Building Resiliency

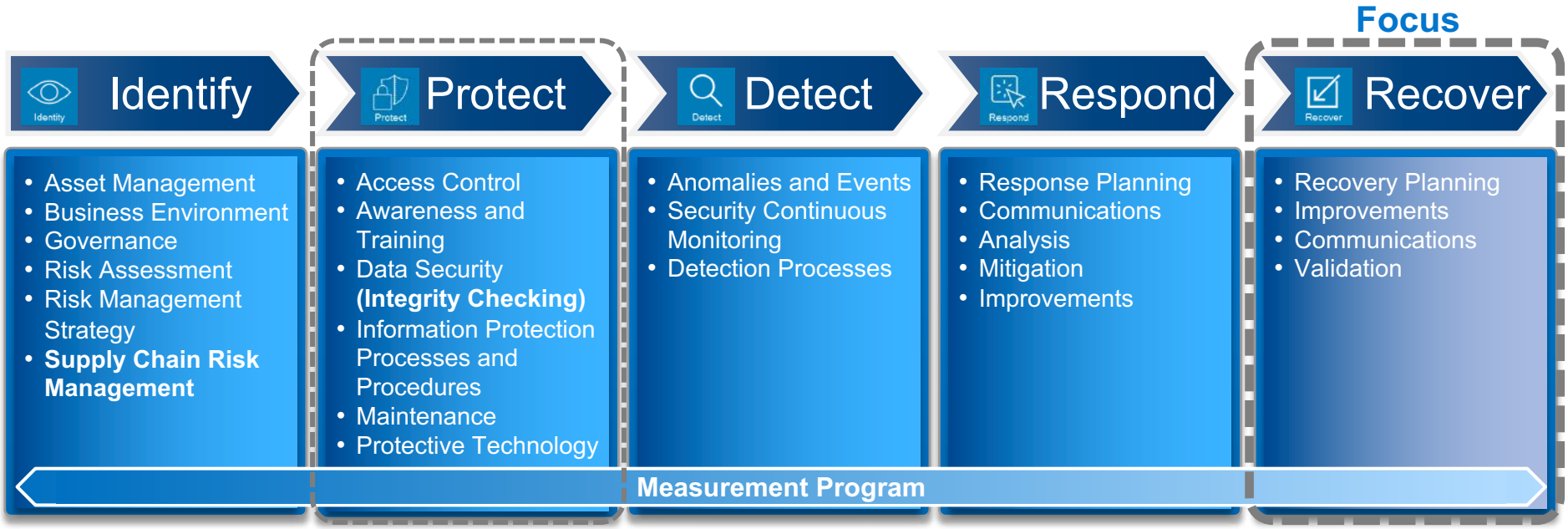
Cyber Recovery Solution

Emiliano Campagnoli

DPS Systems Engineer

DELL Technologies

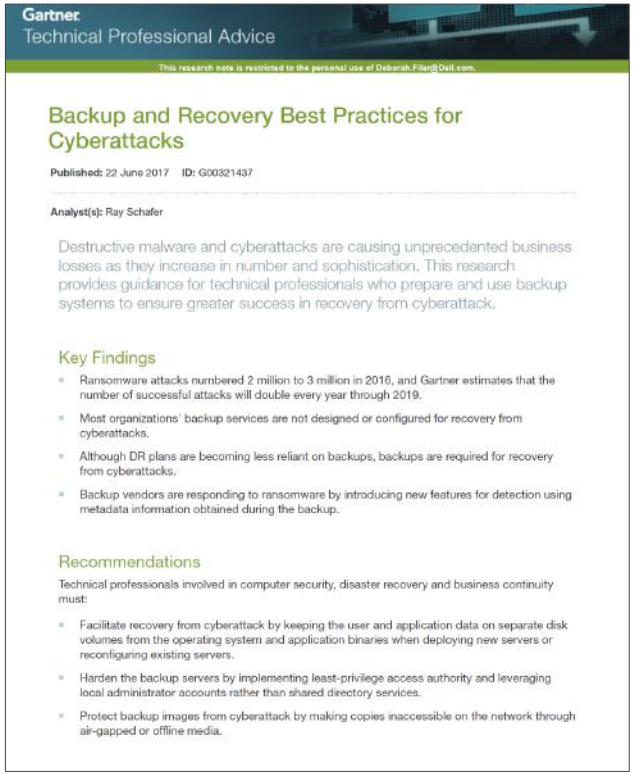
NIST Cybersecurity Framework



Secureworks	Secureworks	Secureworks	Secureworks	DELL EMC
Cybersecurity Maturity Assessment & Compliance Program Management	**Managed Firewall, IDS, IPS**	**Security Monitoring & Management**	**Monitoring, Incident Response, Forensics Analysis & Investigation**	**Cyber Recovery Solutions**

Dell Technologies Aligned Services

Gartner Best Practices for Cyberattacks



Gartner
Technical Professional Advice

Backup and Recovery Best Practices for Cyberattacks

Published: 22 June 2017 **ID:** G00321437

Analyst(s): Ray Schafer

Destructive malware and cyberattacks are causing unprecedented business losses as they increase in number and sophistication. This research provides guidance for technical professionals who prepare and use backup systems to ensure greater success in recovery from cyberattack.

Key Findings

- Ransomware attacks numbered 2 million to 3 million in 2016, and Gartner estimates that the number of successful attacks will double every year through 2019.
- Most organizations' backup services are not designed or configured for recovery from cyberattacks.
- Although DR plans are becoming less reliant on backups, backups are required for recovery from cyberattacks.
- Backup vendors are responding to ransomware by introducing new features for detection using metadata information obtained during the backup.

Recommendations

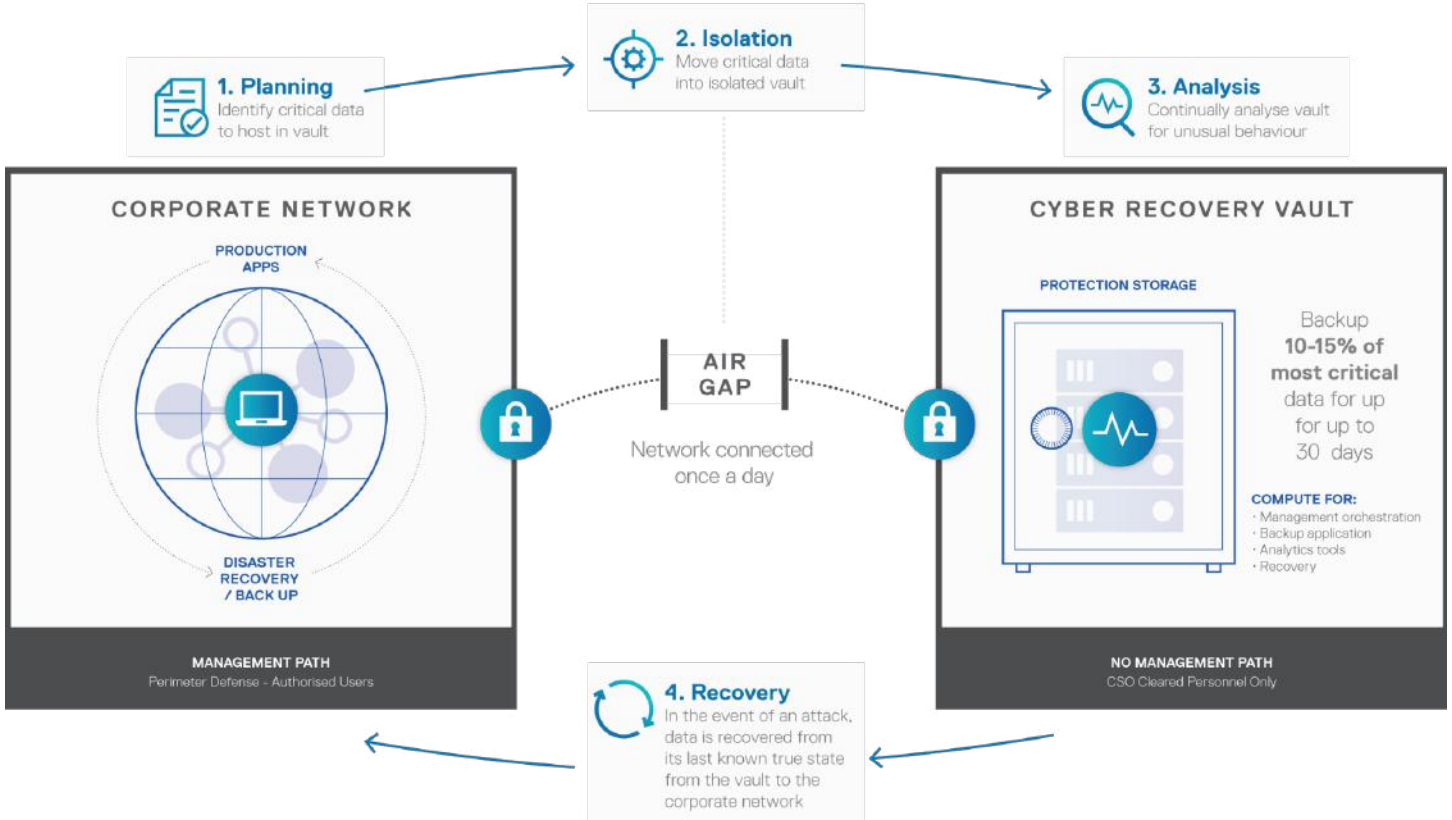
Technical professionals involved in computer security, disaster recovery and business continuity must:

