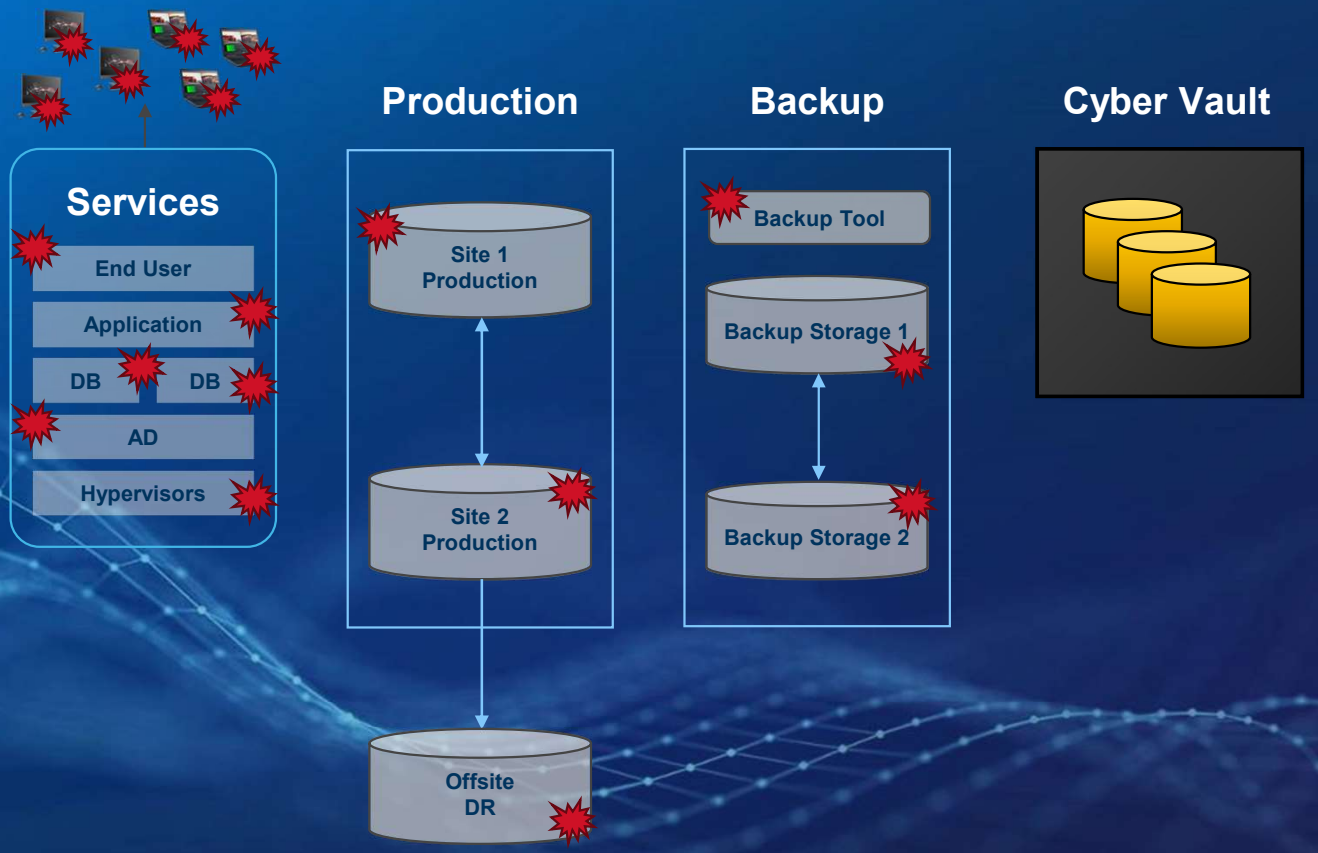
# EFEKTÍVNA OCHRANA KRITICKÝCH DÁT A ZÁLOH PRED KYBERNETICKÝMI HROZBAMI A ICH GARANTOVANÁ OBNOVA

