Dell PowerProtect Backup Services 助力加快从勒索软件攻击中恢复

只需数小时即可从勒索软件攻击中恢复，而无需耗费一天时间

重要功能

勒索软件攻击愈发频繁，手段更加先进，造成的代价也愈发高昂

- 无法快速识别和还原未受感染的备份或文件
- 感染扩散，恢复数据再次受到感染
- 数据丢失，无法恢复完整的数据集
- 难以协调事件响应编排
- 需要缩短 RPO/RTO 时间
- 代价高昂的业务中断造成收入损失和品牌声誉受损
- 数据保护力度不足导致面临法律和监管罚款

难题

勒索软件对每个企业都造成了严重威胁。网络攻击愈发频繁，并可能会使企业蒙受灾难性损失。79% 的组织担心他们将在未来 12 个月内经历中断性事件 1。灾难发生后，丢失数据的公司将面临宣告破产的风险。勒索软件攻击不仅变得愈发频繁，而且采用的技术更加先进，造成的代价也愈发高昂。

解决方案

快速可靠地进行恢复后，企业将没有任何理由再考虑支付赎金。但是，在发生安全事件或网络攻击时，组织需要先了解其影响范围和根本原因，然后再进行恢复。凭借全天候可用的工作负载和虚拟机原始安全隔离快照、对用户和数据异常的持续监视、与安全工具的集成以及自动恢复干净数据的功能，您可以改善安全态势，并将毁灭性的攻击转变为可应对的事件。

功能

针对所有工作负载：

• 确保全天候提供不可变的安全隔离备份

• 在本地或云中恢复干净数据，RPO/RTO 仅为数小时，而无需数天或数周

• Managed Data Detection and Response (MDDR) 服务可全天候实时监视备份环境

• 还原所有 AWS 区域/账户中的工作负载和虚拟机。当使用来自生产部门的数据、创建多个拷贝并将其存储在多个位置时，会给您的组织带来巨大风险。

加快关键工作负载从勒索软件攻击中恢复：

• 使用基于 ML 的算法监视和主动检测异常

• 通过集成 SIEM 和 SOAR 来编排响应和恢复活动

• 在恢复之前对快照进行恶意软件扫描，并从备份中删除受感染的快照和文件

• 在指定时间范围内从黄金快照自动恢复每个文件的全新干净版本

保护

要防止勒索软件造成损害，首先要确保拥有不可变的安全隔离数据拷贝。Dell PowerProtect Backup Services 基于高弹性云基础架构而构建，可防止勒索软件加密备份数据。零信任体系结构（包括多因素身份验证、信封加密和独立的账户访问）可确保勒索软件无法使用遭到泄露的主环境凭据来篡改备份环境或数据。最后，防止过度删除的功能和软删除（回收站）功能增加了一层安全保护，可保护备份免遭删除。

检测

尽快检测勒索软件攻击可帮助事件响应团队做出响应，并防止感染扩散。Dell PowerProtect Backup Services 助力加快从勒索软件攻击中恢复的模块提供了一个安全命令中心，用于监视备份环境的态势。凭借访问见解和异常检测，您可以快速识别整个环境和所有数据中发生的异常活动。查看用户和 API 进行的所有访问尝试的位置、身份和活动信息。使用专有的 ML 算法检测异常，这种算法可针对异常的数据活动（例如，删除、加密等）提供警报。该算法会学习特定备份环境的模式，因此无需设置任何规则或进行调整。它还使用基于熵的见解来减少误报

响应

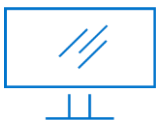
当安全或 IT 分析师检测到可疑事件，或者在更糟糕的情况下，确认已发生勒索软件事件时，快速响应至关重要。有许多主要的环境安全工具很有价值，可用于进行检测和响应编排，但您也可以使用辅助数据（备份系统）中的分析和变更日志数据来改进调查、响应和取证活动。Dell PowerProtect Backup Services 助力加快从勒索软件攻击中恢复的模块提供了强大的现成 API 集成，可帮助您轻松将解决方案融入整个安全生态系统。使用 SIEM 和 SOAR 解决方案编排响应活动可自动完成相关操作，例如根据预先确定的勒索软件手册隔离受感染的系统或快照，或者对备份进行 IOC 扫描。这可以显著缩短平均响应时间 (MTTR)。

恢复

经过初始响应阶段后，就需要努力进行恢复了。对于许多公司来说，这是一个手动过程，非常耗时。恶意行为者和勒索软件的驻留时间从数周到数月不等，因此企业很难知晓要回溯到多久之前，才能找到干净数据。 即使确定了理想的快照，隐藏的恶意软件也可能导致再次感染。不过，大多数企业用户都无法接受将恢复点设为 2 周前。然而，在勒索软件事件发生后，需要手动查找和验证日期更近的数据，这项工作十分繁琐，通常难以完成。

凭借有效的备份体系结构和自动化工具，Dell PowerProtect Backup Services 可加快恢复，从而减轻这一负担。Dell PowerProtect Backup Services 云平台将工作负载直接备份到云，以便在发生勒索软件攻击时即时恢复。

助力加快从勒索软件攻击中恢复的模块可确保恢复数据安全、干净，让您放心无忧地完成恢复。您可以使用内置的防病毒检测功能，或者利用来自自己的取证调查或威胁情报源的威胁情报，对快照进行恶意软件和 IOC 扫描。在恢复之前扫描快照可以防止再次感染。



详细了解 PowerProtect Backup Services

联系方式 Dell Technologies 专家