HongKe 虹科

实施指南

启用LEPIDE 进行

数据访问治理

目录

1. 导言

数据访问治理（DAG）是指确保只对需要访问的数据进行访问，并确保此后对此类访问进行检查和监控的过程。

也称为 DAG，市场上有一整套单独的解决方案来解决这个问题，不过，我们有一个非常实际的解决方案，

可以为实现这一目标的组织提供很多价值。

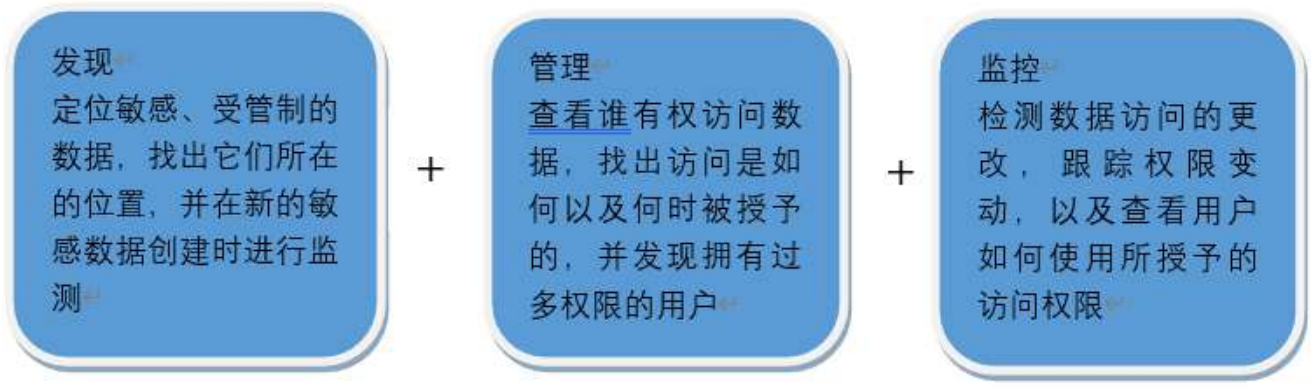
我们的解决方案可帮助企业确定其最敏感数据的位置，显示谁拥有访问权、访问权是如何授予的、拥有何种级别的访问权，以及权限的使用方式和时间，即他们是否正在使用他们有权访问的文件。

从安全角度来看，对这些领域的管理和洞察不力会导致不必要的风险。由于我们比其他任何安全厂商都更了解

Windows 文件系统，因此我们能够提供其他安全厂商无法提供的治理价值。

2. 调整 Lepide 以实现数据访问治理

要发现、管理和监控数据访问，您需要回答一些关键问题。



在下表中，我们将 Lepide 技术与这些问题进行了对比：

类别	应采取的行动	实施技术
发现	查看何时创建新的敏感数据。	数据分类（Lepide 识别） 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） 增加威胁表面区域威胁模型（Lepide 识别） 文件服务器报告中的所有修改（Lepide 审计）
治理	查看谁能访问什么。	用户权限报告（Lepide 信任） 非活跃用户报告（（Lepide 审计） 用户权限过多报告（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） 对象报告权限（Lepide 信任）
	找出授予访问权限的方式	用户权限报告（Lepide 信任） 对象报告权限（Lepide 信任） 用户管理权限报告（Lepide 信任
	查看何时授予数据访问权限	权限修改报告-所有数据源（Lepide 信任） 历史权限分析报告（Lepide 信任）
	查看访问未被使用的敏感数据的用户	用户过度权限报告（Lepide 信任） 对象报告权限过大（Lepide 信任）

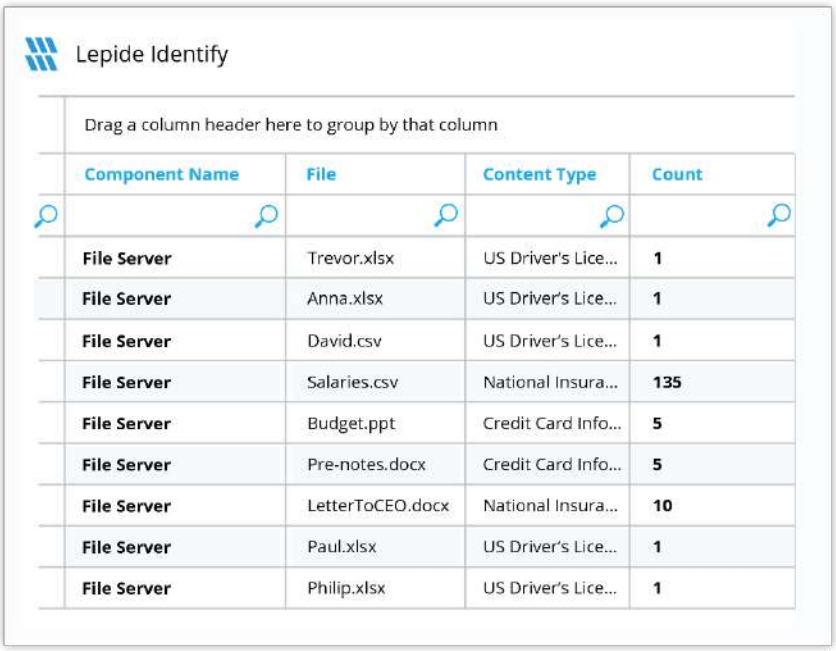
监管	在敏感数据访问权限发生变化时进行检测	权限修改报告 (Lepide 信任) 当前权限分析报告 (Lepide信任) 历史权限分析报告 (Lepide信任) 任何权限更改威胁模型 (Lepide检测)
	看看你最敏感的数据在哪里，为什么敏感	数据分类 (Lepide识别) 机密邮件报告 (Lepide 识别) 分类SharePoint对象报告 OneDrive分类对象报告 (Lepide 识别) 分类DropBox对象报告 (Lepide 识别)
	跟踪许可蔓延	用户过度权限报告 (Lepide 信任) 对象报告权限过大 (Lepide 信任) 用户管理权限报告 (Lepide 信任) 历史权限分析报告 (Lepide信任) 用户权限报告 (Lepide 信任) 对象报告权限 (Lepide 信任) 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) 权限修改报告-所有数据源 (Lepide 审计)
	查看用户如何利用他们被赋予的数据访问权限	用户过度权限报告 (Lepide 信任) 对象报告权限过大 (Lepide 信任) O365报告外部数据共享 (Lepide 信任) 文件服务器报告中的所有修改-所有数据源(Lepide 审计)

