Top Reasons to Trust Dell PowerProtect Cyber Recovery

5

Protect and recover critical data with confidence

Cyberattacks are designed to destroy, steal or otherwise compromise your valuable data – including your backups. The modern threat of cyberattacks and the importance of maintaining the confidentiality, availability, and integrity of data require modern solutions and strategies to protect vital data and systems. PowerProtect Cyber Recovery provides the trusted data protection and recovery needed in keeping the organization protected from outside or insider cyberthreats. Here are the top five reasons why customers trust Dell PowerProtect Cyber Recovery to isolate your critical data away from sophisticated cyber threats and recover known good data so that you can resume business operations with confidence.

1 | Physical and Logical Isolation of Critical Data

PowerProtect Cyber Recovery protects critical data through an air-gapped vault environment. The PowerProtect Cyber Recovery 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 center, 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. Safeguards include an automated operational air gap to provide network isolation and eliminate management interfaces that could be compromised. PowerProtect Cyber Recovery automates data synchronization between critical production systems and the data vault creating immutable copies with locked retention policies.

2 | Immutability to Preserve the 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. Those who do not want or require such a strong control, or want operational flexibility, can configure governance retention lock (which is also the available mode on our PowerProtect DD Virtual Edition (DDVE)).

5 Top Reasons to Trust Dell PowerProtect Cyber Recovery

3 | Machine Learning with CyberSense For 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. CyberSense analytics are powerful because they can read and evaluate the backup format, so there is no need to restore data. 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

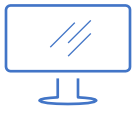
Dell Technologies offers flexible recovery options to meet your cyber resiliency requirements. Recovery procedures mostly follow standard processes, but special considerations apply across various scenarios. Recovery is integrated with your incident response process. After an event occurs, the incident response team analyzes 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. Then, when the production is rea dy for recovery Cyber Recovery provides management tools and the technology that performs the actual data recovery. It automates the creation of the restore points that are used for recovery or security analytics. The ultimate goal of Dell Cyber Recovery is to provide an organization with the confident and most reliable path to recovery of business-critical systems.

5 | Trusted Strategy with Dell Resiliency Services

Dell Technologies Services will strategize, implement, adopt and scale a Cyber Recovery program to support the organization. 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 are here for you every step of the way. The latest Global Data Protection Index survey showed that 62% are concerned their organization's existing data protection measures may not be sufficient to cope with malware and ransomware threats[1]. With Dell Technologies, organizations can protect their business from ransomware, insider attacks, and other cyber threats with confidence.

[1] Global Data Protection Index 2021: https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm

---



Learn more about Dell PowerProtect Cyber Recovery solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #PowerProtect

DELL Technologies