解决方案简介

THALES
Building a future we can all trust

CYBERSECURITY

Thales Data Encryption + Continuous Monitoring

密码学与可观测性如何提升数据保护

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Thales CipherTrust 数据安全平台（CDSP）与数据安全架构（DSF）通过将先进数据保护与跨数据基础架构的实时可观测性及威胁检测相结合，构建强大的防御体系。组织可追踪对加密、未加密及隐藏数据库的访问，应对近三分之二的数据泄露涉及人为因素这一现实，同时确保法规合规。

挑战：关键安全缺口

虽然保护数据库中敏感数据的方法多种多样，但安全性、性能和可用性的 IT 要求有时会相互冲突。在包括传统数据库、数据仓库、大数据平台和多云环境在内的复杂混合环境中，找到正确的平衡点对于保护和管理关键数据至关重要。

组织仅靠加密或监控无法有效展示全面的数据库保护。HIPAA、PCI DSS、SOX 和 GDPR 等合规框架既要求强大的数据保护，又要求详细的访问监控，然而传统方法却造成了危险的缺口。

许多企业选择以部署加密解决方案作为数据安全之旅的第一步。而其他组织则可能选择另一种方式，通过实施传统的数据库活动监控（DAM）工具来监控数据库访问并检测未授权或可疑活动。

然而，没有监控的加密使组织对内部威胁和具有合法解密权限的授权用户的策略违规行为视而不见。

没有加密的监控在安全控制被绕过时，会使敏感数据面临未授权访问的风险。

此外，单点解决方案增加了运营复杂性、供应商蔓延和集成开销，同时未能解决大规模性能方面的根本挑战。总而言之，这些工具存在隐性成本，且无法满足所有数据资产的一致合规要求。

组织为何立即采取行动

- 多环境风险：40% 的泄露事件涉及跨多个环境的数据，平均损失 517 万美元，检测时间长达 283 天
- 影子数据问题：35% 的泄露事件涉及未受管理的数据，损失比平均事件高出 16%
- 人为因素：60% 的数据泄露涉及人为因素，包括社会工程、人为错误、凭证泄露和内部威胁
- 内部威胁现实：具有合法数据库访问权限的授权用户可能滥用其权限或遭受凭证泄露，造成安全盲点
- 数字化转型：云端迁移为完整安全策略的建立创造了契机

解决方案：统一数据库安全

数据库泄露会暴露组织最关键的资产——驱动业务价值的客户记录、财务数据和知识产权。所有威胁的核心是"数据"，敏感数据由用户、系统和 AI 从业务关键应用程序、数据库和云端存储库中访问，若未建立适当的策略和控制措施，这些数据可能面临泄露风险。

为何要新增数据库加密？

对于目前部署传统数据库活动监控 （DAM） 的组织而言，新增 CipherTrust Database Protection 加密控制可补充现有监控能力，同时弥补需要敏感数据保护、监控和检测的监管缺口。您可以充分利用现有投资，同时加强合规覆盖范围。

CipherTrust Database Protection（CDP）在高性能环境中保护结构化数据，同时保留用于关联和分析的格式与可用性。CDP 高性能列级数据库加密确保每次数据库写入和读取几乎以未受保护数据库的速度进行。

CDP 的优势在于能够在不造成应用程序停机或重写的情况下轮换加密密钥。数据保护最佳实践要求定期更换用于保护数据的加密密钥。密钥轮换或数据重新加密通常每一至两年对所有加密数据执行一次。CDP 提供具备实时密钥轮换功能的 AES 加密，以消除轮换中断并免除手动轮换密钥的工作。

CipherTrust 透明加密（CTE）持续对非结构化数据执行文件级加密，防止用户和进程的未授权访问。CTE 在无需变更应用程序、基础架构、系统管理任务或业务流程的情况下，为所有活动建立详细的数据访问审计日志。

