Executive summary

Improve cyber resiliency and protect data from cyber ransomware threats by using an isolated vault, AI-based ML analytics software, and more

With Dell Technologies PowerProtect Cyber Recovery with CyberSense

As the frequency of cyber threats continuously grows and attack methods evolve, data protection plans must take an approach that secures and analyzes all IT components, from the most superficial to the deepest reaches. Dell PowerProtect Cyber Recovery can help protect the most critical and sensitive data while also helping ensure proper recovery in the face of a cyberattack or another disruptive event.

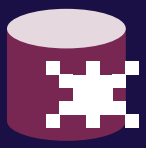
Dell PowerProtect Cyber Recovery is a data management, protection, and recovery solution that helps organizations protect their data and applications against ransomware, destructive cyberattacks, and unexpected events. The solution uses a multi-copy approach, meaning that after creating backups, it copies those backups to isolated storage for safeguarding and analysis. PowerProtect Cyber Recovery comprises many components, including one or more storage vaults, located either potentially on-premises in a PowerProtect DD (formerly known as Data Domain) appliance or in the cloud via software-defined Dell APEX Protection Storage for Public Cloud (formerly known as DD Virtual Edition). In both cases, the vault is operationally air-gapped, i.e., isolated from the production environment--potentially physically air-gapped in the case of the on-premises environment, and logically air-gapped in the case of the APEX environment. This makes it extremely difficult for bad actors or unauthorized users to log in and compromise backup copies.

PowerProtect Cyber Recovery also includes CyberSense, a fully automated and integrated intelligent security analytics engine that automatically scans data, files, databases, and images in the vault for signs of corruption from a ransomware attack. CyberSense provides full content analysis; takes observations from files to use as inputs for its artificial intelligence (AI)-based machine learning (ML) model; and detects malicious activity that includes mass deletions, encryption, and other suspicious changes in core infrastructure (including Active Directory and DNS), user files, and critical production databases that might indicate ransomware or a destructive attack. When CyberSense detects patterns of corruption, it generates an alert in the PowerProtect Cyber Recovery dashboard that gives additional information on the scale and impact of the attack.[1]

PowerProtect Cyber Recovery helps organizations mitigate cyberattacks, enhance data resilience with multiple copies of data backups from separate locations, reduce downtime, and maintain business continuity. This report uses publicly available data to highlight key data protection features and functionality and presents our findings from a competitive analysis of CyberSense.

Protect sensitive data

Encrypt immutable data in flight during backup replication to physically and logically isolated vaults



Detect SQL Server page corruption

CyberSense found an infection where a competing solution could not

Identify uncorrupted backup copies

CyberSense identified the most recent uninfected backup copy for recovery

Security

Dell PowerProtect Cyber Recovery offers several security features to help protect critical data from ransomware and other sophisticated threats, prevent unauthorized users from gaining access to sensitive information, and make recovery swift so organizations can resume normal operations.

The features and functionality of PowerProtect DD appliances can be critical to the security, integrity, and recovery that PowerProtect Cyber Recovery solutions deliver. These features include Retention Lock, DDBoost, Role-based access control (RBAC), dual authorization, and more.

Isolation

Data isolation refers to the separation of and restricted access to data created by barriers or boundaries to prevent unauthorized access. Isolation often uses temporary network connections instead of persistent connections.

Data isolation helps critical data remain unconnected from an infected network where a bad actor could try to modify configurations, delete data, change policies, or sniff network traffic for user credentials. Isolation also helps reduce the attack surface, giving bad actors fewer opportunities to gain access and control. Additionally, organizations can restrict access to only authorized personnel, which helps prevent unauthorized users from overwriting data.

In addition to features we noted, PowerProtect Cyber Recovery can provide physical and logical isolation, in the form of air gaps, to help protect data. A physically isolated on-premises PowerProtect DD could function as the vault, in which users or systems from the production environment cannot access the components, and the vault is physically disconnected from the production network.[2] By eliminating access to the recovery environment from the production network, an organization could reduce its surface of attack.

Immutability*

Making backups immutable, and thus read only, helps ensure that an organization can trust those backups for recovery. Operationally, immutability helps maintain data authenticity and reliability. DD systems, including those in PowerProtect Cyber Recovery solutions, can provide immutability in how they store data using logical partitions of the filesystem called MTrees. The solutions also use MTree replication to copy immutable data copies from a production DD to another DD in the vault via the DDBoost protocol.[3]

*Dell's products are designed to support customers' efforts to secure their critical data. As with any electronic product, data protection, storage and other infrastructure products can experience security vulnerabilities. It is important that customers install security updates as soon as they are made available by Dell.

CyberSense

Protecting your data well requires a comprehensive strategy that provides security at every level. Despite all the self-healing, security, immutability, and isolation features of a Dell PowerProtect Cyber Recovery solution, less obvious attacks could still dive deeper into an enterprise infrastructure, such as at the data backup level, potentially going undetected until production data or an entire user group became compromised. Dell PowerProtect Cyber Recovery solutions provide a last line of defense against cyberattacks and an efficient approach to help expedite recovery via CyberSense.

We tested CyberSense and a similarly functioning tool from the data management platform of a competitor (that we refer to as "Vendor X") for a similarly sized appliance. In our testing, we found that PowerProtect Cyber Recovery detected infection in SQL database pages—something that the Vendor X solution could not do. PowerProtect Cyber Recovery also required fewer backups than the Vendor X solution to determine corruption in the data.

1. Dell, "CyberSense® for PowerProtect Cyber Recovery," accessed September 8, 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cyber-sense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, "MTree replication," accessed September 11, 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack," accessed August 21, 2023, http://facts.pt/rkew01n.

Read the report at https://facts.pt/64FU3b2 ▶

Principled Technologies®

Facts matter.®