



启用指南

启用LEPIDE为

防止数据丢失

目录

1. 导言.....	3
2. 调整Lepide以防止数据丢失.....	3
3. Lepide核心能力	5
3.1. - Lepide 识别	5
3.2. - Lepide 信任	6
3.3. - Lepide 审计	7
3.4. - Lepide 检测	9

1. 引言

数据丢失防护是通过监控、检测以及在某些情况下阻止移动和静态敏感数据来检测潜在数据泄露的手段。虽然我们 Lepide 无法阻止数据通过 USB 或通过端点上的 Web 服务离开，但我们可以检测、警报和阻止敏感数据通过 MS Teams、OneDrive 和 MS Exchange 离开。与其他 DLP 供应商相比，在了解哪些数据是敏感数据、数据如何在企业内部移动以及如何在 Exchange、Office 365 (Teams/OneDrive) 之间移动方面，我们的知识水平使我们的 DLP 解决方案独一无二。

2. 调整 Lepide 以防止数据丢失

















这里有一些关键问题，您需要能够使 Lepide 适应数据丢失防护。








检测	调查	预防	响应
大规模复制和共享敏感数据，违反了公司政策	调查数据是否被外部分享，并获得关于用户对数据的操作的审计记录	减少员工能够访问的敏感非结构化数据的数量	在发现异常行为时，响应并封锁或锁定用户。实时应对勒索软件

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
检测	检测敏感数据的批量复制。	<ul style="list-style-type: none">  文件复制报告 (Lepide 审计)  海量数据复制(FS)威胁模型 (Lepide 检测)  海量数据复制(FS)威胁模型响应-禁用用户帐户 (Lepide 检测)
	构建警报，以便能够检测正在共享的违反公司政策的数据	<ul style="list-style-type: none">  外部数据共享警报 (Lepide 检测)  潜在数据丢失威胁模型 (Lepide 检测)

如何启用 Lepide 的数据丢失防护功能

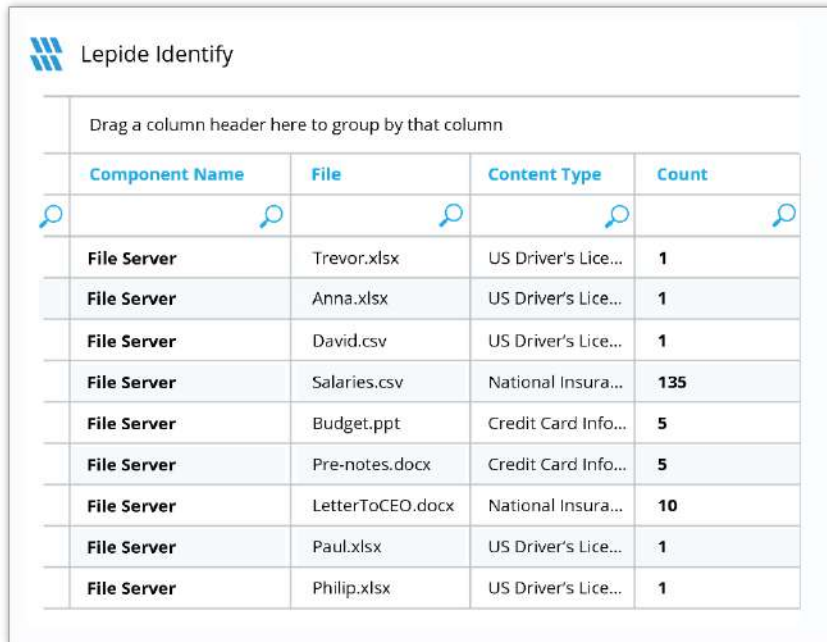
		 海量数据复制威胁模型 (Lepide 检测)  文件复制警报 (Lepide 检测)
调查	查看哪些敏感或受监管的数据正在通过 MS Exchange 内部或外部通过电子邮件发送	 潜在数据丢失威胁模型 (Lepide 检测)
	查看哪些敏感数据通过 Teams 或 OneDrive 对外共享	 Office 365 报表中的永久数据共享 (Lepide 审计)
	看看公司内部有哪些数据被复制了, 是谁在复制	 文件复制报告 (Lepide 审计)  海量数据复制 (FS) 威胁模型 (Lepide 检测)  文件服务器报告中的所有修改 (Lepide 审计)
	获取关于特定用户如何处理敏感数据的完整审计跟踪	 所有环境变化报告 (Lepide 审计)  所有修改报告-所有数据源 (Lepide 审计)
预防	如何减少我的员工可以访问的敏感数据的数量, 以降低风险	 非活跃用户报告 (Lepide 审计)  按用户报告的过多权限 (Lepide 信任)  按对象报告的过度权限 (Lepide 信任)  按用户报表划分权限 (Lepide 信任)  具有管理员权限的用户报告 (Lepide 信任)  公开股份报告 (Lepide 信任)  数据分类 (Lepide 识别)

