cpl.thalesgroup.com

THALES
Building a future we can all trust

Evaluation Guide : CipherTrust Data Discovery and Classification

Bringing agility and confidence to your data management

Thank you for agreeing to take part in an evaluation of the Thales CipherTrust Data Discovery and Classification (DDC) solution.

We are confident that it will help improve visibility on all the data in your organization, wherever it resides, enabling you to take the appropriate actions to protect sensitive or vulnerable assets with greater confidence.

About CipherTrust Data Discovery and Classification

Out of the box, CipherTrust Data Discovery and Classification (DDC) enables you to uncover the sensitive data you have (relating to all major privacy laws and regulations) and all the places it is stored, on-premises or in the cloud. Flexible customization capabilities enable you to discover and classify other sensitive assets, secrets and intellectual property, specific to you. Such comprehensive insight helps you make critical business decisions including precisely what data can be safely migrated to the cloud or shared with third parties for example.

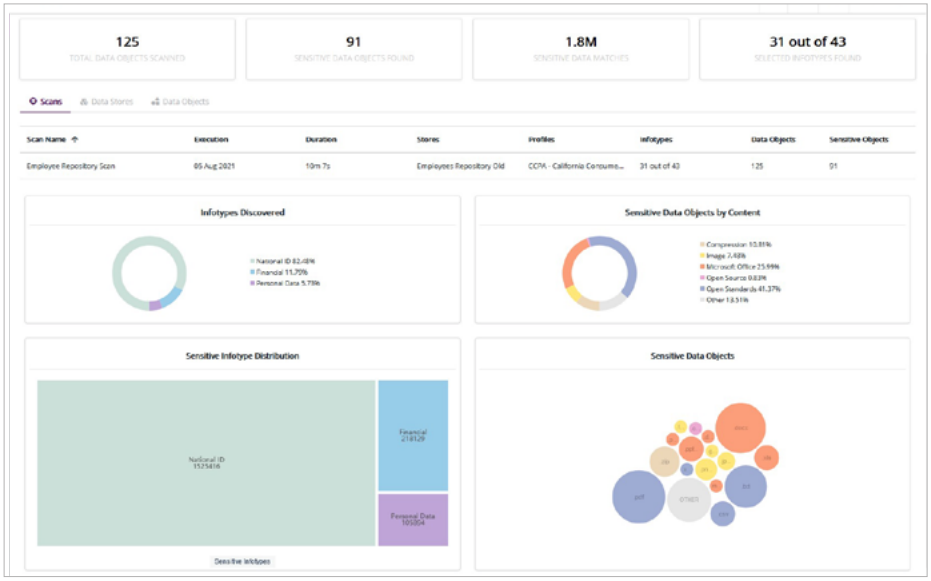
The visual reports created as part of the discovery and classification analysis of the data locations you select are key to helping your team make better decisions about what specific data needs to be better protected – a strong factor in minimizing disruption in the event of a future data breach. Guidance is provided relating to data that can be eliminated, which if otherwise left to grow out of control could significantly increase both risk and liability for your organization.

Unlike the manual approach to searching for data, the use of our specialist solution eliminates the assumptions about what sensitive data may or may not exist – it provides a high degree of confidence that you are building a solid data management strategy with no critical data left unprotected.

