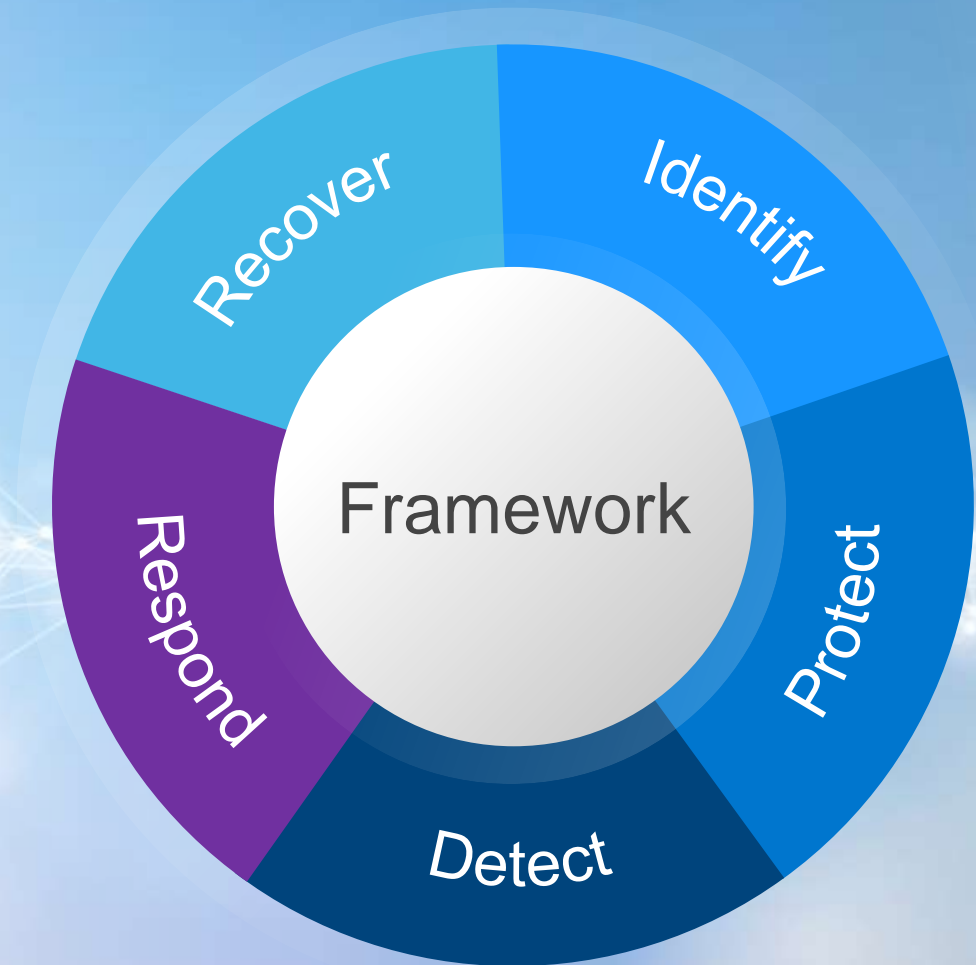# Cyber Recovery Vault

Dell Technologies – Data Protection Solutions
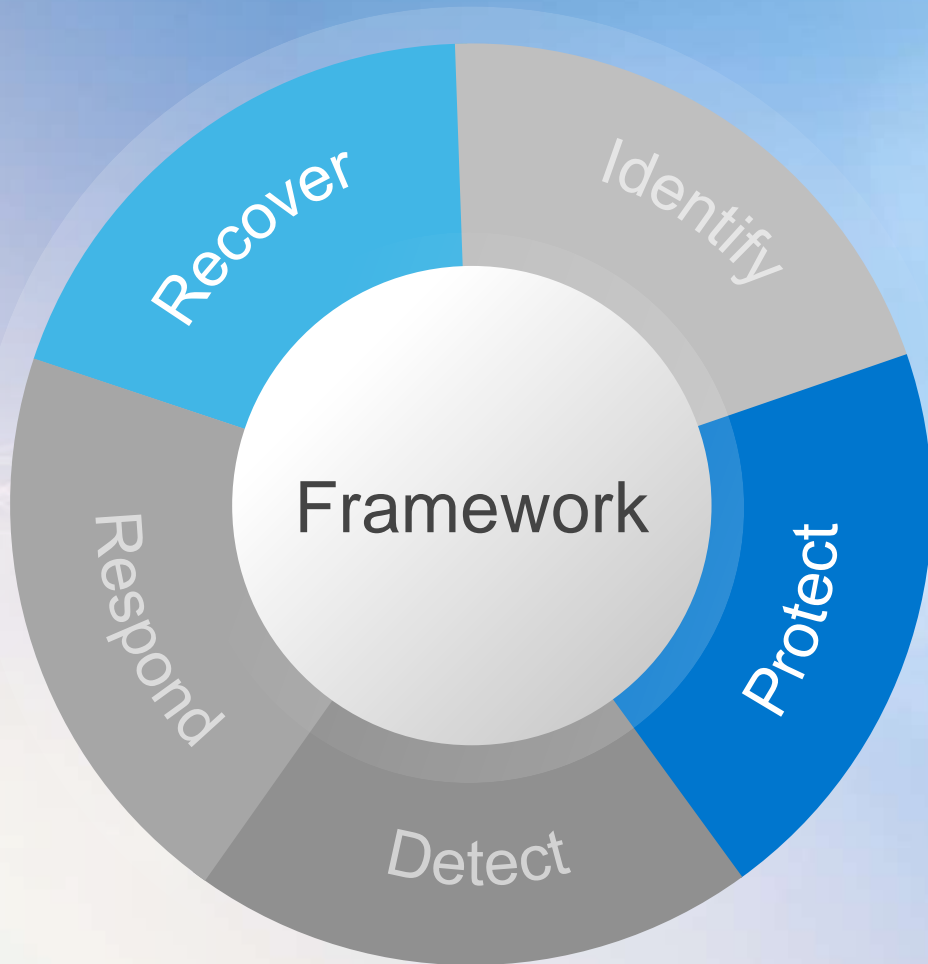David Steinbrink

Cyber resilience
is a strategy.

A high-level holistic strategy that includes
