itbigtec
艾体宝

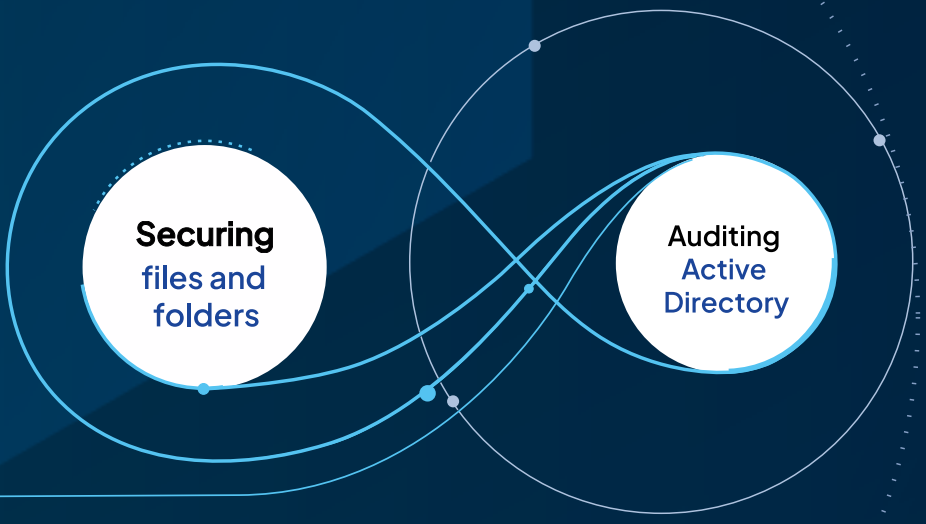
艾体宝Lepide

数据安全管理平台

目录与数据安全化繁为简

itbigtec.com

引言



在数字化转型不断深入的今天，
数据已成为企业最核心的资产之一。
但与此同时，数据泄露、权限滥用、
内部违规操作等风险频发，合规审计
的压力也愈加严峻。企业不仅需要
“把数据管起来”，更需要“看得清、
控得住、查得准”。

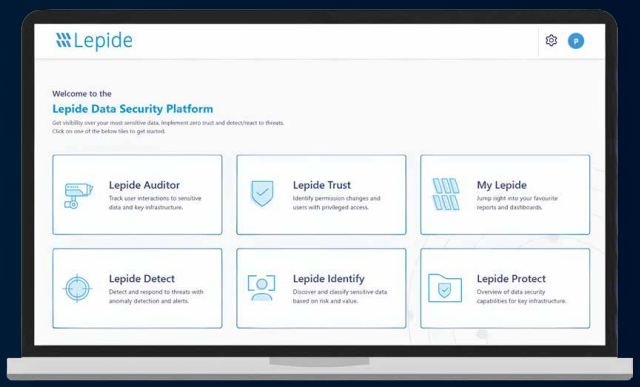
Lepide 正是为解决这一难题而生。
作为一个全栈数据安全管理平台，
Lepide 集成了数据访问审计、用户行为分析、
敏感数据识别与权限治理等能力，帮助企业实时掌握“谁在访问什么数据、做了什么操作”，及时识别风险并满足合规要求。无论是敏感数据分布、访问权限管理，还是异常行为检测与快速响应，Lepide 都能提供一体化、自动化的解决方案。

通过与企业现有的 AD、文件服务器、数据库等系统深度集成，Lepide 实现了对数据访问与用户权限的全面可视、实时预警与持续优化，助力企业构建“看得见、控得住、反应快”的数据安全体系。

本手册将向您全面介绍 Lepide 的功能模块、应用场景与部署方式，帮助您深入理解这一平台如何在多种业务环境中落地，为数据安全保驾护航。

六大模块

构建完整安全能力闭环



- Lepide Auditor - 审计追踪关键数据访问与权限变更
- Lepide Trust - 分析与治理用户权限与资源访问风险
- Lepide Detect - 实时发现异常，智能告警响应
- Lepide Identify - 识别敏感数据，自动分类打标
- Lepide IQ - 汇总数据与行为，支持风险分析决策
- Lepide Protect - 权限修复与访问控制，防止数据外泄

