eBook

Data Security Best Practices Guide

5 approaches for reducing risk and accelerating compliance in the modern enterprise using the CipherTrust Data Security Platform

cpl.thalesgroup.com

THALES
Building a future we can all trust

Data security business challenges

To support digital innovation and business transformation initiatives, many organizations are migrating workloads to the cloud to increase agility, improve quality of service to customers, and reduce cost. However, migrating critical business data to multiple cloud service providers also introduces new challenges and attack surfaces for cybercriminals to exploit.

Explosive data growth and greater demand for access

Enterprises of every size and industry around the globe are producing more data than ever before. IDC forecasts that the Global DataSphere will more than double in size from 2022 to 2026. At the same time, there is a greater demand for access to this information. From business intelligence and marketing teams to partners and third-party vendors—everyone wants to use data to reduce costs, improve efficiency, develop new products, optimize offerings, and make smarter, data-driven business decisions. To meet these demands, data must be produced, stored, and processed in, and shared and distributed to, more places.

Rapidly increasing threats and evolving compliance requirements

At the same time, data breaches continue to threaten the IT landscape at an increasing rate. According to the findings in the 2024 Thales Data Threat Report, the vast majority (93%) of enterprises reported an increase in threats. Enterprises identified malware (41%), phishing (36%) and ransomware (32%) as the fastest growing attacks, and they reported cloud assets such as SaaS applications, cloud-based storage, and cloud infrastructure management as the biggest targets for attack. In response to the evolving global threats targeting personally identifiable information (PII), an increasing number of compliance mandates now aim to strengthen the protection of sensitive data controlled and processed by enterprises. These include Europe's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Brazil's Lei Geral de Proteção de Dados (LGPD).

Operational complexity

CISOs must protect a broader digital surface area with more attack vectors and risks. Distributed and cloud technologies are powerful, but tend to create management complexity. The adoption of cloud, containers, APIs, and disparate tools from multiple vendors adds to complexity and risk. With enterprise security perimeters becoming increasingly blurry, organizations need help implementing and managing consistent, unified access policies to distributed IT resources. Every organization has a mix of legacy and new platforms. According to the Thales Data Threat Report, the percentage of enterprises that agree or strongly agree that managing security in the cloud is more complex than on-premises has consistently grown from 46% in 2021 to 55% in the 2024 survey.

This eBook outlines 5 best practice approaches to address common data security challenges based on Thales' experience working with organizations large and small across geographies and industry verticals, including financial services, healthcare, insurance, government, and retail. Thales' CipherTrust Data Security Platform aims to reduce the complexity and risk of managing sensitive data with a broad range of capabilities, unifying data discovery, classification, data protection, and centralized management for keys and secrets into a single platform.

5 best practices to reduce data exposure risk and increase compliance

- Reduce the risk of data exposure with data discovery and classification
- Protect and control data with advanced encryption and tokenization
- Safeguard sensitive data when migrating workloads to the cloud
- Foster innovation in the cloud without compromising sensitive data
- Enable developers to protect and automate access to secrets

1. Reduce the risk of data exposure with data discovery and classification

Major change programs like digital transformation and extensive migration projects involve moving large amounts of sensitive data from one environment to another. Uncontrolled dispersal of data across cloud platforms increases the potential of a data breach event, as well as infringement of privacy regulations, so data must be managed effectively throughout the migration process.

Fundamental to delivering an effective digital transformation program is knowing your data. To put it bluntly, if you can't find it, you can't protect it. As IT environments become more complex and data is shared across multiple cloud service providers (CSPs) and geographic boundaries, it becomes more difficult to discover sensitive data and have oversight or manage access across data sources. According to the 2024 Thales Data Threat report, 70% of enterprises are able to classify only 50% or less of their sensitive data. Data discovery and classification tools provide visibility into exactly what information you have stored so you can plan an effective strategy for transformation to safeguard data at each stage of the process.

Gartner predicts that "by 2026, more than 20% of organizations will deploy data security posture management (DSPM) technology, due to the urgent requirements to identify and locate previously unknown data repositories and to mitigate associated security and privacy risks." DSPM solutions locate and classify sensitive data, assess the security risks to that data, remediate vulnerabilities, and constantly monitor for ongoing threats. Data discovery and classification are the starting point of every organization's data security posture because any data security strategy will not achieve its full potential if it consistently fails to discover sensitive structured and unstructured data within repositories. This is especially a problem with data repositories arising from new development or testing programs outside of IT's control. They create "shadow data" that can expose an organization to various risks.

Implementing data discovery requires organizations to create an inventory of sensitive and critical information and establish who has access to those assets. While an organization might know the location of structured data, such as a primary customer database store, unstructured data is more difficult to locate. Most businesses can't rely on data flow diagrams alone because at least 80% of their data is unstructured. Hence, a data discovery product that scans for structured and unstructured data across on-premises and cloud systems is crucial for complete coverage.

Thales supports data visibility to help remediate exposure risk and improve data security posture

- Thales CipherTrust Data Discovery and Classification (DDC) helps you efficiently discover, classify and protect sensitive data across traditional and modern data repositories on-premises and in the cloud, so you can uncover and close compliance gaps. DDC scans structured and unstructured data stores and has over 250 pre-built info types based on leading regulatory requirements.