3. Lepide 核心能力

3.1. - Lepide 识别

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。

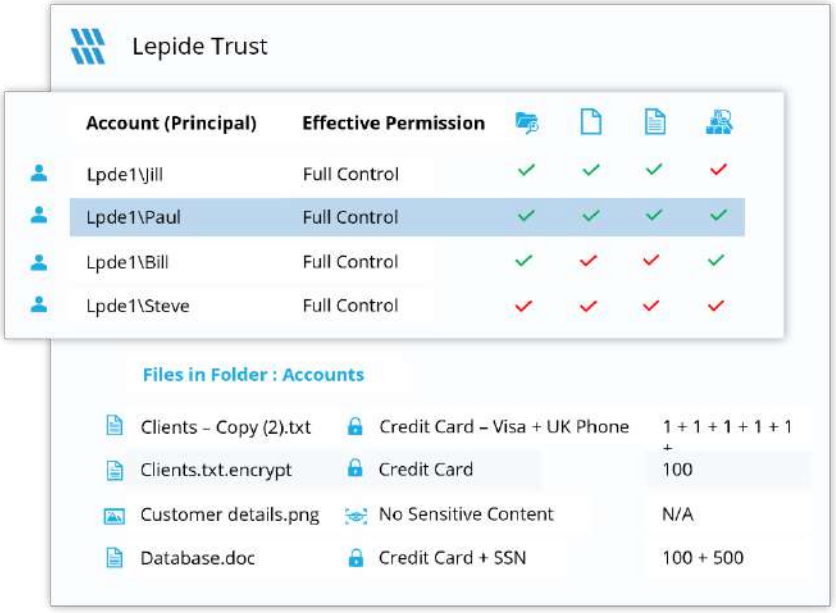


总之:

- 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

报告谁有权访问最敏感的数据，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。
- 识别权限过大的员工（权限最小）。
- 查看历史许可。
- 跟踪权限更改。

3.3. - Lepide 审计

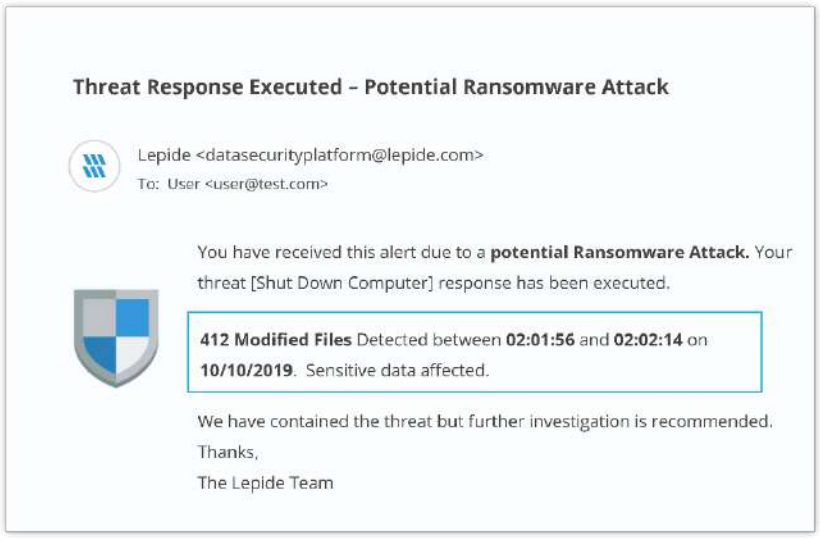
对敏感数据和混合环境所做的更改进行审计、报告和警报。回滚不需要的更改并恢复已删除的对象，以维护系统的完整性。跟踪用户对关键文件和文件夹所做的任何更改和修改。

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 检测

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

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