- Facilitate recovery from cyberattack by keeping the user and application data on separate disk volumes from the operating system and application binaries when deploying new servers or reconfiguring existing servers.
- Harden the backup servers by implementing least-privilege access authority and leveraging local administrator accounts rather than shared directory services.
- Protect backup images from cyberattack by making copies inaccessible on the network through air-gapped or offline media.

- Ransomware attacks number 2-3 million in 2016 and Gartner estimates that the number will **double every year** through 2020
- Most organizations' backup services are not designed or configured for recovery from cyber attacks
- **Backups** are required for recovery from cyber-attacks but are increasingly **targeted by attackers**
- **Protect backup images** from cyberattack by copies **inaccessible to the network**

Cyber Recovery Solution in a nutshell

The Last Line of Defense Against Cyber-Attacks



Cyber Recovery

- ✓ **Airgap Vault Solution**
- ✓ **End-to-End Automated**
- ✓ **Modern & Simple UI**
- ✓ **Flexible Rest API**
- ✓ **Fully Supported**
- ✓ **Enables Vault Analytics**

INDEX ENGINES

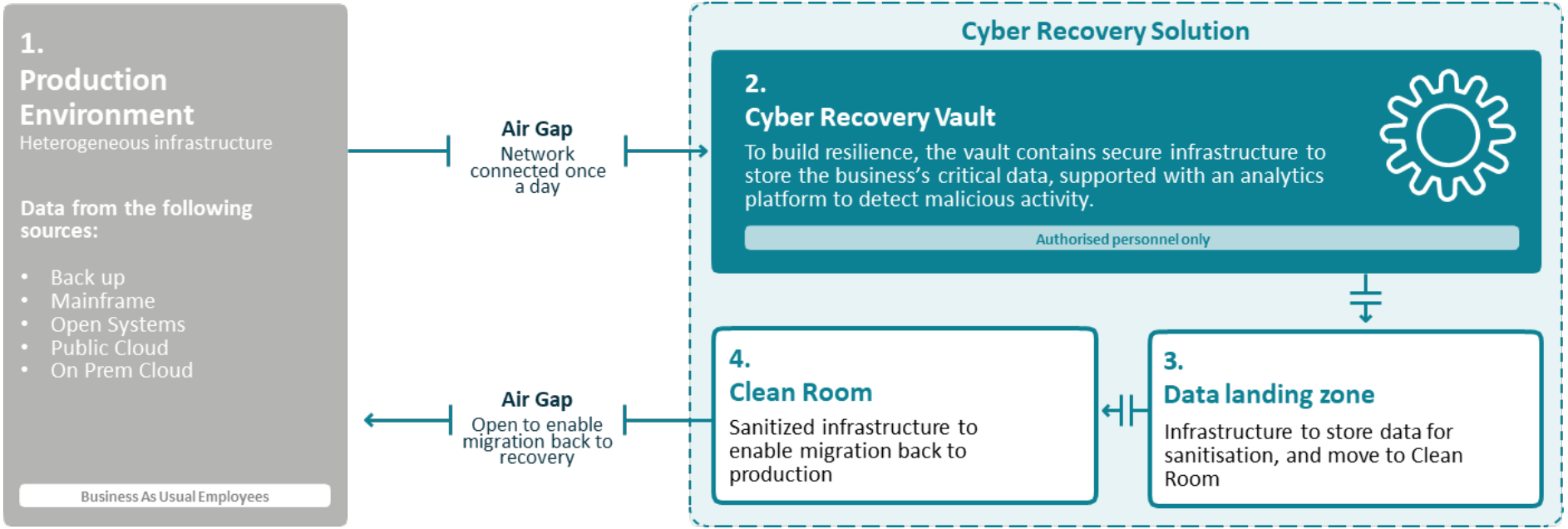
docker

HTML 5

DELL Technologies

The Components of Cyber Recovery

The following diagram outlines the major components of a resilient Cyber Recovery Solution



Cyber Recovery – PowerProtect DD

Innovation in Solutions

1 Isolation

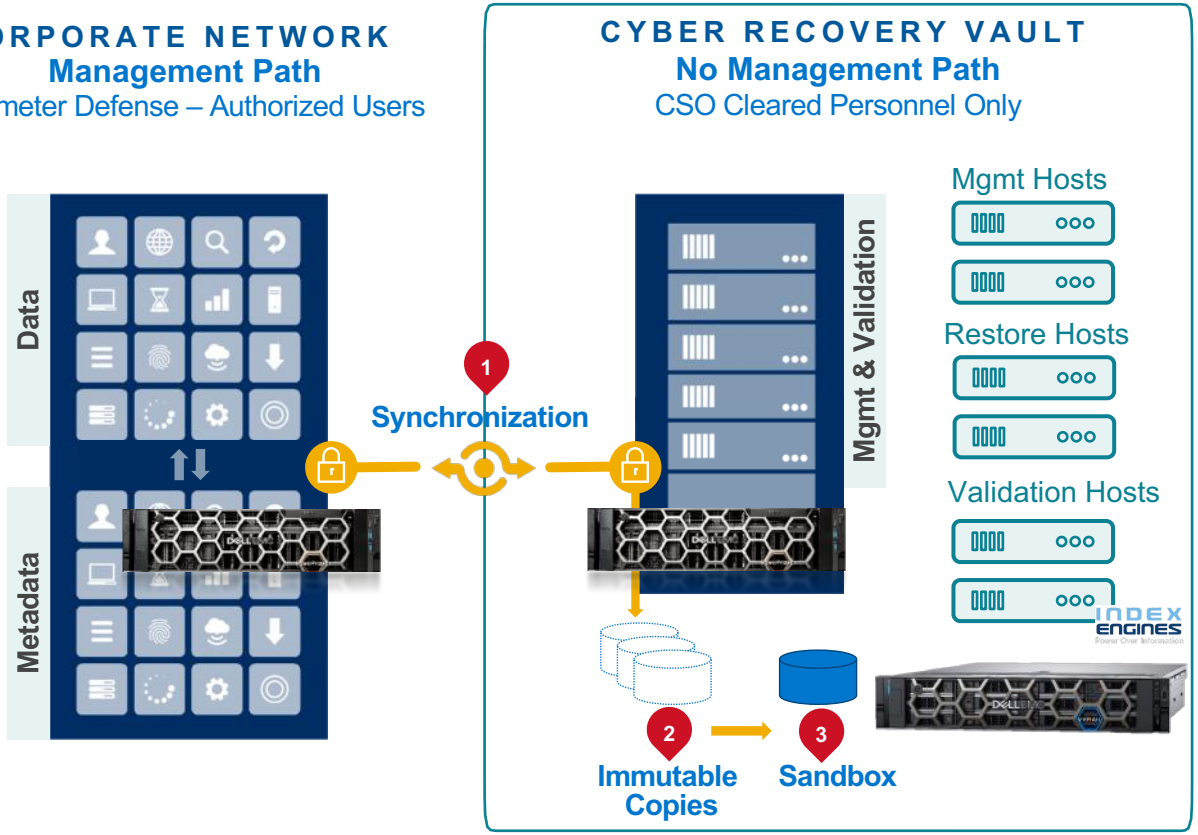
- Secure copy stored away from the surface of attack

