THALES

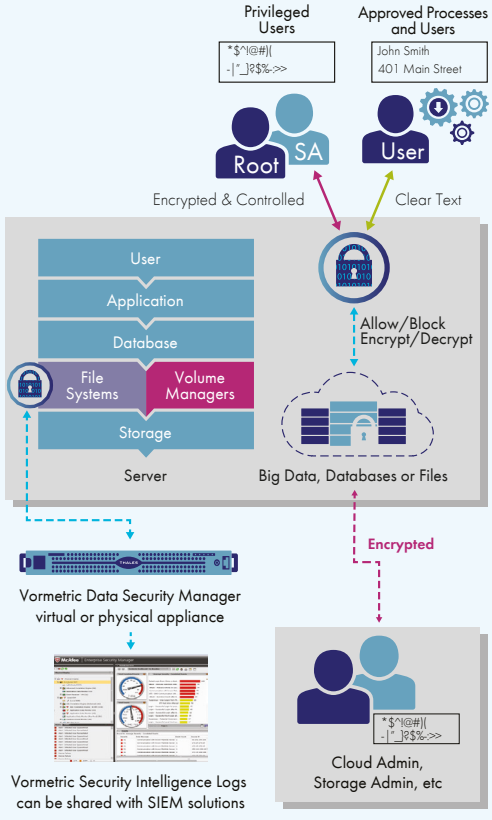
www.thalesesecurity.com

SECURING SENSITIVE DATA-AT-REST WHEREVER IT RESIDES

- Achieve compliance with data security mandates for data-at-rest by securing files, volumes and linked cloud storage with encryption, access controls and data access audit logging wherever it resides – across multiple clouds, on-premises and within system, big data and container environments
- Simplify data security administration with centralized key management, encryption and access policies that reach across cloud and data center environments
- Quickly protect existing and new data sets against data breaches without impacting applications, users or operational workflows
- Easily implement 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, volume and linked cloud storage access

CHALLENGE: PROTECTING MORE DATA, IN MORE ENVIRONMENTS, AGAINST MORE 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, while compliance and regulatory mandates around protection of sensitive information have become more stringent.

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, unstructured files, and linked cloud storage accessible from systems 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.

‹Thales eSecurity›

VORMETRIC TRANSPARENT ENCRYPTION FROM THALES

KEY ADVANTAGES

- **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.
- **Non-intrusive 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, 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.
- **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. 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.** 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 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 from the Vormetric Data Security Platform. These include **Vormetric Tokenization with Dynamic Data Masking**, **Vormetric Application Encryption** and the **CipherTrust Cloud Key Manager**.

LEARN MORE

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

Follow us on:

Americas – Thales eSecurity 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