Gateway also supports S3 Standard, S3 Infrequent and S3 Glacier

Microsoft Azure – SSD/STD Disks, GRS & LRS storage with SMB/CIFS via Azure Files

Container Support

Docker, Red Hat OpenShift

SIEM integration:

Splunk, McAfee, LogRhythm, ArcSight, Q1labs, Solarwinds, FireEye, Informatica

Users and Groups:

System, LDAP/AD, Hadoop and Containers

Note: Platform support is regularly expanded, so please contact Thales eSecurity if a technology deployed in your environment isn't listed.

Powerful protection against root and privileged user risks

Vormetric Transparent Encryption (VTE) includes highly intelligent protection against root user attacks. The solution will log and control access based on user roles and groups (system, LDAP/AD, Hadoop, Containers), but also has additional capabilities to combat root user attacks. The root user role has the capability to both create system level accounts and to log in to other system level accounts. When root users use these capabilities to change to an account that has access to sensitive data, access to the data will still be denied if root is not specifically allowed access by VTE policy (as defined at the DSM). The solution will be aware of the original login account as root, and deny or allow access based on that account.

Vormetric Data Security Manager

The Vormetric Data Security Manager (DSM) is the common centralized management environment for all Vormetric Data Security Platform products. It provides policy control as well as secure management and storage of encryption keys, includes a Web-based console as well as CLI, SOAP and REST APIs. The DSM is available as FIPS 140-2, and Common Criteria certified virtual and physical appliances.

The DSM also provides a unified way to manage keys for third-party platforms, such as IBM Guardium Data Encryption (GDE), Oracle Transparent Data Encryption (TDE), Microsoft SQL Server TDE, and KMIP-compliant encryption products. The DSM can also store and manage X.509 certificates, symmetric keys, and asymmetric keys.

Available appliance form factors:

- FIPS 140-2 Level 1 virtual appliance
  - The virtual appliance is available in VMware, HyperV, KVM, Amazon Web Services, and Azure compatible formats
  - A FIPS 140-2 Level 3 root of trust available with nShield Connect HSM integration
- FIPS 140-2 Level 2 hardware appliance
  - A FIPS 140-2 Level 3 root of trust available with nShield Connect HSM integration
- FIPS 140-2 Level 3 Hardware appliance - Includes an internal nShield Solo HSM

Strong Separation of Duties

The DSM can be configured as a multi-tenant device that runs many different virtual DSMs, which are called "domains." The DSM can enforce strong separation of duties by requiring more than one data security administrator to manage or change key and policy permissions. DSM administration can be broken into three categories: system, domain, and security. In this manner, no one person has complete control over security activities, encryption keys, or administration. Also, the DSM supports two-factor authentication for administrative access.

Users and groups for data security management tasks can be based on locally defined users or groups or imported via LDAP from Active Directory or other directory services and identity management environments.

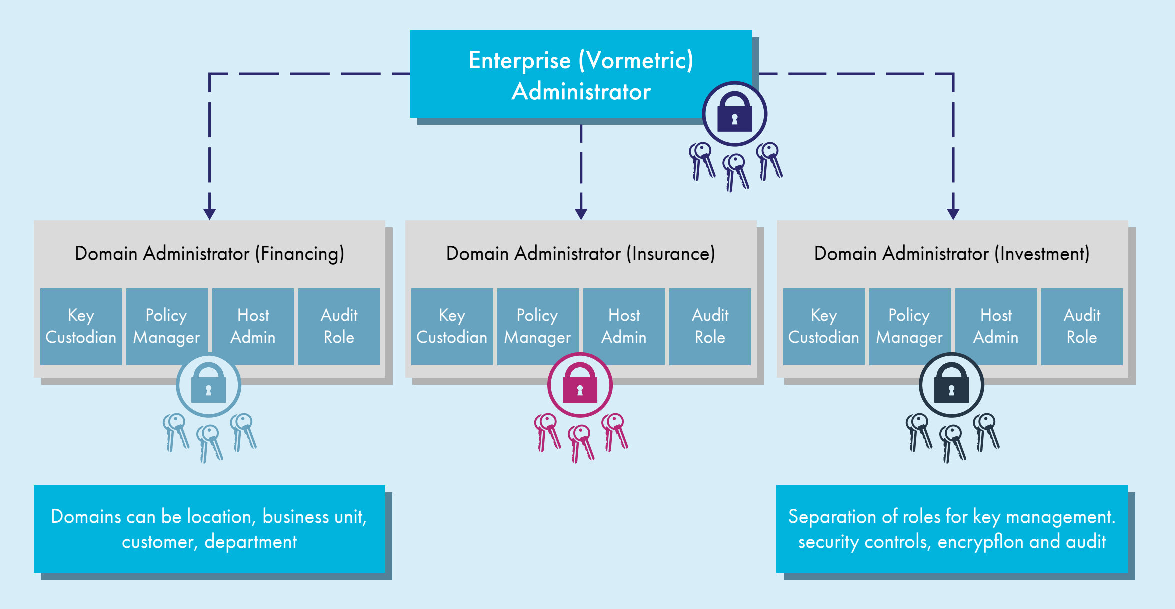
Enterprise (Vormetric) Administrator
Domain Administrator (Financing)
Key Custodian
Policy Manager
Host Admin
Audit Role
Domain Administrator (Insurance)
Key Custodian
Policy Manager
Host Admin
Audit Role
Domain Administrator (Investment)
Key Custodian
Policy Manager
Host Admin
Audit Role
Domains can be location, business unit, customer, department
Separation of roles for key management. security controls, encrypflon and audit

Figure 5. Multitenant Key Management and Strong Separation of Duties

To further isolate and protect sensitive data, the DSM and Vormetric Transparent Encryption work in tandem to allow security administrators to create a strong separation of duties between data owners and privileged IT administrators. Users and groups used in policies for access control to data can be based on system level roles, LDAP/AD, Hadoop users/groups/zones as well as container environment users and groups.

If desired, Vormetric Transparent Encryption can encrypt files, while leaving their metadata in the clear. This capability enables IT administrators to perform system administration tasks (such as replication, backup, migration, snapshots, and system updates), without exposure to sensitive data. Also included are capabilities to control basic system commands such as copy, write and directory listings.