2 Generations

- Ability to vault longer retention vs. typical DR

3 Anomaly Detection with Machine Learning

- Automated sandbox creation enabling data forensics/scrubbing

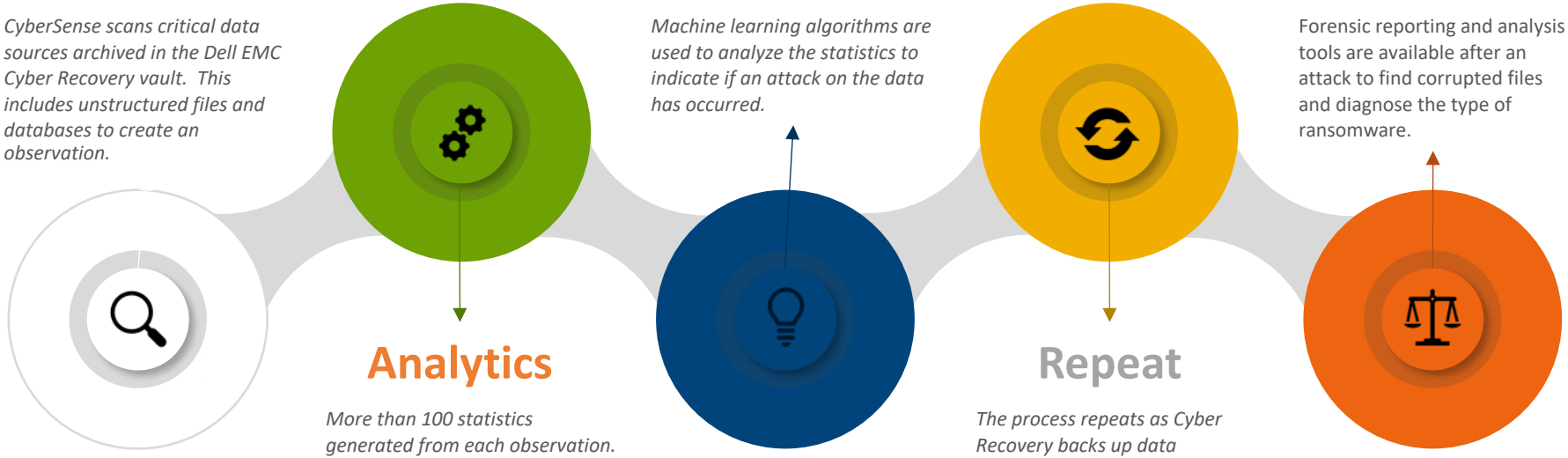


DELL Technologies

CyberSense Workflow for Cyber Recovery

Scan

CyberSense scans critical data sources archived in the Dell EMC Cyber Recovery vault. This includes unstructured files and databases to create an observation.



Analytics

More than 100 statistics generated from each observation. Statistics include analysis of file entropy, similarity, corruption, mass deletion/creations, and much more.

Analysis

Machine learning algorithms are used to analyze the statistics to indicate if an attack on the data has occurred.

Repeat

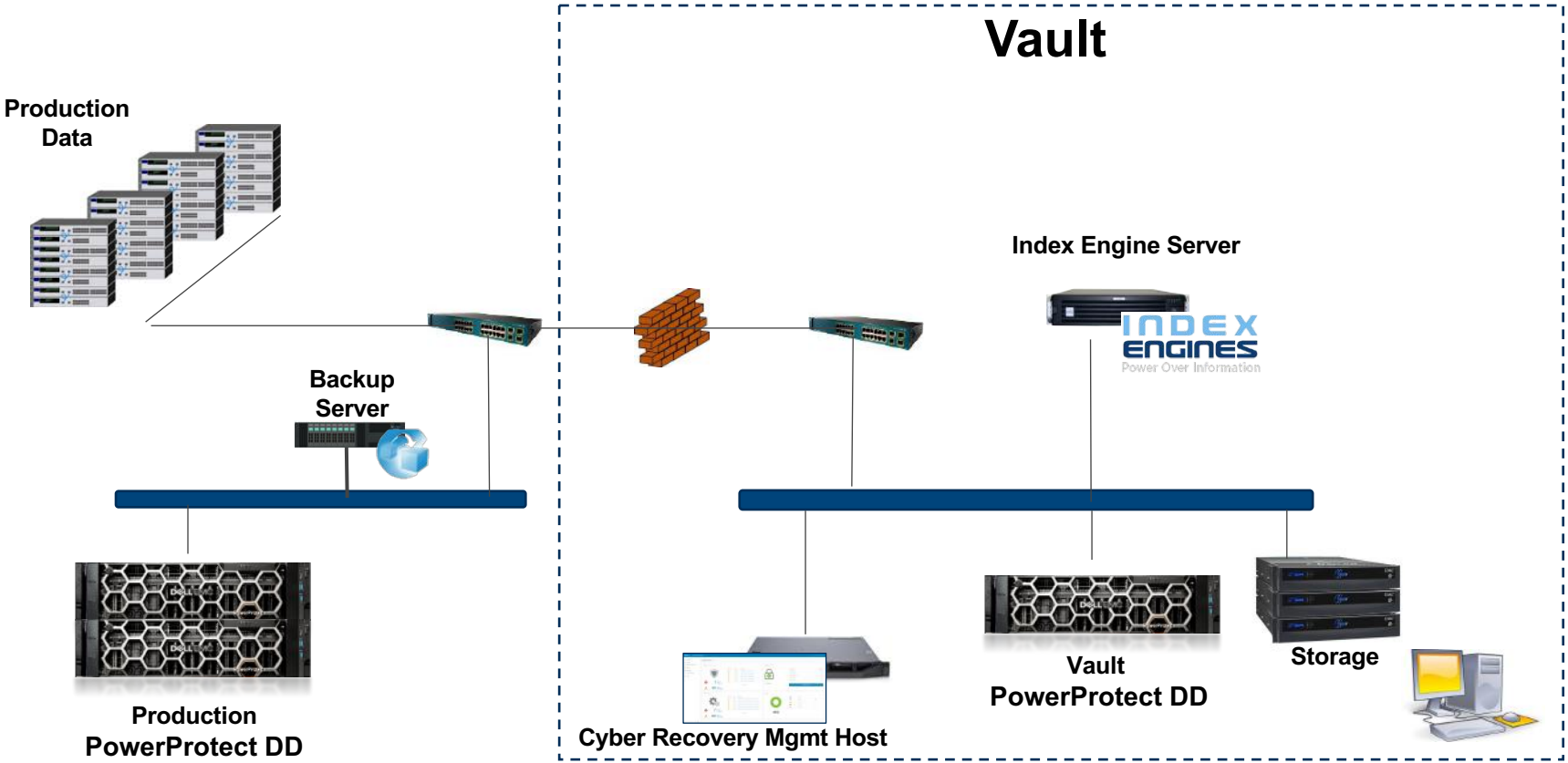
The process repeats as Cyber Recovery backs up data incrementally to the vault and a new observation is created. New observations are compared to previous observations to see how data changes.

