

# The Key Pillars for Protecting Sensitive Data in Any Organization

## CipherTrust Data Security Platform

Discover

Protect

Control



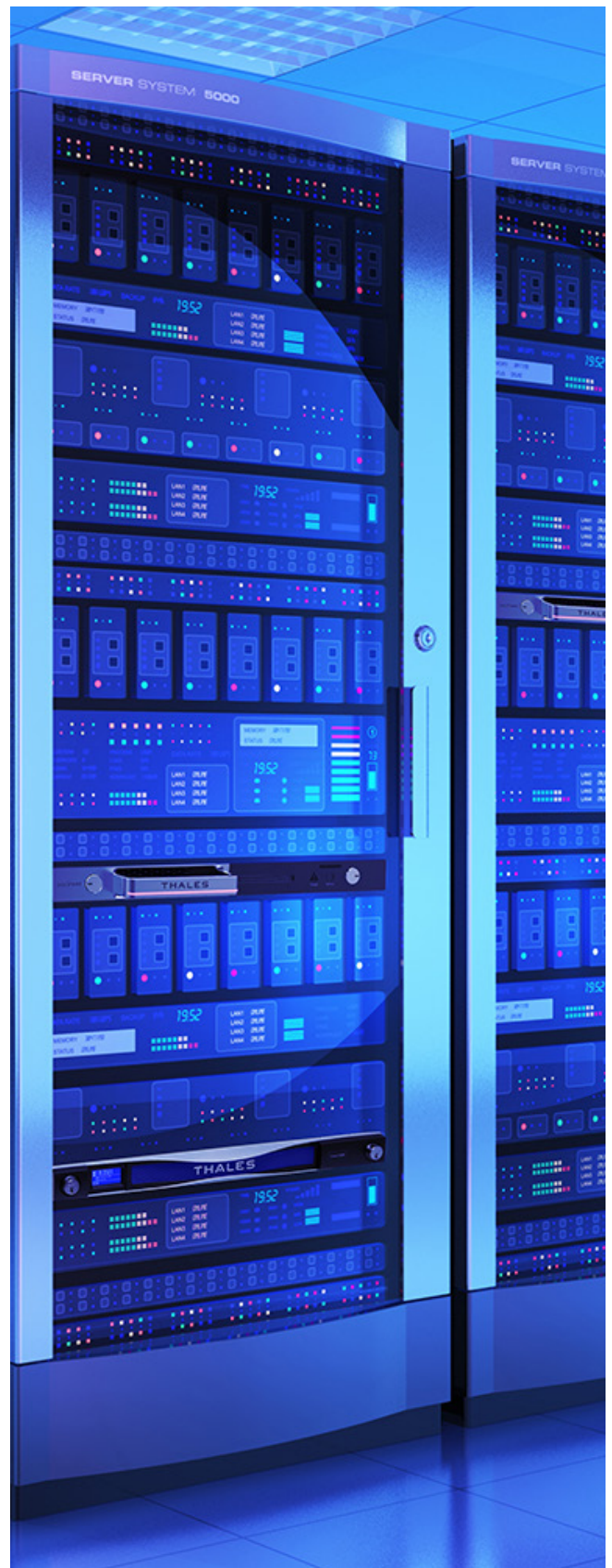
# Contents

- 3 Overview**
- 4 Data proliferation, increased regulations, and better cybercriminals**
- 7 Three-point strategy for protecting sensitive data in your organization**
- 8 Benefits of effective data-centric security**
- 9 How Thales can help you implement a three-point security strategy**

# Overview

Traditionally organizations have focused IT security primarily on perimeter defense, building walls to block external threats from entering the network. While this is still important, it is not enough. Cybercriminals regularly breach perimeter defenses and data frequently lives outside those defenses in the cloud elsewhere, so organizations need to apply a data-centric security strategy that protects data wherever it is. With today's proliferation of data, evolving global and regional privacy regulations, growth of cloud adoption, and advanced persistent threats, data-centric security enables organizations to be in control of their data regardless of location while rendering it unreadable to data thieves. But, to be effective, this protection must happen automatically without relying on user intervention.

