



Thales Data Security Portfolio

Trust your data. Move at the speed of opportunity. A modern portfolio for discovering, analyzing, protecting and controlling sensitive data, anywhere.

Security strategies built to meet today's AI-driven, post-quantum and data-intensive challenges.

Your organization depends on trusted data, secure applications and resilient digital operations. But the landscape has fundamentally changed.

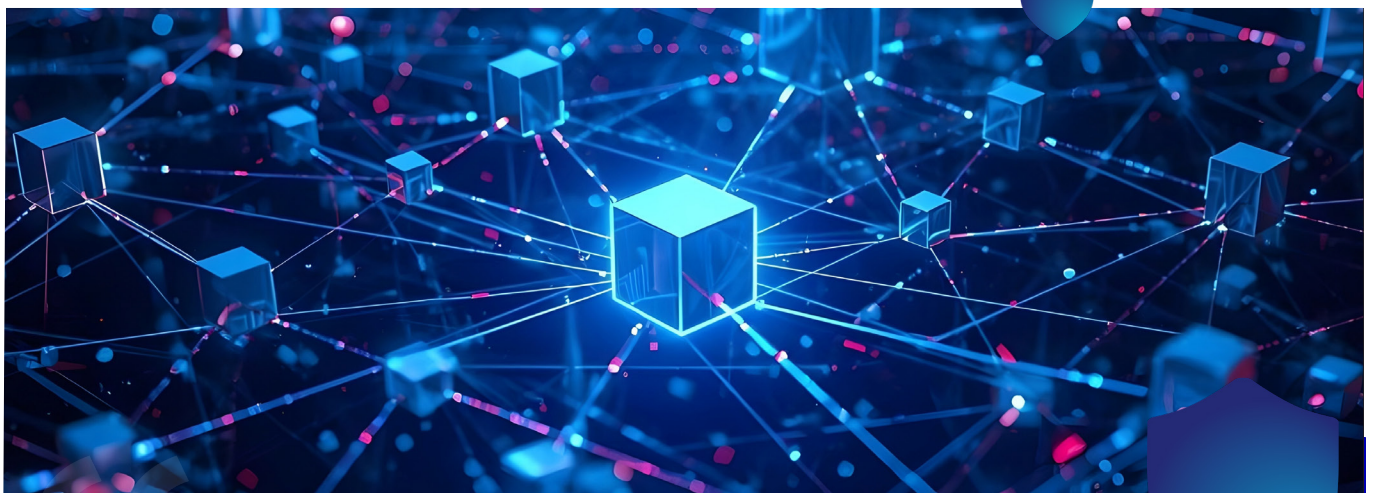
AI is driving unprecedented scale and speed - creating, accessing and exposing data in ways that, without a strong security foundation, are increasingly difficult to control. Growing pressure around sovereignty, privacy and compliance is tightening requirements on where data lives, how it moves and who can access it. Quantum computing is fundamentally reshaping how organizations approach long-term cryptographic security, increasing the need for crypto agility, and a clear mitigation path as standards and requirements evolve.

At the same time, the role of the CISO has evolved. As strategic leaders responsible for managing risk at the highest level, today's CISOs must balance

security with growth — reducing risk while enabling transformation and helping the business move faster, with confidence. Yet many data security approaches were not built for this reality, stopping at visibility and leaving organizations to close the gap between insight and action.

Thales helps organizations address these challenges by bringing together data intelligence, protection and cryptographic security in one connected portfolio — turning visibility into action and helping teams protect sensitive data wherever it lives, moves or is accessed.

Thales gives organizations the visibility, protection and control they need to secure sensitive data and the cryptographic foundations that protect it across on-premises, hybrid and multi-cloud environments — while enabling trusted, confident growth.



Only **34%** of organizations have complete knowledge of where their data is stored.