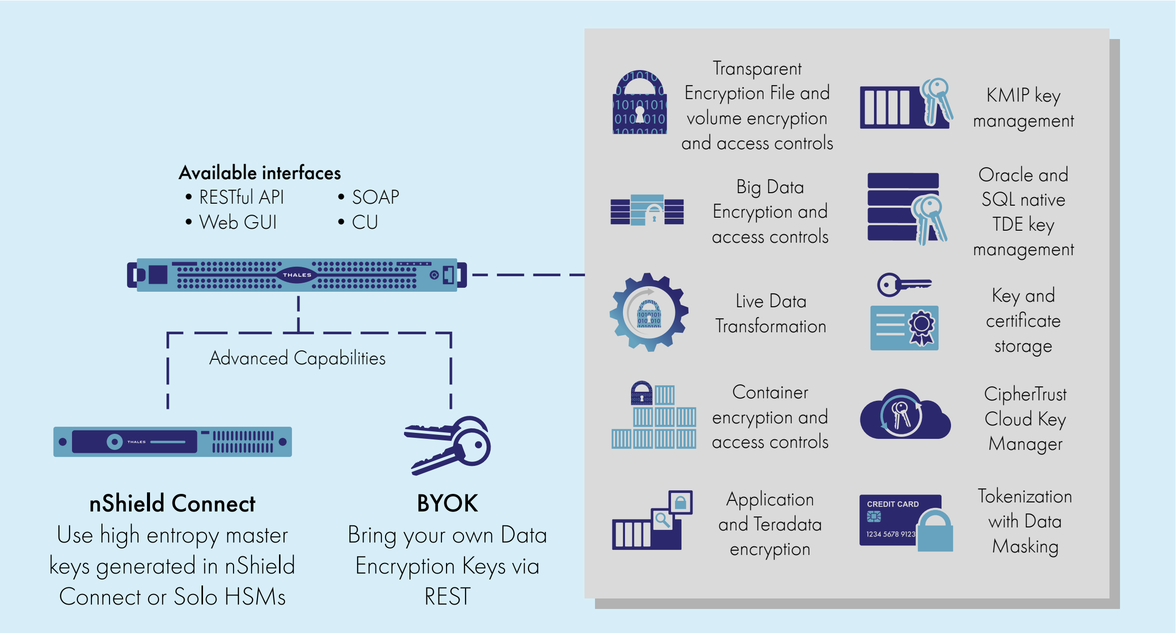
Available interfaces
• RESTful API
• SOAP
• Web GUI
• CU
THALES
Advanced Capabilities
nShield Connect
Use high entropy master keys generated in nShield Connect or Solo HSMs
BYOK
Bring your own Data Encryption Keys via REST
Transparent Encryption File and volume encryption and access controls
KMIP key management
Big Data Encryption and access controls
Oracle and SQL native TDE key management
Live Data Transformation
Key and certificate storage
Container encryption and access controls
CipherTrust Cloud Key Manager
Application and Teradata encryption
CREDIT CARD
1234 5678 9123
Tokenization with Data Masking

Figure 6. Centralized, integrated policy and encryption key management for all Vormetric Data Security Platform products

DSM High Availability

DSMs are clusterable for High Availability (HA), and Thales recommends this configuration for all implementations with a minimum deployment of two DSMs. When configured for HA, one DSM acts as the primary and others are used for failover, scalability or in additional locations where latency is a concern, such as a remote data center or cloud location.

All configuration settings, including changes to administrators, domains, hosts, keys, and policies, are made on the primary DSM, other DSMs are read-only. Configuration changes and updates on the primary DSM are pushed to the other DSMs at set intervals using replication.

APIs and interfaces

A web-based UI console, RESTful and SOAP APIs and command line interfaces are available. APIs make it possible to manage DSM functions remotely and are designed to operate in environments that require high levels of automation, such as service providers with cloud environments or highly automated data centers. SNMP MIBs are also available.

Security Intelligence Advanced data access audit logging and SIEM integration

Vormetric Transparent Encryption (VTE) agents and Vormetric Data Security Managers (DSMs) provide extensive logging capabilities detailing successful and attempted access attempts to protected data and the DSM management environment, agent interactions and key operations, as well as the actions of administrators at the DSM. Logs are designed to meet a range of needs for information from the solution. These include:

- Audit level information required by compliance, regulatory mandates, and best practice security reports
- Immediate insight into attempted access events by users and processes that may represent threats
- Detailed historical usage data that can be used to create baselines of expected operation from access pattern recognition

Logs are available in standard formats used by security information and event management (SIEM) systems (RFC5424, CEF and LEEF), and are available from DSMs as well as from systems hosting VTE agents. The primary DSM can be used as a collection point for all logs from DSMs and VTE agents if desired.

These logs are combined with pre-built integrations and dashboards for leading SIEM vendor environments. This deep visibility into data access can be used to alert on unauthorized access attempts to protected data that may represent a threat and to build typical access patterns when combined with other infrastructure and access information. For instance, a user that typically accesses information in small quantities from within a local network, if seen to be accessing large volumes of data from a remote location, would represent a threat that should be investigated and alerted.

Detailed logs include information about 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. Logs are designed to be able to easily meet the auditing requirements of compliance mandates and regulations as well by delivering the detailed evidence needed to prove to an auditor the encryption, key management, and access policies are appropriate and operating correctly.

