Data Sheet

Top reasons for using CipherTrust Data Discovery and Classification

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Complying with the constant evolution of data privacy laws and regulations is very challenging. Knowing where all your sensitive data resides is a timely and costly ongoing task when you are relying solely on manual methods. Minimizing your risks due to the inevitable data sprawl, if left unchecked, can get out of hand.

Good news, help is readily at hand in the form of CipherTrust Data Discovery and Classification using AI, which delivers considerable benefits including:

- **Enhanced security.** Uncovering compliance gaps to help you reduce risk
- **Improved efficiency.** Securing your data at highest risk in a timely manner
- **Inherent scalability.** Enabling you to add more locations to your scans on-demand as your data footprint grows

CipherTrust Data Discovery and Classification helps your organization get complete visibility into your sensitive data with efficient data discovery, classification, and risk analysis across heterogeneous data stores. In the following, we state top reasons why you should consider implementing CipherTrust Data Discovery and Classification now.

Enhanced security

Uncover 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.

Highlight 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.

Identify Policy Misconfigurations

It is widely recognized as good security practice to limit access to data, especially sensitive data, to only those that need it. However, a thorough investigation can take time if conducted in a manual, ad-hoc manner and it may not provide all the evidence you need regarding errors made when configuring access control policies. This is where CipherTrust Data Discovery and Classification can step in with its comprehensive scans and associated reports. You can easily review the report data to see exactly where access to sensitive data needs to be controlled more strictly or where mistakes made in configuring access rights need to be rectified.

Discard 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.

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 can proactively scan code for specific patterns, making developers aware of them before they enter the main repository, get deployed in protection, and 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.

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.

Improved efficiency

Leverage risk factors

Discovering sensitive data is a big challenge, as is knowing how to react based on the risk to your business by accidental exposure to sensitive data. To achieve this you need a basis for defining the risk factor associated with any given data set. CipherTrust Data Discovery and Classification helps by allowing you to set risk levels for each data store and classify risk according to the types of data elements held in a data store. This way you can run multiple scans and combine them into a single report for analysis. You can then sort the report to review the risk factors and enable you to prioritize the appropriate protection action.

Coordinate actions centrally

After sensitive data has been discovered and classified, it is important to secure the data quickly and efficiently while applying appropriate access controls and data protection mechanisms. CipherTrust Data Discovery and Classification is a component of the broader CipherTrust Data Security Platform, which offers various data protection actions and access control settings via connectors configurable from the CipherTrust Manager console. For example, the market-leading CipherTrust Transparent Encryption connector can be configured to encrypt a recently discovered sensitive data store, or certain data sections can be tokenized to protect data privacy from one console.

Reduce integration effort

When you need the ability to discover the locations of sensitive data you possess, subsequently protect the data you identify and then control strict access to reduce your risk, dealing with multiple products from different vendors that do not integrate easily or require proprietary management tools is cumbersome. The CipherTrust Data Security Platform provides all you need in a single platform – your one-stop shop to discover, protect and control. The sensitive data found by CipherTrust Data Discovery and Classification can be protected quickly (using encryption, tokenization or data masking) by the appropriate CipherTrust data protection agents (all under the control of the centralized CipherTrust Manager). Different CipherTrust Data Discovery and Classification groups can be assigned to different data stores to help speed up the time it takes to run and analyse data from scans. This approach enables an organization the ability to split complex activities into manageable chunks, each covered by a different expert team, while providing cross-team functionalities to facilitate a coherent solution flow.

Inherent scalability

Incorporate New Sources

As your data footprint expands and you use different types of data stores, you need to ensure that your data discovery capabilities can find and classify your sensitive data at all times, especially as your data store requirements are changing. It does not matter if your data is structured or unstructured, CipherTrust Data Discovery and Classification enables you to add a variety of different data stores (local, network, database, Big Data, cloud) at any time to cover your latest storage locations, so that you can be sure that your ongoing scans are looking at all the places that your sensitive data resides.

Expand Discovery Capability

New types of information are regularly emerging which need to be analysed. For example, your data footprint may be changing to encompass more cloud-based storage locations. You need a solution that is regularly being updated to keep relevant to your changing needs as well as technology advances. CipherTrust Data Discovery and Classification offers you the ability to create customized definitions for the sensitive data you are trying to find if it is not part of a recognized data regulation. We call this capability 'custom InfoTypes' and it enables you to find just about anything. You can to scan data both on-premises and in multi-cloud data stores. A mixture of local and proxy discovery agents are available to help simplify logistics, increase performance and enable you to scale rapidly when required.

CipherTrust Data Discovery and Classification offers you the ability to create customized definitions for the sensitive data you are trying to find if it is not part of a recognized data regulation.

Address Proprietary Needs

You may have sensitive data that falls outside the predefined templates that also needs to be located and remediated. You may also have some sensitive data (e.g. intellectual property) that is proprietary to your organization that needs to be protected. CipherTrust Data Discovery and Classification provides the ability to add new custom classification profiles and edit the predefined classification profiles we have developed on your behalf – you get the best of both worlds. In addition, you can add new custom tags for your data types not covered by the predefined tag list. It is the discovery and classification solution that all your likely needs now and well into the future.

Simplified Installation

Thales has simplified the set up of CipherTrust Data Discovery and Classification by automating the 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.

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