PowerProtect Cyber Recovery: Building Cyber Resilience

Fortify your organization against destructive cyberattacks leveraging Dell PowerProtect Cyber Recovery to recover the lifeline of your business

Aurimas Pažėra

Advisory Systems Engineer,
ISG Technology Consulting
Dell Technologies

DELL Technologies

Agenda

1. The challenges
2. Why Immutable does not mean Invulnerable
3. Data isolation and analysis

Cyber threats 2021: the facts

Every 11 seconds

A cyber or ransomware attacks occur[1]

$6T

Total global impact of cyber crime in 2021[2]

$13M

Average cost of cybercrime for an organization[3]

Banking	$18.4M
Utilities	$17.8M
Software	$16.0M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

*[1] Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

[2] Cybersecurity Ventures: *https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021*

[3] Accenture Insights, Ninth Annual Cost of Cyber crime Study March , 2019 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

DELL Technologies

Cyber Resiliency Challenges Today

Ransomware may now be a customer's biggest threat!

- Customers are faced with an uphill battle in the current landscape
- Ransomware switching from consumer campaigns to businesses
- Cyber Criminal attacks are now heavily focused on backups

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

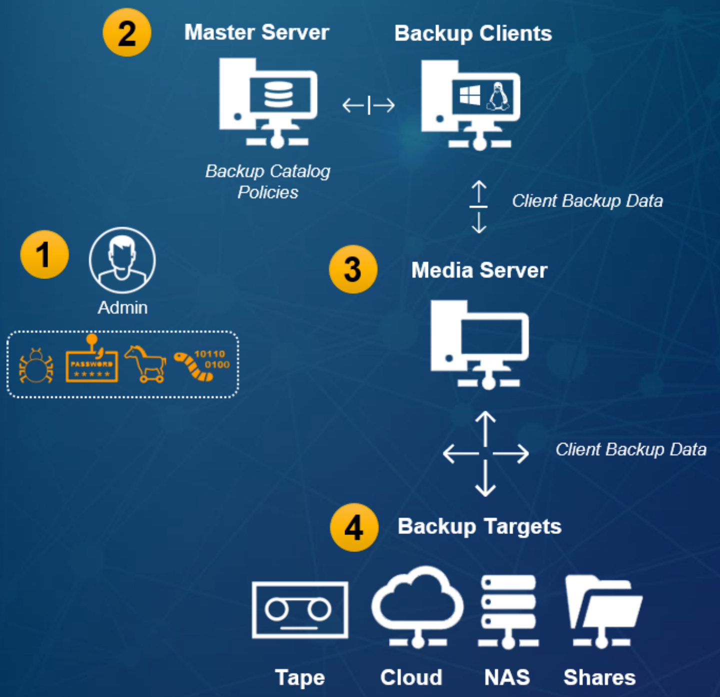
Terrorism

Sabotage & destruction to instill fear

Warfare

Nation-state actors with destructive cyber weapons (NotPetya)

Ransomware Targeting Backups



1 **IT and Backup admins are main targets for compromise**

2 **Master Server (Backup Catalog):** Backup master server is targeted and infected resulting in encrypted/wiped backup catalog, or pre-mature policy expiration

3 **Media Server:** All mounted filesystems on the media server are targeted and encrypted/wiped

4 **Backup Targets:**

Disk / NAS: Filesystems on the media server are targeted and encrypted/wiped. Backup repositories can become encrypted/wiped from ransomware crawling network file shares

Tape: Provides a better chance to recover from the destructive event if threat was removed from the environment prior to attack. However, if backup catalog is held hostage or destroyed, recovering from the tape will be increasingly difficult

Cloud: General-purpose or Public Cloud offer the advantage of remote protection but are inherently less secure due to reliance on internet (always on) or unsecure networks, leaving data, backups and catalogs exposed

Immutability ≠ Invulnerable

Immutability is part of any good Cyber Resilience Strategy…However

Where and how Immutability is implemented by vendor is different

Immutability is used differently by vendors and varies in implementation and effectiveness. Therefore, it's important to understand what each vendor means by "immutable" and how its functionality is implemented to assess the risk that hackers can override it.

