Solution Brief

Sensitive Data Discovery and Classification

Efficiently discover and classify sensitive data, get a clear understanding of data and risks, and take actions to close the gaps, from a single pane of glass

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

CipherTrust Data Discovery and Classification (DDC) provides complete visibility into the location of sensitive data across your enterprise, empowering you to make better use of your data while mitigating risks and ensuring compliance.

The Challenge

Only 54% of organizations know where all of their sensitive data is stored. 80% of organizations consider data they store in the cloud as sensitive, while only 58% of it is encrypted. While organizations might already know the location of structured data such as a primary customer database store, unstructured data is more difficult to locate. Data is a challenge to classify, which creates compliance gaps and increase security risk.

The Solution

CipherTrust Data Discovery and Classification discovers and classifies data enabling organizations to become more secure and compliant. Bring agility and confidence to your data management. CipherTrust Data Discovery and Classification provides complete visibility into the location of sensitive data across your enterprise, so you can uncover and close compliance gaps. DDC scans structured as well as unstructured data stores for named entities in different formats and global languages to help you find any type of sensitive data, in any language, anywhere across your enterprise.

Enhanced Security

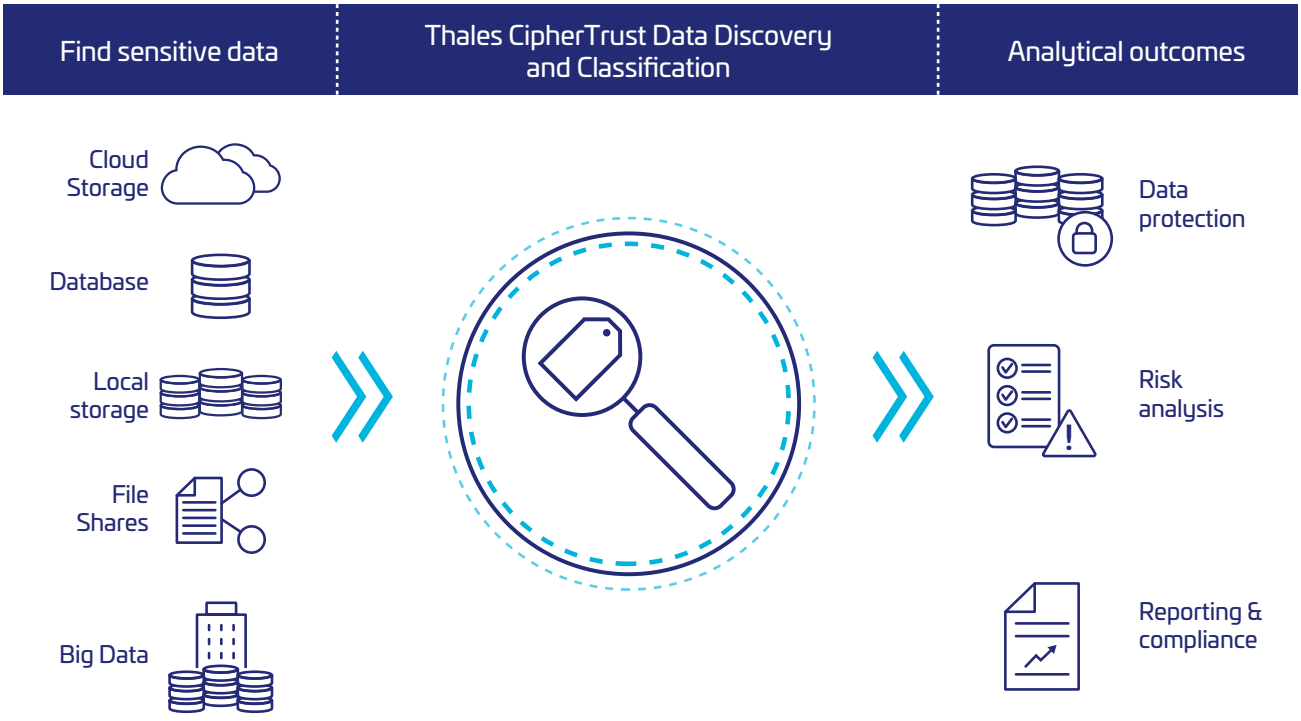
Without understanding where your data is, it's hard to prevent data breaches, unauthorized access, and implement security measures to protect your data. Classifying your data enables to ensure it is managed in accordance to compliance regulations.

