SYNAPSE 360

5 Reasons to trust PowerProtect Cyber Recovery

Protect and recover

Cyberattacks are designed to destroy, steal or otherwise compromise your valuable data – including your backups.

PowerProtect Cyber Recovery provides the trusted data protection and recovery needed in keeping your organisation protected from outside or insider cyberthreats.

Here are the top five reasons why customers trust PowerProtect Cyber Recovery to isolate your critical data away from sophisticated cyber threats and recover known good data.

1 Physical and logical isolation of critical data

The PowerProtect Cyber Recovery air-gapped vault offers multiple layers of protection to provide resilience against cyberattacks, even from an insider threat.

Critical data is away from the attack surface, physically isolating it within a protected part of a data centre, or in the cloud. It requires separate security credentials and multi-factor authentication for access different from other administrative access controls, such as disaster recovery or data backup administration.

2 Immutability to preserve original integrity of your data

PowerProtect Cyber Recovery offers multiple layers of security and controls that protect against destruction, deletion and alteration of vaulted data.

Using PowerProtect DD's Compliance Mode Retention Lock capability, data is prevented from deletion or change for a set time period, usually two weeks to a month (customer configurable). The lock cannot be overridden, even by an administrator with full privileges.

Unique to PowerProtect DD are 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.

3 CyberSense: an intelligent layer of protection

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

Running analytics on the data in the vault is a vital component to enable a speedy recovery after an attack. Analytics help to 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 unusable. The entire contents of the critical data files are evaluated, not just its metadata, to deliver superior analytics without exposure in the vault to potential risk.

4 Flexible recovery options

There are flexible recovery options available to meet your cyber resiliency requirements. Recovery procedures mostly follow standard processes, but special considerations apply across various scenarios. Recovery is integrated with your incident response process.

After an event occurs, the incident response team analyses the production environment to determine the root cause of the event. CyberSense also provides post-attack forensic reports to understand the depth and breadth of the attack and provides a listing of the last good backup sets before corruption.

5 Trusted strategy and support

At Synapse360, we can help strategise, implement, adopt and scale a Cyber Recovery solution to support your organisation.

Whether aligning protection and recovery with business needs, deploying cyber recovery technologies, responding to a cyber incident, or ensuring your teams are trained on our experts' latest skills, we are here for you every step of the way.

Great! I'm ready to learn more...

0330 660 0001 hello@synapse360.com synapse360.com