DELL Technologies

数据表

适用于对象数据的 ECS 网络保护解决方案

网络攻击已成为各种规模的企业和垂直领域持续面临的一项严峻威胁。每 11 秒钟就发生一起网络攻击[1]，一次攻击造成的平均损失为 1300 万美元[2]，而且这个数字还在不断增长。网络攻击会扰乱运营、损害声誉，并可能导致与数据保护法规相关的法律诉讼。虽然完全规避不现实，但 IT 组织可以做很多工作来显著提高系统的网络弹性，以保护业务关键型数据和设置系统，从而更快地恢复业务运营。

阅读本概述，了解戴尔 ECS 网络保护解决方案何以成为卓越的适用于对象数据的网络安全对象存储解决方案。[3]

参考资料：

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://www.accenture.com/zh-cn/insights/security/cost-cybercrime-study

[3] 基于 2022 年 9 月戴尔对戴尔 ECS 与同类产品提供的网络安全软件功能进行的比较分析。

适用于对象数据的 ECS 网络保护解决方案

对象数据会成为网络攻击者的下一个前沿阵地。除了需要对象存储的现代应用程序正在迅速增多，大量备份数据和法律合规数据也使用对象存储。应用程序服务器通常将身份验证密钥存储在磁盘上，使得这些应用程序主机成为显而易见的攻击目标。攻击者只需一个密钥和几行 Python 代码，即可获得对象数据，进而可以访问海量的数据。更糟糕的是，任何安全工具都不会监控对对象数据的访问，导致这类攻击不会被察觉。Dell Technologies 正在与 Superna 合作推出全面的零信任功能，以针对对象存储进行网络攻击检测、防护和恢复。零信任方法是一种经验证可用于保护应用程序和数据免遭各种网络攻击的方法，它构成了基于安全框架（例如 NIST 的安全框架 [https://www.nist.gov/cyberframework]）的网络安全策略的基础。

网络攻击

每**11 秒**[1] 发生一次

据估计，美国联邦机构遭受网络攻击的平均成本为

1,370 万美元[2]

Dell Technologies 对象数据解决方案

利用智能安全隔离 Air Gap 技术进行隔离

强大的网络弹性策略涉及使用数据保护方面的所有最佳实践：正确级别的访问控制、不可变的数据拷贝、防病毒和反恶意软件。除了这些功能之外，Ransomware Defender 还提供了行之有效的保护方式，那就是将数据拷贝放置在与生产环境隔离的网络存储区中。数据最初复制到网络存储区后，生产环境与存储区拷贝之间会保持网络阻断。要进一步进行增量复制，只能在确保没有已知事件表明生产站点上存在安全漏洞后，通过关闭网络阻断来间歇性地完成。

生产站点

Cyber Recovery 数据避风港存储区

参考资料：

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://www.accenture.com/zh-cn/insights/security/cost-cybercrime-study

检测：实时检测可疑的数据访问活动

对于任何网络安全框架而言，检测和早期响应都是重要的组成部分。Ransomware Defender for Dell PowerScale 已迅速成为 IT 和安全团队不可或缺的工具，利用它可以针对勒索软件攻击进行检测、防护和快速恢复，从而保护 PB 级业务关键型文件数据。目前，Dell Technologies 正携手 Superna 将这项技术应用于对象存储。通过向客户提供实时检测攻击事件的全面功能，Eyeglass Ransomware Defender for Dell ECS 实现了 S3 原生实时数据保护。基于行为的对象数据访问分析可实现对象数据的零信任保护。

学习模式

人工智能和机器学习是应用于网络安全的关键技术。Ransomware Defender 带有学习模式，可帮助建立安全访问基准，这种基准可能随不同应用程序而异。随着时间的推移，系统能够更准确地检测可疑的数据访问行为并最大限度减少误报。

应用程序白名单

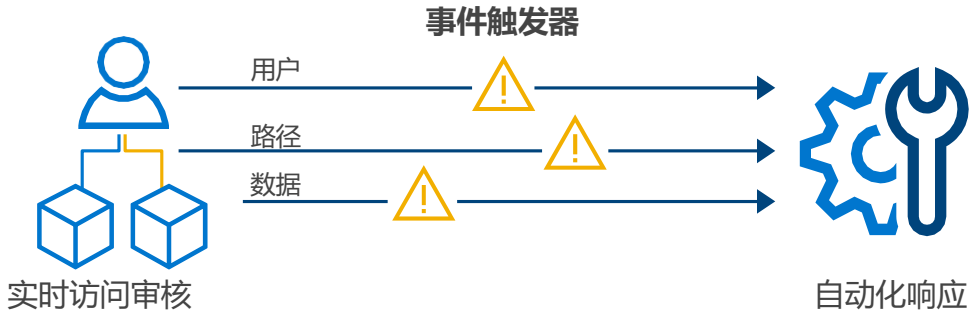
白名单功能是基于零信任的方法的关键组成部分，它允许经验证的名单中的应用程序和网络配置对数据进行独占访问。借助 Ransomware Defender，安全管理员可以保存一份名单，允许特定对象存储区、用户帐户和服务器 IP 地址访问特定对象数据。