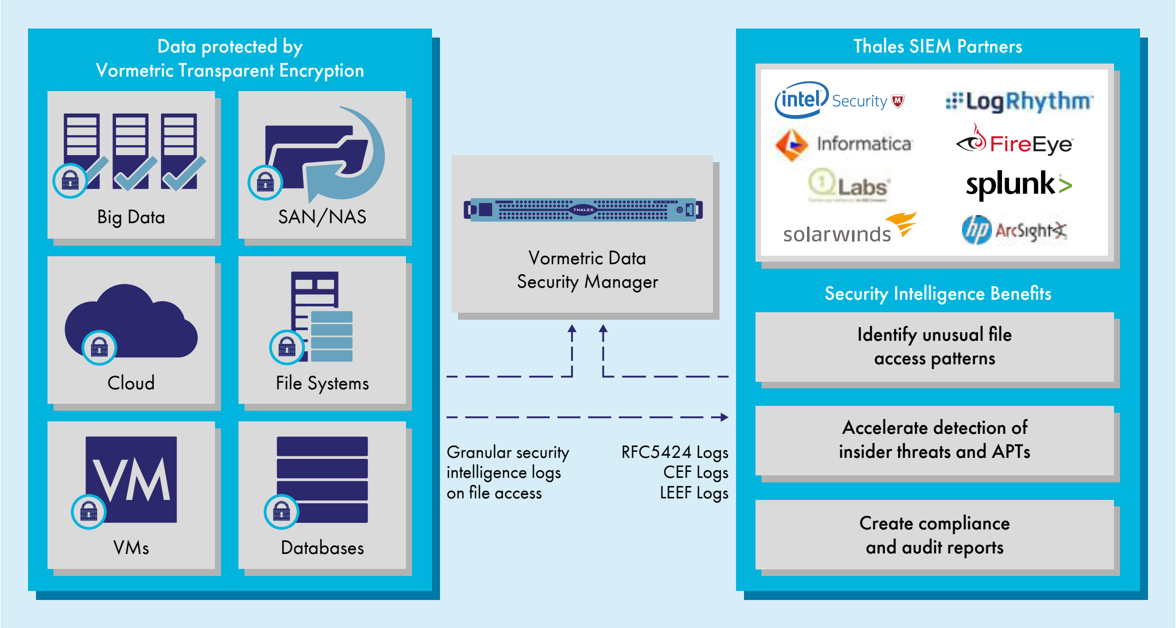

Figure 7. Vormetric Security Intelligence

Broad SIEM Platform Integration

Vormetric Security Intelligence offers proven integration 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.

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: Lack of visibility beyond simple OS logs into the activity around sensitive data access 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 an unauthorized download of files, while logged in from a remote location. Such inconsistent usage patterns could point to an APT attack or malicious insider activities.

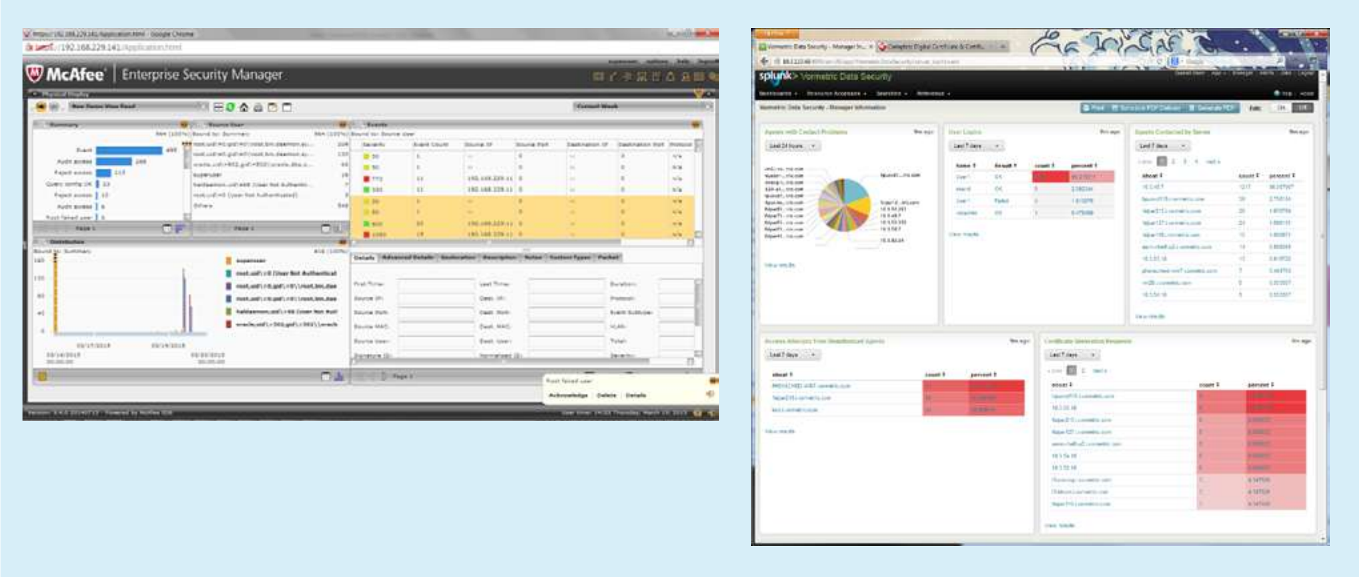

Figure 8. McAfee Enterprise Security Manager and Splunk SIEM Integration

Live Data Transformation Extension

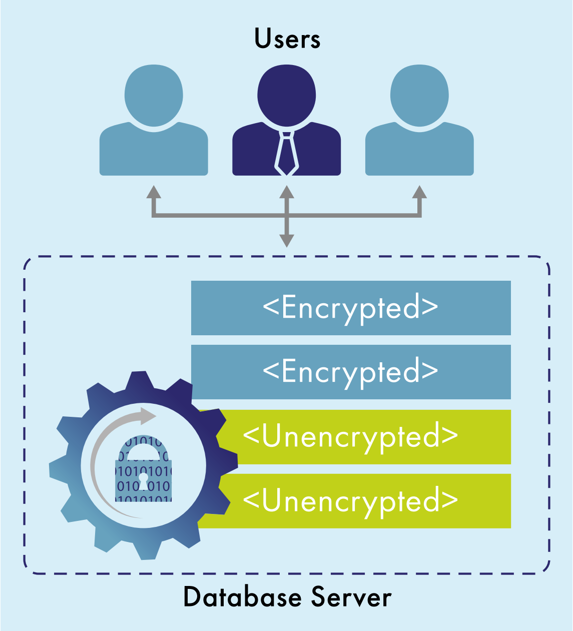

Figure 9. Vormetric Transparent Encryption with Vormetric Live Data Transformation Enabled

Thales patented Vormetric Live Data Transformation extension for Vormetric Transparent Encryption is designed to solve problems that have plagued encryption solutions in the past with the downtime and expense required to encrypt data sets initially, and then to periodically rekey encrypted information as required by compliance and best practice requirements.

Live Data Transformation (LDT) solves these problems. Enabled for Vormetric Transparent Encryption agents with a license key at the Vormetric Data Security Manager, LDT makes it possible for initial encryption and later rekeying operations to occur while the data set is still in use. The results are zero-downtime encryption deployment and seamless, non-disruptive key rotation.

In the past, organizations typically took one of two approaches to encrypt data initially or later rekey the information.

- Failover application operation to a backup location while operations occur on the primary data set
- Take critical applications off-line for the time required

Either approach can be costly in terms of people-time, physical resource use, risk and even loss of income (for mission-critical applications that drive revenue).

