It is all about recovery…

David Průša
Security and Resiliency Platform Senior Systems Engineer CSH

DELL Technologies

Don’t let security risks stifle innovation

Advance cybersecurity & Zero Trust maturity

Reduce the attack surface

Minimize the vulnerabilities and entry points that can be exploited to compromise the environment.

Recover from a cyber attack

Restore the organization to a previous, known secure and operational state after a security incident.

Detect and respond to cyber threats

Actively identify and address potential security incidents and malicious activities.

DELL Technologies

The Cost of Recovery?

The Impact of Compromised Backups

Restricting the victim's ability to recover

Ransomware actors almost always attempt to compromise your backups

94%

Of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack

SOPHOS: The Impact Of Compromised Backups On Ransomware Outcomes, 2024

PowerProtect Data Domain Platform

Recover faster from the unexpected. Guaranteed.*

* Cyber Recovery Guarantee and Data Protection Deduplication Guarantee. Terms and conditions apply.

Security to ensure data is not tampered with or corrupted

Zero Trust

Hardware Root of Trust | Secure Boot | RBAC | Secure Period

Immutability

Retention Lock Compliance Mode | SEC 17a-4(f) Compliance | FDA 21 Part II

End-to-End Encryption

Data in Flight TL2 1.2 256 Bit | Data at Rest FIPS 140-2 Crypto Libraries

Multi-factor Authentication (MFA)

