thalesesecurity.com

THALES

Addressing key provisions of the General Data Protection Regulation (GDPR)

Data encryption and key management strategies to develop a compliant posture

White Paper

Contents

GDPR requirements and penalties

Through the General Data Protection Regulation (GDPR)[1,2] the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). The Commission's primary objectives for the GDPR are to return to citizens control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

This legislation, although firmly based on EU principles and approaches, has major impact on a global level. Notably, any organisation that holds EU cititzens' personal data, irrespective of where it is headquartered or operates, must comply or face severe penalties.

Adopted in April 2016, the GDPR superceded the EU's Data Protection Directive and effective May 25, 2018[3]. The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonisation of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations. The regulation does not apply to the processing of personal data for national security activities or law enforcement ("competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties").

Consequences of non-compliance

The consequences on non-compliance cross geographical boundaries.

Fines

The regulation imposes a strict data protection compliance regime with severe penalties of "up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."

Breach notification

In addition, in the case of a breach of personal data, the organisation breached will be required to notify the subjects of the breach "without undue delay." A timeline of 72 hours has been highlighted in the official documentation.

Personal data definition

According to GDPR: 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Security of personal data

GDPR guidelines on protecting personal data

GDPR outlines measures an organisation should take to protect personal information.

Article 32: Security of processing

1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

   (a) *the pseudonymisation and encryption of personal data;*

   (b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

   (c) *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

   (d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

GDPR guidelines for when breach notification is necessary

The regulation also details what an organisation must do to avoid having to notify subjects in case of a breach.

Article 34: Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

   (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; [4]

   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

   Encryption and data pseudonymisation of the personal data are state of art technologies providing appropriate technical protection measures to ensure the level of security outlined in the articles above. As per Section 3, Article 34 of the regulation, if the breached data is encrypted the communication about the data breach will not be required.

The right to be forgotten

One of the most potentially onerous elements of the GDPR is covered in Section 3, Article 17, Right to erasure ('right to be forgotten')[5]. This Article stipulates that organisations must erase a data subject's records upon request 'without undue delay' where there is no compelling reason to keep them on hand. If the organisation has shared the requestor's data externally, it must also notify other data controllers that the data subject has requested the erasure.

Although certain circumstances obviate the need to comply with Article 17 (e.g. the organisation using the data is exercising its right of freedom of expression and information, or the data is being used in the interest of public health, among others), this requirement is far-reaching, especially when considering that the GDPR applies to data in both digital and print formats.

Auditability

The right to erasure requirement is made even more daunting when potential audits are brought into the equation. Not only will the organisation need to take the proper steps to ensure the deletion of the data subject's personal information, but it will also need auditable proof of having done so.

Summary: Having outlined key requirements of GDPR, the following section illustrates how Thales can enable organisations to adhere to the mandate.

GDPR compliant data protection strategy

Overall, the GDPR calls for a Layered or "Defence in Depth" security approach to protect sensitive data from compromise. The layers should include not only perimeter security, but also, among others:

1. Limiting access to unencrypted data
2. Encrypting sensitive data with integrated cryptographic key management or otherwise pseudonymising it
3. Monitoring and reporting user access patterns to identify breaches in progress

Limiting access to unencrypted data

Privileged user access

Privileged user roles for system, network, storage and other administrative accounts have traditionally been allowed unfettered access to storage and resources associated with systems that they maintain. As such, these roles are a prime vector for insider threats, and the theft of the credentials for these accounts are top targets for external attackers.

Amount of data accessed and data-at-rest

The impact of a breach depends on the system and data assets malicious users (outsider or insider) access. Most organisations have millions of structured data records, and terabytes of unstructured data stored at rest in file servers, databases, network storage, big data nodes, cloud-based storage, etc. Therefore, the breach of the data-at-rest (DAR) may have the biggest negative impact on the enterprise that holds the data.

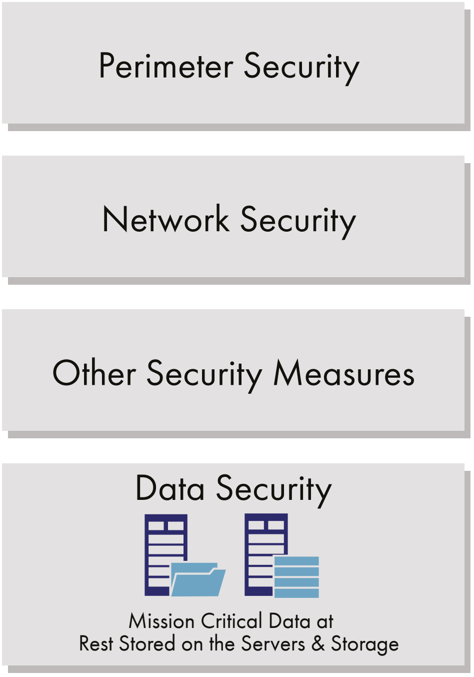


Figure 1 – Layered security approach

Limiting DAR access to authenticated and authorised users limits the risk of data breach

To minimise the risk to the DAR, enterprises should limit access to the data to authenticated and authorised users and processes. Privileged users (admin and root) may be required to maintain and manage systems holding the sensitive data, but they must not be able to access the actual contents of the dataset. If they can, the compromise of a privileged system user's identity or any rogue privileged user may cause the data breach.