- Gartner

Immutability

System Factory Reset

Clock based attack

IMMUTABILITY Alone is not enough

Depending on where and how Immutability is implemented it can be disrupted

System Override

Snap Corruption

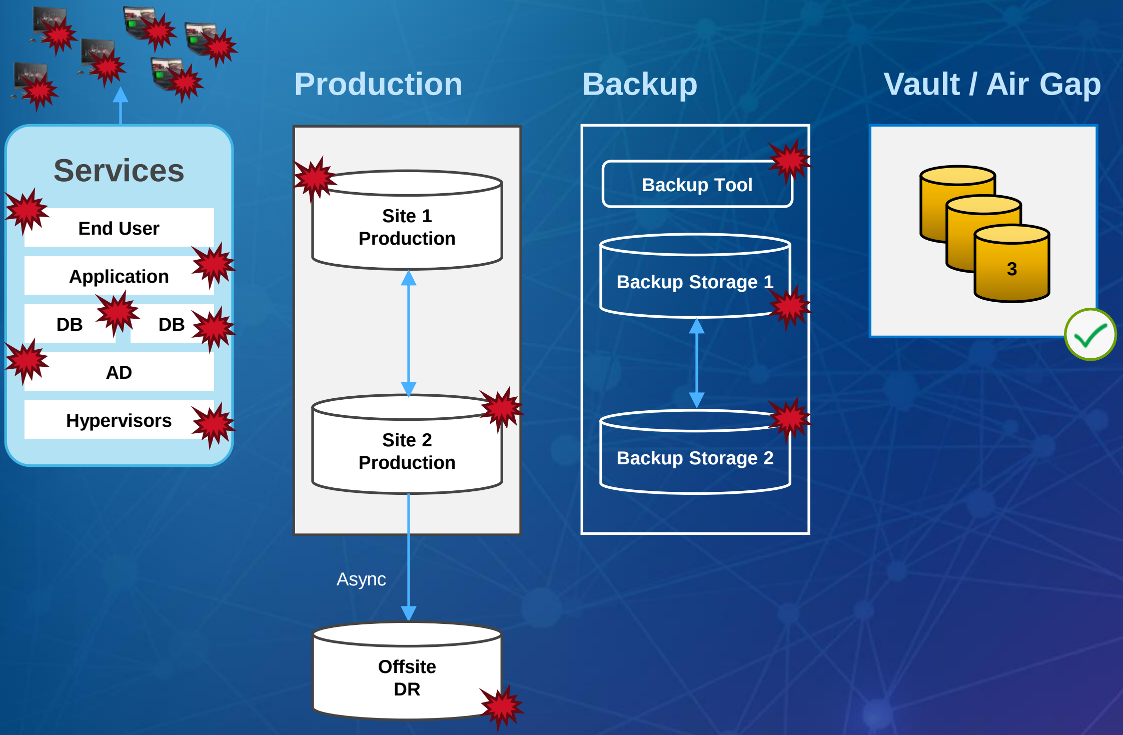
