DELL Technologies

Solution Brief

# 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.

A successful cyberattack on a U.S. bank, credit union or brokerage firm would damage that financial institution's reputation, undermine consumer confidence in the U.S. financial system, and possibly trigger a global financial crisis.

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 cyberattack 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 Technologies is the first technology Solution Provider in the Sheltered Harbor Alliance Partner Program, developing a Sheltered Harbor turnkey data vaulting solution for U.S. financial institutions.

PowerProtect Cyber Recovery for Sheltered Harbor will be the first on-premises turnkey data vaulting solution designed to meet all technical product requirements for Participants implementing the Sheltered Harbor standard, expected general availability in CQ2 2020.

**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 air gap management assure preservation of data integrity, 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 operations.

### The Challenge: Cyberattack on the Financial Services Industry Could Trigger Global Financial Crisis

All organizations are concerned about the crippling impact a malicious cyberattack could have on their business, even while 97% of organizations will use sensitive data in their digital transformation efforts.[1] There is great reward in unlocking the value of data.

There is also great risk if sensitive data falls into the wrong hands, is destroyed or is released into the public. Malware and ransomware have evolved – Enterprise ransomware attacks rose 12% in 2019 to account for 81% of all ransomware infections according to Symantec's 2019 Internet Security Threat Report.[2] Furthermore, 51% of all data breaches are of malicious intent in 2019, up 30% from just five years ago, according to a recent Ponemon Institute report.[3]

What's more, the threat actors' tactics and tools have evolved to make detection nearly impossible and attack prevention increasingly so. Cybercrime tactics continue to evolve, with 34% of reported cyberattacks involving insiders, up from 25% just two years ago, according to Verizon Data Breach Investigations Report 2019.[4]

The U.S. industry has suffered the highest losses due to cybercrime over the past three years according to Accenture's 2019 Annual Cost of Cybercrime report,[5] and these forces combine into a perfect storm of threats for global financial markets to address.

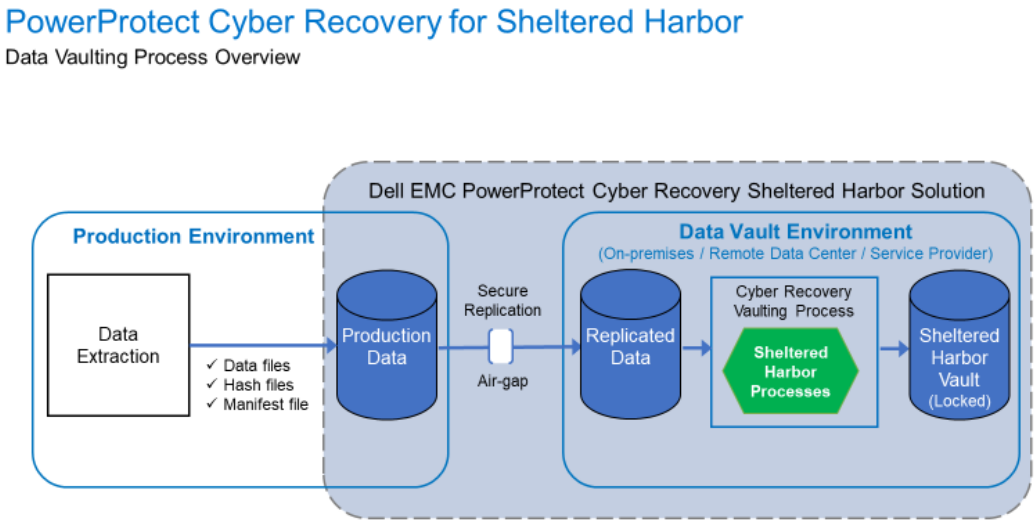
Sheltered Harbor was formed in 2015 as a nonprofit, industry-led initiative to guide U.S. financial institutions to decrease the risk of a cyberattack compromising customer data and interrupting normal banking services. The Sheltered Harbor ecosystem comprises participating institutions (U.S. banks, 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.

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 operations is readily available with integrity while full recovery procedures continue.

## Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor – Robust cyber resilience for financial institutions' most critical data

Dell Technologies is the first technology solution provider to join the Sheltered Harbor Alliance Partner Program. The solution is based upon the Dell PowerProtect Cyber Recovery solution, a market leader with an almost five-year history of protecting organizations' most critical data.

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




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 services can be quickly resumed for customers. Deployment can be measured in a matter of weeks instead of months, and with a certainty of compliance with the Sheltered Harbor Specification.

### Summary

Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor is being developed to provide participating institutions a fast, cost-effective and efficient alternative to each institution building a one-off, proprietary vault in order to maintain compliance with the Sheltered Harbor Specification. Banks, credit unions and brokerage firms choosing to implement the Sheltered Harbor standard will soon be able to turn to Dell Technologies for a fully supported turnkey solution.

With the added benefit of leveraging a mature vault-based technology, Sheltered Harbor participants choosing PowerProtect Cyber Recovery for Sheltered Harbor can confidently meet their immediate deployment needs, as well as establish a foothold for their future data vaulting requirements. A participating institution has a path to survival and public confidence in the U.S. financial system is maintained.


Sources:

1. 2019 Thales Data Threat Report – www.thalessecurity.com/DTR
2. 2019 Symantec Internet Security Threat Report - https://www.symantec.com/security-center/threat-report
3. 2019 Cost of Data Breach report, Ponemon Institute, LLC - https://www.ibm.com/security/data-breach
4. 2019 Verizon Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/dbir/
5. 2019 Accenture Cost of Cybercrime report - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study