Data-at-rest encryption with access controls and strong key management

Data encryption

The GDPR specifically requires encryption or pseudonymisation of personal data and does not require breach disclosure to subjects, if the breached data is encrypted.

Data encryption converts data into another form, or code, so that only people with access to a secret cryptographic key can read it. The security benefits offered by the data encryption solution rely on the control placed around the secret cryptographic key. Therefore, protection of the cryptographic key is a critical aspect of the encryption.

The value of encryption with proper key management is that even if a malicious entity gains access to encrypted data, it is meaningless and therefore useless to the malicious entity. If all other defences fail, the encrypted data itself is useless. The thief is deprived of his or her prize.

Cryptographic key management

As mentioned above, cryptographic key management is essential to the success of encryption as a data security measure. According to Forrester Research:

> *The final encrypted solution has two parts: the encrypted data itself and the keys that control the encryption and decryption processes. Controlling and maintaining the keys, therefore, is the most important part of an enterprise encryption strategy. Encryption methods and algorithms are standardized and well understood, but key management is unique to each organization.*[6]

Tokenisation as an alternative to encryption

Tokenisation creates an unrecognisable tokenised form of the data that maintains the format of the source data. For example, a credit card number (1234-5678-1234-5678) when tokenised (2754-7529-6654-1987) looks similar to the original number and can be used in many operations that call for data in that format without the risk of linking it to the cardholder's personal information. The tokenised data is also the same size and format stored as the original data. So storing the tokenised data requires no changes in data base schema or process.

If the type of data being stored does not have this kind of structure – for example, text files, PDFs, MP3s, etc., tokenisation is not an appropriate form of pseudonymisation. Instead, file-system level encryption would be appropriate. It would change the original block of data into an encrypted version of the data.

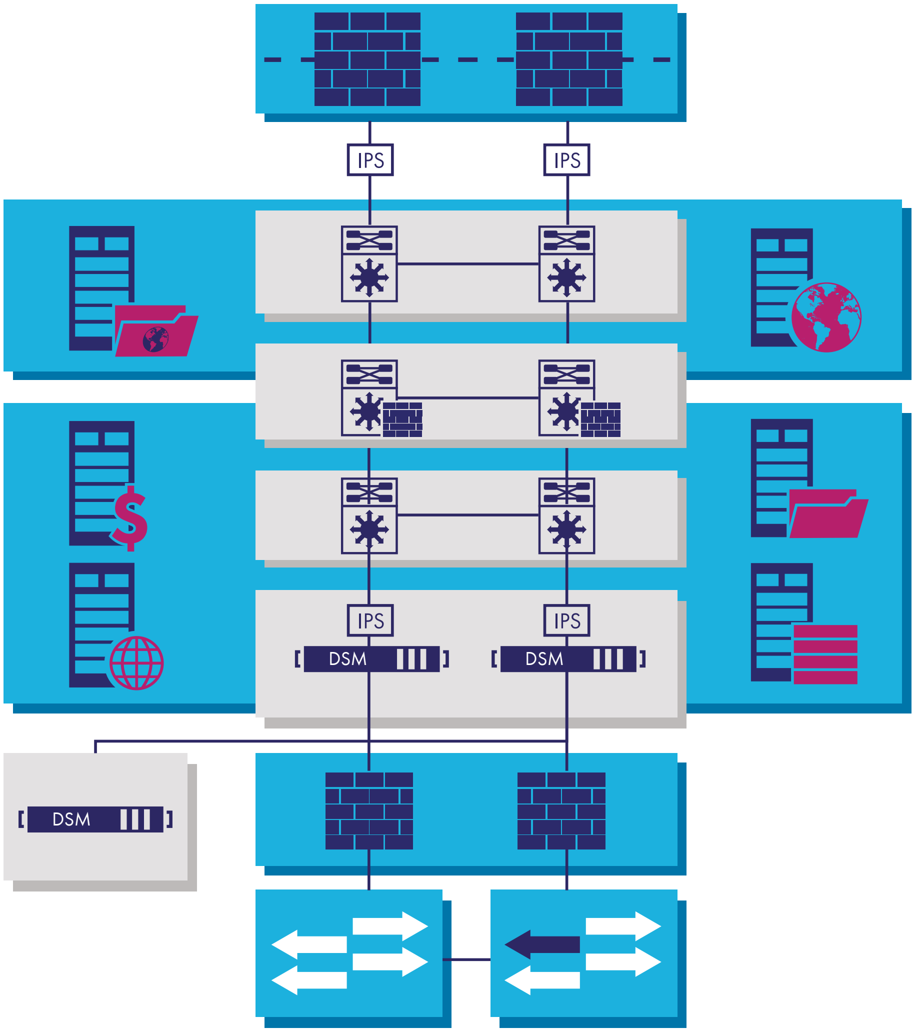


Figure 2 – Example network architecture with sensitive data-at-rest on various servers

