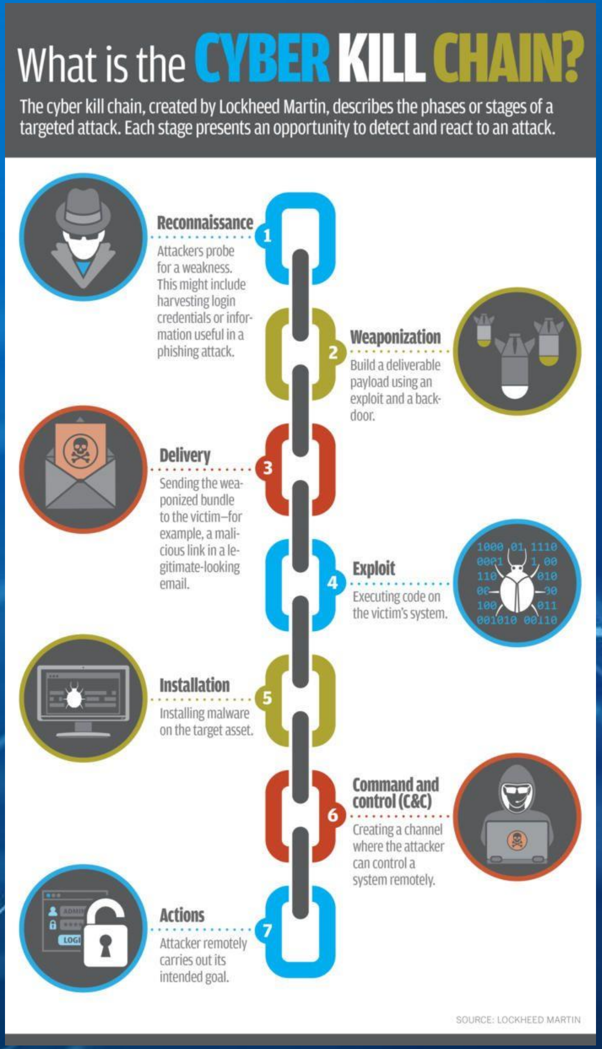
Účinná ochrana kritických dát pred kybernetickými útokmi

Marián Kováčik
Associate Systems Engineer

DELL Technologies

Cyber Kill Chain*

Stages of a targeted attack



What is the CYBER KILL CHAIN?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.

1 **Reconnaissance** Attackers probe for a weakness. This might include harvesting login credentials or information useful in a phishing attack.

2 **Weaponization** Build a deliverable payload using an exploit and a backdoor.

3 **Delivery** Sending the weaponized bundle to the victim—for example, a malicious link in a legitimate-looking email.