Investigate

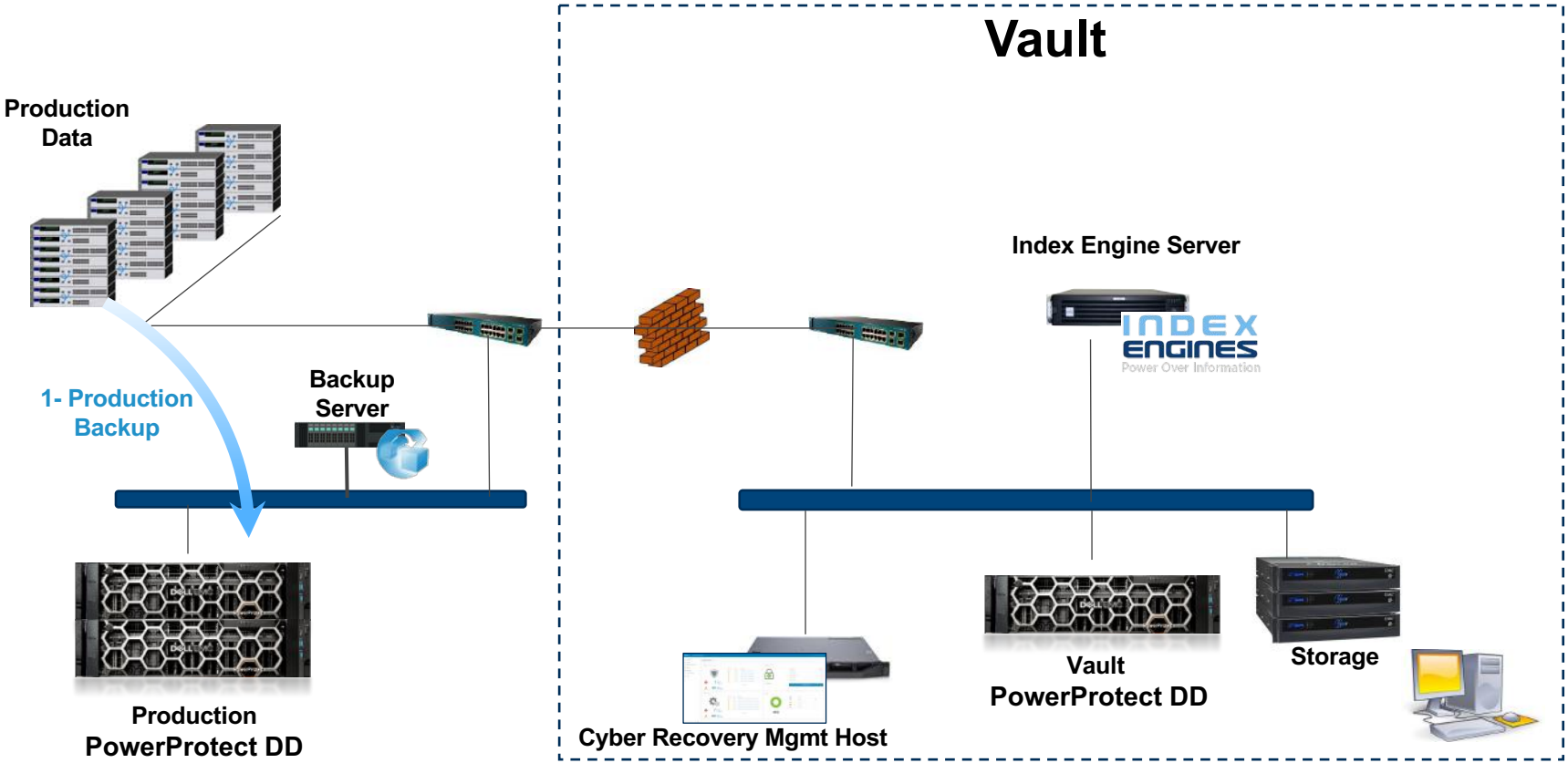
Forensic reporting and analysis tools are available after an attack to find corrupted files and diagnose the type of ransomware.

