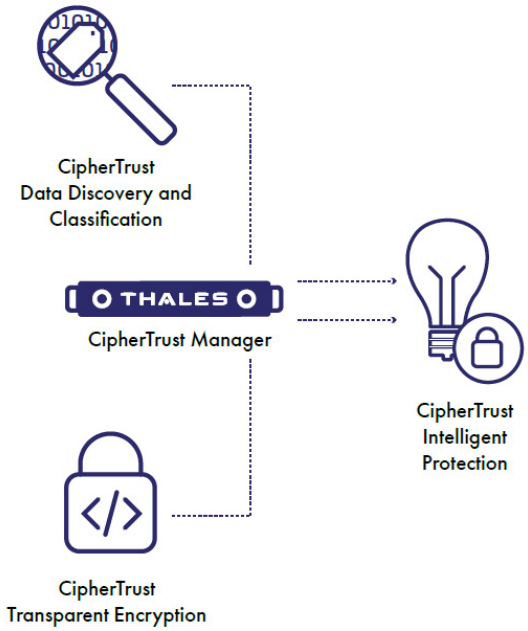
Trusted Cyber Technologies

THALES
Building a future we can all trust

Top 10 Reasons CipherTrust Intelligent Protection will Protect Your Data & Reduce Your Risk

You and your colleagues are undoubtedly creating, storing and managing more data than ever before – a study from Dell finds that organizations are managing 10 times more data than they did 5 years ago. Keeping this enormous amount of data secure and in compliance with stringent regional and global data security and privacy laws is extremely challenging. Uncertainty over compliance status elevates your business risk and increases your potential liability. Perhaps a critical ongoing task for your organization is finding and classifying the data you have efficiently – if you don't know what you have (and where it resides), you can't protect it effectively and your data is vulnerable. Reducing the time between discovery and subsequent protection of your sensitive data is certainly advantageous, bringing a new level of agility and confidence to your overall data management.



CipherTrust Intelligent Protection discovers and classifies data based on sensitivity and vulnerability before proactively protecting any sensitive data using encryption and access controls. It is a solution configuration within the Thales CipherTrust Data Security Platform that leverages CipherTrust Manager, CipherTrust Data Discovery and Classification and CipherTrust Transparent Encryption – an all-in-one solution delivering a proven unified approach. For those of you already experiencing the benefits of these connectors, this new, innovative feature enables you to create an integrated workflow to simplify and strengthen data security. To help you better understand the advantages of our offering, we have complied a top 10 reasons for using CipherTrust Intelligent Protection.

CipherTrust Intelligent Protection if available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

Accelerate time to compliance

1. Automated compliance work low

A long elapsed time between identifying sensitive data and protecting it can leave you non-compliant with data security privacy laws and regulations and therefore at increased risk.

With CipherTrust Intelligent Protection, the ongoing, proactive discovery, classification and protection processes reduce the time to attain or remain in compliance, delivering substantial improvements in operational efficiency. The transparent operation based on an integrated workflow enables you to discover, classify and then encrypt in a single step with no manual intervention when new sensitive data is found. It makes use of policies[1] and GuardPoints[2] which are quick and intuitive to define.

2. Support for evolving regulations

Data privacy laws and regulations are never static – new ones appear regularly and existing ones often get enhanced, making it difficult for you to keep pace.

That is where CipherTrust Data Discovery and Classification steps in with its comprehensive coverage of all major regional and global laws and regulations. The built-in classification profile[3] templates and infotypes[4] (which define the types of sensitive data that are important to protect) are constantly kept up to date to reflect the latest mandates. CipherTrust Transparent Encryption provides the appropriate policies to enable you to implement the encryption and access controls necessary to achieve and maintain compliance in a timely manner.

3. Reduced risk

It is often the data that you don't know you have that can damage your brand, reputation or bottom line. Finding a way to rapidly identify data compliance gaps and potential security risks is of paramount importance. Using the high performance and accurate discovery engine is an extremely useful way to find data subject to regulations that you may not realize even exists within your organization. Linking this discovery process automatically to encryption of any sensitive data found enables you to fast track your route to a fully compliant environment and at the same time enjoy peace of mind.

