cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform
发现、保护和控制

IT团队寻求一种以数据为中心的解决方案，该解决方案需要在数据从网络到应用程序和云进行传输时对数据进行保护。当外围网络控制和终端安全措施失败时，以数据为中心的解决方案可以使企业能够始终符合不断变化的隐私法规，并满足支持大量员工在线办公的需求。

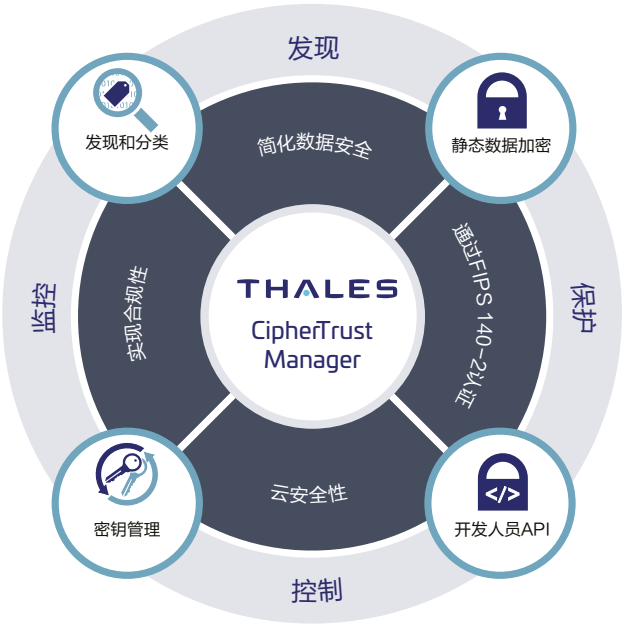
CipherTrust Data Security Platform（CDSP）是一种以数据为中心的解决方案，可显著降低企业的业务风险，并减少维护强大的数据安全所需的资源数量。

CDSP集成了数据发现、分类、数据保护和精细访问控制的集中式密钥管理。通过集中和简化数据安全，CDSP加快了合规速度，并确保了云迁移的安全。

关键特性

- 集中式管理控制台
- 监测和报告
- 数据发现和分类
  - 利用数据可视化进行风险分析
- 数据发现和分类可与透明加密相结合，在文件级别自动加密敏感数据
- 勒索软件保护
  - 主动监测恶意行为
  - 通过行为监控和数据分析可实现：
    - 防范零日攻击
    - 当系统与互联网断开时提供保护
    - 在终端上安装勒索软件后提供保护
- 机密管理
  - 集中管理所有类型的机密
  - 为DevOps集成、自动化和编排提供易于使用的功能
  - 管理混合、多云（所有云）、多租户、预置和传统系统的机密，并支持人工或机器访问
- 数据保护技术
  - 文件、数据库和大数据的透明加密
  - 应用层数据保护
  - 格式保留加密
  - 动态数据屏蔽令牌化
  - 静态数据屏蔽
  - 特权用户访问控制
- 集中式企业密钥管理
  - 符合FIPS 140-2的企业密钥管理

- 独特的KMIP集成合作伙伴生态系统
- 多云密钥管理
- 数据库加密密钥管理（Oracle TDE、大数据、MS SQL、SQL Server Always Encrypted等）



合规性

CipherTrust Data Security Platform支持全球安全和隐私法规，包括：

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS140-2
- FISMA, FedRAMP
- NIST 800-53修订版4
- 南非POPI法
- ISO/IEC 27002:2013
- 日本My Number合规性
- 韩国PIPA
- 印度Aadhaar法案
- 菲律宾数据隐私法
- 新加坡货币法
- 澳大利亚隐私修正案

关键优势

- **简化数据安全性。**借助下一代统一数据保护，随时随地发现、保护和控制敏感数据。CipherTrust Data Security Platform（CDSP）通过集中式管理控制台简化了数据安全管理，即使数据存储在云中或任何外部提供商的的预置和云数据基础架构中，该控制台为企业提供了强大的工具来发现和分类敏感数据、应对外部威胁、防范内部滥用并建立持久控制。在开始或推进数字化转型以从根本上改变企业的运营方式和为客户提供价值之前，企业可以轻松发现并弥合隐私差距、检测和阻止勒索软件、管理机密、确定保护的优先级，并就隐私和安全要求做出明智的决策。
- **加快合规速度。**监管机构和审计机构要求企业控制受监管的敏感数据以及报表来证明这一点。CDSP支持无处不在的数据安全和隐私要求，如数据发现和分类、勒索软件保护、机密管理、加密、访问控制、审计日志、令牌化和密钥理。数据安全控制可被添加到新的部署中，或响应不断变化的合规性要求。该平台的集中性和可扩展性使得能够通过增加许可和脚本化部署来添加新的控制。
- **安全的云迁移。**CipherTrust Data Security Platform 提供高级加密、集中式机密管理和集中式密钥管理解决方案，使企业能够在云中安全地存储敏感数据。该平台提供先进的多云自带加密（BYOE）解决方案，以避免云厂商锁定，并确保数据移动性，从而通过集中、不依赖云的加密密钥管理高效保护多个云供应商之间的数据。无法自带加密的企业仍然可以遵循行业最佳实践，使用CipherTrust Cloud Key Management（CCKM）从外部管理密钥。CCKM支持自带密钥（BYOK）和自持密钥（HYOK）使用案例，并简化了跨多个云基础设施和SaaS应用程序的本地密钥管理。由Akeyless Vault提供支持的CipherTrust Secrets Management提供企业级机密生命周期管理，包括创建、存储、轮换和删除所有类型机密的自动流程。