Web UI, CLI, Security Officer, and iDRAC

Secure System Clock | NTP Clock | Tamper Controls

Clock Change | Drift | Synchronization

File System - DDFS

Hashed Containers – not recognized by malware

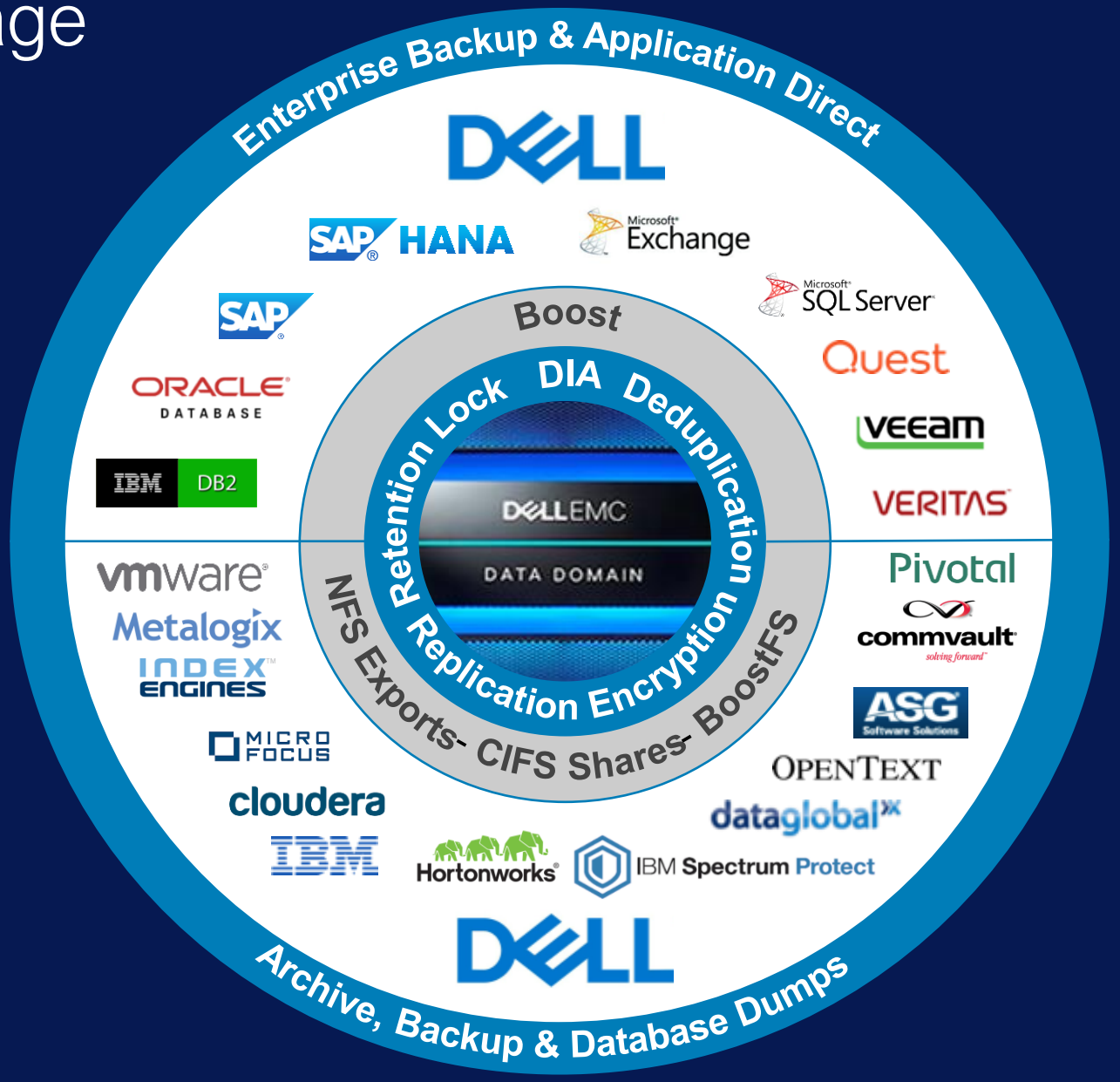
Transport Protocol – DD Boost

Encrypted, Secure, Authorized, Not Open

DELL Technologies

Data Domain Protection Storage

- Multiple Applications and Protocols Supported
- Multiple vendor support
- Global deduplication for high-density storage
- Built-in Data Verification and Protection
- Single platform for backup and archive
- Peace of mind ‘set and forget’
- Investment Protection

