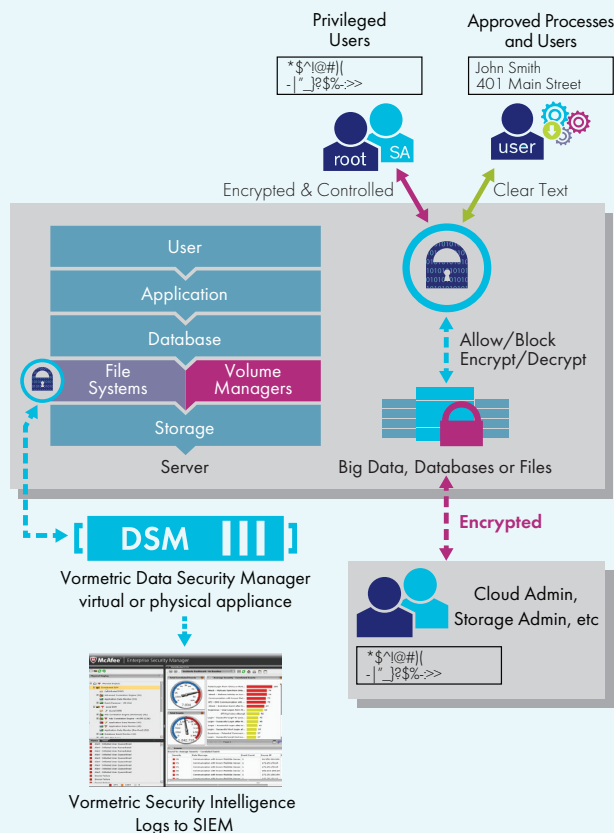


SAFEGUARD DATA EVERYWHERE AND ACHIEVE COMPLIANCE

- Achieve compliance with data protection mandates by securing data-at-rest with encryption, access controls and data access audit logging wherever it resides – across multiple clouds, on-premises or within big data and container environments
- Realize data security faster without changing business processes with encryption transparent to users, applications and infrastructure
- Simplify data security administration with centralized key management, encryption and access policies that reach across cloud and data center environments
- Privileged user access controls that enable administrators to work as usual, but never be exposed to sensitive data
- Minimize deployment and maintenance downtime by encrypting and re-keying while data is in use

Thales eSecurity

VORMETRIC TRANSPARENT ENCRYPTION FROM THALES



Vormetric Transparent Encryption encrypts, enforces access policies, and logs all file access

CHALLENGE: SAFEGUARDING MORE DATA, IN MORE ENVIRONMENTS, AGAINST MORE THREATS

For IT and security teams in today's organizations, adaptation is a key part of the job. Sensitive data continues to make it into a broader set of environments, including cloud deployments, big data platforms, containers, virtualized systems, and more. Policies and regulatory mandates continue to grow more stringent even as cyber attacks have grown in sophistication and power.

To adapt to these expanding demands, IT and security professionals have to leverage technologies that offer a strong mix of security, implementation flexibility, and operational efficiency—and that's exactly what they get from Vormetric Transparent Encryption.

SOLUTION: VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging that helps organizations meet compliance reporting and best practice requirements for protecting data, wherever it resides. Transparent Encryption protects structured databases and unstructured files on-premises, across multiple cloud environments, and even within big data and container implementations. Designed to meet data security requirements with minimal disruption, effort, and cost, implementation is seamless – keeping both business and operational processes working without changes even during deployment and roll out.

VORMETRIC TRANSPARENT ENCRYPTION FROM THALES

KEY ADVANTAGES

- **Continuous protection.** Unlike full disk encryption technologies, Vormetric Transparent Encryption's protection does not end after encryption is applied. Vormetric Transparent Encryption 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.** Vormetric Transparent Encryption enforces granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by user (including for administrators with root privileges, other system level users and LDAP/Active Directory users and groups), 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
- **Non-intrusive and easy to deploy.** Vormetric Transparent Encryption agents are deployed on servers at the file system or volume level, 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, standard-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
- **Flexible and scalable.** 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. This agent based architecture eliminates the bottlenecks and latency that plague legacy proxy-based solutions
- **Hardware accelerated encryption.** Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs (Intel AES-NI, AMD AES-NI, IBM Power8 encryption and Oracle SPARC encryption), delivering encryption with optimal performance even in virtual and cloud environments

ADVANCED SECURITY

- **Zero-downtime data transformation.** Vormetric Transparent Encryption can alleviate the planned downtime required for initial encryption and scheduled rekeying operations seamlessly by adding the Vormetric Live Data Transformation option to deployments
- **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 automates 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

SOLUTION ARCHITECTURE

Deployments consist of Vormetric Transparent Encryption agents and Vormetric Data Security Manager (DSM) appliances. Agents are deployed on servers in environments from data centers to cloud, containers and big data. Policy and key management is centralized at the DSM. The DSM is available as a FIPS 140-2 level, 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 on the Vormetric Data Security Platform. These include [Vormetric Tokenization with Dynamic Data Masking](#), [Vormetric Application Encryption](#), the [Vormetric Cloud Encryption Gateway](#).

LEARN MORE

Visit us at www.thalesecurity.com to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

