FORWARD THINKING IT SOLUTIONS

Vormetric Data Security Platform

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

Built on an extensible infrastructure, the platform features multiple data security products that can be deployed individually or in combination to deliver advanced encryption, tokenization and centralized key management. This data security solution prepares your organization for the next security challenge and new compliance requirement at the lowest TCO.

Benefits

One platform, centrally managed for delivering comprehensive data security solutions.

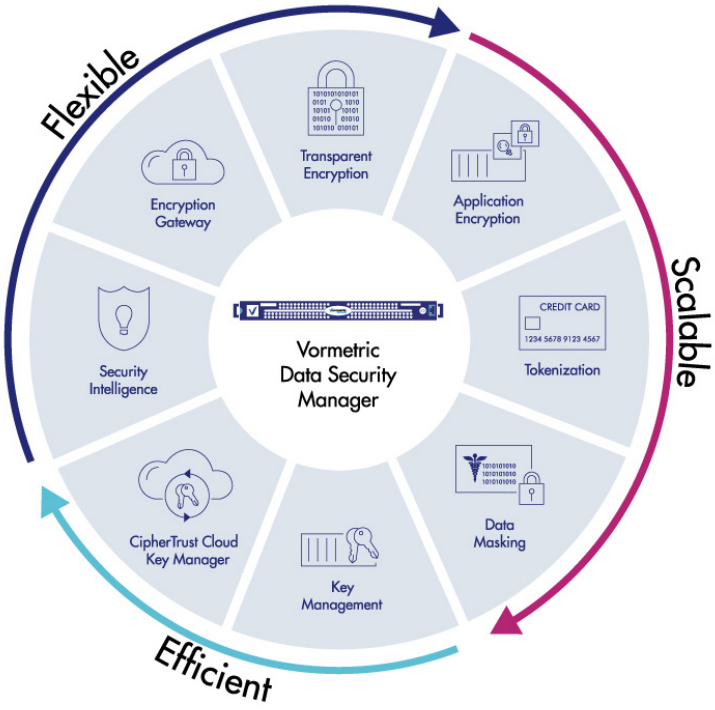
Specification

Policy and Key Management: FIPS 140-2 compliant virtual appliance or hardware appliance

Supported Environments: Physical Server, Virtual Server, Public-Private-Hybrid Cloud, Big Data, Container

Encryption Techniques: Advanced Encryption Standard (AES), Format Preserving Encryption (FPE), Granular Database, Transparent File-level, Cloud Gateway

Data Pseudonymization Techniques: Cryptographic Tokenization, Random Tokenization, Dynamic Data Masking, Static Data Masking, Batch Transformation



ergonomics

Vormetric Data Security Manager - Centrally manage your organization's encryption keys

The Vormetric Data Security Manager (DSM) is at the heart of the Thales e-Security product line. The DSM provisions and manages keys for the Vormetric Data Security Platform and manages keys and certificates for third-party devices.

Benefits

Unified, Simplified Management: The DSM enables centralized management of data security policies and key management, simplifying training, deployment and operations.

Flexible Form Factors: The DSM is available in different form factors and FIPS 140-2 levels. Deploy virtual appliances on-premises, in private and public clouds or select high-assurance hardware.

Centralize Key and Policy Management: Provision and manage keys for all Thales e-Security products, and manage keys and certificates for third-party devices.

Features

Flexible Deployment Form Factors: The DSM is offered as a FIPS 140-2 Level 1 virtual appliance, as well as two hardware appliances: The V6000, which is FIPS 140-2 Level 2 certified, and the V6100, which is FIPS 140-2 Level 3 certified. The platform is also available on the Amazon Web Services (AWS) Marketplace and the Microsoft Azure Marketplace.

Unified Management and Administration: The DSM provides central management and secure storage of encryption keys, including those generated by Thales e-Security products, KMIP-compliant devices, Microsoft SQL Server TDE, Oracle TDE and IBM Guardium Data Encryption. Its intuitive Web-based console, CLI, or APIs are used for managing encryption keys and policies.

Maximum Security and Reliability: To maximize uptime and security, the DSM features redundant components and the ability to cluster appliances for fault tolerance and high availability. Strong separation-of-duties policies can be enforced to ensure that one administrator does not have complete control over data security activities, encryption keys or administration. In addition, the DSM supports two-factor authentication for administrative access as well as nShield Remote Administration with smart card access in the V6100.

Specifications

Administrative interfaces: Secure Web, CLI, SOAP, REST

API support: PKCS #11, Microsoft Extensible Key Management (EKM), SOAP, REST

Security authentication: Username/password, RSA two-factor authentication (optional)

Backup: Manual and scheduled secure backups. M of N key restoration.

Network management: SNMP, NTP, Syslog-TCP

Certifications: FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level 3, Common Criteria (ESM PP PM V2.1)

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00