

解决方案简介

THALES

CYBERSECURITY

CipherTrust 数据安全态势 管理

识别风险、确定行动优先级、
降低风险。

cpl.thalesgroup.com

数据规模与复杂度已超越传统安全防护

机敏数据如今已成为现代企业的核心资产。它支撑客户信任、数字化运营、数据分析和人工智能创新。然而，这些数据日益分散在云平台、SaaS 应用、协作工具、分析环境、文件共享和传统系统当中。

随着环境持续扩张，许多企业无法自信回答以下三个关键问题：

- 机敏数据目前位于何处？
- 谁有权限访问这些数据？他们是否应当拥有访问权限？
- 哪些风险漏洞会带来最大业务风险？

传统安全工具的设计，已经无法应对当前数据大量分散、运营环境高度复杂化带来的挑战。

CipherTrust 数据安全态势管理（DSPM），通过持续发现、智能风险分析、内置防护和集中式治理，帮助企业重新掌控数据安全。

多数企业已经拥有可视化工具。企业当下真正需要的是控制权。

为何数据安全必须变革：

我们正处在网络安全新时代

安全风险环境的变化速度，已经超出很多企业现有的安全运营模式。

- AI 加速数据风险：智能代理 AI（Agentic AI）与 AI 驱动的分析应用，正在快速复制、转换并生成新的机敏数据存储环境。企业如果无法保障数据全生命周期的可信度与有效管控，就无法真正信任基于这些数据产出的 AI 结果。
- 机敏数据无处不在：关键信息不再只存放于数据库。它分散存储在云端、SaaS 平台、协作工具、数据湖和非托管存储库中。
- 董事会重视可量化成果：安全负责人越来越需要证明可量化的风险降低成效，而不只是展示工具的部署落地。
- 法规与数据主权愈发受到重视：全球隐私法规、数据本地化要求以及各行业监管规范持续增加。
- 工具泛滥造成运营效率低下：很多企业依靠相互独立的工具，分别开展数据发现、访问治理、加密、合规以及态势管理工作。

结果

仅有可见性，无法落地行动；只有告警，缺少修复；识别到风险，却无人负责。

安全管理者面临的五大挑战

很多企业面临的不是可见性问题，而是管控问题。

1. 未知机敏数据：机敏数据存在于安全团队未监控的位置，形成盲点与隐藏风险。AI 与智能代理 AI 系统快速普及进一步加剧该挑战，这类系统会在云、SaaS、协作和 AI 环境中生成、复制与使用机敏数据。
2. 过度访问权限：大量用户、第三方及服务账号，在超出业务必要的前提下，持续保有机敏信息的访问权限。
3. 风险优先级排序能力不足：团队收到大量检测结果，但无法针对会产生实际业务影响的风险做优先级划分。
4. 人工合规负担重：审计准备工作往往需要数周时间，从多个分散、未集成的系统中收集佐证材料。
5. 防护存在漏洞：即便识别风险，若要应用加密、脱敏、令牌化或策略变更，还需要不同团队与工具开展修复。

数据安全全新运营模式

CipherTrust DSPM

发现 | 分析 | 保护 | 管控

发现：在恶意攻击者之前定位关键信息

持续发现并分类云、SaaS、数据库、文件共享与本地环境中的结构化、非结构化机敏数据，确保所有关键信息清晰可见。您将获得：

- 机敏数据完整实时清单
- 发现、分类并关联影子数据
- 掌握关键数据的存储位置与流转路径
- 摸清各类环境下的数据访问主体

消除盲点，掌握关键数据存放位置。

分析：聚焦核心风险

关联数据敏感度、访问风险、漏洞、行为与业务背景，判断哪些因素会产生真实企业风险。您将获得：

对潜在影响最高的风险进行清晰排序并优先处置

- 可追踪人为、非人为以及特定代理活动，例如过度共享、数据泄露与异常访问行为
- 深入了解过度访问、配置错误与攻击路径
- 更快识别并响应安全漏洞
- 更高效利用有限安全资源

减少无效告警，将资源集中于潜在影响最大的风险。

保护：从风险检测到即时防护

直接在平台上应用加密、令牌化、脱敏与基于策略的修复措施，更快降低数据暴露风险。您将获得：

- 高风险问题快速修复
- 集成调查与取证工具，支持快速事件响应与数据安全事件根因分析
- 在最关键位置部署防护措施
- 可审批的自动化工作流
- 降低风险暴露与泄露带来的影响

