

October 2024 – Security Day




Dell Technologies Advantage

Keep Your Data Secure



Aurimas Pažėra
Advisory Systems Engineer, Solution Architect
ISG Technology Consulting

DELLTechnologies



INTRINSIC SECURITY

10 cybersecurity measures mandated by the NIS2 & DORA

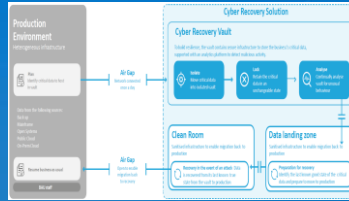
#1 Risk Analysis



#2 Incident handling



#3 BC and Crisis management



#4 Supply Chain Security



#5 Vulnerability Assessment



#6 Testing and auditing



#7 Basic Hygiene and awareness training



#8 Cryptography and Encryption



#9 Access Control and asset management



#10 Multi-factor Authentication



STIG Compliance

Standards-based hardening by Security Technical Implementation Guides



Access Control

Use role-based access control (RBAC) to manage user permissions effectively



Data Encryption

Ensure that data at rest and data in transit are encrypted using strong encryption algorithms



Patch Management

Regularly update and patch the storage system's firmware and software to address security vulnerabilities. Ensure that security patches are tested and applied promptly



Network Security

Implement network segmentation to isolate storage systems from other parts of the network



Audit and Logging

Enable audit logging to track and monitor activities on the storage system. Maintain log files and regularly review them for suspicious activities



Secure Configuration

Guidelines for secure configuration of Dell storage systems, including disabling unnecessary services and features



Account Management

Enforce strong password policies and regularly review and update user accounts. Ensure that default and unused accounts are disabled or removed



Vulnerability Assessment

Regularly conduct vulnerability assessments and security scans to identify and remediate vulnerabilities in the storage system



Physical Security

Secure the physical environment of the storage systems to prevent unauthorized access to the hardware

Know when your data is compromised in a production environment –

AIOPS

Anomaly detection

Monitoring storage and data access for suspicious activity



AI powered tools

Look for patterns in data access that are indicative of a compromise



Security alerts

Integrated with upstream security platforms with API-based automation



Continuous monitoring

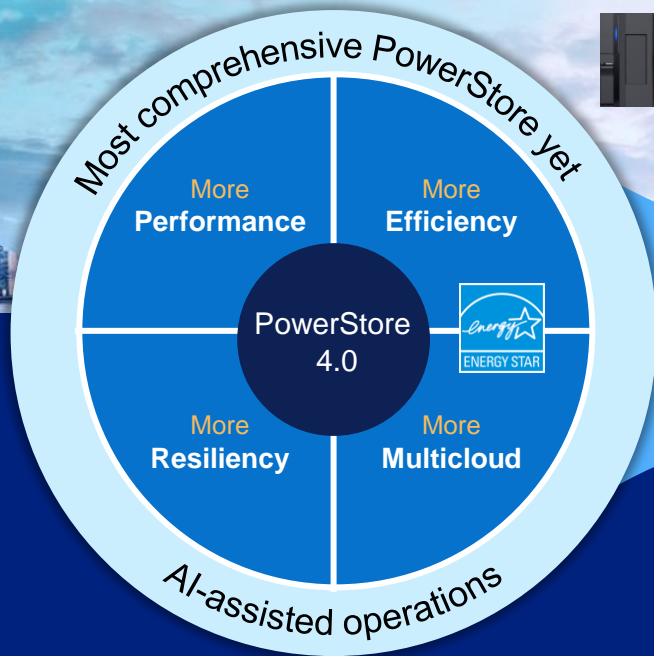
Centralized storage and cybersecurity monitoring for early detection



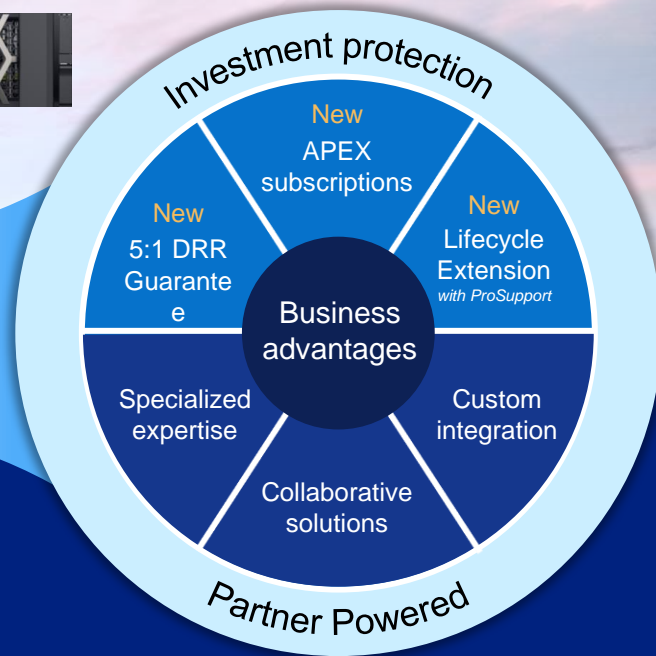
Identifies malicious activity + Minimizes exposure

Introducing PowerStore Prime

The smart choice for all-flash storage



Integrated offering
Everything you need
to succeed!



PowerStore 4.0 Overview and Highlights

New PowerStore QLC Offering
PowerStore 3200Q



Enhanced Service Provider Support

QoS capabilities for block
Network Scalability Enhancements



New Sync Replication

Support for Sync replication
for block and file



New Capacity Accounting

Capable of identifying and
reporting unreduceable data



New Metro Volume Enhancements

Additional Metro OS support for
Windows and Linux
Additional support for VGs



Data Compression Enhancements

New variable block-size
compression



New Data Migration Enhancements

File Migration from Unity to PowerStore
Universal Storage array migration



Scalability and Performance Enhancements
Volumes, Connectivity, Data Protection and other objects
scalability enhancements



New PowerStore 3200Q model

Improved economics, while Maintaining all PowerStore's key winning properties

Latest NAND Technology QLC-only 'Capacity-Optimized' PowerStore offering!



