Brochure

THALES

CYBERSECURITY

Thales Data Security Platforms

cpl.thalesgroup.com

Data Security **Challenges**

As security breaches escalate and regulatory pressures grow, organizations face an urgent need to discover, protect, control, and monitor sensitive data—wherever it resides. From on-premises infrastructure to hybrid and multi-cloud environments, the complexity of modern IT ecosystems demands a unified, scalable approach to data security.

The Thales CipherTrust Data Security Portfolio provides comprehensive, centralized solutions to address today's data protection challenges. It enables organizations to do the following. Discover sensitive data across all environments for complete visibility. Analyze activity in real time to detect anomalies and ensure compliance. Protect it with robust encryption and tokenization. Control access through granular policy enforcement and key management.

By simplifying and unifying data security operations, Thales enhances efficiency, accelerates compliance, and significantly reduces risk. Whether deployed on-prem, via cloud service providers, or as a fully managed Thales service, Thales empowers enterprises with marketleading protection, full control, and exclusive ownership of their encryption keys.

Discover **Challenges**

Identifying sensitive data:

Discover and classify sensitive data across files, databases, and cloud storage environments.

Understanding data exposure:

Gain visibility into where sensitive data resides and how it is accessed, helping organizations assess risk and prioritize protection efforts.

Key and Secrets Discovery:

Automatically locate and detect cloud-based keys, secrets, and certificates.

Streamlining compliance:

Identify and classify regulated data to support audit readiness and compliance requirements.

Analyze **Challenges**

Centralized Audit Logs:

Gain unified visibility into data access and policy activity, with support for SIEM-driven analysis.

Encryption activity monitoring:

Analyze encryption usage to detect anomalies and identify potential threats.

Improved data visibility:

Discover and assess sensitive data across environments with actionable insights.

Simplified protection planning:

Apply risk-based insights to prioritize security controls and data protection strategies.

Protect **Challenges**

Protecting data at rest:

Secure sensitive data across on-premises, cloud, and hybrid environments using strong encryption.

Transparent encryption:

Protect data with minimal impact on applications and without requiring code changes.

Dynamic data protection:

Safeguard data throughout its lifecycle, whether at rest or in motion.

Tokenization and masking:

Replace sensitive data with tokens to reduce exposure and limit unauthorized access.

Centralized key management:

Manage encryption keys across multi-cloud environments with centralized control.

Secure hybrid and multi-cloud platforms:

Extend protection across cloud providers such as AWS, Azure, and Google Cloud.

22%

have little or no confidence in identifying where their data is stored.

2025 Data Threat Report, Financial Services Edition

Control **Challenges**

Integrate security into DevOps:

Embed security into development workflows to protect data without slowing innovation.

Protect data in development:

Safeguard sensitive data across development, testing, and deployment environments.

Improve operational efficiency:

Automate policy enforcement and streamline security operations across environments.

What is a **Data Security Platform?**

A data security platform is a comprehensive set of technologies designed to help organizations protect sensitive data across their entire environment. By integrating capabilities such as discover, analyzation, protection, and control, a data security platform enables organizations to manage data risk consistently across cloud, on-premises, and hybrid infrastructures.

Data security platforms unify multiple security functions into a single, coordinated framework. Instead of relying on disconnected point solutions, organizations can apply consistent policies, automate security processes, and gain visibility into how sensitive data is stored, accessed, and used across systems and applications.

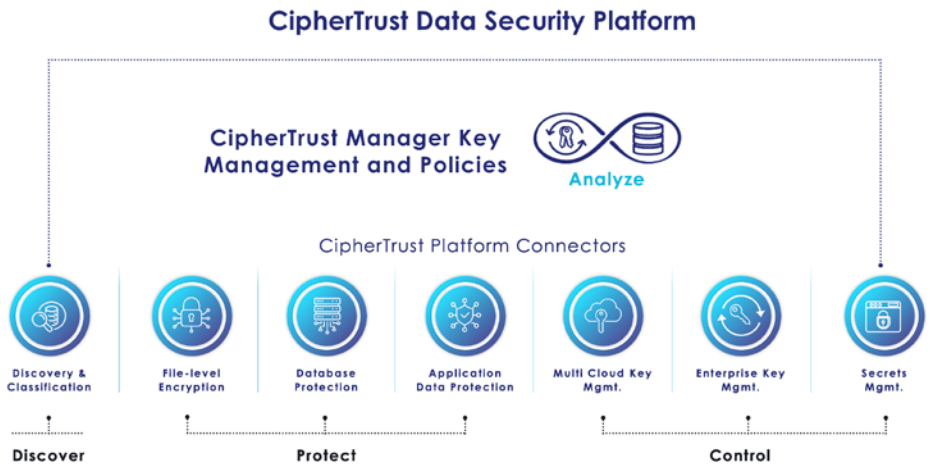
By providing an integrated approach to data protection, a data security platform helps organizations discover sensitive information, classify it appropriately, enforce protection policies, and continuously analyze activity around critical data assets—regardless of where that data resides.