功能概览

数据环境全面可视化

全面掌握 "谁、何时、访问了什么数据、做了什么操作"

- 实时掌握敏感数据访问及操作，数据访问行为全程留痕
- 快速发现权限漂移与违规访问，避免高风险账户长期隐匿
- 可视化的访问行为图，提升内部审计效率，强化安全问责机制

价值

让敏感数据访问变得 "看得见、说得清"，降低数据滥用和审计风险

用户行为分析与异常检测

发现内部威胁、识别 "非正常" 用户行为

- 建立用户基线，识别非常规操作（如非工作时段大量访问敏感数据）
- 快速定位异常访问或批量操作行为，提升内部安全可控性
- 避免关键数据被无声泄露或破坏，增强整体安全感知

价值

提前发现 "内部威胁"，防止损失于未然

权限管理与访问治理

找出权限过多的用户，自动修复权限风险

- 分析当前权限分布，识别冗余或过度权限
- 可视化权限结构图，便于理解继承链
- 提供权限收紧建议，并支持自动修复（Zero Trust支持）

价值

让权限 "最小化、可控化"，从源头降低数据被滥用的风险

数据发现与敏感分类

找到企业最关心的数据，并给它贴上标签

- 自动扫描文件服务器、NAS、SharePoint等位置
- 识别身份证号、银行卡号、邮箱、医疗记录等敏感信息
- 按内容风险值对数据分类评分，使用户行为分析和权限策略聚焦在最重要的数据上

价值

让企业清楚知道 "我有哪些敏感数据/数据资产，放在哪，谁能看"

审计日志分析与合规报告

生成 "合规级" 报告，快速应对审计检查

- 内置GDPR、ISO、HIPAA等多种合规模板
- 报告图表丰富、操作溯源清晰，适合汇报与审计使用
- 支持自动调度导出日报、周报、月报等

价值

轻松应对内外部审计检查，减少合规压力与时间成本

实时告警与威胁响应

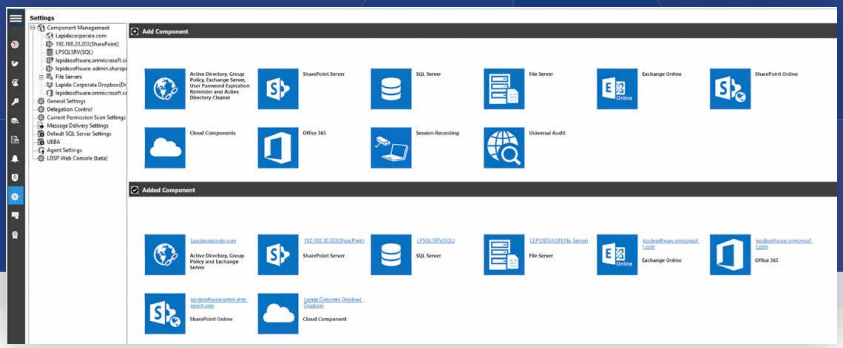
安全事件发生时，第一时间知道，第一时间应对

- 可自定义告警规则，实时推送至邮件、SIEM、Webhook等
- 内置威胁模型与工作流，支持自动响应（如通知、记录、联动阻断等）
- 帮助企业构建主动防御机制

价值

从 "事后追责" 走向 "即时响应"，大幅提升安全防御能力

平台对接能力



支持平台一览

用户目录：Windows Active Directory，Microsoft Entra ID
协作套件：Microsoft 365、Exchange Online、Teams、Google Workspace
存储及数据库：Windows File Server、NetApp、Dell EMC Data Storage、SharePoint、Exchange Server、SQL Server、Dropbox、Amazon S3、Nasuni、Nutanix