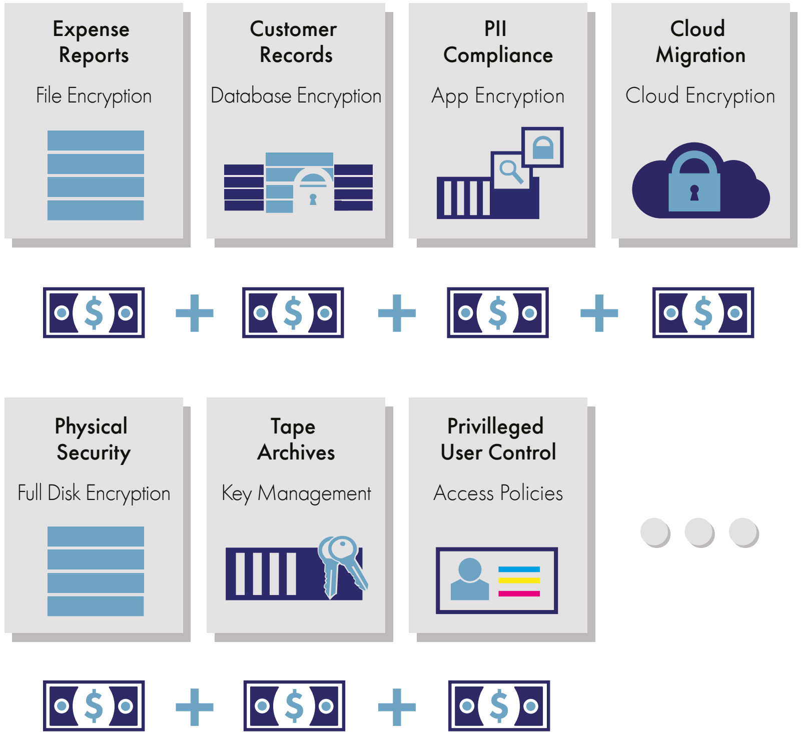
Historical approach to encryption and key management for data-at-rest

Historically, organisations have protected data by building walls around it – perimeter protection – with firewalls and intrusion prevention systems (IPSs) to deny unauthorised users access to networks. This is the equivalent of locking one's door to deter burglars. However, with the increasing sophistication of cybercriminals, this has not been a satisfactory solution for many years.

The next step was to add layers of protection by approaching each problem with a point solution. These might include:

- File encryption solutions for unstructured data
- Multiple database data security solutions
- Customised applications for application layer security
- Purchasing full-disk-encryption enabled storage for network-attached storage (NAS) (and spending more and limiting selection to do so)
- Multiple key managers and techniques for managing policies and keys for all these security solutions
- An entirely different infrastructure and policy management process to guard data from privileged users

This disjointed data security strategy quickly becomes very expensive to maintain and grow and very challenging to manage as an organisation acquires more and more new vendors; and its IT staff installs, learns and maintains new devices; etc.



Each use case require individual infrastructure, management consoles and training

Complex – Inefficient – Expensive

Figure 3 – The disjointed security solution

Vormetric Data Security Platform – one-stop data-at-rest security

Vormetric data security products from Thales eSecurity provide a solution that meets GDPR compliance regulations whilst overcoming the challenges and expense of the disjointed security approach.

The Vormetric Data Security Platform[7]

Thales Vormetric Data Security Platform makes it efficient to manage data-at-rest security across your entire organisation. Built on an extensible architecture, Vormetric Data Security Platform products can be deployed individually, whilst sharing efficient, centralised key management. With this platform's comprehensive, unified capabilities, you can efficiently scale to address your expanding security and compliance requirements, whilst significantly reducing total cost of ownership.

The Vormetric Data Security Platform delivers capabilities for transparent file-level encryption, application-layer encryption, tokenisation, dynamic data masking, key management for platform products as well as cloud platforms, KMIP devices and TDE database encryption, privileged user access control, and security intelligence.

With the solution, you can address security policies and compliance mandates across databases, files, and big data nodes—whether assets are located in cloud, virtualised, or traditional environments.

