Trusted Cyber Technologies

THALES

Thales Trusted Cyber Technologies Key Management

Simplify data security by centrally managing keys and policies across the enterprise

White Paper

Table of Contents

Executive Summary

Today, every IT organization is striving to protect valuable digital assets of any organization from accidental exposure or intentional misuse by cyber criminals. Many organizations have deployed a variety of point encryption solutions as a primary method of protecting sensitive data to meet various digital privacy regulations and compliance mandates. Unfortunately, the majority of these disparate encryption solutions have fallen short in their ability to address their enterprise key management challenges.

This white paper looks back at the evolution of encryption and key management systems, and examines the key challenges faced by IT teams around encryption systems, including regulation and compliance, complexity, lack of proper management tools. This is followed by a review of the recent industry initiatives and compliance regulations that are shaping the future of key management.

The paper concludes with an introduction to CipherTrust Manager, the next generation enterprise key management offering from Thales, which provides a powerful integrated solution that enables organizations to centrally manage encryption key lifecycle and policies for Thales Data Protection Connectors and third-party KMIP compliant products in the enterprise.

Data Security Challenges

Many organizations are adopting digital transformation and migrating to the cloud to drive operational efficiency into their data-intensive processes. According to the 2020 Thales Data Threat Report, which is based on a global-IDC survey of 1,723 executives who have responsibility or influence over IT and data security, we are at an inflection point with the cloud as half of all data is now stored in cloud environments, and 48% of that data is sensitive. Additionally, most organizations rely on multi-cloud environments to deploy their applications, in order to avoid vendor lock-in.

Data migration to third-party hosted environments and multiple cloud service providers is creating new attack surfaces for cybercriminals to exploit. Hence, data breaches continue to threaten the IT landscape at an increasing rate. All of this adds up to today's data environments becoming even more complex; operation complexity is a top barrier to data security.

" We are at an inflection point with the cloud as half of all data is now stored in cloud environments, and 48% of that data is sensitive."
– 2020 Thales Data Threat Report, IDC Survey

Looking Back at Encryption and Key Management Techniques

The Internet has been the most significant driving force in the evolution of encryption and key management technologies. Providing easy access to a company's data to those who need it- employees, partners, and customers has taken priority, with data security being implemented as an afterthought. This connection of public and private resources over the internet to any company's sensitive data has given rise to the increase in data breaches.

In response, a variety of perimeter and endpoint security controls and security policies have been adopted to defend against these threats. In addition, data privacy regulations and a myriad of compliance requirements have been developed to battle these forces. However, they are not enough to stop cyber theft.

As attacks become more sophisticated, the industry has been improving these early encryption systems, eliminating the difficulties of disparate native key repositories that were then scattered across the various information systems in the enterprise.

Data Encryption Across Disparate Systems – Security Silos

The increased adoption of encryption solutions has improved security for enterprises, but it has made life much more challenging for the IT security team, now tasked with managing a variety of cryptographic keys. Nearly all offline data storage devices and many database management systems (DBMS) include the option of embedded native encryption capability. A challenge with these islands of encryption is that keys and key management software from each provider don't usually interoperate well with one another.

The resulting silos of security, where system administrators and database administrators (DBAs) have to become the managers of the encryption keys for a particular system, distracts them from their primary tasks of IT and database administration. Along with the resource inefficiency of such a methodology, it also puts an enterprise's overall security posture at risk.

