DELL Technologies
戴 尔 科 技 集 团

技术白皮书

从破坏性网络攻击中恢复

利用戴尔 PowerProtect Cyber Recovery 数据避风港恢复业务生命线

摘要

网络攻击正在呈上升态势，复杂性与破坏性也与日俱增。事实上，2021 年网络犯罪造成的全球影响估计达 6 万亿美元[1]。勒索软件攻击不仅会让组织每天蒙受数百万美元的损失，还会损害其声誉并对股价产生负面影响。预计网络威胁将持续增加，居家办公和分布式工作环境更是加剧了这一趋势。

大多数组织已经具备强大的数据保护和检测能力。但是，如果攻击者突破防线，然后加密或擦除您的数据，贵组织能够恢复吗？此外，您对恢复数据的完整性又有多大把握？组织需要将恢复能力视为其网络弹性和风险管理战略的一环。本白皮书重点介绍了戴尔 PowerProtect Cyber Recovery 数据避风港如何保护和隔离关键数据，使其免受勒索软件和其他复杂威胁的侵害。

2022 年 2 月

[1]Cybersecurity Ventures：https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

目录

执行摘要

无论哪种行业、组织规模如何，网络攻击都呈现上升态势。事实上，据 Cyber Security Ventures 估计，每 11 秒钟就有一次网络或勒索软件攻击。[1]攻击几乎永不停歇，每次攻击造成的损失也在不断上升，Accenture 估计，网络犯罪给组织造成的平均损失为 1,300 万美元。[2] 随着组织对威胁其任务关键型运营及其声誉的网络安全风险的意识不断高，IT 安全已成为企业数字战略的重要组成部分。

保护组织要从保护数据做起，也就是要抵御勒索软件和其他复杂网络威胁。然而，网络威胁正变得愈加复杂，给了犯罪分子大量可乘之机，他们利用现代化工具和方法攫取您的关键数据，用于各种目的；或者为了某些目的或利益破坏数据并索要赎金。64% 的组织担心自己会在未来 12 个月内遭遇中断事件。[3]

就网络安全而言，问题的关键不在于您是否会面临这种攻击，而在于何时会面临这种攻击。面对极为复杂的网络威胁，组织不应将精力放在防范勒索软件或网络攻击上，而应专注于保护关键数据或应用程序，确保完整恢复关键资产，从而放心恢复正常业务运营。然而，许多组织对其数据保护解决方案缺乏信心，全球数据保护指数报告明确指出，67% 的 IT 决策者对在发生破坏性网络攻击后顺利恢复所有关键业务数据没有太大信心[3]。

网络攻击带来的现代威胁，加上维护数据机密性、可用性和完整性的重要性，要求企业采用现代解决方案和战略来保护至关重要的数据和系统。由于了解当今数据驱动型世界涉及的风险，积极进取的组织正在采用网络弹性战略来识别、保护、检测、响应勒索软件和其他网络攻击并从中恢复。实施网络弹性战略可将人员、流程和技术纳入能够保护整个业务、组织或实体的整体框架之中。

制定网络弹性战略对于所有组织和政府领导者而言必不可少，而且在当今由数据驱动的世界中可视为一项竞争优势。网络弹性的实现需要部署多层保护，以确保关键数据得到妥善保护并与攻击面隔离，这样才能在遭受勒索软件攻击后放心地快速恢复，从而更快地让业务恢复正常运营。

戴尔 PowerProtect Cyber Recovery 数据避风港为您宝贵的数据和关键业务系统提供更高级别的保护，保持它们的完整性和机密性，并且是全面的网络弹性战略的一个重要组成部分。这可以确保在发生网络事件或其他中断性事件后能快速恢复最关键的数据和系统，这是恢复正常业务运营的关键一步。强大的现代化网络弹性战略和 Dell Data Protection 对于帮助客户提高业务敏捷性、缩短上市时间、改善云经济性并降低业务风险至关重要。

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

[2]Accenture Insights，《Ninth Annual Cost of Cybercrime Study March》，2019 年 3 月：

https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[3]Gartner《Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware》报告，2021 年 1 月：

https://www.gartner.com/doc/reprints?id=1-25T81BQP&ct=210416&st=sb

戴尔 PowerProtect Cyber Recovery 数据避风港概述

可靠、全面的网络弹性战略应利用美国国家标准与技术研究院（NIST）网络安全框架（CSF）等框架，这些框架可帮助勾勒出连贯的端到端网络攻击防御体系。简而言之，网络弹性战略能够将人员、流程和技术纳入能够保护整个业务、组织或实体的整体框架之中。这种战略可以帮助您做好万全准备，无惧情况的不断变化，抵御中断并快速从中恢复。弹性涵盖抵御蓄意攻击、事故或自然威胁或事件并从中恢复的能力。数据以及随时随地在任何设备上实时访问数据的能力是当今数字世界赖以存在的基础，因此基于非技术能力实现弹性变得愈发困难重重。

