

HongKe

虹科

启用指南

如何启用 LEPIDE

合规性

目录

1. 导言.....	3
2. 调整 Lepide 以符合规定.....	3
3. Lepide核心能力.....	10
3.1. - Lepide 识别.....	10
3.2. - Lepide 信任	11
3.3. - Lepide 审计.....	12
3.4. - Lepide 检测.....	13

1. 引言

合规是企业面临的一个巨大问题，随着越来越多的法规开始发挥作用，现有法规的执行也将更加严格，这个问题在未来几年将变得更加棘手。到 2023 年底，现代隐私法将覆盖全球 75% 人口的个人信息。

企业要求安全团队提供审计报告，以证明他们采取了以下措施。
必要的步骤，以确保它们符合要求。

我们对核心窗口基础架构以及受监管数据的存储和使用方式和地点有着深入的了解，这使我们在帮助企业实现合规目标方面处于独一无二的地位。如果没有我们的解决方案，企业要回答这些常见的合规性问题即使不是不可能，也会非常困难。

2. 调整 Lepide 以实现合规
















为了能够保护数据并满足法规遵从性规定，您需要能够回答许多关键问题。

















在下表中，我们将lepipe技术与这些问题结合起来：

类别	应采取的行动	实施技术
数据保护	确保员工只能访问所需的数据。减少蔓延	<ul style="list-style-type: none"> 不活动用户报告 (Lepide 审计) 用户权限过多报告 (Lepide 信任) 对象权限过大报告 (Lepide 信任) 用户权限报告 (Lepide 信任) 具有管理权限的用户报告 (Lepide 信任) 公开股份报告 (Lepide 审计) 数据分类 (Lepide 识别) 增加威胁表面区域威胁模型 (Lepide 检测)

		<ul style="list-style-type: none"> 权限升级（组）威胁模型 (Lepide 检测) 权限升级（文件）威胁模型 (Lepide 检测) 权限升级（文件夹）威胁模型 (Lepide 检测)
	管理活动目录中的非活动用户账户。	<ul style="list-style-type: none"> 不活动用户报告 (Lepide 审计) 活动目录清理器 (Lepide 审计)
	获取员工使用受监管数据的审计报告	<ul style="list-style-type: none"> 机密电子邮件报告 (Lepide 识别) 分类 SharePoint 对象报告 (Lepide 识别) 分类的 OneDrive 对象报告 (Lepide 识别) 分类 DropBox 对象报告 (Lepide 识别) 所有环境变化报告 (Lepide 审计) 文件服务器、SharePoint、SharePoint Online、OneDrive 的所有数据交互报告 (Lepide 审计) 所有邮箱访问报告 (Lepide 审计)

	处理加入者、搬迁者和离开者，以保持适当的进出通道	<ul style="list-style-type: none"> 用户权限报告 (Lepide 信任) 历史权限报告 (Lepide 信任) 对象权限过大报告 (Lepide 信任) 不活动用户报告 (Lepide 审计) 具有管理权限的用户报告 (Lepide 信任)
	查看谁有权限访问 Active Directory	<ul style="list-style-type: none"> 具有管理权限的用户报告 (Lepide 信任) 活动目录权限报告 (Lepide 信任)
	查看员工何时通过 Active Directory 登录公司网络	<ul style="list-style-type: none"> 工作时间以外的活动报告 (Lepide 审计) 登录/注销审计 (Lepide 审计) 登录失败报告 (Lepide 审计) 成功用户登录/注销报告 (Lepide 审计) 用户登录多台计算机报告 (Lepide 审计) 并发登录报告 (Lepide 审计) 域控制器登录/注销报告 (Lepide 审计) 潜在暴力攻击威胁模型 (Lepide 检测)