DELL Technologies

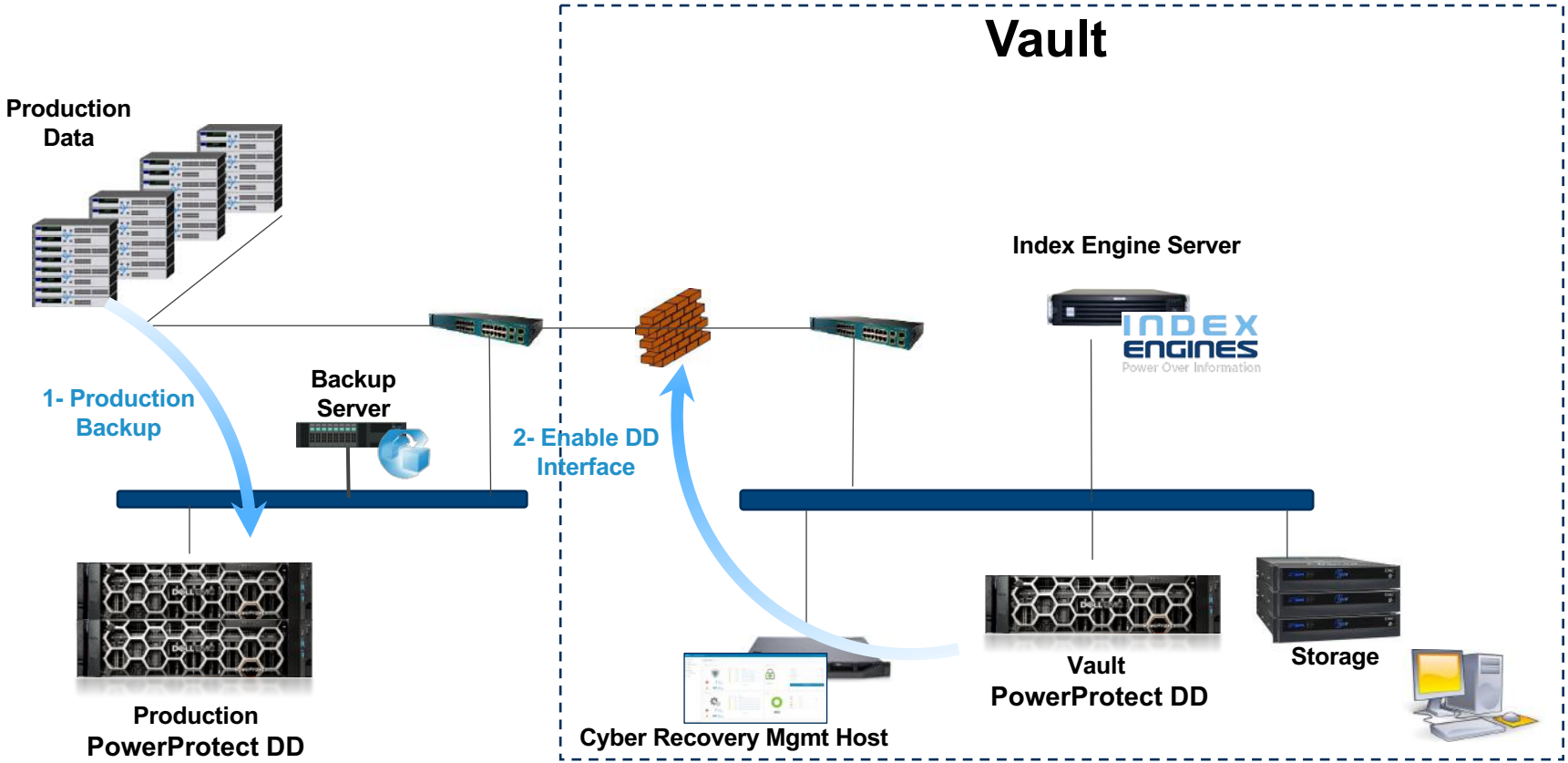
Cyber Recovery Workflow



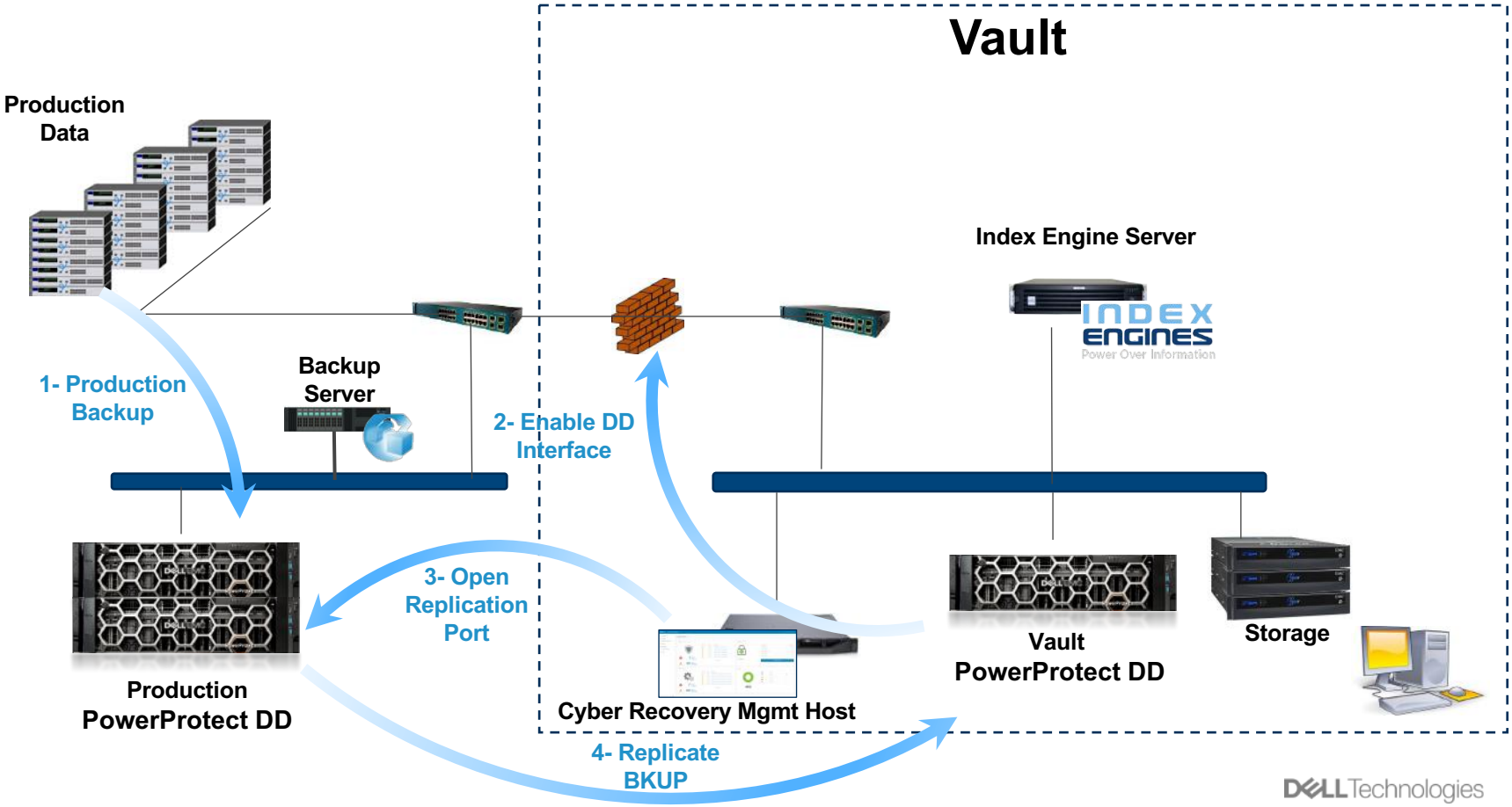
Cyber Recovery Workflow



Cyber Recovery Workflow

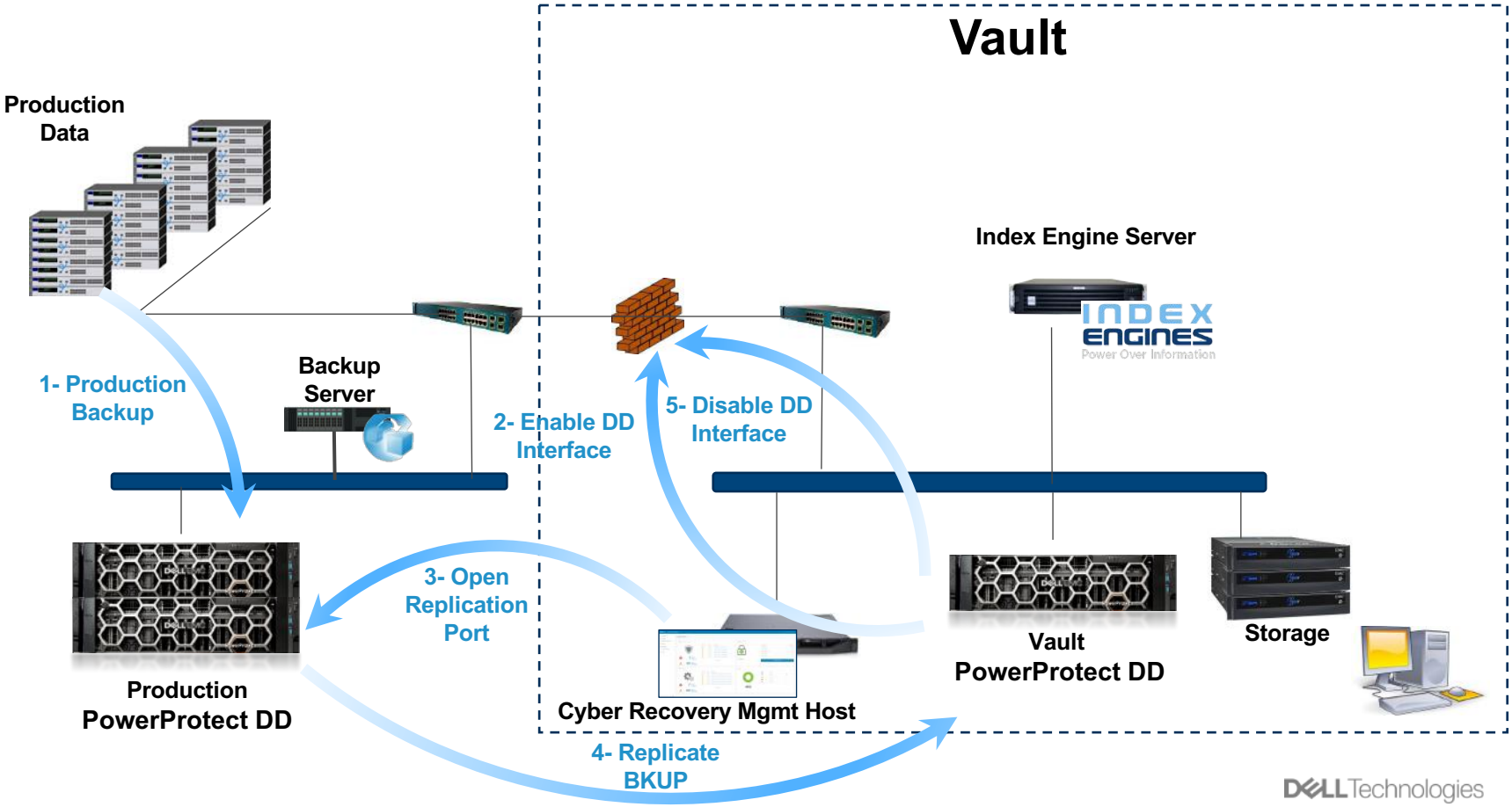


Cyber Recovery Workflow



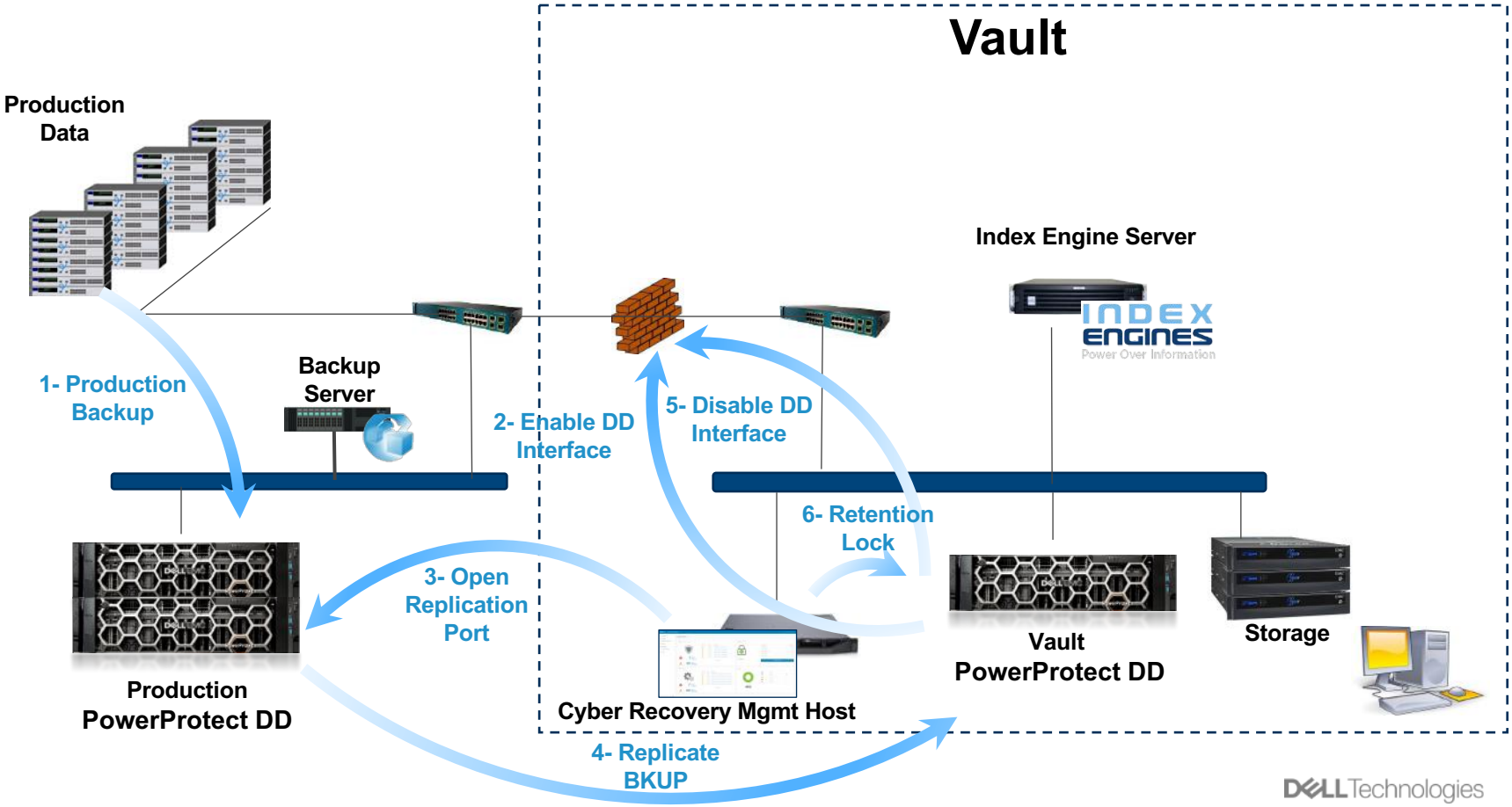
DELL Technologies

Cyber Recovery Workflow