高效快速降低风险暴露，减少泄露事件造成的损失。

管控：依托持续治理维持掌控力

通过单一管控平台，跨混合环境管理访问权限、策略、密钥、机密信息以及合规证据。您将获得：

- 确保仅授权用户可以访问数据
- 数据所在位置的策略执行保持一致
- 云端与本地集中管控
- 访问与防护状态随时可审计、可视化

伴随数据与环境的持续演变，保持常态化管理。

企业为何选择 CipherTrust DSPM

CipherTrust DSPM 内置风险修复能力，将风险可视化转化为实际处置动作，安全团队不仅能够识别风险，还可快速降低风险，无需依赖零散工具或手动流程。

CipherTrust DSPM 提供覆盖数据全生命周期的全面防护，从风险发现到风险修复，并配套必要治理机制，弥补传统单点解决方案短板，保障敏感数据在跨环境传输过程中始终安全。CipherTrust 分析数据交互行为识别风险并完成优先级排序，引导企业将时间与资源投入到可能造成重大影响的风险项。

CipherTrust DSPM 在强化数据安全的同时，不干扰企业业务运转；通过自动化加密、令牌化与访问控制降低数据暴露风险，同时保障数据在分析、AI 以及日常运营场景的可用性。例如，CipherTrust DSPM 能够找到未加密或者加密强度不足的数据，并支持企业通过自动化管控应用合适的加密强度。

除此之外，CipherTrust DSPM 通过持续保持审计就绪状态，简化合规管理，让企业实时掌握机敏数据位置、防护方式以及拥有访问权限的人员。CipherTrust DSPM 提供审计日志与报告，企业可随时调取所需合规资料，持续做好审计准备。

最后，它支持企业在混合云、多云环境实现统一管控，无论数据存储在何处，均可强制执行策略、降低风险暴露、落实治理。

可集成至您的数据安全与响应体系

CipherTrust DSPM 能够对接现有安全与事件响应生态，包含 SIEM 平台以及 ServiceNow 等工单系统，将数据风险洞察转化为实际安全处置动作。通过把发现、风险分析和修复工作流直接接入企业安全架构，企业可以加快事件响应速度、自动化修复流程，缩短在混合云和多云环境中识别、处置关键数据泄露所需的时间。

适用场景

- 在混合资产环境发现未知机敏数据
- 缩减关键数据的过度访问权限
- 强化审计与监管合规准备
- 保障智能代理 AI 与 AI 驱动分析的数据安全
- 保护高价值监管数据与核心业务数据

部署灵活，性能不打折扣

在不放弃管控能力的前提下，完成安全现代化改造。

SaaS 部署

快速实现价值、降低运营负担、持续迭代创新、支持全球扩展。

本地部署 / 混合部署

保障数据主权、满足内部信任与监管要求，各类部署模式下功能保持一致。

为什么选择泰雷兹？

CipherTrust DSPM 承袭泰雷兹数十年保护全球关键系统、数据与基础设施的领先经验。

从全球银行、医疗机构，到政府部门、制造业以及强监管企业，各类机构在零容错场景下都信赖泰雷兹。

唯有泰雷兹，将新一代 DSPM 创新技术，结合加密、密钥管理、令牌化、活动监控与风险分析领域成熟深厚的技术优势，帮助企业降低数据风险，同时维持对机敏信息的管控。

依托服务全球大型企业的规模能力，以及适配数据主权、数据本地化与法规要求的灵活性，泰雷兹打造可信赖平台，助力企业应对当下日趋复杂的全球 IT 环境。

泰雷兹优势

多数 DSPM 供应商仅帮助您了解风险	CipherTrust DSPM 帮助您降低风险
• 侧重周期性发现与分类 • 事件清单，无优先级排序 • 告警数量过多 • 需要手动修复 • 依赖独立防护工具	• 持续发现与分类 • 基于情报做优先级排序 • 内置防护能力 • 集中式治理 • 搭建于成熟的泰雷兹数据安全平台之上

结语

CipherTrust DSPM 帮助企业摆脱碎片化工具以及仅展示态势信息的仪表盘，实现可量化的风险降低。

它融合持续发现、智能优先级排序、内置防护与集中管控，让安全负责人能够全面管理跨云、SaaS、AI 以及混合环境中的机敏数据。

多数供应商可以帮您识别数据风险。泰雷兹能够帮您规避风险。

借助 CipherTrust DSPM，重新掌控机敏数据。

关于泰雷兹

泰雷兹是网络安全领域全球领导者，致力于帮助企业、政府及全球高可信组织，以最高投资回报率大规模保护核心应用、机敏数据、身份与软件。我们拥有超过 30,000 家客户，其中包含 58% 的《财富》世界 500 强企业，解决方案已部署在全球 148 个国家。依托创新服务与集成平台，泰雷兹助力客户洞悉风险、抵御网络威胁、弥补合规缺口，每天为数十亿消费者提供可信数的字化体验。