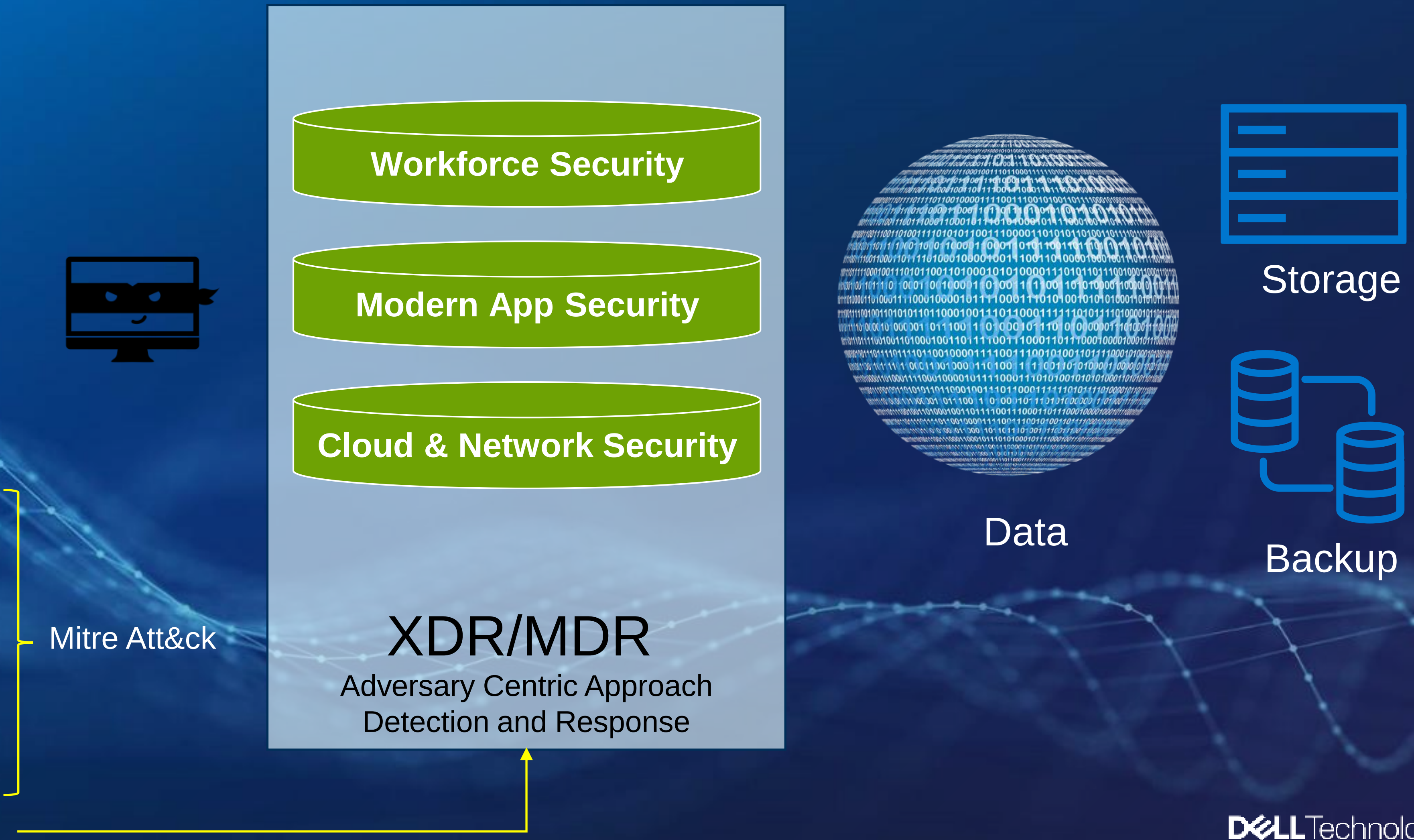
4 **Exploit** Executing code on the victim's system.

5 **Installation** Installing malware on the target asset.

6 **Command and control (C&C)** Creating a channel where the attacker can control a system remotely.

7 **Actions** Attacker remotely carries out its intended goal.