典型应用场景

金融行业
防止敏感数据外泄

某银行的客户资料存储在共享文件服务器中，由多个部门共用。IT 部门发现部分文件被不相关人员访问，并存在外发风险

Lepide 的做法

- 自动审计所有文件访问行为，标记与岗位权限不符的访问操作
- 对客户数据文件打标签，识别高风险访问
- 提供权限优化建议并发送实时告警

价值

防止敏感客户信息在不知情中被非法访问，满足金融行业对数据安全和合规的高要求

制造行业
防止研发资料外泄

某制造企业在文件服务器中保存大量图纸、BOM、设计资料。某员工离职前，批量复制了多个项目文件

Lepide 的做法

- 建立访问基线模型，识别“非正常批量复制”行为
- 实时告警、记录文件被访问路径
- 提供离职用户操作审计报告，便于责任追溯

价值

在关键资产泄露前实现预警与定位，保护企业核心竞争力

教育行业
审查文件访问记录，应对合规调查

某高校在接受教育部检查时，
需提交所有教师对教学成果
与学生数据的访问记录

Lepide 的做法

- 快速生成访问审计报告，支持按用户/目录/时间筛选
- 支持导出中文报告，图表清晰，合规汇报适用
- 可设定关键数据目录，长期监控访问行为

价值

轻松应对审计与监管要求，
节省内部人力时间成本

泛企业场景
权限审查与最小化治理

安全团队担心权限配置过于复杂，
历史继承混乱，存在“看不清、控不了”
的问题

Lepide 的做法

- 可视化权限结构图，发现冗余权限
- 支持权限回收建议与自动修复
- 提供高权限用户列表与访问行为追踪

价值

让企业权限管理有章可循，
落地 “Zero Trust” 最小权限原则

核心功能模块解析

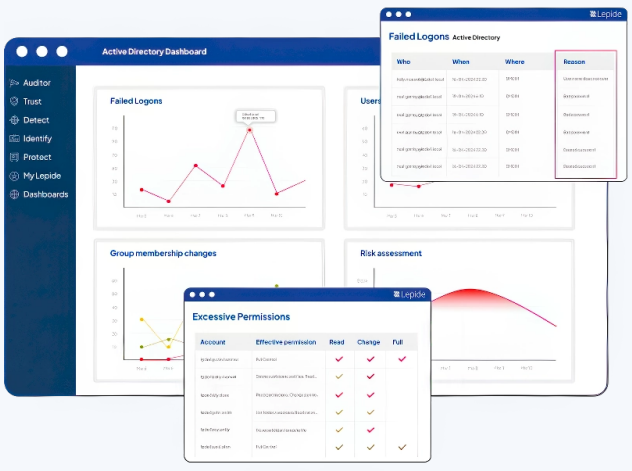
Lepide Auditor

统一审计平台，记录一切关键操作

跟踪用户与敏感数据、关键基础设施的交互；
审计目录与存储并生成详细报告，
帮助企业了解数据与系统安全状态。

- 审计用户在文件服务器、Active Directory、SharePoint、Exchange 等系统中的访问、创建、删除、权限修改行为
- 提供详尽记录：谁、在何时、做了什么、对哪类数据
- 支持快速生成合规审计报告（GDPR/ISO等）

应用场景示例：
发现某员工在凌晨访问了大量项目资料，
可立即定位行为详情。



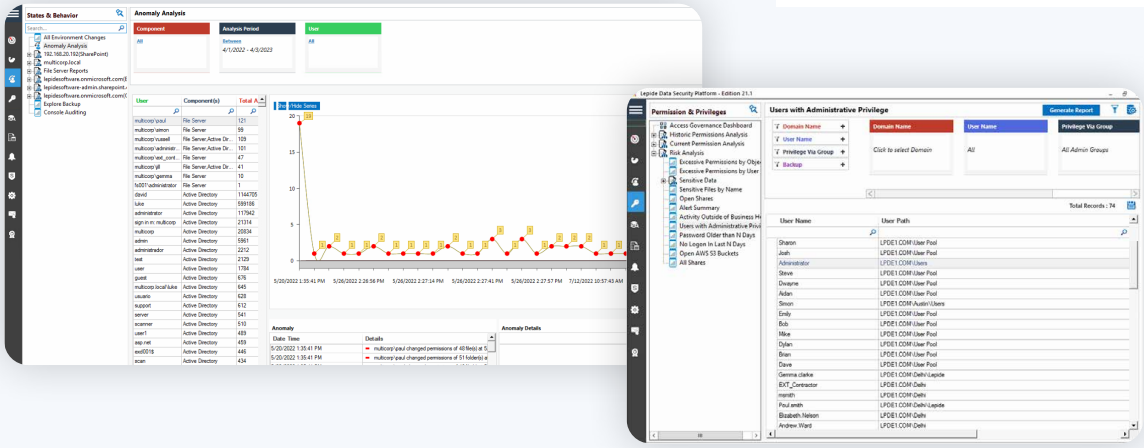
Lepide Trust

权限分析与治理，解决 “权限谁来管”