11 Drive starting point (15.3TB QLC drives)

- 103.2 TiBu minimum config per appliance
- 1.04 PiBu maximum config per appliance
- 5.2 PiBe per appliance

Cost-effective enterprise solution

**Feature parity with
PowerStore T**

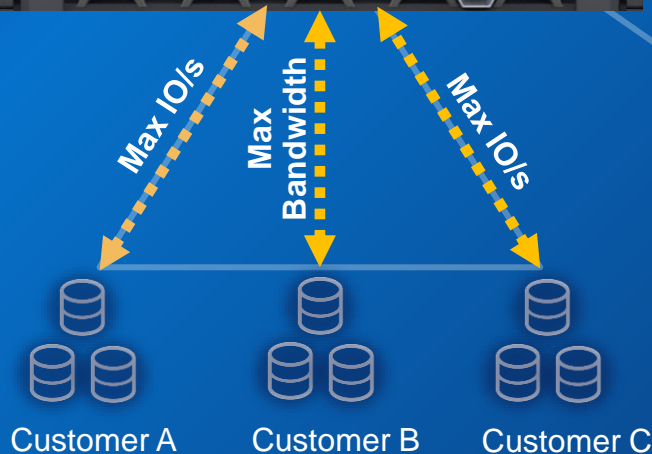
**Scale-up and Scale-out –
Mix-and-match appliances
(clustering / replication)**

**Minimal to no system
level performance
degradation**

**No throttling performance
between QLC and TLC
hardware!**

PowerStore QoS for Block Resources

Supporting Internal and External Service Provider's use-cases
eliminating "Noisy Neighbor"



Create Block IO Limit Rule

General

Name

IO Limit Type

Absolute Limit

Max IOPS Max Bandwidth (KBps)

Density based Limit

Max IOPS per Provisioned GB Max Bandwidth (KBps) per Provisioned GB

Burst %

Customers now guaranteed service for critical applications!

Simplified Management

- PowerStore Manager
- PowerStore CLI
- REST API

Applicable on:

- Volume
- Volume Group

QoS Policy Limit Types:

- Absolute IOPS (IOPS)
- Absolute Bandwidth (MB/s)
- Density (Max IOPS/GB or BW/GB)

Burst Definition:

- %Burst from Max value

Expanded Metro Volume Support

Automated, intelligent high availability shared storage across sites

Active/Active: Now expanded for Windows and Linux hosts!

All new Volumes and Volume Groups support!

Simple

Included with PowerStore – no additional equipment or purchase required

Supported OS's

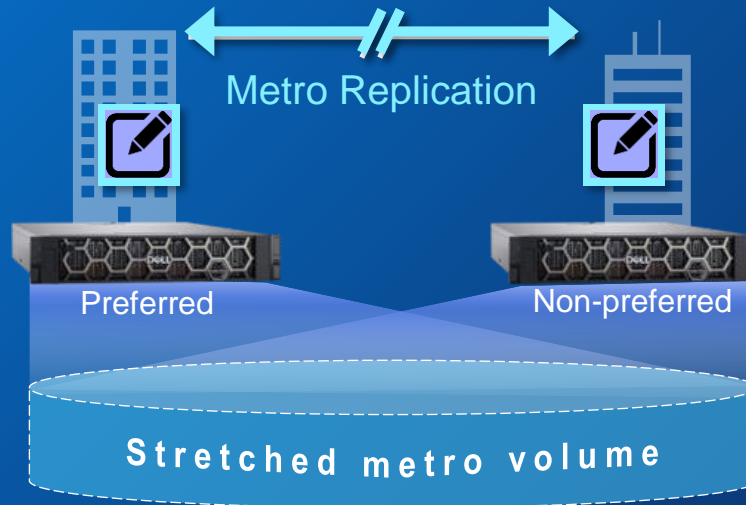
- RedHat (RHEL / OEL) Linux 8.2 +
- SLES 15 +
- Windows 2016 +

Benefits

- Zero RPO/ RTO
- Auto-failover
- Disaster avoidance
- Load balancing
- Migration

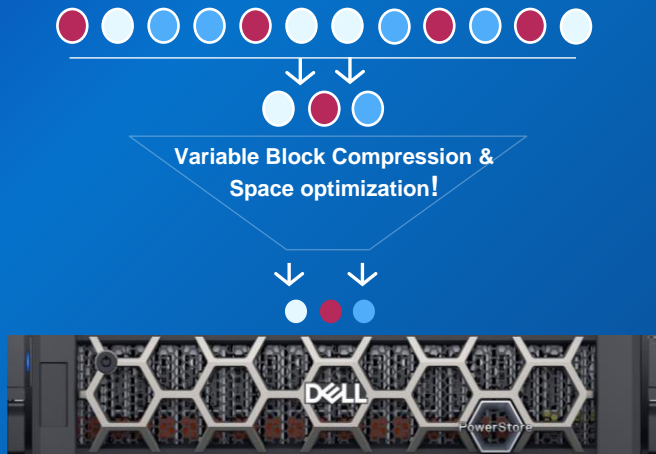
Leverages Metro Behavior

Seamlessly switches between Witness and Local Role if Witness is not available



Storage Efficiency Gains - 5:1 DRR

Enhanced services work proactively on your behalf



Always on | HW-assisted

Storage efficiency **without compromise**

Enhanced Compression

- All new large block-size compression, supporting better compression ratios and capacity savings
- **Enhanced compression gains of up to ~20%**

