

**HongKe**

虹科

启用指南

启用LEPIDE进行

# 远程办公管理

## 目录

1. 导言.....	3
2. 远程工作者调整 Lepide .....	3
3. Lepide核心能力 .....	6
3.1. - Lepide 识别 .....	6
3.2. - Lepide 信任 .....	7
3.3. - Lepide 审计 .....	8
3.4. - Lepide 检测 .....	9

---

# 1. 引言

我们可以帮助那些担心员工在家工作带来额外风险而影响敏感数据安全性的组织。73% 的安全团队认为，在家工作的员工比在办公室工作的员工构成的威胁更大。我们可以帮助减轻这些担忧。

我们为企业提供审计线索，跟踪每位员工对其最敏感数据采取的每项行动，并根据对特别敏感文件采取的具体行动实时发出警报。

利用我们的异常检测或威胁模型，我们可以识别可能标志着恶意员工或用户账户被入侵的行为。我们还能让企业跟踪登录和注销活动的时间/日期和趋势，并检测出可能意味着潜在威胁的异常趋势和异常情况。我们提供详细的审计跟踪，记录员工通过 MS Teams、OneDrive 和 SharePoint 在内部和外部通过 Exchange 共享的敏感数据。

# 2. 为远程工作者调整 Lepide

为了能够保护数据、检测威胁并遵守访问治理，您需要能够回答许多关键问题



在下表中，我们将Lepide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	监控在家工作时使用您的[敏感]数据的员工。	<ul style="list-style-type: none"><li>用户权限报告 (<a href="#">Lepide 信任</a>)</li><li>具有管理权限的用户报告 (<a href="#">Lepide 信任</a>)</li><li>公开资源报告 (<a href="#">Lepide 信任</a>)</li></ul>

		<ul style="list-style-type: none"><li> 数据分类 (<a href="#">Lepide 识别</a>)</li><li> 文件服务器修改报告 (<a href="#">Lepide 审计</a>)</li><li> SharePoint 在线修改报告 (<a href="#">Lepide 审计</a>)</li><li> OneDrive 修改报告 (<a href="#">Lepide 审计</a>)</li><li> MS Teams 修改报告 (<a href="#">Lepide 审计</a>)</li><li> 外部数据共享 0365 报告 (<a href="#">Lepide 审计</a>)</li><li> 非业主访问邮箱报告 (<a href="#">Lepide 审计</a>)</li><li> 文件重命名报告 (<a href="#">Lepide 审计</a>)</li><li> 读取失败报告 (<a href="#">Lepide 审计</a>)</li><li> 所有环境变化报告 (<a href="#">Lepide 审计</a>)</li></ul>
	跟踪员工复制的敏感数据。确保数据不会扩散	<ul style="list-style-type: none"><li> 文件复制报告 (<a href="#">Lepide 审计</a>)</li><li> 勒索软件威胁模型 (<a href="#">Lepide 检测</a>)</li><li> SharePoint 在线文档复制报告 (<a href="#">Lepide 审计</a>)</li><li> 大规模数据复制威胁模型 (<a href="#">Lepide 检测</a>)</li></ul>
威胁检测	在员工的 Active Directory 账户受到威胁时及时发现。	<ul style="list-style-type: none"><li> 暴力攻击威胁模型 (<a href="#">Lepide 检测</a>)</li><li> 潜在密码泄露威胁模型 (<a href="#">Lepide 检测</a>)</li></ul>