CipherTrust Data Security Platform

CDSP由CipherTrust Manager（CM）和一组连接器组成。

CM可以部署在本地、云端或混合环境中，也可以作为一项服务进行订阅。

CipherTrust Manager

作为CDSP的中央管理点，CM简化了所有加密密钥的密钥生命周期管理任务。CM可管理安全密钥的生成、备份/恢复、聚集、停用、删除以及对连接器和合作伙伴集成的访问，从而支持多种使用案例（如数据发现、静态数据加密、企业密钥管理和云密钥管理）。CM为密钥和策略提供基于角色的访问控制、强大的审计和报告，并提供开发和管理友好的REST API。CM提供物理和虚拟化型号。硬件和虚拟设备可以利用嵌入式Luna网络HSM或选择云HSM来实现FIPS 140-2 Level 3最高级别的信任根。

CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification 跨云、大数据和传统数据存储定位受监管的结构化和非结构化数据。单一控制台提供了对敏感数据及其风险的了解，从而能够更好地做出关于弥补安全差距、合规性违规和确定补救优先级的决策。该解决方案提供了从策略配置、发现和分类到风险分析和报告的所有简化工作流程，有助于消除安全盲点和复杂性。

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption（CTE）提供静态数据加密、特权用户访问控制和详细的数据访问审计日志记录。客户端可以保护云和大数据环境中，无论物理或虚拟服务器形态，Windows、AIX和Linux操作系统上的文件、卷和数据库中的数据。实时数据转换扩展组件可用于CTE，提供零停机加密和数据密钥更新。此外，安全情报日志和报表使用领先的安全信息和事件管理（SIEM）系统简化了合规性报告加快了威胁检测。

CipherTrust Ransomware Protection

CipherTrust Transparent Encryption Ransomware Protection（CTE-RWP）可监控行为、注意可疑活动，并在检测到勒索软件迹象时阻止进程。通过利用行为监控和数据分析，而不是恶意软件特征数据库，即使在断开网络的情况下，CTE-RWP也能保护系统免受零日攻击。其特别易于部署和管理。

CipherTrust Secrets Management由Akeyless Vault提供支持

CipherTrust Secrets Management（CSM）是由Akeyless Vault Platform提供支持的一种最先进的企业级机密管理解决方案。CSM可保护并自动访问DevOps工具和云工作负载中的机密，包括凭证、证书、API密钥和令牌。DevSecOps可快速轻松地将机密管理集成到多云应用程序中，以确保持续集成和持续交付流程的安全性并加快其速度。其特别易于部署和管理。

CipherTrust Intelligent Protection

CipherTrust Intelligent Protection使企业能够根据敏感性、漏洞和风险状况快速发现和分类数据，并使用加密和访问控制主动保护有风险的数据。它将CipherTrust Data Discovery and Classification与CipherTrust Transparent Encryption相集成，以提高运营效率、加快合规性速度，并主动弥合安全差距。

CipherTrust Application Data Protection

CipherTrust Application Data Protection（CADP）通过API提供密钥管理、签名、哈希和加密服务等加密功能，因此开发人员可以轻松保护应用服务器或大数据节点上的数据。该解决方案附带了提供支持的示例代码，因此开发人员可以快速保护应用程序中处理的数据。CADP加速了定制数据安全解决方案的开发，同时从开发人员的责任和控制中消除了密钥管理的复杂性。此外，CADP还通过仅由安全运营部门管理的密钥管理策略强制执行强大的职责分离。

CipherTrust Tokenization

CipherTrust Tokenization提供存储库和无存储库两种形式，有助于降低遵守数据安全要求（如 PCI-DSS）的成本和复杂性。令牌化用令牌替换敏感数据，因此敏感数据与数据库和未经授权的用户和系统保持分离和安全。无存储库产品包括基于策略的动态数据屏蔽。这两种产品都使得向应用程序添加令牌化变得很容易。

CipherTrust Database Protection

CipherTrust Database Protection解决方案将数据库中敏感字段的数据加密与安全、集中的密钥管理相集成，无需更改数据库应用程序。CipherTrust Database Protection 解决方案支持 Oracle、Microsoft SQL Server、IBM DB2和Teradata数据库。

CipherTrust Key Management

CipherTrust Key Management为管理整个企业的加密密钥提供了一个强大的基于标准的解决方案。它简化了围绕加密密钥管理的管理挑战，以确保密钥是安全的，并始终配置给授权的加密服务。CipherTrust Key Management解决方案支持多种使用案例，包括：

- CipherTrust Cloud Key Management (CCKM) 简化了Amazon Web Services（AWS）、Google Cloud Platform（GCP）、Microsoft Azure[1]、Oracle Cloud Infrastructure（OCI）[1]、Salesforce和SAP 1的“自带密钥”（BYOK）、“自持密钥”（HYOK）和本地密钥管理。即使所有云密钥都是本地密钥，CCKM也能减轻运营负担，从而提高效率。为客户提供生命周期控制、云内和云间的集中式管理以及云加密密钥的可见性，来降低密钥管理的复杂性和运营成本。
- CipherTrust TDE Key Management 支持广泛的数据库解决方案，如 Oracle、Microsoft SQL和Microsoft Always Encrypted。
- CipherTrust KMIP Server 集中管理KMIP客户端，如全磁盘加密（FDE）、大数据、IBM DB2、磁带归档、VMware vSphere和vSAN加密等。

关于泰雷兹

那些保护您个人隐私的企业，正在依赖泰雷兹保护其关键数据。在数据安全方面，组织机构正在面临越来越多的决定性时刻。无论是在构建加密策略、迁往云端，还是在满足合规性方面，您都可以依赖泰雷兹为您的数字转型保驾护航。

决定性时刻的决定性技术。

1请向我们查询HYOK支持此云的日期。

> cpl.thalesgroup.com <

联系我们 – 有关所有办公地点和联系信息，请访问 cpl.thalesgroup.com/contact-us