PowerProtect Cyber Recovery 数据避风港是整体网络弹性战略的一个组成部分。PowerProtect Cyber Recovery 数据避风港与传统的备份和灾难恢复解决方案的区别在于，它能够在解决方案、系统和数据/文件级别提供额外的物理和逻辑安全保护层。这确保关键数据能够完整、机密地妥善保存，并在需要时可用于恢复。PowerProtect Cyber Recovery 数据避风港侧重于保护关键数据免受网络威胁并远离攻击面，以及在必要时从隔离环境中恢复这些数据。

PowerProtect Cyber Recovery 数据避风港致力于保护您的关键数据并在网络攻击和勒索软件事件后恢复业务运营，同时灵活运用具备以下三大网络恢复解决方案关键要素的专业服务和技术：

1. **隔离 —** Gartner 近期建议，如果组织希望免遭勒索软件攻击，则需要建立一个隔离的恢复环境[1]。PowerProtect Cyber Recovery 数据避风港提供了一个在物理上和逻辑上都隔离的数据中心环境，它与公司网络和备份网络都不相连，并且会限制没有相应权限的用户访问。自动化工作流通过一个可操作的安全隔离 Air Gap 安全地将关键业务数据移至隔离环境。您还可以创建保护策略，这只需不到 5 个步骤，并可以使用直观的控制面板实时监视潜在威胁。存储区最好在物理限定区域内运行，如网笼或上锁的房间，这有助于防范内部威胁。当安全隔离 Air Gap 处于“锁定”状态时，没有数据可以流动，因此无法访问解决方案的任何部分。当为了更新或“同步”数据而处于“解锁”状态时，则从安全的存储端控制操作，而非生产端。在这一阶段，存储区可保持非常安全的状态。仅允许代表复制数据的网络流量，并且始终禁止访问其他存储区组件或者访问存储或解决方案的管理平面。这样，不法之徒就无法等待存储区解锁，然后长驱直入了。
2. **不可篡改 —** PowerProtect Cyber Recovery 数据避风港提供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，数字存储区和流程可在生产/备份环境和存储区之间形成可操作的安全隔离 Air Gap。使用戴尔 PowerProtect DD 的合规模式锁功能，可以确保数据在设定的时间段内不会被删除和更改。即使是拥有全部权限的管理员，也无法覆盖此锁。PowerProtect DD 具备独特的增强功能，进一步加强了该锁的安全性，使之可以防范针对时钟（或者 NTP 服务器）的攻击；若无此防范机制，不法之徒就能想方设法让该锁提前过期。不想要或者不需要如此强的控制机制的客户，或者希望具备操作灵活性的客户，可以配置治理锁（这也是我们的 PowerProtect DD Virtual Edition (DDVE) 可提供的一种模式）。

3. **智能 —** 您可以利用 CyberSense 自适应分析、机器学习 (ML) 和取证工具进行检测、诊断并加快在 Cyber Recovery数据避风港存储区保护之下的数据恢复，在瞬息万变的威胁形势中始终保持积极主动，应对复杂的网络犯罪。CyberSense 与 PowerProtect Cyber Recovery 数据避风港完全集成，可监视文件和数据库，通过分析数据的完整性来确定是否发生了攻击。将数据复制到 Cyber Recovery 数据避风港存储区并应用保留锁后，CyberSense 会自动扫描备份数据，从而创建文件、数据库和核心基础架构的时间点观察结果。这些观察结果使 CyberSense 能够跟踪文件随时间变化的规律，甚至可发现非常高级的攻击类型。自动化的完整性检查可确定数据是否受到恶意软件的影响，以及可在必要时支持修正的工具。

[1]Gartner《Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware》：https://www.gartner.com/doc/reprints?id=1-25T81BQP&ct=210416&st=sb