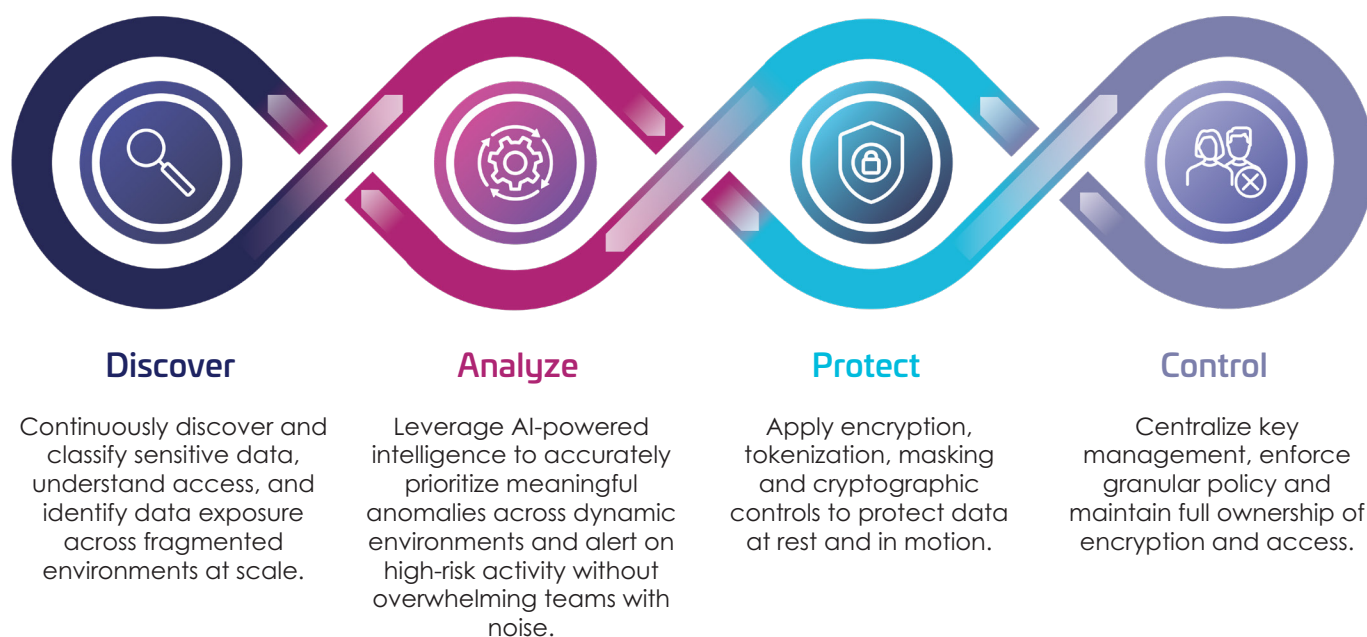
— 2026 Thales Data Threat Report

A complete portfolio for protecting data at rest, in motion and in the cloud.

Thales Cybersecurity delivers a holistic approach to securing critical data, applications and identities at scale, wherever they reside. Built for the demands of the AI era, the portfolio brings together a wide range of capabilities to enhance visibility, reduce risk, and enable more automated, intelligent approaches to data protection. By combining data discovery, protection, posture management, monitoring, certified cryptographic infrastructure and cloud-delivered services, Thales provides a coordinated, end-to-end approach to securing sensitive data across increasingly complex environments.

Rather than relying on fragmented point solutions, organizations can leverage a broad, award-winning portfolio designed to work as a connected system — enabling them to scale security, simplify operations and maintain control across distributed, hybrid and multi-cloud environments. This integrated approach supports continuous protection, helping organizations adapt to evolving threats while enabling secure innovation and operational resilience.

This approach can be understood through four core capabilities:



Our Data Security Portfolio

CipherTrust DSPM - Continuous data security posture management

What it does

CipherTrust Data Security Posture Management helps organizations understand where sensitive data resides, how it is exposed, and what actions should be prioritized to reduce risk. By providing continuous visibility across cloud, on-premises, hybrid, multi-cloud and SaaS environments, DSPM helps security teams identify sensitive and regulated data, assess exposure and connect insight directly to remediation.

