

# Dell PowerProtect Cyber Recovery

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

## WHY CYBER RECOVERY?

Cyberattacks are designed to destroy, steal or otherwise 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. Could your business survive? Here are five components of a proven and modern cyber recovery solution:

### 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.

### Data Isolation and Governance

An isolated data center environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance.

### Intelligent Analytics and Tools

Machine learning and full-content indexing with powerful analytics within the safety of the vault. Automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.

**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 internet economy and a critical asset that must be protected, kept confidential and made available at a moment's notice. Today's global marketplace relies on the constant flow of data across interconnected networks, and digital transformation efforts put more sensitive data at risk.

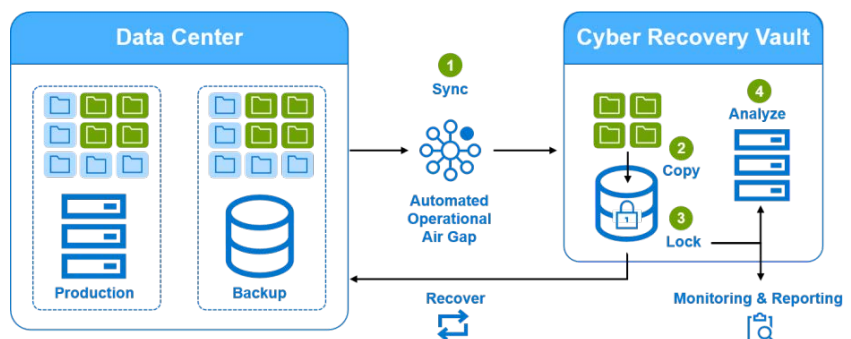
This makes your organization's data an attractive and lucrative target for cyber criminals. Cybercrime has been called the greatest transfer of wealth in history, and it's all about the data. In fact, Cybersecurity Ventures estimates that \$6 trillion is the estimated global impact of cybercrime in 2021<sup>1</sup>.

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. According to Accenture Insights, \$13 million is the average cost to organizations resulting from cybercrime<sup>2</sup>.

Having a cyber recovery 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 67% of IT decision makers are not very confident that all business-critical data can be recovered in the event of a destructive cyberattack<sup>3</sup>.

So, what can you do to protect your organization and its valuable data?

## The Solution: PowerProtect Cyber Recovery



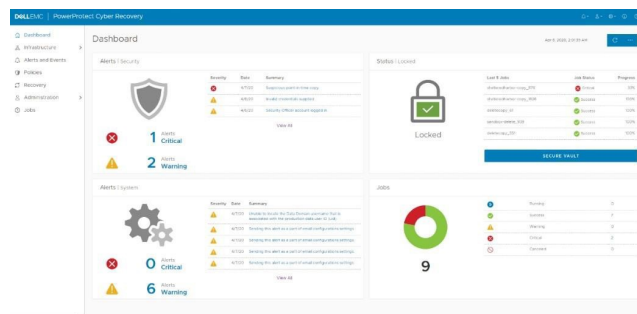
To reduce business risk caused by cyberattacks and to create a more cyber resilient approach to data protection, you can modernize and automate your recovery and business continuity strategies and leverage the latest intelligent tools to detect and defend against cyber threats.

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

## PowerProtect Cyber Recovery – proven, modern and intelligent protection to reduce business risks from cyber threats

### Cyber Recovery vault

The PowerProtect Cyber Recovery vault offers multiple layers of protection to provide resilience against cyberattacks even from an insider threat. It moves critical data away from the attack surface, physically isolating it within a protected part of the data center and requires separate security credentials and multi-factor authentication for access. Additional safeguards include an automated operational air gap to provide network isolation and eliminate management interfaces which could be compromised. PowerProtect Cyber Recovery automates the synchronization of data between production systems including open systems and mainframes, and the vault creating immutable copies with locked retention policies. If a cyberattack occurs you can quickly identify a clean copy of data, recover your critical systems and get your business back up and running.



### CyberSense

PowerProtect Cyber Recovery is the first solution to fully integrate CyberSense which adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. This innovative approach provides full content indexing and uses machine learning (ML) to analyze over 100 content-based statistics and detect signs of corruption due to ransomware. CyberSense finds corruption with up to 99.5% confidence, helping you identify threats and diagnose attack vectors while protecting your business-critical content – all within the security of the vault.

### 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 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 ready 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. Dell and its ecosystem partners provide a comprehensive methodology for protecting data, as well as performing damage assessments and forensics to provide an organization with the confident and most reliable path to recovery of business-critical systems.

### Solution Planning and Design

Optional Dell Advisory Services 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.

Protecting your vital data from cyberattacks requires proven and modern solutions. 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.

<sup>1</sup>Cybersecurity Ventures: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021>

<sup>2</sup>Accenture Insights, Ninth Annual Cost of Cybercrime Study March, 2019 - <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

<sup>3</sup>Based on research by Vanson Bourne commissioned by Dell Technologies, "Global Data Protection Index 2021 Snapshot," carried out February – March, 2021. Results were derived from a total of 1,000 IT decision makers worldwide from both private and public organizations with 250+ employees.



Learn more about Dell  
PowerProtect Cyber  
Recovery



Contact a Dell  
Technologies Expert



View more resources



Join the  
conversation with  
#PowerProtect