2. Protect and control data with advanced encryption and tokenization

From lost business to regulatory fines and remediation costs, data breaches have far-reaching consequences. According to the 2024 Thales Data Threat report, 93% of respondents said they experienced an increase in attacks, with malware, ransomware and phishing were identified as the largest growth categories.

Encryption plays a major role in data security and is a popular tool for protecting sensitive data against malicious attacks. To protect data at-rest, enterprises can encrypt sensitive data in files and databases prior to storing the data, as well as encrypt the storage drive itself. Enterprise security then depends on encryption key and policy management—the ability to generate, distribute, store, rotate, and revoke/destroy cryptographic keys as needed to protect the sensitive information with which they are associated. Organizations need to follow data security best practices such as strong separation of duties between key administrators and users. Key management systems must allow leveraging a hardware-based root of trust for secure key creation and storage.

When properly implemented, data-centric security gives an organization complete control over its sensitive data from the moment that each file or database record is created. Access to protected data can be granted or revoked at any time, and all activity should be logged for auditing and reporting. While nearly all data repositories include the option of embedded native encryption, managing keys across siloed systems is inefficient and risks compromising data if keys are kept local to the encryption systems they protect.

In order to properly deploy a data-centric security approach, it's critical to have a breadth of data protection methods available at your disposal, and to audit authorized and unauthorized access to the encryption keys and data you are protecting.

Thales provides advanced capabilities for encryption and key management

- The **CipherTrust Data Security Platform** offers the broadest set of encryption and tokenization solutions to protect data in files, folders, databases and applications via dedicated market-leading Connectors in traditional, cloud or virtualized environments.
  - **CipherTrust Manager**, an enterprise key management system, consolidates encryption keys to facilitate consistent security policies across multiple file servers, databases and applications. **CipherTrust Cloud Key Management (CCKM)** consolidates encryption keys across enterprise and cloud platforms.
  - **CipherTrust Transparent Encryption (CTE)** delivers data-at-rest encryption and defends files from privilege escalation attacks. The **CTE Ransomware Protection** extension protects against zero-day ransomware attacks, and the **CTE Live Data Transformation** extension ensures continuous protection with automatic key rotation. **CTE for Kubernetes** provides native support to protect Kubernetes persistent volume claims for filesystem storage.
  - **CipherTrust Application Data Protection**, **CipherTrust RESTful Data Protection** and **Data Protection Gateway** provide application-level data protection, the ability to change ciphers in less than a minute without modifying applications, centrally-managed policies and separation of duties.
  - **CipherTrust Database Protection (CDP)** and **CipherTrust Application Key Management (CAKM)** are vendor-independent database protection tools. CDP protects column-level data within a database, and CAKM offers key management tools for transparent database encryption.
- **Luna Hardware Security Modules (HSMs)** can be leveraged as a secure root of trust for CipherTrust Manager to create a holistic data security solution.

By 2025 Gartner predicts that "30% of enterprises will have adopted Data Security Platforms, due to the pent up demand for higher levels of data security

3. Safeguard sensitive data when migrating workloads to the cloud

The "cloud" simply means someone else's computer, and where that system is located may violate digital sovereignty regulations. What is sovereignty? According to the World Economic Forum, digital sovereignty refers to the ability to have control over your own digital destiny – the data, hardware, and software that you rely on and create. Today, the World Economic Forum estimates that over 92% of all data in the Western world is stored on servers owned by a handful of US-based companies. This concentration creates a situation of high dependence and a challenge for business resilience. Consequently, digital sovereignty has become an important topic for many nation states, and privacy regulations continue to evolve to manage these risks.

Digital sovereignty has raised questions for CIOs considering their cloud strategy, governance, and risk management. Sensitive data includes not only personal data, but also classified and other regulated data, such as financial, healthcare and government-related data. And, the challenge is not only where the sensitive data resides geographically, but also who has access to sensitive data inside a corporation, and where and how that data is shared.

Thales sovereignty-enhancing controls for hybrid IT help organizations simplify governance, achieve regulatory compliance, and reduce risk in the cloud. Organizations are taking different approaches to cloud migration, including:

- Re-hosting virtual machines (VMs) via lift-and-shift into an IaaS environment, redeploying existing data and applications on the cloud server
- Re-architecting applications with major code changes to take advantage of microservices and other cloud features
- Rebuilding a fully cloud native app from scratch, discarding the existing code base and replacing it with a new one built for the cloud
- Replacing legacy applications and migrating to a third party, prebuilt application provided by a vendor with a SaaS model

Thales supports all cloud migration approaches

Regardless of the migration approach, Thales can help organizations control digital sovereignty by supporting the desired path with security solutions that discover sensitive data, protect access to that data, and allow control of access to that data based on granular policies based on regulations.