Key capabilities

Discover and classify data

Automatically identify and classify sensitive data across structured and unstructured sources, building a comprehensive view of what data exists, where it resides and how it may be exposed.

Assess exposure and risk

Deliver continuous, risk-aware visibility into data environments, helping teams understand exposure, monitor posture and move from reactive investigation to proactive data security management.

Prioritize remediation

Focus attention on the exposures that matter most through risk-based prioritization. DSPM helps organizations direct remediation efforts where risk is highest based on data sensitivity and exposure.

Reduce risk through action

Support remediation through guided workflows and policy-based recommendations, helping organizations reduce exposure by strengthening policies, enforcing access controls and applying data protection measures.

Strengthen governance and compliance

Provide centralized visibility, risk scoring and actionable insights that help improve governance, support compliance initiatives and strengthen security posture over time.

Outcome By connecting discovery, analysis and remediation into a continuous process, CipherTrust DSPM helps organizations reduce risk, improve visibility and maintain control of sensitive data across increasingly complex environments.



CipherTrust Data Security Platform (CDSP) - Unified data protection and control

CipherTrust Data Security Platform (CDSP) helps organizations discover, analyze, protect and control sensitive data across complex enterprise environments. By bringing together data discovery and classification, encryption, tokenization, masking, key management and secrets management into a single platform, CDSP reduces complexity and helps organizations apply consistent security policies across their data ecosystem.

Key capabilities

Discover and classify sensitive data

Gain visibility into sensitive data across cloud, on-premises and hybrid environments, helping organizations identify critical information and understand exposure risks.

Protect data wherever it resides

Safeguard sensitive information through encryption, tokenization and masking, reducing exposure and helping organizations meet regulatory and compliance requirements.

Centralize policy and key management

Manage encryption keys, policies and secrets from a single control point, improving consistency, governance and operational efficiency across environments.

Simplify compliance and operations

Consolidate multiple data security functions into one coordinated platform, reducing complexity while supporting security, governance and compliance objectives.

Deploy with flexibility

Implement CDSP on-premises or as a cloud-delivered service, enabling organizations to align data protection with their infrastructure, operating model and scalability requirements.

Industry recognition

Recognition by industry analysts, including the KuppingerCole 2025 Leadership Compass for Data Security Platforms and Gartner's Market Guide for Data Security Platforms, reinforces CDSP's position as a comprehensive, data-centric security solution.

Outcome

By connecting discovery, analyzation, protection and control within a single platform, CDSP helps organizations strengthen security, maintain compliance and reduce operational complexity while protecting sensitive data across the full data lifecycle.



Data Security Fabric (DSF) - Visibility, activity monitoring and risk intelligence

What it does

Thales Data Security Fabric (DSF) provides a comprehensive framework for visibility, activity monitoring and risk intelligence across distributed data environments. As sensitive data moves across cloud, on-premises, hybrid and multi-cloud infrastructures, DSF helps organizations understand how data is accessed, used and exposed. By bringing together security controls, monitoring and intelligence into a centralized approach, DSF helps organizations improve visibility, strengthen governance and protect sensitive data consistently across complex environments.

Key capabilities

Gain visibility across distributed environments

Understand where sensitive data resides, how it moves and how it is being accessed across applications, users, repositories and cloud services — enabling a more complete view of data exposure and risk.

Monitor activity and identify threats

Provide continuous insight into data activity and exposure, helping security teams detect threats, identify anomalies and prioritize risks before they become larger security issues.

Unify security and governance

Bring together encryption, key management, access controls and data protection policies within a centralized framework to promote consistent security and compliance across the enterprise.

