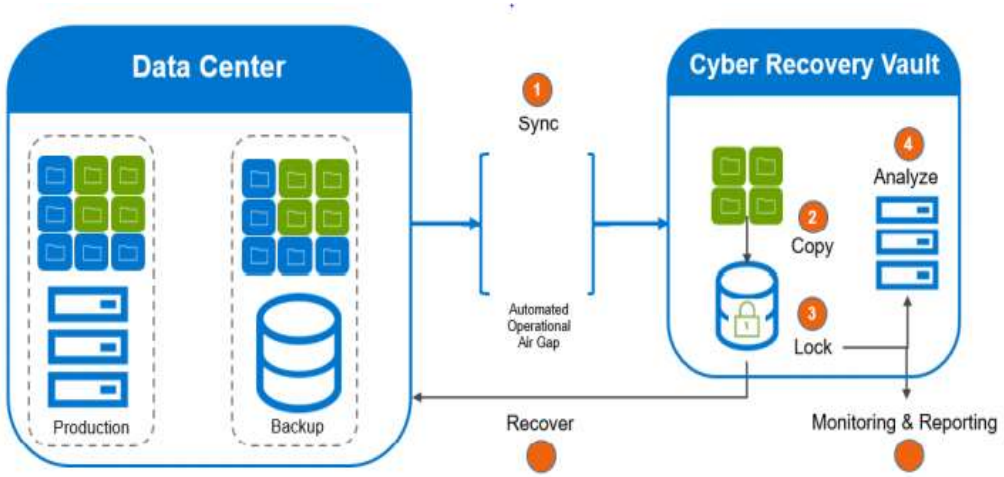
PowerProtect® Cyber Recovery® Analysis

Futurewei Intelligent Data Lab

5/21/2021

Introduction

On-Premises



Proven and Modern Protection for Critical Data from Ransomware and Destructive Cyber Attacks

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 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.

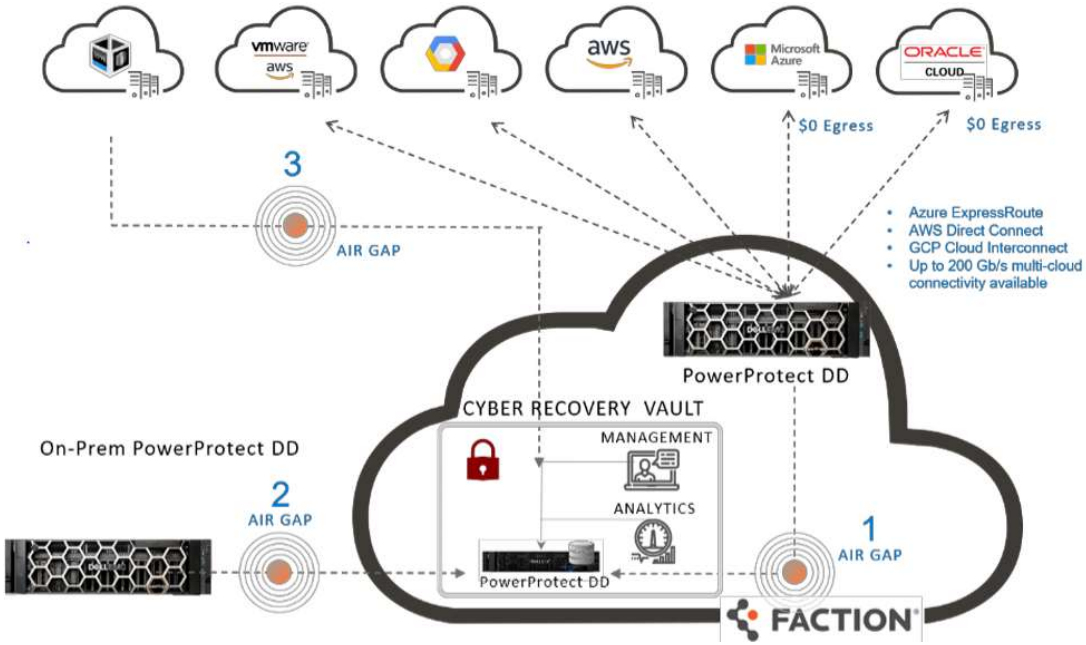
© *isolated-recovery-solution-overview.pdf (delltechnologies.com)*