通过 FIPS 140-3 L1 认证的 CipherTrust 透明加密代理常驻于操作系统文件系统或设备层，加密和解密对其上运行的所有应用程序透明。无论数据位于何处——本地、跨多个云端还是在大数据和容器环境中——均可受到保护。

CipherTrust Database Protection 的优势

满足敏感数据规定和法规要求。PCI DSS、HIPAA、GDPR、CCPA 等法规明确要求对静态和/或传输中的敏感数据进行加密。加密是有助于确保数据保密性的具体技术控制措施。

降低数据暴露风险。若发生泄露，没有密钥的加密数据无法读取，可减轻潜在罚款和损失。

增强数据完整性。合规审计人员将加密视为强大的主动保护措施，能够保护敏感信息，增强并确保符合风险管理法规。

限制合规审计范围。通过加密数据，组织可以减少受严格合规控制约束的系统和环境数量。

为何要新增可见性与控制？

对于已部署数据库加密的组织，新增数据安全架构（DSF）这一全面的可观测性平台，可提供跨本地、混合和多云环境的实时数据活动监控、行为分析与异常检测，以及策略执行。

虽然现有的数据保护控制措施规范了谁可以访问敏感数据，但 DSF 揭示了数据的实际使用方式——包括具有合法解密权限的授权用户和应用程序如何使用数据。

数据保护的有效性取决于多个因素，包括加密算法的强度、密钥管理实践以及对行业标准和法规要求的遵守。

通过 DSF 审计加密实践，组织可以评估其加密实施的充分性、识别漏洞并解决潜在的安全缺口。

安全管理员可获得对加密数据使用情况的完整可见性。系统观察授权用户如何与受保护数据交互，即使访问凭证合法，也能快速检测滥用行为。

工作人员可立即响应策略违规行为，并通过审计追踪和报告在所有监管框架中展示合规准备状态。

数据安全架构的优势

观察所有数据访问。通过数据安全架构（DSF），在显示系统事件、告警、违规、被封锁来源、警告、数据库审计、文件服务器审计、归档信息等的集中统一仪表板中，获得对所有数据存储的可见性，无论其位置如何。持续监控捕获并分析来自应用程序和特权用户账户的所有数据存储活动，提供详细的审计追踪，显示谁在何时访问了哪些数据以及对数据进行了哪些操作。

增强审计监督。具有详细访问追踪和加密状态的自动化合规报告，统一了跨多个本地平台的审计，为关系型数据库、NoSQL 数据库、大型机、大数据平台和数据仓库提供监督。还支持托管在 Microsoft Azure 和 Amazon Web Services（AWS）上的数据库——包括 Azure SQL 和 Amazon 关系型数据库服务（RDS）等 PaaS 产品。详细的数据活动自动捕获，使审计请求更易于履行。

随处扩展合规。通过针对 GDPR、PCI、NYDFS、HIPAA 和 CPRA 等法规的通用策略监控、执行工作流程和报告，简化法规合规活动。整合所有受审计数据资产的信息——完全索引并高效存储——通过实时数据访问多年的信息，

数据库保护与数据可见性及控制

从单一供应商实施数据库保护和监控的组织，在降低运营复杂性并展示全面法规合规的同时，实现了卓越的安全成果。

具备数据可见性和控制能力的数据库保护，通过将强大的加密和密钥管理与精细的访问监控和行为分析相结合，采用协同方法——提供端到端数据安全和治理。这可带来更强的保护、更好的合规性和运营效率。

弥补安全缺口：无与伦比的覆盖范围

CipherTrust 数据安全平台（CDSP）通过数据库加密、集中式密钥管理、令牌化和数据脱敏提供强大的数据发现、控制和保护功能。这些功能共同弥补安全缺口并简化运营。