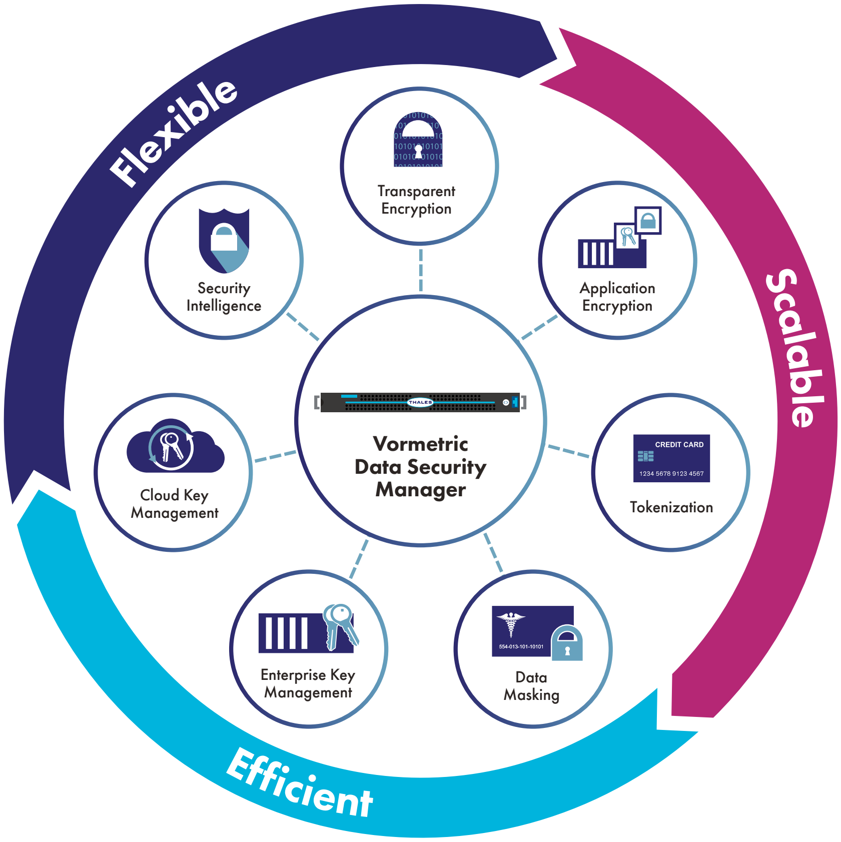


Figure 4 – The Vormetric Data Security Platform

Solutions that limit access to unencrypted data

The Vormetric Data Security Manager

Thales eSecurity's Vormetric Data Security Manager (DSM) centralizes encryption key and policy management to remove data security deployment and operational complexity.

Figure 5 – The Vormetric Data Security Manager

The DSM can enforce strong separation of duties by requiring the assignment of key and policy management to more than one data security administrator. In this manner, no one person has complete control over security activities, encryption keys, or administration. In addition, the DSM supports two-factor authentication for administrative access.

With the DSM, administrators can create a strong separation of duties between privileged administrators and data owners. Thales solutions encrypt files, whilst leaving their metadata in the clear. In this way, IT administrators, such as hypervisor, cloud, storage, and system administrators can perform their system administration tasks, without being able to gain access to the sensitive data residing on those systems.

Also, because they can leave metadata in the clear, Thales encryption solutions don't have an impact on management activities like replication, migration, and snapshots. The platform's fine-grained controls can even be used to define whether privileged users can perform such functions as copy, write, or directory listing.

Solutions that encrypt sensitive data with integrated key management or pseudonymise it

Vormetric Transparent Encryption

Vormetric Transparent Encryption from Thales enables data-at-rest encryption, privileged user access control and the collection of security intelligence logs without re-engineering applications, databases or infrastructure. The deployment of Vormetric data-at-rest encryption software is simple, scalable and fast, Vormetric Transparent Encryption Agents are installed above the file system on servers or virtual machines to enforce data security and compliance policies. As with all Thales eSecurity encryption products, on-going policy and encryption key management operations are centralised and efficient with the Vormetric Data Security Manager.

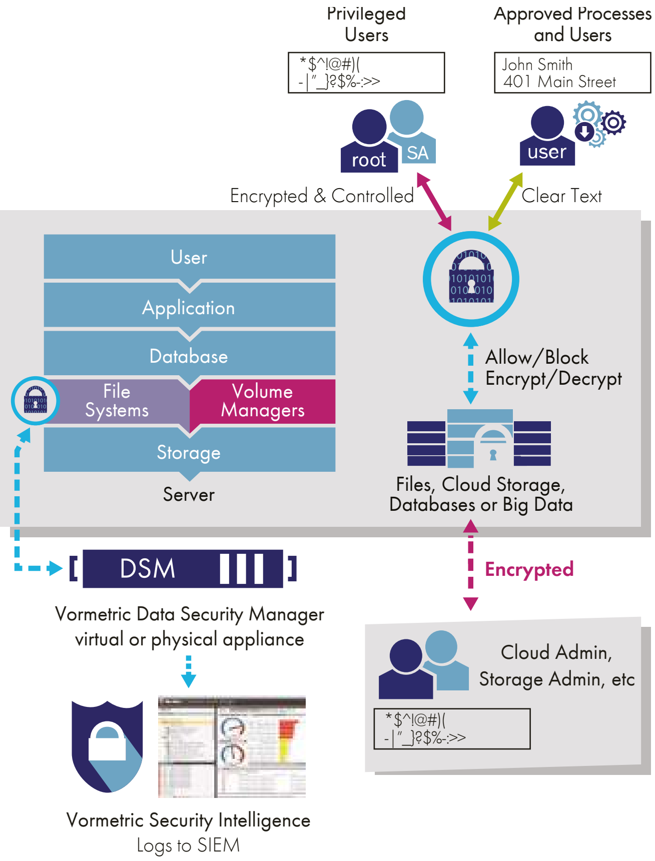


Figure 6 – Vormetric Transparent Encryption

Vormetric Key Management

In addition to providing integrated enterprise encryption key management for Vormetric Transparent Encryption and Vormetric Application Encryption, the Vormetric Data Security Platform centralises third party encryption keys and stores certificates securely. The Vormetric Data Security Platform provides high availability, standards-based enterprise encryption key management for Transparent Database Encryption (TDE), KMIP compliant devices, and offers vaulting and inventory of certificates. Consolidating enterprise encryption key management delivers consistent policy implementation between systems, reduces training and maintenance costs.