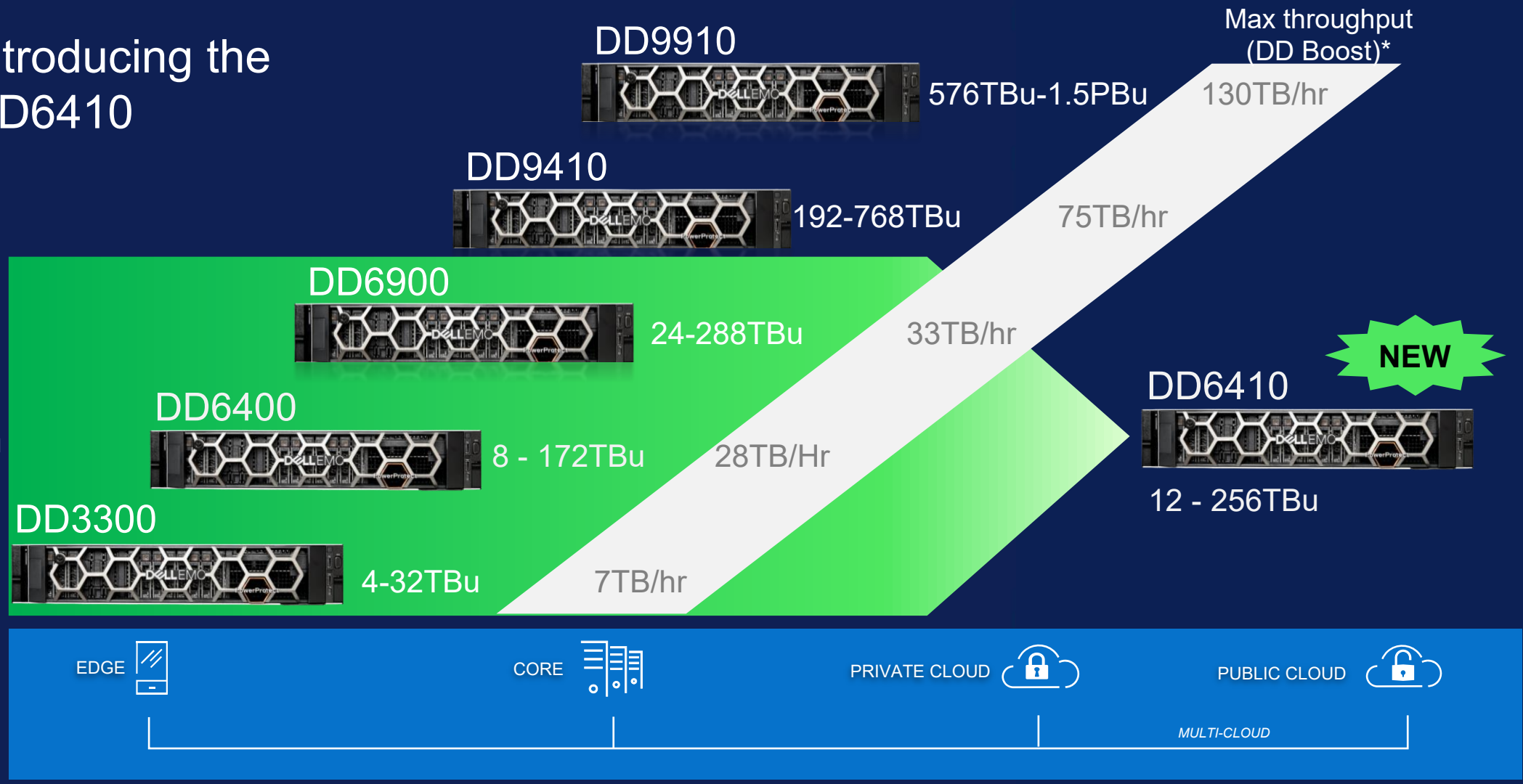


PowerProtect “Data Domain” Portfolio

Introducing the DD6410

DELL Technologies APEX Protection Storage

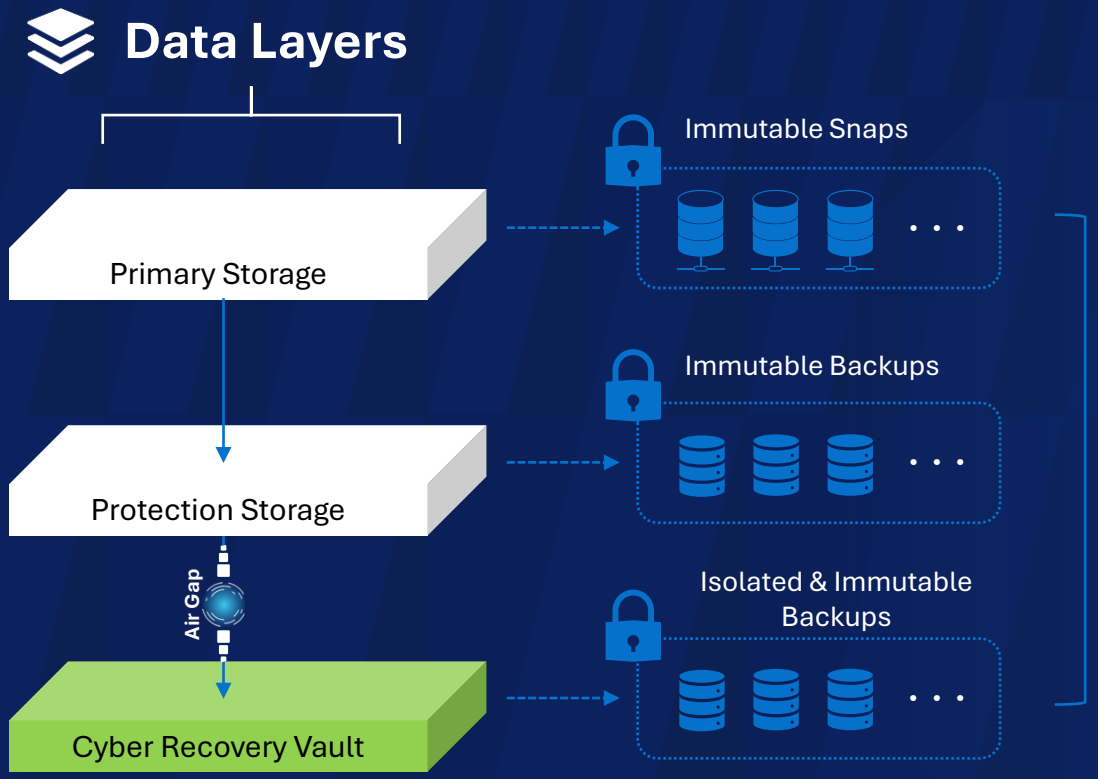
On-prem: 1TBu – 96TBu
In-Cloud: 1TBu – 256TBu



Recover

Detecting threats at the **Data** Layer

Layered approach to resilience



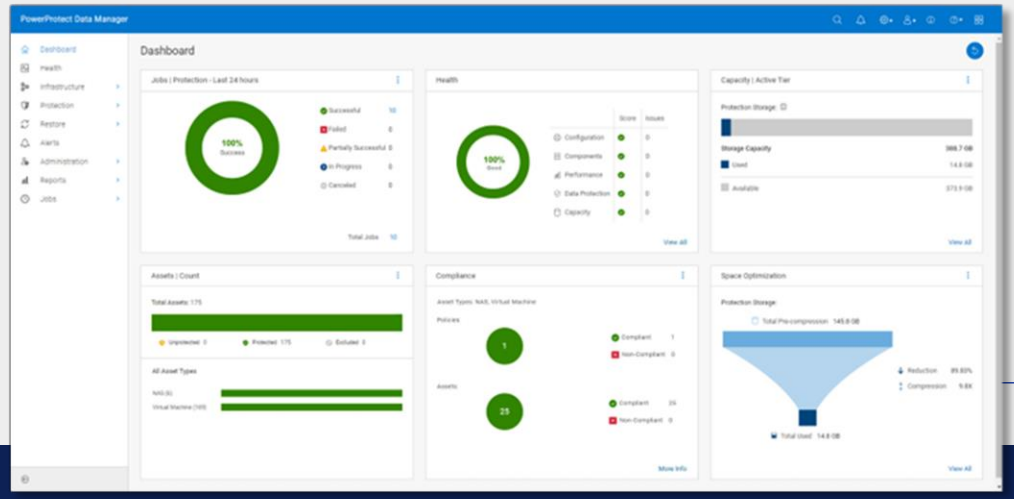
CyberSense
Primary Storage → Scan storage snapshots to identify indicators of compromise and quickly find clean snaps for recovery