Vormetric Transparent Encryption with Live Data Transformation enables non-disruptive initial encryption and simplified, more-compliant encryption key rotations. To put it simply, users and applications continue to operate as usual while encryption and rekeying operations take place. This capability enables organizations to:

- Meet compliance requirements for encryption and access control without taking applications offline
- Expand encryption implementations with minimal impact on application operations and users
- Reduce the impact and cost of implementing encryption by eliminating encryption and rekeying downtime

Further, the solution easily supports versioned backups and archives using encryption metadata. The result when restoring an older data set is immediate usability using the encryption key version applied when the backup or archive was created. Resiliency is another key characteristic of the solution. Issues such as system failures, power outages, and network downtime are accounted for, and interrupted encryption processes will seamlessly recover after system restart.

Container Security Extension

Vormetric Container Security is an extension of Vormetric Transparent Encryption that directly extends the solution's encryption, key management, access controls and data access audit logging capabilities to support Container environments (at the time this document is written – Docker and OpenShift). With an agent installed on the container host, capabilities are available to all container images running within the environment with no changes to containers or the applications that run within their environments required.

Enabled for Vormetric Transparent Encryption agents with a license key at the Vormetric Data Security Manager, Container Security extends VTE's available security controls to include:

- Container users and groups
- Data stored within containers
- Data stored within linked storage environments (SAN, NAS, disk, cloud, and others)

The solution mitigates the additional risks found within these environments, as well as protecting container images while in storage or use.

- **Exposure to privileged user abuse.** By default Docker processes run with root privileges, while for OpenShift, Cluster Administrators have full access to all Tenant Secrets. This level of privileged access can pose multiple risks. For example, container administrators may have unchecked access to images and the data stored within them, as well as expose organizations to privilege escalation attacks.
- **Cross container access.** Poor configuration of permissions can result in multiple containers having access to information that should remain private. Further, when containers are hosted in shared virtualized or cloud environments, critical information can be exposed to third parties.
- **Compliance risks.** Many compliance mandates require strong controls for, and auditing of, data access. However, many security teams have limited controls available for managing and tracking access to data that is 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.

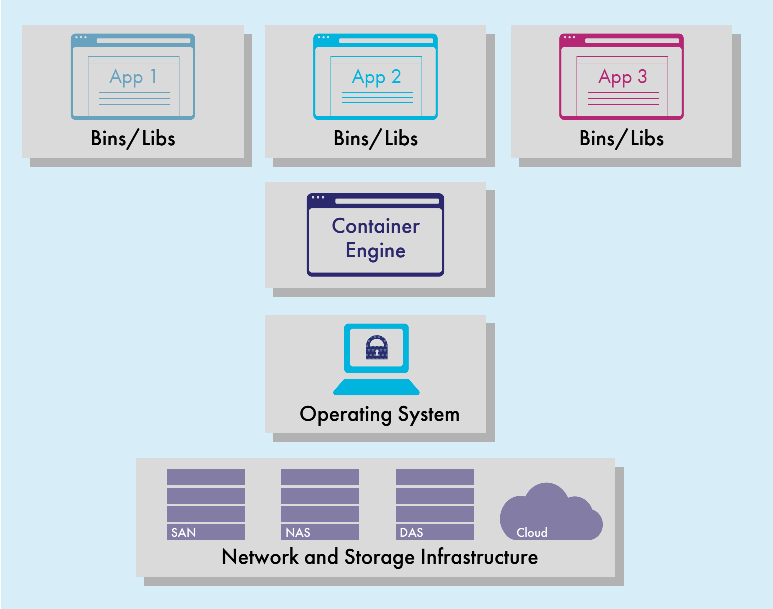

Figure 10. Vormetric Transparent Encryption with Vormetric Container Security Enabled

Deployment and Maintenance with Vormetric Orchestrator

Larger organizations and cloud service providers alike face a daily challenge in maintaining systems. With thousands of systems per administrator, and high rates of changes as systems come and go, how can systems remain up-to-date with policy, patches and configuration changes? The answer to the need for encryption at scale is automation.

To aid organizations in solving this problem, the Vormetric Orchestrator from Thales includes extensive capabilities for deploying and maintaining VTE agents and policies. Easily integrated with existing IT configuration management tools the Orchestrator also includes a plug-in architecture that supports Chef, Ansible, and Puppet with RESTful APIs and CLI tools that allow for scripting and extended integration when needed. Deployed as a virtual appliance, the solution can be employed wherever Vormetric Data Security Platform products are used – in data centers, virtual infrastructure, and cloud environments.