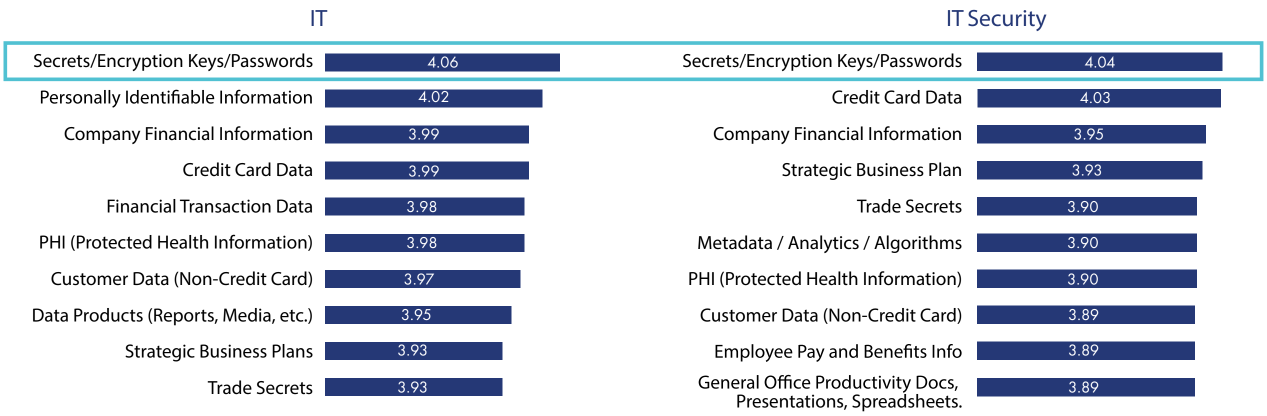


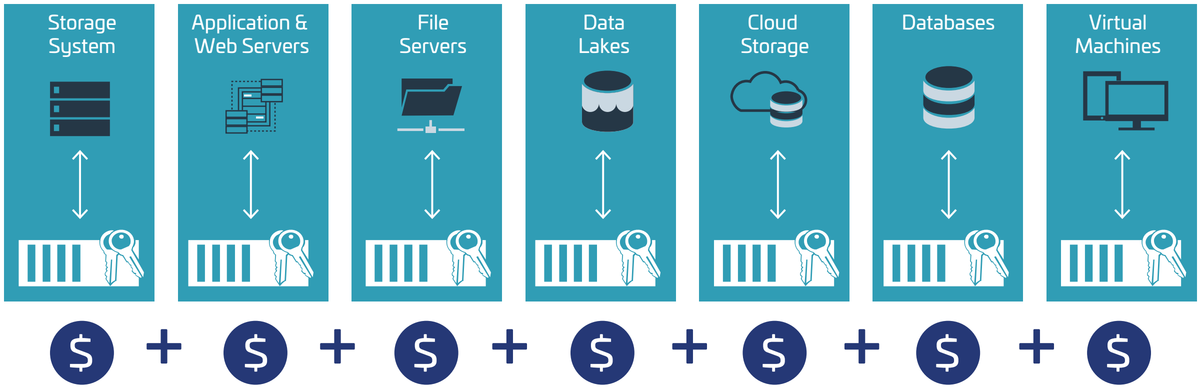
Figure 1: 2020 IDC Data Security Survey - Most Critical Assets that Require Protection

According to the 2020 IDC Data Security Survey (shown in Figure 1), both IT and IT Security practitioners rated Secrets, Encryption Keys and Passwords as the most critical assets that requires protection.

The Problem - Too Many Silos

Without a centralized encryption key management solution, security administrators are faced with a costly, inefficient and often impossible task managing disparate encryption keys for many different databases accumulated over time from separate vendors. This heterogeneous world means that an enterprise looking to secure databases, such as Oracle and Microsoft SQL Server using native TDE, has to factor in the increased costs and administrative resources required for managing multiple, incompatible encryption solutions. It is costly and complex to manage separate encryption systems required for each data store, without consistent security policies, repeatable processes and error prone, as shown in Figure 2 below.

When each system administrator separately controls encryption keys for each data repository they manage, the keys are generally stored in the same location as encrypted data, it leaves room for security compromises – the electronic equivalent of taping the key to the front door. Manual systems to store and transmit the encryption keys, lack of password control and the failure to revoke keys when an employee leaves the company can result in data breaches waiting to happen. And strict adherence to compliance requirements is nearly impossible in this situation.



Essentials of Enterprise Key Management

As organizations deploy an ever-increasing number of encryption solutions, they should look for a centralized key management solution that enables them to securely store and backup/restore the encryption keys, define consistent access control policies, audit all key management operations and separate encryption tasks from key management tasks.

Here are the essential elements of a robust enterprise key management solution that can help address the challenges listed in the previous section.

Secure Key Storage

Secure key storage is the foundation for any enterprise key management system. The use of Hardware Security Modules (HSMs) is a well-established approach for protecting encryption keys. Mandated in government and certain financial/payment markets HSMs protect cryptographic keys and perform various cryptographic functions in a secure tamper-resistant environment. Enterprise key management solutions should provide options to support built-in HSMs, external network attached HSM or a cloud-based HSM-as-a-service, based on the level of assurance your needs.

