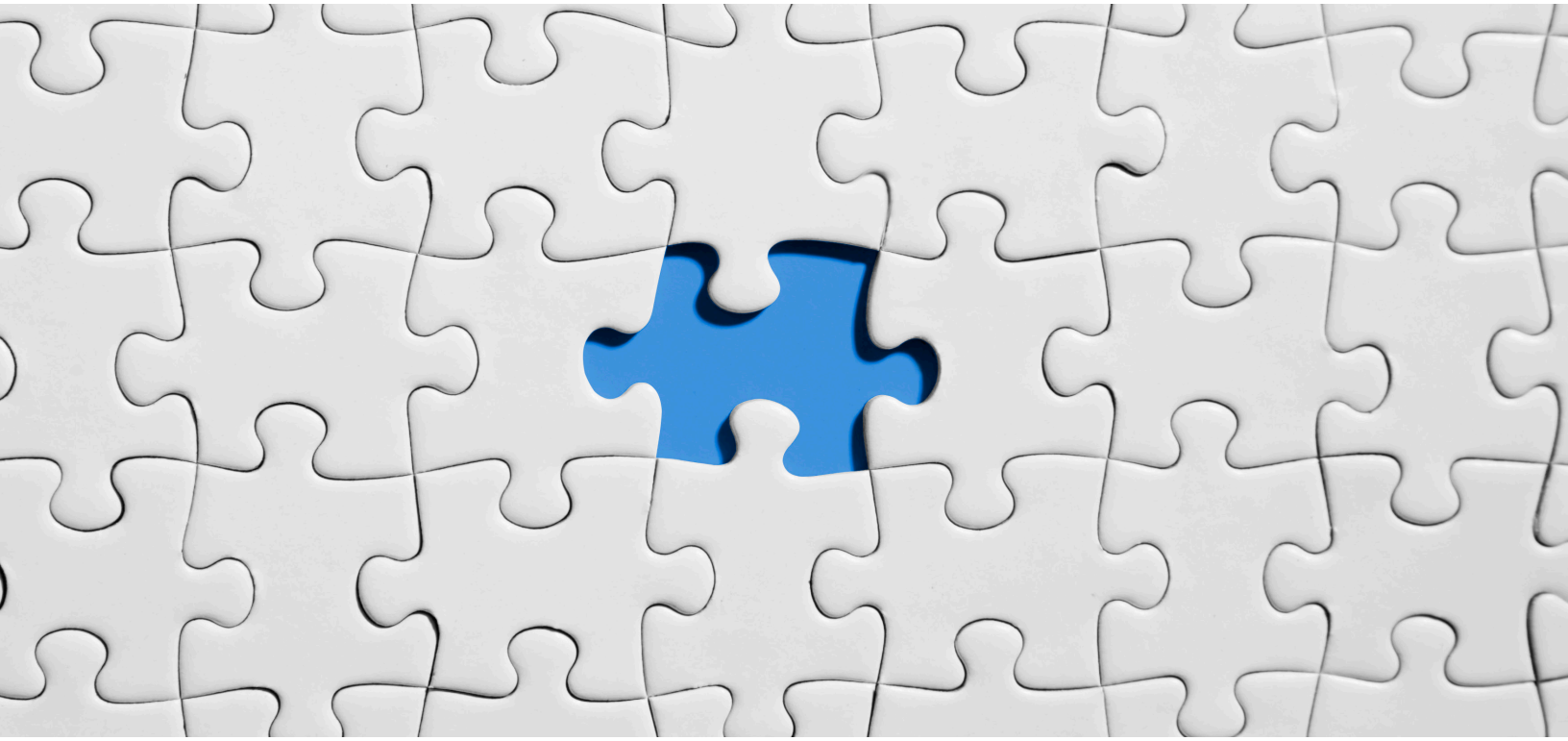
DELL Technologies

# SECURING INDUSTRIES WITH CYBER RECOVERY




## Sindhu Hegde

Systems Engineer Analyst

Dell Technologies

Sindhu.h@dell.com

## Varun Christian

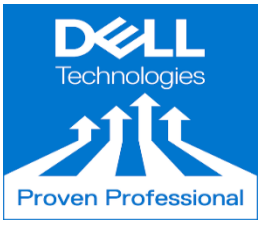
Systems Engineer Analyst

Dell Technologies

Varun.christian@dell.com


DELL Technologies Proven Professional

Knowledge Sharing Article




The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

## Table of Contents

## Abstract

Data is a key component of a digitalized era and its protection is a priority for all organizations. As the digitalization grows, cyber-attacks also increase, and these cyber threats incur huge damage for industries; it's not hundreds/thousands of dollars of loss anymore – the damage is in trillions.

Cyber-attacks take many different forms and the attackers may have a variety of motivations, techniques and even platforms from which to launch their attacks. Cyber-attack can occur in any industry vertical – financial, healthcare, education and so forth.