了解哪些人可以访问您的敏感数据以及这些访问权限是如何授予的。根据对象、用户或邮箱确定有效的权限设置。识别导致特权用户产生的权限变更。查明这些权限的来源，并在必要时撤销相关变更。生成特权用户列表，并查看其权限的来源。

- 分析用户权限过高、漂移及继承等风险
- 绘制访问关系图，支持权限回收建议
- 识别哪些敏感数据在外暴露

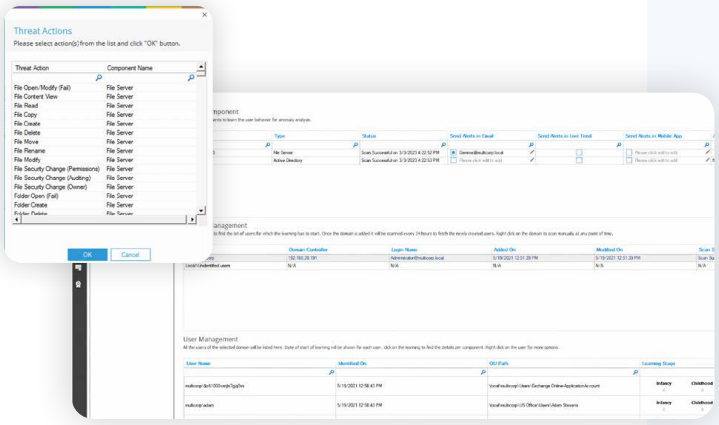
应用场景示例：
定期审查敏感文件夹是否被普通员工访问，自动标记“高风险访问”



Lepide Detect

用户行为分析（UBA），识别异常动作

Lepide Detect 采用人工智能技术，实现对安全威胁及异常或可疑用户行为的实时自动检测。通过加速检测内部威胁、被入侵的用户账户、勒索软件、暴力破解攻击以及权限滥用，有效防范可能导致严重安全漏洞的风险。



- 建立用户访问基线，识别 “谁与众不同”
- 检测批量访问、非工作时间访问、异常登录等行为
- 与SIEM、Webhook联动实时告警

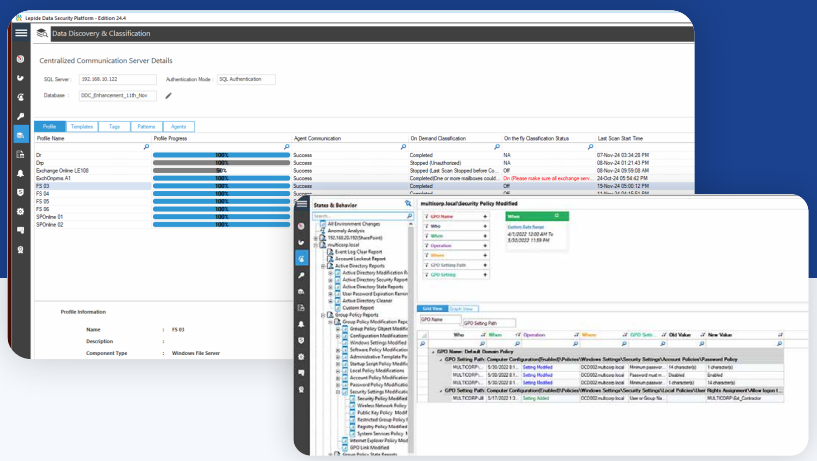
应用场景示例：员工短时间内复制上千份文档并发送邮件，立即触发告警

Lepide Identify

敏感数据发现与分类，实现 "数据可视"

自动扫描、发现并分类数据，确保随时掌握敏感数据存储位置。通过proximity技术减少误报，提升分类准确性，超越多数分类解决方案。根据合规性、风险、发生频率和经济价值等因素对数据评分，实时掌握最敏感数据动态。