SOURCE: LOCKHEED MARTIN



XDR/MDR

Adversary Centric Approach
Detection and Response

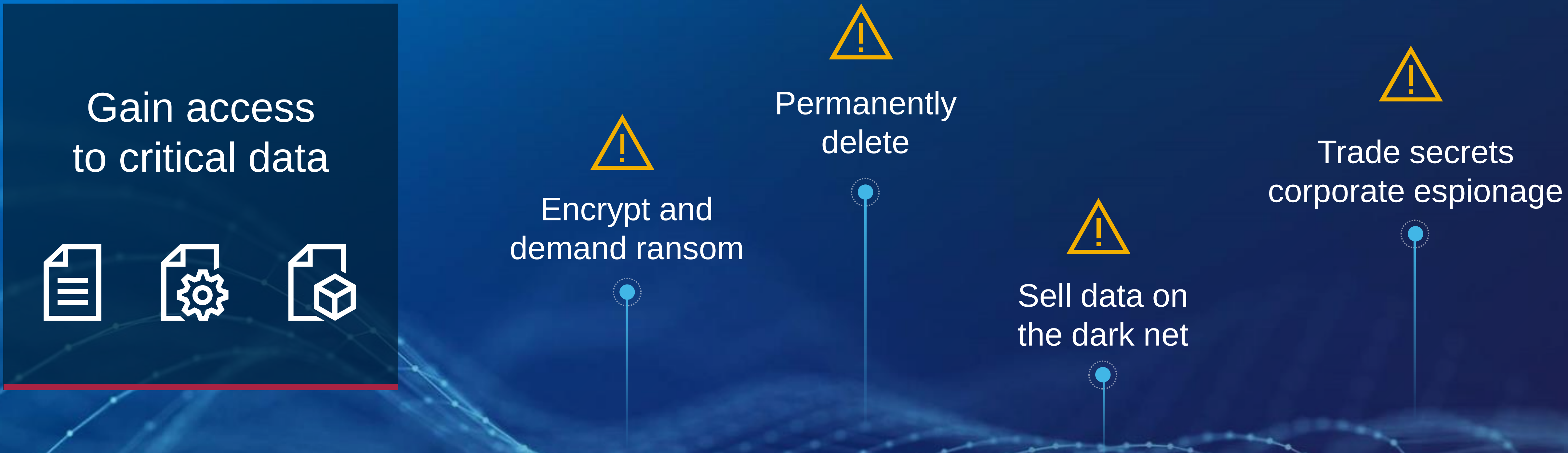
Attacker's playbook

DELL Technologies

* Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

What can happen to data?