Support compliance and zero-trust strategies

Enable advanced access management, centralized monitoring and policy enforcement across cloud, hybrid and on-premises environments, helping organizations meet regulatory requirements and strengthen zero-trust initiatives.

Turn insight into action

Correlate monitoring, access insights and risk analytics to identify exposure risks earlier, prioritize remediation efforts and support more informed security decision-making.

Outcome As a core component of the Thales Data Security portfolio, DSF strengthens the visibility and intelligence layer for enterprise data security. DSF provides organizations with continuous visibility into where sensitive data resides, who has access to it, and how it is being used. DSF helps organizations reduce risk, tighten governance, and accelerate compliance efforts across cloud, on-premises, and AI environments.



Hardware Security Modules (HSMs) - The foundation for digital trust

What it does

Thales Hardware Security Modules (HSMs) provide a hardened, tamper-resistant foundation for generating, storing and managing cryptographic keys. Acting as a hardware root of trust for critical cryptographic operations, Luna and payShield HSMs help organizations protect the keys that secure data, applications, identities and digital transactions. For regulated, high-assurance and mission-critical environments, HSMs provide the dedicated protection needed to maintain control, support compliance and reduce exposure of sensitive assets for long-term cryptographic resilience.

Key capabilities

Secure cryptographic keys and operations

Generate, store and manage cryptographic keys securely within a trusted environment, helping safeguard encryption, authentication and digital signing processes.

Support a wide range of security use cases

Enable critical capabilities including PKI, code and document signing, application protection, database encryption, identity protection and transaction security to help enable regulatory compliance.

Maintain control and sovereignty

Provide strong separation of duties and secure key ownership, helping organizations maintain control over cryptographic assets while supporting governance and compliance requirements.

Scale across modern environments

Protect cryptographic operations wherever applications and workloads run, with the flexibility, crypto agility and scalability across cloud, hybrid and on-premises environments.

Simplify management and operations

Leverage centralized reporting, monitoring and resource management, helping reduce operational complexity while maintaining high-assurance security.

Prepare for a post-quantum future

Build long-term cryptographic resilience with crypto-agile infrastructure designed to support evolving algorithms and enable the transition to post-quantum cryptography (PQC).

Outcome

By providing a trusted hardware foundation of trust for critical applications, data and identities, Thales HSMs help organizations strengthen security, maintain compliance and protect digital trust today while building the crypto-agility for tomorrow's cryptographic challenges.



High Speed Encryptors (HSE) - Network encryption for data in motion

What it does

Thales High Speed Encryptors (HSE) protect sensitive data as it moves across enterprise, cloud, metro, WAN, OT, industrial and tactical network environments. As organizations increasingly rely on distributed infrastructure, HSE delivers certified encryption for data in transit, helping secure communications between sites, data centers, cloud environments and critical operational systems without compromising performance.

Key capabilities

Secure data in motion at scale

Protect sensitive communications, real-time data, voice, video and metadata as information moves across enterprise, cloud and operational networks.

Deliver high-performance encryption

Provide wire-speed encryption with microsecond latency, enabling organizations to secure network traffic without introducing performance bottlenecks or operational disruption.

Support diverse deployment environments

Protect data across on-premises, cloud, hybrid and multi-cloud infrastructures, with solutions designed for a wide range of deployment scenarios including data centers, metro networks, branch locations and operational technology environments.

Enable crypto agility and future readiness

Support evolving cryptographic requirements through crypto-agile, quantum-safe capabilities that help organizations maintain long-term security resilience.

Prepare for quantum-era threats

Help mitigate emerging risks such as “harvest now, decrypt later” attacks through advanced support for quantum-safe security, including Transport Independent Mode and Quantum Key Distribution (QKD) integrations.

Outcome By combining high-assurance security with wire-speed performance, Thales HSE enables organizations to protect sensitive data wherever it travels — maintaining trust, performance and operational continuity across increasingly distributed and interconnected environments.