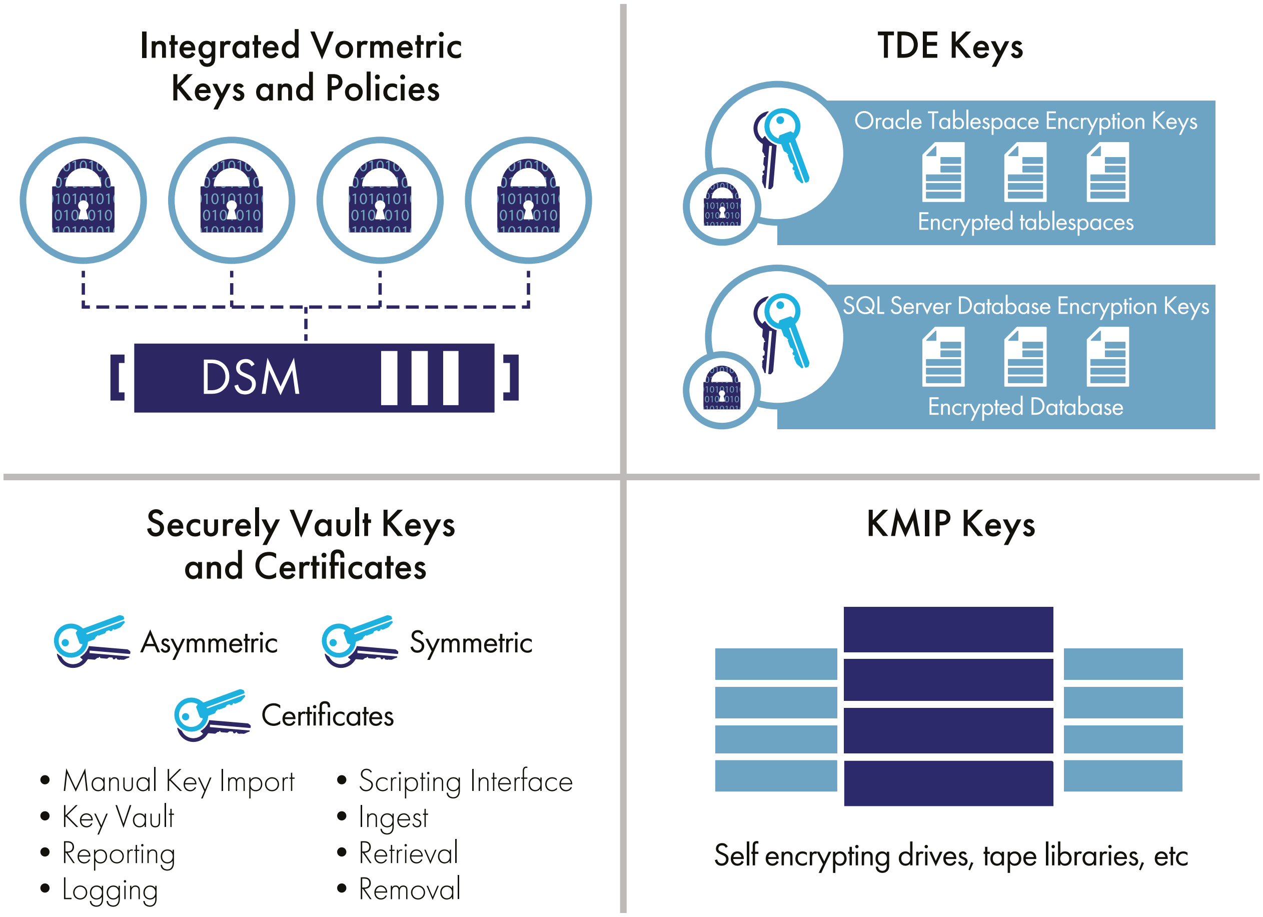


Figure 7 – Vormetric Key Management

Vormetric Application Encryption

However, for the applications that require field-level encryption for database, big data, PaaS or other applications there is Vormetric Application Encryption from Thales.

Vormetric Application Encryption is for data security needs that require field-level encryption for database, big data, PaaS and other applications. Vormetric Application Encryption is a library to simplify integrating application-level encryption into existing corporate applications, as well as RESTful APIs that enable remote encryption access. The application encryption library provides a set of documented standard-based APIs used to perform cryptographic and encryption key management operations. The innovative product design enables developers to choose standard AES encryption or schema-maintaining Format Preserving Encryption (FPE). Vormetric Application Encryption removes the complexity and risk of implementing an in-house encryption and key management solution. Vormetric Application Encryption supports Unicode and the library is in the process of being certified for FIPS 140-2.