What is the **CipherTrust Data Security Platform?**

Recognized as a Leader in the KuppingerCole 2025 Leadership Compass for Data Security Platforms and featured in Gartner's Market Guide to Data Security Platforms, the CipherTrust Data Security Platform delivers a comprehensive, integrated suite of data-centric security solutions designed to eliminate complexity, accelerate compliance, and secure cloud and on-premises environments.

CipherTrust unifies data discovery, classification, protection, analyzation, and centralized key and secrets management into a single, streamlined platform. This consolidation dramatically reduces the operational burden on security teams, enforces consistent compliance controls, and minimizes risk across your organization.

By offering a unified approach to data security, the CipherTrust Data Security Platform empowers organizations to seamlessly discover, classify, protect, and analyze their sensitive data—regardless of where it resides.



What is the **Data Security Fabric?**

The Data Security Fabric is a unified framework designed to help organizations protect sensitive data across complex, distributed environments. As data moves between cloud platforms, applications, data centers, and devices, the Data Security Fabric connects security controls, policies, and visibility into a cohesive architecture that enables organizations to protect data consistently wherever it resides.

By integrating key capabilities such as data discovery, classification, encryption, key management, and access controls, the Data Security Fabric helps organizations simplify data protection while maintaining strong governance and compliance. This integrated approach reduces operational complexity and enables security teams to apply consistent protections across hybrid and multi-cloud environments.

Through a connected, platform-driven approach to data security, the Data Security Fabric empowers organizations to discover, classify, protect, and monitor sensitive data across their entire digital ecosystem—ensuring data remains secure as it is created, shared, stored, and used.

What is **CipherTrust Data Security Posture Management?**

CipherTrust Data Security Posture Management (DSPM) provides a comprehensive, unified approach to data visibility and protection by precisely identifying the locations of your sensitive data—no matter where it resides. Whether your data is stored across multiple cloud environments, on-premises systems, or within an expanding array of SaaS applications, CipherTrust DSPM delivers deep insight and control to help you maintain a strong security posture and meet compliance requirements.

Built on years of proven industry expertise, CipherTrust DSPM goes beyond simple discovery. It continuously detects, classifies, and assesses data risks while applying advanced protection mechanisms to safeguard your most critical information. Through powerful monitoring and analytics, it enables organizations to track how sensitive data is accessed, shared, and utilized, reducing exposure to potential breaches or misuse. With CipherTrust DSPM, you gain the visibility, intelligence, and automation necessary to protect your most valuable asset—your data—across its entire lifecycle.

Data Discovery and Classification

Data Discovery and Classification provides enhanced security and streamlined compliance, enabling you to close compliance gaps and policy configurations which minimizes data risk. It is a single solution to improve efficiency and discover data, secrets, and classify data wherever it resides. Data Discovery and Classification improves operational efficiency, reduces impact of a breach, reduces costs of development, and avoids costs of tooling and storage.

Key Management

Key Management enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer friendly REST APIs. It provides centralized management of encryption keys and policies for its data protection connectors. CipherTrust Manager is the central management point for the CipherTrust Data Security Platform and is available in both virtual and physical formfactors that are FIPS 140-2 compliant up to level 3 for securely storing keys with an elevated highest root of trust.

Secrets Management

CipherTrust Secrets Management is a centralized solution for securely storing, accessing, and managing secrets such as API keys, passwords, certificates, and tokens. It helps eliminate hardcoded credentials, enforce access controls, and support DevOps and cloud-native environments. Integrated with the CDSP, it ensures strong security, auditability, and scalability across hybrid and multi-cloud infrastructures.