	<p>查看对 Active Directory 所做的更改。获取审计跟踪。</p>	<ul style="list-style-type: none">  活动目录修改报告 (Lepide 审计)  历史权限 - 活动目录分析报告 (Lepide 信任)  用户权限报告 (Lepide 信任)
	<p>跟踪组员资格和组策略的变更。</p>	<ul style="list-style-type: none">  组策略对象创建报告 (Lepide 审计)  组策略对象删除报告 (Lepide 审计)  组策略对象重命名报告 (Lepide 审计)  组策略对象修改报告 (Lepide 审计)
	<p>在创建、删除或修改新的 Active Directory 用户账户时进行报告。</p>	<ul style="list-style-type: none">  活动目录对象创建报告 (Lepide 审计)  活动目录对象删除报告 (Lepide 审计)  活动目录对象修改报告 (Lepide 审计)
	<p>确保活动目录中没有不活动/不需要的用户账户。</p>	<ul style="list-style-type: none">  活动目录清理器 (Lepide 审计)  不活动用户报告 (Lepide 审计)
<p>威胁检测</p>	<p>及早发现事件，防止受监管数据外泄。</p>	<ul style="list-style-type: none">  触发任何威胁模型 (Lepide 检测)  具有管理权限的用户报告 (Lepide 信任)  用户权限报告 (Lepide 信任)

		<ul style="list-style-type: none"> 不活动用户报告 (Lepide 审计) 权限过高报告 (Lepide 信任) 所有环境变化报告 (Lepide 审计) 异常点检测 (Lepide 检测) 复制的档案报告 (Lepide 审计) 外部数据共享报告 (Lepide 审计) 潜在数据泄漏威胁模型 (Lepide 检测)
准入管理	查看密码或密码策略更改的时间	<ul style="list-style-type: none"> 密码政策修改报告 (Lepide 审计) 密码年龄政策修改报告 (Lepide 审计) 密码复杂性政策修改报告 (Lepide 审计) 密码加密策略修改报告 (Lepide 审计) 密码历史政策修改报告 (Lepide 审计)
	确保我们按照合规要求适当存储个人数据	<ul style="list-style-type: none"> 数据分类 (Lepide 识别) 机密电子邮件报告 (Lepide 识别) SharePoint 对象分类报告 (Lepide 识别) 分类的 OneDrive 对象报告 (Lepide 识别)

		<ul style="list-style-type: none"> 分类 DropBox 对象报告 (Lepide 识别) 所有股票报告 (Lepide 信任) 用户权限过多报告 (Lepide 信任) 对象权限过大报告 (Lepide 信任) 用户权限报告 (Lepide 信任) 按对象分列的权限报告 (Lepide 信任)
	查看保存了哪些个人或受监管数据, 以及 保存在何处	<ul style="list-style-type: none"> 数据分类 (Lepide 识别) 机密电子邮件报告 (Lepide 识别) SharePoint 对象分类报告 (Lepide 识别) 分类的 OneDrive 对象报告 (Lepide 识别) 分类 DropBox 对象报告 (Lepide 识别) 所有股票报告(Lepide 信任) 用户权限过多报告 (Lepide 信任) 对象权限过大报告 (Lepide 信任) 用户权限报告 (Lepide 信任) 按对象分列的权限报告 (Lepide 信任)
	查看我们在企业内部拥有哪些受监管的数据	<ul style="list-style-type: none"> 数据分类 (Lepide 识别) 机密文件报告 (Lepide 识别)