Physical Access

Boot Lock

Kernel Access

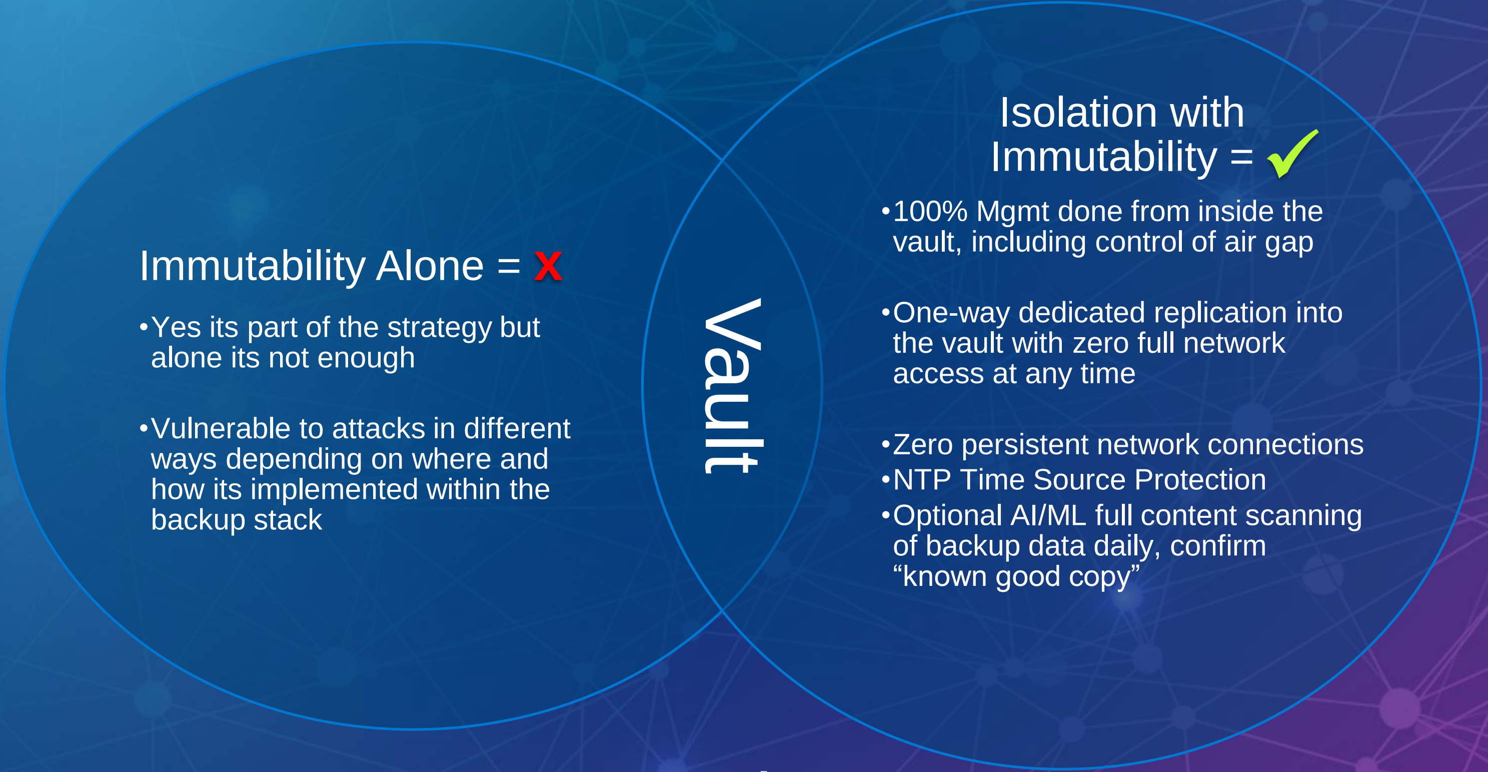
Firmware Corruption

Malware/Data Destruction/Insider Threats



Isolated **copies** of protected Data

Why you need a Vault?