cyber security standards, guidelines,
people, business processes and
technology solutions.

Example: NIST Cybersecurity Framework

Recover

Identify

Framework

Protect

Respond

Detect

DELLTechnologies

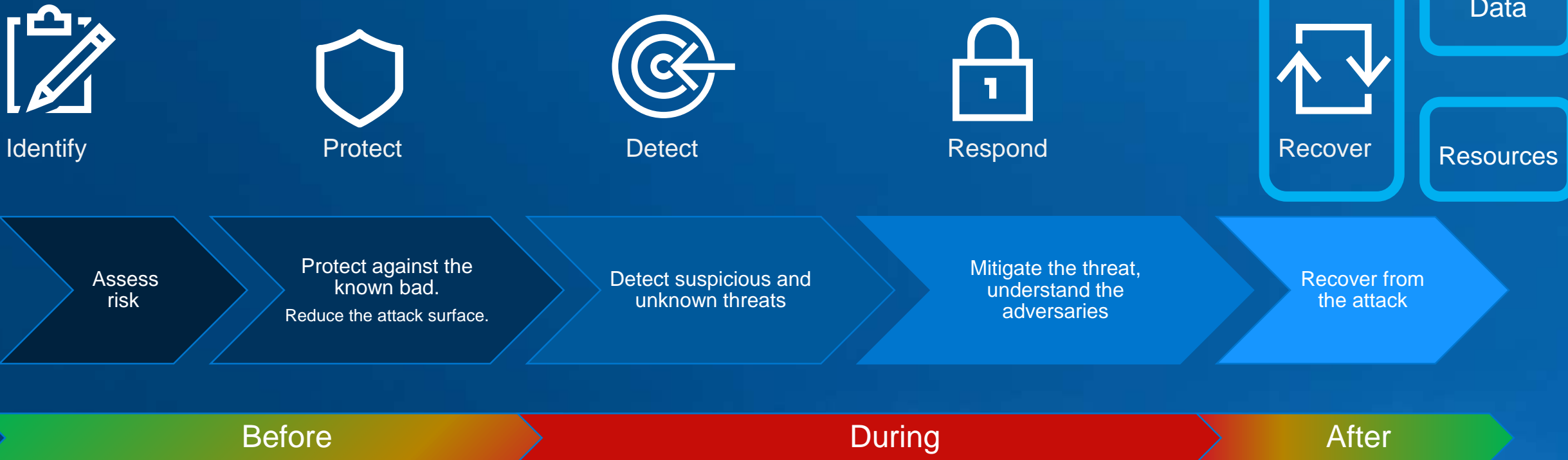# Cyber Recovery
is a solution.