通过持续分类帮助组织构建敏感数据图景，让组织知道敏感数据在哪里、谁有权访问，以应对GDPR、CCPA等合规要求，Lepide Identify助力企业追踪敏感数据、建立合规基础。



- 扫描文件服务器、NAS、SharePoint等位置
- 支持识别身份证号、邮箱、银行卡号、健康信息等
- 按内容风险值对数据分类评分，使用户行为分析和权限策略聚焦在最重要的数据上

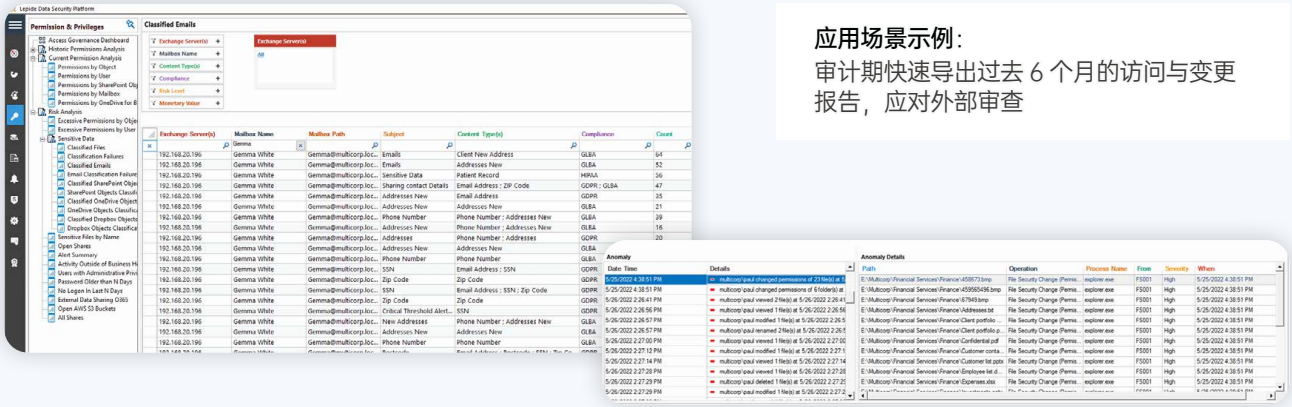
应用场景示例：
合规前期盘点企业所有服务器中涉及 PII 的文件位置与类型"

Lepide IQ

智能分析与洞察，提供决策支持

Lepide IQ 分析数据并快速提供关键洞察，允许生成报告摘要，突出重要信息，而无需完整生成报告在大量细节中筛选

- 汇总平台数据，生成多维度统计报表
- 提供高风险用户、高敏感资产等安全视图
- 支持趋势分析、行为对比、违规排行等图形化展示



应用场景示例：
审计期快速导出过去 6 个月的访问与变更报告，应对外部审查

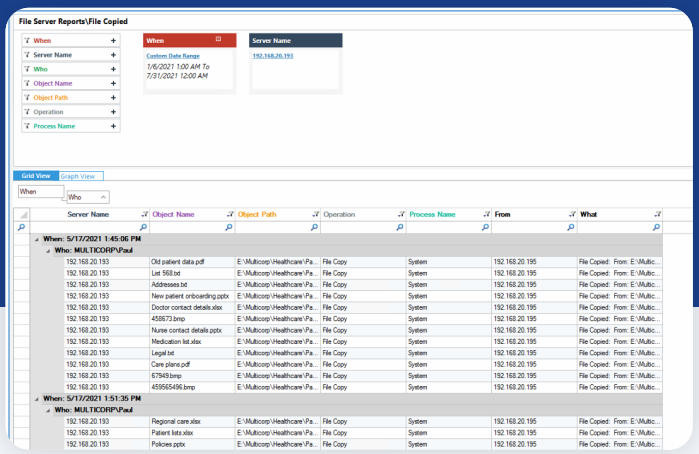
Lepide Protect

权限修复与主动防护

Lepide 通过权限管理系统，帮助简化用户权限的管理复杂性。该功能可清晰展示哪些用户拥有哪些访问权限，包括哪些用户拥有过多权限。一旦识别出过多权限，即可在 Lepide 解决方案内撤销这些权限，并移除不活跃用户。