Insights you can expect from your evaluation

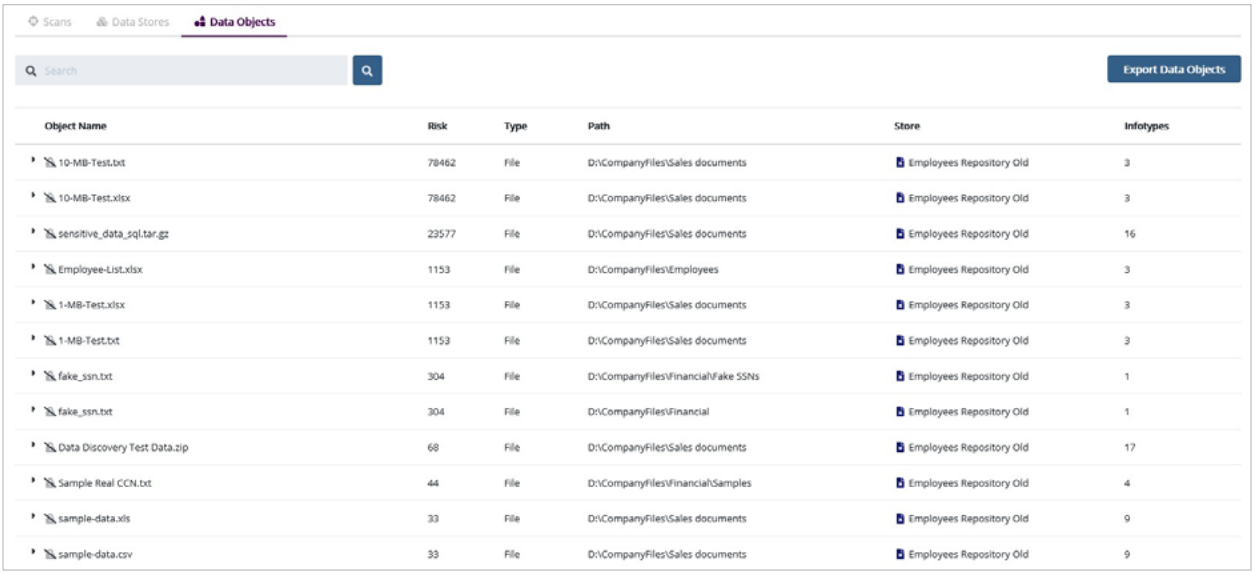
The solution focuses on delivering rapid and insightful analysis of your data. You can configure scans to look for specific types of data in locations of your choice and then utilize the reporting module capabilities to establish what sensitive data you have, where it resides, its risk of exposure and any compliance gaps that may exist. You are then in prime position to take the necessary corrective actions.

The screen shots below provide a quick look at the main aspects you will be using.

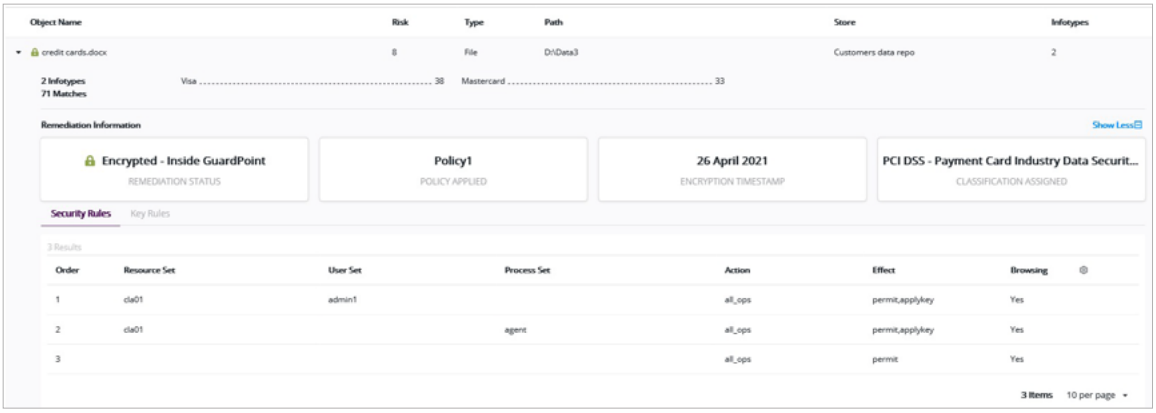


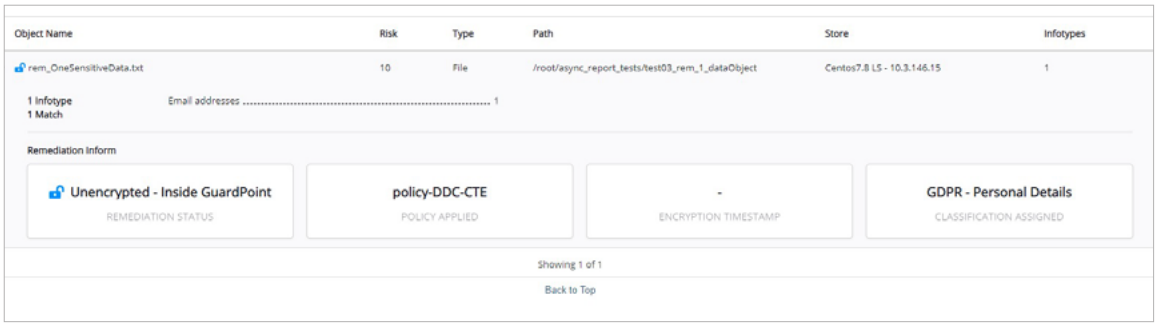
Type of sensitive data stored (financial, national IDs, personal, medical)