Depends on the motive of the attack



Gain access to critical data

⚠ Encrypt and demand ransom

⚠ Permanently delete

⚠ Sell data on the dark net

⚠ Trade secrets corporate espionage

Consequences of cyber attacks

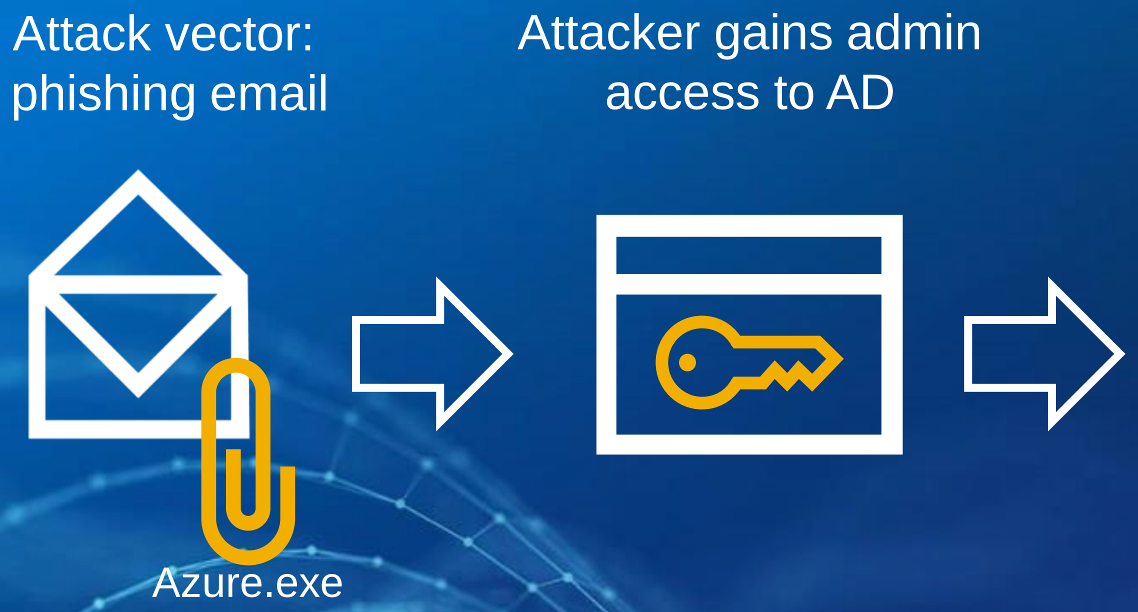
Disrupted operations

Data theft/breach

Ransom money

Business reputation

Anatomy of a cyber attack



Attack vector: phishing email

Azure.exe

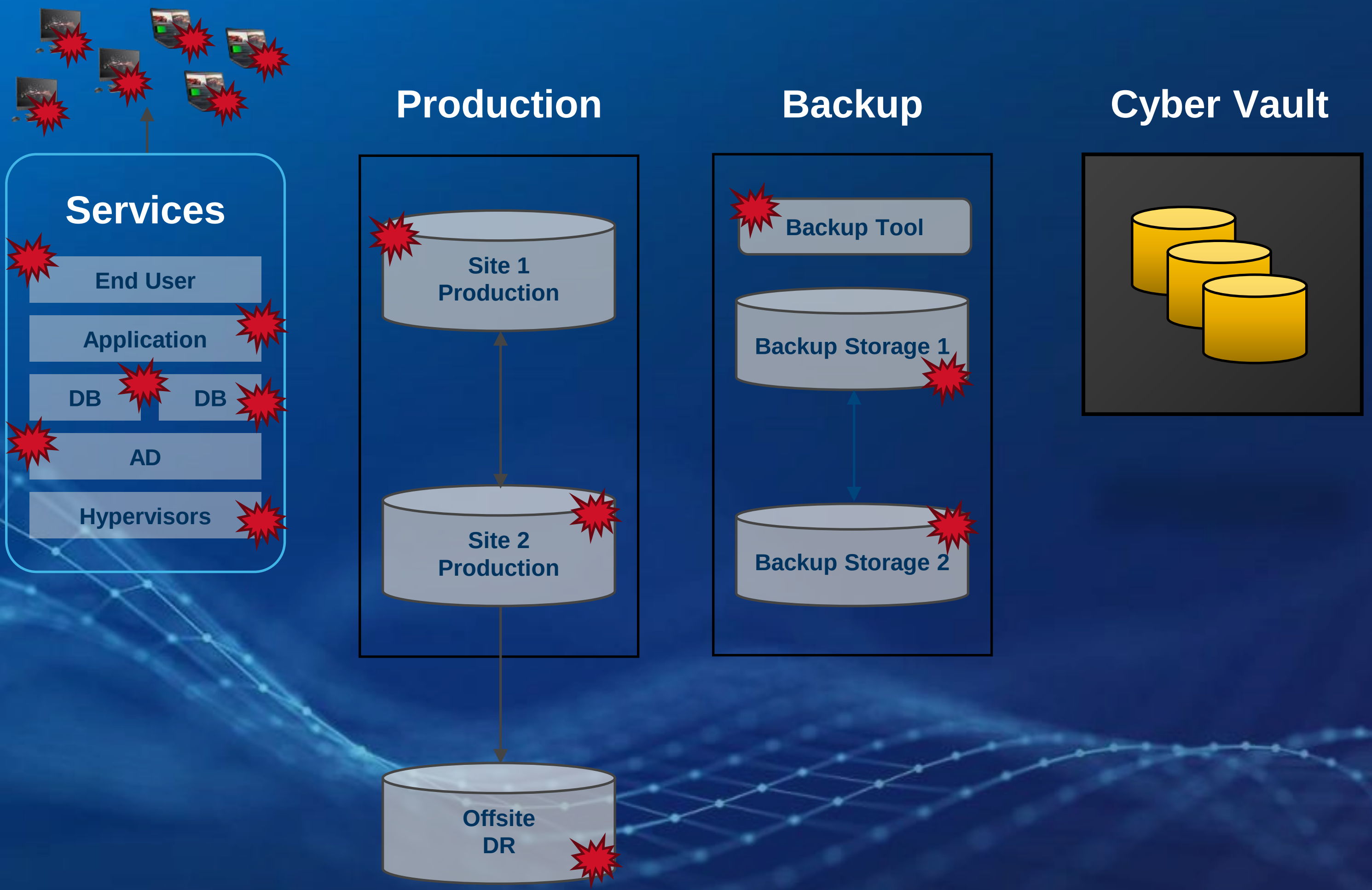
Attacker gains admin access to AD

Critical IT systems down

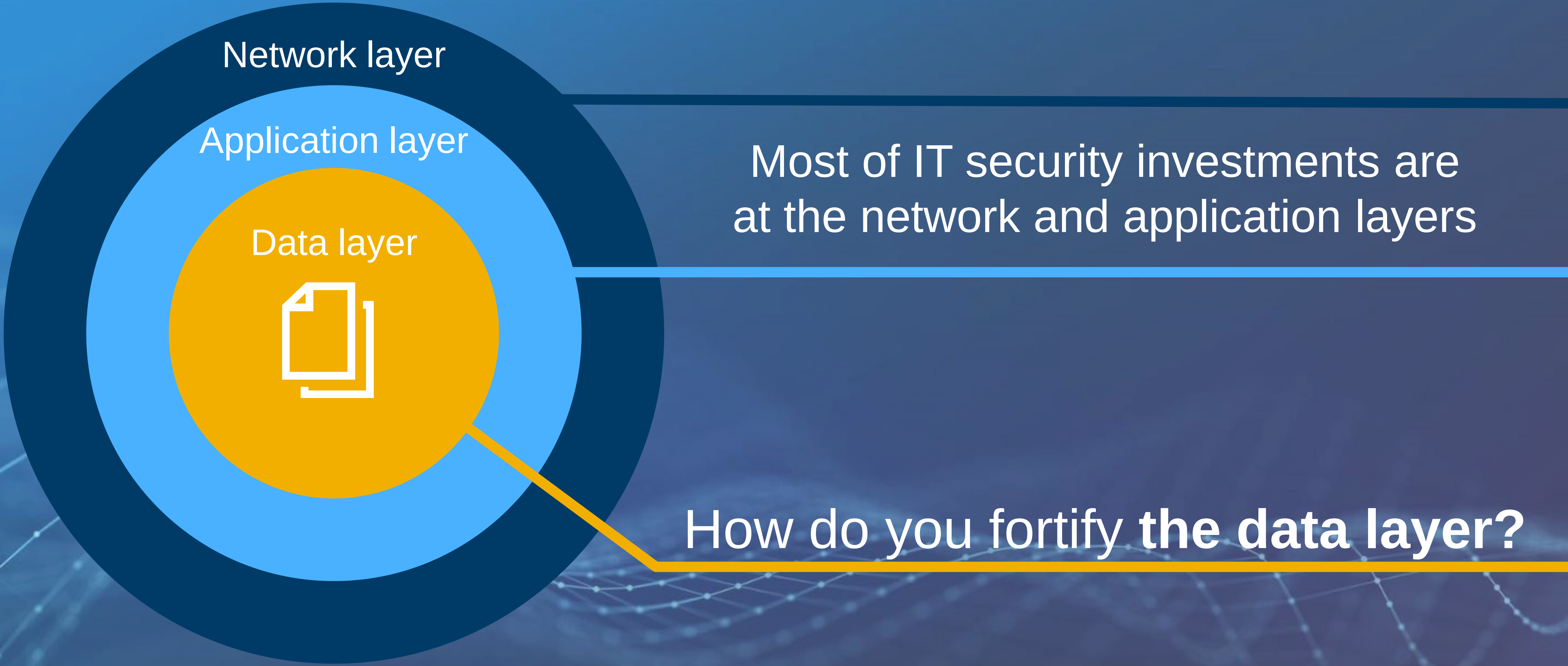
- Network Management Down
- IP Phone System down
- No call list access
- Bridge access down
- Email Access Blocked
- Active Directory Destroyed
- All Windows Logins Disabled
- DNS Erased – systems can’t resolve
- Imaging gateways erased
- Customer Care Erased
- Internet Access Disabled
- Data Centers Isolated
- Gmail used for DR
- Cell phones
- Manual monitoring
- Med tracking and distribution offline
- 66% of NAS storage encrypted
- Snaps overwhelmed by amount of data change
- Unable to roll back snaps

