DELL Technologies

解决方案简介

PowerProtect Cyber Recovery for Sheltered Harbor

保护关键客户数据，并保持消费者对美国金融市场的信心

Sheltered Harbor 是什么?

Sheltered Harbor 标准由金融行业于 2015 年制定，包含一系列网络弹性和数据保护最佳实践以及保障措施，用于保护美国金融数据。网络威胁（包括勒索软件、数据销毁或针对生产和备份系统的盗窃）使消费者和企业的财务数据面临风险。

针对美国银行、信贷协会或经纪公司的成功网络攻击会损害金融机构的声誉，削弱消费者对美国金融系统的信心，并可能引发全球金融危机。

Sheltered Harbor 通过在数字存储区中隔离关键客户帐户记录和其他数据并使其保持不可变，提高美国金融稳定性和机构的网络弹性。如果机构的主要或备份系统受到网络攻击（如勒索软件或其他事件），这些关键数据可以快速恢复，从而促进面向客户的关键银行服务的连续性，保持公众信心。

为什么选择 Cyber Recovery?

Dell Technologies 是 Sheltered Harbor 联盟合作伙伴计划中的主要解决方案提供商，为美国金融结构开发了 Sheltered Harbor 全包式数据存储解决方案。

PowerProtect Cyber Recovery for Sheltered Harbor 是率先获得 Sheltered Harbor 认可的内部全包式数据存储解决方案。它符合针对实施 Sheltered Harbor 标准的参与者的各项技术要求。

数据存储区 — 参与机构或服务提供商以 Sheltered Harbor 标准格式对关键数据进行夜间备份。数据存储区经过加密，不可更改，且与机构的基础架构（包括备份、灾难恢复和其他数据保护系统）隔离开来。

隔离和治理 — 与公司网络断开的隔离、安全的环境可限制没有适当许可的用户。自动化数据拷贝和网络阻断管理可确保实现数据完整性、可用性、安全性和保密性。

恢复和补救 — 如果启用了 Sheltered Harbor 弹性计划，参与机构可以快速从存储区中恢复数据，从而更快地恢复银行运营。

挑战：对金融服务行业的网络攻击可能引发全球金融危机

所有组织都担心恶意网络攻击可能对他们的业务造成严重影响，尽管如此，97% 的组织会在其数字化转型工作中使用敏感数据。[1]释放数据价值可以带来巨大的回报。

如果敏感数据落入坏人之手、被破坏或发布到公众面前，也会造成巨大风险。恶意软件和勒索软件不断演变，攻击日益增多 — 根据 Symantec 的 2019 年互联网安全威胁报告，2019 年企业勒索软件攻击增加了 12%，占所有勒索软件感染的 81%。[2]此外，根据最近的一份 Ponemon Institute 报告，2020 年，52% 的数据泄露为恶意泄露，比五年前增加了 30%。[3]

更甚的是，威胁人员的手段和工具已经演变，使得检测到它们几乎无法实现，而攻击预防也越来越多地呈现此趋势。根据 2020 年 Verizon 数据泄露调查报告，网络犯罪手段不断演变，在报告的网络攻击中，30% 的攻击涉及内部威胁，比三年前增加了 25%。[4]

根据 Accenture 的 2019 年度网络犯罪成本报告，美国金融行业在过去三年里因网络犯罪而遭受了巨大损失，[5]这些力量结合在一起，形成了全球金融市场需要应对的巨大威胁风暴。

