DELL Technologies

解决方案简述

戴尔 PowerProtect Cyber Recovery 数据避风港

针对勒索软件和破坏性网络攻击，为关键数据提供富有弹性的现代保护。

为什么选择 Cyber Recovery 数据避风港?

网络攻击的意图在于损害您的宝贵数据，包括您的备份。保护您的关键数据并以有保障的完整性来恢复数据，是在攻击后恢复正常业务运营的关键。

网络弹性解决方案包括以下组件：

数据不可变性
创建不可更改的数据副本，通过多层安全和控制保持数据完整性和机密性。

数据隔离和治理
与企业网络和备份网络相互断开的隔离恢复环境，以及更严格的用户访问控制。

自动化数据拷贝和安全隔离 Air Gap
在安全的数字存储区和流程中创建不可更改的数据副本，从而在生产/备份环境和存储区之间形成一个可操作的安全隔离 Air Gap。

智能分析
使用基于 AI 的机器学习和完整内容索引编制进行的自动化完整性检查，以及在安全存储区内进行的强大分析，用以确定数据是否受到恶意软件的影响。

恢复和修正
使用动态还原过程和您现有的灾难恢复程序在事件发生后执行恢复操作的工作流和工具。

解决方案规划和设计
提供专家指导，帮助选择关键数据集、应用程序和其他重要资产，以确定 RTO 和 RPO 并简化恢复。

挑战：网络攻击是数据驱动型企业的劲敌。

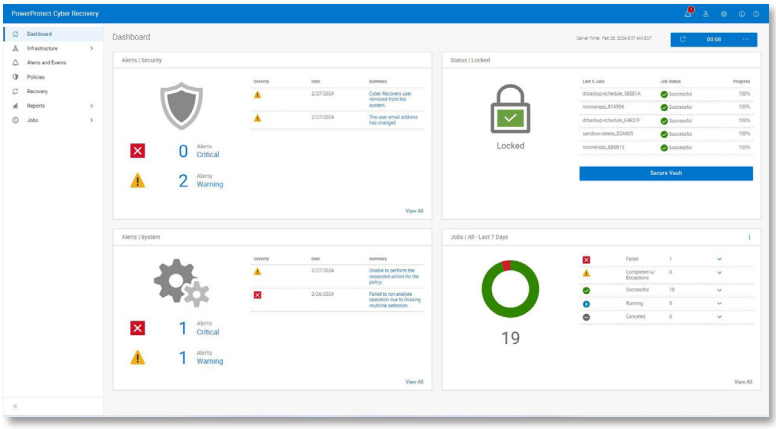
在数字经济中，数据就是货币，是一种必须加以保护、保密并且要确保可以随时访问的重要资产。数据在互连网络中能够畅通无阻，是现代化全球市场得以繁荣的必要条件。随着数字化转型计划的开展和生成式 AI 的日益普及，敏感信息被泄露的风险与日俱增。

这使您组织的数据成为对网络犯罪分子极具吸引力且有利可图的目标。无论处于哪个行业或者组织规模如何，网络攻击都会使企业和政府不断面临各种风险：数据泄露、因停机造成收入损失、声誉受损以及巨额监管罚款。

制定网络弹性战略已经成为企业和政府领导的职责所在，然而许多组织对他们的数据保护解决方案都缺乏信心。全球数据保护指数报告称，79% 的 IT 决策者担心他们将在未来 12 个月内经历中断性事件，75% 的决策者担心其组织现有的数据保护措施可能不足以应对恶意软件和勒索软件威胁[1]。

解决方案：戴尔 PowerProtect Cyber Recovery 数据避风港

为了降低网络攻击造成的业务风险，并制定更具网络弹性的数据保护方法，您可以对恢复和业务连续性战略进行现代化和自动化改造，并利用新的智能工具来检测和抵御网络威胁。



Dell PowerProtect Cyber Recovery 数据避风港提供经验证的现代化智能保护，可隔离关键数据、识别可疑活动、加快数据恢复，助您以更智能的方式恢复关键数据，从而快速恢复正常的业务运营。