FUTUREWEI Technologies

Key Components

- Source (production) and destination (vault) DD system
- Cyber Recovery® Management Host & Cyber Recovery® Software:
  - Orchestrates sync
  - Manages/locks data copies
  - Orchestrates recovery
  - Governs process of analytics
  - Transmit alerts through SMTP to production environment
- Recovery host - in-vault recovery
- Analytics/indexing host – run data-analysis software
- SMTP server (production) – receive alerts

Multi-Cloud Solutions



Multi-Could Data Services

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

© *Cyber Data Recovery Software & Solutions | Dell Technologies US*

FUTUREWEI Technologies

Analysis

Planning

- Determine the Cyber Recovery® metrics and goals to regulate recovery
- Assess mission-critical data to be saved in vaults
- Data synchronization frequency and data retention time
- Select backup/replication technologies
- Workflows and tools to perform recovery after an incident
- Data analytics techniques

Isolation (Vault)

- Physical Isolation
  - Secure location (dedicated room, cage, etc) with physical access control, video surveillance
  - Secure access to Cyber Recovery® management server
  - Management and analytical hosts inside vault
- Network
  - Vault has its own switching infrastructure
  - Air-gapped replication link between vault and production environment: only enabled when the replication is going on
  - Optional dedicated link from CR management host to SMTP server for events-reporting
- Network Security
  - FW for replication link, allowing only desired traffic
  - One-way VPN tunnel for event link
  - Zero-Trust network with Unisys Stealth (network segmentation)
- Software Security
  - separate security credentials (RBAC)
  - multifactor authentication for access

Replication

- DD MTree replication (DD Boost MTree and DD vdisk MTree)
  - Incremental replication
  - At least 3 MTrees in vault:
    - One as the replication destination
    - One or more for Retention Locked copies
    - One or more for read/write sandboxes
- Cyber Recovery® software manages the synchronization
- Encrypted traffic in and out of vault
- Replication link is disconnected most of the times. It is connected only during data synchronization operation
- Backup workflow with NetWorker®, Avamar® and PowerProtect® Data Manager
- Immutable restore points are automatically created for recovery and analytics
- WORM for immutable copies

Retention Lock

- DD Retention Lock software provides immutable file locking and secure data retention capabilities
- Compliance with SEC 17a-4(f) and other regulations
- Lock on a per-MTree basis
- Retention time on a per-file basis
- Can apply different retention periods for different types of data stored on MTree.

© EMC Data Domain Retention Lock Software - A Detailed Review (datastorageasean.com)

FUTUREWEI Technologies

Data Analytics (CyberSense®)

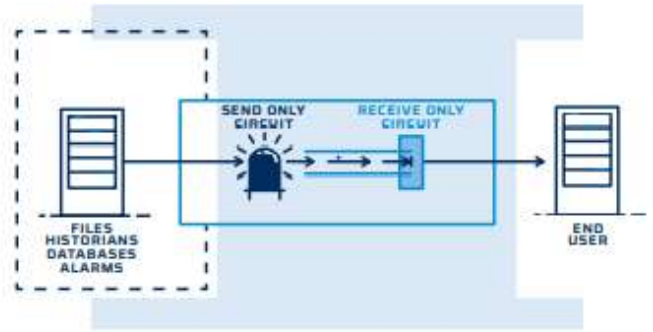
- In vault (isolated and controlled environment)
- System-level analytics:
  - Ensure data synchronization and immutable copies are created successfully
  - Identify health issues of the vault
- Anomaly detection
  - Detect unusual patterns and trigger alarms
- Application-level analysis
  - Verify the integrity of the application, database stack
- Malware detection
  - Signature-based technologies
  - Behavioral analysis

Recovery

- Identify the restore points created before the attack
- Perform damage assessment
- Remediate and remove malware
- Restore the data to a recovery host
- Test-run production applications
- Recover the data back to production site
- Automate the recovery procedure for NetWorker® and PowerProtect® Data Manager applications

Events Report

- One-way SMTP connectivity from the Cyber Recovery® management host to the SMTP server
- VPN tunnel for security
- One-way Data Diode device – OWL data Diodes



© owlcyberdefense-use-case_financial-services-data-vault.pdf

FUTUREWEI Technologies

References

- Dell EMC PowerProtect Cyber Recovery Soluton Guide (delltechnologies.com)
- isolated-recovery-solution-overview.pdf (delltechnologies.com)
- Cyber Data Recovery Software & Solutions | Dell Technologies US
- EMC Data Domain Retention Lock Software - A Detailed Review (datastorageasean.com)
- CyberSense for Dell EMC (indexengines.com)
- owlcyberdefense-use-case_financial-services-data-vault.pdf

Thank You.