# Building Business Resilience to Protect Against a Destructive Cyber Attack

Cyber Recovery with Dell Technologies

DELL Technologies

# Table of Contents

# What Is Cyber Recovery? And Why Does It Matter?

Regardless of the industry, data drives today's enterprise. The global marketplace relies on the constant flow of data across interconnected networks, and digital transformation efforts put even more data at risk.

The increase in volume and value of data presents an opportunity for criminals using modern tools and tactics — in fact, 68% of business leaders state their cyber security risks are increasing (Accenture). The modern threat of cyber attacks and the importance of maintaining the confidentiality, availability and integrity of data require modern, proven solutions and strategies to protect vital data and systems

Unfortunately, in today's data-driven environment, traditional Disaster Recovery (DR) and Business Continuity are not enough to address modern cyber threats. 69% of respondents lack confidence that they could recover all business-critical data in the event of a cyber attack.[1] Although cyber attacks take many forms and attackers have a variety of motivations the target of their efforts is consistent: destroy, steal and ransom valuable digital data for financial gain, social or political purposes.

Cyber Recovery, sometimes called Isolated Recovery, is a new segment of data protection solutions designed to address the modern threat of ransomware and other cyber threats, to limit the spread of malware and reduce the surface of attack on a global basis.

**71%**

of breaches are financially motivated

**$5.2T**

of global risk over the next 5 years

A cyber attack occurs every

**39 sec**

The stability of a company's revenue and very existence hinges on its ability to isolate data and ensure its availability to support a post-cyber attack business continuance strategy and recovery operations.

[1] Dell Technologies Global Data Protection Index

# Data is Your Business…
# and Cyber Threats Puts Your Business at Risk

## Technical Risks

- All data is susceptible to a cyber attack
- Primary storage replication can replicate corrupted data
- Backup catalog is not replicated
- Recovery from tape is slow and failure prone
- Backup copies not isolated from network

## People And Process Risks

- IT and Ops access most, if not all, backup assets
- Security teams not assigned to assets
- Bad actors inside firewall can delete primary backups
- Business-critical/non-critical data are not segregated
- Backup images can be 'expired' without approval

HEALTHCARE

RETAIL

OIL & GAS

LIFE SCIENCES

FINANCIAL SERVICES

GOVERNMENT

MANUFACTURING

LAW FIRMS/ CORP LEGAL

# Top 10 Reasons to Choose Dell EMC PowerProtect Cyber Recovery

1 Dedicated hardened digital vault with physical and operational air gap

2 Protects against insider attacks by requiring multiple separate log-ins to access the vault

3 Data written to the vault is immutable and unchangeable

4 Malware may enter the vault but does NOT have ability to execute or infect data outside of the vault

5 1st to integrate full content indexing, intelligent analytics, machine learning and forensic tools

6 Quickly identify and restore last known good file or data set for rapid recovery

7 Full recovery workflow automation to quickly resume business operations

8 1st technology Solution Provider in the Sheltered Harbor Alliance Partner Program

9 1st technology provider developing a Sheltered Harbor turnkey data vaulting solution

10 Single source for solution design, implementation and support for Cyber Recovery, CyberSense and Sheltered Harbor solutions

# Disaster Recovery and Business Continuity are Not Enough to Address Modern Cyber Threats

Attackers are attacking systems, data and backups. They are encrypting the backup catalog in addition to the systems and data. Disaster recovery is online and not isolated to the degree a cyber vault is, and that makes DR vulnerable to these attacks. An air-gap cyber vault solution ensures that a protected copy of mission critical data is kept in original form.

**True cyber resilience requires cyber recovery.**

The PowerProtect Cyber Recovery solution includes a secure digital vault that is physically and logically isolated from product and backup network with an operational air gap. Critical data is protected within the vault in an immutable format with retention periods locked. This gives you the best possible chance for recovery if your primary backups have been compromised or your DR location has been breached or infected. Without a Cyber Recovery solution a company spends significant time recovering the last backups without knowing if they are good or not. This is a long, labor intense, iterative and costly.

| CATEGORY | DISASTER RECOVERY | CYBER RESILIENCE |
|---|---|---|
| Recovery Time | Close to Instant | Reliable & Fast |
| Recovery Point | Ideally Continuous | 1 Day Average |
| Nature of Disaster | Flood, Power Outage, Weather | Cyber Attack, Targeted |
| Impact of Disaster | Regional;<br>typically contained | Global;<br>spreads quickly |
| Topology | Connected,<br>multiple targets | Isolated,<br>in addition to DR |
| Data Volume | Comprehensive,<br>All Data | Selective, includes foundational services |
| Recovery | Standard DR<br>(e.g. failback) | Iterative, selective recovery; part of CR |

# Protecting Against Ransomware and Destructive Attacks

Global regulators in variety of industries agree upon how to best protect critical data and digital assets from cyber threats. They have determined that protecting a copy of critical data in an isolated manner is the best-known way to provide recovery from ransomware and destruction attacks.

