DELL Technologies

Solution Brief

Dell PowerProtect Cyber Recovery

Modern and Resilient Protection for Critical Data from Ransomware and Destructive Cyberattacks.

WHY CYBER RECOVERY?

Cyberattacks are designed to compromise your valuable data – including your backups. Protecting your critical data and recovering it with assured integrity is key to resuming normal business operations post-attack.

Here are components of a cyber resilient solution:

Data Immutability
Create unchangeable data copies to preserve data integrity and confidentiality with layers of security and controls.

Data Isolation and Governance
An isolated recovery environment that is disconnected from corporate and backup networks with elevated restricted user access.

Automated Data Copy and Air Gap
Create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production / backup environment and the vault.

Intelligent Analytics
Automated integrity checks using AI-based Machine learning and full-content indexing with powerful analytics within the safety of the vault to determine whether data has been impacted by malware.

Recovery and Remediation
Workflows and tools to perform recovery after an incident using dynamic restore processes and your existing DR procedures.

Solution Planning and Design
Expert guidance to select critical data sets, applications and other vital assets to determine RTOs and RPOs and streamline recovery.

The Challenge: Cyberattacks are the enemy of data-driven businesses.

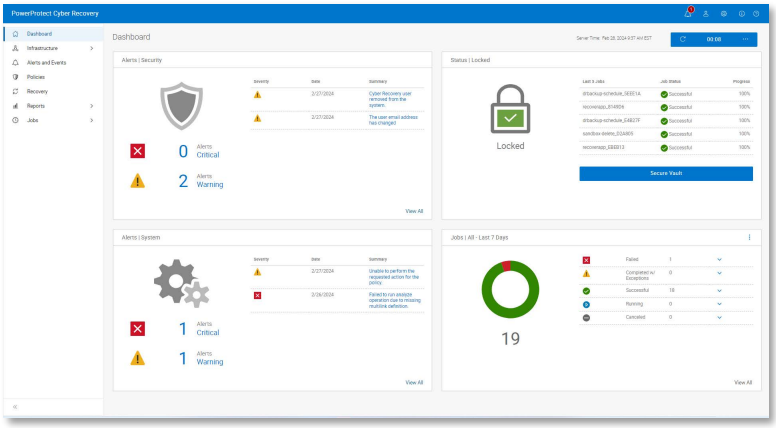
Data is the currency of the digital economy and a vital asset that must be safeguarded, kept confidential and readily accessible. The modern global marketplace depends on the continuous flow of data across interconnected networks. Digital transformation initiatives and the increasing use of generative AI heighten the exposure of sensitive information.

This makes your organization's data an attractive and lucrative target for cyber criminals. Regardless of the industry or size of the organization, cyberattacks continually expose business and governments to compromised data, lost revenue due to downtime, reputational damage and costly regulatory fines.

Having a cyber resilience strategy has become a mandate for business and government leaders, yet many organizations lack confidence in their data protection solutions. The Global Data Protection Index reported that 79% of IT decision makers are concerned they will experience a disruptive event in the next 12 months, and 75% are concerned their organizations existing data protection measures may not be sufficient to cope with malware and ransomware threats[1].

The Solution: Dell PowerProtect Cyber Recovery

To reduce business risk caused by cyberattacks and to create a more cyber resilient approach to data protection, you can modernize and automate your recovery and business continuity strategies and leverage the latest intelligent tools to detect and defend against cyber threats.



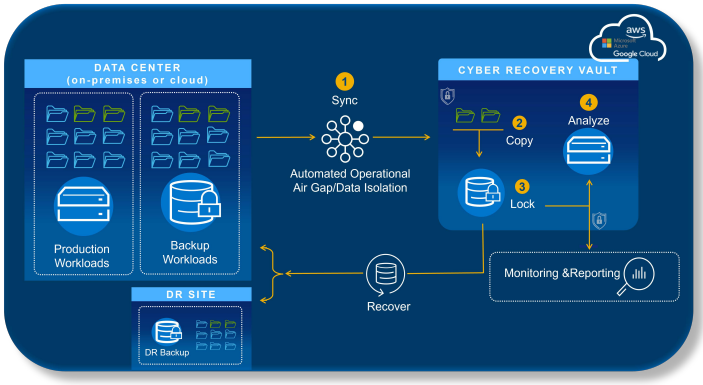
Dell PowerProtect Cyber Recovery provides proven, modern, resilient and intelligent protection to isolate critical data, identify suspicious activity and accelerate data recovery allowing you to facilitate a smarter recovery of your critical data to quickly resume normal business operations.

PowerProtect Cyber Recovery – Immutability, Isolation, and Intelligence

Immutability - PowerProtect Data Domain

PowerProtect Data Domain is the foundation of Dell PowerProtect Cyber Recovery. With multiple layers of Zero Trust security, it provides immutable backup copies to ensure data integrity and confidentiality. Features such as hardware root of trust, secure boot, encryption, retention lock, role-based access, and multi-factor authentication help ensure the recoverability of your data.

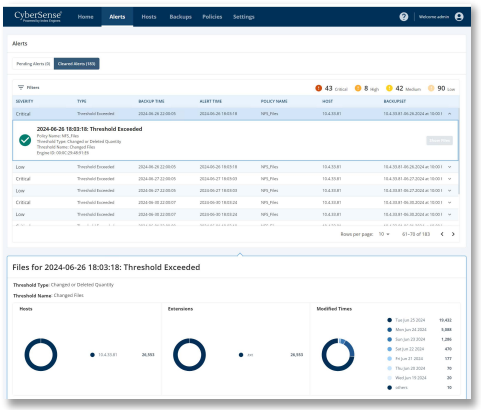
Isolation - Cyber Recovery vault



The PowerProtect Cyber Recovery vault is an isolated recovery environment (IRE) that offers multiple layers of protection to provide resilience against cyberattacks even from an insider threat. Its operational air gap automatically moves (Sync) critical backup data copies away from the attack surface of production environments, including open systems and mainframes to a physically isolated vault. Once critical data has been sync'd to the vault, an immutable copy is automatically created to keep the data from being modified. With dedicated management, network, and services independent of the production environment, separate security credentials and multi-factor authentication are required for access the data for recovery and testing operations.