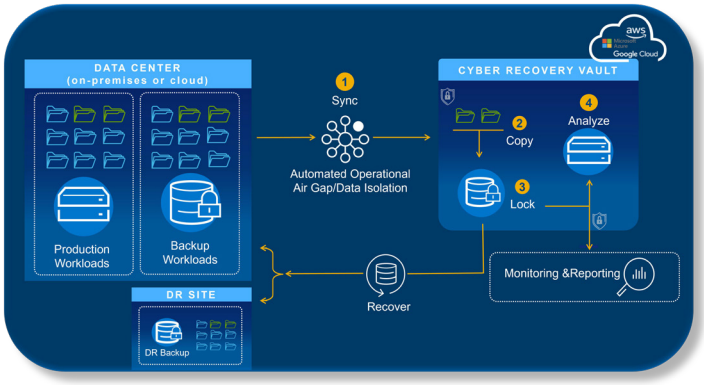
PowerProtect Cyber Recovery 数据避风港 — 不可变性、隔离和智能

不可变性 — PowerProtect Data Domain

PowerProtect Data Domain 是 PowerProtect Cyber Recovery 数据避风港的基础。它采用多层零信任安全性，可以提供不可变的备份副本，以确保数据的完整性和机密性。硬件信任根、安全启动、加密、保留锁、基于角色的访问和多因素身份验证等功能可助您确保数据的可恢复性。

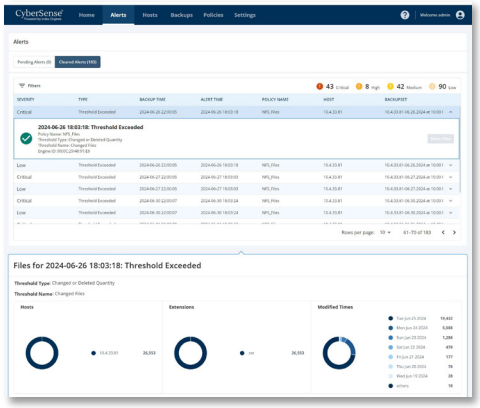
隔离 — Cyber Recovery 数据避风港存储区

PowerProtect Cyber Recovery 数据避风港存储区是隔离的恢复环境 (IRE)，具有多层保护，可提供应对网络攻击（甚至包括内部威胁）的抗风险能力。其可操作的安全隔离 Air Gap 会自动将关键备份数据副本从生产环境的受攻击面（包括开放系统和大型机）移动（同步）到物理隔离的存储区。将关键数据同步到存储区后，系统会自动创建一个不可变的副本，以防止数据被修改。除了独立于生产环境的专用管理、网络和服务，还需要提供单独的安全凭据并进行多因素身份验证，才能访问用于恢复和测试操作的数据。



智能 — CyberSense®

PowerProtect Cyber Recovery 数据避风港是较早实现对 CyberSense® 完全集成的解决方案，可针对网络威胁进行更智能的恢复，而且所有流程都在 Cyber Recovery 数据避风港存储区的安全环境中进行。CyberSense 并非仅限于元数据的解决方案，它会进行完整内容分析，以检测攻击发生后的数据损坏情况（准确率高达 99.99%[2]），并有助于进行智能而快速的恢复。



CyberSense 利用不可变的数据备份来观察数据在不同时间的变化，并利用基于 AI 的机器学习来检测遭到勒索软件攻击的损坏迹象。CyberSense 可检测核心基础架构（包括 Active Directory、DNS 等）、用户文件和数据库中由复杂攻击导致的批量删除、完全和部分加密以及其他可疑更改。您可以创建自定义的阈值警报。如果检测到数据损坏的迹象，警报控制面板和攻击后取证报告可帮助快速诊断攻击的规模和影响，包括识别可用于恢复关键系统的干净数据副本。

PowerProtect Cyber Recovery 数据避风港 — 部署选项

混合云和多云环境中的 Cyber Recovery 数据避风港

关键数据可能存在于企业中的许多不同位置，可能在本地，可能托管在不同的数据中心内，也可能位于全球的多个云和区域。当需要从网络攻击中进行恢复时，无论数据位于何处，都必须确保安全且无损。