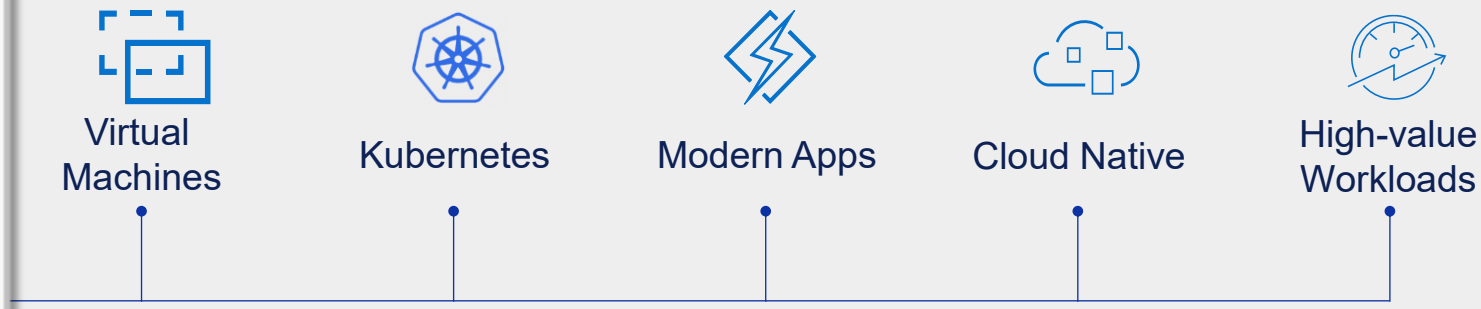
PPDM
Anomaly / Malware Detection → Scan primary backups to identify indicators of compromise and quickly find clean recovery points

CyberSense
CR Vault → Scan isolated vault backups to enable forensic analysis, identify indicators of compromise and quickly find clean recovery points

PowerProtect Data Manager – One Platform

Software-defined data protection platform





Modern

Powerful protection innovation

Simple

Flexible user experience

Resilient

Operation and cyber resilience

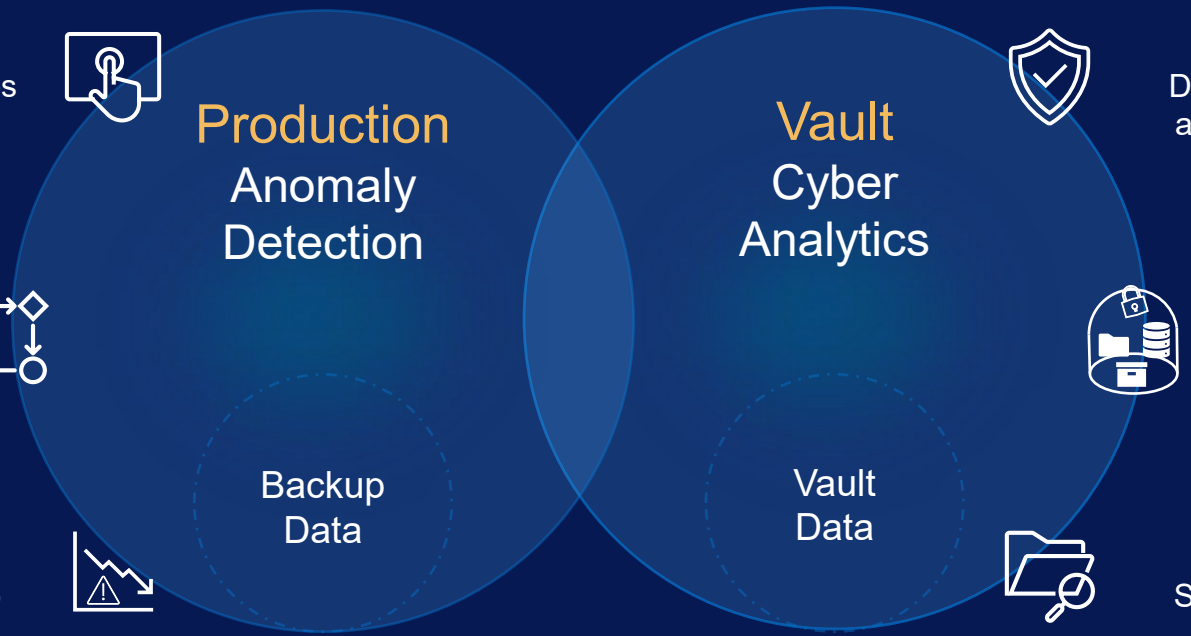
Complementary Anomaly Detection

Unusual Data Activity Anomalies are part of a comprehensive MDR strategy

Identify Anomalies
UDA across primary data backups

Integrated Backup App
Quarantine to avoid reinfestation

Remove from Backups
Remove from primary backups to eliminate future risk



Trusted Accuracy
Detect data corruption with 99.5% accuracy with intelligent recovery