Centralized Key Lifecycle Management

The key management system should be able to centrally manage keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation, and deletion. It should also provide policy-based access control to keys, support various authentication providers including Active Directory and LDAP, and robust auditing of all key management operations.

Enabling Scalability and Flexibility

As the complexity of an organization's IT infrastructure grows from a single data-center to external hosted environments to multiple cloud service providers, so should the ability of enterprise key management solution to adopt to changing requirements.

A flexible key management solution should be able to support both on-premises infrastructure and be deployable as a virtual appliance in public cloud environments, wherever your sensitive data resides, such as AWS, Azure, Google Cloud and more.

Guaranteed Availability

Organizations cannot function without the availability of business critical data, which is most likely encrypted to reduce business risks due to unauthorized exposure. The key management system should support high-availability clustering options, using two or more physical and/or virtual appliances to reduce security lapses.

Interoperability with Third-party Systems

Any enterprise key management solution should support the following three major interoperability standards that enable you to work with multiple sever, storage and device vendors, who utilize the keys for authentication, digitally signing or encrypting data.

- **PKCS#11** – Public Key Cryptographic Standard #11 specifies an API for devices to interoperate with hardware security modules (HSM) and smart cards, which hold cryptographic tokens. It is also used to access signing keys from Certification Authorities (CAs) or to enroll user certificates for digital signing and encryption using asymmetric keys. As an example, PKCS#11 is used by Oracle TDE.
- **EKM/MSCAPI** – Extensible Key Management (EKM) using the Microsoft Cryptographic APIs (MSCAPI), enables MS SQL Server to communicate with third-party key management servers. The keys must be exported from a provider before they are stored in the database. This approach enables key management that includes an encryption key hierarchy and key backup for Microsoft SQL Server Transparent Data Encryption.
- **OASIS KMIP** – Key Management Interoperability Protocol (KMIP), maintained by the Organization for Advancing Open Standards for the Information Society (OASIS), defines the standard protocol for any key management server to communicate with clients (e.g. storage devices, databases) that utilize the keys for embedded encryption. KMIP improves interoperability for key lifecycle management between encryption systems and enterprise applications.

Facilitate Governance and Reporting

The most important aspect of governance is a discipline for managing, controlling, and protecting the security and privacy of data. A policy-driven key management system forces the adherence to procedures for separation of duties and user authorization, and it automates all the security processes involved in the key lifecycle. Some of the more notable industry standards and compliance requirements affecting key management today include:

- **General Data Protection Regulations (GDPR)**
Perhaps the most comprehensive data privacy standard to date, GDPR affects any organization that processes the personal data of EU citizens - regardless of where the organization is headquartered. GDPR is designed to improve personal data protections and increase organizational accountability for data breaches. With potential fines of up to four percent of global revenues or 20 million EUR (whichever is higher), the regulation has impact on many businesses.
- **Payment Card Industry Data Security Standard (PCI DSS)**
Any organization that plays a role in processing credit and debit card payments must comply with the strict PCI DSS compliance requirements for the processing, storage and transmission of account data. The PCI DSS standard involves assessment against over 200 tests that fall into 12 general security areas representing six core principles. These PCI DSS tests span a wide variety of common security practices along with technologies such as encryption, key management, and other data protection techniques.
- **Gramm Leach Bliley Act (GLBA)**
The United States requires that firms acknowledge publicly when a disclosure event occurs, taking whatever damages to their reputation or market position that such a statement would entail. Led by California's Database Security Breach Notification Act in 2003, more than half of all states have passed additional rules beyond the general notification requirements of GLBA to require firms to notify disclosure victims of the event, with higher associated costs to the business than GLBA exacted.
- **The U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act**
HITECH does not require breach notification if the Protected Health Information (PHI) being exposed in the event of a data breach is already encrypted. For "unsecured PHI data", notification of the breach to every individual affected must be made. With the increasing cost of recovering from a data breach, it is important to invest in a strong encryption strategy for PHI data, and centralized key management system as its underpinning.

Introducing CipherTrust Manager

The Foundation of Thales Key Management Solutions

CipherTrust Manager enables organizations to centrally manage encryption key lifecycles and policies, independent of where the data resides, and help them meet their data privacy and compliance requirements. It simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion. It provides role-based access control to keys and policies, multi-tenancy support with ultimate separation of duties, and robust auditing and reporting of all key management operations.