PowerProtect Cyber Recovery 数据避风港的优势
面向关键数据的现代化保护，助力实现安全转型

PowerProtect Cyber Recovery 数据避风港针对破坏性网络攻击提供了一种有效的策略，但它并非对所有攻击都同样有效。

通常，上述攻击载体会组合出现。在以下部分中，我们将通过六个应用场景来介绍一些比较重要的攻击。

应用场景 1：**本土医院**

挑战：济宁市第一人民医院以“理念引领、运行畅顺、流程智能、管理到位”的智慧医院样板为目标，快速推进现代化医疗数据中心建设，在提升传统HIS、CIS、LIS、PACS、HRP等医疗系统服务效能的同时，加快医疗数字化转型，完成医疗信息化向一站式医疗服务的升级，在“电子健健康卡”、“一卡通”、“银医”系统、预约挂号、远程医疗会诊平台、门诊流程再造、信息安全、用药监控等多个数字化医院建设方面实现新的突破。同时还要将电子病历覆盖到包括门诊医药、日常护理、麻醉手术、影像、检验、病理等在内的各个诊疗环节，实现两个院区各诊疗环节的信息互联互通，在医疗健康数据治理与互联互通的基础上，打造健康医疗大数据平台，达到国家“电子病历应用水平分级评价5级标准”和 “医疗健康信息互联互通标准化成熟度四级甲等测评标准”。

成果：

· 提升了临床一线的工作效率，将医疗服务整体效率提升 200%

· 医疗服务 IT 支撑能力提升 8-9 倍

· 实现了自动化远程数据保护，备份速度提升 10-20 倍

· 达到国家“电子病历应用水平分级评价 5 级标准”

阅读客户案例分析

应用场景 2：**本土教育机构**

挑战：山东文化产业职业学院需要全面提升教育管理数字化服务水平，以数字化为重要手段持续推动教育业务、教务服务、教学管理等工作的效率提升，充分利用超融合、第五代存储、数据备份容灾与数据避风港等先进技术方案，构建多方位、全过程的数字化校园IT支撑体系。站在学院长远发展的高度，从整体需求出发，全面考虑业务部门需求、教学部门需求、师生服务需求、综合教学需求、管理辅助决策需求、IT系统运维需求等，用统一规划、统一建设、统一部署的方式，建设一个支持高校整体运营、管理统一、互联互通、信息共享的系统化高校资源管理与运营管理平台，为教育教学、教务管理和校园服务的改革发展做好服务。

成果

· 数据中心IT服务效能提升 8-9 倍

· 学院的业务管理与运营效率提升 3-4 倍

· 构建三位一体数据保护体系架构，抵御各种潜在风险，确保数据能够得到及时的恢复

· 数据可靠性和安全性达到 99.9999%

· 存储系统 I/O 性能提升 8-9 倍，数据管理效率提升 80%

阅读客户案例分析

应用场景 3：**公共事业机构**

挑战：为确保电力系统的安全稳定运行，国家电网某电力公司建立了覆盖危险识别、数据保护、安全检测、快速响应和业务恢复五位一体的现代化数据安全防御体系。该体系可将电力营销业务相关的数据进行本地高速备份，做到异地容灾及预防站点级别的灾难发生，并且建立防止勒索病毒的戴尔 PowerProtect Cyber Recovery 数据避风港，防止数据被勒索病毒绑架。同时，面向云端业务构建灵活、高效支持全业务应用的非结构化存储平台，充分发挥电力大数据优势，全面提高电力系统的数据安全保障体系水平，推进能源电力数据价值普惠化服务。

成果：

· 全面提高电力系统的数据安全保障体系水平

· 加快了备份作业进程，数据备份效率提升超过 200%

· 数据备份与容灾系统 TCO 降低 30%-40%，重复数据消除率达到 26:1

阅读客户案例分析

应用场景 4：**大型金融机构**

挑战：Founders Federal Credit Union 是一家在北卡罗来纳州和南卡罗来纳州经营的地方金融机构，资产总额约 35 亿美元，会员超 250,000 人。Founders Federal Credit Union 所属的行业是更复杂勒索软件的攻击目标，他们需要安全隔离 Air Gap 带来的网络安全弹性，并配备可与其 IT 环境无缝集成的 AI、机器学习和自动化功能，从而使其能够在竞争激烈的地方银行市场中拓展业务。数据保护和数据完整性是 Founders 客户承诺的基石，因此他们需要一款能够在任何设备上提供快速、可靠且安全的服务的解决方案。

成果：PowerProtect Cyber Recovery 数据避风港为 Founders Federal Credit Union 提供了真正的安全隔离 Air Gap 解决方案，能够在隔离式网络存储区中保护超过 10 PB 的数据。除了所有网络安全报告之外，戴尔 PowerProtect Cyber Recovery 数据避风港还可以自动执行备份、恢复和分析工作流。如果发生网络攻击，Cyber Recovery 数据避风港存储区中的 CyberSense 分析会识别已知的良好数据副本，让 Founders Federal 确信他们可以恢复业务运营，安心无虞。Cyber Recovery 数据避风港让 Founders Federal 高枕无忧，Founders Federal Credit Union 首席技术官 Bob Bender 表示：“在使用 PowerProtect Cyber Recovery 数据避风港解决方案三年多后，我晚上可以放心地睡觉了。”