Isolated & Available
CyberSense secured inside the vault to ensure analytics are available

Identify Malware
Scan signatures of all vaulted data

Cyber Recoveries

Triage & Recovery Options

Three Proven Recovery Options with Immutable Copies

Two-Copy Solution

- Two Immutable Copies
  - Immutable Copy in Production
  - Immutable Copy in DR Site
- Recovery is launched in Production
- Lacks the advantage of Isolation
- Recovery can be held until Triage/Forensic work is completed
  - Hardware would be inaccessible

Two-copy + Isolated Vault

- Third Immutable Copy in a Vault
- Hardware and Immutable Copies kept off the Production Network
- No SSH capabilities into the Vault
- Option for scanning and analysis of Immutable Copies in the Vault

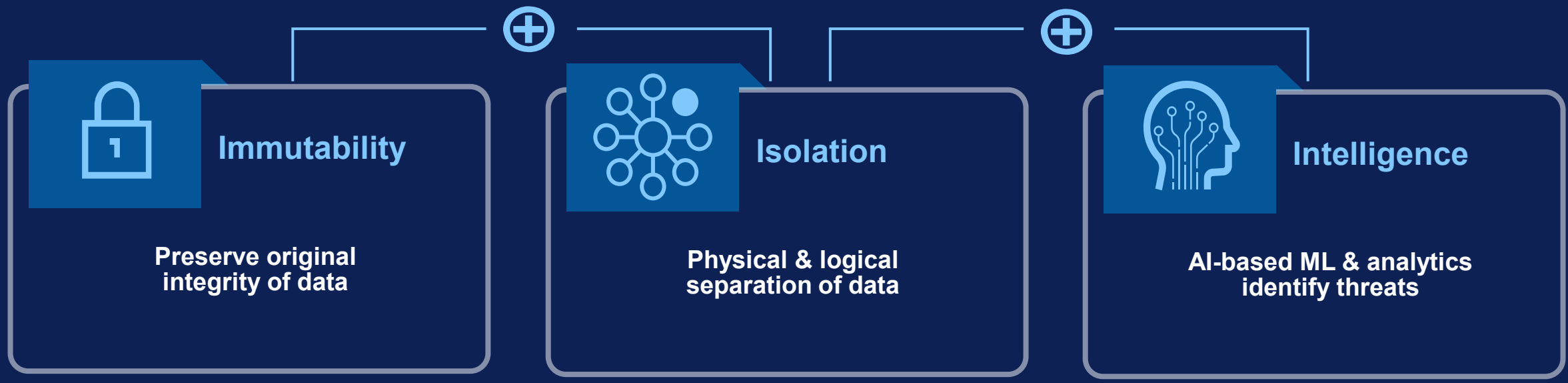
Vault with Clean Room / MVB

- Extensions to Isolated Vault
- Clean Room for Analytics and Forensics
- Minimum-Viable-Compute standing up Platinum Applications
- Can provide a reduced time to Resolve/Recovery for selected applications/services