“An air-gapped data backup architecture…”

“Confidentiality, integrity, availability and resilience”

“Consider maintaining backups offline and unavailable”

“Ensure backups are not connected to the networks they are backing up.”

# Why PowerProtect Cyber Recovery?

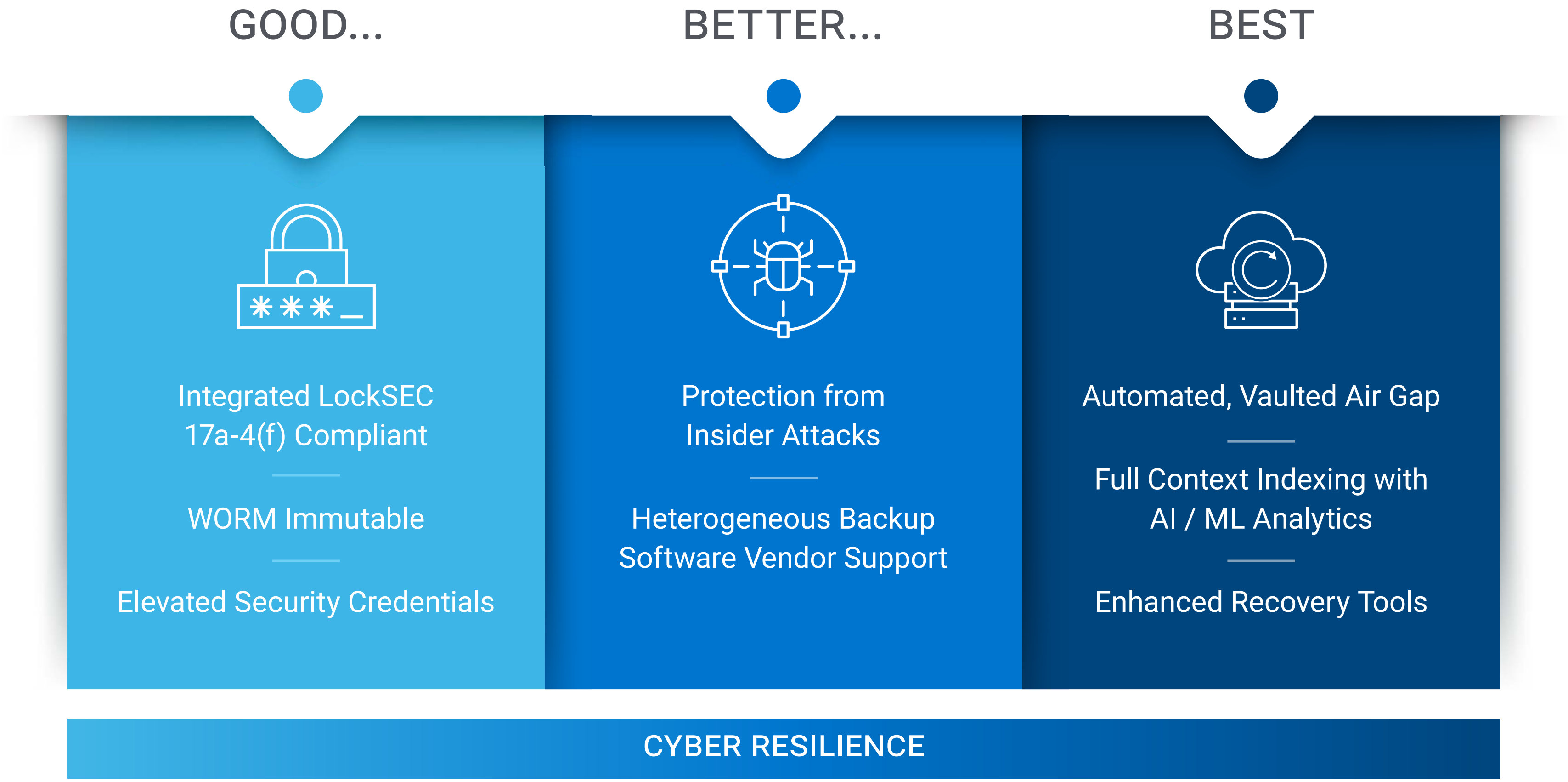
## The last line of data protection defense against cyber attacks