自动化响应

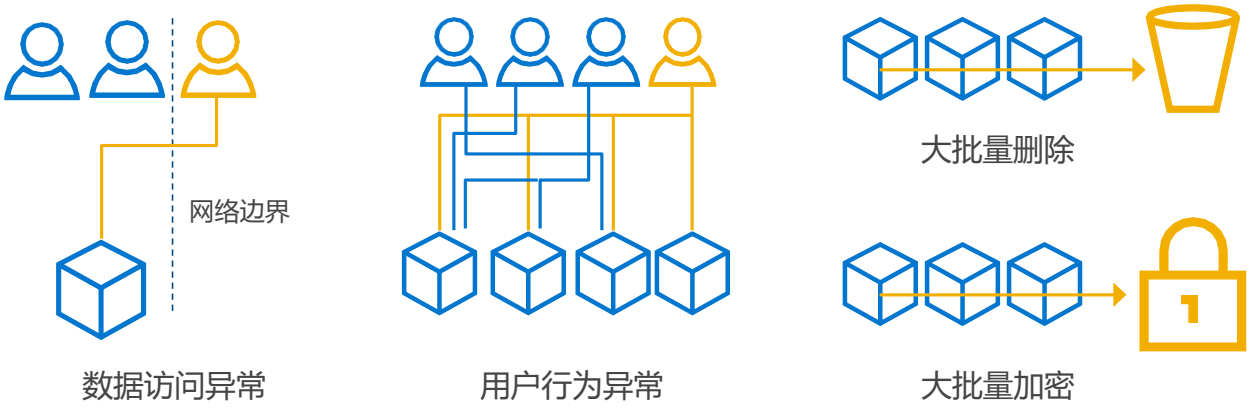
Ransomware Defender 提供了响应攻击事件的一系列选项。发现异常数据访问行为时，管理员会收到相应的提醒。可对系统进行配置以允许实现从仅监控到立即锁定用户等多种多样的自动化响应。利用与 ECS 的 API 集成，可以撤销访问密钥来阻止攻击，并通过追踪遭破坏的对象，帮助管理员使用 ECS 对象版本控制功能从原先的版本进行恢复，从而加快数据恢复。

安全防护下的渗透测试

在检验针对网络攻击而建立的防御体系时，渗透测试可谓是一种最佳实践。Ransomware Defender 提供了自动化渗透测试来确保防御体系行之有效。渗透测试日志使管理员可以轻松查看安全防御体系的运行状况，并针对失败的渗透测试生成警报。



可检测到的模式示例



运营和数据恢复

遭网络攻击后的恢复工作涉及识别遭破坏的数据、用户帐户以及发起攻击的客户端 IP。Ransomware Defender 可提供这方面的信息，以帮助管理员隔离被感染的对象存储区和命名空间。Ransomware Defender 提供受损对象数据和 S3 存储区的列表，可实现精确的数据恢复。这可加快恢复速度，以尽快让系统重新投入运行，同时还能提供一系列事后补救措施来修补安全漏洞，从而强化系统环境以应对日后的攻击。借助 ECS 的 S3 兼容版本，可以使用已知良好的对象数据版本来还原受影响的数据。

保护

ECS 的固有 S3 兼容安全功能

1. 面向 ECS 的 S3 对象锁

从 ECS 2.X 开始，Dell EMC ECS 就支持基于 WORM（一次写入，多次读取）的保留功能。为了对更多的应用程序提供更高的兼容性，ECS 现在支持对象锁功能（从 ECS 3.6.2 开始），兼容 Amazon S3 对象锁的功能。对象锁也被设计为满足法规遵从性要求，例如 SEC 17a4(f)、FINRA 第 4511(c) 条规则和 CFTC 第 17 条规则。

对象锁可防止对象版本在用户定义的保留期限内被删除。不可改变的 S3 对象利用 WORM 的存储区级配置及保留属性获得保护。保留策略使用 S3 API 或存储区级默认设置进行定义。对象在保留期限内处于锁定状态，并且也支持合法保留方案。

单击此处了解有关 ECS 对象锁定的更多信息

2. S3 身份和访问管理

借助 ECS 身份和访问管理 (IAM)，您可以安全地对 ECS S3 资源进行细粒度访问。此功能可确保识别、验证和授权对 ECS 资源的每个访问请求。ECS IAM 允许您添加用户、角色和组。您还可以通过向 ECS IAM 实体添加策略来授予和限制访问权限。

单击此处详细了解 ECS IAM

3. S3 版本控制

通过 ECS 上的 S3 版本控制，您可以在同一存储区中保留一个对象的多个变体，以保护数据，并在发生意外丢失（包括意外、灾难或网络攻击）的情况下实现快速恢复。如果需要较旧版本的对象，您可以通过 ECS S3 API 检索或将其还原到以前的版本。此外，通过在 ECS 对象锁定中启用存储区级版本控制，您可以在特定保留期内锁定对象版本（支持治理和法规遵从性场景），或无限期锁定对象版本（满足法律封存要求）。

单击此处详细了解 ECS 版本控制

了解有关戴尔 ECS 企业对象存储的更多信息

详细了解戴尔 ECS 平台

在 Twitter 上关注 Dell Storage

联系 Dell Technologies 销售或支持专家

DELL Technologies