[1]Not a commitment. Some items under consideration only

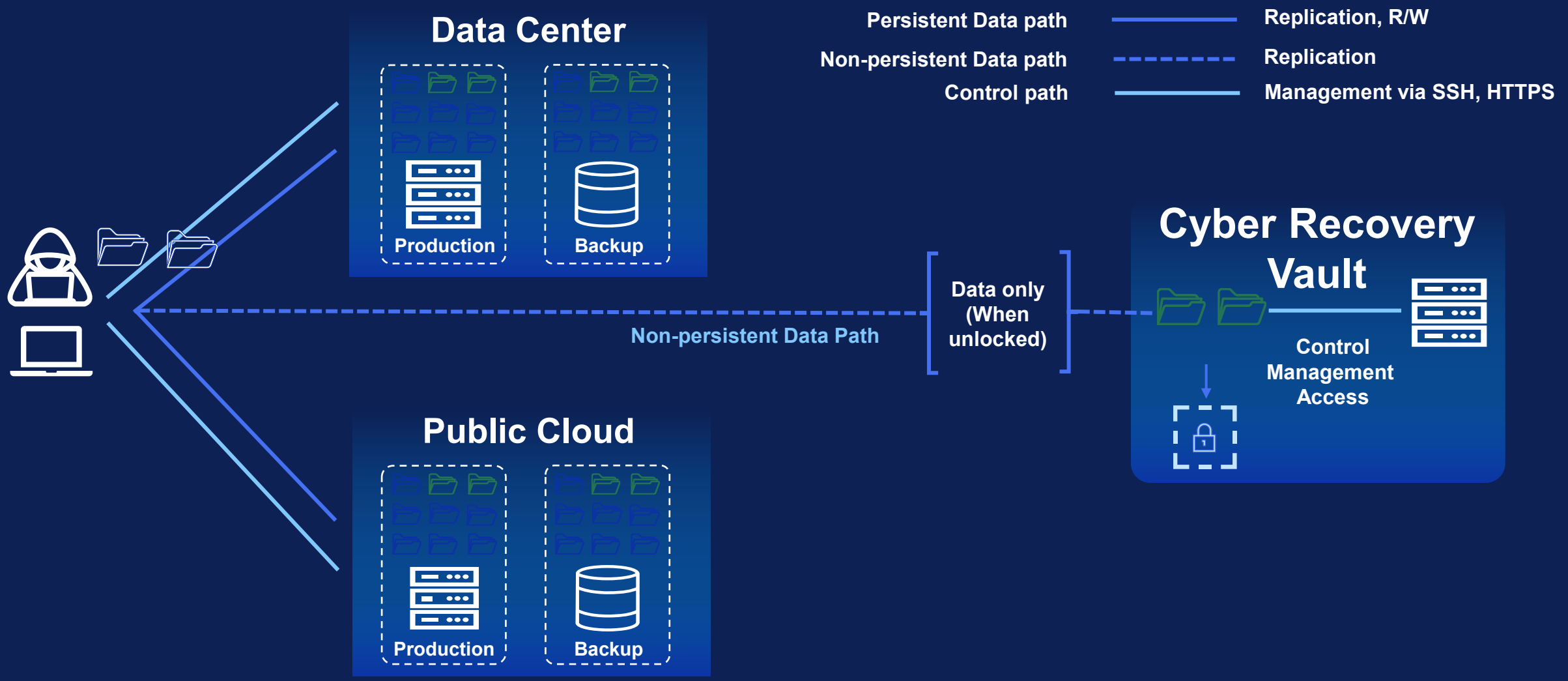
DELL Technologies

Comprehensive cyber resilience



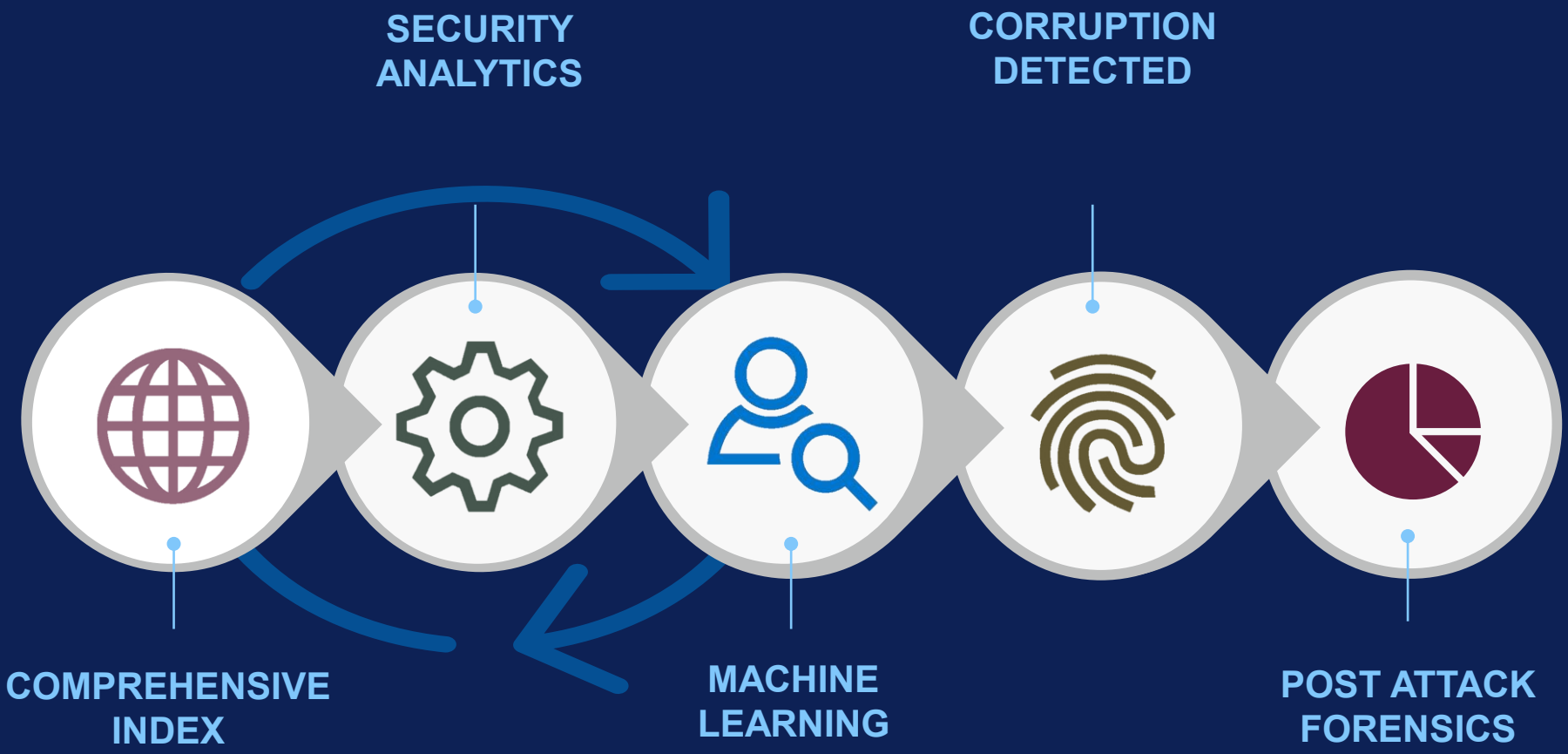
The importance of isolation

Improve on immutability by denying access



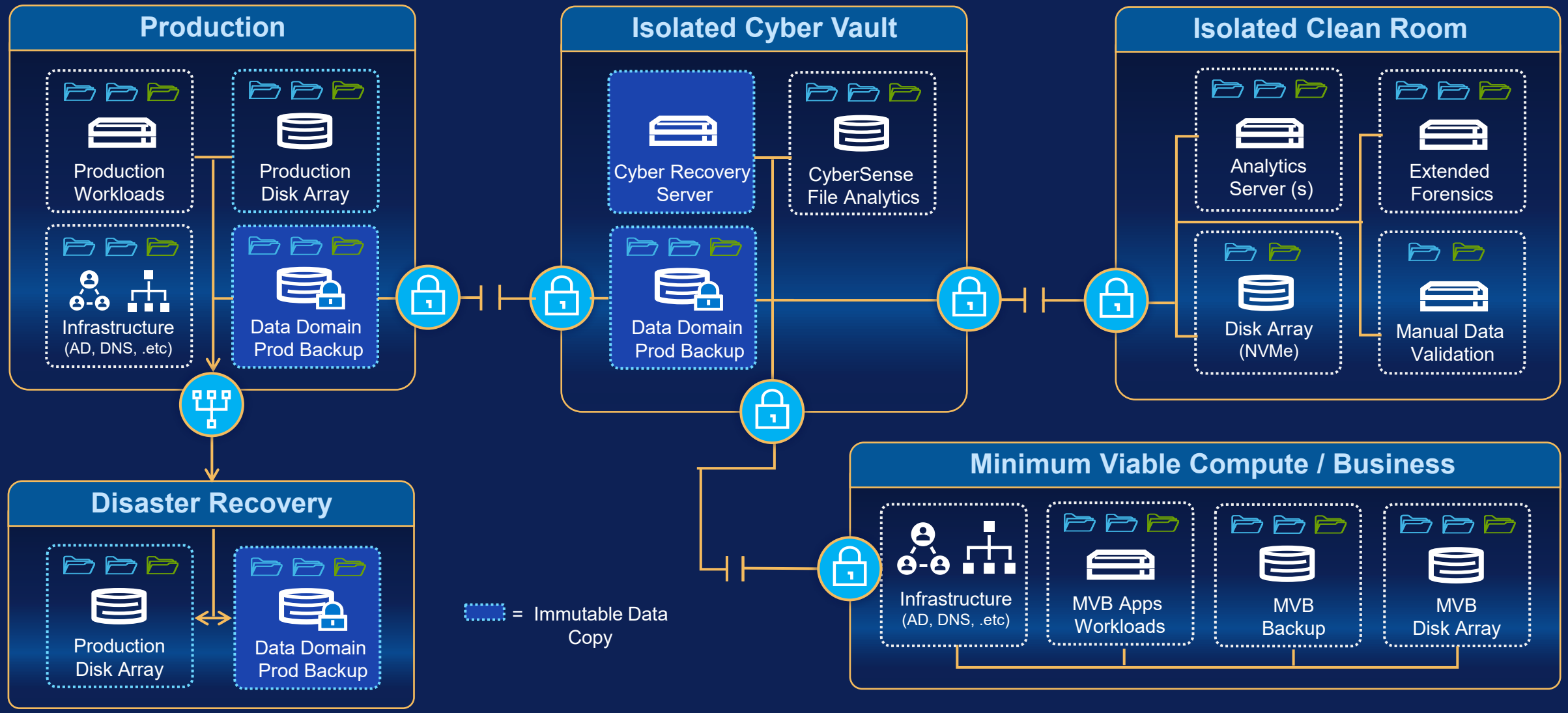
How CyberSense Works

Analytics, machine learning and forensic tools to detect & recover from cyber attacks



Backup Images in Production + Vault + Clean Room + Minimum Viable Compute

Two-Copy plus Isolated Vault plus Clean Room plus Minimum Viable Compute



DELL Technologies

MDR is like the security cameras monitoring a house

NIST

Identify	Protect	Detect	Respond	Recover
When building or remodeling a house you first make a plan and determine what you need	Good house design includes protection against intruders, like locks on the doors and windows	You can also add an alarm system that includes security cameras from a company that monitors the alerts	Security experts are keeping watch and will respond quickly and appropriately, 24x7	All these efforts may still not be enough. If a theft or fire happens, you will need help right away!