Dell EMC PowerProtect Cyber Recovery automates workflows end-to-end to protect critical data, identify suspicious activity, and perform data recovery when required. The Cyber Recovery vault is disconnected from the network via an automated air gap and stores all critical data off-network to isolate it from attack. This promotes business resiliency, provides assurance following extreme data loss or destruction and includes both business and technology configuration data to enable rapid recovery of the environment and resumption of normal business operations.

- ✓ Critical data resides off-network and isolated from cyber attack
- ✓ Cyber Recovery vault is air gapped from the network to prevent access
- ✓ Updated through replication process based on acceptable risk exposure limits of uptime connectivity and data loss parameters
- ✓ Remediated against threats while off-line and capable of retaining iterative copies to current –n versions (based on business needs)
- ✓ Allows complete visibility into the integrity of all the data and metadata protected
- ✓ Increase effectiveness of Prevent/Detect cybersecurity when performed in protected environment
- ✓ Diagnosis of attack vectors can take place within an isolated vault environment
- ✓ Analytics monitor the integrity of data that is backed up and the integrity of the backup catalog

# Why PowerProtect Cyber Recovery is Best

Only PowerProtect Cyber Recovery combines multiple layers of protection and security into a turnkey solution to provide maximum protection for critical data.



GOOD...

Integrated LockSEC 17a-4(f) Compliant

WORM Immutable

Elevated Security Credentials

BETTER...

Protection from Insider Attacks

Heterogeneous Backup Software Vendor Support

BEST

Automated, Vaulted Air Gap

Full Context Indexing with AI / ML Analytics

Enhanced Recovery Tools

CYBER RESILIENCE

# CyberSense to Detect, Diagnose and Quickly Recover from Cyberattacks

Fully integrated with Dell EMC PowerProtect Cyber Recovery, CyberSense audits your data and detects indicators of compromise and attacks:

- Proactively understand when an attack is in motion with over 99% accuracy
- Enable you to identify and diagnose potential threats and recover "known good" data quickly
- Reduce downtime and business interruptions so you can resume normal operations with confidence

When an attack gets past real-time defenses and corrupts files or databases, you have confidence that clean data is isolated in the Cyber Recovery vault and has been analyzed by CyberSense. CyberSense is constantly monitoring data integrity within the vault and detects mass deletions, encryption, and over 100 types of changes in files and databases that result from common attacks. If CyberSense detects signs of corruption, an alert is generated, with the attack vector and listing of files affected. This enables business operations to continue with minimal or no interruption and quickly rather than within many weeks or months.

Analytics

Machine Learning

Forensic Tools

# 8 Ways CyberSense Powerfully Combats Ransomware and Other Cyber Attacks

1 Detect cyber attack risks that competitors can’t identify

2 Machine learning and unique full content level analysis

3 Provides over 100 heuristics to identify suspicious activity

4 Deep integration with Cyber Recovery for workflow automation and alerting

5 Post-attack forensics to quickly determine attack vector and impacted data list

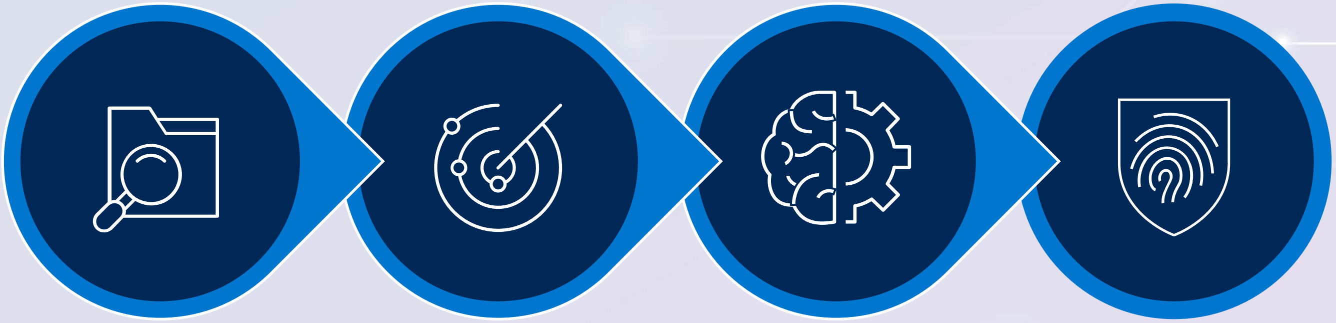
6 Identify last known good dataset for recovery