A data protection solution that isolates business-critical data away from attack surfaces.

Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality.

DELLTechnologies

NIST Cyber Security Framework

A high-level holistic strategy that helps organisations:

Identify

Protect

Detect

Respond

Recover

Data

Resources

Assess risk

Protect against the known bad.
Reduce the attack surface.

Detect suspicious and unknown threats

Mitigate the threat, understand the adversaries

Recover from the attack

Before

During

After

Immutability is not offline

Cyber Attack Ziel: … die Datensicherungen

IT / Backup
Admin

Master Server

Backup Catalog Policies

Backup Clients

Client Backup Data

Media Server

Client Backup Data

Backup Targets

Tape   Cloud   NAS   Shares

DELLTechnologies
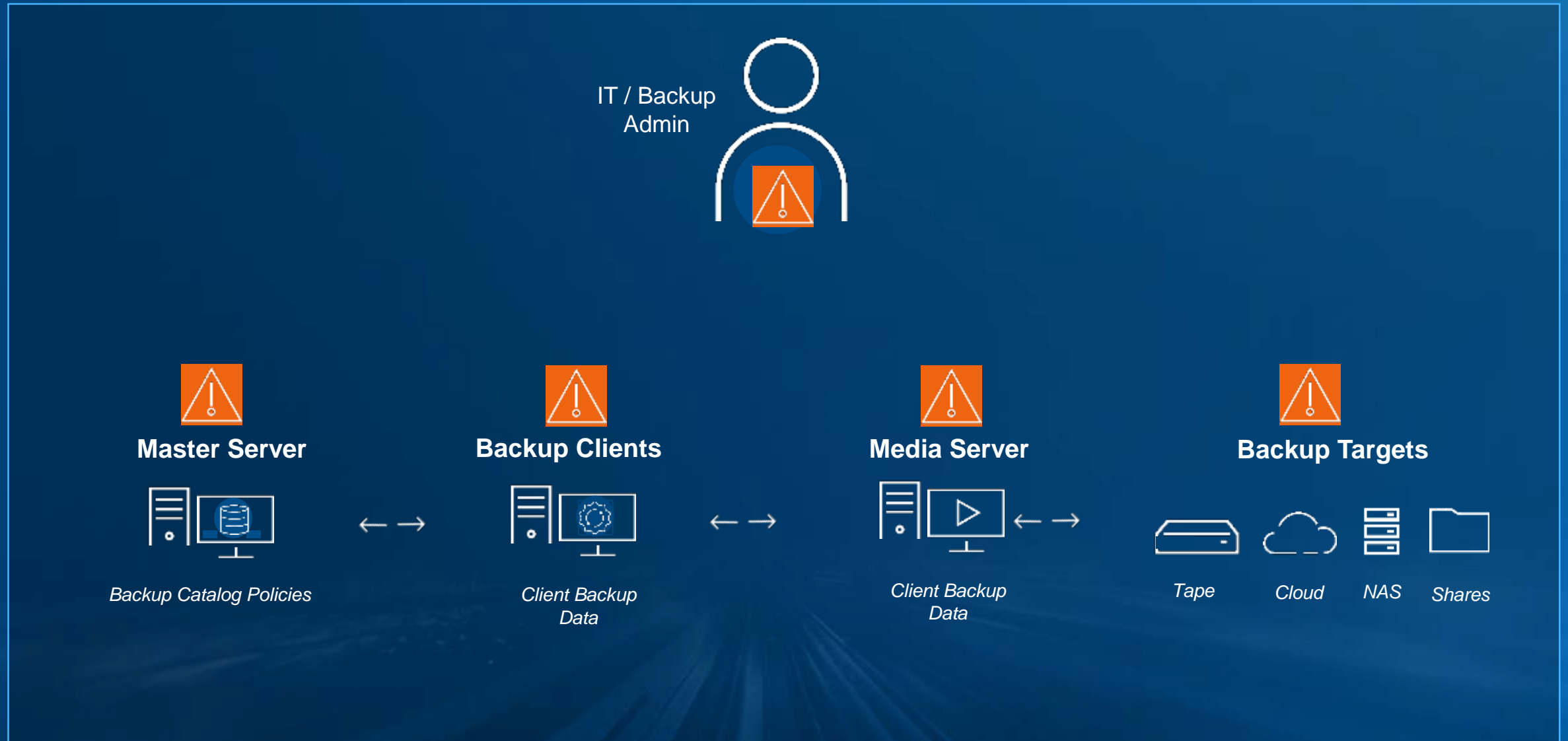
Cyber Recovery Requirements