This white paper outlines the challenges of data security in this age of data proliferation. It also provides strategies to discover and classify your critical data and apply data-centric security to it.

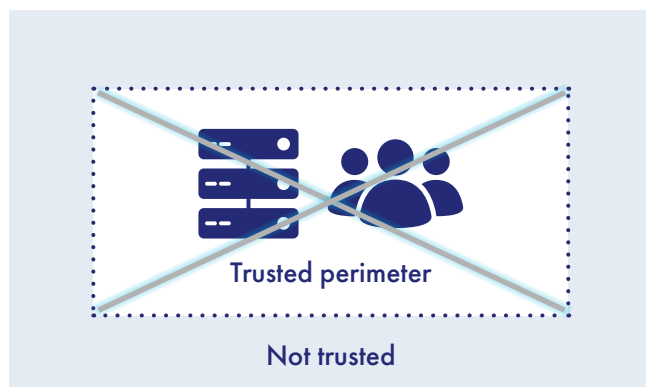


# Data Proliferation, Increased Regulations, and Better Cybercriminals

Many legacy data security architectures were built on the assumption that data will live in a data center and be consumed on-premises. The traditional IT environment was controlled by IT from end-to-end. IT owned and operated the infrastructure, security, and applications and in turn had immense visibility into and control over both data and users. All access to data and applications passed through layers of perimeter security, such as firewalls, next generation firewalls, VPN, anti-virus, intrusion prevention system, etc.

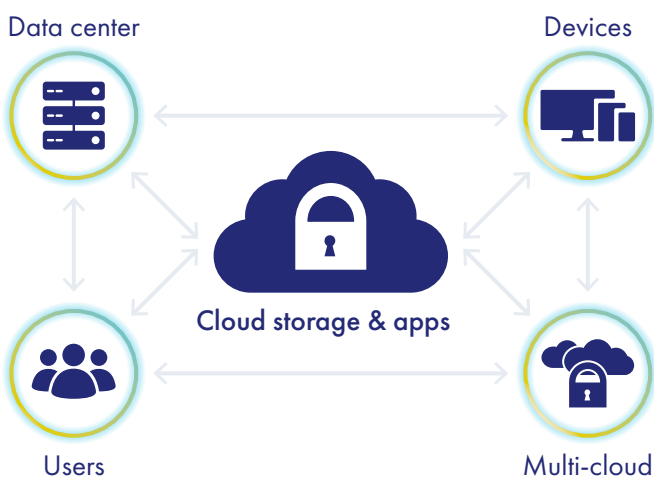
## Move Security beyond the Perimeter to Defend what Really Matters Most

### Legacy Data Security Architecture



Security based on trusted perimeter

### Data-centric Security Architecture



Security protects the data everywhere

However, for the modern organization these checkpoints no longer exist. No matter how strong the perimeter around the datacenter is, the security it delivers is merely conceptual, because:

#### 1. Perimeter security cannot scale for the movement and proliferation of data

The widespread adoption of cloud services, big data environments, and IoT technologies means organizations are moving huge amounts of data very rapidly, often to third party infrastructures and partners. This presents a host of challenges:

- Diverse data forms, including structured, semi-structured and unstructured data
- Perimeter security choke points, which add latency and performance bottlenecks that violate service level agreements (SLA) and therefore users often have direct access to cloud services.
- Insiders everywhere: No longer are the insiders your employees within your perimeter. Your data is now in the hands of contractors, service providers, and other third parties. These "insiders" are individuals you didn't vet, can't monitor, and don't control.

#### 2. Operational complexity and regulation

Movement of data to the cloud, containers, big data technologies, and disparate tools from multiple vendors add to complexity. With increasingly blurred security perimeters, organizations are challenged to afford, implement, and manage consistent, unified policies to distributed IT resources. Every organization has a mix of legacy and new platforms.

