thalesesecurity.com

THALES

Vormetric Transparent Encryption

Challenge: securing sensitive data across changing environments and increasing threats

Safeguarding sensitive data requires much more than just securing a data center's on-premises databases and files. The typical enterprise today uses three or more IaaS or PaaS providers, along with fifty or more SaaS applications, big data environments, container technologies, and their own internal virtual environments and private clouds.

To further complicate the problem, cyber-attacks have grown in sophistication and power. New compliance and regulatory mandates around protection of sensitive information keep on coming, and existing regulations have become more stringent.

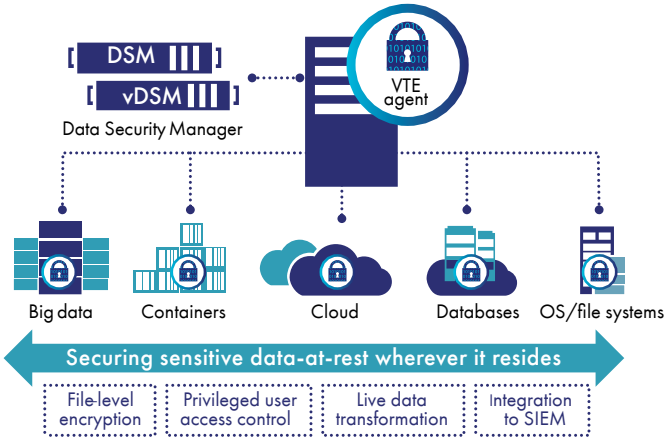
Solution: Vormetric Transparent Encryption

Vormetric Transparent Encryption (VTE) delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging that helps organizations meet compliance and best practice requirements for protecting data, wherever it resides. The FIPS 140-2 level 1 validated VTE agent resides at the operating file-system or device layer and encryption and decryption is transparent to all applications that run above it. VTE provides rich access controls, which allow organizations to determine who can access data, when they can access it, and what type of access they have.

Securing sensitive data-at-rest wherever it resides

- Meet compliance and best practice requirements for encryption, access control and data access logging using a proven hardware accelerated encryption solution that secures files, volumes and linked cloud storage, while enabling access control and data access audit logging in physical, virtual and cloud environments.
- Deployment is simple, scalable and fast with centralized key management, encryption and access policies that reach across multiple clouds, on-premises and within big data, and container environments.
- Easily implement privileged user access controls to enable administrators to work as usual, but protect against users and groups that are potential threats to data.

Vormetric Transparent Encryption



- Leverage detailed, actionable security event logs that provide unprecedented insight into file access activities to identify and stop threats faster.
- Broadest platform support in the industry. Protects structured and unstructured data accessed by Linux, UNIX and Windows systems, as well as cloud storage environments like Amazon S3 and Azure Files.
- Eliminate the downtime required for initial encryption and re-keying operations by adding the Live Data Transformation option. There is no other data encryption solution that offers this unique capability.

Key advantages

Transparent data protection. Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.

Seamless and easy to deploy. 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.

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

High-performance hardware accelerated encryption. Vormetric Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.

Comprehensive security intelligence. Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enables data security analytics. Pre-built integration and dashboards are available for major system vendors that make it easy to find denied access attempts to protected data.

Broadest system and environment 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.

Advanced security

Zero-downtime data transformation. Live Data Transformation option eliminates the downtime required for initial encryption and scheduled rekeying operations.

This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.

Container support. Vormetric Container Security extends policy-driven 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 provides the automation needed to easily deploy and maintain Vormetric Transparent Encryption at scale.

Advanced access controls for big data (Hadoop). When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.

SAP HANA qualified. SAP has qualified Vormetric Transparent Encryption with HANA v2.0 to deliver data encryption, key management, privileged user access control, and granular file access audit logs.

Solution architecture

Deployments consist of Vormetric Transparent Encryption agents and Vormetric Data Security Manager (DSM) appliances. Policy and key management is centralized at the DSM. The DSM is available as a FIPS 140-2 level 1, 2 or 3 appliance and features RESTful, SOAP and command line APIs as well as web-based management interfaces.

Fulfill all your data protection requirements

Thales eSecurity simplifies securing data at rest with comprehensive data security solutions available from the Vormetric Data Security Platform. These include Vormetric Tokenization with Dynamic Data Masking, Vormetric Application Encryption and the CipherTrust Cloud Key Manager.

About Thales eSecurity

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.

> thalesesecurity.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 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