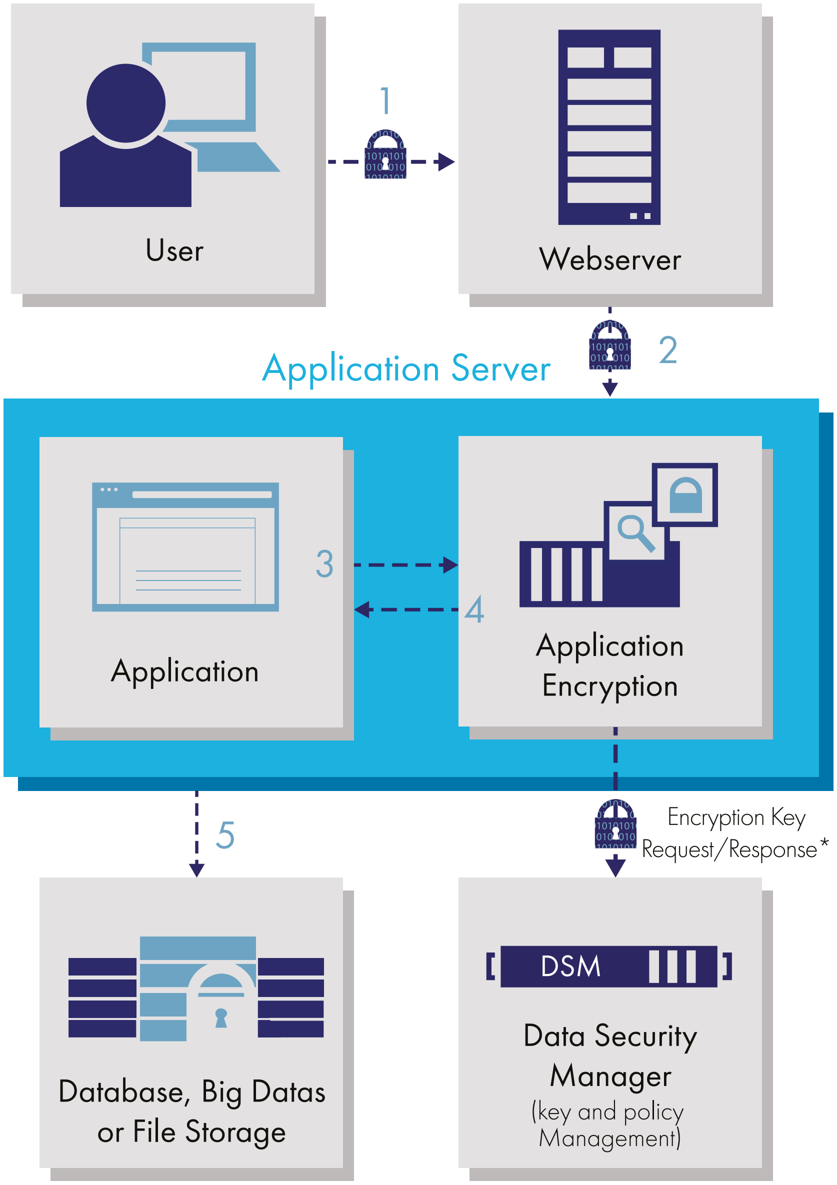

User
1
Webserver
2
Application Server
Application
3
4
Application Encryption
5
Encryption Key Request/Response*
Database, Big Datas or File Storage
DSM
Data Security Manager
(key and policy Management)

Figure 8 – Vormetric Application Encryption

Vormetric Vaultless Tokenization with Dynamic Data Masking

Vormetric Vaultless Tokenization makes it easy to use format-preserving tokenisation to protect sensitive fields in databases. Vormetric Vaultless Tokenization supports both Random-token and Crypto-token generation. The solution offers a virtual appliance that tokenises records and manages policies for accessing tokens and clear-text data and uses REST APIs for tokenization requests.

Vormetric Vaultless Tokenization makes it fast and easy to add policy-based dynamic data masking to applications. In addition, by leveraging the latest standards-based format preserving encryption (FPE) and random tokenisation techniques, the Vormetric solution eliminates the need for a token vault and an associated database. As a result, the solution reduces cost and complexity, enhances performance, and makes it easier to achieve global scale and high availability.

Example applications of Vormetric Vaultless Tokenization with Dynamic Data Masking include:

- Replacing stored credit card numbers with random-tokens to remove underlying infrastructure from expensive PCI DSS audit requirements
- Protecting passports numbers, national identity numbers (such as the U.K. National Insurance number), drivers licenses and other personally identifiable information (PII) by replacing them in everyday use with crypto-tokens that exactly duplicate the format of the original information
- Enabling call-center, medical, and other applications where PII is protected by limiting access to only a portion of the sensitive data, such as the last four digits of a credit card or insurance number

