DELL Technologies

Solution Brief

Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect

Multi-Cloud Enabled Cyber Recovery Service

Trusted and Secure

- Physically and logically isolated vault environment, disconnected from corporate networks via operational air gap
- Immutable data copies in a secure off-premise vault maintaining data integrity
- Intelligent analytics provide M/L and full-content indexing within the vault

Cost-Effective

- Core vault infrastructure delivered as a service
- Available high-bandwidth, low-latency direct connection to public cloud providers
- $0 egress fees from Microsoft Azure and Oracle Cloud

Convenience without Compromise

- Protect critical data that resides either in the cloud or on-premises
- Restore data to any public cloud provider seamlessly
- Gain the flexibility and convenience of the cloud without compromising on security

Cyber Protection for On-Premises and Cloud Deployments

Every minute of every day, ransomware and other sophisticated cyber attacks threaten to steal or compromise a businesses' most critical asset – their data. This can lead to lost revenue, reputational damage and costly regulatory fines. Protecting your critical data and recovering it with validated data integrity is key to resuming normal business operations post-attack.

Hybrid and multi-cloud environments offer operational flexibility, the ability to scale up quickly, and access to innovative services and hardware. However, the approach of scattering and duplicating data across multiple clouds can lead to new 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 today's constantly evolving cyber threats. A better way is needed to make your data simultaneously accessible to public cloud providers without compromising security, retain your freedom to choose any cloud provider and avoid vendor lock-in.

As you move more workloads and data to the cloud, it's imperative to invest in a cyber protection solution for critical data, wherever your data lies. Dell Technologies delivers a secure data vault and intelligent analytics that safeguards your critical data from cyber attacks, ransomware and insider threats.

Multi-Cloud Enabled Cyber Recovery

Setting up a Cyber Recovery vault with Multi-Cloud Data Services for Dell EMC PowerProtect, powered by Faction, is simple. This secure data vaulting service is a logically air-gapped vault built upon secure, multi-cloud-enabled infrastructure that safeguards your critical data from cyber attacks. 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.

CyberSense intelligent analytics are fully integrated with this Cyber Recovery service and takes a unique approach in uncovering cyber attacks, observing how data changes over time and using analytics to detect signs of corruption due to ransomware. This provides an additional layer of assurance by validating the integrity of the data protected within the off-premises within the Cyber Recovery vault.

Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect Secure Architecture

The secure vault environment includes a Multi-Cloud Data Services for Dell EMC PowerProtect system to serve as the replication target for your primary Dell EMC PowerProtect DD or Dell EMC PowerProtect DD Virtual Edition (DDVE) systems. Dedicated compute resources run the Cyber Recovery Management tools and any CyberSense analytics tools. Combined with the physical security and isolation of the vault, this solution includes an operational air gap – this air gap enables access to the vault only long enough to replicate data from the primary system and even then, access is severely limited. At all other times, the vault is disconnected from the client's production environment. Immutable copies of user-selected data are created in the Cyber Recovery vault hosted in a Faction data center. Once a copy of the selected data is safely within the secure, isolated vault, the

data cannot be altered, deleted or otherwise changed for a prescribed duration. CyberSense analytics, with its machine learning and full-content indexing capabilities, can analyze each data set within the security of the vault.

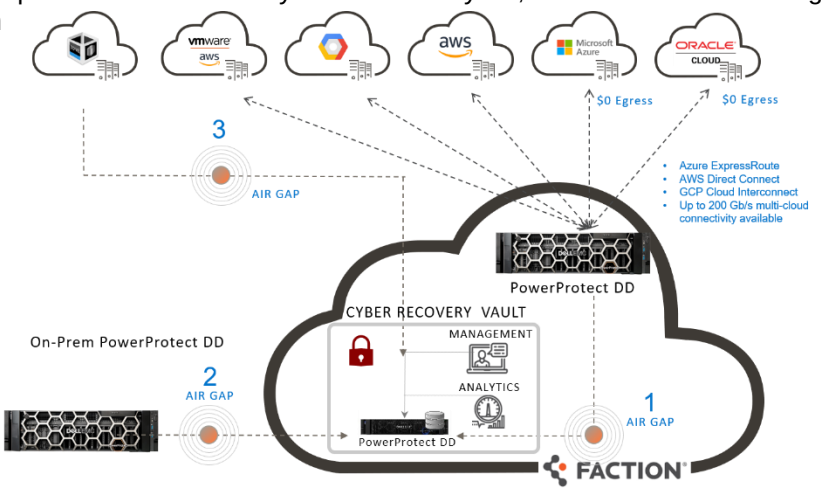

Figure 1 - Multi-Cloud Data Services for Dell EMC PowerProtect Use Cases

1. Protection for Existing Multi-Cloud Data Services for Dell EMC PowerProtect deployments

2. Protection of data on customer premises

3. Protection of data in the public cloud

Protection for Existing Multi-Cloud Data Services for Dell EMC PowerProtect Deployments

When combined with Multi-Cloud Data Services for Dell EMC PowerProtect, clients achieve sovereign data protection across all clouds (AWS, Google Cloud, Oracle, and Azure) and are then able to protect their critical data within a secure Cyber Recovery vault. Multi-Cloud Data Services for Dell EMC PowerProtect can be used as a multi-purpose system: a backup target for cloud-native application data or a replication target for existing PowerProtect systems. The Cyber Recovery vault is an additional option that can easily be added to provide isolation of critical data from cyber attacks and validation of data integrity.

Protection of Data on Customer Premises

Customers can replicate data from an on-premises PowerProtect DD to a Cyber Recovery vault in one of Faction's data centers. This gives organizations the best possible chance for recovery when their production or primary backups have been compromised or their DR location has been breached or infected. If a cyber attack occurs, they can quickly identify the most current clean copy of data within the remote Cyber Recovery vault and recover their critical systems back on-premises or choose to recover into the cloud if their service has been architected with this recovery motion.

Protection of Data in the Public Cloud

For cloud-native applications already using PowerProtect DDVE (a virtual backup target in the cloud supported in AWS, Google Cloud, and Azure), the Cyber Recovery vault service is an optional service that enables customers to replicate critical data to a secure vault.

Dell EMC PowerProtect Cyber Recovery with 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 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.

Dell Technologies Data Protection Solutions – Leading Your Way to the Cloud

You can protect critical data in the cloud without compromising integrity, confidentiality or availability. Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect protects your critical data regardless of whether it is hosted in the cloud or on-premises from a single destination with confidence. For more information, start here.

Learn More about Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect	Contact a Dell Technologies Expert	Learn more about Cloud Data Protection and Backup Solutions	