PowerProtect Cyber Recovery 数据避风港可通过 *AWS*、*Microsoft Azure* 和 *Google Cloud* 的公有云市场获取和购买，以快速保护云中 Cyber Recovery 数据避风港存储区中的数据。PowerProtect Cyber Recovery 数据避风港可在生产系统与公有云中的 Cyber Recovery 数据避风港存储区之间自动执行关键数据同步。与基于云的标准备份解决方案不同，对管理接口的访问被网络控制措施锁定，需要单独的安全凭据和多因素身份验证才能访问。跨多个云散布和复制数据的做法可能会导致安全和合规风险、潜在的同步问题以及更高的资源成本。这种做法还会降低您对各种环境的了解程度，导致无法充分抵御不断变化的网络威胁。

采用多云数据服务的 Dell PowerProtect Cyber Recovery 数据避风港 由 Faction 提供支持，使公有云提供商可以同时访问您的数据，而不影响安全性，还允许用户自由选择任意云提供商，避免受制于特定的供应商。这种安全的数据存储服务是一种逻辑上安全隔离的存储区，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。

Dell APEX Protection Storage All-Flash for Cyber Recovery

随着关键数据的持续增长，快速高效地从网络事件中恢复的能力对于确保业务连续性和网络弹性至关重要。那些正在扩展关键数据管理的组织必须能够很好地从隔离的恢复环境（如 Cyber Recovery 数据避风港存储区）检索数据。Dell APEX Protection Storage All-Flash 基于软件定义的 PowerProtect Data Domain 版本，提供经过简化、节能且经济实惠的网络恢复解决方案，具有增强的 CyberSense 分析和快速恢复功能，可满足组织 SLA 要求。通过减少使用的硬件、空间和能源，组织可以加快数据访问速度，提高运营效率并确保数据完整性，最终缩短停机时间并降低总体维护成本。

PowerProtect Cyber Recovery 数据避风港 — 恢复业务运营

恢复和修正

PowerProtect Cyber Recovery 数据避风港可提供自动化还原和恢复流程，使业务关键型系统能够快速、可靠地恢复正常运行。恢复融入事件响应流程之中。发生事件后，事件响应团队将通过分析生产环境找出根本原因。CyberSense 提供攻击后取证报告，以便了解攻击的深度和广度，并提供损坏之前最后良好备份集的列表。然后，当准备好执行生产环境的恢复时，Cyber Recovery 数据避风港会提供执行实际数据恢复所需的管理工具和技术。

解决方案规划和设计

Dell Professional Services for Cyber Recovery 可以帮助您确定哪些业务关键型系统需要保护并可为相关的应用程序和服务创建依赖关系图，以及恢复运营需要哪些基础架构。咨询服务还可以生成恢复要求和设计备选方案，并确定分析、托管和保护数据所需的技术，以及业务案例和实施时间表。

结论

Sheltered Harbor 等行业计划一直在利用 PowerProtect Cyber Recovery 数据避风港来保护客户、金融机构以及公众对美国金融系统的信心，以避免发生导致关键系统（包括备份）崩溃的网络攻击。具备 CyberSense 功能的 Cyber Recovery 数据避风港拥有成千上万个客户，可以让业务经理安心无忧，而且事实证明，在发生网络威胁时，它可以加快数据的恢复速度。根据 Forrester Consulting 的研究，在发生网络攻击时，PowerProtect Cyber Recovery 数据避风港可将停机时间缩短 75%，将恢复时间缩短 80%。[3]

PowerProtect Cyber Recovery 数据避风港使您能够快速识别和还原已知良好的数据，并在网络攻击后快速恢复正常的业务运营。恢复运营，刻不容缓。

[1] 根据 Vanson Bourne 受 Dell Technologies 委托开展的研究《2024 年全球数据保护指数报告》。2023 年 10 月。
[2] 基于 Index Engines 委托撰写的一份 ESG 报告：《Index Engines’ CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption》。2024 年 6 月
[3] Dell Technologies 委托 Forrester Consulting 进行的研究，《The Total Economic Impact of Dell PowerProtect Cyber Recovery》，2023 年 8 月

详细了解 Dell PowerProtect Cyber Recovery 数据避风港

联系 Dell Technologies 专家

查看更多资源

加入 #PowerProtect 对话