- 提供权限重置、敏感权限移除建议
- 可联动 AD 和资源平台实施权限修复操作
- 防止高权限账户滥用、数据外泄

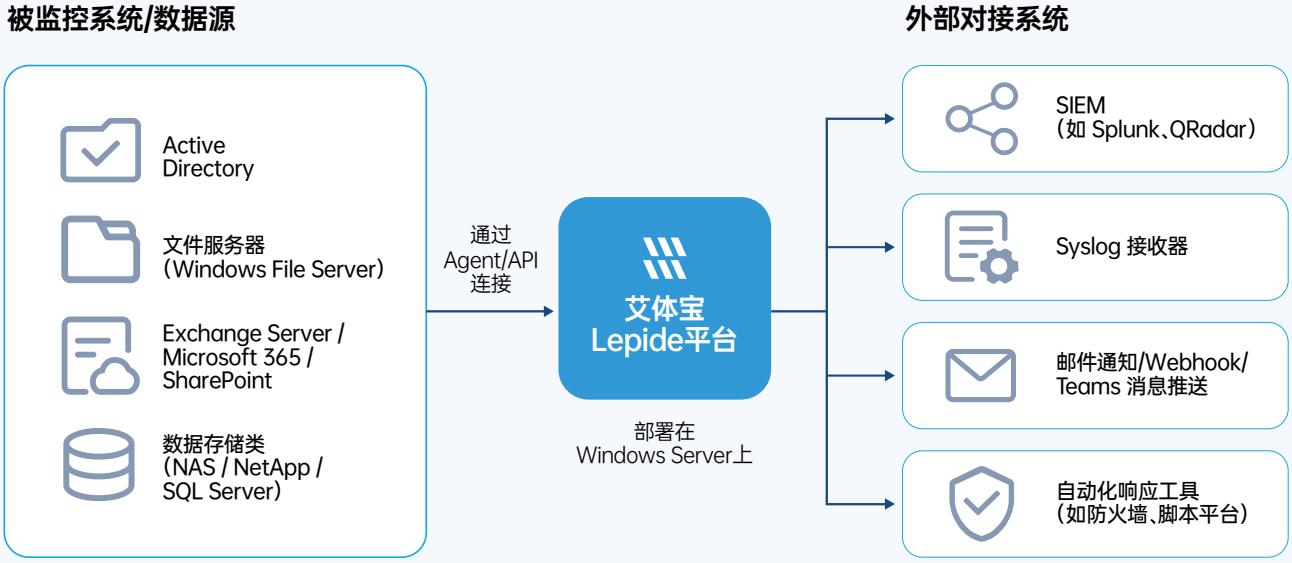
应用场景示例：
发现某用户拥有对财务目录的完全权限，平台建议降权并支持自动执行



Lepide 部署方式

Lepide 采用本地部署（On-Premises）架构，安装在 Windows Server 上，通过 Agent/API 与企业现有系统集成，具备高可控性与数据私密性，适用于对数据安全与合规性要求严格的行业客户。

Lepide 部分模块 / 解决方案可按需进行 SaaS 部署，详情请咨询艾体宝团队。



产品优势与对比亮点

与传统安全产品不同，Lepide专注于内部数据安全可视化与治理，不是防火墙，但能解决"看不清、管不到、反应慢"的核心痛点。

产品对比详情

	Lepide	传统SIEM/日志平台	传统DLP/权限工具
适用定位	数据访问审计 + 权限治理	外部威胁检测为主	AD管理自动化、DLP防护
可视化程度	图形化访问路径、权限结构、行为趋势	数据抽象为主，配置复杂	权限结构清晰，行为可视能力有限
整合能力	一体支持文件、AD、M365、SQL等关键平台	需对接多系统，依赖人工	聚焦AD及部分SaaS平台
异常检测	内置用户行为分析模型，识别异常访问行为	日志规则构建复杂	无行为分析，异常检测依赖SIEM联动
权限分析与治理	自动发现冗余权限，支持修复建议(Zero Trust)	缺乏权限分析能力	擅长权限分配与审批流，分析能力一般
报表与合规	丰富图表、自带模板，适合审计与汇报	报表需定制，非合规导向	中文报告支持好，合规性视图简洁
部署与上手速度	本地部署，1-2周上线，界面清晰	架构重，实施周期长	安装简单，功能聚焦AD，学习成本低
使用灵活性	模块化架构，支持按需启用与组合	模块耦合，拓展难	工具型产品，灵活性有限
总体适配场景	数据内部安全、审计合规、权限风险治理	威胁监测、事件响应	AD权限管理、自动化工作流