7 Unparalleled resiliency to recover and restore data quickly from an attack

8 All performed within the security of the Cyber Recovery vault

# CyberSense Enables Early Detection and Assured Recovery

CyberSense performs full content indexing of all data entering the vault and generates statistics that are compared to previous scans. Analytics are then input into the machine learning model and the results are used to determine the data's integrity and if the data has been corrupted. In addition, CyberSense provides reports and details to assist in the diagnosis and recovery from the attack and provides the attack vector utilized to manipulate the data.



**COMPREHENSIVE INDEX**

Changes in content over time

**SECURITY ANALYTICS**

100+ statistics indicative of cyber attack

**MACHINE LEARNING**

Trained on thousands of trojans and 20+ attack vectors

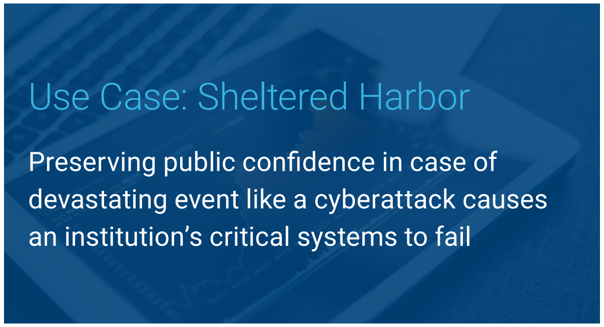
### Cyber Recovery with CyberSense

- Full content indexing
- Attack vector notification
- Corrupted file identification
- Data changes / deletions
- Breached user accounts
- Breached executables
- Identification of last good copy

# Dell EMC PowerProtect Cyber Recovery In Action

"Cyberattacks are maturing every minute, in every corner of the world. To succeed in this environment, we had to change how we think about data, how we use data and how we protect data. We want to keep it clean coming in then make sure it's backed up. Then we have to test that protection, make sure that it's in a data bunker so that whatever plan of attack is coming at us from malware in the future, we have 100% protected that golden copy and we can go pull that out of the safe, the protected area, and put it back, so people's lives are back to normal, so people do not experience disruption."

BOB BENDER
CHIEF TECHNOLOGY OFFICER,
FOUNDERS FEDERAL CREDIT UNION
READ MORE



## Use Case: Sheltered Harbor

Preserving public confidence in case of devastating event like a cyberattack causes an institution's critical systems to fail

## Case Study: Healthcare

Protecting critical sensitive data and business operations

## Case Study: Financial Services

Protecting securities trading platform and critical data

# Proven, Experienced Cyber Recovery Consulting Services

With a team of consultants who bring deep experience in the design and deployment of Cyber Recovery solutions, as well as decades of disaster recovery and business knowledge, Dell can help your business operationalize a Cyber Recovery vault. This can include identifying vault requirements, data sets, apps, workload sequencing and more for the vault.

### Cyber Recovery Base Delivery

Quickly install and initialize operation of the cyber recovery vault

### Cyber Recovery Advanced Implementation

Provides a limited ability to deliver some custom options, generate a sample runbook and work with some third-party software

### Cyber Recovery Advisories

Cyber Recovery Advisory services provide varying levels of strategic options, target architectures, and even an actionable roadmap for Cyber Recovery adoption

### Custom Cyber Recovery

Custom cyber recovery services implement advanced options, customized recovery plans, additional runbooks and more