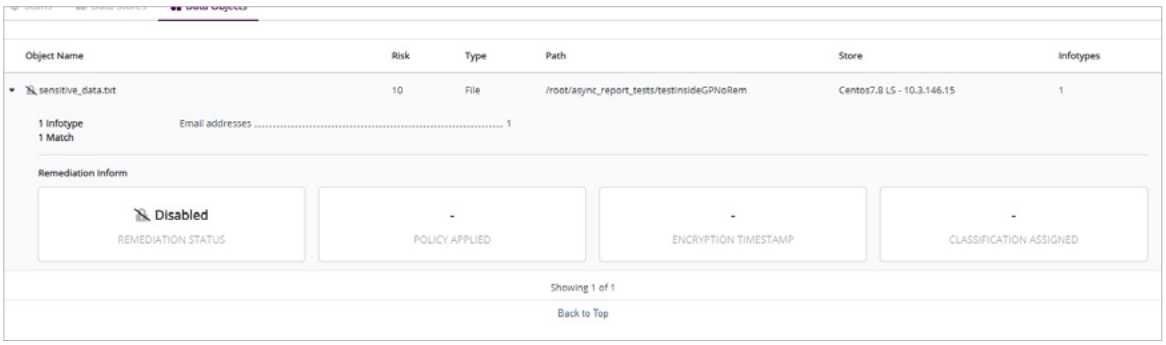
Sensitive data location



Risk assessment







Compliance gaps

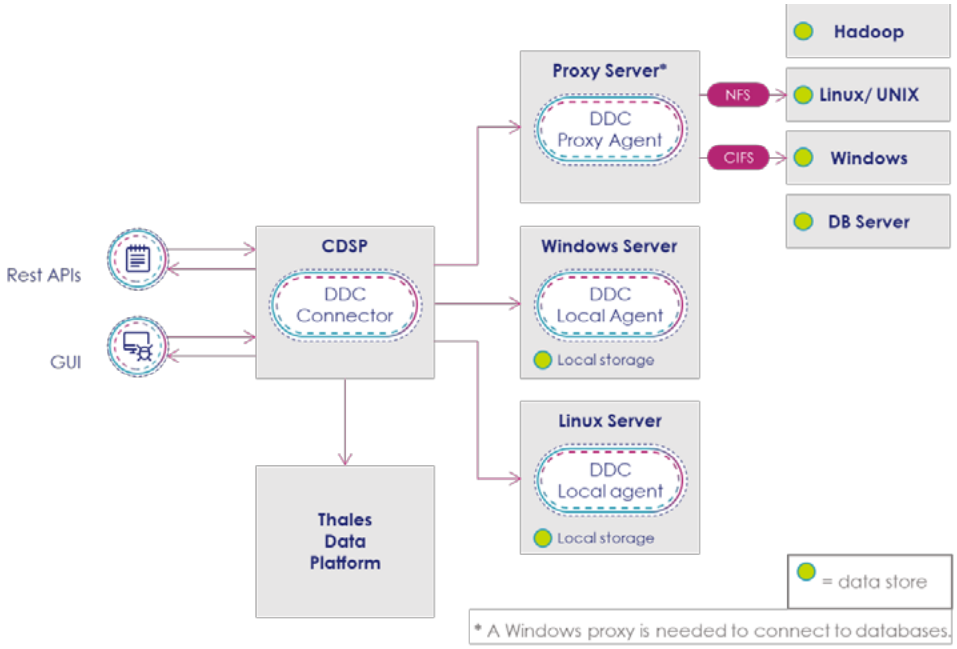
A quick overview

As part of the CipherTrust Data Security Platform (CDSP), CipherTrust Data Discovery and Classification (DDC) allows you to search data repositories for sensitive data elements such as credit card numbers, tax IDs or personal information including names and email addresses. When the search is complete it can build reports that assess what data elements were present, their location within the data repositories and assign a risk assessment based upon the number and type of data elements found.