Transparent Encryption

Transparent Encryption delivers data at rest encryption, privileged user access controls and detailed data access audit logging. It protects data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers, in cloud and big data environments. The Live Data Transformation product is available for CipherTrust Transparent Encryption, which provides zero-downtime encryption and data rekeying. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

Tokenization

Tokenization helps reduce the cost and complexity of complying with data security mandates such as PCI DSS. Vaultless tokenization includes policy-based dynamic data masking, whereas vaulted tokenization has additional environment specific APIs. CDSP's suite of Tokenization products makes it easy to add tokenization to applications via RESTful APIs.

Data Masking

Data Masking simplifies compliance and enhances data security by obfuscating sensitive information while preserving its format. It supports both static and dynamic data masking, enabling secure access based on user roles. Integrated with CDSP, it works seamlessly alongside vaultless tokenization, offering flexible, policy-driven protection via RESTful APIs—ideal for reducing PCI DSS scope and mitigating data exposure risks.

Database Protection

Database Protection integrates data encryption for sensitive fields in databases with secure, centralized key management without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, and IBM DB2 and Teradata databases.

Application Data Protection

Application Data Protection delivers crypto functions for key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. CipherTrust Application Data Protection enables accelerated development of customized data security solutions, while removing the complexity of key management from the developer's responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations.

File Activity Monitoring

Unstructured file security is essential for preventing unauthorized individuals or entities from accessing sensitive or confidential information, such as personal data, financial details, trade secrets, intellectual property, and other critical information. File Activity Monitoring (FAM) provides continuous oversight of access to unstructured and encrypted data stored in various By utilizing advanced machine learning technology, organizations can safeguard enterprise data in file shares and SaaS applications. The AI Data Security Assistant is a generative AI-powered chatbot integrated into FAM that dramatically reduces manual workload and enhances response speed—turning complex data trails into clear, actionable insights in seconds. This technology enables users to identify access rights, review file permissions, quickly gain insights into sensitive files, and enhance incident response and forensic investigations through analytics and alerts related to abnormal activity.

Data Activity Monitoring

Thales provides Data Activity Monitoring (DAM) for all data assets across on-premises data repositories, hybrid, and multi-cloud environments. It provides real-time monitoring and auditing of all data activity, including actions taken by both application and privileged users. This visibility helps organizations in understanding who is accessing data, and when, as well as what actions are being performed, thereby preventing potential security threats and blocking privileged user accounts with extensive access to sensitive data and business critical systems.

Data Risk Analytics

Thales risk analytic capabilities help identify security threats and malicious activities across data assets and cloud services. It enables you to detect unauthorized access, suspicious data transfers, and abnormal behavior, assess their impact, and provide strategies to mitigate them. Data Risk Analytic policy-based detection prioritizes alerts and blocks users and applications from further access to data. The system filters out low-risk events, allowing security teams to focus on genuine threats.

Data Risk Intelligence

Thales enables you to prioritize data risks based on severity and likelihood by using Data Risk Intelligence. It provides risk scoring and actionable insights by analyzing user permissions, data vulnerabilities, encryption standards, and suspicious activities. Combining incident modeling and risk prioritization, executives can understand their security posture and manage security threats effectively. ML/AI-analytics are used to fuse together risk indicators from vulnerability scanning, entitlement assessments, and configuration management so that business leaders receive high-accuracy risk profiles to enforce security policies and remediate security gaps.

Data Security Posture Management

As data proliferates across hybrid multi-cloud environments, organizations must manage their data security dynamically to protect sensitive information from emerging vulnerabilities. CipherTrust Data Security Posture Management (DSPM) automates data discovery, classification, protection, and risk assessment, ensuring adherence to data protection best practices and providing visibility into sensitive data locations and access controls. DSPM quickly identifies vulnerabilities, generates alerts, and offers remediation guidance to address data security risks. By integrating with other security systems and facilitating compliance reporting, DSPM helps organizations maintain a strong data security posture and meet regulatory requirements.

About **Thales**

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

The Companies you trust rely on Thales

- 58% of the Fortune Global 500
- More than 30,000 customers
- Thales solutions deployed in 148 countries
- More than 6700 global resellers, system integrators, distributors, managed service provider and technology companies in Thales Accelerate Partner Network

THALES

Building a future we can all trust

Contact us

For contact information,please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com