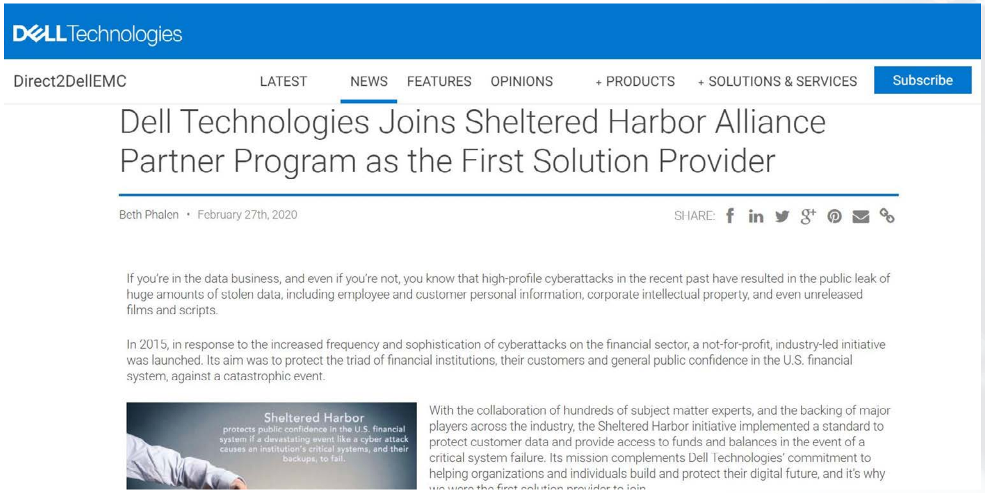
# Protecting Customer Data and Preserving Public Confidence in U.S. Financial Markets

## Leading the Way in Sheltered Harbor Preparedness

Sheltered Harbor was created to protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyberattack causes critical systems—including backups—to fail. By implementing the Sheltered Harbor standard, institutions can be prepared to provide customers timely access to balances and funds in these worst-case scenarios.

Dell Technologies is the first Solution Provider in the Sheltered Harbor Alliance Partner Program and anticipates endorsement of its solution in June 2020.

LEARN MORE



Dell Technologies Joins Sheltered Harbor Alliance Partner Program as the First Solution Provider

Beth Phalen • February 27th, 2020

If you're in the data business, and even if you're not, you know that high-profile cyberattacks in the recent past have resulted in the public leak of huge amounts of stolen data, including employee and customer personal information, corporate intellectual property, and even unreleased films and scripts.

In 2015, in response to the increased frequency and sophistication of cyberattacks on the financial sector, a not-for-profit, industry-led initiative was launched. Its aim was to protect the triad of financial institutions, their customers and general public confidence in the U.S. financial system, against a catastrophic event.

Sheltered Harbor protects public confidence in the U.S. financial system if a devastating event like a cyber attack causes an institution's critical systems, and their backups, to fail.

With the collaboration of hundreds of subject matter experts, and the backing of major players across the industry, the Sheltered Harbor initiative implemented a standard to protect customer data and provide access to funds and balances in the event of a critical system failure. Its mission complements Dell Technologies' commitment to helping organizations and individuals build and protect their digital future, and it's why we were the first solution provider to join.