There are 3 main components of the solution.

- CipherTrust Manager (CM) – Management node where you use a browser interface to access this node to perform setup, define searches and view reports
- Thales Data Platform (TDP) – Thales-built Hadoop node which acts as the data repository of the solution for configuration and scan data
- Discovery Agent – The DDC agent which performs the data scan

The diagram below illustrates a typical DDC deployment. The agent component can be deployed directly on the server to be scanned or remotely on a proxy server. An agent deployed as a proxy can scan any supported databases or shared file systems. In contrast, a local agent must be deployed directly on severs to scan files that are only available on local file systems.



Typical DDC deployment

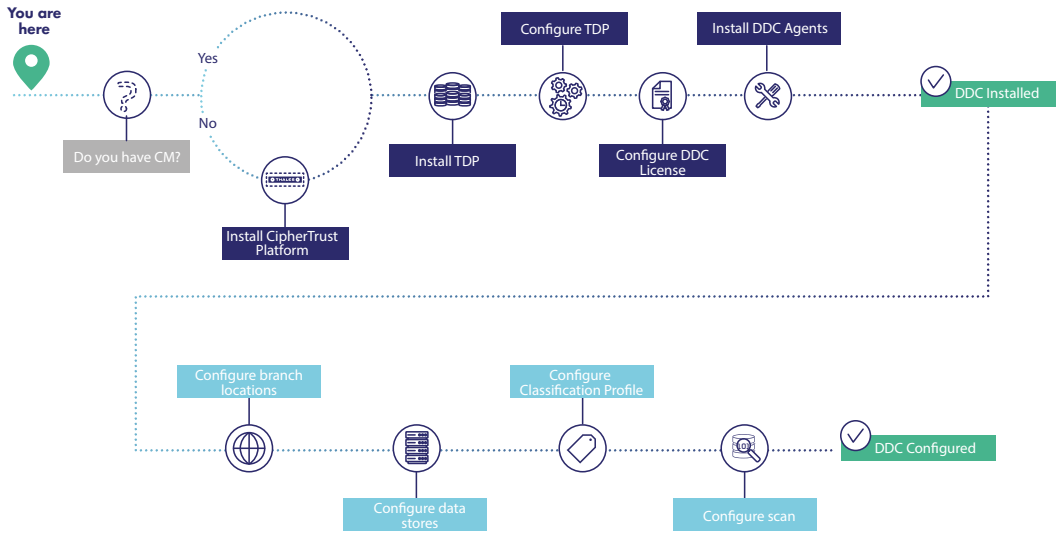
Steps to consider before deployment

There are some preparations you need to make before installing and using DDC. The table below provides guidance on ensuring you have the best possible environment in place to run your DDC evaluation.

Step	Action	Details
1.	Ensure you have suitable servers and network access	At certain stages of the installation you will need to install discovery agents – make sure you have details of the server names, their IP addresses to use and that the appropriate access rights are available to the team involved. The credentials required for all the locations to scan should have "read only" access rights.
2.	Decide which team members will participate in the evaluation	You may wish to check data belonging to different teams – make sure you have identified the critical people involved and secured their availability in advance.
3.	Clarify the locations and types of data stores to be part of your scans	Our recommendation would be to have clarity on the data store category, type and version in order to be able to properly select the agent for scanning. Specific information and supplementary guidance is provided in the online documentation. It is very important to select the correct agent and define the proper data store in order to be able to provide accurate scan results.
4.	Define the type(s) of data you wish to find	Ask the data owners well in advance, what types of data they wish to find during the evaluation – everything linked to data privacy laws are covered using pre-defined templates, but other data types proprietary to your organization will require extra preparation time (and subsequent use of the customization capabilities of the solution).
5.	Identify any data that is already encrypted (possibly using another vendor solution)	Will DDC be able to gain access to that data during the scan to perform some meaningful analysis? Please check with your Thales Account Manager or authorized reseller, if CipherTrust Manager is able to manage the keys for any third party product in question being used for the encryption.
6.	Decide when and how often you will activate the scans	Although the scanning process does not have any significant impact on the performance of your systems, you should start thinking about when you will run the scans and how many different types of scan you intend to perform during the evaluation period. Our recommendation is to start with simple scans over a small data footprint to gain experience of how long it takes in your environment - then you can add more complex search parameters and run more frequent scans. The targets, classification profiles, filters and frequency of the scan can be edited after a scan has been defined.
7.	Consider what action(s) you will take when you uncover sensitive data that is not protected	A main benefit of the evaluation is in qualifying whether or not you have sensitive data that is not currently protected. This may come as a surprise or you may have suspected such data would be found somewhere throughout your network of servers. If you are unfortunate enough to find regulated data that is not secure then you need to be prepared to take rapid corrective action to reduce your risk. Making use of other CipherTrust Data Security Platform connectors such as CipherTrust Transparent Encryption or CipherTrust Tokenization may prove to be an astute move.