The New Data Center Reality

Vaulting your data in an isolated environment



Cyber Defense at the Data Layer



Most of IT security investments are at the network and application layers

How do you fortify **the data layer?**

Protecting the Complete Data Landscape

Data Landscape

Enterprise databases

VMware

IT Workloads

- Archive
- Home directories
- Video surveillance
- File shares

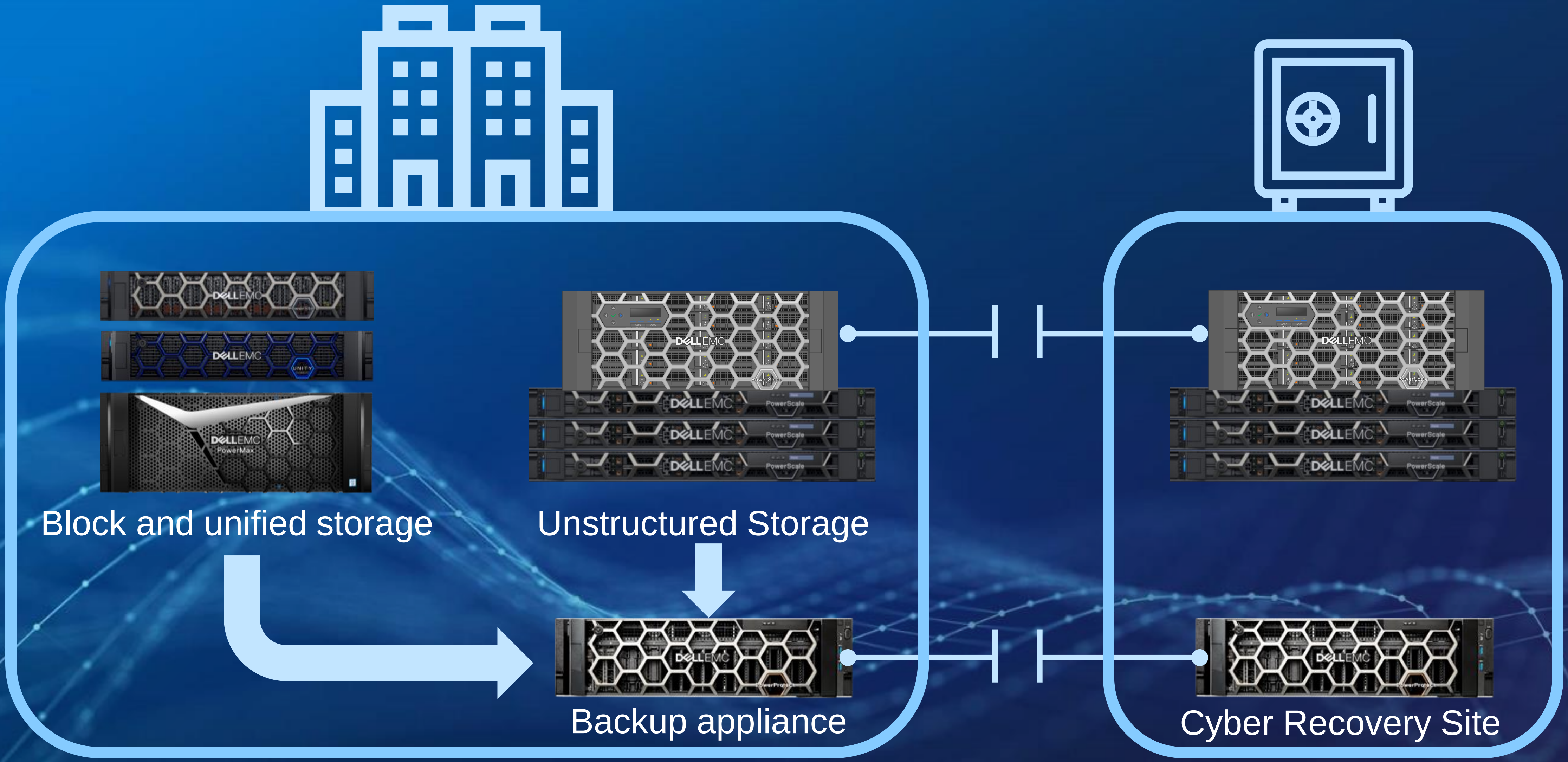
Emerging Workloads

- Artificial intelligence
- Data analytics
- Internet of things

Industry Workloads

- Assisted driving
- EDA
- HC & Life Sciences
- Energy
- High Freq Trading
- Manufacturing