Explosive data growth is further complicated by the increasing number of global and regional privacy regulations with differing compliance requirements. To effectively comply, organizations can no longer rely on siloed and legacy approaches to secure their data.

All of this adds up to today's data environments becoming increasingly complex. So, it comes as no surprise that [organizations perceive operational complexity as the top barrier to deploying data security](#). Chief Information Security Officers (CISOs) and Chief Data Officers (CDOs) increasingly recognize the need for comprehensive and integrated data security solutions that provide strong protections for sensitive data regardless of where it is stored or used.

Because legacy data security architectures do not address many of the characteristics of the modern data-centric world, they cannot protect organizations against sophisticated data breaches coming from increasingly determined attackers. If today's CISOs and CDOs want to break the reactionary cycle of measures and counter measures, they must take a completely new approach to security.

**Operational complexity is the top barrier to deploying data security**



# Three-Point Strategy for Protecting Sensitive Data in your Organization

Legacy security architectures have failed often and dramatically, because they reflect outdated views of how organizations interact with their data. Data security today needs to recognize not only that data is the most valuable asset of the organization, but also that it is ever-proliferating exponentially.


Data-centric security protects the data itself rather than just the endpoints, networks, and applications it moves between. Consequently, the data itself is secure, so it can move as much as the organization needs it to without increased risk. Instead of slowing down progress and inhibiting the proliferation of data, data-centric security empowers the organization to make the most of its data wherever it's stored and used.

This chart demonstrates the three core pillars of data-centric security.

## Three Core Pillars of Data Security


**#1**  
**Discover and classify sensitive data**

- Efficiently discover and classify sensitive data
- Get a clear understanding of data and its risks



**#2**  
**Protect sensitive data**

- Protect sensitive data with encryption, access controls and tokenization
- Making it unreadable and useless, if it's stolen or leaked



**#3**  
**Control encryption keys**

- Centralize key management
- Manage key lifecycle
- Unified key management and encryption policies



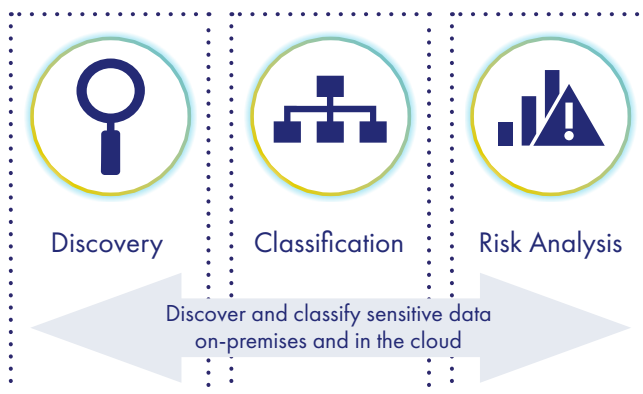
A data-centric security approach must be woven into the DNA of the organization. This holistic approach is based on Thales' experience working with hundreds of enterprise CISOs, CDOs, CIOs, and architects on the frontline of data security and protection as well as best practices required by numerous regulations and industry standards. To adopt this approach to data security, organizations need to do the following:

### 1. Discover and classify your sensitive data

Sensitive data sprawls across the enterprise, the cloud and well beyond. Typically, IT security has limited visibility into where data is stored and who has access to it. Distributed data risks range from breaches to compliance violations. Start by identifying where the most sensitive data assets reside in your on-premises data center, and then move to your extended environments, such as cloud and hosted services. Begin by searching your storage and file servers, applications, databases, and virtual machines. Find data across the organization, wherever it exists, and classify its sensitivity and importance based on internal policies and external regulations.

Discovering, identifying, and classifying your sensitive data is the critical first step in this process, but it also needs to be repeatable and agnostic of technology or geography. Today's data discovery and classification solutions provide visualized dashboards and drill-downs that help you get a clear understanding of what kind of sensitive data you have, where it is located, and its risk score. The risk scores aggregate various parameters, such as protection level, number of elements found, location, amount of sensitive data, etc., and allow organizations to identify the sensitivity of data objects, such as files and databases. Businesses can then protect data and mitigate risks, for example, by prioritizing remediation or making educated decisions about third-party data sharing or cloud migration.