Getting started

All of the documentation you need is available online. To help you navigate through the important pieces, below you will find an outline of the minimal set of installation and configuration steps you need to complete before you can start defining the locations you wish to scan for sensitive data.



Pre-requisites:

1) Make sure you fulfill all the requirements for having DDC in place before you start with the installation steps

Installation steps:

1) If you are new to the CipherTrust platform or wish to install a separate version of CipherTrust Manager to use with your DDC evaluation, then you need to install Virtual CipherTrust Manager

2) If you are an existing CipherTrust Data Security Platform customer, then you will already have CipherTrust Manager installed and in use - ***please note that currently DDC is designed to work with Virtual CipherTrust Manager rather than the physical appliance***

3) Once CipherTrust Manager is installed you can then install DDC in a specific sequence as follows:

a. Install TDP

b. Configure TDP

c. Configure the DDC license in CipherTrust Manager

4) Install DDC agents

When installation of CM, TDP and DDC is complete, you can then launch DDC from within the CM console and begin configuring the various items needed to create and run a scan.

Configurations steps:

1) Configure branch locations - a branch location specifies a site where the file servers, databases, and data centers that contain data to be scanned are physically located

2) Configure data stores - a data store is the entity where the data is actually stored, with DDC supporting various types - local, network, database, Big Data and cloud

3) Configure classification profiles using pre-defined infotypes where possible - an infotype is used to categorize specific data (such as passport numbers or email addresses) to look for during a discovery scan, forming an integral component in the definition of a classification profile

4) If necessary create one or more custom infotypes to meet your specific needs

5) Configure scan - a scan is part of the discovery process that is used to search for sensitive data within data stores using criteria defined in classification profiles

Suggested use case to explore – local storage protection

Following the steps below will help you plan your local storage protection. The links take you to the relevant section in our online documentation portal, Thales Docs.

1) Set up your local data store in DDC

2) Configure a scan defining what type of data you want to look for using one of the pre-defined classification profiles (GDPR, PCI DSS, CCPA, etc.)