Modern threats require modern solutions

Isolation

Physical & logical separation of data

Immutability

Preserve original integrity of data

Intelligence

ML & analytics identify threats

DELLTechnologies

Cyber Recovery Vault
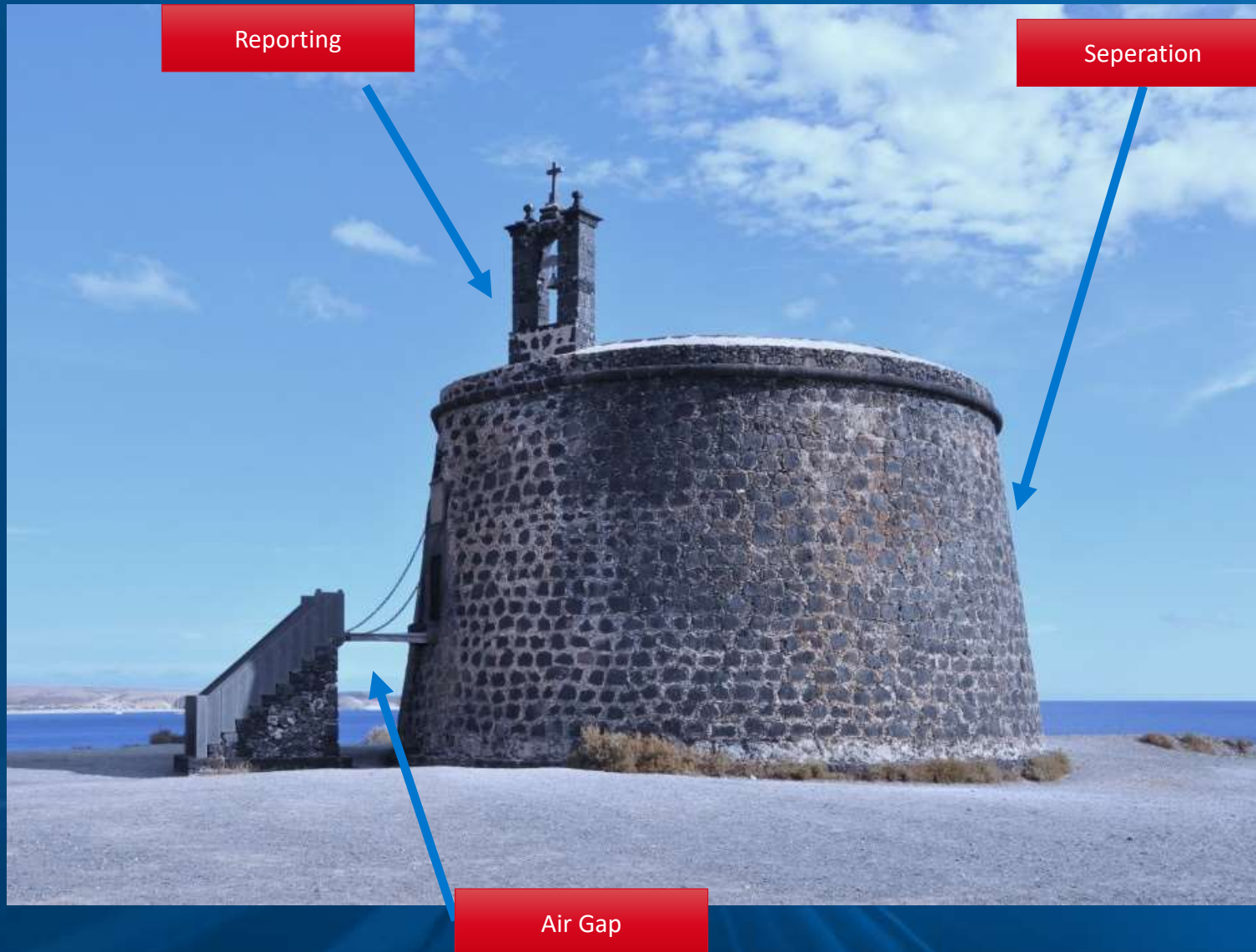
PowerProtect Cyber Recovery
Data Vaulting For Critical Data