### Data Discovery and Classification is the First Step in Effective Data Security





## 2. Protect your sensitive data

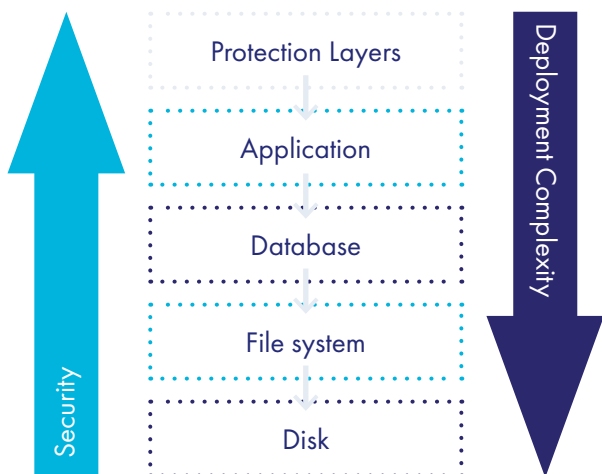
Ideally, to protect the sensitive data itself, you set across your organization a baseline encryption strategy, which mitigates data leakage and breach disclosure risks.

With your data discovered and classified, you can determine the risk each data set adds to your business and prioritize how and where to implement access controls and obfuscation security mechanisms, such as file-level encryption with granular access controls and tokenization with dynamic data masking. This means protecting the data by making it more difficult for unauthorized users to access and making it unreadable and useless, if it's stolen or leaked.

Currently, encryption is one of the most popular and effective data security methods used by organizations. Data encryption translates data into another form, cipher text, so only authorized users can access the data as clear text. While encryption transforms data using a specific algorithm, tokenization protects sensitive data by substituting non-sensitive data. Tokenization creates an unrecognizable tokenized form of the data that maintains the format of the source data. The tokenized data can also be stored in the same size and format as the original data. So, storing the tokenized data requires no changes in database schema or process. If the type of data being stored does not have this kind of structure – for example text files, PDFs, MP3s, etc., tokenization is not an appropriate form of obfuscation. Instead, file-system level encryption would be appropriate. It would change the original block of data into an encrypted version of the data.

When determining which data encryption solution type will best meet your requirements, there are several considerations. At a high level, data encryption types can be broken out by where they are employed in the technology stack. There are four levels in the technology stack in which data encryption is typically employed: disk, file system, database, and application. In general, the lower in the stack encryption is employed, the simpler and less intrusive the implementation will be. However, the number and types of threats these data encryption approaches can address are also reduced. On the other hand, by employing encryption higher in the stack, organizations can typically realize higher levels of security and mitigate more threats.