Uncover and close security gaps

4. Risk-based guidance

Not all potentially vulnerable data can be encrypted immediately, especially where the volume of data in question is extremely large and spread across multiple locations. There always needs to be some level of prioritization applied.

1 A policy is a collection of rules that govern data access and encryption
2 A GuardPoint specifies the list of folders or paths to be protected – access to files and encryption of files under the GuardPoint is controlled by security policies
3 A classification profile uses a list of infotypes to define what kind of sensitive information to search for during a discovery scan
4 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

CipherTrust Data Discovery and Classification provides risk-based guidance on what specific data to encrypt. The discovery engine delivers a comprehensive analysis (via scan results and associated reports), enabling you to make a decision on what additional protection (if any) is needed for any data identified and classified as being at risk.

5. Controlled data encryption

If you lock down all your data (using encryption for example), you are unlikely to realize its full value and potential. Equally, if not protected properly, it can be a significant liability. Finding the right balance is the key, but also the biggest challenge.

Careful use of our intelligent protection capability will give you the flexibility and control needed to address your specific data protection requirements. It enables you to define policies that will encrypt only the sensitive data that matters to your organization. Dynamic GuardPoints enable you to set a path for discovery and only the at-risk data identified on that path (or in the associated sub-directories) will be encrypted, rather than the complete path – importantly all of this is totally under your control.

6. Custom discovery capabilities

Not all data that is sensitive to your organization is directly linked to data privacy laws and regulations. After all you likely are storing sensitive assets that are specific to your agency and would cause damage if exposed through a data breach.

The customization capabilities inherent in our data discovery product help you find such confidential data. You can create custom classification profiles and infotypes to supplement the pre-built ones defined by Thales. This enables discovery of data proprietary to your organization which can then be protected using any of the numerous encryption, tokenization or access control methods supported by the CipherTrust platform. The encryption use case has the added benefit of an automated mode if desired.

7. Highly scalable solution

As we already know, your data footprint is only likely to get significantly larger in the future and the rate of change can be quite daunting – ensuring that your chosen data protection solution can meet your demand well into the future is a very important consideration.

The CipherTrust platform inherently is designed and proven to be highly scalable to keep pace with your growth. Additional data storage capacity for CipherTrust Data Discovery and Classification and extra connectors for CipherTrust Transparent Encyrption (together with new GuardPoints) can be added easily to keep pace with your data growth in terms of both locations and volumes. Connector installation operates seamlessly in the background, requiring minimal resource overhead, no application changes and no system downtime.

Build operational efficiencies

8. Single vendor platform

Why work with multiple vendors for different elements of your data protection strategy when you could cover the vast majority of your requirements via a single vendor and achieve better return on investment?

Discover, protect and control capabilities are all provided from within the CipherTrust platform, eliminating the complexity of dealing with the integration of components from multiple vendors. It is fast, efficient and simple to setup, validate and activate the CipherTrust Intelligent Protection feature as part of the platform. You have the added advantage of being able to cover a comprehensive range of unstructured data types, resident on a wide range of environments.

9. Centralized management console

You are faced with a myriad of different graphical interfaces, terminology and operating environments when using data discovery, encryption and access control solutions from different vendors – integrating, maintaining and the ongoing training of your staff is complex.

Our platform is an all-in-one integrated solution delivering a consistent user experience and reduced training costs for your organization. When deploying CipherTrust Intelligent Protection, you benefit from CipherTrust Manager being used to launch and manage both CipherTrust Data Discovery and Classification and CipherTrust Transparent Encryption, supported by granular user access controls and logging.

10. Common policy approach

If considering linking your data discovery process automatically to your encryption process, you obviously want to avoid unnecessary complexity.

When using CipherTrust Intelligent Protection, there is a common approach to defining the data discovery and protection security policies. The method and syntax of policies are consistent on the same data set when you define them using the appropriate security policy management interface for discovery and encryption connectors. This enables you to fine tune the precise encryption and data store path to your exact needs to achieve the automated protection.

CipherTrust Data Security Platform

CipherTrust Intelligent Protection is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, and data protection. It provides unprecedented granular access controls and centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your agency.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com