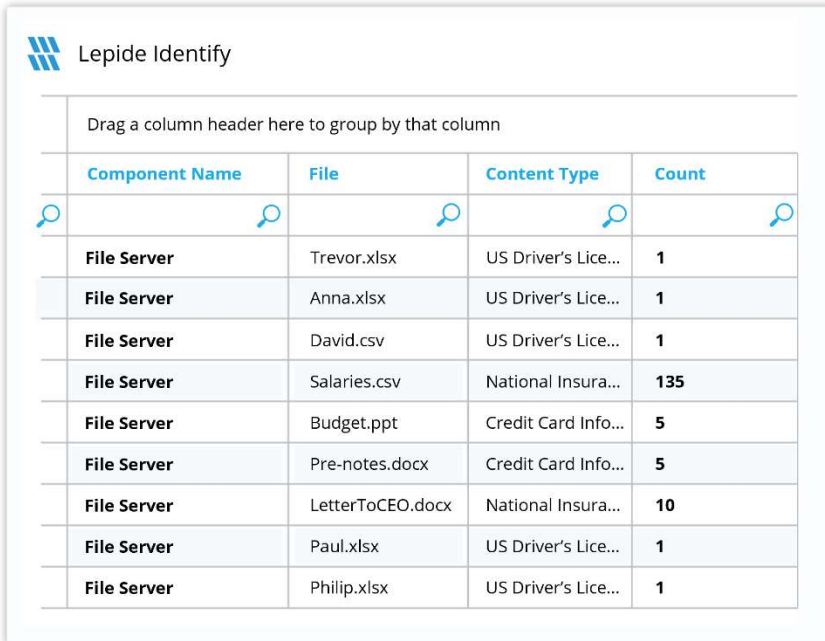
## 如何为远程工作人员启用 Lepide

		<ul style="list-style-type: none"><li> 异常点检测 (<a href="#">Lepide 检测</a>)</li><li> 活动目录权限修改报告 (<a href="#">Lepide 审计</a>)</li></ul>
	发现员工叛变的迹象	<ul style="list-style-type: none"><li> 所有环境变化报告 (<a href="#">Lepide 识别</a>)</li><li> 异常点检测 (<a href="#">Lepide 检测</a>)</li><li> 威胁模型 (<a href="#">Lepide 检测</a>)</li><li> 工作时间以外的活动报告 (<a href="#">Lepide 审计</a>)</li></ul>
	检测并响应通过 OneDrive、MS Teams 或 Exchange 共享的敏感数据。	<ul style="list-style-type: none"><li> 外部数据共享 O365 报告 (<a href="#">Lepide 审计</a>)</li><li> 使用自动脚本创建警报 (<a href="#">Lepide 检测</a>)</li><li> 文件修改报告 (<a href="#">Lepide 审计</a>)</li></ul>
准入管理	跟踪员工可以访问哪些敏感数据。	<ul style="list-style-type: none"><li> 不活动用户报告 (<a href="#">Lepide 审计</a>)</li><li> 用户权限过多报告 (<a href="#">Lepide 信任</a>)</li><li> 用户权限报告 (<a href="#">Lepide 信任</a>)</li><li> 具有管理权限的用户报告 (<a href="#">Lepide 信任</a>)</li><li> 公开资源报告 (<a href="#">Lepide 信任</a>)</li><li> 数据分类报告 (<a href="#">Lepide 识别</a>)</li></ul>

## 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 'Lepide Identify' with a logo. Below it, a text prompt says 'Drag a column header here to group by that column'. A table is displayed 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 信托基金会

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。

The screenshot displays the 'Lepide Trust' interface. It features a table of user permissions and a section for file access logs.

Account (Principal)	Effective Permission	🗨️	📄	📄	👤
Lpde1\jill	Full Control	✓	✓	✓	✓
Lpde1\Paul	Full Control	✓	✓	✓	✓
Lpde1\Bill	Full Control	✓	✓	✓	✓
Lpde1\Steve	Full Control	✓	✓	✓	✓

**Files in Folder : Accounts**

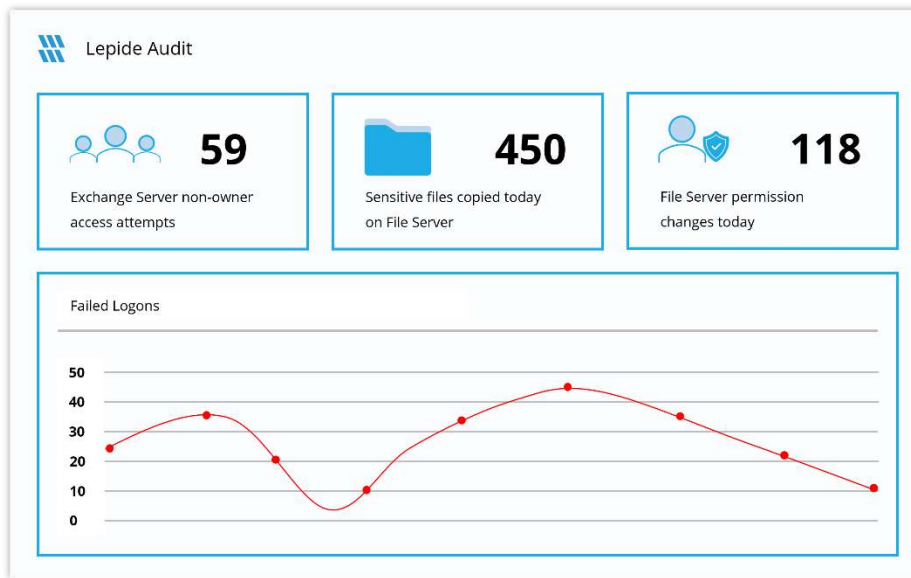
📄 Clients - Copy (2).txt	🔒 Credit Card - Visa + UK Phone	1 + 1 + 1 + 1 + 1
📄 Clients.txt.encrypt	🔒 Credit Card	100
🖼️ Customer details.png	👁️ No Sensitive Content	N/A
📄 Database.doc	🔒 Credit Card + SSN	100 + 500

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。



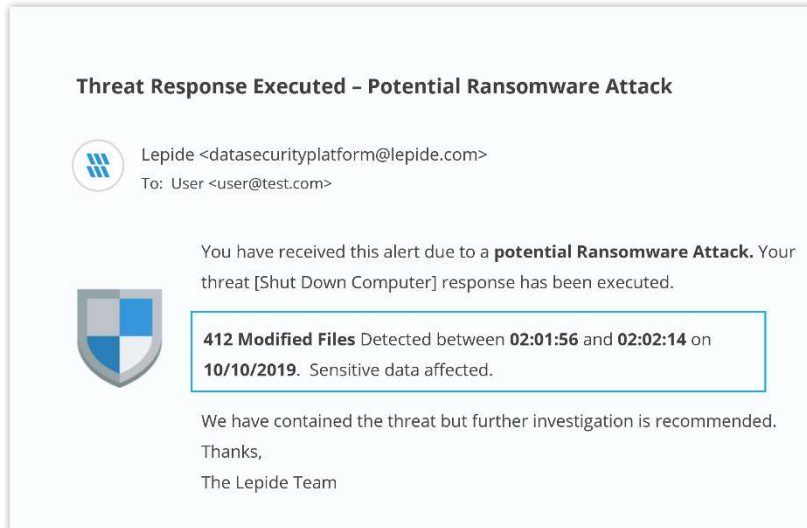
总之：

- 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