The unified management console in CipherTrust Manager makes it easy to discover and classify data, and protect sensitive data using a comprehensive set of data protection connectors from Thales.

Figure 3: CipherTrust Manager

Key Benefits

Simplified Management

CipherTrust Manager provides a unified management console that enables you to discover and classify sensitive data, and protect data using integrated set of Thales Data Protection connectors across on-premises data stores and multi-cloud deployments. It offers advanced self-service licensing for improved visibility and control of licenses.

Cloud Friendly Deployment

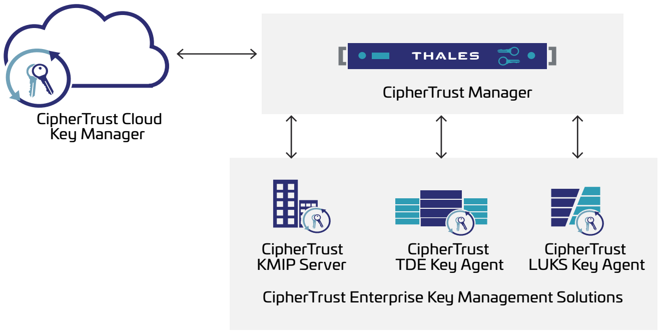
CipherTrust Manager offers users with additional hosting options, and can run as a native virtual machine on AWS, Microsoft Azure, Google Cloud, VMware, Microsoft HyperV, and more. Additionally, native support for CipherTrust Cloud Key Manager is available on CipherTrust Manager, to streamline key management across multiple cloud infrastructures and SaaS applications.

Flexible Form Factors

CipherTrust Manager is available in both virtual and physical form factors and FIPS 140-2 levels. Flexible deployment options can easily scale to provide key management at remote facilities or in cloud infrastructures.

Thales Enterprise Key Management Solutions

Thales Enterprise Key Management solutions are built on CipherTrust Manager. They deliver a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise. It simplifies the administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.



CipherTrust Cloud Key Manager
THALES
CipherTrust Manager
CipherTrust KMIP Server
CipherTrust TDE Key Agent
CipherTrust LUKS Key Agent
CipherTrust Enterprise Key Management Solutions

Figure 4: CipherTrust Enterprise Key Management Solutions

CipherTrust Enterprise Key Management solutions enable organizations to centrally manage and store cryptographic keys and policies for the following third-party products as shown in Figure 4. The following three elements comprise the CipherTrust Enterprise Key Management solution.

- KMIP Server: provides a simple interface to the key management functions on the CipherTrust Manager, delivering powerful, centralized key management capabilities for KMIP-compliant applications/systems such as SAN and NAS storage arrays, self-encrypting drives, and hyper-converged infrastructure solutions.
- TDE Key Agents: CipherTrust Manager centralizes and simplifies key management across Oracle TDE and Microsoft SQL Server TDE using TDE Key Agents, and keeps the TDE keys separate from your database servers.
- LUKS Key Agent: Linux Unified Key Setup (LUKS) provides transparent disk encryption for Linux. The LUKS Key Agents enables you to centrally manage encryption keys for Linux disk partitions.

In addition, CipherTrust Manager integrates with CipherTrust Cloud Key Manager to manage keys for multi-cloud environments, such as AWS, Azure, Salesforce and more.

Thales Hardware Security Module Solutions

Thales offers a variety of hardware security modules (HSMs), which are the highest performing, most secure and easiest to integrate in the market today. They act as trust anchors to protect the master keys that encrypt your data and digital identities in a high assurance FIPS 140-2 Level 3-certified, tamper-resistant appliance. Thales offers the following types of purpose-built HSMs:

- General Purpose HSMs: Luna HSMs come in several form-factors — a network attached appliance, an embedded PCI module, and a portable USB appliance. They can be easily integrated with a wide-range of applications to accelerate general cryptographic operations. The CipherTrust Manager model k570, includes a built-in Luna HSM card.
- Cloud HSMs: Data Protection On Demand (DPoD) is a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple on-line marketplace.

Summary

Data is only as secure as the system that manages the encryption keys protecting that data. A centralized enterprise key management solution is critical to ensuring all sensitive enterprise data is secure and available. CipherTrust Key Management from Thales help organizations maximize IT efficiency through a centralized, extensible platform based solution, and support the burdens of encryption key management across the enterprise and into the cloud – without disrupting existing application or database environments.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com