Data Protection and Isolation



Block and unified storage

Unstructured Storage

Backup appliance

Cyber Recovery Site

Key Characteristics of our Cyber Recovery Solution

Isolation

Physical & logical separation of data

Immutability

Preserve original integrity of data

Intelligence

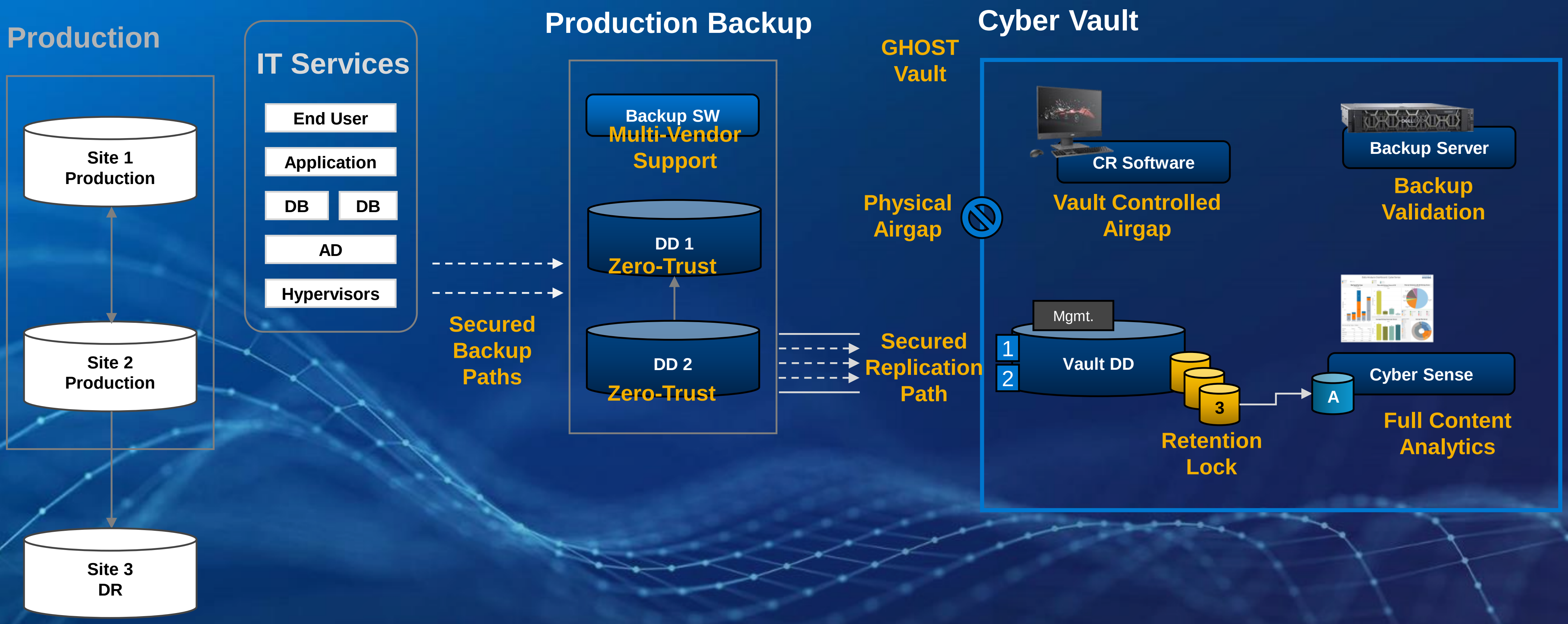
Machine learning based threat detection, alerting and reporting

Recovery

Fast recovery for minimal operational impact

PowerProtect Cyber Recovery

Vault features



Recover with CyberSense

01

Detect: Know When it Happens

Direct analysis of backups to detect corruption

02

Investigate: What Happened

Who was impacted? How much damage was done?
What was attacked? Listing of corrupt files.
Where is the source? What user account and ransomware was used?
When did it happen? What backup sets contain the last good version of data?