3) Run the scan

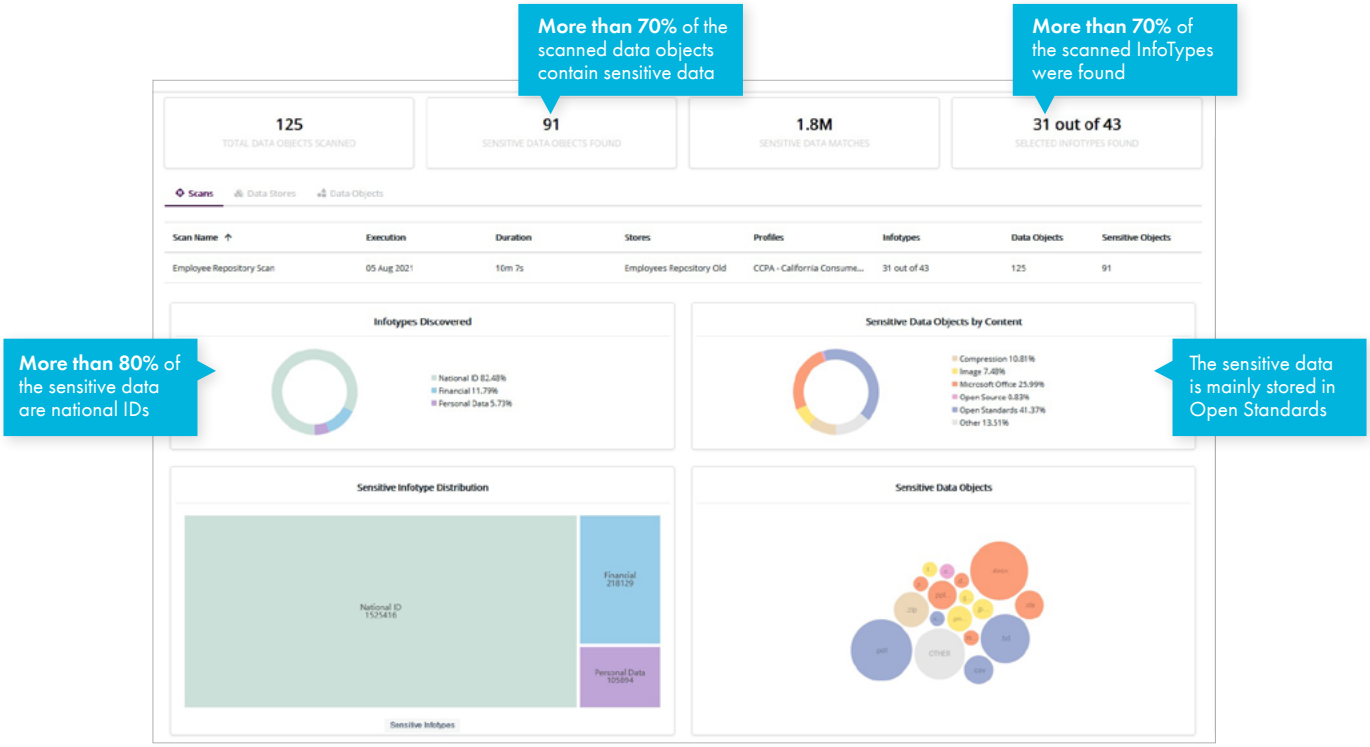
4) Generate the report for the scan you have just run - the report will show locations and associated risk levels associated with data objects in the various data stores

5) Analyze the results locating the paths that contains sensitive data without protection and define your actions over those locations