Intelligence - CyberSense®

PowerProtect Cyber Recovery is the first solution to fully integrate CyberSense® for smarter recoveries against cyber threats - all within the security of the cyber recovery vault. CyberSense goes beyond metadata-only solutions, with full-content analytics it detects data corruption after an attack with 99.99% accuracy[2] and facilitates intelligent and rapid restoration. CyberSense leverages immutable data backups to observe how data changes over time and utilizes AI-based machine learning to detect signs of corruption indicative of a ransomware attack. CyberSense detects mass deletions, full and partial encryption, and other suspicious changes in core infrastructure (including Active Directory, DNS, etc.), user files, and databases resulting from sophisticated attacks. Custom threshold alerts can be created and if signs of corruption are detected, the alerts dashboard and post-attack forensic reports facilitate swift diagnosis of the scale and impact of the attack including the identification of a clean copy of data to recover your critical systems.



PowerProtect Cyber Recovery – Deployment Options

Cyber Recovery in Hybrid and Multi-cloud environments

Critical data can exist in many different locations across a business, whether on-premises, collocated at different datacenters or globally in multiple clouds and regions. Regardless of the location, the data needs to be secure and non-comprised when recovery from cyberattacks is needed.

PowerProtect Cyber Recovery is available and transactable through public cloud marketplaces for *AWS, Microsoft Azure*, and *Google Cloud* to provide fast access to protect data in a cyber recovery vault in the cloud. PowerProtect Cyber Recovery automates the synchronization of critical data between production systems and the cyber recovery vault in the public cloud. Unlike standard cloud-based backup solutions, access to management interfaces is locked down by networking controls and require separate security credentials and multi-factor authentication for access. Scattering and duplicating data across multiple clouds can lead to security and compliance risks, potential synchronization issues, and increased resource costs. This approach can also reduce visibility across your various environments, leading to insufficient protection from constantly evolving cyber threats.

Dell PowerProtect Cyber Recovery with MultiCloud Data Services, powered by Faction makes your data simultaneously accessible to public cloud providers without compromising security and provides the freedom to choose any cloud provider and avoid vendor lock-in. This secure data vaulting service is a logically air-gapped vault built upon secure, multi-cloud-enabled infrastructure that safeguards your critical data from cyberattacks. When data recovery is required, you can choose to restore your data from your vault to AWS, Microsoft Azure, Google Cloud, Oracle Cloud, or back to your on-prem environment.

Dell APEX Protection Storage All-Flash for Cyber Recovery

While critical data continues to grow, the ability to recover from a cyber event swiftly and efficiently is paramount for ensuring business continuity and cyber resilience. Organizations that are expanding the management of critical data must excel in retrieving their data from isolated recovery environments, such as the Cyber Recovery vault. Dell APEX Protection Storage All-Flash, based on a software-defined version of PowerProtect Data Domain, offers a streamlined, energy-efficient, and cost-effective cyber recovery solution that features enhanced CyberSense analytics and rapid restoration capabilities to meet organization SLAs. By utilizing less hardware, space and energy, organizations can enhance data access speeds, boost operational efficiency, and ensure data integrity, ultimately leading to reduced downtime and overall maintenance costs.

PowerProtect Cyber Recovery – Getting Back to Business

Recovery and Remediation

PowerProtect Cyber Recovery provides automated restore and recovery procedures to bring business critical systems back online quickly and with confidence. 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 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 ready for recovery Cyber Recovery provides management tools and the technology that performs the actual data recovery.

Solution Planning and Design

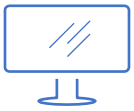
Dell Professional Services for Cyber Recovery help you determine which business critical systems to protect and can create dependency maps for associated applications and services, as well as the infrastructure needed to recover them. The service also generates recovery requirements and design alternatives, and it identifies the technologies to analyze, host and protect your data, along with a business case and implementation timeline.

Conclusion

Industry initiatives such as Sheltered Harbor, have been utilizing PowerProtect Cyber Recovery to protect customers, financial institutions, and public confidence in the U.S. financial system in the event of a cyberattack that causes critical systems to fail – including backups. With thousands of customers, Cyber Recovery with CyberSense gives confidence to business leaders and has proved to accelerate the recovery of data in the event of a cyber threat. Based on Forrester Consulting research, in the event of a cyberattack, PowerProtect Cyber Recovery helps to reduce downtime by 75% and helps in the reduction of hours spent on recovery by 80%.[3]

PowerProtect Cyber Recovery can give you confidence that you can quickly identify and restore known good data and resume normal business operations after a cyberattack. It's time to get back to business.

[1] Based on research by Vanson Bourne commissioned by Dell Technologies, "Global Data Protection Index 2024 Snapshot". October 2023.
[2] Based on an ESG report commissioned by Index Engines, "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption". June 2024
[3] Research by Forrester Consulting commission be Dell Technologies, "The Total Economic Impact of Dell PowerProtect Cyber Recovery," August 2023



Learn more about Dell PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

View more resources

Join the conversation with #PowerProtect

DELL Technologies