阅读客户案例分析

应用场景 5：**学校**

挑战：当邻近学校遭到网络攻击时，莫雷诺谷联合学校的技术领导知道他们需要升级自身的数据保护和网络弹性。莫雷诺谷需要保护他们的学生、员工和财务数据，同时确保教职人员能够适应调整、顺畅协作、发挥创造力。他们之前的数据保护解决方案缺乏分析功能，无法监控所保护数据的完整性。他们还需要一款能够快速恢复业务运营的解决方案，以维持面向社区的关键教育服务。

成果：莫雷诺谷始终认为要通过不同的层（如防火墙和备份）来自我保护，但他们没有像 PowerProtect Cyber Recovery 数据避风港那样集所有功能于一体的解决方案。有隔离式安全隔离 Air Gap 的 Cyber Recovery 数据避风港存储区为其关键数据额外提供了一层安全保护，让莫雷诺谷知晓其 PII 数据安全无虞，能够在发生网络攻击后恢复，消除了后顾之忧。100 倍的日平均压缩率意味着可以存储和保护更多数据，且 CyberSense 还提供主动网络威胁分析和警报，从而能够轻松监控 Cyber Recovery 数据避风港存储区，确保数据完整性。
莫雷诺谷联合学校技术、创新和评估执行总监 Glenn Alegre 表示：“有了 CyberSense，我们不再是不法之徒能够轻易攻破的目标。”阅读客户案例分析，了解 PowerProtect Cyber Recovery 数据避风港如何确保学生、员工和财务数据的安全和可恢复性，让客户高枕无忧。

应用场景 6：**大型州政府**

挑战：俄克拉荷马州的公共安全信息、DHS 信息、ODOT 等州服务和数据库中有超过 2.6 PB 的关键数据需要现代化的网络保护，2020 年的特殊情况使IT转型势在必行。这些关键服务不能中断，否则他们可能面临州政府停摆的境况。因此，他们需要一款可靠的解决方案来确保数据可用性，并保护他们的数据免受网络攻击等威胁影响。他们之前用于恢复数据的解决方案需要非常多的手动操作，无法让他们真正安心。

成果：俄克拉荷马州开启了数字化转型之旅，以上问题迎刃而解。根据州长的指示，该州选择采用 PowerProtect Cyber Recovery 数据避风港来保护其关键数据，完成了 IT 流程和基础架构的现代化改造。PowerProtect Cyber Recovery 数据避风港让州政府能够抵御勒索软件、DDoS 和网页篡改等全球网络攻击并在遭遇攻击后恢复，从而高枕无忧。事实上，自 2021 年 1 月以来，PowerProtect Cyber Recovery 数据避风港已经帮助俄克拉荷马州抵御了 3.8 万亿次网络攻击。俄克拉荷马州首席运营官 Steven Harpe 表示：“Cyber Recovery 数据避风港让我们能够从攻击中恢复，扫除了我们的后顾之忧。这是一种分层式方案，绝对非常关键。”阅读案例分析

戴尔 PowerProtect Cyber Recovery 数据避风港详细信息

戴尔 PowerProtect 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。它可以自动创建用于执行恢复或安全分析的还原点。Cyber Recovery 数据避风港存储区的设计和实施都需要戴尔实施服务。要设计有效的恢复策略，我们推荐采用戴尔咨询服务。

技术因素

将数据恢复所需要的基础架构与生产环境隔离，能帮助组织大幅减少来自于内部和外部威胁的攻击面。用于定期同步数据的数据路径将是他们需要的唯一连接。为进一步减少攻击面，这一数据链路只有在执行数据同步时才会联机。这一逻辑性的安全隔离 Air Gap 通过减少攻击面，提供了另一层防护。PowerProtect Cyber Recovery 数据避风港将最关键的数据保护在存储区环境之中。理想情况下，此存储区应该单独锁放起来，实现物理上的隔离，并通过可操作的安全隔离 Air Gap 始终保持逻辑上的隔离。存储区的任一组件都无法从生产环境访问，在安全隔离 Air Gap 解锁时，对存储区目标的访问也严格受限。在 Cyber Recovery 数据避风港存储区内需要一定的算力来执行系统管理、基础架构服务、备份应用程序、按需安全分析和恢复测试。所需的算力取决于组织希望在 Cyber Recovery 数据避风港存储区中达到的恢复测试水平。