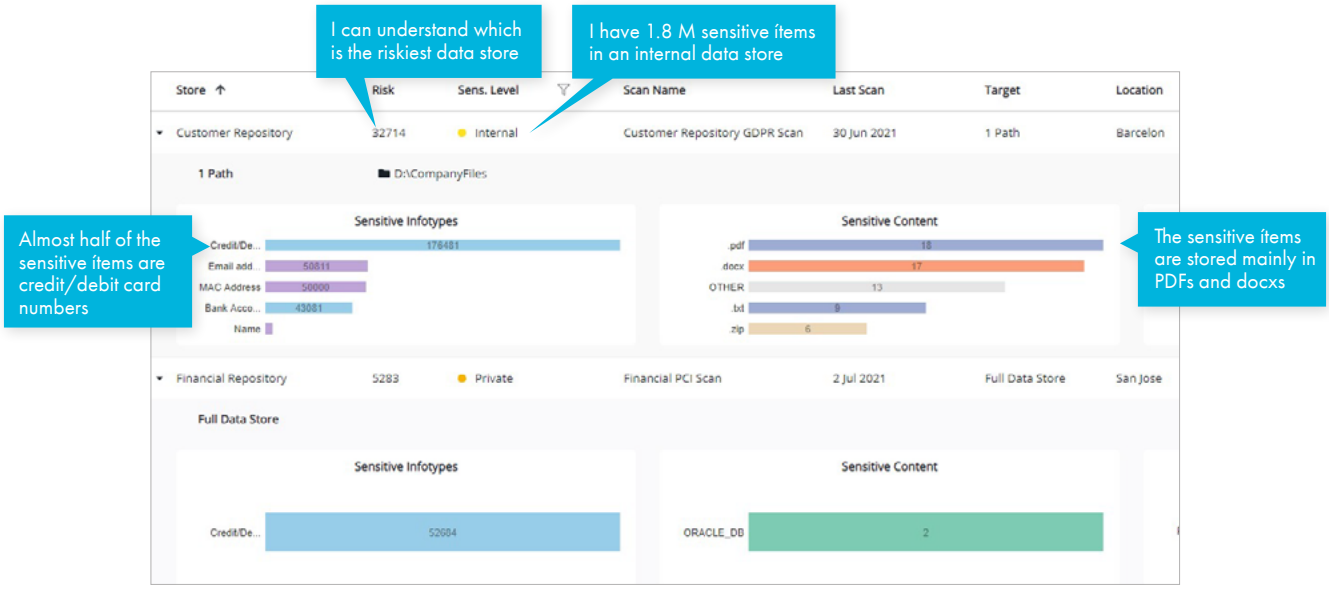
Analyzing the results

The screen shots below provide an overview of how to interpret the results from the scans. We are using some examples from the Thales test environment to illustrate the power of the scanning and reporting capabilities of DDC.

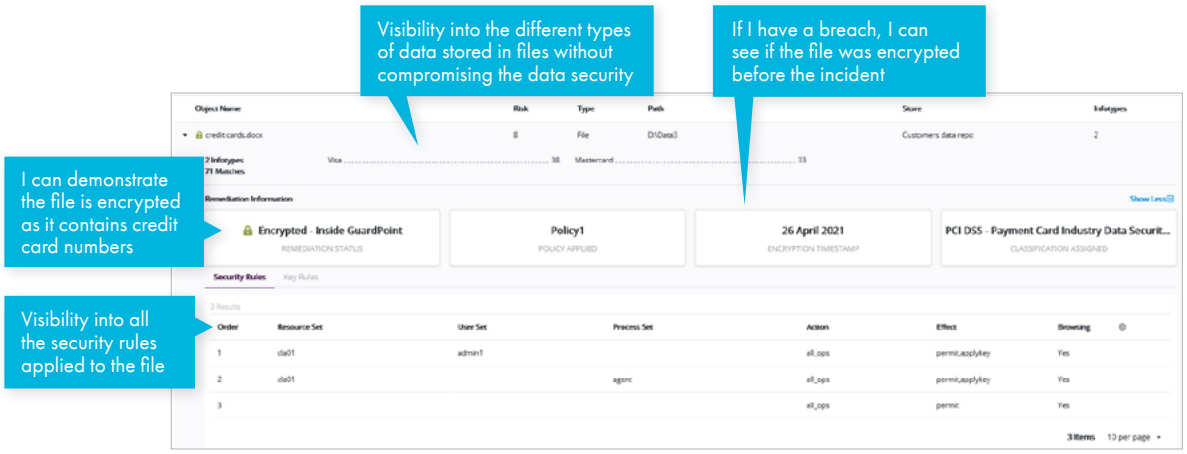
In this first example, we are scanning a local storage called "Employee Repository Old" to search for CCPA data.



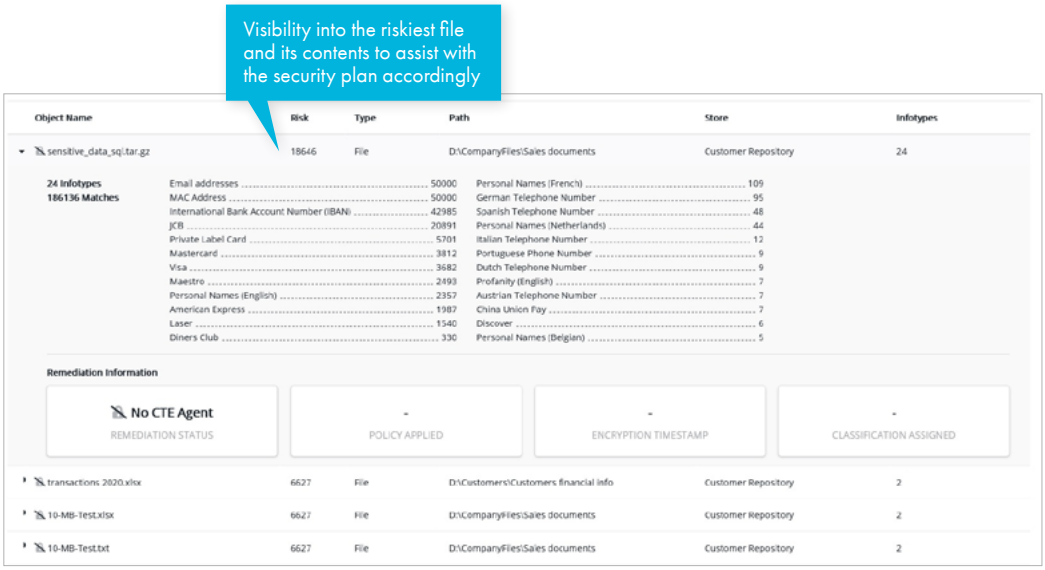
In this second example, we are grouping the information that we got after scanning a customer repository searching for GDPR data and a financial repository (Oracle DB) searching for PCI data.