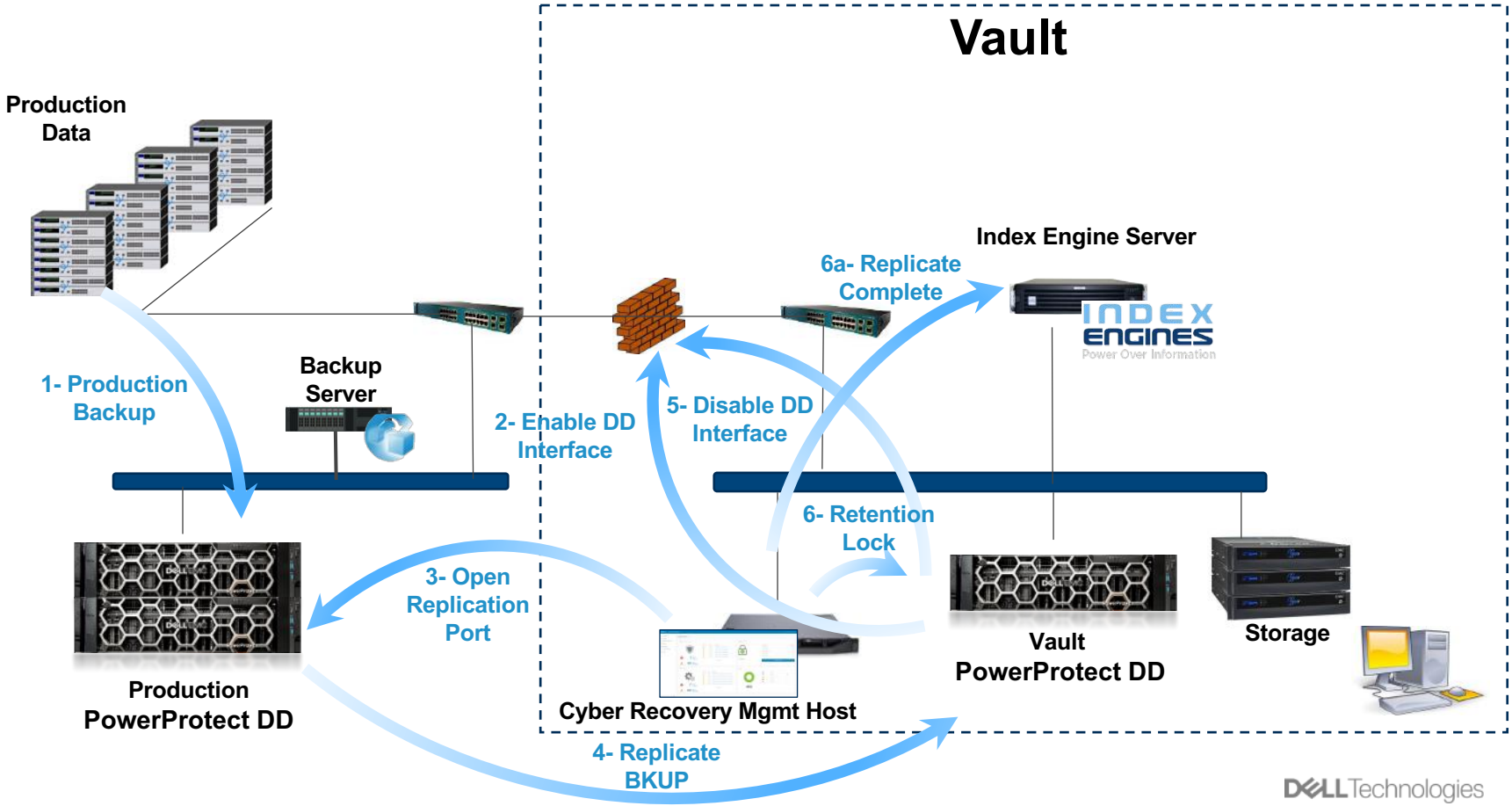
DELL Technologies

Cyber Recovery Workflow



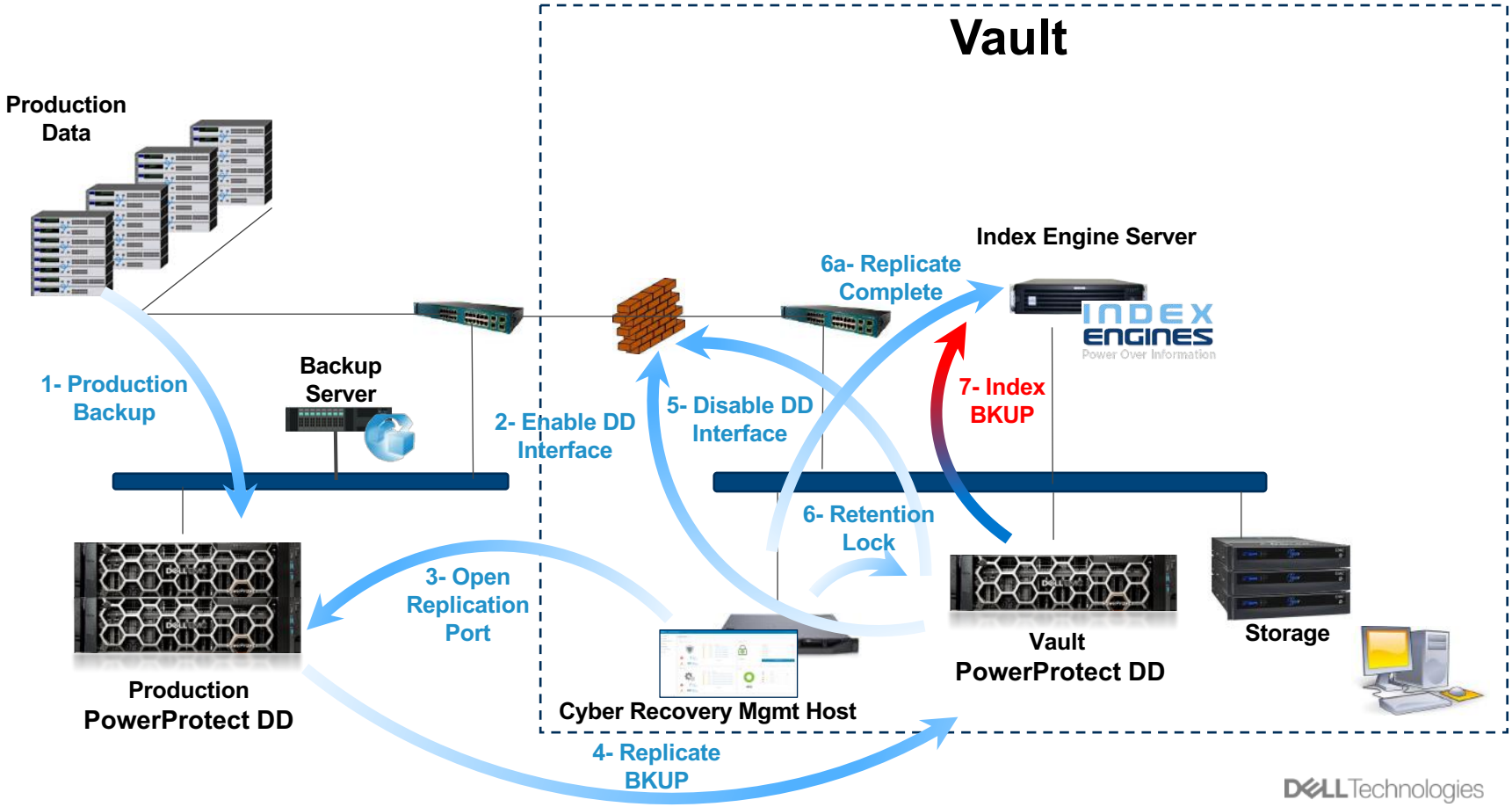
DELL Technologies

Cyber Recovery Workflow



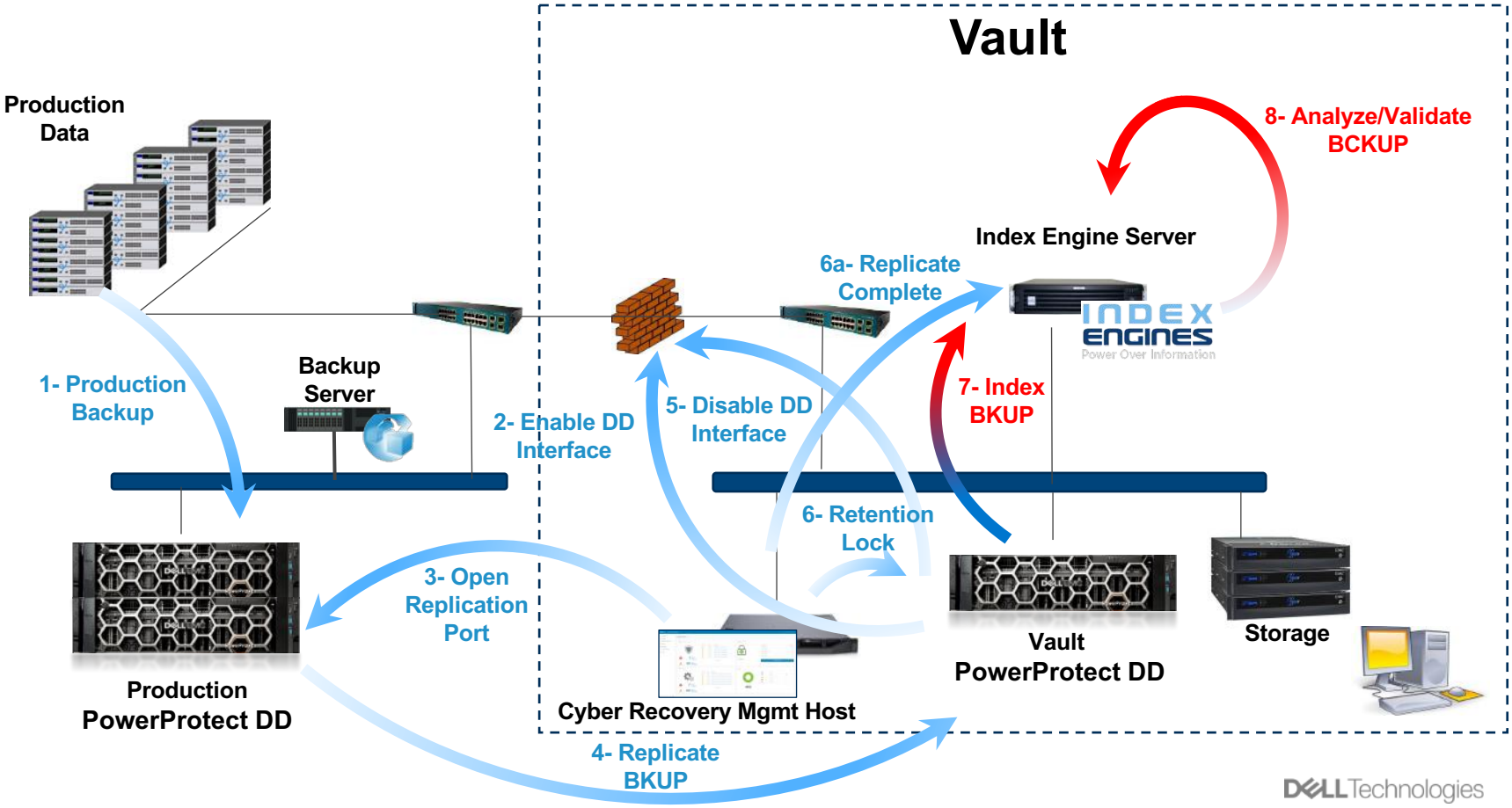
DELL Technologies

Cyber Recovery Workflow

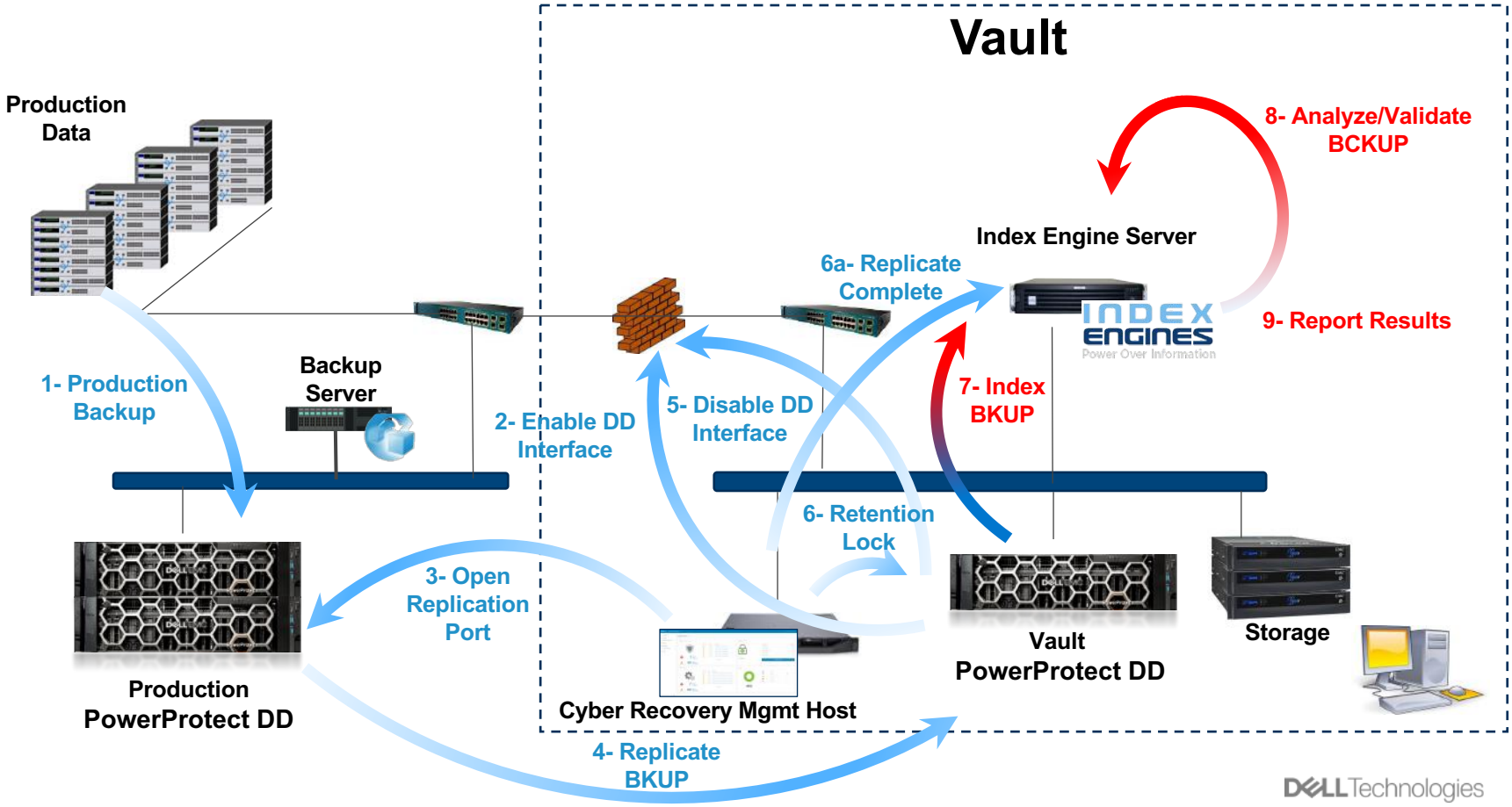


DELL Technologies