David Průša
Data Protection and Cyber Recovery Systems Engineer CSH

DELL Technologies

# The New Data Center Reality

## Vaulting your data in an isolated environment



# Requirements from the Industry

1. Supply Chain Inspection
2. Separation of Duty
3. Data Isolation (offline)
4. Ability to Test Recoveries
5. Run Book Creation
6. Observability
7. Timely Recovery in the event of a Cyber Attack

# Key Characteristics of our Cyber Recovery Solution

## Isolation

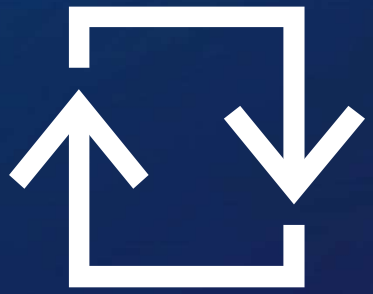
Physical & logical separation of data

## Immutability

Preserve original integrity of data

## Intelligence

Machine learning based threat detection, alerting and reporting



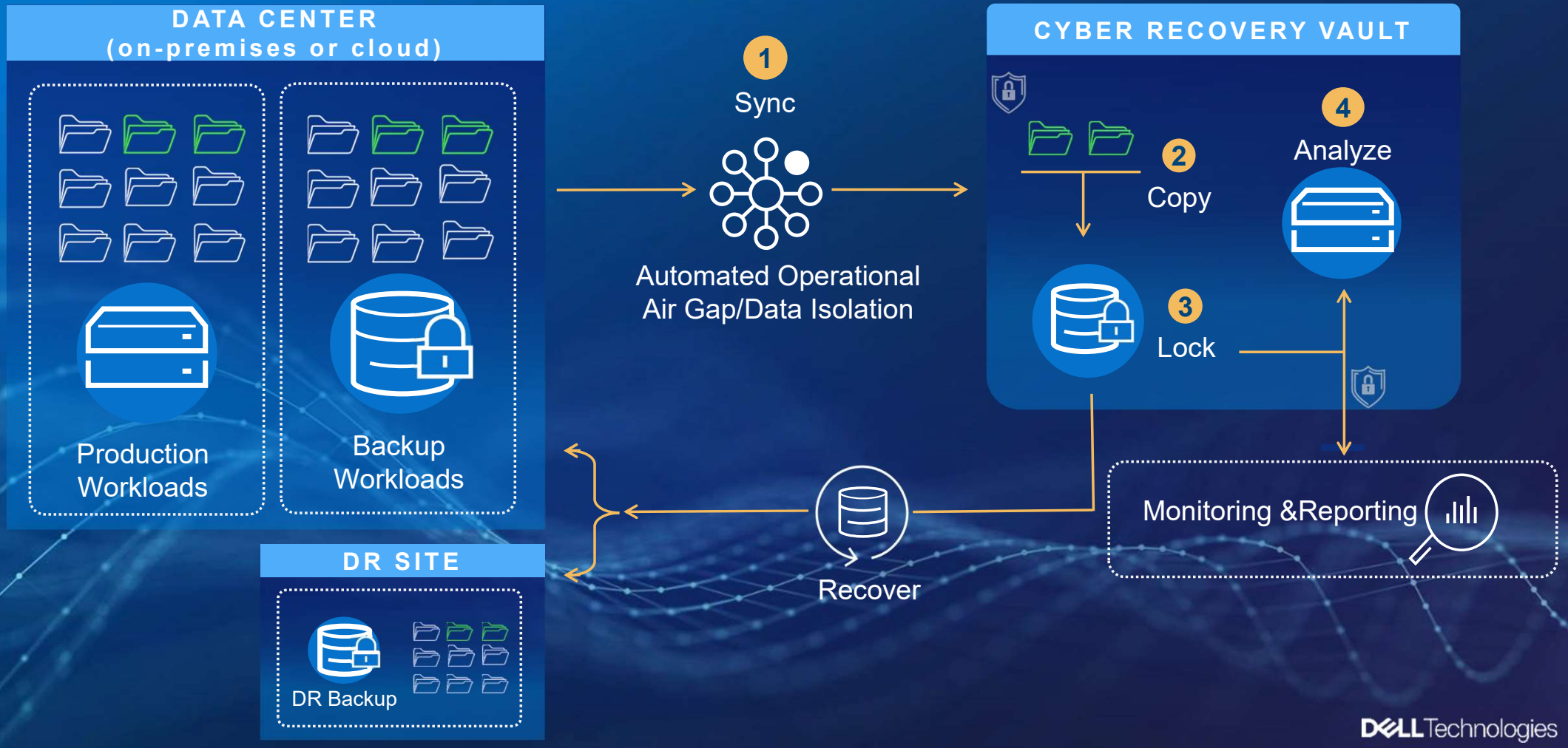
## Recovery

Fast recovery for minimal operational impact

DELL Technologies

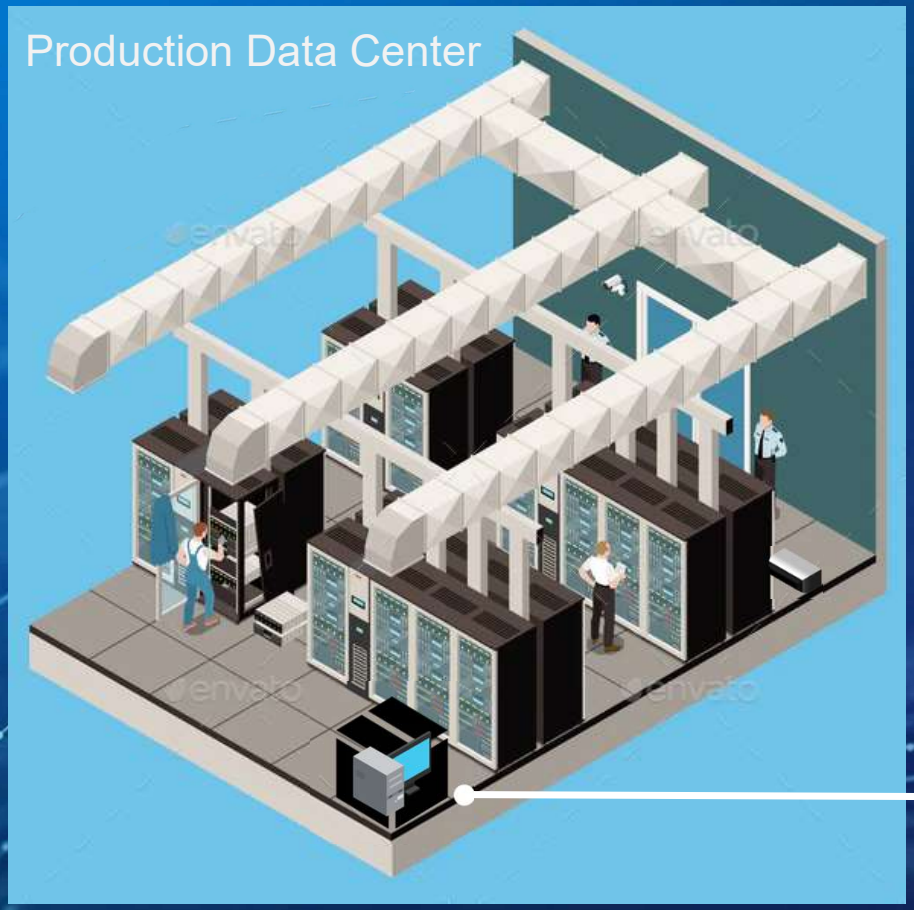
# Dell PowerProtect Cyber Recovery

## Ensuring the Recovery of Critical Rebuild Data in case of Cyber Threats



# Cyber Recovery Solution

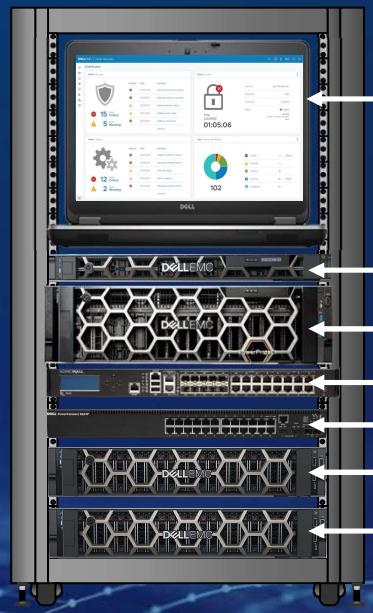
## The Gold Standard for Cyber Resiliency




Replication

Air Gap

Cyber Vault



- Cyber Recovery Application
- Cyber Recovery Server
- Data Domain
- Data Diode Switch
- Cyber Sense (opt.)
- Management Server (opt.)