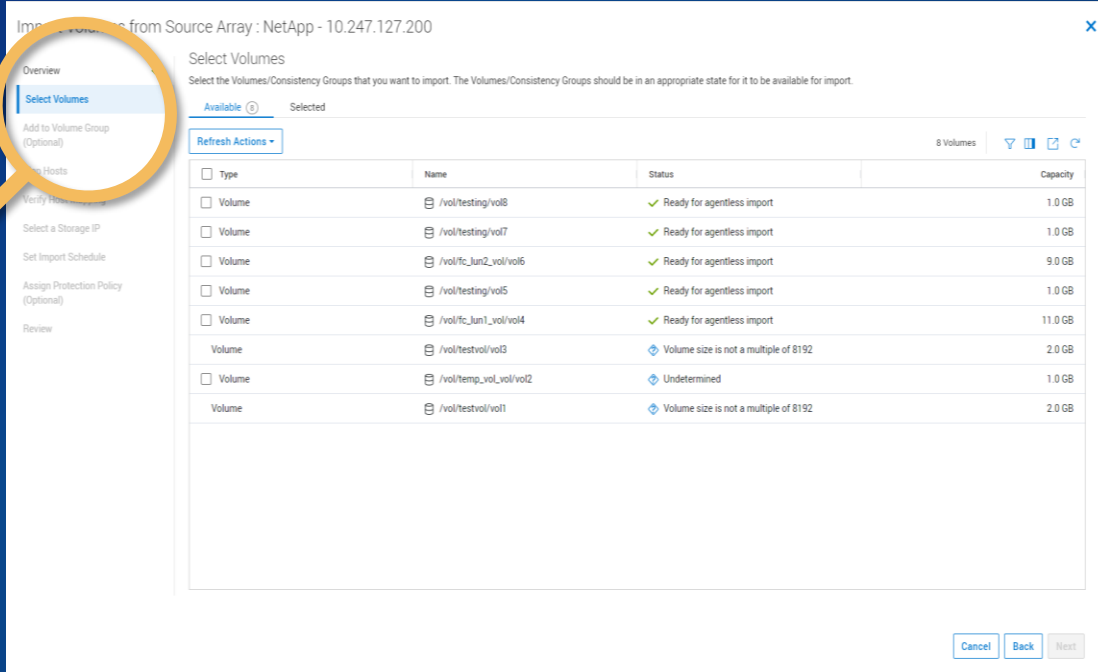
NEW DRE spare space efficiency optimization increasing Usable Capacity

- Increase total usable capacity for new and existing systems by 2% optimizing DRE spare space

Guarantee increased to 5:1

Universal Storage Import

Provides simple way to import block storage from ANY array!



Import Volumes from Source Array : NetApp - 10.247.127.200

Select Volumes

Select the Volumes/Consistency Groups that you want to import. The Volumes/Consistency Groups should be in an appropriate state for it to be available for import.

Available (8) Selected

Refresh Actions

Type	Name	Status	Capacity
<input type="checkbox"/> Volume	/vol/testing/vol8	Ready for agentless import	1.0 GB
<input type="checkbox"/> Volume	/vol/testing/vol7	Ready for agentless import	1.0 GB
<input type="checkbox"/> Volume	/vol/fc_lun2_vol/vol6	Ready for agentless import	9.0 GB
<input type="checkbox"/> Volume	/vol/testing/vol5	Ready for agentless import	1.0 GB
<input type="checkbox"/> Volume	/vol/fc_lun1_vol/vol4	Ready for agentless import	11.0 GB
<input type="checkbox"/> Volume	/vol/testing/vol3	Volume size is not a multiple of 8192	2.0 GB
<input type="checkbox"/> Volume	/vol/temp_vol/vol2	Undetermined	1.0 GB
<input type="checkbox"/> Volume	/vol/testing/vol1	Volume size is not a multiple of 8192	2.0 GB

Cancel Back Next

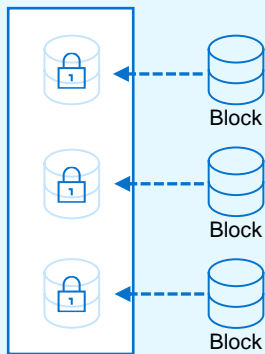
- Driven from PowerStore Manager
- Completely agent-less
- Scalability identical to Destination PowerStore
- Intuitive, consistent workflow and alerting
- FC and iSCSI support



DELL Technologies

Secure and immutable snapshots

New security option for volume and volume group snapshots

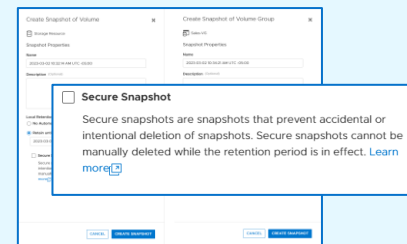


CANNOT be modified
or deleted prior to
expiration date – *even
by an administrator*



Virtual Vault protection against...

- Ransomware attacks
- Accidental or malicious deletion by admin
- Point in time overwrites
- Prevents deletions even when out of capacity

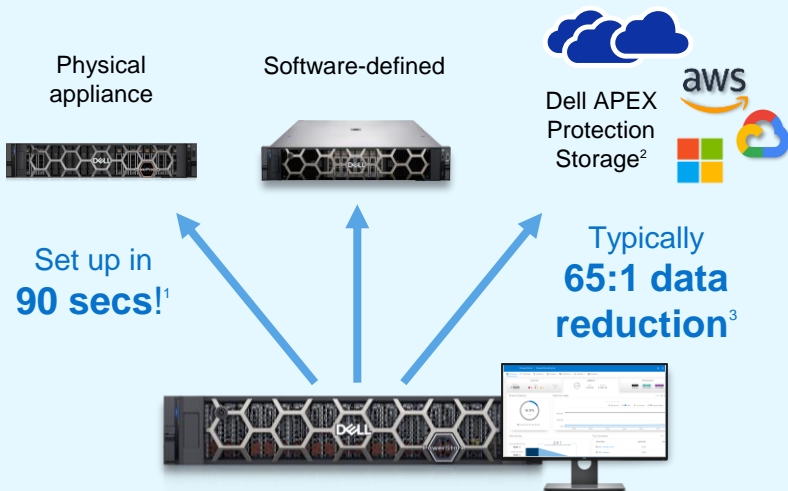


Easy to manage

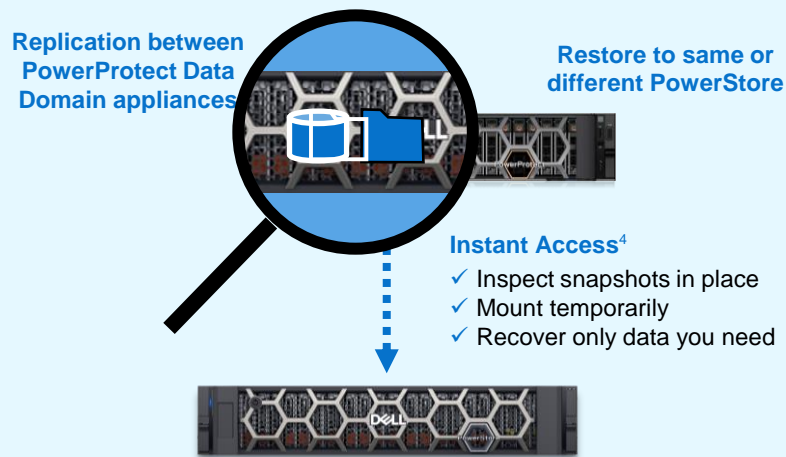
- Schedule / automate by policy
- PowerStore Manager, CLI, REST API
- Changes only affect future creation -- previously locked snaps **stay** locked