Data Center

Production

Backup

1 Sync

Automated Operational Air Gap

Recover

Cyber Recovery Vault

4 Analyze

2 Copy

3 Lock

Monitoring & Reporting

DELLTechnologies
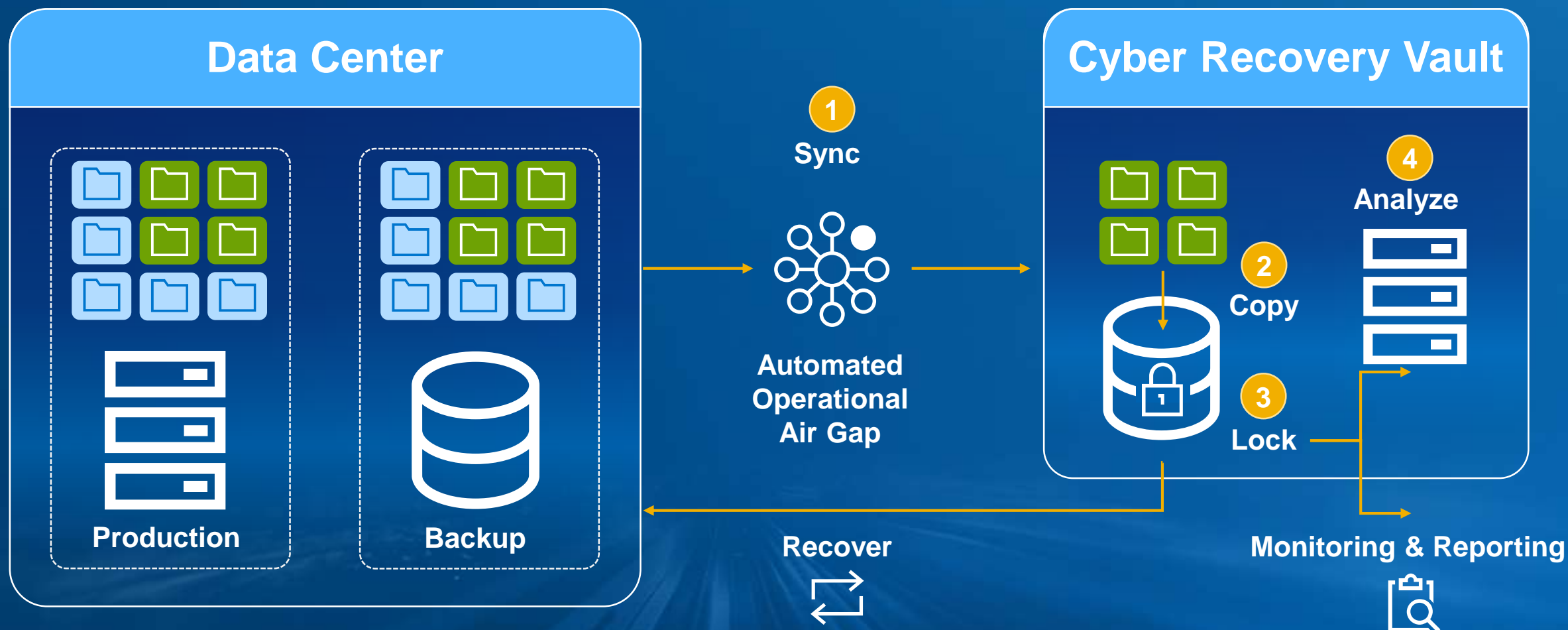
How CyberSense Works

