

Dell PowerProtect Cyber Recovery for Sheltered Harbor

Protecting Critical Customer Data and Preserving Consumer Confidence in U.S. Financial Markets.

WHAT IS SHELTERED HARBOR?

Created in 2015 by the financial industry the Sheltered Harbor standard incorporates a set of cyber resilience and data protection best practices and safeguards for protecting U.S. financial data. Cyber threats, including ransomware, data destruction, or theft targeting production and backup systems, put consumer and corporate financial data at risk.

Sheltered Harbor enhances U.S. financial stability and institutions' cyber resilience by isolating critical customer account records and other data immutably within a digital vault. In the event an institution's primary or backup systems are compromised by a cyberattack like ransomware or other event, rapid recovery of this critical data is enabled, facilitating the continuity of critical customer-facing banking services, ensuring public confidence is maintained.

WHY CYBER RECOVERY?

Dell PowerProtect Cyber Recovery for Sheltered Harbor stands out as the first on-premises solution to receive Sheltered Harbor's endorsement, meeting all the technical requirements needed by Participants adopting the Sheltered Harbor standard.

Traditional disaster recovery and business continuity are necessary to help restore full operational capabilities after a natural or man-made event. In the wake of a targeted, sophisticated cyberattack, Sheltered Harbor aims to ensure that data necessary to restore basic banking and financial operations are readily available with integrity while full recovery procedures continue.

To comply with the Sheltered Harbor Specification, the Cyber Recovery vault architecture has been extended to perform the Archive Generation and Secure Repository processes. Extracted Sheltered Harbor data is saved in production, then securely replicated via the automated data isolation connection to the vaulted environment where the remaining steps, such as retention locking, are performed.

The Challenge: Cyberattacks on the Financial Services Industry Could Trigger Financial Crisis.

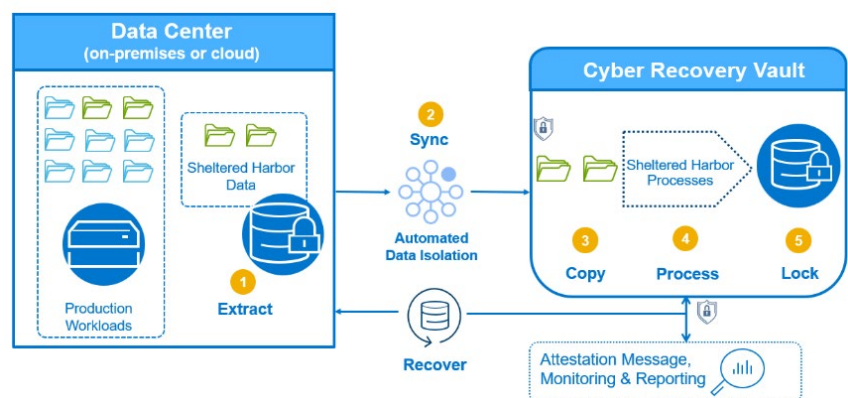
A successful cyberattack on U.S. bank, credit union or brokerage firm would damage those financial institutions reputation, undermine consumer confidence in the U.S. financial system, and possible trigger a global financial crisis. All organizations are concerned about the crippling impact a malicious cyberattack could have on their business. The [Global Data Protection Index](#) reported that 79% of IT decision makers are concerned they will experience a disruptive event in the next 12 months, and 75% are concerned their organizations existing data protection measures may not be sufficient to cope with malware and ransomware threats¹.

There is a significant risk if sensitive data falls into the wrong hands, is destroyed or is released into the public. Cyberattacks are continuously evolving, and the threat actors' tactics, tools and the use of generative AI make detection nearly impossible and attack prevention more difficult.

The Solution: Dell PowerProtect Cyber Recovery for Sheltered Harbor

Sheltered Harbor was formed in 2015 as a nonprofit, industry-led initiative to guide U.S. financial institutions to decrease the risk of a cyberattack compromising customer data and interrupting normal banking services. The Sheltered Harbor ecosystem comprises participating institutions (U.S. banks, credit unions, brokerages, asset managers), national trade associations, solution providers and service providers dedicated to enhancing the stability and cyber resilience of the financial sector.

Dell Technologies is the first solution provider to join the Sheltered Harbor Alliance Partner Program. Our endorsed solution for Sheltered Harbor is based upon Dell PowerProtect Cyber Recovery, a market leader with more than six years history of protecting organizations' most critical data from cyberattacks, such as ransomware and insider threats.



By creating a dedicated, isolated environment, physically separated from corporate networks and backup systems, critical data sets, which Sheltered Harbor Participants are required to protect, are available in standardized format so that basic banking or financial services can be quickly resumed for customers. Deployment is measured in weeks instead of months, and with a certainty of compliance with the Sheltered Harbor Specification.



Data Vault – Nightly backups of critical data in the Sheltered Harbor standard format are created by the participating institution or service provider. The data vault is encrypted, unchangeable and isolated from the institution’s infrastructure, including backup, disaster recovery and other data protection systems.

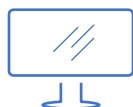
Isolation & Governance – An isolated, secure environment disconnected from corporate networks restricts users other than those with proper clearance. Automated data copy and isolation management assure preservation of data integrity, availability, security and confidentiality.

Recovery & Remediation – If a Sheltered Harbor Resilience Plan is activated, the participating institution can quickly recover data from the vault to enable the fastest restoration and resumption of banking or financial services.

Conclusion

Dell PowerProtect Cyber Recovery for Sheltered Harbor offers banks, credit unions and brokerage firms a fully endorsed, efficient, and cost-effective data vaulting solution that complies with Sheltered Harbor standards. This mature, vault-based technology not only meets immediate deployment needs but also provides a foundation for future data protection, ensuring institutional survival and maintaining public confidence in the U.S. financial system.

¹ Based on research by Vanson Bourne commissioned by Dell Technologies, "Global Data Protection Index 2024 Snapshot". October 2023.



[Learn more](#) about Dell PowerProtect Cyber Recovery



[Contact](#) a Dell Technologies Expert



[View more](#) resources



Join the conversation with #PowerProtect