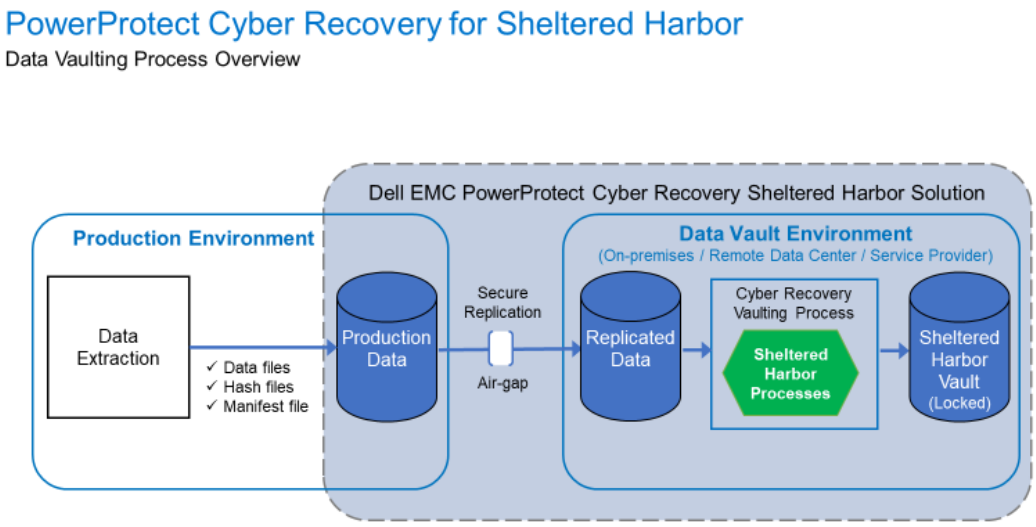
Sheltered Harbor 成立于 2015 年，是一项非营利性的行业主导计划，旨在指导美国金融机构降低因网络攻击而危及客户数据并造成正常银行服务中断的风险。Sheltered Harbor 生态系统包括参与机构（美国银行、信贷协会、经纪公司、资产经理）、国家贸易协会、解决方案提供商和服务提供商，致力于提高金融行业的稳定性和网络弹性。

传统的灾难恢复和业务连续性是在发生自然或人为事件后帮助恢复全面运营功能所必需的。在有针对性的复杂网络攻击发生后，Sheltered Harbor 旨在确保恢复基本银行运营所需的数据完整且随时可用，而且完整恢复过程可以继续。

Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor — 针对金融机构的关键数据提供强大的网络弹性

Dell Technologies 是加入 Sheltered Harbor 联盟合作伙伴计划的主要解决方案提供商。我们获得认可的 Sheltered Harbor 解决方案基于 Dell PowerProtect Cyber Recovery，这是一款业界卓越的解决方案，在保护组织的关键数据免受网络攻击（例如勒索软件）影响方面拥有近五年的经验。

为了遵守 Sheltered Harbor 规范，Cyber Recovery 存储区体系结构已扩展，可执行归档生成和安全存储库流程。提取的 Sheltered Harbor 数据将保存在生产环境中，然后通过阻断网络的专用逻辑连接安全地复制到存储环境，随后在该环境中执行其余步骤，例如保留锁定。



通过创建一个在物理上独立于公司网络和备份系统的专用隔离环境，Sheltered Harbor 参与者需要保护的关键数据集将以标准化格式提供，以便为客户快速恢复基本的银行服务。部署以周而非月为单位进行，并且可确保符合 Sheltered Harbor 规范。

总结

Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor 为参与机构提供了完全获得认可、经济实惠且快速高效的替代方案，可为每个机构构建一次性专有存储区，从而实现 Sheltered Harbor 规范合规性。选择实施 Sheltered Harbor 标准的银行、信贷协会和经纪公司可以求助于 Dell Technologies，以获取完全获得认可且全面受支持的全包式数据存储解决方案。

凭借利用基于存储区的成熟技术的附加优势，选择 PowerProtect Cyber Recovery for Sheltered Harbor 的 Sheltered Harbor 参与者可以满怀信心地满足即时部署需求，并为其未来的数据存储需求奠定基础。参与机构具有生存下去的途径，而且可保持公众对美国金融系统的信心。

来源：

1. 2019 年 Thales 数据威胁报告 — www.thalessecurity.com/DTR
2. 2019 年 Symantec 互联网安全威胁报告 — https://www.symantec.com/security-center/threat-report
3. 2020 年数据泄露代价报告，Ponemon Institute, LLC — https://www.ibm.com/security/data-breach
4. 2020 年 Verizon 数据泄露调查报告 — https://enterprise.verizon.com/resources/reports/dbir/
5. 2019 年 Accenture 网络犯罪成本报告 — https://www.accenture.com/us-en/insights/security/cost-cybercrime-study