入门
Ransomware Protection

NetApp
July 19, 2022

目录

入门

了解勒索软件保护

勒索软件攻击可能会耗费业务时间，资源和声誉。通过勒索软件保护服务、您可以查看有关网络安全的相关信息、并评估您的组织对网络攻击的抵御能力。此外，它还会为您提供一系列警报和修复措施，帮助您提高数据的安全性。

"了解勒索软件保护的用例"。

勒索软件保护服务目前为测试版产品。

功能

勒索软件保护提供了单一的可见性和控制点、可用于管理和完善不同工作环境和基础架构层的数据安全性、以便更好地应对发生的威胁。它目前提供多种功能、可帮助您保护网络存储。将来还会添加其他功能。当前功能可确定何时执行以下操作：

- 工作环境中的卷不会通过定期创建 Snapshot 副本来受到保护。
- 工作环境中的卷不会通过使用创建云备份来受到保护 "云备份"。
- 您的工作环境和数据源中的数据不会使用进行扫描 "云数据感知" 确定合规性和隐私问题，并寻找优化机会。

  从勒索软件保护角度来看、此功能也很重要、因为它可以让您更好地了解重要(敏感的业务关键型)数据的位置、从而确保您将保护重点放在这些数据上。

- 如果您因勒索软件攻击而需要恢复、则不会备份您最重要的数据类别。
- 工作环境或数据源中加密文件的百分比异常增加。

  这可能表明您的网络上已开始勒索软件攻击。

- 在文件中发现敏感数据，并且在工作环境或数据源中访问权限级别过高。
- 用户已添加到 Active Directory 域管理员组。
- 集群上的 ONTAP 软件版本较旧，应进行更新以提供最佳的保护和安全功能。
- ONTAP 系统未启用 NAS 文件系统审核。

  启用 CIFS 审核会为系统管理员生成审核事件，用于跟踪文件夹权限更改，读取或写入文件失败尝试以及创建，修改或删除文件的时间等信息。

- 您的 ONTAP 系统未启用机载反勒索软件功能。

  ONTAP 反勒索软件功能可以主动检测并警告可能指示勒索软件攻击的异常活动。

"请在勒索软件保护信息板中查看如何查看这些潜在问题。"

使用 Cloud Volumes ONTAP 系统时，您可以直接从工作环境中部署一些额外的勒索软件保护。 "了解如何针对勒索软件添加额外保护"。

支持的工作环境和数据源

"云数据感知" 是使用勒索软件保护服务的前提条件。安装并激活 Data sense 后，您可以使用勒索软件保护来查看数据在以下类型的工作环境和数据源上受到网络攻击时的弹性：

- 工作环境： *
- Cloud Volumes ONTAP （部署在 AWS ， Azure 或 GCP 中）
- 内部 ONTAP 集群
- Azure NetApp Files
- 适用于 ONTAP 的 Amazon FSX
- Amazon S3
- 数据源： *
- 非 NetApp 文件共享
- 对象存储（使用 S3 协议）
- 数据库(Amazon RDS、MongoDB、MySQL、Oracle、PostgreSQL、 SAP HANA、SQL Server)
- OneDrive 帐户
- SharePoint 帐户
- Google Drive帐户

勒索软件保护还会监控您的全局 Active Directory 配置（如果有） "已在 Cloud Data sense 中配置此配置"。

勒索软件保护的工作原理

总体而言，勒索软件保护的工作原理如下：

1. 勒索软件保护会从您的存储系统、云数据感知、Cloud Backup以及其他Cloud Manager资源中收集信息、以填充勒索软件保护信息板。
2. 您可以使用勒索软件保护信息板来简要了解您的系统受到的保护程度。
3. 您可以使用提供的报告工具帮助您保护网络存储。

成本

在测试期间，勒索软件保护服务不会单独产生成本。