Control backups directly from PowerStore Manager

Any PowerProtect Data Domain target



Easy, granular data recovery



Native PowerProtect Data Domain integration empowers data owners with self-service backup and recovery

¹ – Based on Dell analysis, March 2023. ² – Qualified with AWS, Azure and Google Cloud qual pending.

³ – Logical capacity based on up to 50x deduplication (DD3300) and typically deduplication (DD6400, DD6900, DD9400, DD9900) based on additional hardware-assisted data compression of typically 30% more logical capacity per TB.

⁴ – Instant Access is not currently supported for VMFS datastores. VMFS support planned for 2H 2023. In current release VMFS datastores can still perform retrieves using PowerStore Manager.

PowerProtect DD series

The next generation of Data Domain



Fast,
efficient, and
easy to use

Industry-leading
multi-cloud
protection

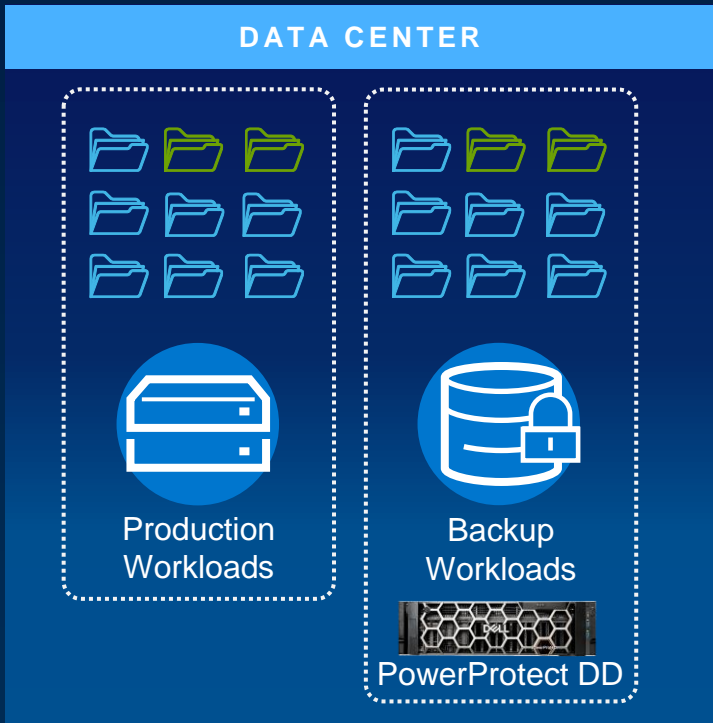
Broad eco-
system support
of backup
software and
applications

Reliable and
secure



PowerProtect DD Series

The Foundation for Data Protection



Avamar – Networker – Data Manager
Data Protection Advisor – DD Series

Retention Lock Compliance (Immutability)

SEC 17a-4f Compliance

Role Based Access

End to End Encryption

Dual Role Authorization

Multi-Factor Authentication

Secure System Clock

NTP Clock Tamper Controls

Key Management

Custom System DDOS

DD File System Hardened

DDBoost

Integrated Lights Out Mgt Hardening (iDRAC)

Data Invulnerability Architect (DIA)

Secure AD/LDAP Authentication

Secure Remote support

Anomaly Reporting with DPA



Dell Technologies

Unified Protection Storage

- **Multiple Applications and Protocols Supported**

NFS, CIFS, VTL, DDBoost, BoostFS

- **Multiple vendor support**

Large application ecosystem

- **Global deduplication**

Highest data reduction rates

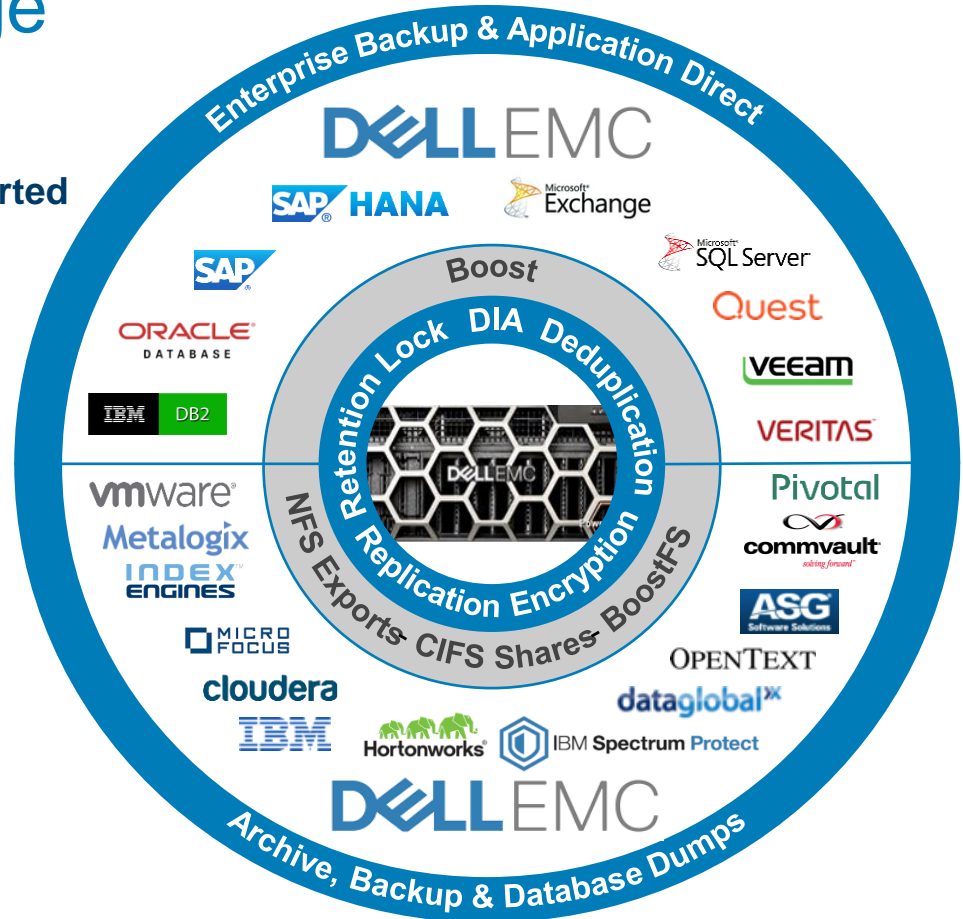
- **Built-in Data Verification and Protection**

