COMPLYING WITH SOUTH AFRICA'S PROTECTION OF PERSONAL INFORMATION ACT

- Prevent breaches through granular access control and separating privileged user access from sensitive data
- Avoid breach notification requirements by encrypting or tokenising the data
- Identify irregular access patterns and breaches in progress through security intelligence logs
- Apply access controls to ensure only credentialed users can retrieve the data

‹Thales eSecurity›

HELPING ORGANISATIONS COMPLY WITH SOUTH AFRICA'S POPI ACT

Thales eSecurity's Vormetric Data Security Platform provides tools you need to help comply with South Africa's Protection of Personal Information Act and prevent data breaches, irrespective of your data environment – on-premises, cloud or hybrid. Should a breach occur, you may be able to avoid a public breach notification if affected data has been encrypted with the Vormetric Platform.

REGULATION

Summary

The South African Protection of Personal Information (POPI) Act, which became law on 11th April, 2014, requires organisations that handle Personally Identifiable Information (PII) to ensure they comply with the legislation or face large fines, civil law suits or even prison. The Act extends certain rights to data subjects that give them control over how their personal information can be collected, processed, stored and shared.

HELPING ORGANISATIONS COMPLY WITH SOUTH AFRICA'S POPI ACT

Penalties

According to Chapter 11 (Offences, Penalties and Administrative Fines) of the POPI Act:

> 107. Any person convicted of an offence in terms of this Act, is liable, in the case of a contravention of–
>
> (a) section 100, 103(1), 104(2), 105(1), 106(1), (3) or (4) to a fine or to imprisonment for period not exceeding 10 years, or to both a fine and such imprisonment; or
>
> (b) section 59, 101, 102, 103(2) or 104(1), to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

According to Chapter 11, "a Magistrate's Court has jurisdiction to impose any penalty provided for in section 107."

COMPLIANCE

Summary

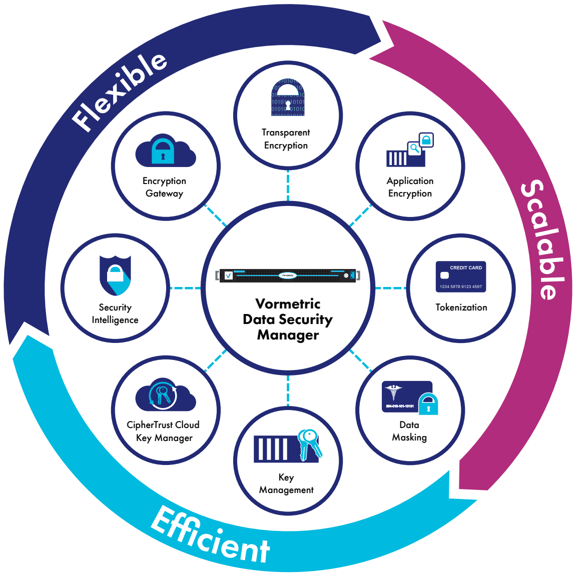
Condition 7 of the POPI Act outlines the criteria for securing personal information. Thales eSecurity helps organisations address items 19 and 22 of Condition 7.

Item 19 of Condition 7 states that an organisation must secure the integrity and confidentiality of personal information against loss, damage, unauthorised destruction and prevent unlawful access. Item 19 also requires organisations to assess the potential risks to personal information and establish safeguards against such risks. These safeguards must be regularly assessed, maintained, updated and audited to ensure a company's compliance.

Item 22 outlines the action that organisations must take if "the personal information of a data subject has been accessed or acquired by any unauthorised person." The responsible party must notify the Regulator and the data subject whose data has been breached "as soon as reasonably possible after the discovery of the comprise." The Regulator has the right to force the organisation concerned to publish details of the data breach with the only exception being the security of either the nation or the individuals.

To address Item 19, Thales eSecurity's **Vormetric Data Security Platform** helps safeguard personal data against loss, damage, as well as unauthorised destruction or unauthorised access. Specifically, **Vormetric Transparent Encryption** protects personal information with data-at-rest encryption using the AES hardware encryption algorithms built into system CPUs. Further, Vormetric Transparent Encryption's integrated **Key Management** offers highly secure, centralised protection of encryption keys.

Vormetric Transparent Encryption provides data-centric protection that ensures that, if data is stolen, it is unintelligible to those who steal it. Therefore, organisations can avoid the breach notification requirement in Item 22 because data subjects' personal information will not have been compromised.