Immutability Alone = X

- Yes its part of the strategy but alone its not enough
- Vulnerable to attacks in different ways depending on where and how its implemented within the backup stack

Vault

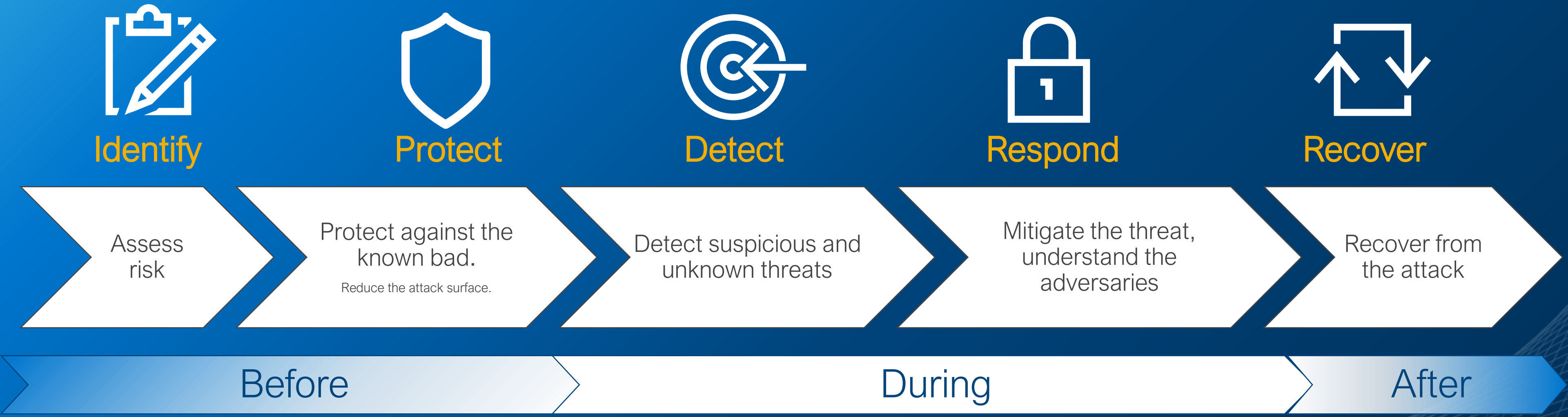
Isolation with Immutability = ✓

- 100% Mgmt done from inside the vault, including control of air gap
- One-way dedicated replication into the vault with zero full network access at any time
- Zero persistent network connections
- NTP Time Source Protection
- Optional AI/ML full content scanning of backup data daily, confirm “known good copy”

PowerProtect Cyber Recovery

A cyber resilience strategy

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



Identify

Assess risk

Protect

Protect against the known bad.

Reduce the attack surface.

Detect

Detect suspicious and unknown threats

Respond

Mitigate the threat, understand the adversaries

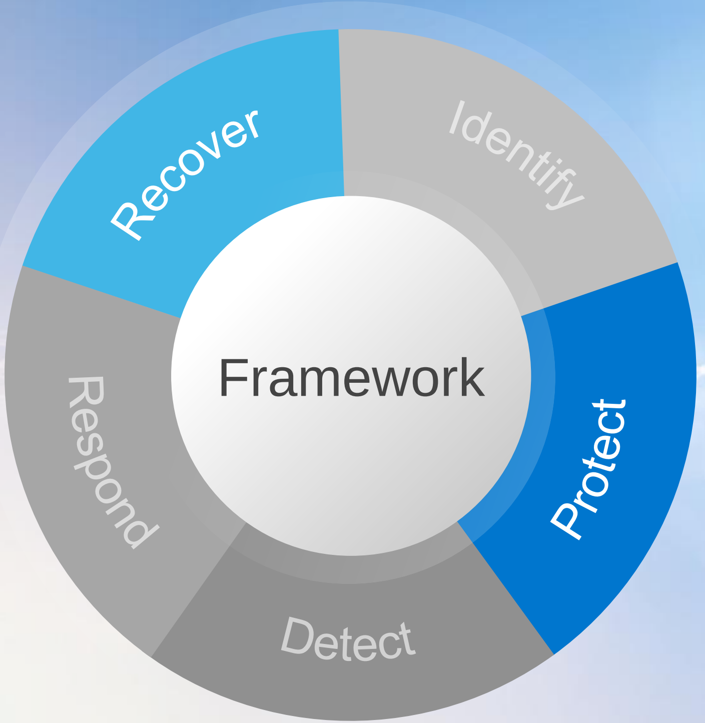
Recover

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.