		<ul style="list-style-type: none"> 增加威胁表面积威胁模型 (Lepide 检测) 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)
响应	如果发现异常行为，阻止或锁定用户	<ul style="list-style-type: none"> 从Lepide移动应用程序手动执行威胁响应 (Lepide 检测) 创建带有自动威胁响应的警报 (Lepide 检测)
	侦测勒索软件攻击的早期阶段，并采取行动，以防止资料外泄/被破坏	<ul style="list-style-type: none"> 勒索软件威胁模型(侦测及回应) (Lepide 检测)

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 prompt: 'Drag a column header here to group by that column'. The main content is a table with four columns: 'Component Name', 'File', 'Content Type', and 'Count'. Each column header has a magnifying glass icon. The table contains ten rows of data, all with 'File Server' in the 'Component Name' column. The 'File' column lists various files like 'Trevor.xlsx', 'Anna.xlsx', 'David.csv', 'Salaries.csv', 'Budget.ppt', 'Pre-notes.docx', 'LetterToCEO.docx', 'Paul.xlsx', and 'Philip.xlsx'. The 'Content Type' column shows categories like 'US Driver's Lice...', 'National Insura...', and 'Credit Card Info...'. The 'Count' column shows the number of occurrences for each file, ranging from 1 to 135.

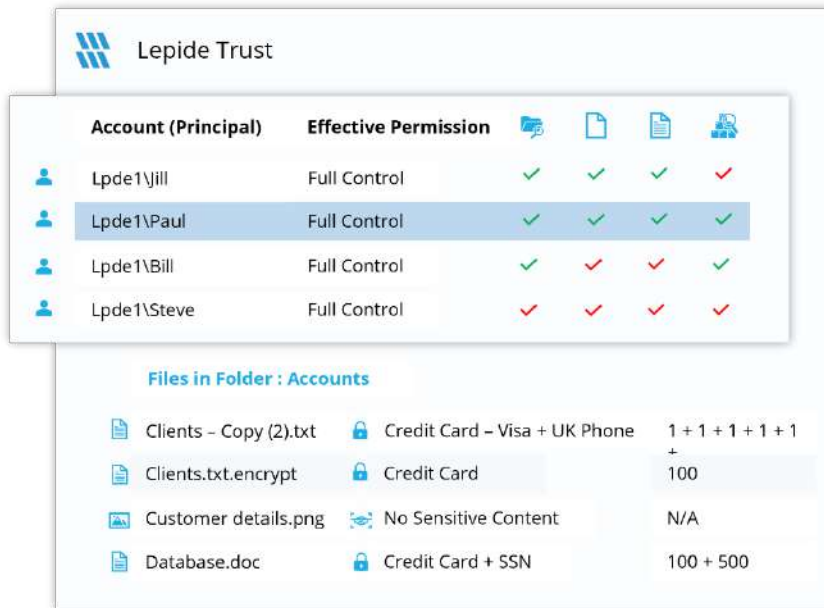
Component Name	File	Content Type	Count
File Server	Trevor.xlsx	US Driver's Lice...	1
File Server	Anna.xlsx	US Driver's Lice...	1
File Server	David.csv	US Driver's Lice...	1
File Server	Salaries.csv	National Insura...	135
File Server	Budget.ppt	Credit Card Info...	5
File Server	Pre-notes.docx	Credit Card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



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量身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