Improved Efficiency

Eliminate excess storage and costs by reducing redundant data, obsolete data, or data that's stored yet has no business value to your organization. Create streamlined workflows that automate future processes and grant access based on user needs.

Scalaability

Use your discovered and classified data to make analytical and business intelligence decisions. Authorized users are able to find the data they need.



Enhancing security posture: Delivers a detailed report of what sensitive data you have, where it resides and associated risk to help you make better decisions about what data needs protection.

Ongoing compliance: Keeps you up to date automatically with all major global and regional compliance requirements, while reducing the risk of failed audits or fines by proactively identifying compliance gaps.

Finding and classifying data: DDC scans easily help you discover all of your data and categorize it based on sensitivity and value, allowing you to uncover hidden data risks.

Why choose Thales for Data Discovery and Classification?

CipherTrust Data Security and Classification provides enhanced security, enabling you to close compliance gaps and policy configurations which minimizes data risk. The CipherTrust Data Security and Classification Platform is the single point to improve efficiency and discovery data, secrets, and classify data wherever it resides. Improve operational efficiency, reduce impact of a breach, reduce cost of development, and avoide costs of tooling and storage.

Secrets Discovery

When secrets such as tokens, API keys, passwords, or usernames are discovered by threat actors, they can be used to break into IT systems. CipherTrust Data Discovery and Classification using AI proactively scans code for specific patterns, making developers aware of them before they become security threats. Thales Secrets Discovery is the most comprehensive and reliable secrets discovery tool in the marketplace today and proactively helps stop malicious actors before they gain unauthorized access to your data.

Simplified Installation

Manually discovering secrets is time-intensive and inaccurate. Thales has simplified the discovery of secrets by automating the DDC installation through the Thales Data Platform (TDP). A script for on-prem installations automates the deployment for one or five nodes. For installations in the cloud, set up is just one click for customers, and everything is automatically built into the cloud.

Platform Comprehensiveness

DDC discovers and classifies complex data, making organizations more secure and compliant. DDC provides complete visibility into the location of sensitive data across a customer's enterprise, so they can uncover and close compliance gaps. DDC scans structured as well as unstructured data stores for named entities in different formats and global languages to help customers find any sensitive data, in any language, anywhere across their enterprise.

Uncovering of Compliance Gaps

To avoid the significant business risk of non-compliance with the numerous data privacy acts and regulations, you must know your sensitive data and where it resides. With pre-defined templates for a wide range of data regulations, including CCPA, GDPR, HIPPA and PCI DSS, you can quickly set up comprehensive scans using CipherTrust Data Discovery and Classification to identify all sensitive data across your data stores, wherever they reside. Most compliance gaps you find can be rectified immediately using data protection methods such as CipherTrust Transparent Encryption.

> " 40% of respondents acknowledged they failed a compliance audit in the past 12 months."
>
> – **2023 Thales Data Threat Report**

Understanding your Security Risks

Knowing the precise types of sensitive data in your infrastructure and their associated risk levels can help deliver the deep insight you need to apply additional layers of protection. CipherTrust Data Discovery and Classification enables you to assign specific sensitivity levels for data (none, public, internal, private, restricted) when you are defining your data stores and your classification profiles for different types of data sets subject to regulatory compliance, privacy laws or just internal business requirements. After running your scans, the information can be sorted by risk levels, defined by you, to assist with highlighting potential security risks, such as when no access control or encryption is applied. You can take the appropriate remediation actions, knowing that you are eliminating security risks from your organization.

Discovery and Discarding of Unnecessary Data

It is too easy to end up with uncontrolled data sprawl which costs you money in storage and also increases your risk of a damaging data breach – retaining the data you really need is something recommended as part of PCI DSS requirements. By filtering the report generated by a CipherTrust Data Discovery and Classification scan event, you can pinpoint specific information that needs to be deleted, archived or removed from the data store in question - normally because it is a duplicate, stale or redundant.

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.

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