Source: https://en.wikipedia.org/wiki/Cyber_resilience

DELL Technologies

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

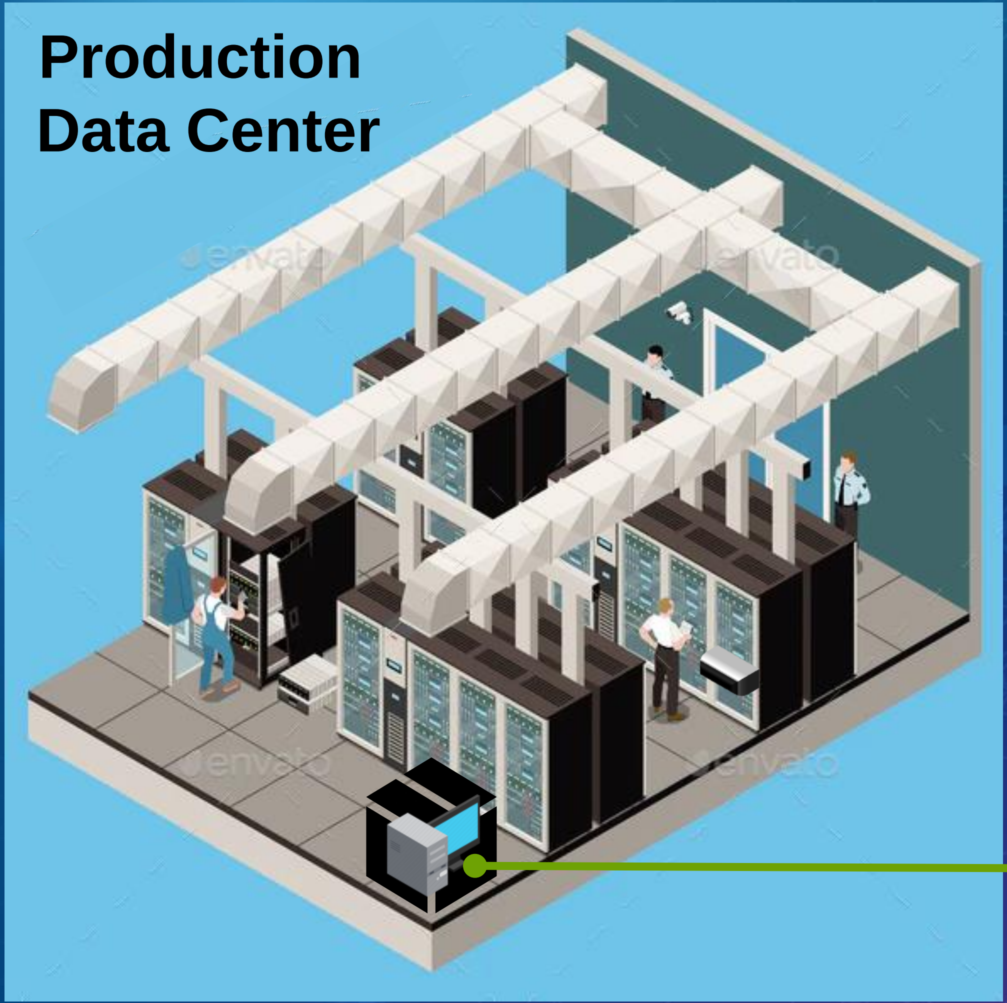
CyberSense enables assured recovery of good data and offers insight into attack vectors from within the Cyber Recovery vault