SHELTERED HARBOR

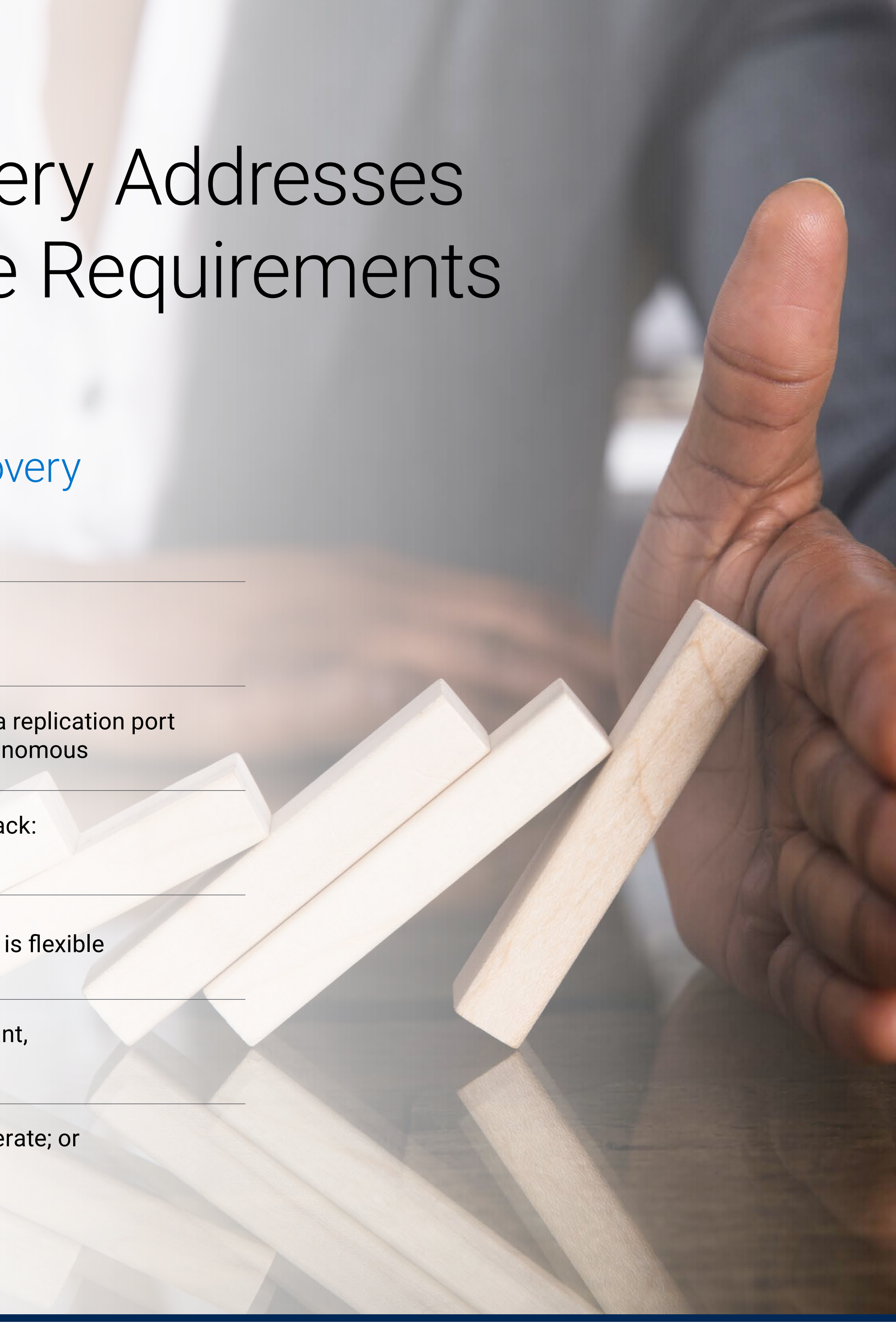
### Core Elements of Sheltered Harbor

Data Vaulting

Resiliency Planning

Certification

# PowerProtect Cyber Recovery Addresses Sheltered Harbor Resilience Requirements



| SHELTERED HARBOR<br>DATA VAULT | PowerProtect Cyber Recovery for Sheltered Harbor |
|---|---|
| Unchangeable | Data in vault is retention locked (assessed to be compliant with 17a-4(f)(2)) |
| Separated | Physical and network isolation — air gap via replication port enable / disable. Fully automated and autonomous |
| Survivable | Designed to withstand a focused cyber attack: APT, Insider, Ransomware |
| Accessible | Accessible to owner, transfer methodology is flexible |
| Decentralized | Flexible physical location: one per participant, consolidated, etc. |
| Owned by participant | Flexible consumption options: own and operate; or own and have managed by third party |

# Healthcare Industry

## Protect critical sensitive data and business operations

### Challenges

- Targeting of healthcare institutions, impact of large attacks
- Budget constraints
- Regulatory pressures

