DELL Technologies

解决方案简介

Dell EMC PowerProtect Cyber Recovery 数据避风港

针对勒索软件和破坏性网络攻击，为关键数据提供经过验证的现代保护

为什么选择 Cyber Recovery 数据避风港?

网络攻击旨在销毁、窃取或以其他方式损害您的宝贵数据，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。您的企业能否生存下来？下面是经过验证的现代化网络恢复解决方案的五个组件：

数据隔离和治理
隔离的数据中心环境，与企业和备份网络断开连接，并且只允许具有适当权限的用户访问。

自动化数据拷贝和网络阻断
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运营网络阻断。

智能分析和工具
机器学习和完整内容索引编制，在存储区的安全保障下进行强大的分析。自动完整性检查可确定数据是否受到恶意软件的影响，并可在必要时提供支持修正的工具。

恢复和修正
工作流和工具用于在事件发生后使用动态还原过程和您现有的灾难恢复程序执行恢复。

解决方案规划和设计
提供专家指导，以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

数据是互联网经济的货币，是一种必须受到保护、严格保密和随时可用的重要资产。当今的全球市场依赖于数据在互连网络之间的不断流动，而数字化转型工作使得更多敏感数据面临风险。

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。

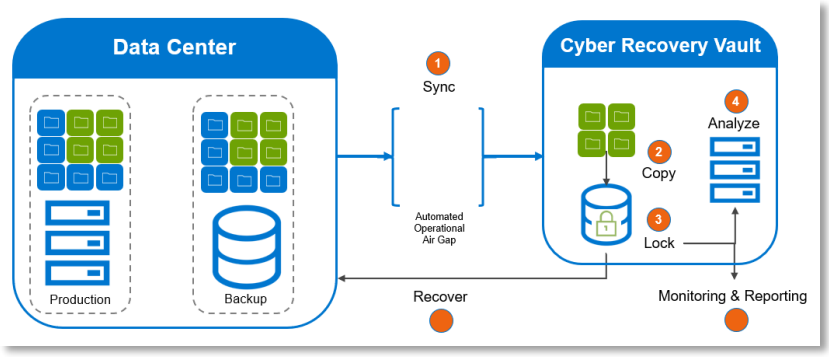
网络犯罪被称为史上最大笔的财富转移，而这一切都与数据有关。埃森哲估计，未来 5 年，将有 5.2 万亿美元的全球价值面临网络犯罪风险。[i]

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、声誉受损以及高昂的监管罚款。2018 年，每家公司的网络犯罪平均年度损失增加到 1300 万美元，仅在过去 5 年中就激增了 72%。[ii]

制定网络恢复战略已成为企业和政府领导者的任务。根据 2019 年 Marsh & Microsoft 的一项调研，79% 的全球高管将网络攻击列为组织的最高风险管理优先事项之一。[iii]

那么，您可以做些什么来保护您的组织及其宝贵的数据呢?

解决方案：PowerProtect Cyber Recovery 数据避风港

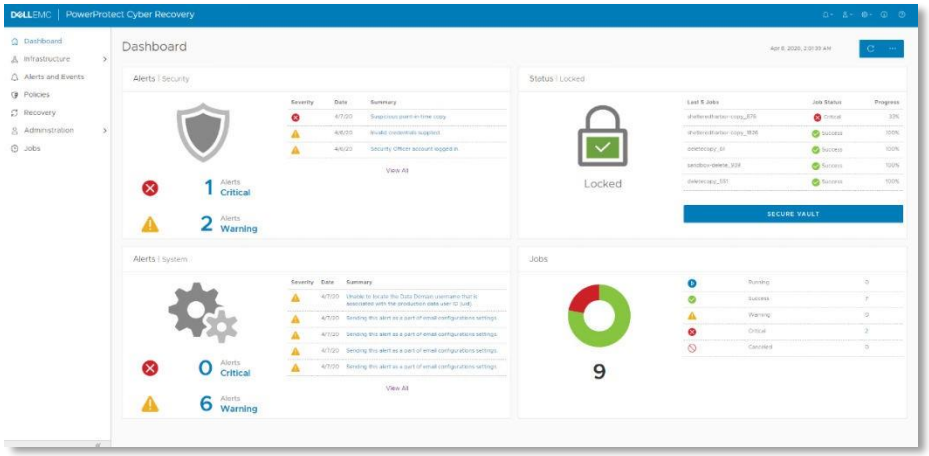


为了降低网络攻击造成的业务风险，并创建更具网络弹性的数据保护方法，您可以实现恢复和业务连续性战略的现代化和自动化，并利用新的智能工具来检测和抵御网络威胁。

Dell EMC PowerProtect Cyber Recovery 数据避风港的特点包括：成熟的现代化智能保护，可隔离关键数据；识别可疑活动，加快数据恢复；让您能够快速恢复正常的业务运营。

PowerProtect Cyber Recovery 数据避风港 — 成熟的现代化智能保护，可降低网络威胁带来的业务风险

- **Cyber Recovery 数据避风港存储区** — PowerProtect Cyber Recovery 数据避风港存储区通过多层保护来提供抵御网络攻击的弹性，即使是面对内部威胁也不例外。它将关键数据从受攻击面移走，通过物理方式将其隔离在数据中心的受保护部分中，需要单独的安全凭据和多因素身份验证才能进行访问。其他保护措施包括利用自动化运营性网络阻断提供网络隔离，以及消除可能遭受攻击的管理接口。PowerProtect Cyber Recovery 数据避风港可在生产系统和存储区之间自动执行数据同步，然后使用锁定的保留策略创建不可更改的副本。一旦发生网络攻击，您可以快速找到干净的数据副本，恢复业务关键型系统，并让您的业务恢复正常运行。



- **CyberSense** — 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 (ML) 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。
- **恢复和修正** — PowerProtect Cyber Recovery 数据避风港可提供自动还原和恢复流程，使业务关键型系统能够快速、可靠地恢复正常运行。作为 PowerProtect Data Manager 的一部分，对于运行 Dell EMC NetWorker 的客户，Cyber Recovery 数据避风港可从存储区进行自动恢复。Dell EMC 及其生态系统合作伙伴提供了一种全面的方法，不仅可以保护数据，还可通过执行损坏评估和取证来恢复系统或者删除违规恶意软件并采取修正措施。
- **解决方案规划和设计** — 可选的 Dell EMC 咨询服务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所需的基础架构。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。

保护您的重要数据免遭网络攻击需要经过验证的现代解决方案。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。

详细了解 Dell EMC PowerProtect Cyber Recovery 数据避风港

联系 Dell EMC 专家

[来源：埃森哲《The Cost of Cybercrime Study 2019》]
[来源：埃森哲《The Cost of Cybercrime Study 2019》]
[来源：Marsh & Microsoft《Global Cyber Risk Perception Study 2019》]