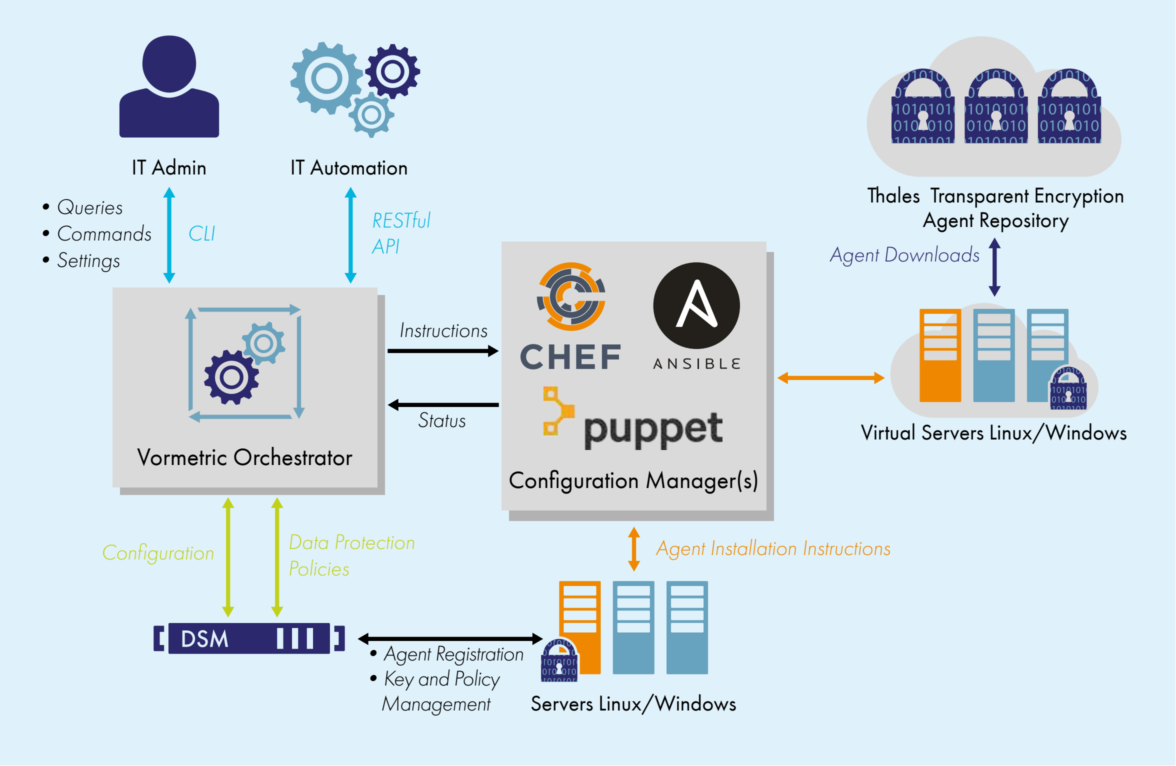

Figure 11. Using Vormetric Orchestrator with Vormetric Transparent Encryption

Bring your own data encryption keys

As organizations increasingly place business-critical data within multiple cloud environments the question of who controls the encryption keys that protect sensitive data becomes increasingly important. Enterprises prefer to control and even create the data encryption keys protecting their cloud environment data. Those with the highest levels of IT security requirements, may even wish to control the creation of their in-house keys for maximum complexity, randomness and assurance.

The Vormetric Data Security platform provides the capability for cloud service providers and enterprises to offer multi-tenanted access to Vormetric Data Security Managers (DSMs) that enables them to create and bring in data encryption keys used with Vormetric Transparent Encryption agents rather than use the data encryption keys generated by the DSM. Data encryption keys can be created by a trusted hardware device (such as a Thales or third-party Hardware Security Module) or from an existing key management and creation application. Keys imported for use with VTE agents can then be used as needed with policies created within the DSM.

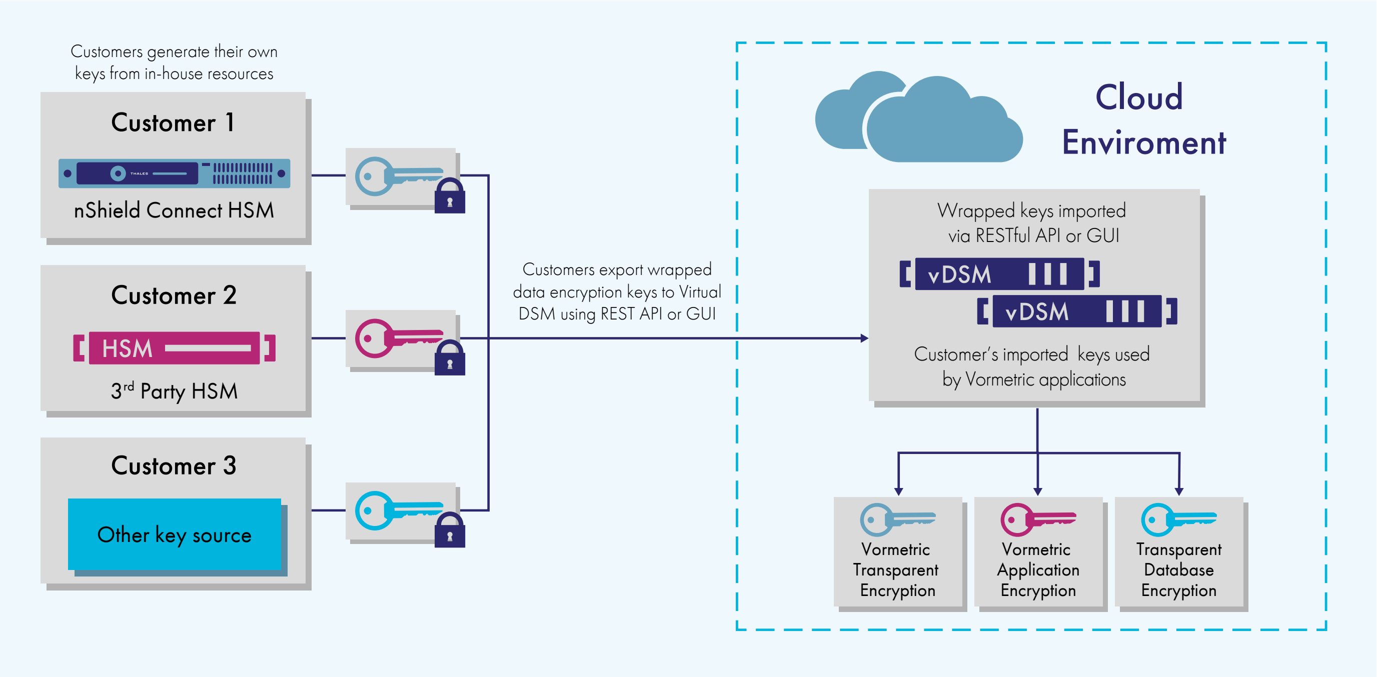
Customers generate their own keys from in-house resources
Customer 1
nShield Connect HSM
Customer 2
HSM
3rd Party HSM
Customer 3
Other key source
Customers export wrapped data encryption keys to Virtual DSM using REST API or GUI
Cloud Enviroment
Wrapped keys imported via RESTful API or GUI
vDSM
vDSM
Customer's imported keys used by Vormetric applications
Vormetric Transparent Encryption
Vormetric Application Encryption
Transparent Database Encryption

Figure 12. Maintion complete control of encryption keys, even within multi-tenant cloud enviroments

Use cases

Databases and unstructured files – across data centers and cloud environments

As organizations continue to grow their infrastructure and data sets, they must increasingly deal with a mix of in-house and cloud-based data assets and applications. Regardless of where this data is located, it requires the same level of data security and protection. Vormetric Transparent Encryption enables enterprises to choose their implementation mode for data security based on their risk tolerance, compliance, and privacy requirements.

Most enterprises will opt for a solution that includes managing and controlling encryption keys and access policies for both local data center resources and cloud environments from their local data center for both local and cloud deployments. This approach keeps control of keys firmly within the enterprise, eliminating the risk of remote legal access or compromise at the cloud provider. Enterprises that are "all in" the cloud and make no use of local data center compute resources may wish opt for a cloud-based deployment of key and policy management, either co-locating cloud key management in the same cloud with data protected by VTE, using a secondary cloud environment for the DSM to provide a greater degree of separation and lower risk, or to use a co-location or hosting provider for hardware versions of DSMs.