Businesses unable to recover from having their sensitive information compromised places them in a costly position financially and threatens the long-term prospects of the business itself. Hence, it is very important for businesses to not only protect their critical data in a secured, air-gapped vault but also be able to recover it correctly whenever required. Dell Technologies Power Protect Cyber Recovery can save businesses from such deadly attack's and weeks of business downtime.

This Knowledge Sharing article provides an overview of Dell Technologies Power Protect Cyber Recovery air-gapped, vault solution and the vital role it plays in securing data for across all industry verticals. Also discussed is how it differs from traditional backup/replicated copy – what businesses typically require to protect their most valuable asset – data.

## What is Cyber Threat?

Data encryption and malware attacks, generally known as “cyber threats” are now being designed to target data backups in ways that were once unimaginable. As daily security incidents create new challenges, we see threats not only against production data but also against secondary copies of data used for backup, disaster recovery, analytics, and more.

Various kinds of cyber-attacks can gain access to backup and disaster recovery locations, leaving both primary and backup data unusable and significantly delaying the ability to restore production-level operations. The interconnection between company servers, end-user devices, and the rest of the Internet at large leaves business-critical data open to attack from malicious entities that take sensitive data hostage, ruining consumer confidence and threatening revenues. When it comes to protecting critical assets and avoiding downtime, cybersecurity is an often-overlooked piece of the puzzle, but a critical step in the risk management process.

## Why Cyber Recovery?

Cyber-attacks and their results are the reasons as why “Cyber Recovery” has been an integral IT priority governing the methods, processes and tactics used to protect data and systems. It means implementing the technology and best practices needed to prevent unauthorized data access and also, by making backup copies more resilient, enabling recovery after more sophisticated attacks.

Therefore, the goal is to demonstrate confidence in data integrity using one of the unique air-gapped solutions and immutable data copies that assure availability of data within minutes for continued business operations. Rather than pay the ransom, the organization decided to focus on recovery. Paying ransom is not recommended and would have not been effective in this case. Hackers promised a decryption key upon ransom payment, but forensic analysis of the malware determined that a decryption key would not have allowed the data to be recovered.

Dell Technologies Cyber Recovery solution is not a disaster recovery or a secondary copy of the data; it can be determined as the last line of defense. Not just securing and protecting the data, one should also be able to recover the data whenever there is an attack and avoid downtime or surrendering to any kind of malware and losing thousands of dollars to the attackers.

## History of Industry Verticals without/before adapting Cyber Recovery

Industry Verticals refer to sectors like Healthcare, Education, Finance, Fashion, Media, Government, the list goes on.

In today’s data landscape, security and privacy are at the top of any industry’s agenda. No industry wants to be in the news when it comes to data protection, which is why the ability to recover instantly at any point in time is required. Cyber-attacks occur in all industries and it is very important to safeguard the data no matter which industry the data belongs to.

For example:

- A large financial and banking Company was attacked and lost data throughout their environment. This a good example of a multi-stage attack conducted for a single motive. Sensitive data was exposed and while the attackers demanded ransom. However, for banking/financial institutes, safeguarding data is paramount since it is directly associated with money. The attackers can also intrude on any of the individual bank accounts.

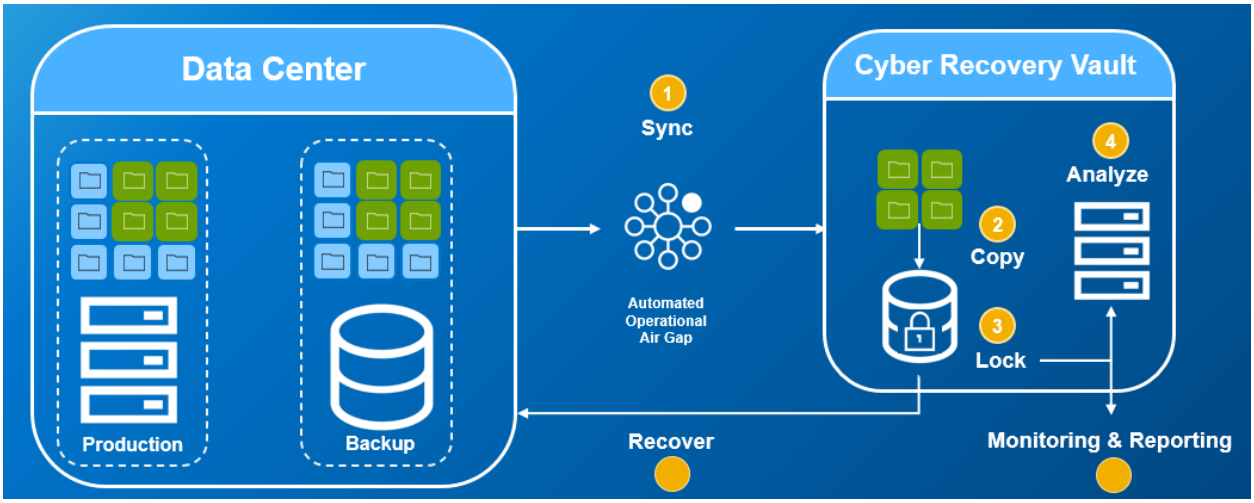
  In this scenario, the bank has to either pay the huge ransom to the attackers or compromise their data – clearly not an option because they would be losing customers' money and trust.