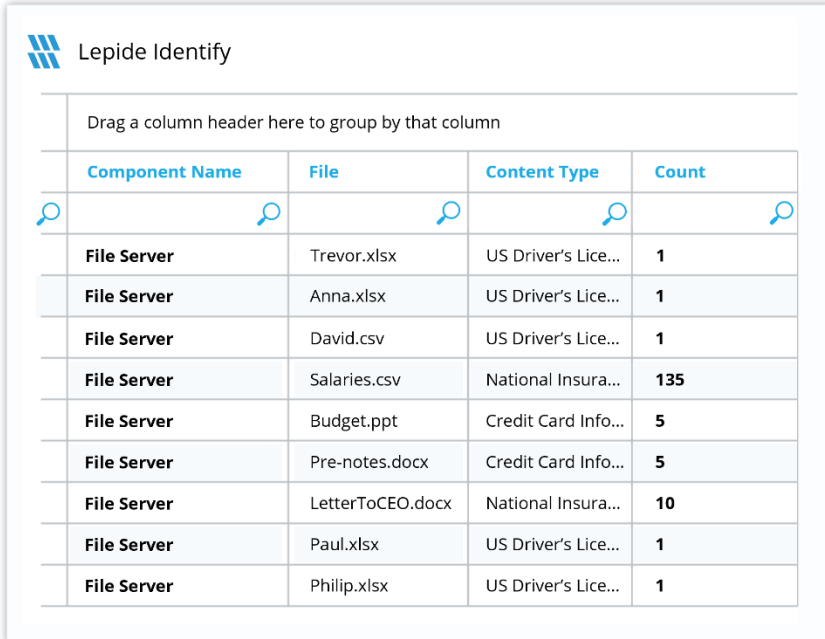
The diagram consists of two large, empty light blue rectangular boxes on the left side, representing source systems. To their right is a vertical list of four items, each preceded by a circular icon containing a magnifying glass. These items represent reports generated from the source systems.

-  机密电子邮件报告
([Lepide 识别](#))
-  SharePoint 对象分类报告
([Lepide 识别](#))
-  分类的 OneDrive 对象报告
([Lepide 识别](#))
-  分类 DropBox 对象报告
([Lepide 识别](#))

3. Lepide 核心能力

3.1. - Lepide Identify

在创建时自动扫描、发现数据并进行分类，帮助您随时掌握敏感数据的位置。利用近距离扫描技术消除误报。与大多数分类解决方案相比，这有助于进一步提高准确性。根据合规性、风险、发生率、货币价值等因素对数据进行分类和评分，随时掌握最敏感的数据。



The screenshot shows the 'Lepide Identify' interface. At the top, there is a header with the Lepide logo and the text 'Lepide Identify'. Below the header is a search bar with the placeholder text 'Drag a column header here to group by that column'. The main content is a table with the following columns: 'Component Name', 'File', 'Content Type', and 'Count'. Each cell in the table has a magnifying glass icon. The table contains the following data:

Component Name	File	Content Type	Count
File Server	Trevor.xlsx	US Driver's Lice...	1
File Server	Anna.xlsx	US Driver's Lice...	1
File Server	David.csv	US Driver's Lice...	1
File Server	Salaries.csv	National Insura...	135
File Server	Budget.ppt	Credit Card Info...	5
File Server	Pre-notes.docx	Credit Card Info...	5
File Server	LetterToCEO.docx	National Insura...	10
File Server	Paul.xlsx	US Driver's Lice...	1
File Server	Philip.xlsx	US Driver's Lice...	1

总之：

- 在真实 Tag 数据中发现数据并对其进行分类。
- 数据估值。
- 识别风险最大的数据。

3.2. - Lepide 信任

报告谁可以访问最敏感的数据，以及他们是如何被授予访问权限的。针对权限过大的用户的特定报告能让你发现哪些用户最有可能成为内部威胁。在权限发生变化时及时发现并逆转，从而维护零信任策略。

Lepide Trust					
Account (Principal)	Effective Permission				
Lpde1\jill	Full Control	✓	✓	✓	✓
Lpde1\Paul	Full Control	✓	✓	✓	✓
Lpde1\Bill	Full Control	✓	✓	✓	✓
Lpde1\Steve	Full Control	✓	✓	✓	✓

