SYNAPSE 360

PowerProtect Cyber Recovery Benefits

Isolation

Physical and Logical Separation of Data

PowerProtect Cyber Recovery vault is protected with operational air gap either on-premises or in cloud and multi-cloud offers

Immutability

Preserve Original Integrity of Data

Multiple layers of security and controls protect against destruction, deletion and alteration of vaulted data

Intelligence

ML and Analytics Identify Threats

CyberSense enables assured recovery of good data and offers insight into attack vectors from within the recovery vault

1. Isolation

Gartner recommends that organisations who are looking to protect themselves need to create an isolated recovery environment.

PowerProtect Cyber Recovery provides a physically and logically isolated data centre environment that is disconnected from corporate and backup networks and restricted from users who don't have the proper clearance.

Automated workflows securely move business critical data to an isolated environment via an operational air gap. You can also create protection policies in less than 5 steps and monitor potential threats in real time with an intuitive dashboard.

The vault is ideally operated in a physically restricted area, such as a cage or locked room, that helps to guard against an insider threat.

When the air gap is an a "locked" state — no data can flow — there is no access to any part of the solution.

2. Immutability

PowerProtect Cyber Recovery offers an automated data copy and air gap, which creates unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production /backup environment and the vault.

Using the Compliance Mode Retention Lock capability from Dell PowerProtect DD, data is prevented from deletion or change for a set time period. The lock cannot be overridden, even by an administrator with full privileges. PowerProtect DD offers unique enhancements that further secure the lock from an attack on the clock (or NTP server), which might otherwise allow a bad actor to create an early expiration of the lock.

Those who do not want or require such a strong control, or want operational flexibility, can configure governance retention lock.

3. Intelligence

CyberSense allows you to stay ahead of the rapidly changing threat landscape and sophisticated cyber criminals with CyberSense adaptive analytics, machine learning (ML) and forensic tools to detect, diagnose and accelerate data recovery within the security of the Cyber Recovery vault.

CyberSense is fully integrated with PowerProtect Cyber Recovery and monitors files and databases to determine if an attack has occurred by analysing the data's integrity.

Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically scans the backup data, creating point-in-time observations of files, databases, and core infrastructure.

These observations enable CyberSense to track how files change over time and uncover even the most advanced type of attack. Automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.