Data Protection on Demand (DPoD) – A cloud-based marketplace

What it does

Thales Data Protection on Demand (DPoD) gives organizations on-demand access to scalable data security services through a cloud-based marketplace, including free trials. Rather than investing in, managing and maintaining dedicated infrastructure, organizations can consume selected Thales data security capabilities as services. This simplifies deployment, reduces operational complexity, and enables faster access to enterprise-grade security capabilities.

Key capabilities

Access security services on demand

Rapidly deploy data security capabilities through a simple online marketplace, enabling organizations to consume services as needed without infrastructure overhead.

Simplify deployment and management

Provision services, add users and devices, and access reporting through a centralized interface designed to streamline administration and reduce operational effort.

Leverage trusted Thales capabilities

Access a range of Thales solutions, including CipherTrust Key Management, DSPM, Luna Cloud HSM and payShield Cloud HSM services, through a flexible, service-based consumption model.

Scale security with business demand

Deploy and expand services quickly as requirements evolve, supporting cloud, hybrid and multi-cloud environments without the burden of additional hardware investments.

Improve operational efficiency

Benefit from rapid deployment, real-time reporting and visibility, multi-tier management, and integration with existing applications, infrastructure and security workflows.

Adopt cloud-delivered security with confidence

Support security and compliance requirements through SLA-backed availability and standards such as ISO 27001, helping organizations accelerate adoption while maintaining trust and control.

Outcome As the flexible delivery layer within the Thales Data Security portfolio, DPoD enables organizations to consume data protection capabilities as services — accelerating deployment, simplifying management and supporting security transformation without slowing innovation.



From insight to protection to control - one connected approach to data security

The Thales Data Security portfolio is designed to deliver data protection as a unified capability — enabling organizations to move from fragmented security to a connected, lifecycle-based approach.

This capability is delivered through a set of integrated components that work together to provide visibility, protection and control across the data lifecycle — from understanding where sensitive data resides, to safeguarding it, to ensuring it is used securely and appropriately.

DSPM, CDSP, and DSF combine to connect insight to action — helping organizations identify risk, prioritize remediation and maintain control across increasingly complex environments. Thales Luna and payShield HSMs serve as hardware roots of trust, protecting the critical cryptographic keys and operations that secure applications, identities and digital transactions. Thales High Speed Encryptors (HSEs) deliver certified network encryption to protect sensitive data in motion. Through DPoD, organizations gain cloud-delivered access to data security services, enabling them to deploy and scale security with speed and flexibility.

Together, these capabilities enable security teams to move faster, shifting from reactive risk management to proactive control.



Security that keeps pace without slowing your business down

Take control of your data security strategy and move forward with confidence.

Thales combines deep expertise in hardware, software and cloud-delivered security to help organizations protect sensitive data with greater confidence, control and flexibility.

From global enterprises to governments and highly regulated industries, organizations rely on Thales to secure critical data, maintain sovereignty and support transformation across AI, cloud and post-quantum environments.

The Thales advantage

Organizations choose Thales because we bring together a broad, award-winning portfolio trusted by organizations worldwide - delivering capabilities others cannot in one integrated, end-to-end approach:



A unified platform strategy that connects visibility, protection and control



A broad, proven portfolio spanning data discovery, protection, monitoring, encryption and key management



Deep expertise across hardware, software and cloud, delivering security from root of trust infrastructure through to data intelligence



Full ownership and control of encryption keys, supporting sovereignty and compliance requirements



A connected view of risk, linking insight directly to action



Recognized by leading industry analysts, with strong customer validation across platforms such as Gartner Peer Insights

While many vendors address parts of the problem, only Thales brings them together into one coordinated data security strategy.

Protect what matters most and move at the speed of opportunity.

Visit - cpl.thalesgroup.com/contact-us

Contact us

For contact information visit:
cpl.thalesgroup.com/contact-us

THALES

CYBERSECURITY