- CipherTrust Data Discovery and Classification (DDC) provides visibility into where your sensitive information is stored so you can plan an effective strategy for transformation to safeguard data at each stage of the process.
- CipherTrust Cloud Key Management (CCKM) enables centralized external key management for multi-cloud environments, and restricts access to sensitive assets by Cloud Service Provider employees and unauthorized users with support for Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) services.
- CipherTrust Transparent Encryption (CTE) can be deployed to encrypt sensitive data before migration to the cloud using a Bring Your Own Encryption (BYOE) approach.

4. Foster innovation in the cloud without compromising sensitive data

In the rapidly evolving digital landscape, Software as a Service (SaaS) offers unparalleled business opportunities and efficiencies, resulting in a significant shift towards multi-cloud and multi-SaaS usage in today's enterprise environments. In the 2024 Thales Data Threat Report survey, Thales found that the percentage of enterprises reporting 50 or more SaaS apps in use has grown from 27% in 2021 to more than 40% in 2024. In fact, the survey-wide average is now 84 SaaS applications in use. Common examples of enterprise SaaS applications include calendaring and office tools like Microsoft Office 365, communications technology like Zoom, and cloud-based customer relationship management (CRM) software like Salesforce.

The SaaS adoption trend, while unlocking numerous benefits, introduces new challenges to ensuring seamless interoperability and robust data protection across diverse cloud infrastructures. The expanded use of SaaS applications across multiple cloud platforms has led to an increased attack surface, making SaaS applications a prime target for cyberattacks. Over 39% of enterprises have experienced a data breach in their cloud environment, predominantly due to the increased surface area and operational complexities of managing multiple platforms.

Encryption and key management play a critical role in enabling collaboration and innovation in SaaS applications without compromising sensitive data. Thales helps both SaaS providers as well as enterprise SaaS customers mitigate against the threats of a data breach by providing options for greater control over data.

Thales solutions help address digital sovereignty concerns in SaaS applications

- CipherTrust Manager allows customers to maintain exclusive control and storage of encryption keys in the geographic region of their choice.
- CipherTrust Cloud Key Management (CCKM) is the market-leading multi-cloud encryption key lifecycle management solution with the broadest set of cloud and SaaS partner integrations for BYOK, HYOK and cloud native encryption keys including AWS, Google Workspace CSE, Oracle Cloud Infrastructure, Microsoft Azure, Azure Stack, Microsoft 365, SAP Data Custodian , Salesforce, Snowflake, Workday and Zoom.

5. Enable developers to protect and automate access to secrets

Modern development trends like containerization, DevOps, and automation have contributed to a massive increase in the use of secrets such as credentials, certificates, and keys for authentication. This proliferation can lead to uncontrolled secrets sprawl and increased security risk. According to the Verizon 2024 Data Breach Investigation report, the use of stolen credentials is the leading cause of data breaches, appearing in almost one-third (31%) of breaches over the past 10 years. In the 2024 Thales Data Threat Report survey, enterprises ranked secrets management as the number one DevOps challenge.

Secrets are scattered through IT environments, not just in source code but also in configuration files, automation scripts, and tools like Ansible/Chef/Puppet, which makes secrets difficult to track and secure. Secrets also need to be available across multiple environments, like development, test, staging, and production. Secrets management focuses on controlling secrets sprawl and reducing the risk of secrets exposure, while keeping your business running. Using a centralized secrets management solution that integrates seamlessly with AWS, Azure, GCP and other cloud service providers ensures consistent policy enforcement and simplifies governance across diverse environments.

As organizations mature their DevSecOps practices, dedicated security engineering and security champions will improve overall engineering performance in terms of quality and resilience. The 2024 Thales Data Threat Report survey found that over half (53%) of organizations have implemented a formal security champions program as part of a DevSecOps program. Successful security champions programs are proactive efforts at developer enablement. Providing clear, concrete, and repeatable security guidance for developers and operators is critical as security champions are frequently part of the development team, with only "dotted line" reporting to central security teams.

Thales offers enterprise-ready secrets management to address the challenge of secrets sprawl

- CipherTrust Secrets Management provides automatic processes for creating, storing, rotating, and removing secrets to reduce the potential for human error and consistently enforce security policies.

Summary

Thales' CipherTrust Data Security Platform is an integrated set of data-centric solutions that remove complexity from data security, accelerate time to compliance, and secure cloud migrations. The CipherTrust Platform unifies data discovery, classification, data protection, and centralized management for keys and secrets into a single platform. This results in fewer resources dedicated to security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

Discover sensitive data	Protect data wherever it lives	Control access to data
Get complete visibility into sensitive data exposure risk across your organization	Secure your data throughout its lifecycle with enterprise-grade encryption and tokenization	Centrally manage encryption keys and configure security policies to retain control of sensitive data on-premises and in the cloud
• CipherTrust Data Discovery and Classification	• CipherTrust Transparent Encryption • CipherTrust Tokenization • CipherTrust Application Data Protection	• CipherTrust Enterprise Key Management • CipherTrust Cloud Key Management • CipherTrust Secrets Management

Thales offers a choice of key management deployment options designed to meet your needs:

On-premises	Hybrid	As-a-Service
Physical appliance or virtual (cloud) appliance running in private cloud	Single management interface across physical and virtual (cloud) appliances in private or public cloud	Hosted cloud-based key management and data protection services managed by Thales

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com