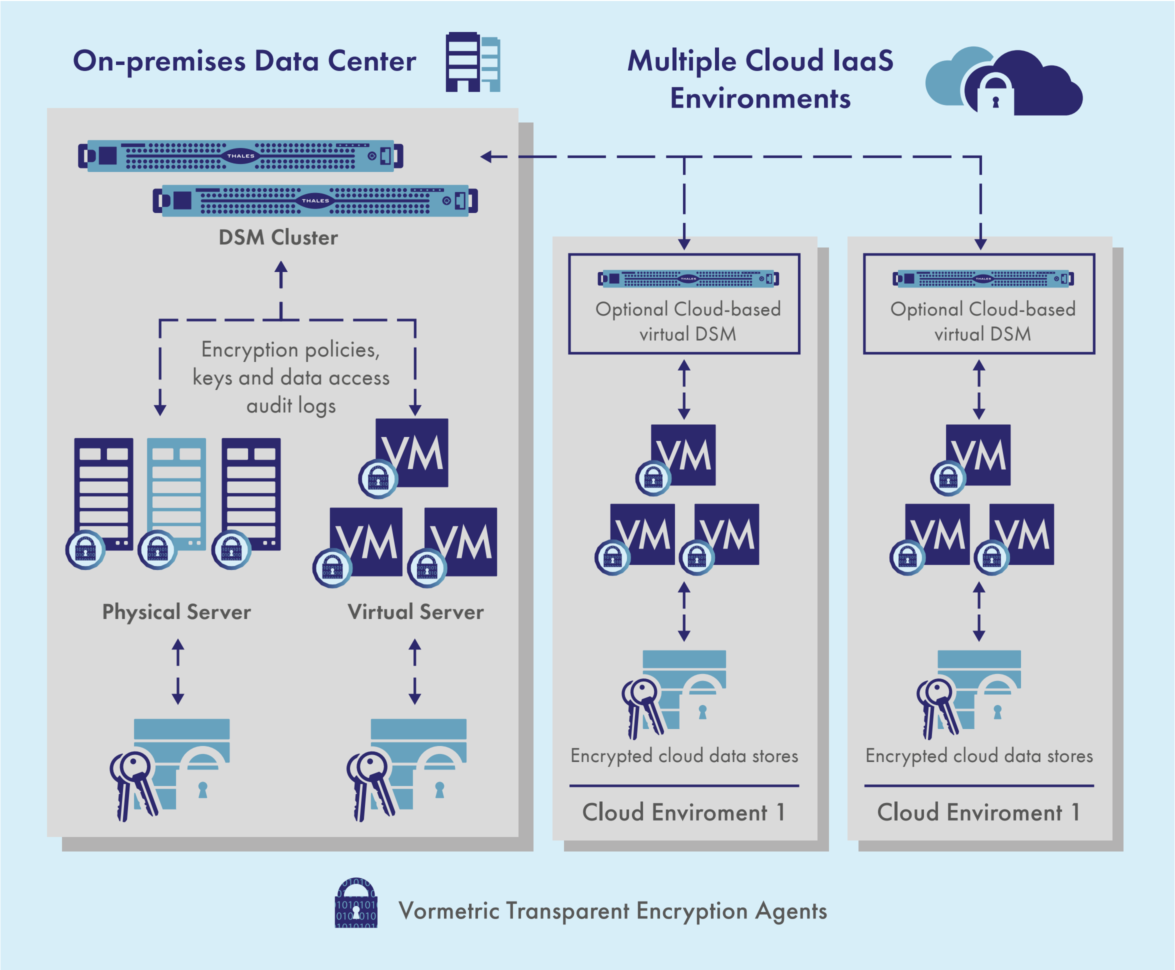
On-premises Data Center
Multiple Cloud IaaS Environments
DSM Cluster
Encryption policies, keys and data access audit logs
VM
Physical Server
Virtual Server
Optional Cloud-based virtual DSM
Optional Cloud-based virtual DSM
Encrypted cloud data stores
Encrypted cloud data stores
Cloud Enviroment 1
Cloud Enviroment 1
Vormetric Transparent Encryption Agents

Figure 13. Fully integrated enterprise on-premises and cloud enviroment deployment

All of these scenarios are easily supported with Vormetric Transparent Encryption by locating physical or virtual DSMs in local data centers, co-location vendors, hosting solutions or cloud environments as needed.

Regardless of the deployment model, a typical database protection scenario includes a VTE agent deployed to database servers with a simple policy – a signed database process and the database user are allowed cleartext access to the protected data store, all others will only see file metadata and ciphertext. This effectively shields the database access from compromise by root and privileged user-based attacks, local system and LDAP users and groups while also meeting compliance and best practice requirements for safeguarding the data set with encryption.

For larger data-sets customers will typically purchase the Live Data Transformation extension to VTE, enabling immediate encryption of the database without taking critical applications offline, and periodic rekeying to meet compliance and best practice requirements without downtime.

For a typical unstructured file system protection example, we'll use a Microsoft SharePoint server. The VTE agent is deployed to the server with separate policies for LDAP/Active Directory user groups. For instance, allowing only Finance department members to access critical accounting data, HR to access confidential employee information and Engineering to access development documents. Each data store section is encrypted with an individual key by policy, effectively limiting the access to only those who require it for their work.

Big Data

With nearly every enterprise embracing big data environments, and with large numbers of these environments implemented in the cloud, the security of the sensitive data within the data lake, source data environments and the reports that hold high-value correlated results have become an insistent concern.

Vormetric Transparent Encryption is an important tool for protecting this information. The solution can be used to protect data at the file system level within compute notes (and underlying storage), source data locations as well as the repositories used for logs and reports. However, this protection extends beyond the system level users/groups and LDAP/AD users and groups that are enforced by VTE on a typical server. The solution also enforces policy-based encryption, access controls and data access logging by Hadoop users, groups and zones. This capability provides further protection for privileged users within the big data lake or users within the environment

A typical deployment includes agents installed on compute nodes, source data servers and servers accessing log/report repositories. Data is encrypted throughout the environment with appropriate access policies, and data access logging controls provided by the Vormetric Data Security Manager. Further, the use of underlying hardware encryption capabilities in underlying compute infrastructure results in minimal overhead from encrypt/decrypt operations – making it possible to use the solution even where speed and compute capability are critical.

Further, Thales works with leading big data environment vendors as a partner to ensure solution capability and operation. At the time this document is written, these partners include DataStax, MondoDB, Teradata, IBM, Cloudera, Couchbase, SAP HANA, Hortonworks and AWS (with EMR cluster in AWS Compute).