Machine learning enables early detection & rapid recovery from a cyber attack

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
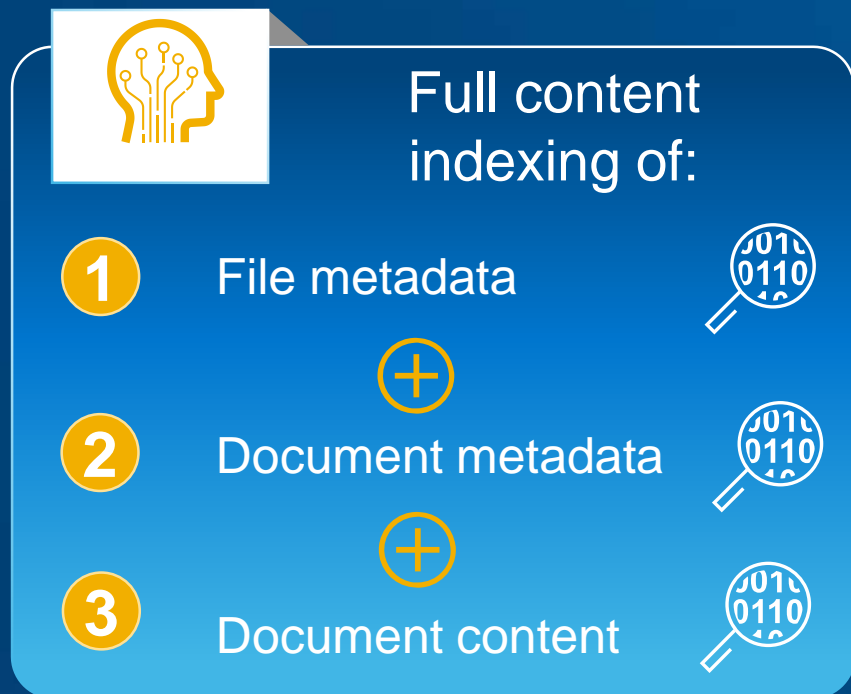Detailed reports, including last good backups for rapid recovery
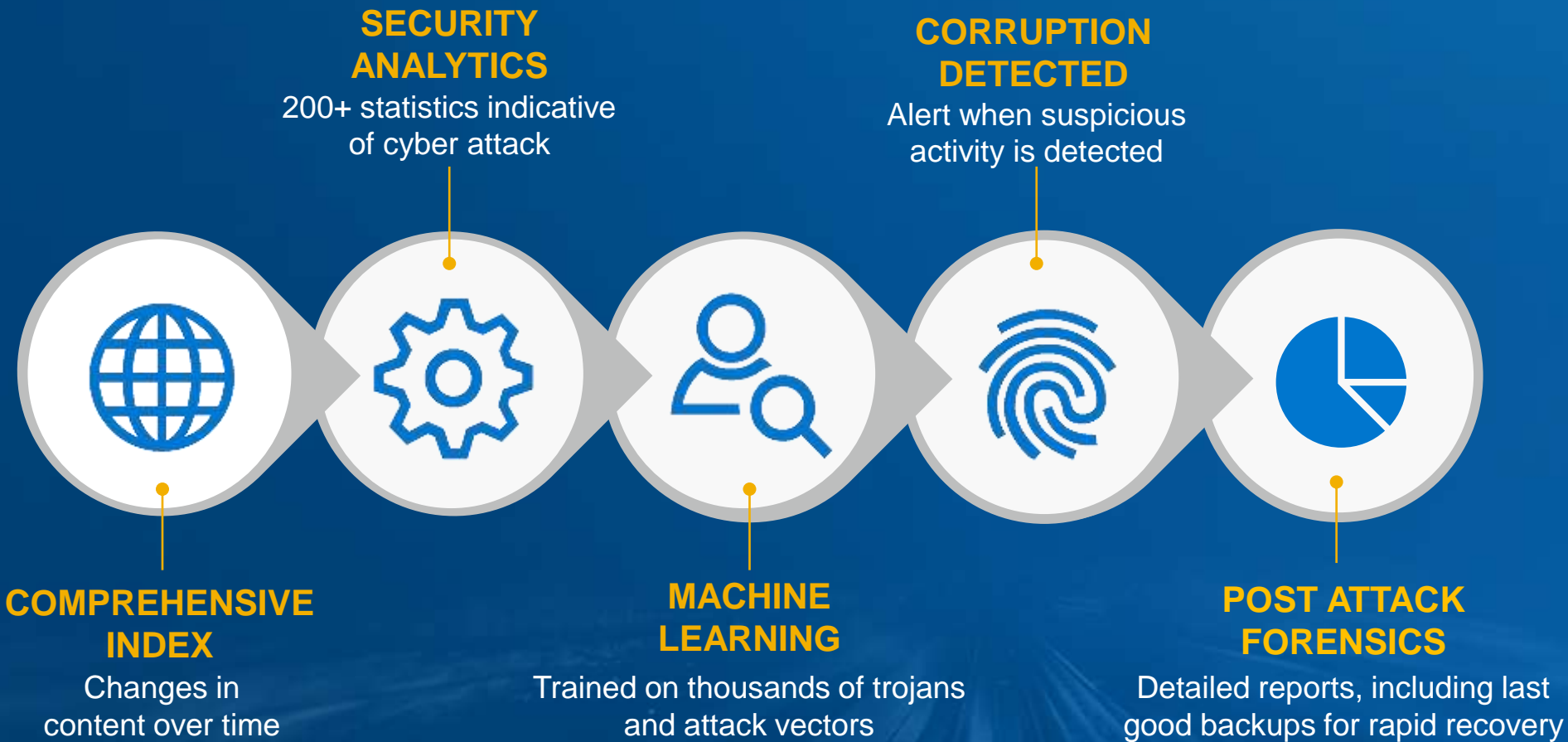
CyberSense Provides