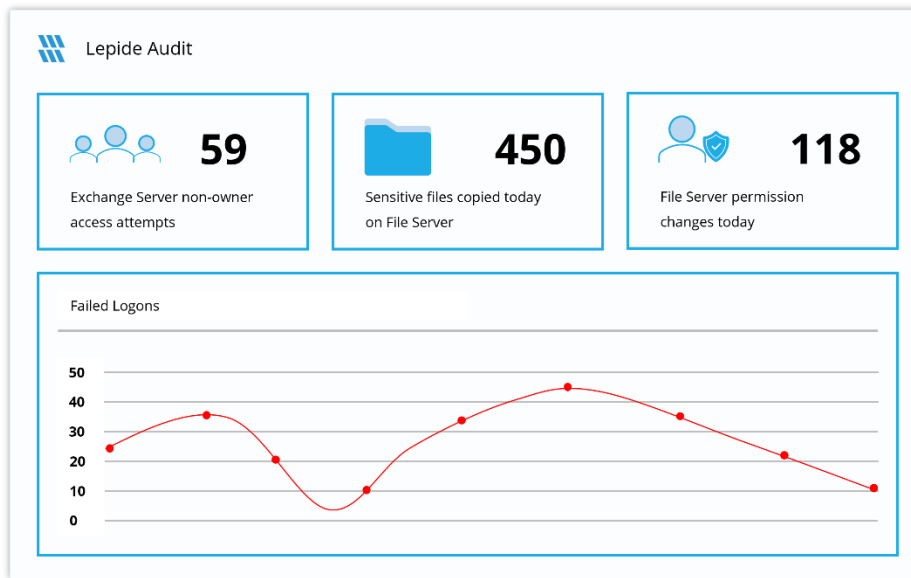
Files in Folder : Accounts		
Clients - Copy (2).txt	Credit Card - Visa + UK Phone	1 + 1 + 1 + 1 + 1
Clients.txt.encrypt	Credit Card	100
Customer details.png	No Sensitive Content	N/A
Database.doc	Credit Card + SSN	100 + 500

总之：

- 分析权限。
- 识别特权过大的员工（最小特权）。
- 查看历史许可。
- 跟踪权限更改。

3.3. - Lepide 审计

对敏感数据和混合环境所做的更改进行审计、报告和警报。回滚不需要的更改并恢复已删除的对象，以维护系统的完整性。跟踪用户对关键文件和文件夹所做的任何更改和修改。

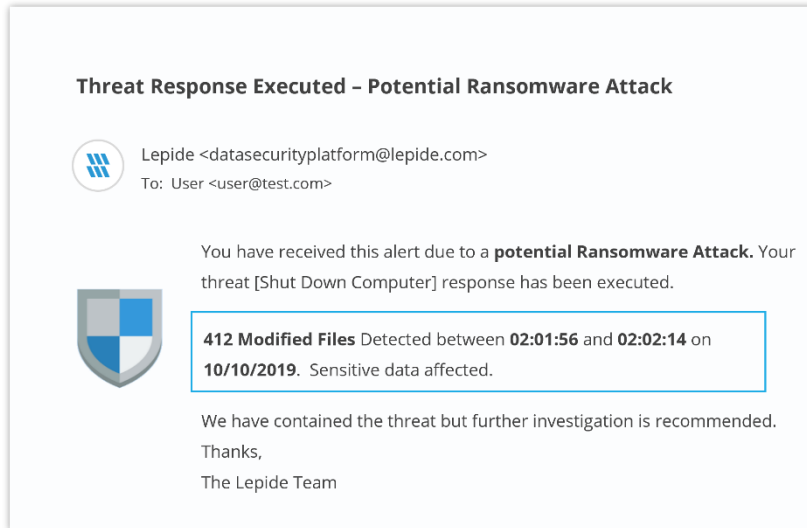


总之：

- 查看与数据的交互。
- 查看与管理数据访问的系统之间的互动。
- 员工审计日志。
- 调查事故和违规情况。

3.4. - Lepide Detect

机器学习支持的异常点发现技术可让您确定用户何时成为内部威胁。针对特定数据安全威胁定制的数百种威胁模型可在数据安全受到威胁时生成实时警报。可触发自动威胁响应，执行威胁缓解措施，如关闭受影响的计算机或服务器。



总之：

- 利用预定义的威胁模型实时检测威胁。
- 员工行为基准/档案。
- 识别异常员工行为。
- 实时预警和应对威胁。

HongKe



虹科电子科技有限公司

www.haocst.com
network@hkaco.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼1-7层

T (+86) 400-999-3848
M (+86) 135 3349 1614

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

版本：V1.0 - 23/09/07



联系我们



获取更多资料



haocst.com