DELL Technologies

# How CyberSense Works

## Analytics, Machine Learning and Forensic Tools to Detect & Recover from Cyber Attacks

**SECURITY ANALYTICS**
200+ statistics indicative of cyber attack

**CORRUPTION DETECTED**
Alert when suspicious activity is detected

**COMPREHENSIVE INDEX**
Changes in content over time

**MACHINE LEARNING**
Trained on thousands of trojans and attack vectors

**POST ATTACK FORENSICS**
Detailed reports, including last good backups for rapid recovery

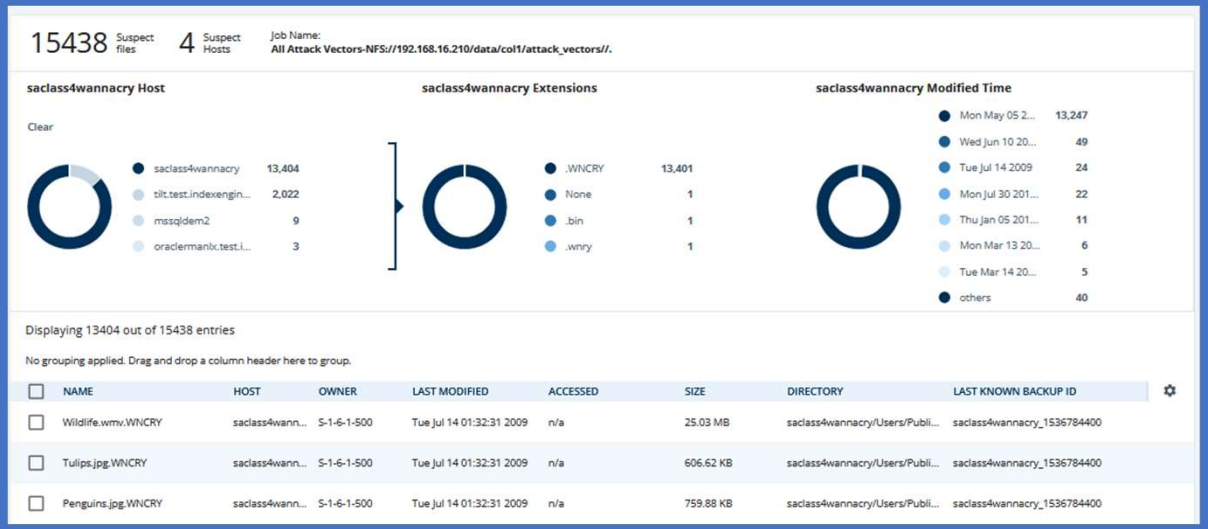
### CyberSense Provides

- Attack type notification
- Ransomware detection
- Corrupted file details
- Data changes / deletions
- Breached user accounts
- Breached executables
- Last good backup copy