### Security increases but development complexity also increases when implemented higher in the stack



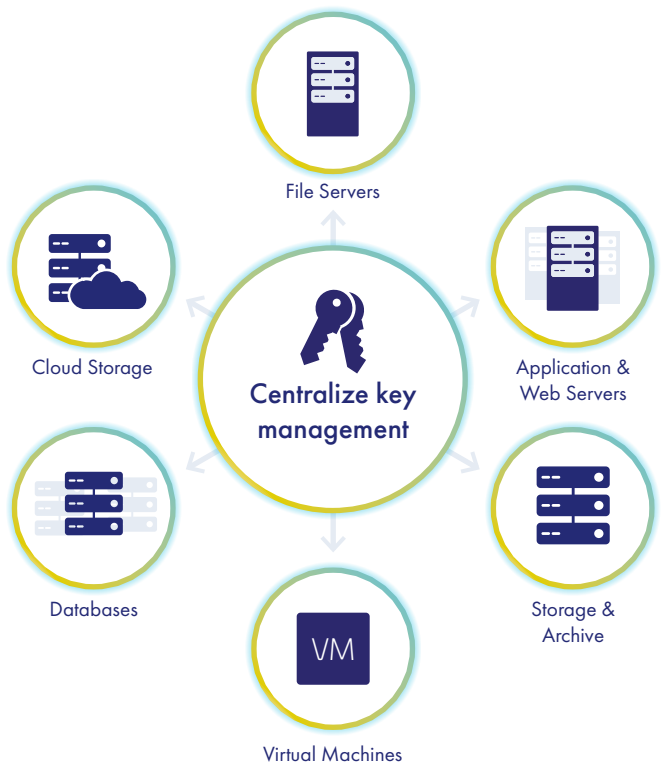
## 3. Control encryption keys

The security of cryptographic processes is dependent on the security of the cryptographic keys used to encrypt the data. If the keys used to encrypt or tokenize data are stolen with the encrypted or tokenized data, the data is not secure, because it can be deciphered and read in plain text. For encryption and tokenization to successfully secure sensitive data, the cryptographic keys themselves must be secured, managed and controlled by your organization and not a third-party or cloud provider.

As organizations deploy ever-increasing numbers of siloed encryption solutions, they find themselves managing inconsistent policies, different levels of protection, and escalating costs. The simplest path through this maze is to transition to a centralized key management model. Encryption key management involves administering the full lifecycle of cryptographic keys and protecting them from loss or misuse. Keys have a life cycle: They're created, live useful lives, and are retired. Key lifecycle management includes generating, using, storing, distributing, archiving, and deleting keys. Some of the benefits of centralized key management are:

- Unified key management and encryption policies
- System-wide key revocation
- Reduced risk of human errors in setting user and administrative permissions
- High availability and scalability
- Secure FIPS 140-2 validation
- Cost savings with automation
- Consolidated audit information
- Simplified backup and recovery
- Enhanced security with comprehensive separation of duties

### Centrally Manage Your Encryption Keys



# Benefits of Effective Data-Centric Security

With an effective data-centric security solution you can address the security challenges incurred by data proliferation and the emergence of global and regional privacy regulations and prepare your organization for a more secure future.

A properly deployed data-centric security solution:

- Helps organizations mitigate risks and reduce costs. Organizations can reduce costs by operationalizing existing security infrastructure on a global scale, reducing manual processes that are labor intensive, repetitive, and error prone, and future proofing their investment by enabling new technology.
- Provides a comprehensive and continuous view of all data assets and facilitates governance of security policies and control.
- Helps organizations understand their data and its risk and prioritize remediation.
- Secures the data, so it can move safely across multiple on-premises and cloud environments while still maintaining its protection profile.
- Ensures that data is protected from malicious users and advanced persistent threats (APTs) attempting to steal sensitive information.
- Reduces fines and helps organizations meet government, organizational, and industry regulations. Organizations can monitor infractions and enforce security policies and rules while creating automated reports and auditing security procedures.
- Creates a defensible legal position in response to a data breach or audit challenge.