数据安全架构（DSF）提供全面的数据监控能力，包括实时数据活动监控、威胁检测、用户行为分析和合规报告。这为数据库访问模式和策略违规行为创造了持续可见性。

CipherTrust Data Security Platform (CDSP)	Data Security Fabric (DSF)
• 静态数据保护：保护存储在本地、云端或备份中的数据。	• 全面的数据活动监控：获得对所有数据存储和数据类型的完整可见性。
• 透明加密：在不需要变更应用程序或工作流程的情况下加密数据。	• 敏感数据实时分析：检测并报告所有数据存储库中的不合规、高风险或恶意数据访问。
• 集中式密钥管理：确保加密密钥安全生成、存储和管理。	• 自动化数据分类和发现：发现未受治理的数据，对所有数据进行分类，并评估漏洞。
• 令牌化：用非敏感令牌替换敏感数据，使未授权人员难以访问或滥用数据	• 企业级风险优先排序：获得关键数据风险指标的统一视图，以了解风险概况并弥补缺口。
• 动态数据脱敏：实时遮蔽或编辑敏感数据，即使在数据使用中也能防止未授权访问	• AI/ML 行为异常和威胁检测：识别异常用户行为，并将复杂的技术事件转化为通俗语言，供 IT 运营团队和安全人员立即采取行动

CipherTrust 数据安全平台的优势

供应商整合节省。减少采购、合同管理和培训开销，同时利用现有基础架构和专业知识，加速实现数据保护。

降低风险。通过应对外部攻击和内部威胁的分层防御策略降低潜在泄露成本，通过避免事件成本和提高运营效率创造可衡量的投资回报率。

通用合规覆盖。每项主要法规都要求数据保护和访问监控，在这些能力之间形成天然协同效应：

HIPAA
受保护健康信息加密
+ 访问审计追踪

PCI DSS
持卡人数据保护
+ 用户访问日志

SOX, GLBA, DORA
财务数据控制
+ 访问监控

GDPR, CCPA
个人数据加密
+ 处理记录

FISMA
联邦安全标准
+ 审计能力

NERC CIP, NIS2
关键基础架构数据保护
+ 访问追踪

Thales 的优势：无与伦比的创新与专业知识

预防性 + 检测性控制：加密阻止未授权访问，同时监控检测滥用行为

审计准备就绪：具有详细访问追踪和加密状态的自动化合规报告

运营效率：统一方法减少供应商蔓延和集成开销

快速响应：通过集中式策略管理在数分钟内弥补安全缺口

经验证的业务影响

组织可通过单一供应商策略从第一天起部署全面的数据库安全，在降低运营复杂性的同时，以一致的策略和精简的运营提供数据层安全。

数据库加密提供令人信服的投资回报率，Forrester 的总体经济影响研究记录了三年内 221% 的投资回报率以及 910 万美元的量化效益。实施可在不到六个月内收回成本，同时通过自动化和集中化将密钥管理工作量减少 70%。

行业认可

KuppingerCole 将 Thales 评选为 2025 年数据安全平台"整体领导者"，而 Forrester 将 Thales 定位为"强劲表现者"，在受评供应商中战略得分排名第二。Gartner Peer Insights 在 190 多条客户评论中给予 Thales 4.5 星评价，多项 FIPS 140-2 Level 3 认证验证了企业安全架构。

联系我们的安全专家

准备好弥补您的数据库安全缺口了吗？立即联系您的 Thales 代表，了解 CipherTrust 数据库加密解决方案和数据安全架构平台如何协同工作，以提供全面的数据保护、加速合规并创造可衡量的业务价值。

关于 Thales

Thales 是网络安全领域的全球领导者，帮助企业、政府和世界上最受信赖的组织在任何地方、大规模保护关键应用程序、敏感数据、身份和软件——并以最高的投资回报率实现。我们拥有超过 30,000 名客户，其中包括全球财富 500 强中的 58%，我们的解决方案部署在全球 148 个国家和地区。通过我们的创新服务和集成平台，Thales 帮助客户更好地了解风险、抵御网络威胁、弥补合规差距，并每天为数十亿消费者提供可信赖的数字体验。

© Thales - November 2025 • External • V5