Data Invulnerability Architecture

- **Single platform for backup and archive**

- **Investment Protection**

Clear price, hardware upgrades

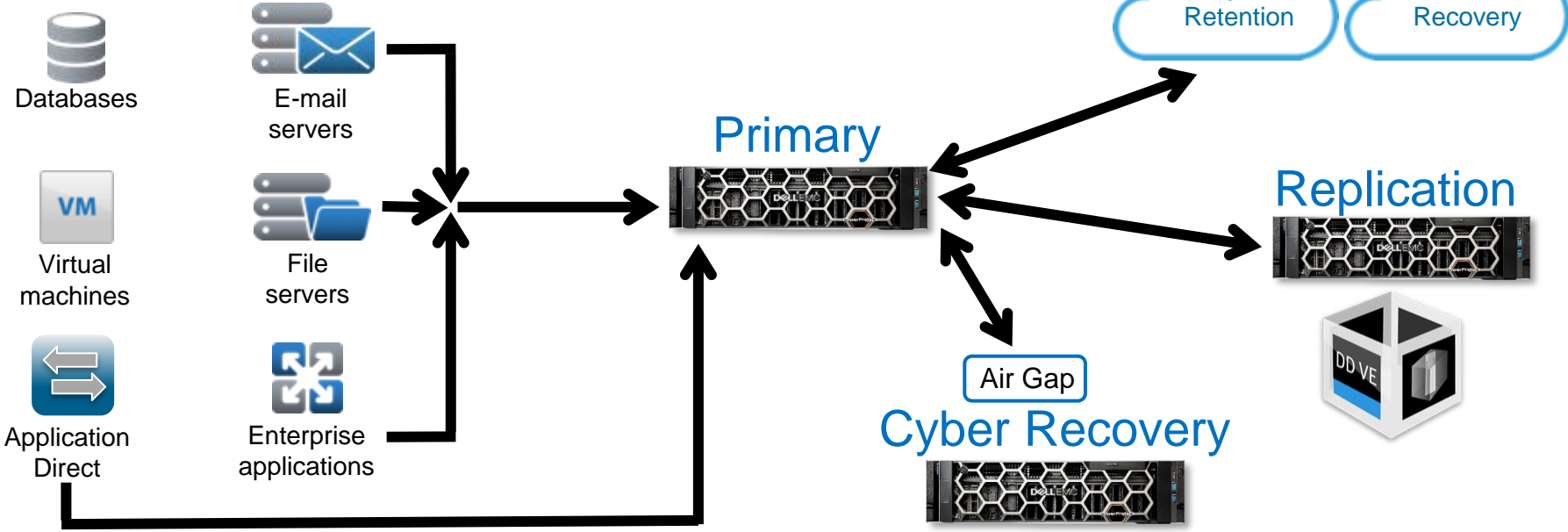


Key use cases

Backup, Archive, Copy Reuse

- Up to 65x average data reduction rate
- Inflight encryption
- Broad application ecosystem

Cloud-enabled



Evolution of Cyber Threat Actors

Motivations, Techniques and Goals



Crime

Theft & extortion for financial gain



Insider

Trusted insiders steal or extort for personal, financial, & ideological reasons. Increasingly targeted because of privileged access to systems