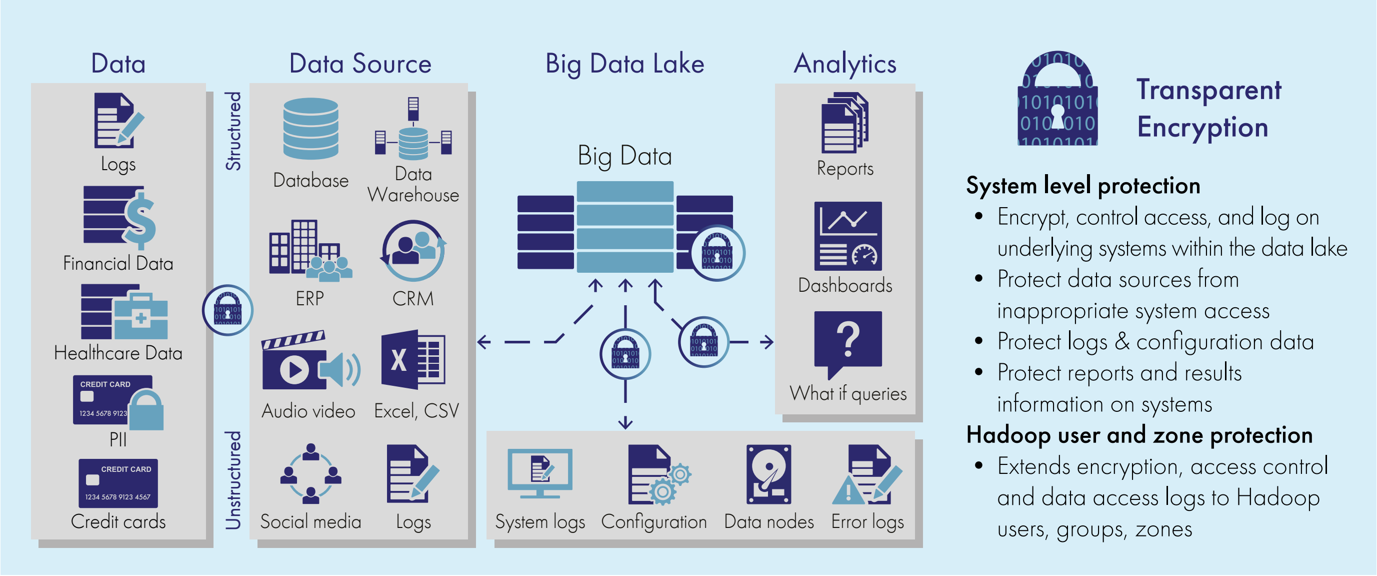

Figure 14. Protecting data within big data environments using Vormetric Transparent Encryption

Using AWS S3 and Azure Files storage – In cloud and on premises

As organizations increasingly use cloud storage as part of new application implementations, as well as backups and failover environments, they now need to protect data within these cloud storage environments just as they would have if the storage were located within their own data center.

Vormetric Transparent Encryption provides explicit support for these needs with AWS and Azure cloud storage. All the benefits, controls and features available with VTE – encryption, policy-based access controls, integrated key management and data access audit logs apply to operation with cloud storage as well.

AWS support includes the standard in cloud EBS/EFS file system support, and with use of the AWS Storage Gateway supports S3 bucket access (Standard, Infrequent and Glacier) for use both in the cloud and from customer data centers.

Similarly for Microsoft Azure, in cloud Azure compute instances support SSD/STD Disks as well as both GRS & LRS storage with SMB/CIFS via Azure Files from both in the cloud and on enterprise premises.

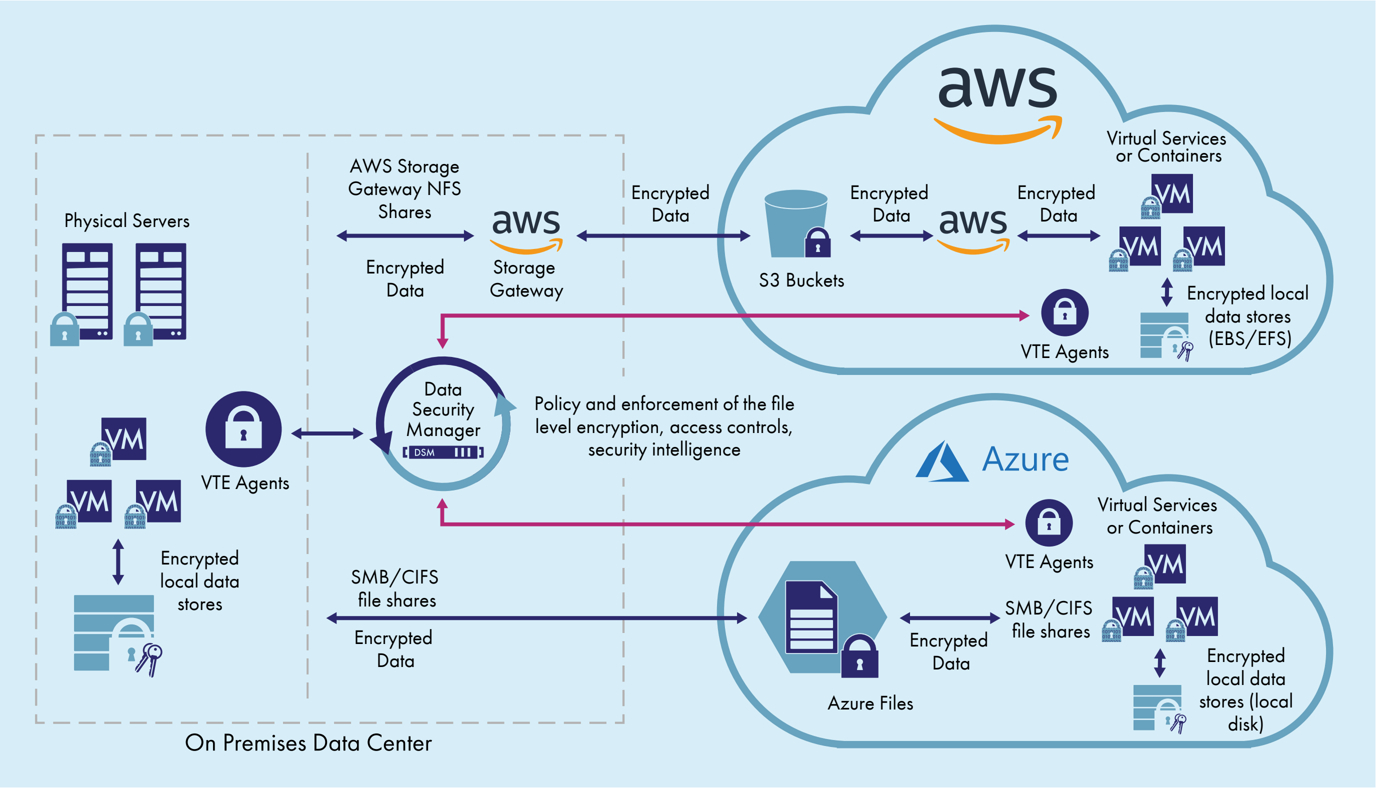
aws
Virtual Services or Containers
VM
Physical Servers
AWS Storage Gateway NFS Shares
Encrypted Data
aws Storage Gateway
Encrypted Data
S3 Buckets
Encrypted Data
aws
Encrypted Data
Encrypted local data stores (EBS/EFS)
VTE Agents
Data Security Manager
DSM
Policy and enforcement of the file level encryption, access controls, security intelligence
VTE Agents
Encrypted local data stores
Azure
Virtual Services or Containers
VTE Agents
SMB/CIFS file shares
Encrypted Data
Azure Files
Encrypted Data
SMB/CIFS file shares
Encrypted local data stores (local disk)
On Premises Data Center