- In health sectors, data can be related to a patient's personal information which would be critical for them. Should an attack occur, all the health information and personal information can be in the attacker's hand, posing a great threat to the hospital.

## Architectural overview of Cyber Recovery solution

The Cyber recovery has production site and an air gapped solution which has immutable copies/retention locked copies. The data sent to the vault is synchronized.

To read/write or to perform test on the retention-locked data that is residing in the vault, we need to create a sandbox in the vault and recover the data from the vault to the production site whenever the production is site is up and running.




The PowerProtect Cyber Recovery solution protects the most critical data in a vault environment. The vault is ideally physically isolated – a locked cage or room – and is always logically isolated via an operational air gap. Vault components are never accessible from production, and access to the vault target – when the air gap is unlocked – is extremely limited. This is a key to the maturity of our solution (and can be covered in a separate, more technical

session). The vault is not an extra data center – it is usually located at the production or corporate data center and more frequently now, with a third-party solution provider.

The vault operates in 4 basic steps:

1) Data representing critical applications is synced through the air gap, which is unlocked by the management server into the vault and replicated into the vault target storage. The air gap is then re-locked.
2) A copy of that data is made. Vault retention is configurable, but most keep about a month's worth of copies.
3) The data is retention-locked to further protect it from accidental or intentional deletion.
4) The data is optionally analyzed by our analytics engine, CyberSense (more on that later).

Recovering data from the vault in the event of a cyber-attack or simply for recovery testing procedures is critical and there are a number of ways recovery can be performed.

Monitoring and reporting is also provided from within the vault and can be shared outside of the vault environment in a variety of secure methods which we will discuss in more detail.

## Benefits of Dell Technologies PowerProtect Cyber Recovery

- With Cybersense – Cybersense is the key software to analyze the malware attack in the vault. It is fully integrated with cyber recovery and monitors files and databases to determine if an attack has occurred based on data corruption. With 100's of analytics that is available, it helps to determine whether a data is valid and useable for recovery or has somehow been improperly altered or corrupted such that it is suspect and potentially unusable.

- Process of how CyberSense works – (1) Scan: CyberSense scans critical data sources archived in the Dell EMC Cyber Recovery vault. This includes unstructured files and databases to create an observation. (2) Analytics: More than 100 statistics generated from each observation. Statistics include analysis of file entropy, similarity, corruption, mass deletion/creations, and much more. (3) Analysis: Machine Learning algorithms are used to analyze the statistics to indicate if an attack on the data has occurred. (4) Repeat: The process repeats as Cyber Recovery backs up data incrementally to the vault and a new observation is created. New observations are compared to previous observations to see how data changes. (5) Investigate: Forensic reporting and analysis tools are available after an attack to find corrupted files and diagnose the type of ransomware.

-

- 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, recovery and other data protection systems.

- The best - Air gap! – An air gap physically isolates an unsecure system or network. A secure air gap needs to be inaccessible and offline, not just in a different location; otherwise, it can still be compromised by bad actors who attempt to breach it or use an IT system for criminal activity.

- Sheltered Harbor – In 2015, about 30 US financial institutions formed Sheltered Harbor. Its mission is to protect confidence in the financial system if a devastating event – like a cyber-attack – causes an institution's critical systems to fail. In short, it is designed to protect the financial system and the consumer while the bank recovers its systems. A key component of the Sheltered Harbor specification is secure storage of the Sheltered Harbor-specific data set in a vault. Dell Technologies is the first solution provider in the Sheltered Harbor alliances program.

## Conclusion

A truly secure, logical air gap needs to protect data by making it inaccessible and offline, not just by storing it in a different location; otherwise, it can still be compromised by bad actors.

It can be difficult to effectively protect against inside threats because they typically have physical access to systems and more knowledge than outsiders. Customers should think beyond just ransomware attacks and consider what an inside threat could do to their systems and data. Automation and orchestration make it easy and efficient to operate the PowerProtect Cyber Recovery solution. In addition, it is fully supported with a help desk, future releases, secure development processes, and more.

CyberSense runs analytics on the data in the vault to enable a speedy recovery after an attack. Analytics helps determine whether a data set is valid and useable for recovery or has somehow been improperly altered or corrupted so that it's "suspicious" and potentially unstable. Dell Technologies is the first solution provider in the sheltered harbor alliances program.

Having Dell Technologies Power Protect Cyber Recovery air gapped, vaulted solution in any industry vertical saves up to millions of dollars and safeguards the data from intruders.