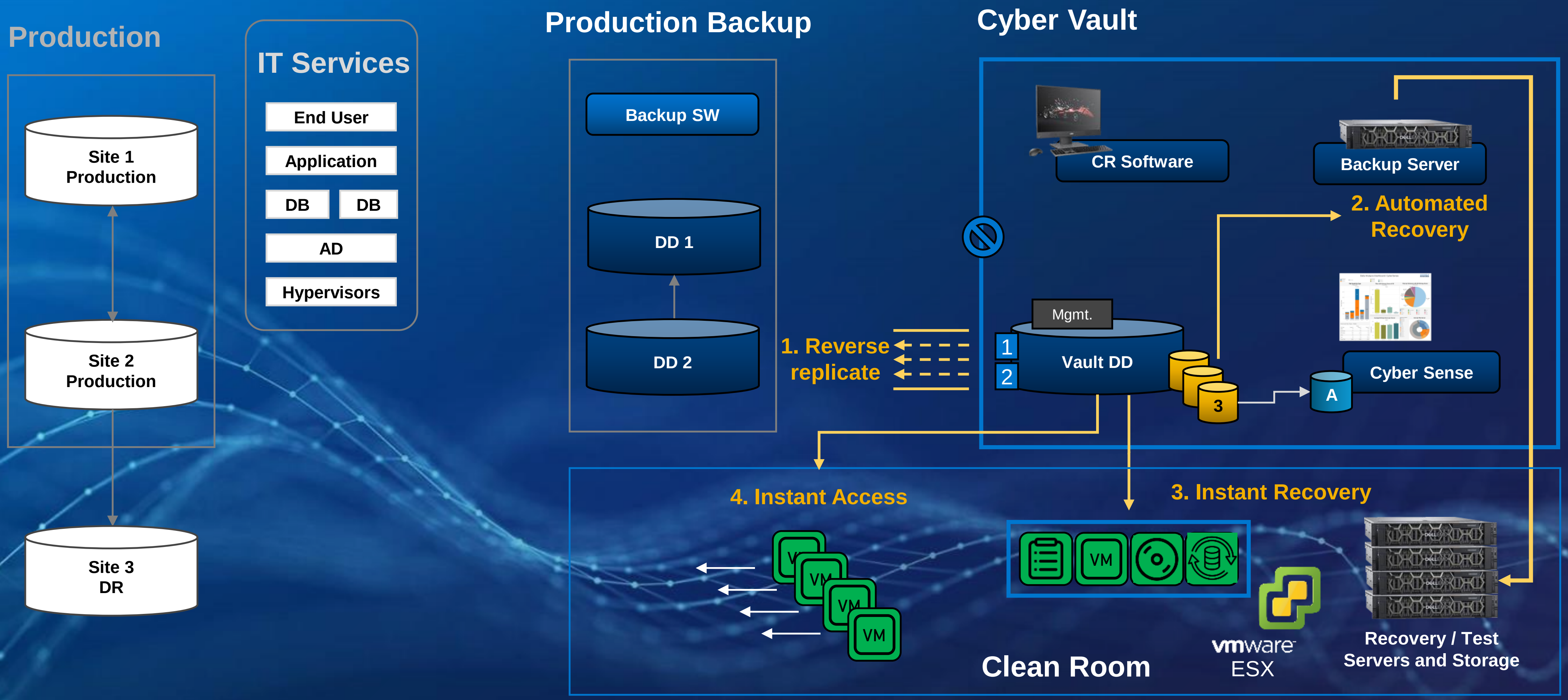
03

Recover: Minimize Down Time

Listing of pre-attack backups to restore business data with confidence

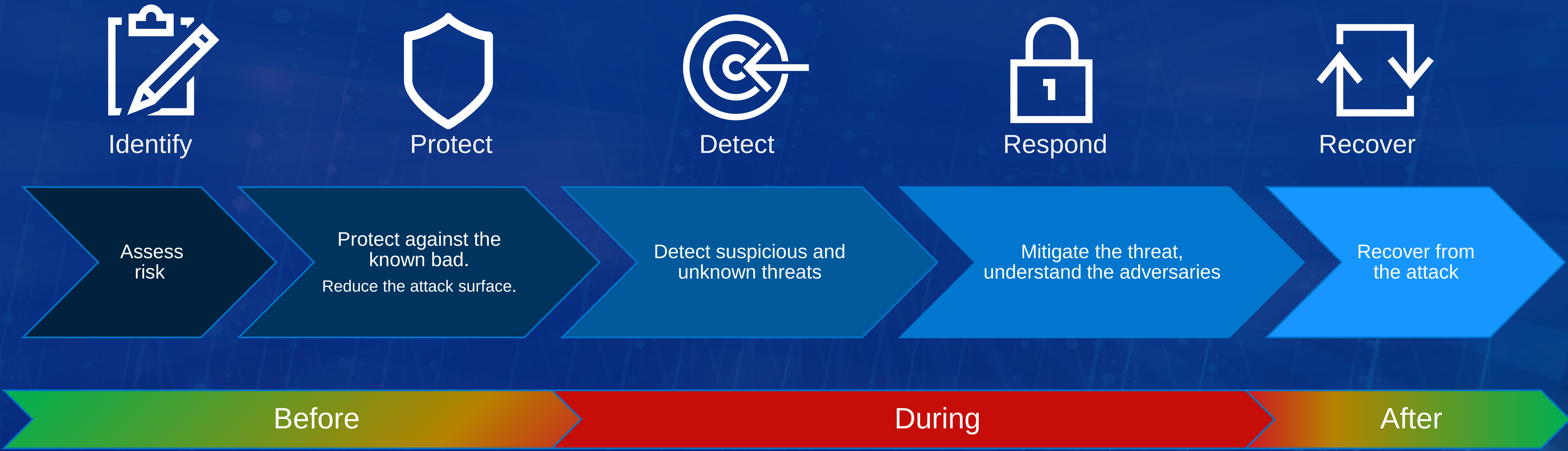
PowerProtect Cyber Recovery

Data Vault restore path



NIST Cyber Security Framework

A high-level holistic strategy that helps organizations



Identify

Protect

Detect

Respond

Recover

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

Ďakujem

DELL Technologies