DELL Technologies

解决方案简介

集成多云数据服务的 Dell EMC PowerProtect Cyber Recovery 数据避风港

支持多云的 Cyber Recovery 数据避风港服务

可信赖且安全

- 物理和逻辑隔离的存储区环境，通过运营性网络阻断与企业网络断开
- 在安全的异地存储区中保留不可变数据副本，从而维护数据完整性
- 智能分析在存储区中提供机器学习和完整内容索引编制

经济高效

- 核心存储区基础架构作为服务交付
- 通过可用的高带宽、低延迟直接连接方式连接到公有云提供商
- Microsoft Azure 和 Oracle Cloud 的出口费用为零

使用方便，性能不打折扣

- 保护驻留在云或本地部署中的关键数据
- 将数据无缝还原到任何公有云提供商
- 在不影响安全性的情况下获得云的灵活性和便利性

适用于本地和云部署的 Cyber Recovery 数据避风港

每时每刻，勒索软件和其他复杂的网络攻击都可能会窃取或破坏企业的重要资产 — 他们的数据。这可能会导致收入损失、声誉受损和高额的监管罚款。保护您的关键数据并以经过验证的数据完整性进行数据恢复，是在攻击后恢复正常业务运营的关键。

混合和多云环境提供运营灵活性、快速扩展的能力以及获得创新服务和硬件的能力。但是，跨多个云分散和复制数据的方法可能会导致新的安全和合规风险、潜在的同步问题以及更高的资源成本。这种方法还会降低您对各种环境的了解程度，从而导致无法充分抵御当今不断变化的网络威胁。需要一种更好的方法让公有云提供商能够同时访问您的数据而不影响安全性，让您能够自由地选择任何云提供商并避免供应商束缚。

随着您将更多工作负载和数据迁移到云中，无论您的数据位于何处，都必须为关键数据投资网络保护解决方案。Dell Technologies 提供安全的数据存储区和智能分析，可保护您的关键数据免受网络攻击、勒索软件和内部威胁的侵害。

支持多云的 Cyber Recovery 数据避风港

使用由 Faction 提供支持的 Dell EMC PowerProtect 多云数据服务来设置 Cyber Recovery 数据避风港存储区非常简单。这种安全的数据保管服务是一种逻辑上网络阻断的存储区，它建立在支持多云的安全基础架构之上，可保护您的关键数据免受网络攻击的侵害。当需要恢复数据时，您可以选择将数据从存储区还原到 AWS、Microsoft Azure、Google Cloud、Oracle Cloud，或还原到您的本地环境。

CyberSense 智能分析与这种 Cyber Recovery 数据避风港服务完全集成，采用独特的方法来发现网络攻击、观察数据如何随时间变化并使用分析来检测勒索软件导致的损坏迹象。这种方法通过验证在 Cyber Recovery 数据避风港存储区中异地保护的数据的完整性，提供额外一层保障。

集成多云数据服务的 Dell EMC PowerProtect Cyber Recovery 数据避风港安全体系结构

安全存储区环境包括适用于 Dell EMC PowerProtect 系统的多云数据服务，可用作您的主要 Dell EMC PowerProtect DD 或 Dell EMC PowerProtect DD Virtual Edition (DDVE) 系统的复制目标。专用计算资源运行 Cyber Recovery 数据避风港管理工具和任何 CyberSense 分析工具。结合存储区的物理安全性和隔离，该解决方案包括一个运营性网络阻断，该网络阻断仅允许在将数据从主系统复制到存储区所需的时间段内访问存储区，即便如此，访问也受到严格限制。在其他情况下，存储区与客户端的生产环境断开连接。在 Faction 数据中心托管的 Cyber Recovery 数据避风港存储区中创建用户选定数据的不可变副本。一旦选定数据的副本安全地存放在安全、隔离的存储区中，在规定的时间内将无法改动、删除或以其他方式更改数据。CyberSense 分析具有机器学习和完整内容索引编制功能，可在存储区的安全保障下分析每个数据集。