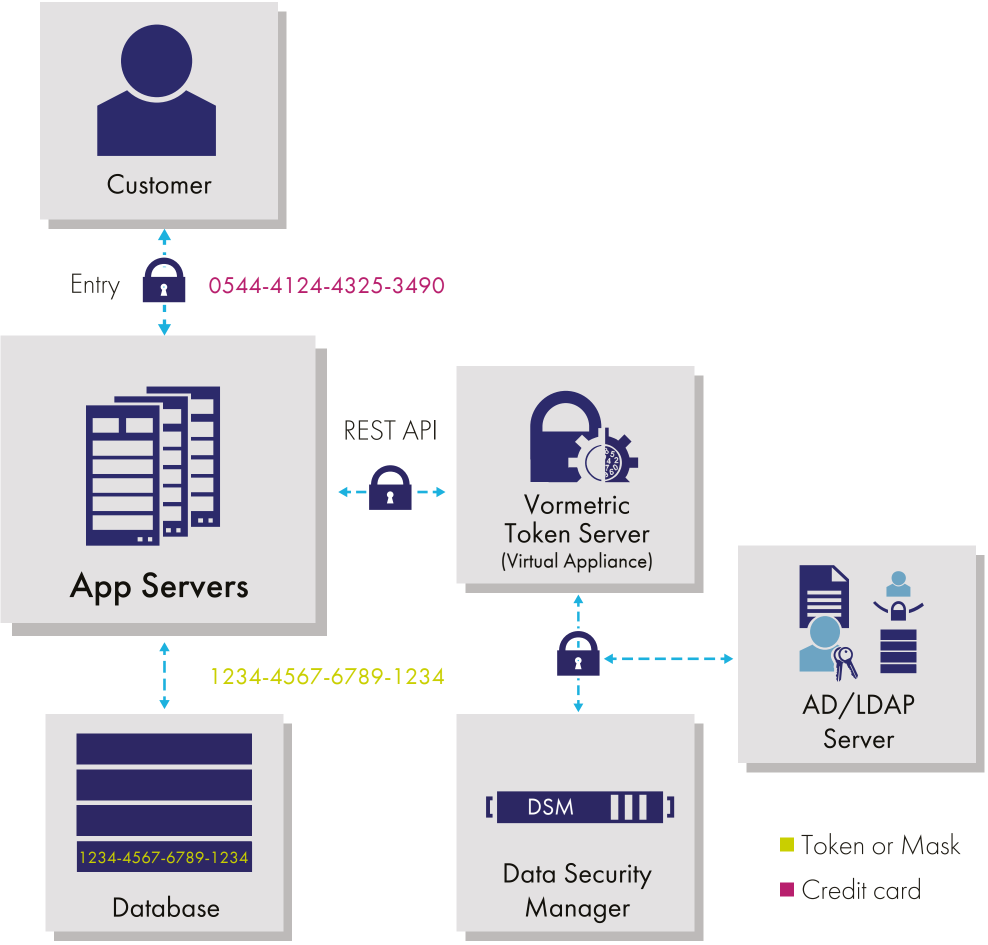


Figure 9 – Vormetric Vaultless Tokenization with Dynamic Masking

CipherTrust Cloud Key Manager

Many cloud service providers offer data-at-rest encryption capabilities. Meanwhile, many data protection mandates require that encryption keys be stored and managed remotely from the cloud service provider. "Bring Your Own Key" (BYOK) services and API's can fulfill these requirements.

Customer key control

BYOK-based customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them. Leveraging BYOK API's, the CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers full lifecycle control of encryption keys with centralized management and visibility. The solution can be deployed almost instantly using CipherTrust Cloud Key Manager as a service or can be deployed on-premises to meet more stringent compliance requirements.

Strong encryption key security

Customer key control requires secure key generation and storage. CipherTrust Cloud Key Manager leverages the security of the Vormetric Data Security Manager or customer-owned hardware security modules (HSMs) to create and store keys.

IT efficiency and compliance tools

The combination of centralized key management for multiple cloud providers in a single browser window, automated key rotation, federated login, and management of native cloud keys offers enhanced IT efficiency. CipherTrust Cloud Key Manager cloud-specific logs and prepackaged reports offer fast compliance reporting.

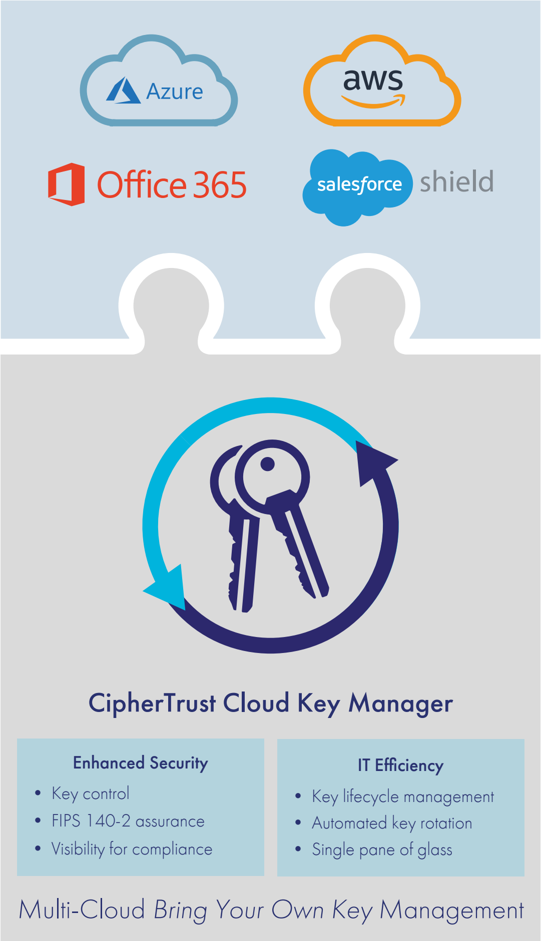


Figure 10 – CipherTrust Key Management

Software-as-a-service

As a Service combines cloud simplicity with the control required for data protection mandates, with FIPS 140-2 Level 1 key security.

On-premises deployment options

On-premises options offer up to FIPS 140-2 Level 3 key security. Virtual appliances are also available in the Azure Marketplace, for AWS, and for VMware.