要在 Cyber Recovery 数据避风港存储区中维护一个环境，超融合设备或者带有虚拟 SAN 的小型 ESX 群集不失为一种经济有效的战略。管理主机必不可少，因为它要运行工具以编排工作流，详情参见下节。此外，还可以额外留出一部分算力，以备定期分析和数据验证。具体规模取决于待分析的数据量、使用的分析工具，以及验证和测试的频率。

自动化工作流

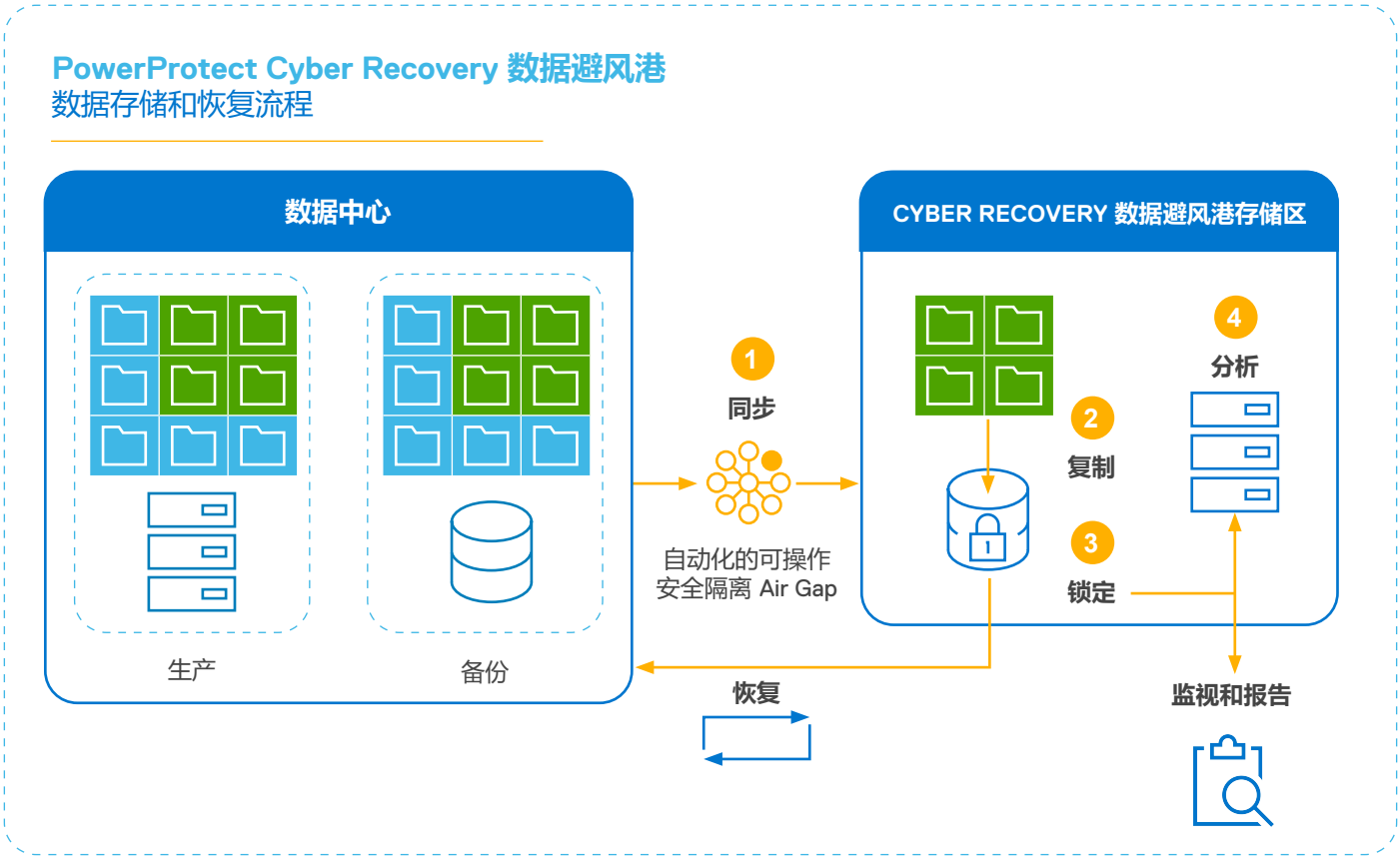
将基础架构迁移到 Cyber Recovery 数据避风港存储区可以防止不法之徒的潜在访问。此外，隔离还给获得批准的管理员带来了额外的管理挑战，因此，自动化十分重要。PowerProtect Cyber Recovery 数据避风港会自动执行与创建恢复或分析所需的还原点相关的工作流。三大核心优势：