Figure 15. Maintion complete control of encryption keys, even within multi-tenant cloud enviroments

Summary

The demands for data-at-rest encryption continue to grow more urgent as compliance requirements, external attacks and digital transformation add more environments, expand attack surfaces and result in more threats to sensitive data. Now more than ever, encryption represents a critical means for guarding critical IP, PII, customer or citizen information and more. With Vormetric Transparent Encryption, organizations can leverage a solution that addresses a wide range of environments and use cases for protecting file and volume data wherever they are used, and is also an element of a single platform solution that provides a comprehensive data-at-rest security solution set. Through these advanced capabilities, organizations can address their security mandates, while minimizing costs and administrative efforts.

Appendix: Performance benchmarks

Intel®, AMD, and PowerPC processor family all include hardware accelerated encryption capabilities that are leveraged by Vormetric Transparent Encryption agents. For Intel, this includes Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI). AES-NI accelerates AES encryption and has been optimized for fast throughput and low latency. Vormetric Transparent Encryption uses AES-NI instructions for hardware-based acceleration of data encryption and decryption. In fact, Vormetric Transparent Encryption has a proprietary encryption engine that is designed to take full advantage of the parallelism that can be achieved with multi-core processor chipsets and it specifically leverages the pipelining capabilities of AES-NI. As a result, the solution delivers the maximum performance possible.

In addition to leveraging hardware-based encryption capabilities, Vormetric Transparent Encryption is tightly integrated with, and optimized for, each supported operating system kernel. Consequently, Vormetric Transparent Encryption leverages the latest features available for every platform supported, rather than being coded to a lowest common denominator across multiple platforms. With each new release, Thales continues to add new capabilities that enable the solution to exploit the latest operating system features.

For many applications, the performance overhead that Vormetric Transparent Encryption introduces is negligible. However, as loads associated with input/output (I/O) increase, there will be increased overhead associated with encryption. Even with demanding, I/O heavy applications, such as databases or big data processing, Vormetric Transparent Encryption generally introduces less than 10% overhead.

One example can be seen in the chart below. In this example, the Yahoo Cloud Serving Benchmark (YCSB) was run against MongoDB 3.0.2, with the WiredTiger storage engine running on top of Vormetric Transparent Encryption. YCSB is a generally available open source framework that has a common set of workloads for evaluating the performance of different "key-value" and "cloud" serving stores. The workload was configured so that less than one-half of the data set could fit in memory, causing a heavy I/O load. As the chart illustrates, Vormetric Transparent Encryption only introduced minimal overhead.

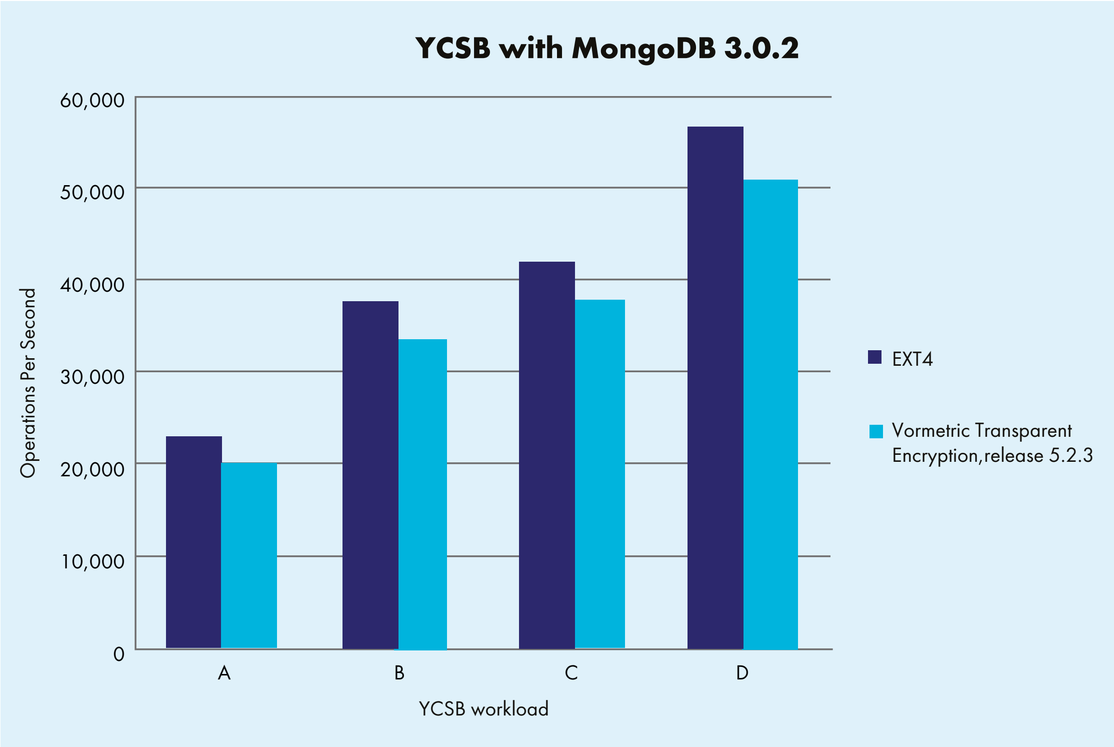

Figure 16. Even when testing in a scenario with a heavy I/O load, Vormetric Transparent Encryption introduces minimal performance overhead.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

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

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

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

> thalescpl.com <