Key benefits

- Leverage the value of "Bring Your Own Key" services with full-lifecycle cloud encryption key management
- Comply with the most stringent data protection mandates with up to FIPS 140-2 Level 3 validated key creation and storage
- Gain higher IT efficiency with centralized key management across multiple cloud environments

Supported cloud environments

- IaaS and PaaS: Microsoft Azure, Azure China and Germany National Clouds, Microsoft Azure Stack, Amazon Web Services
- SaaS: Microsoft Office365, Salesforce.com

Software as a service key security

- FIPS 140-2 Level 1

On-premises secure key origination and storage

- Vormetric Data Security Manager up to FIPS 140-2 Level 3, supporting Amazon, Azure and Salesforce
- Client-owned HSMs: FIPS 140-3 Level 3, supporting Amazon and Azure

Solutions that monitor and report user access patterns

Vormetric Security Intelligence

The Vormetric Data Security Platform produces detailed security event logs that are easy to integrate with SIEM systems to produce compliance and security reports. These security information logs produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into file access activities. Logging occurs at the file system level, removing the opportunity of stealthy access to sensitive data. These security information logs can report unusual or improper data access and accelerate the detection of insider threats, hackers and the presence of advanced persistent threats (APT) that are inside the perimeter security. Logging capabilities also include actions of security administrators, unauthorised access attempts to the data security manager environment as well as key management activities and actions for all Vormetric Data Security Platform products.

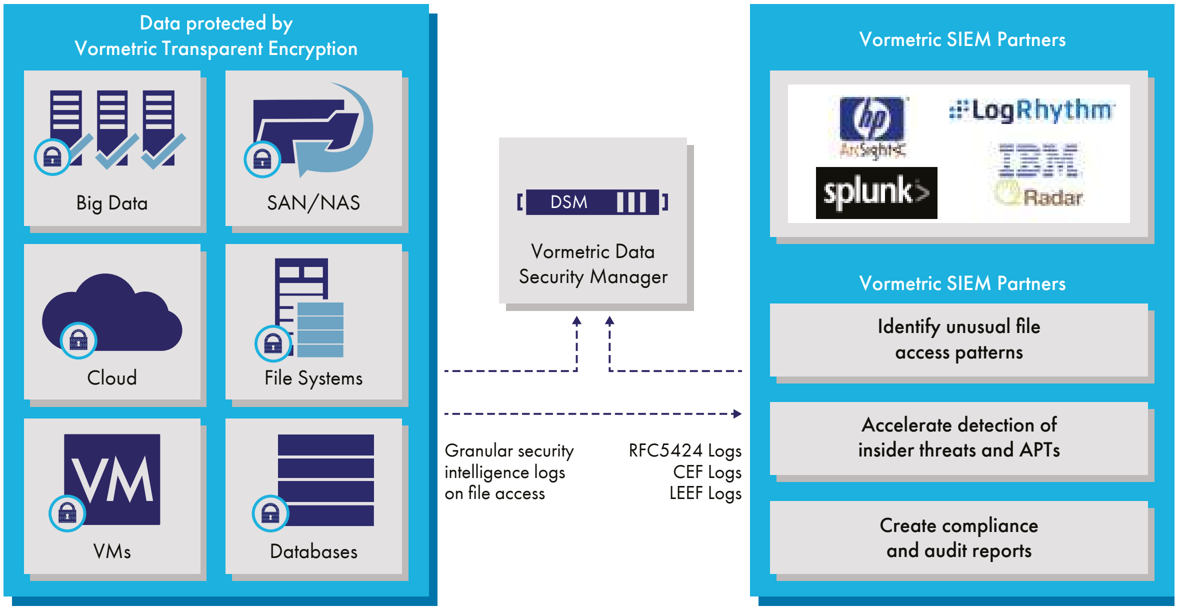


Figure 11 – Vormetric Security Intelligence

Data Protection Measure	GDPR Applicability	Thales Capability
Data encryption or pseudonymisation	Comply with Article 32, Security of processing ("the pseudonymisation and encryption of personal data") Avoid the notification requirements of Article 34, Communication of a personal data breach to the data subject	Vormetric Transparent Encryption Vaultless Tokenization with Dynamic Data Masking
Risk assessments	Comply with Article 32, Security of processing ("a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." Understand compliance with the GDPR, as outlined in Article 39, Tasks of the data protection officer ("monitor compliance with this Regulation... in relation to the protection of personal data")	Vormetric Data Security Platform Security Intelligence Logs

Figure 12 – Thales solutions align with key GDPR requirements

Summary

The GDPR is arguably the most stringent data privacy mandate ever imposed on organisations, and may well represent the future of regulations across the globe. With its focus on protecting the personal data of any EU citizen, regardless of where the controller or processer does business, the impact of the GDPR reaches far beyond the EU's boundaries. Moreover, with fines that could reach tens of millions of euros, it is incumbent upon organisations to take the regulation seriously.

Thales offers leading data encryption and pseudonymisation, tokenisation and security intelligence solutions that help customers secure sensitive data wherever it is created, shared or stored, to ensure compliance with key elements of the GDPR.

For more information, visit www.thalesesecurity.com.

References

1. Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

2. The information cited in this paper comes from the GDPR listed in the first footnote unless otherwise noted

3. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

4. Made bold by Thales for emphasis

5. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure

6. http://apac.trendmicro.com/cloud-content/apac/pdfs/business/white-papers/wp_kill-your-data-to-protect.pdf

7. For more detailed information on these Vormetric data security products visit our website at thalesesecurity.com

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.

THALES

Americas – Thales eSecurity Inc.
2860 Junction Avenue, 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) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 814 | 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

> thalesesecurity.com <