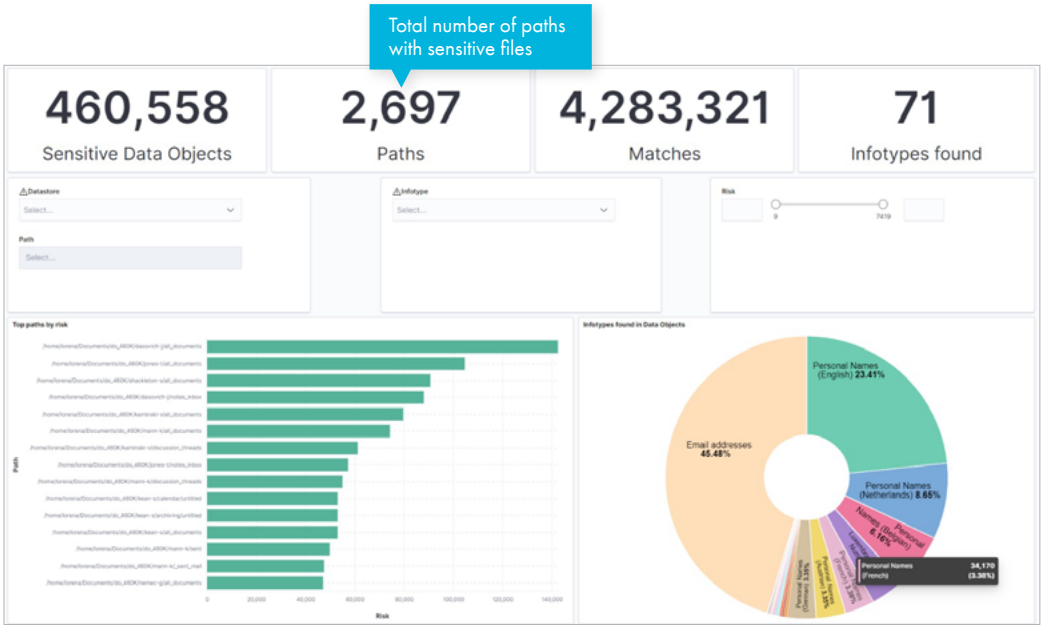
In the following example, we are displaying a Data Object that we encrypted automatically using DDC after we discovered the file contained sensitive data (credit card numbers).



In the following example, we are showing a Data Object that contains sensitive data (email addresses, MC address, financial information, among others) and it cannot be protected as no CTE agent is available in that location.



The following report has been generated based on a NDJSON file created by DDC and using ELK for analysis and display.



Your feedback

Thank you for completing the evaluation of our CipherTrust Data Discovery and Classification solution. We trust you found it useful and look forward to hearing your feedback. We should be grateful if you would answer as many of the following questions as you can.

Question	Your response
How did DDC fit into your overall data security strategy?	
What is the main use case of interest for deployment of DDC?	
What were the highlights or benefits that you saw?	
What information was most useful in the dashboards (e.g. statistics, insights, incident report or something else)?	
What were the drawbacks of the solution for you?	
What, if anything, seemed confusing to you?	
What missing features would you like to see?	
How would that help you?	
Any other feedback you wish to share?	

You can use the following link to take the survey or scan the QR code below to launch the survey on a mobile device.

Thanks in advance.

The CipherTrust team at Thales.

About Thales

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 number 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

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 <