Solution Brief

THALES
Building a future we can all trust

CYBERSECURITY

Thales Data Encryption + Continuous Monitoring

How cryptography and observability boost data protection

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Thales CipherTrust Data Security Platform (CDSP) and **Data Security Fabric (DSF)** create a powerful defense by combining advanced data protection with real-time observability and threat detection across your data infrastructure. Organizations can track access to encrypted, unencrypted as well as hidden databases addressing the reality that nearly two-thirds of data breaches involve the human element, while ensuring regulatory compliance.

Challenge: The Critical Security Gap

While there are many ways to protect sensitive data in databases, IT requirements for security, performance, and availability can sometimes clash. Finding the right balance is crucial for organizations to protect and manage critical data across a complex mix of environments including traditional databases, data warehouses, big data platforms, and multi-cloud environments.

Organizations cannot effectively demonstrate comprehensive database protection with encryption or monitoring alone. Compliance frameworks like HIPAA, PCI DSS, SOX, and GDPR require both robust data protection and detailed access monitoring, yet traditional approaches create dangerous gaps.

Many companies have opted to start their data security journey by deploying encryption solutions as a first step. While other organizations may have opted to take another approach by implementing traditional Database Activity Monitoring (DAM) tools for monitoring access to databases and detecting unauthorized or suspicious activity.

However, encryption without monitoring leaves organizations blind to insider threats and policy violations by authorized users who have legitimate decrypt permissions.

Monitoring without encryption exposes sensitive data to unauthorized access if security controls are bypassed.

Additionally, point solutions increase operational complexity, vendor sprawl, and integration overhead while failing to address the fundamental challenges when it comes to performance at scale. All to say, these tools carry hidden costs and fail to meet consistent compliance requirements across all data assets.

Why Organizations Are Acting Now

- Multi-Environment Risk: 40% of breaches involve data across multiple environments, costing $5.17M on average with 283-day detection times
- Shadow Data Problem: 35% of breaches involve unmanaged data, costing 16% more than average incidents
- Human Factor: 60% of data breaches involve the human element, including social engineering, human errors, compromised credentials, and insider threats
- Insider Threat Reality: Authorized users with legitimate database access can misuse their privileges or have their credentials compromised, creating security blind spots
- Digital Transformation: Cloud migration creates windows for complete security strategies

Solution: Unified Database Security

Database breaches expose organizations' most critical assets—customer records, financial data, and intellectual property that drive business value. At the core of all threats is the "data" and sensitive data is accessed by users, systems, and AI from business-critical applications, databases and cloud repositories that potentially could be compromised if the proper policies and controls are not in place.

Why add Database Encryption?

For organizations currently deploying legacy Database Activity Monitoring (DAM), adding CipherTrust Database Protection encryption controls complement existing monitoring capabilities while closing regulatory gaps that require both sensitive data protection, monitoring, and detection. You can leverage current investments while strengthening compliance coverage.

CipherTrust Database Protection (CDP) protects structured data in performance-intensive environments while preserving format and usability for joins and analytics. CDP high-performance, column-level database encryption ensures that every database write and read happens at almost the speed of an unprotected database.

CDP strength is the ability to rotate encryption keys without application downtime or application rewrite. Data protection best practices require the alteration of the encryption key used to protect data over time. Key rotation or data re-key is commonly executed every year or two for all encrypted data. CDP provides AES encryption with live key rotation capabilities to eliminate rotation outages and eliminate the manual effort to rotate keys.

CipherTrust Transparent Encryption (CTE) continuously enforces file-level encryption of unstructured data that protects against unauthorized access by users and processes. CTE creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.

The FIPS 140-3 L1 certified CipherTrust Transparent Encryption agent resides at the operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. This protects data wherever it resides, on-premises, across multiple clouds and within big data, and container environments.

CipherTrust Database Protection Benefits

Meet sensitive data mandates and regulations. Regulations like PCI DSS, HIPAA, GDPR, CCPA, and others explicitly require encryption of sensitive data at rest and/or in transit. Encryption is a concrete technical control that helps ensure data confidentiality.

Reduce risk of data exposure. If a breach occurs, encrypted data is unreadable without keys, mitigating potential fines and damage.

Enhance data integrity. Compliance auditors view encryption as a strong proactive protective measure that enables the protection of sensitive information, enhances and ensures compliance with risk management regulations.

Limit the scope of compliance audits. By encrypting data, organizations can reduce the number of systems and environments subject to stringent compliance controls.

Why add Visibility and Control?

For organizations with existing database encryption, adding Data Security Fabric (DSF), a comprehensive observability platform, provides real-time data activity monitoring, behavioral analytics and anomaly detection, and policy enforcement across on-premises, hybrid and multi-cloud environments.

While existing data protection controls regulate who can access sensitive data, DSF reveals how that data is actually used —including by authorized users and applications with legitimate decrypt permissions.

Efficacy of data protection hinges on several factors, including the strength of encryption algorithms, key management practices, and adherence to industry standards and regulatory requirements.

With DSF, auditing encryption practices allows organizations to assess the adequacy of their encryption implementations, identify vulnerabilities, and address potential security gaps.

Security administrators gain complete visibility into encrypted data usage. The system observes how authorized users are interacting with protected data and quickly detects misuse even when access credentials are legitimate.