易用性 — 创建还原点所需的时间比手动管理流程要少得多。同时，这也减少了潜在（但有限）的暴露窗口。

自动化 — 管理员无需手动创建每个还原点，而是可以安排策略，以特定时间和重复频率创建还原点，然后在保留期到期后自动删除数据。

可靠性 — 手动操作往往容易出错。基于策略的自动化方法可简化基础机制，降低恢复失败的风险。

下一页的插图概述了创建还原点的步骤，它用于恢复关键业务系统。



PowerProtect Cyber Recovery 数据避风港可处理以下独立操作：

1. **数据同步** — 代表关键应用程序的数据通过安全隔离 Air Gap 同步到存储区，并复制到存储区目标存储中，而 Air Gap 由 management server 解锁。然后，Air Gap 将重新锁定。此活动从 Cyber Recovery 数据避风港存储区中触发。该链路在数据同步前启用，然后在同步完成后禁用。单一传输机制能够大幅减少攻击面，并在一次传输中将所有关键数据输入 Cyber Recovery 数据避风港存储区。这可能包括备份目录和元数据，从而实现基于备份的部署。数据同步对生产端的应用程序而言是透明的，因此该活动不会在公共域中“公布”。实际数据传输非常高效，因为只有更改后的数据块才会通过网络复制。 生产端和目标端系统会建立可信连接，防止恶意系统连接到 Cyber Recovery 数据避风港存储区保护存储。

2. **创建 Cyber-Attack 测试和恢复副本** — 数据同步完成且数据路径禁用后，目标系统将执行操作，创建节省空间的数据副本。管理软件能够创建可写沙盒副本，以用于恢复练习和测试、数据验证和分析。建议定期进行恢复练习，确保数据没有受损，同时确保员工做好准备，能够在发生真实攻击时执行恢复。

3. **Retention Lock/创建不可变还原点** — 为防止删除，通过锁定每个文件的保留，进一步防止其被意外或故意删除，从而确保该副本不可变。您可以根据空间需求，利用策略设置保留期。需要注意的是，Cyber Recovery 数据避风港存储区并非归档。保留期通常为 7-45 天。当然也有例外，例如，为了能够恢复可执行文件，组织应将包含二进制文件和操作系统映像的分发包副本保留一年。

4. **分析** — CyberSense 分析引擎可以选择性地对数据进行分析，下一部分将详细介绍 CyberSense。

在存储区中分析

PowerProtect Cyber Recovery 数据避风港不能取代良好的安全预防和检测，而是作为这些安全措施的补充。同时，与生产环境相比，Cyber Recovery 数据避风港存储区具有一些独特的优势：

- 受保护的环境提高了安全分析的有效性。因为 Cyber Recovery 数据避风港存储区与网络隔离，所以恶意软件扫描可以不受阻碍地进行取证，因为它们不会受恶意软件屏蔽程序影响。在隔离的工作台中，可以更好地分析对某些攻击载体的诊断。
- 即使需要十分小心，应用程序重启活动也可以检测仅在应用程序初始启动时发生的攻击。像 DBVERIFY 这样需要停机的应用程序工具也可以在离线环境中使用。

CyberSense

为了在发生攻击之后快速恢复，对存储区内的数据运行分析是不可缺少的重要环节。分析有助于您判断某个数据集是有效、可供恢复使用的，还是已经被不当地篡改或损坏因而是“可疑”、可能无法使用的。PowerProtect Cyber Recovery 数据避风港是为数不多完全集成 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 (ML) 来分析超过 100 组基于内容的统计数据，检测由勒索软件造成的损坏迹象。CyberSense 的损坏检测置信度高达 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保护下进行。

CyberSense 监视文件和数据库，并分析数据的完整性，从而确定是否发生了攻击。将数据复制到 Cyber Recovery 数据避风港存储区并应用保留锁后，CyberSense 会自动扫描备份数据，从而创建文件、数据库和核心基础架构的时间点观察结果。这些观察结果使 CyberSense 能够跟踪文件随时间变化的规律，甚至可发现非常高级的攻击类型。上述扫描直接在备份映像内的数据上进行，无需原始备份软件。生成的分析可以检测文件或数据库页面的加密/损坏、已知的恶意软件扩展名、文件的批量删除/创建等。然后，机器学习算法使用分析来确定是否存在表明有网络攻击的数据损坏。机器学习算法已针对最新的木马病毒和勒索软件进行训练，可检测此类可疑行为。如果发生攻击，Cyber Recovery 数据避风港控制面板中就会显示一条严重警报。CyberSense 攻击后取证报告可用于快速诊断勒索软件攻击并从中恢复。