Cyber Recovery Workflow

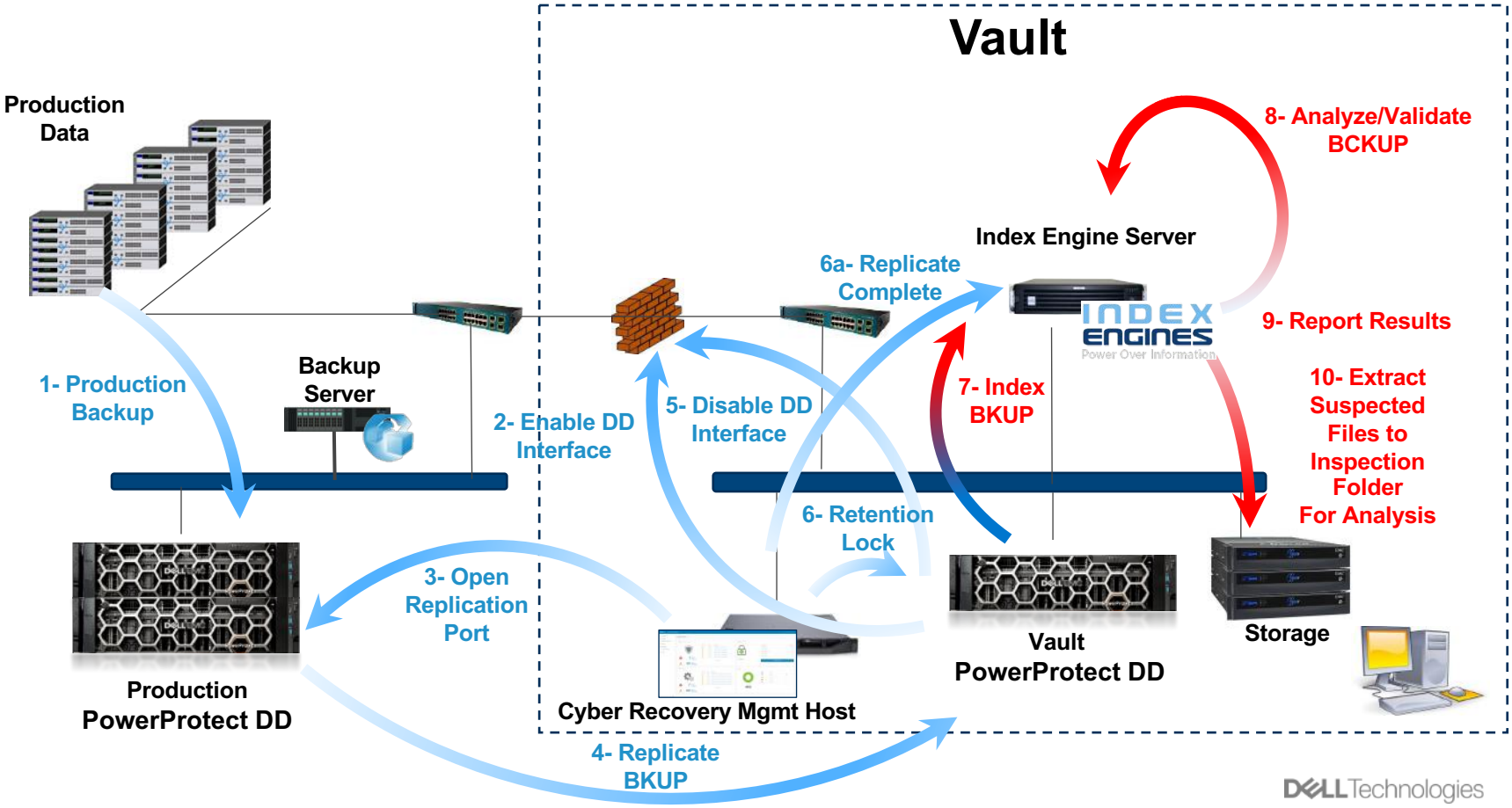


Cyber Recovery Workflow



DELL Technologies

Cyber Recovery Workflow



DELL Technologies

PowerProtect Cyber Recovery

Increase your business' cyber resiliency

- Automated creation of Isolated data vaults
- Recovery/DR for PowerProtect Data Manager
  - Restore to isolated or production recovery environment
- Index Engines CyberSense
  - Integrated reporting and management of data analytics with machine learning
- Flexible
  - REST API interface for integration with industry standard and custom security analytics tools.

Sheltered Harbor Support


DELL Technologies