DELL Technologies

适用于 Cyber Recovery 数据避风港的专业服务

自信满满地增强从网络攻击中恢复的能力

业务挑战

在当今的数字化世界中，随着组织越来越依赖技术，他们也更容易遭受漏洞攻击、欺诈和盗窃等威胁。这些威胁让全球组织面临越来越大的风险，可能导致业务运营中断数天甚至数周，造成数以百万计的损失并对声誉产生负面影响。

除了敏感信息或专有数据泄露风险之外，更令人担忧的是，如今涌现了大量精心策划的网络攻击，企图销毁数据或加密并劫持数据以索要赎金。最近，多起勒索软件攻击相继爆发，造成了严重破坏，尤其是对制造系统、医院信息系统、银行系统和地方政府。

这些攻击可以绕过外围设置的传统安全控制措施，让攻击者能够潜伏数周或数月之久而不被发现，从而入侵尽可能多的系统，令组织措手不及无法及时恢复。更加糟糕的是，除了来自组织外部的攻击以外，来自内部人员的网络攻击也越来越多。为此，领导层需要做好充分准备，让组织能够在遭受攻击后尽快恢复正常运行。

Cyber Recovery 数据避风港服务概述

- **为期一周的咨询服务：**Cyber Recovery 数据避风港存储区规划
- **恢复操作手册：**操作手册编写、测试和验证
- **设计和实施：**通过精心设计的引导式解决方案抵御网络攻击

目前有超过 2300 名客户使用 **Dell Technologies PowerProtect Cyber Recovery** 数据避风港[1]

在网络恢复领域深耕逾 9 年，拥有丰厚的专业知识积淀

Cyber Recovery 数据避风港服务与所有戴尔存储平台和主流备份软件都兼容

基于 Dell Technologies 在 2024 年 7 月进行的分析

Cyber Recovery 数据避风港功能

采用经验证的方法、协作流程和行业最佳实践，帮助您加快实施安全计划并提高网络弹性	我们致力于确保主要利益相关者之间达成共识，通过优化体系结构加快解决方案设计速度，制定战略路线图以提高计划成熟度，并采用敏捷方法在遵循总体目标的前提之下逐步开展活动。
实施根据您的确切业务需求量身定制的**网络恢复解决方案**	我们的实施服务覆盖全面，从基本部署到高度定制化服务无所不包，可根据您的业务需求量身定制解决方案。我们可以根据您的特定业务需求和 IT 需求扩展解决方案，助您快速大规模地实现业务恢复；另外，我们还可以帮助您将网络恢复集成到整个组织的网络事件响应计划中，并与 ITSM/ITIL 流程集成。
制定操作手册和实施流程以实现恢复	通过编写操作手册以及定期测试和验证恢复程序来提高计划成熟度，从而精准敏捷地应对网络攻击。
提高运营一致性并降低风险	在您开始使用 Cyber Recovery 数据避风港解决方案后，我们将通过托管服务来帮助您进行存储区日常运营，并安排全球运营团队来全天候监控运营情况。如此一来，您将能够保持流程一致性、实现定期测试、顺利开展恢复操作并确保明确的职责划分，从而增强安全控制。 我们还提供派驻服务，即安排具有深厚技术技能和丰富经验的资深专家，帮助您测试是否已恢复生产、进行额外的 CyberSense 警报调整或完成其他任务。这些派驻专家将作为“编外人员”与贵公司的 IT 员工开展协作，凭借自身技术专长和经验扩展您的内部能力和资源。
通过全新推出的网络安全培训，**让您的团队掌握最新技能**	我们提供丰富的培训模块，包括专门的 PowerProtect Cyber Recovery 数据避风港培训、DD 概念和功能介绍、Virtual Edition 实施以及 DM 实施和管理，还提供用户身份验证、访问控制和安全标准、NIST 网络安全框架、IT 框架简介等安全培训和认证。借助这些业界卓越的网络安全培训和认证，您的团队能够掌握最新技能。

根据组织需求选择合适的服务

我们的服务旨在助您增强网络弹性。Product Success Accelerator (PSX) for Cyber Recovery 适合需要全包式解决方案的客户。面对更为复杂的环境，我们可以根据您的具体需求提供量身定制的设计、实施和管理服务。

无论您的目标是集成新技术，还是应对新兴威胁，亦或是适应发展需求，我们的服务组合都能确保您的恢复战略与业务目标保持一致。

探索戴尔安全性和弹性服务

联系 Dell Technologies 专家

加入 #DellTechnologies 对话