完整内容分析

CyberSense 可针对存储区中的所有受保护数据提供基于完整内容的分析。此功能使 CyberSense 从众多解决方案中脱颖而出，因为其他这些解决方案只能大概了解数据，并使用分析寻找基于元数据的明显损坏迹象。元数据级别的损坏很容易检测；例如，将文件扩展名更改为 .encrypted 或彻底更改文件大小。但这些类型的攻击并不能代表当今网络犯罪分子所使用的复杂攻击。CyberSense 超越了仅限于元数据的解决方案，因为它基于完整内容分析，可在数据损坏检测方面实现 99.5% 的置信度。它可审查文件和数据库是否受到了攻击，包括仅基于内容的文件结构损坏，或数据库文档或页面内的部分加密。不使用扫描文件内部并比较文件随时间变化的分析方法，就无法发现这些攻击。如果没有针对完整内容的分析，那么漏报数量将会大幅增加，这样您就会对数据完整性和安全性持盲目乐观态度。

恢复程序

CyberSense 提供攻击后取证报告，让您了解攻击的深度和广度之后，还会提供损坏之前的最后良好备份集的列表，以便加快执行恢复流程。戴尔 Cyber Recovery 数据避风港的终极目标是让组织能够通过更为快速可靠的路径恢复关键业务系统。因此，制定网络攻击恢复计划并将其纳入正式的网络事件响应计划至关重要。这通常包含以下要素：

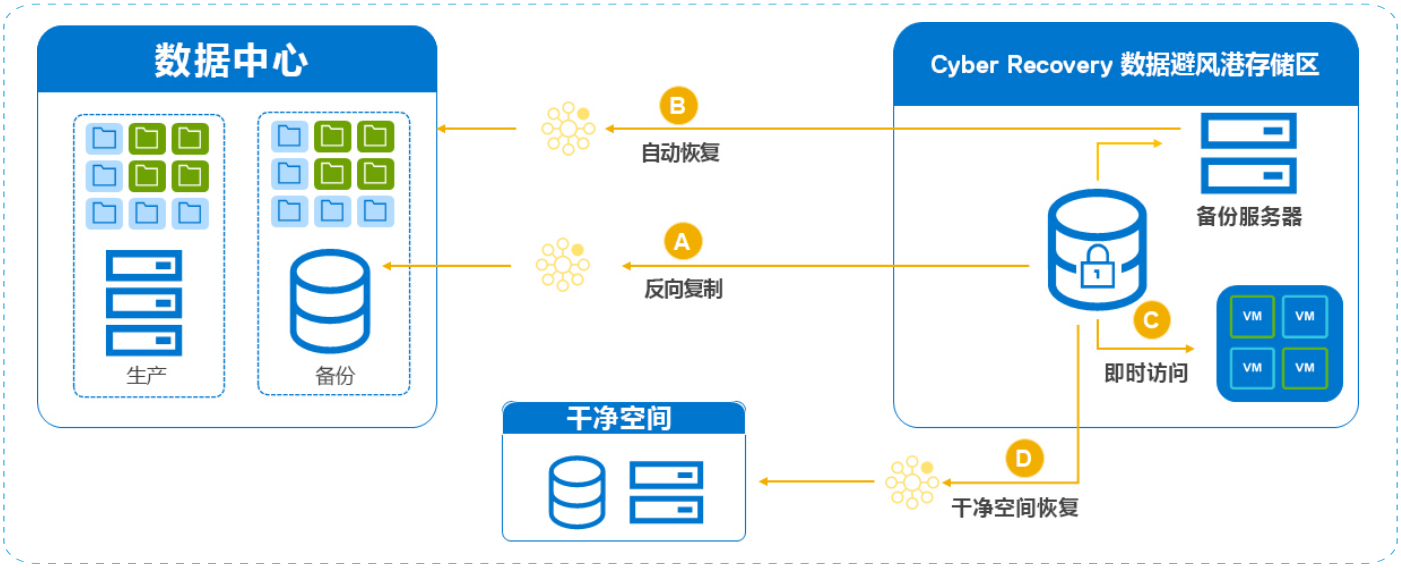
1. **调用网络恢复计划** — 涉及针对漏洞做好防护、调用安全隔离 Air Gap 来关闭与 CR 存储区的连接，以及调度 Cyber Recovery 数据避风港计划中的资源来启动响应流程。

2. **执行取证和损害评估** — 取证分析，识别攻击的类型和范围，并确定是否可以部署可用的修复或修补程序来避免再次感染。损害评估会评估受影响的数据和系统，确定哪些可以修复，哪些需要恢复，包括任何相关联的系统。它还会识别任何未受影响的数据库日志，从而尽可能减少数据丢失，并确定最佳还原点。