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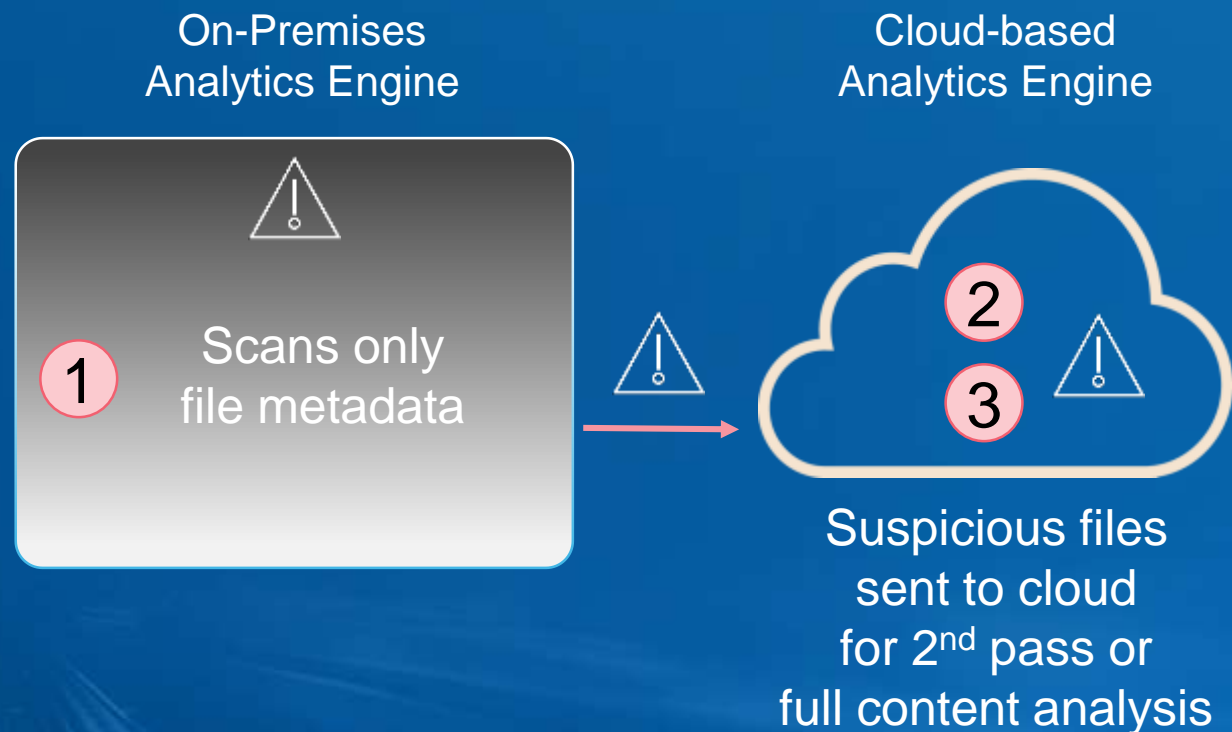
DELLTechnologies

Compare: CyberSense vs. "Basic" Analytics

Machine learning enables early detection & rapid recovery within the Cyber Recovery vault

CyberSense:

Basic Analytics:

Full content
indexing of:

1 File metadata

⊕

2 Document metadata

⊕

3 Document content

VS.

On-Premises
Analytics Engine

1 Scans only
file metadata

Cloud-based
Analytics Engine

2

3

Suspicious files
sent to cloud
for 2nd pass or
full content analysis

D∅LL Technologies