Staff can immediately respond to policy violations and demonstrate compliance readiness across all regulatory frameworks via audit trails and reporting.

Data Security Fabric Benefits

Observe all data access. With Data Security Fabric (DSF), gain visibility of all your data stores, regardless of their location, in a central and unified dashboard displaying system events, alerts, violations, blocked sources, warnings, database auditing, file server auditing, archiving information, and more. Continuous monitoring captures and analyzes all data store activity from both application and privileged user accounts, providing detailed audit trails that show who access what data, when, and what was done to the data.

Enhance audit oversight. Automated compliance reporting with detailed access trails and encryption status unifies auditing across diverse on-premises platforms providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS) — including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill audit requests.

Scale compliance, everywhere. Simplify regulatory compliance activities with universal policy monitoring, enforcement workflows, and reports for regulations such as GDPR, PCI, NYDFS, HIPAA, and CPRA. Consolidate information across all audited data assets – fully indexed and efficiently stored – with live-data access to years' worth of information, significantly reducing time spent on incident investigations and audit inquiries.

Database Protection & Data Visibility and Control

Organizations implementing database protection and monitoring from a single vendor achieve superior security outcomes while reducing operational complexity and demonstrating comprehensive regulatory compliance.

Database protection with data visibility and control capabilities brings together a synergistic approach by combining strong encryption and key management with granular access monitoring and behavioral analytics — delivering end-to-end data security and governance. This can result in stronger protection, better compliance, and operational efficiency.

Close the Security Gaps: Unmatched Coverage

CipherTrust Data Security Platform (CDSP) delivers robust data discovery, control, and protection functions through database encryption, centralized key management, tokenization, and data masking. Together, these functions close security gaps and simplify operations.

DSF (Data Security Fabric) provides comprehensive data monitoring capabilities including real-time data activity monitoring, threat detection, user behavior analytics, and compliance reporting. This creates continuous visibility into database access patterns and policy violations.

CipherTrust Data Security Platform (CDSP)	Data Security Fabric (DSF)
• **Protecting data at rest:** Protect data while it is stored on-premises, in the cloud, or in backups.	• **Comprehensive data activity monitoring:** Gain complete visibility of all data stores and data types.
• **Transparent encryption:** Encrypt data without requiring changes to applications or workflows.	• **Real-time analytics across sensitive data:** Detect and report non-compliant, risky, or malicious data access across all data repositories.
• **Centralized key management:** Ensure encryption keys are securely generated, stored, and managed.	• **Automated data classification and discovery:** Discover ungoverned data, classify all data, and assess vulnerabilities.
• **Tokenization:** Replace sensitive data with non-sensitive tokens, making it difficult for unauthorized individuals to access or misuse the data.	• **Enterprise-scale risk prioritization:** Get a unified view of essential data risk metrics to understand your risk profile and mitigate gaps.
• **Dynamic data masking:** Mask or redact in real time sensitive data, preventing unauthorized access even when data is in use.	• **AI/ML-behavioral anomaly and threat detection:** Identify abnormal user behavior and translate complex technical events into plain language for IT operations teams and security staff members to immediately act on.

CipherTrust Data Security Platform Benefits

Vendor consolidation savings. Reduce procurement, contract management, and training overhead while enabling accelerated paths to data protection that leverage existing infrastructure and expertise.

Risk reduction. Lower potential breach costs through layered defense strategies that address both external attacks and insider threats, creating measurable ROI through avoided incident costs and operational efficiency gains.

Universal compliance coverage. Every major regulation requires both data protection and access monitoring, creating natural synergy between these capabilities:

HIPAA
PHI encryption + access audit trails

PCI DSS
Cardholder data protection + user access logging

SOX, GLBA, DORA
Financial data controls + access monitoring

GDPR, CCPA
Personal data encryption + processing records

FISMA
Federal security standards + audit capabilities

NERC CIP, NIS2
Critical infrastructure data protection + access tracking

The Thales Advantage: Unmatched Innovation and Expertise

Preventive + Detective Controls: Encryption stops unauthorized access while monitoring detects misuse

Audit Readiness: Automated compliance reporting with detailed access trails and encryption status

Operational Efficiency: Unified approach reduces vendor sprawl and integration overhead

Rapid Response: Close security gaps in minutes through centralized policy management

Proven Business Impact

Organizations can deploy comprehensive database security from day one through a single vendor strategy reducing operational complexity while delivering data-layer security with consistent policies and streamlined operations.

Database encryption provides compelling ROI, with Forrester's Total Economic Impact study documenting 221% return on investment over three years alongside $9.1 million in quantified benefits. Implementation achieves less than six-month payback periods while reducing key management effort by 70% through automation and centralization.

Industry Recognition

KuppingerCole names Thales "Overall Leader" in Data Security Platforms for 2025, while Forrester positions Thales as a "Strong Performer" with the second-highest Strategy score among evaluated vendors. Gartner Peer Insights rates Imperva 4.5 stars across 190+ customer reviews, and multiple FIPS 140-2 Level 3 certifications validate enterprise security architecture.

Engage our Security Specialists

Ready to close your database security gaps? Contact your Thales representative today to discover how CipherTrust Database Encryption solutions and Data Security Fabric platform work together to deliver comprehensive data protection, accelerated compliance, and measurable business value.

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.