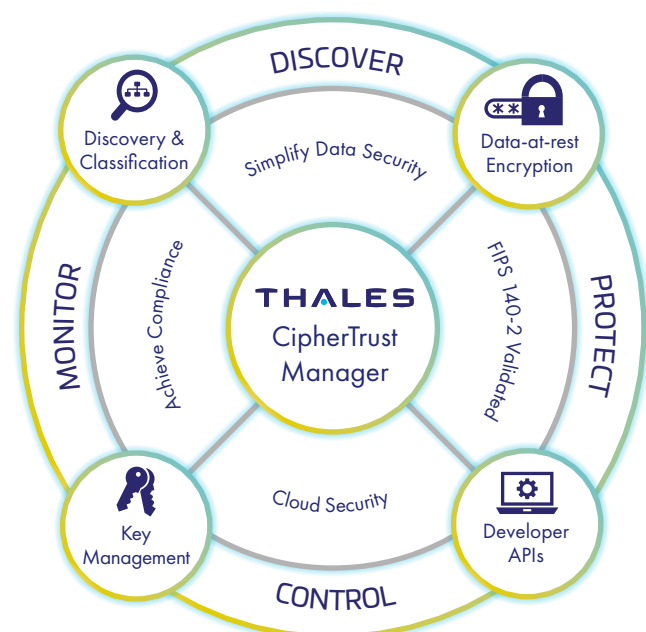




# How Thales Can Help You Implement a Three-Point Security Strategy

Thales is the worldwide leader in data protection. We provide everything an organization needs to discover, protect, and manage its data, identities, and intellectual property: data discovery and classification, encryption, advanced key management, tokenization, and authentication and access management. The CipherTrust Data Security Platform from Thales unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform. This results in less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

## CipherTrust Data Security Platform



## CipherTrust Data Security Platform key capabilities

- Data discovery and classification
  - Risk analysis with data visualization
- Data protection techniques
  - Transparent encryption for files, databases, big data, and containers
  - Application data protection
  - Tokenization with dynamic data masking
  - Format preserving encryption
  - Static data masking
  - Privileged user access controls
- Centralized enterprise key management
  - FIPS 140-2 compliant
  - Multi-cloud key management
  - Unparalleled partner ecosystem of KMIP integrations
  - Database encryption key management (Oracle TDE, big data, MS SQL, SQL Server Always Encrypted, etc.)
- Monitoring and reporting
- Centralized management console

# CipherTrust Data Security Platform benefits

## **Simplify Data Security**

Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform simplifies data security administration with 'single pane of glass' centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or in any external provider's infrastructure. Organizations can easily uncover and close privacy gaps, prioritize protection, and make informed decisions about privacy and security mandates before a digital transformation implementation.

## **Accelerate Time to Compliance**

Regulators and auditors require organizations to have control of regulated and sensitive data and to have reports to prove it. CipherTrust Data Security Platform capabilities, such as data discovery and classification, encryption, access control, audit logs, tokenization, and key management support ubiquitous data security and privacy requirements. These controls can be quickly added to new deployments or in response to evolving compliance requirements. The centralized and extensible nature of the platform enables new controls to be added quickly through the addition of licenses and scripted deployment of the needed connectors in response to new data protection requirements.

## **Secure Cloud Migrations**

The CipherTrust Data Security Platform offers advanced encryption and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored.

## **Reduce Total Cost of Ownership**

The CipherTrust Data Security Platform can reduce TCO for organizations of all sizes by simplifying data security, accelerating time to compliance, and delivering multi-cloud security and control. Built on an extensible infrastructure, the platform enables your IT and security organizations to discover, classify, and protect data-at-rest across your organization in a uniform and repeatable way. Using a legacy approach can often require expensive, dedicated point products which may require further integration and additional staff time to manage, negating any potential cost savings. The many products available on the CipherTrust Data Security Platform can be deployed individually or in combination, and they prepare your organization for the next security challenge or compliance requirement at the lowest TCO. By integrating data discovery, classification, risk analysis, data protection, and reporting into a single platform, the CipherTrust solution frees IT staff and budget for more strategic tasks and empowers the openness and freedom of collaboration the modern organization needs—without sacrificing security.

## **Summary**

Attacks on data are getting more sophisticated because data is becoming more valuable, and organizations need to protect their most sensitive information and defend their reputation. Data-centric security is the only approach that provides both compliance and meaningful protection against today's cybersecurity threats. Effective data-centric security strategies based on the three pillars of data discovery and classification, data protection, and centralized encryption key management enable organizations to securely extract value from sensitive data and confidently adopt digital transformation technologies.

With data-centric solutions from Thales, you can cost-effectively and efficiently protect sensitive structured and unstructured data across your organization.

# THALES

**Contact us**

For office locations and contact information, please visit

**> [cpl.thalesgroup.com](https://cpl.thalesgroup.com) <**