3. **恢复准备** — 确定最合适的恢复技术，然后确定特定系统的恢复优先级和顺序。这种评估也会考虑生产环境中受影响的部分、时间以及其他相关细节。最终目标是选择能够防止或尽可能减少对关键业务系统的损害的恢复路径。

4. **数据、应用程序和服务的恢复** — 此步骤通常是在步骤 1-3 的基础上执行系统和数据恢复。组织可能会选择将数据反向同步回经过清理或重建的生产系统，然后应用修补程序来防止再次感染。或者，它可以选择在 CR 存储区中执行恢复，然后将恢复的基础架构连接回生产网络。

根据网络攻击和它造成的损害，有几种恢复技术可能可行。下文概述了几个场景。



Dell Technologies 提供了灵活的恢复选项，以满足您的网络弹性要求。恢复流程受客户成熟度、具体应用程序等诸多因素影响。此外，恢复流程并不是完全隔绝的，它将与您的事件响应流程集成。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。然后，在准备好恢复生产后，可以通过四种方式来使用 PowerProtect Cyber Recovery 数据避风港执行恢复：

场景 A
反向复制

反向复制或“简化备份恢复”是最简单直接的流程。对于希望还原完整已知良好备份，然后从中恢复应用程序数据的用户，建议使用此选项。您可以从存储区中的单个或多个 PowerProtect DD 中执行反向复制，将数据复制回其来源位置。一旦数据返回到生产环境中的 PowerProtect DD，您就可以使用备份软件执行正常的恢复流程了。

场景 B
自动恢复

自动恢复或“自动化选择性恢复”可以直接从存储区恢复，而无需将所有内容都转移到生产环境中的备份中。对于希望通过在存储区中维护并使用备份应用程序，以将全部或部分应用程序数据恢复到生产环境中的用户，建议使用此流程。此流程要求您在 Cyber Recovery 数据避风港存储区中有单独的备份服务器。该服务器将从存储区内访问 PowerProtect DD 上的数据，然后，您可以使用此服务器将数据集恢复到生产环境中的数据中心。自动恢复还需要额外的步骤，如创建网络连接、DNS 等，但是我们可以利用操作手册，帮助客户解决这些问题。

场景 C
即时访问

即时访问或“虚拟机即时访问”适用于希望即时访问虚拟机的用户。此选项利用 PowerProtect DD 的即时访问功能，让您能够在存储区中的 PowerProtect DD 上运行虚拟机。您可以立即启动这些虚拟机以用于执行测试，也可以将此环境用于生产。即时访问可以用作单独的恢复流程，也可以用作完整流程的一部分。

场景 D
干净空间

干净空间或“全面测试和恢复”适用于希望在恢复之前测试数据以确保数据完整性的用户。干净空间是基础架构中物理上或逻辑上的独立区域，不存在任何连接。这个干净空间可以非常小（即几个虚拟机），也可以是非常大的基础架构，具体取决于您要恢复到干净空间的内容。干净空间有两个恢复选项。

选项 1 – 此选项中的干净空间用于一次恢复一个应用程序并对其进行测试，确保其中没有恶意软件。在确认数据完整性后，您就可以将它从干净空间恢复到生产环境中，并继续处理下一个应用程序。许多事件响应团队都是使用这种方法来确保在重新投入生产之前所有内容都是干净的。在这种情况下，干净空间的大小将由最大的应用程序决定。

选项 2 – 此选项适用于不希望等到数据中心恢复后再恢复应用程序的客户，这类客户希望立即恢复应用程序并且可以访问应用程序。在这种情况下，干净空间中的基础架构可能比选项 1 中要多。您将应用程序从存储区恢复到干净空间，然后像在生产环境中一样运行该应用程序。在这种情况下，您并非使用干净空间进行测试，而是将应用程序恢复到干净空间，并作为生产工具运行。

总结

网络攻击给全球企业带来了灾难性的后果，导致收入减少、声誉受损，还有数百万美元的高昂恢复成本。在瞬息万变的威胁形势下，组织正在寻找有效的恢复策略，因为他们知道仅靠预防和检测远远不够。戴尔 PowerProtect Cyber Recovery 数据避风港针对常见攻击载体提供了有效的恢复解决方案，包括休眠恶意软件、数据擦除和锁定、数据损坏、内部攻击以及备份和存储资产破坏。这使组织确信，在发生网络事件或其他中断性事件后，组织能够快速放心地恢复最关键的数据和系统，然后恢复正常业务运营。

详细了解
戴尔 PowerProtect Cyber Recovery 数据避风港

联系
Dell Technologies 专家

查看更多安全资源

DELL Technologies
戴 尔 科 技 集 团