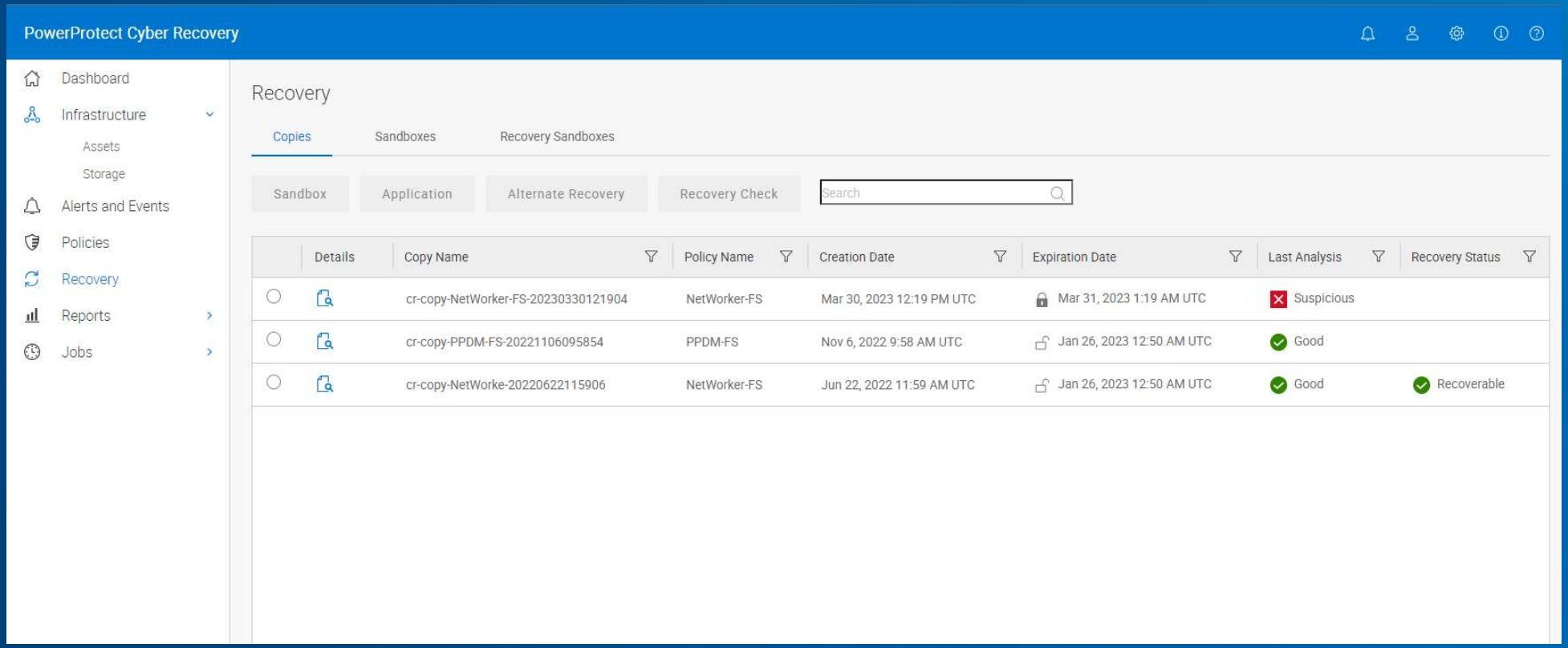
DELL Technologies

# CyberSense Support for Intelligent Recovery

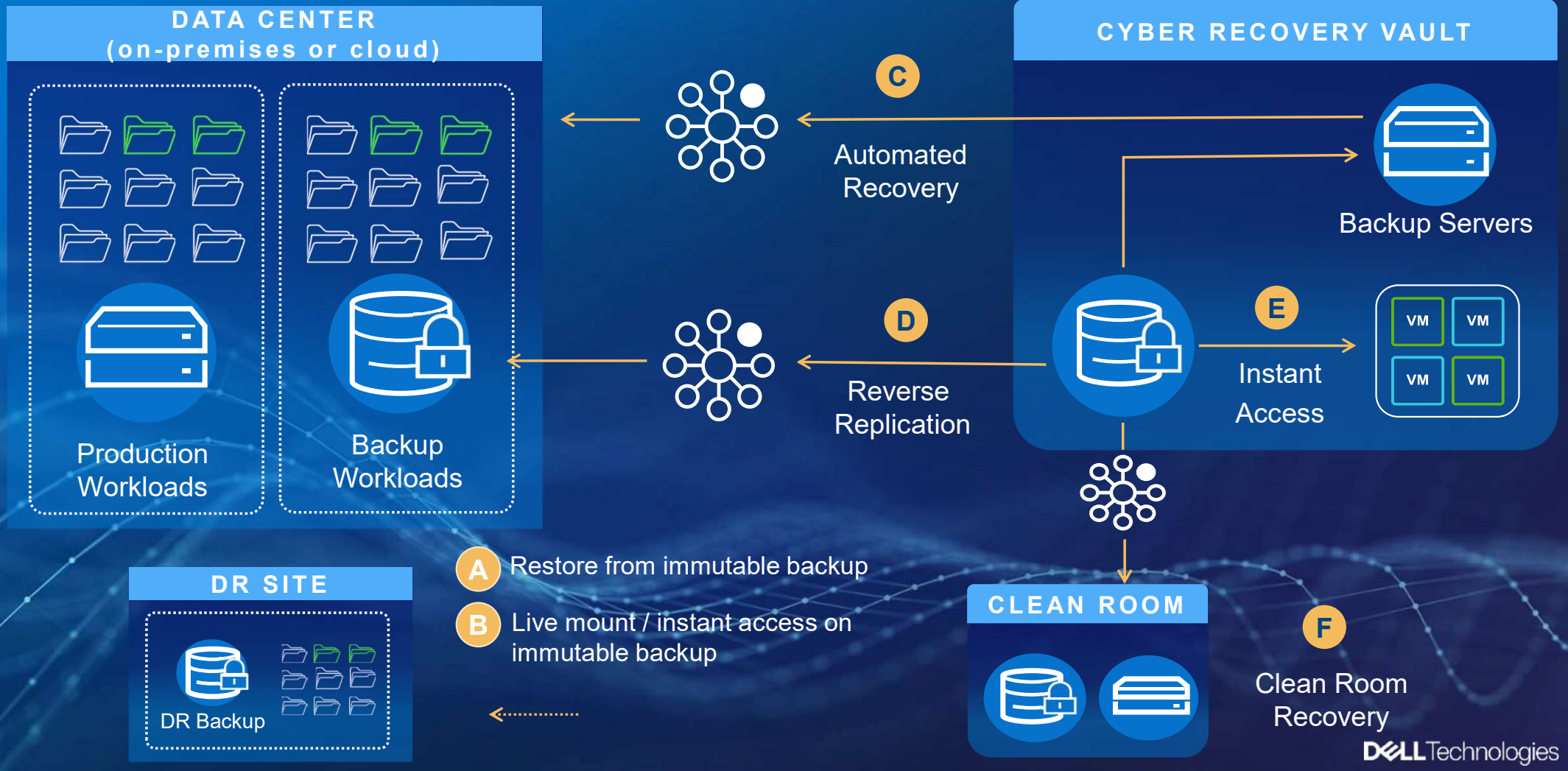
1. **Detect**
   *Detect corruption within a backup cycle*
2. **Investigate**
   *The who, what, where & when of the attack*
3. **Recover**
   *Report on last good backups quickly recover*




- Point in time of the attack
- Listing of corrupted files
- What backups need to be recovered
- Search backups to detect ransomware


PowerProtect Cyber Recovery
Dashboard
Infrastructure
Assets
Storage
Alerts and Events
Policies
Recovery
Reports
Jobs
Recovery
Copies
Sandboxes
Recovery Sandboxes
Sandbox
Application
Alternate Recovery
Recovery Check
Search
Details
Copy Name
Policy Name
Creation Date
Expiration Date
Last Analysis
Recovery Status
cr-copy-NetWorker-FS-20230330121904
NetWorker-FS
Mar 30, 2023 12:19 PM UTC
Mar 31, 2023 1:19 AM UTC
Suspicious
cr-copy-PPDM-FS-20221106095854
PPDM-FS
Nov 6, 2022 9:58 AM UTC
Jan 26, 2023 12:50 AM UTC
Good
cr-copy-NetWorke-20220622115906
NetWorker-FS
Jun 22, 2022 11:59 AM UTC
Jan 26, 2023 12:50 AM UTC
Good
Recoverable

# Recovery Options To Meet Your Cyber Resilience SLAs



# Health Service Executive (HSE): Cyber Attack

Population 5 Million



IMPACT:

- No email
- No network
- No phones
- No mobiles
- All sites are down.
- No IT services
- No health care services

Attackers provided the decryption keys
3 months to recover back primary systems
6 months to fully recover



DELL Technologies

Ďakujem Vám za pozornosť …

DELL Technologies