### PowerProtect Cyber Recovery

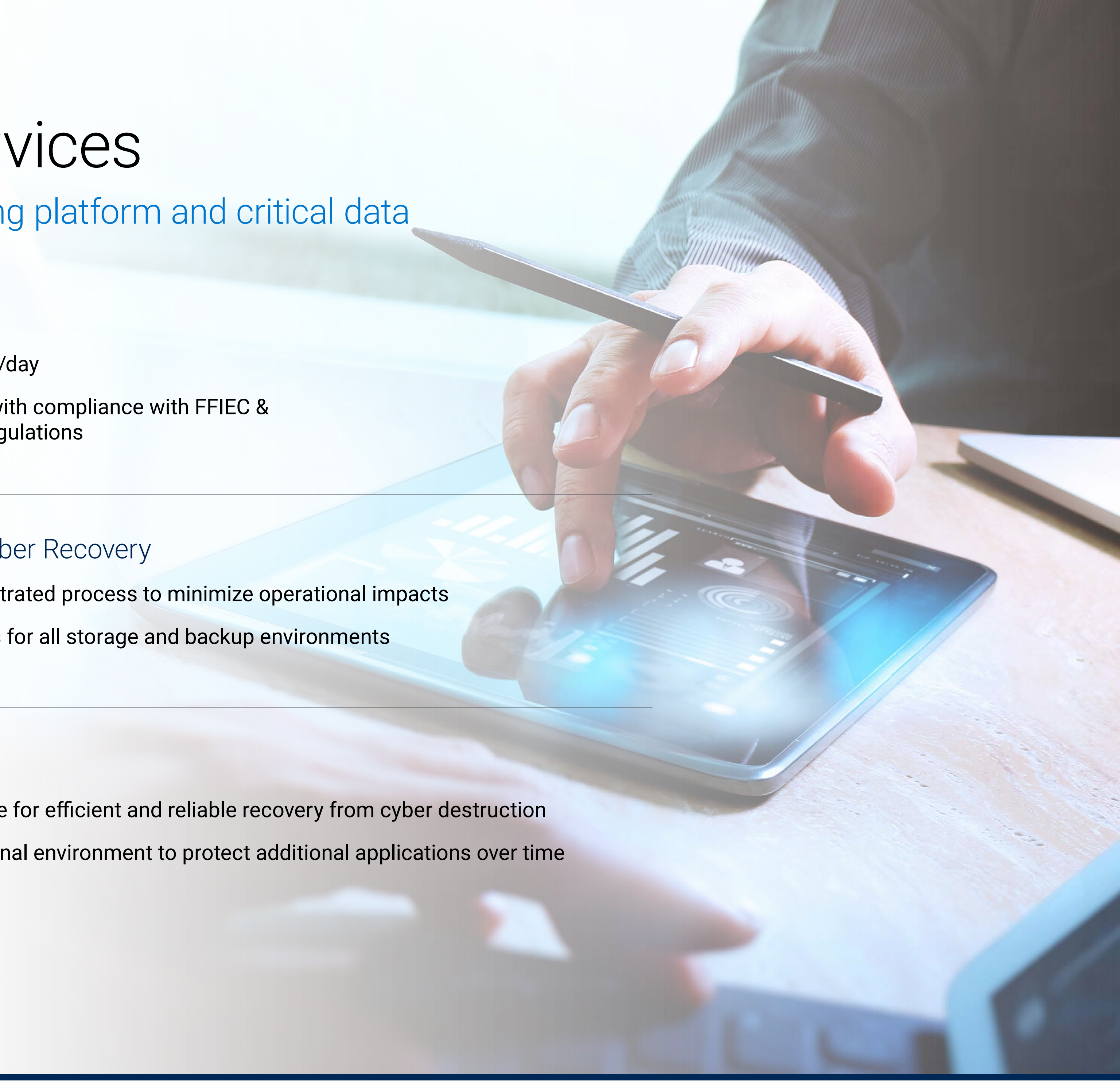
- Quick deployment of turnkey operational air gap and vault
- CyberSense for active cyber threat analysis / alerts

### Results

- “Nobody else has an air gap like Dell Technologies”
- Prepared for response with minimal investment vs. risk of $10M catastrophic incident

# Financial Services

## Protect securities trading platform and critical data



### Challenges

- Outage risks $10M/day
- Board concerned with compliance with FFIEC & Federal Reserve regulations

### PowerProtect Cyber Recovery

- Automated, orchestrated process to minimize operational impacts
- Recovery runbooks for all storage and backup environments

### Results

- Met Board mandate for efficient and reliable recovery from cyber destruction
- Provided foundational environment to protect additional applications over time

# Start Now! Your Checklist to Build Cyber Resiliency

## Take the Next Step

### Authentication, Identity & Security

- Active Directory / LDAP
- DNS dumps
- Certificates
- Event logs (including SIEM data)

### Networking

- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / Microcode / Patches

### Storage

- Backup Hardware configuration
- SAN / Array configurations
- Storage Abstraction settings
- Firmware / Microcode / Patches

### Documentation

- CMDB / asset D/R and Cyber Recovery run-books and checklists
- Management extracts
- HR Resources and contacts lists

### Host and Build Tools

- Physical / Virtual Platform Builds
- Dev Ops tools & automation scripts
- Firmware / Microcode / Patches
- Vendor software
  - > Binaries (golden images)
  - > Configurations & settings

### Intellectual Property

- Source code
- Proprietary algorithms
- Developer libraries

## Protecting your business starts with protecting your data.

Learn more at www.DellTechnologies.com/CyberRecovery