我们的客户

Home Office · Deloitte. · KPMG · Investec · SEB · Moody's · Fujitsu · Clifford Chance · NHS · Fair Trade Certified · West Yorkshire Fire & Rescue Service · Pfizer · hmsa · Mets

客户案例

Western Connecticut Health Network

关于客户

Western Connecticut Health Network拥有 10,000 多名员工，总部设在美国康涅狄格州

解决方案的需求

- 客户原先用竞品方案来跟踪Active Directory中的权限与配置
- 在使用过程中，客户发现报告中存在异常
- 该竞品无法监控受监管数据、用户行为，也无法检测潜在威胁
- 为了满足 HIPAA 法规要求，客户需要在报告中获得更为详尽的数据与分析

"Lepide简单易用，一开始就很有效。此外，他们的耐心、细心和技术知识远远超出了我以前见过的大多数支持和销售团队。"

Drayke Jackson
安全工程师

Lepide 如何提供帮助

- ✓ Lepide 允许客户从一个平台保护 Active Directory 和受监管数据
- ✓ Lepide 确定了存在风险的敏感数据（PHI、ePHI），包括对所有用户开放的数据
- ✓ Lepide 确定了活动目录中存在风险的安全配置，包括非活动用户和不合规的密码
- ✓ Lepide 确定了对敏感数据拥有过多权限的用户
- ✓ Lepide 启用威胁模型，自动检测和响应数据泄露和安全威胁，包括 AD 中的权限升级和勒索软件检测
- ✓ Lepide 与客户的 SIEM 集成，以扩展功能

创新型IT解决方案合作伙伴

关于艾体宝

艾体宝科技有限公司 (简称"艾体宝") 是一家创新型IT解决方案公司, 于2023年正式成立, 专注于提供尖端的数据存储、数据智能、安全与合规性、网络性能监控、DevSecOps解决方案。

我们的使命是通过技术创新, 赋能企业在复杂的数字化转型浪潮中实现卓越运营。核心业务领域包括:

数据存储

提供尖端的分布式缓存数据库和持久性数据存储/备份等解决方案, 确保客户能够有效地管理和利用不断增长的数据资产, 构建高性能、可扩展的数据存储基础。

数据智能

利用最新的数据分析和人工智能技术, 帮助客户实现数据驱动决策, 挖掘深层商业洞察, 推动业务的智能化和优化。

安全与合规

提供全面的解决方案, 覆盖数据安全、终端安全、供应链安全评估和应用安全, 以保障客户在数字化环境中的数据和业务始终安全可控。

网络监控与优化

提供全面的网络性能监控、故障排除及压力及性能测试工具及服务, 确保客户的网络基础设施稳定高效。

DevSecOps

提供软件开发、安全与运维的自动化, 通过持续集成和安全管理自动化, 提升开发效率, 助力企业在激烈市场竞争中保持敏捷与合规。

我们拥有专业的技术团队, 核心成员拥有10年的行业经验沉淀, 经由美国和欧洲行业内顶尖专家培训, 不仅拥有包括红帽、思科、IBM等在内的专业认证资格, 具备丰富的创新技术实践和成功案例经验。

我们以创新为驱动、技术为基础, 持续推动前沿技术发展, 助力企业在激烈市场竞争中更快速、高效、安全地实现业务扩展, 脱颖而出。

国家级专精特新"小巨人"企业

高新技术企业

广东省"专精特新"中小企业

新锐企业培优计划

*所示资质由艾体宝关联公司虹科取得

艾体宝科技有限公司

www.itbigtec.com
sales_it@itbigtec.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼

T (+86)400-999-3848

各分部：广州 | 成都 | 上海 | 苏州 | 西安 |
北京 | 台湾 | 香港 | 日本 | 韩国

版本：V1.0

联系我们
(T: 135 3349 1614)

网络安全交流群

获取更多资料

itbigtec.com