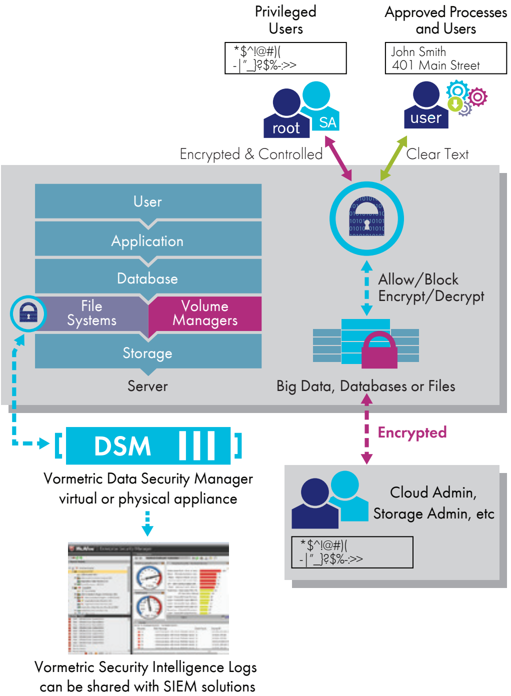


Moreover, Thales eSecurity helps you prevent breaches from happening in the first place through:

- Access control to ensure only credentialed users can retrieve the data
- Security intelligence logs to identify irregular access patterns and breaches in progress
- Highly-secure, integrated key management available in Common Criteria-certified devices

Data-Centric Protection

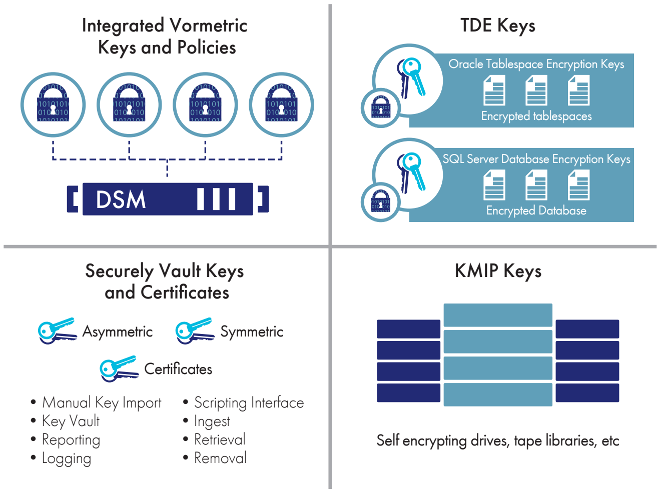
Thales eSecurity protects the data itself through **Vormetric Transparent Encryption** with integrated **Key Management**, **Application Encryption**, **Tokenization with Dynamic Masking** and other solutions. These techniques make the data meaningless and worthless without the keys to decrypt it.


Privileged Users
*$^!@#)(
-|"_]?$%->>
root
SA
Approved Processes and Users
John Smith
401 Main Street
user
Encrypted & Controlled
Clear Text
User
Application
Database
File Systems
Volume Managers
Storage
Server
Allow/Block Encrypt/Decrypt
Big Data, Databases or Files
Encrypted
DSM
Vormetric Data Security Manager virtual or physical appliance
Cloud Admin, Storage Admin, etc
*$^!@#)(
-|"_]?$%->>
Vormetric Security Intelligence Logs can be shared with SIEM solutions

Access Control

The **Vormetric Data Security Platform**, from Thales eSecurity, provides state of the art user access control:

- Separation of privileged access users and sensitive user data. With the **Vormetric Data Security Platform**, administrators can create a strong separation of duties between privileged administrators and data owners. **Vormetric Transparent Encryption** encrypts files, while leaving their metadata in the clear. In this way, IT administrators—including hypervisor, cloud, storage, and server administrators—can perform their system administration tasks, without being able to gain privileged access to the sensitive data residing on the systems they manage.
- Separation of administrative duties. Strong separation-of-duties policies can be enforced to ensure one administrator does not have complete control over data security activities, encryption keys, or administration. In addition, the **Vormetric Data Security Manager** supports two-factor authentication for administrative access.
- Granular privileged access controls. The Vormetric Platform can enforce very granular, least-privileged-user access management policies, enabling protection of data from misuse by privileged users and APT attacks. Granular privileged-user-access management policies can be applied by user, process, file type, time of day, and other parameters. Enforcement options can control not only permission to access clear-text data, but what file-system commands are available to a user.



Security Intelligence Logs

Thales eSecurity lets the enterprise monitor and identify extraordinary data access. Vormetric **Security Intelligence Logs** are detailed management logs that specify which processes and users have accessed protected data. They specify when users and processes accessed data, under which policies, and if access requests were allowed or denied. The management logs will even expose when a privileged user submits a command like 'switch users' in order to attempt to imitate, and potentially exploit, the credentials of another user. Sharing these logs with a security information and event management (SIEM) platform helps uncover anomalous patterns in processes and user access, which can prompt further investigation.

Integrated Key Management

With Vormetric Key Management, you can centrally manage keys from all Vormetric Data Security Platform products, and securely store and inventory keys and certificates for third-party devices—including IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products. By consolidating key management, this product fosters consistent policy implementation across multiple systems and reduces training and maintenance costs.

FOR MORE INFORMATION

For more detailed technical specifications about Thales data encryption and key management, please visit **www.thalesesecurity.com**

THALES

www.thalesesecurity.com

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

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