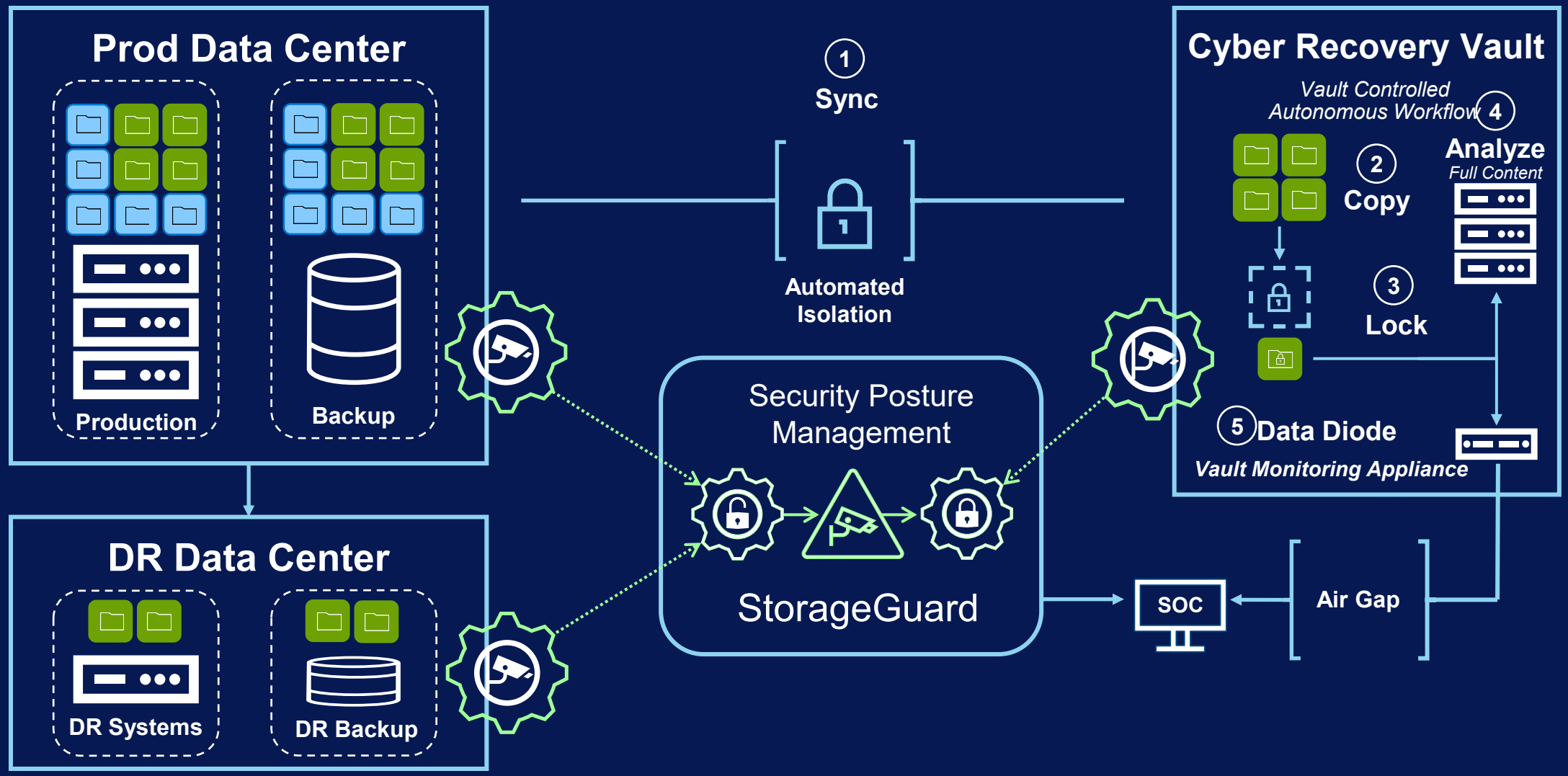
Story

Dell Managed Detection and Response

Our Incident Recovery team can put the fire out, repair the damage and get you going again

Security Posture Management for Data Protection

Ensuring Security Compliance and Vulnerability Management



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

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

Děkuji Vám za pozornost ...

David Průša

david_prusa@dell.com

https://www.linkedin.com/in/prusa/

+420 608 877 515

DELL Technologies