保护现有 Dell EMC PowerProtect 多云数据服务部署

与 Dell EMC PowerProtect 多云数据服务结合使用时，客户可以跨所有云（AWS、Google Cloud、Oracle 和 Azure）实现主权数据保护，然后能够在安全的 Cyber Recovery 数据避风港存储区中保护其关键数据。Dell EMC PowerProtect 多云数据服务可用作多用途系统：云原生应用程序数据的备份目标或现有 PowerProtect 系统的复制目标。Cyber Recovery 数据避风港存储区是一个附加选项，可以轻松添加，以将关键数据与网络攻击隔离并验证数据完整性。

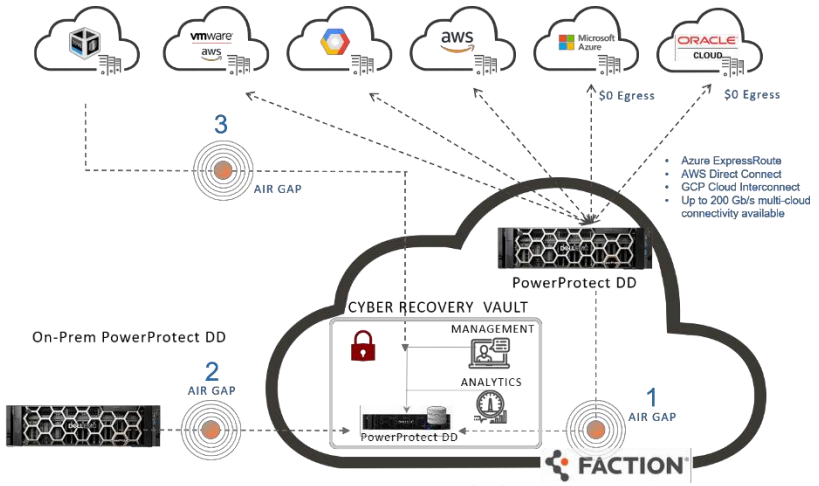

图 1 — Dell EMC PowerProtect 多云数据服务应用场景

1. 保护现有 Dell EMC PowerProtect 多云数据服务部署
2. *保护客户场所的数据*
3. *保护公有云中的数据*

保护客户本地数据

客户可以将数据从本地 PowerProtect DD 复制到 Faction 某一数据中心的 Cyber Recovery 数据避风港存储区。当组织的生产或主要备份遭到破坏或者灾难恢复位置遭到入侵或感染时，这为组织提供了更好的恢复机会。如果发生网络攻击，他们可以快速识别远程 Cyber Recovery 数据避风港存储区中最新的干净数据副本，并在本地恢复关键系统，或者如果他们的服务设计有恢复到云端的功能，还可以选择恢复到云端。

保护公有云中的数据

对于已经使用 PowerProtect DDVE（AWS、Google Cloud 和 Azure 支持的云中的虚拟备份目标）的云原生应用程序，Cyber Recovery 数据避风港存储区服务是一项可选服务，使客户能够将关键数据复制到安全的存储区中。

集成 CyberSense 的 Dell EMC PowerProtect Cyber Recovery 数据避风港

PowerProtect Cyber Recovery 数据避风港是完全集成 CyberSense 的解决方案，CyberSense 可以添加智能保护层，以便在攻击渗透数据中心时帮助发现数据损坏。这种创新方法提供了完整内容索引编制，并使用机器学习来分析超过 100 组基于内容的统计数据，检测由于勒索攻击造成的破坏迹象。CyberSense 的破坏检测成功率高达 99.5%，可帮助您识别威胁并诊断攻击载体，同时保护您的业务关键型内容，所有这些都在存储区的安全保障下进行。

Dell Technologies 数据保护解决方案 — 引领您的云之旅

您可以保护云中的关键数据，而不会影响完整性、机密性或可用性。集成多云数据服务的 Dell EMC PowerProtect Cyber Recovery 数据避风港可在单一目标位置可靠地保护您的关键数据，无论数据是托管在云中还是位于本地。有关详情，请从此处开始了解。

详细了解集成多云数据服务的 Dell EMC PowerProtect Cyber Recovery 数据避风港	联系 Dell Technologies 专家	了解云计算的更多信息数据保护和备份解决方案	