Espionage

Corporate or Nation-state actors steal valuable data



Hacktivism

Advance political or social causes



Terrorism

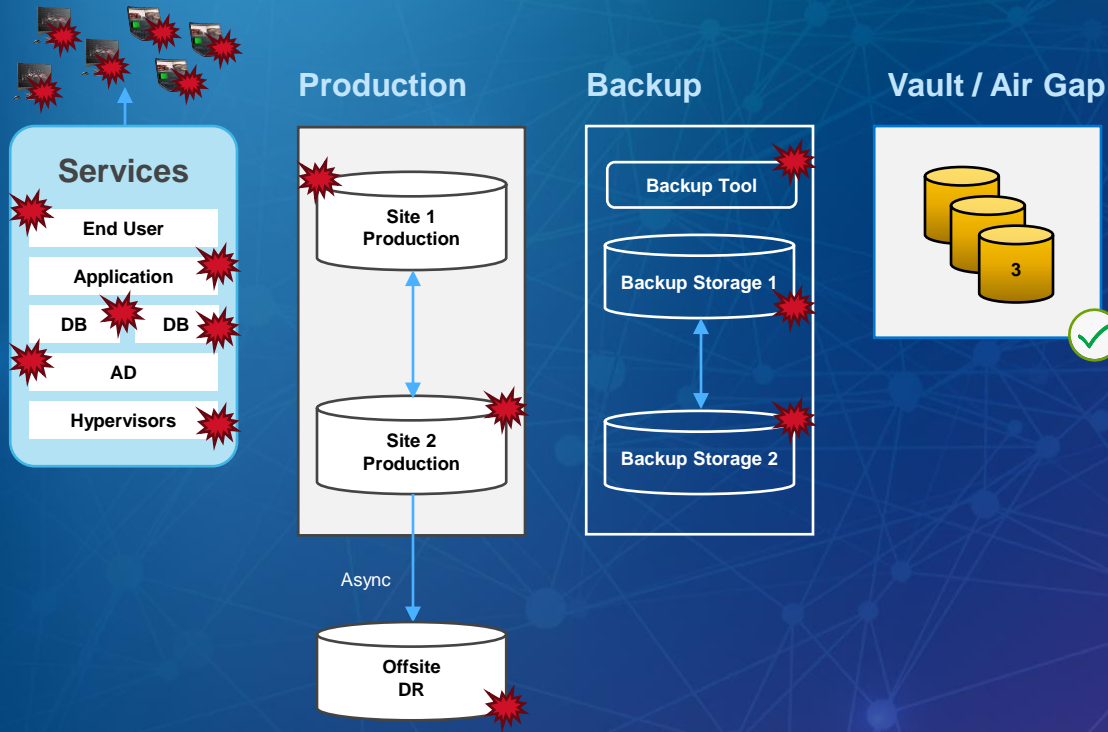
Sabotage & destruction to instill fear



Warfare

Nation-state actors with destructive cyber weapons (NotPetya)

Malware/Data Destruction/Insider Threats



Isolated **copies** of protected Data

A cyber resilience strategy

A high-level holistic strategy example: “NIST Cybersecurity Framework”
(National Institute of Standards and Technology)



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

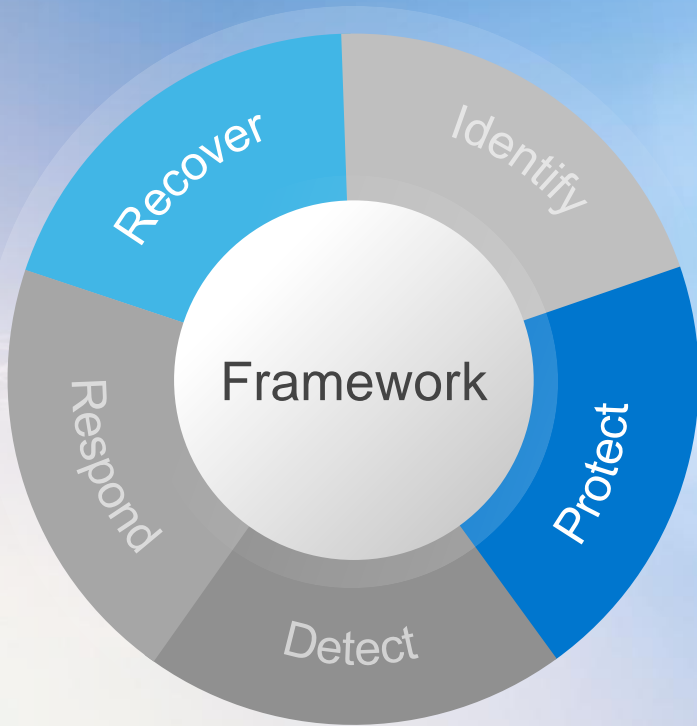
Recover from
the attack

Before

During

After

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.

PowerProtect Cyber Recovery Advantages

Modern protection for critical data and an enabler of Security Transformation



Isolation

Physical & logical separation of data

PowerProtect Cyber Recovery vault is protected with operational air gap either on-premises or in cloud and multi-cloud offers



Immutability

Preserve original integrity of data

Multiple layers of security and controls protect against destruction, deletion and alteration of vaulted data



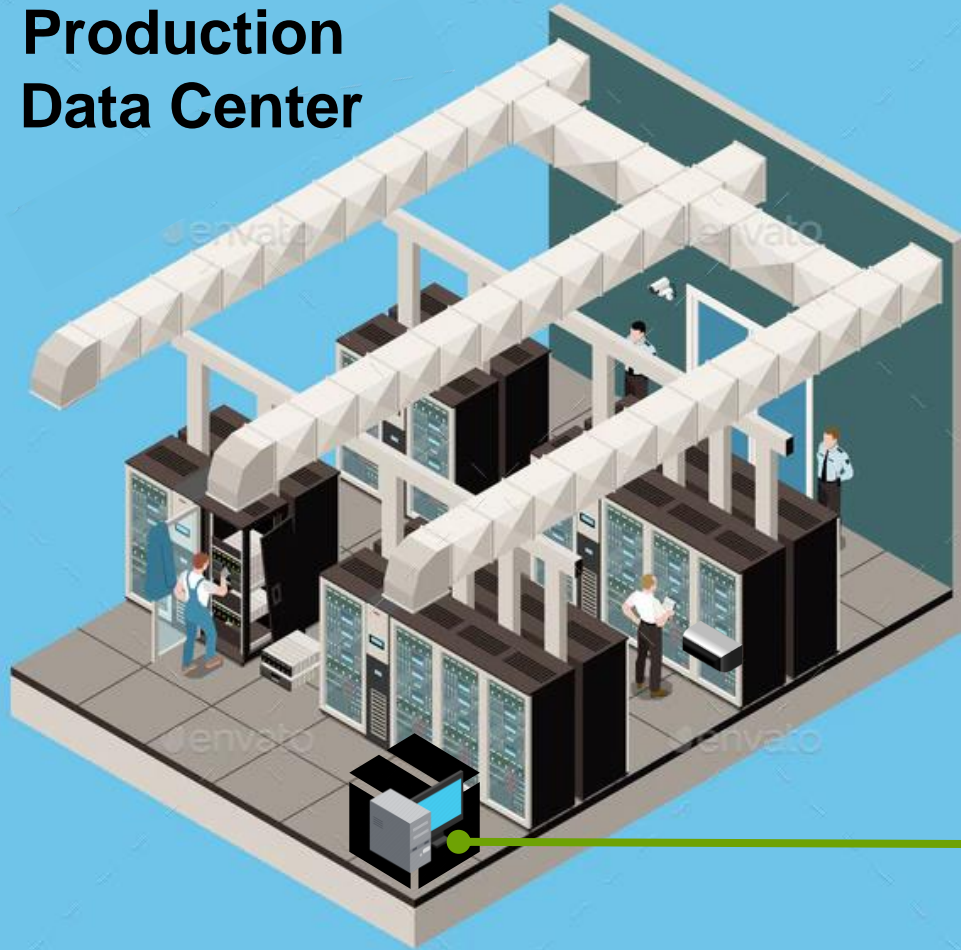
Intelligence

ML & analytics identify threats

CyberSense enables assured recovery of good data and offers insight into attack vectors from within the Cyber Recovery vault



Production Data Center



Cyber Recovery Solution

The Gold Standard for Cyber Resiliency



Cyber Recovery Application

Cyber Recovery Server

PowerProtect DD

Firewall/Data Diode

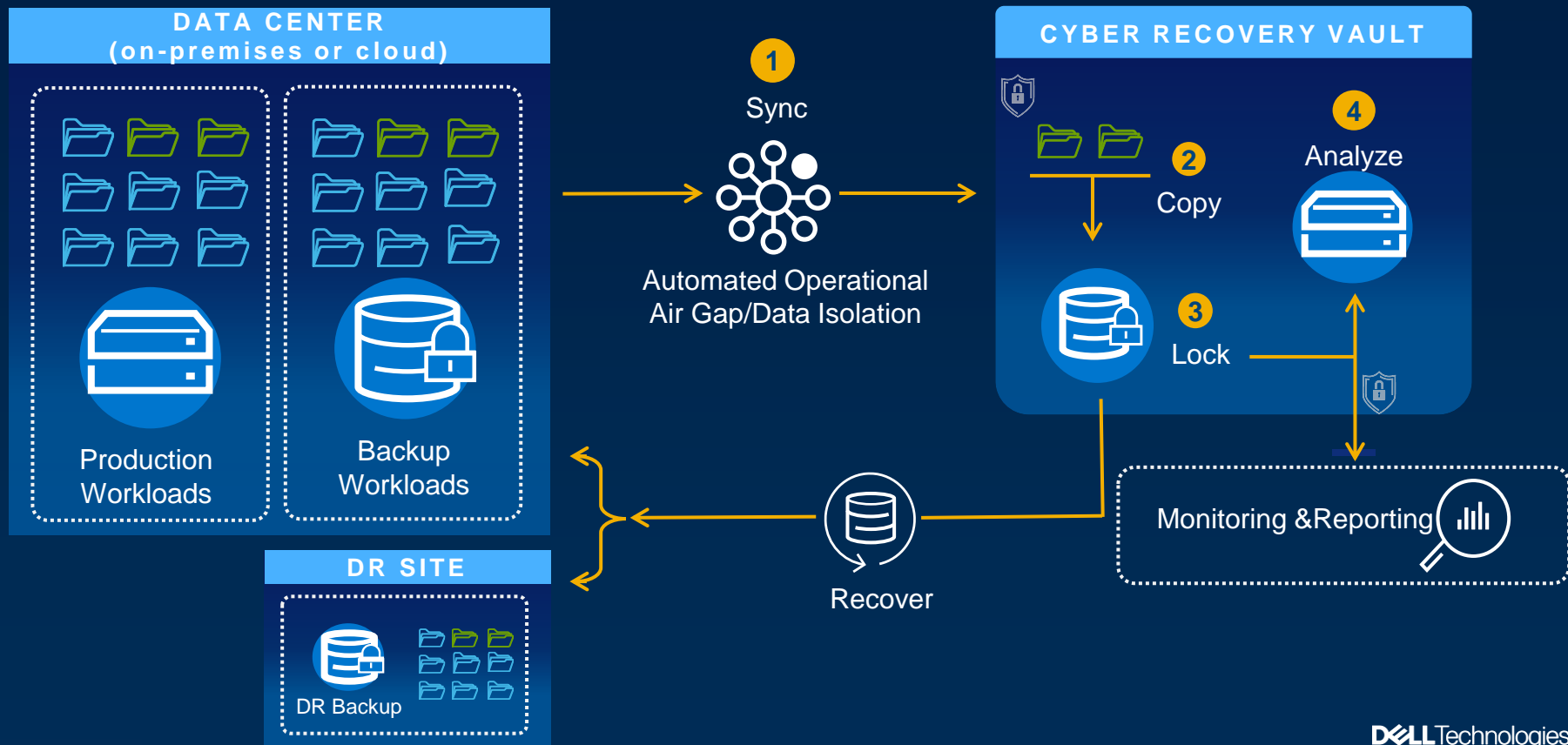
Switch

Cyber Sense

Management Server

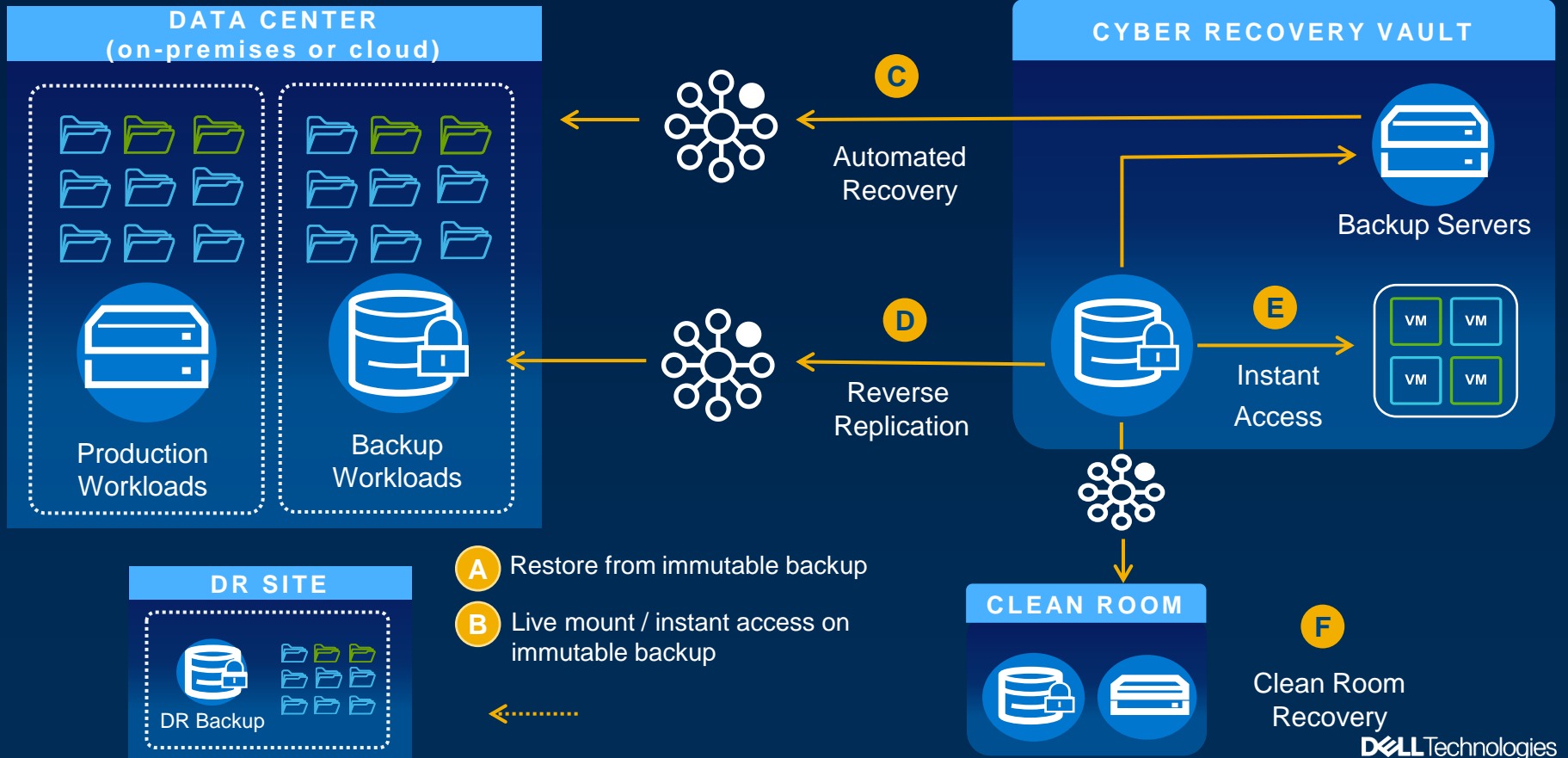
Dell PowerProtect Cyber Recovery

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



Recovery Options To Meet Your Cyber Resilience SLAs

Flexible Recovery options



How CyberSense Works

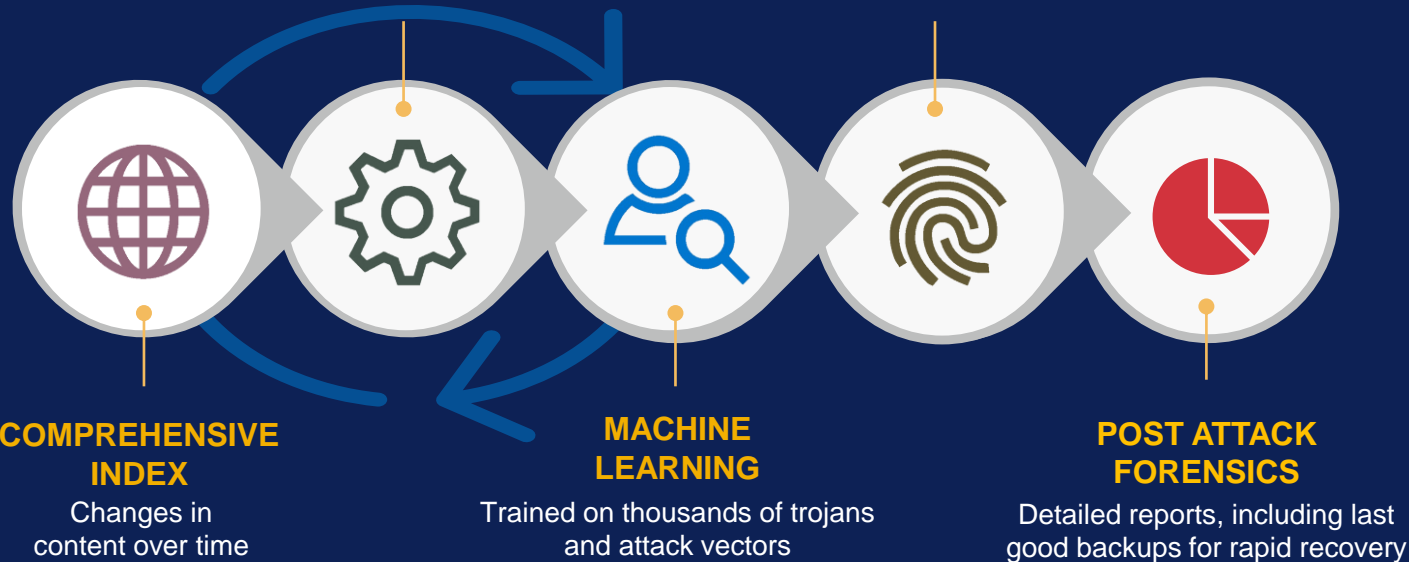
Analytics, Machine Learning and Forensic Tools to Detect & Recover from Cyber Attacks

SECURITY ANALYTICS

200+ statistics indicative of cyber attack

CORRUPTION DETECTED

Alert when suspicious activity is detected



CyberSense Provides

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

Why Cyber Recovery is best



Good...

- Integrated Lock
SEC 17a-4(f) Compliant
- WORM Immutable
- Elevated Security Credentials



Best

- Automated, Vaulted Air Gap
- Full Context Indexing
with AI / ML Analytics
- Endorsed by Sheltered Harbor
- Enhanced Recovery Tools



Better...

- Protection From Insiders
- Multi Backup SW-Vendor
Support

Dell Data Protection Guarantees for Cyber Bunker

Increase confidence in data recoverability, optimize storage efficiency and lower costs



Up to \$10M to assist in recovery of your data from ransomware and qualifying cyber events.¹

Guaranteed Recovery & Optimization



Achieve a guaranteed deduplication ratio or we'll make it right.²

Dell Technologies Future-Proof Program



5 PILLARS OF CYBER HYGIENE



LEAST
PRIVILEGE



MICRO
SEGMENTATION



TARGETED
ENCRYPTION



MULTI FACTOR
AUTHENTICATION



AUTOMATION OF
LIFECYCLE MANAGEMENT

DELLTechnologies