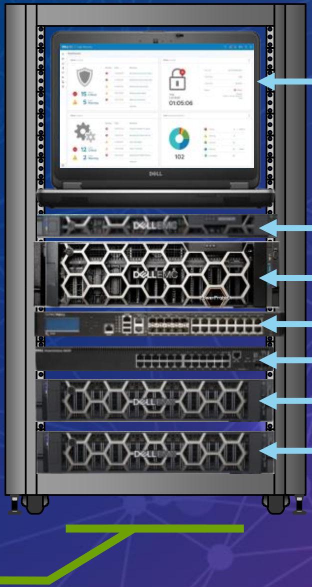
DELL Technologies

Cyber Recovery Solution

The Gold Standard for Cyber Resiliency

Production Data Center




Cyber Recovery Application

Cyber Recovery Server

PowerProtect DD

Firewall/Data Diode

Switch

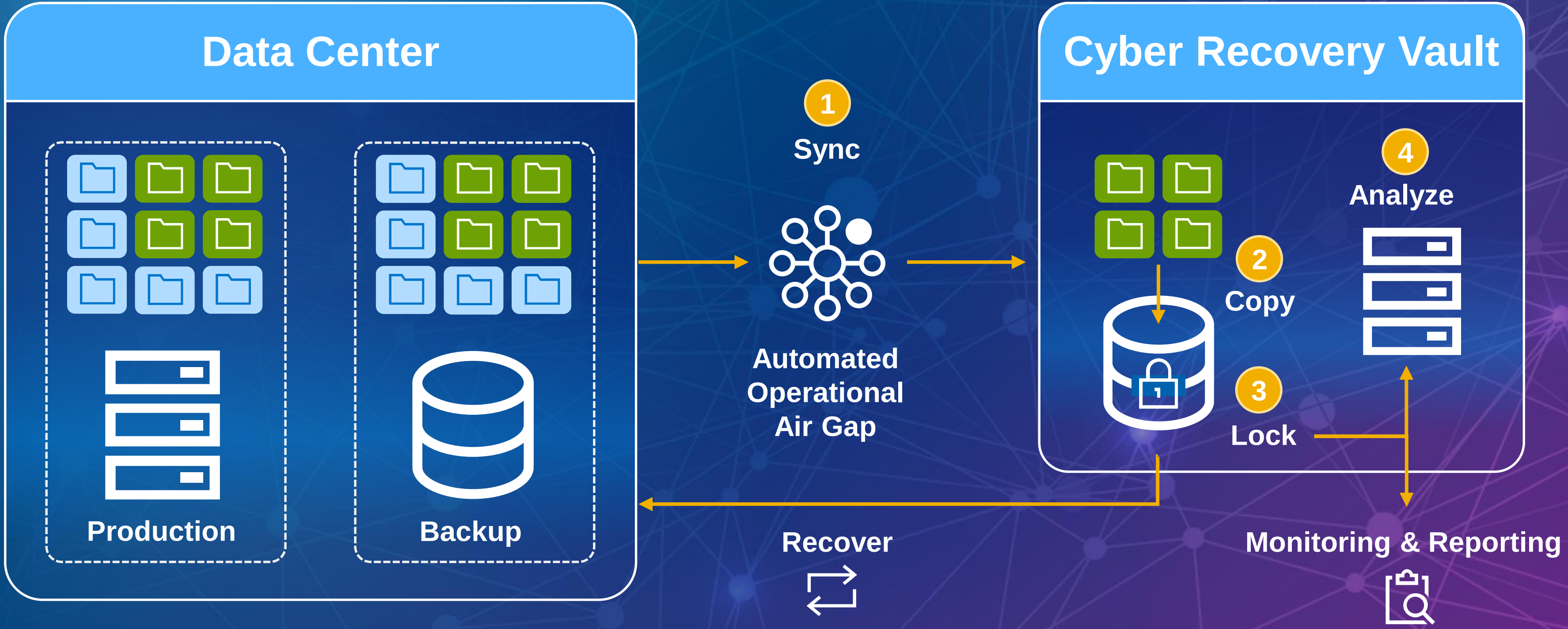
Cyber Sense

Management Server

Data Protection and Vaulting Process

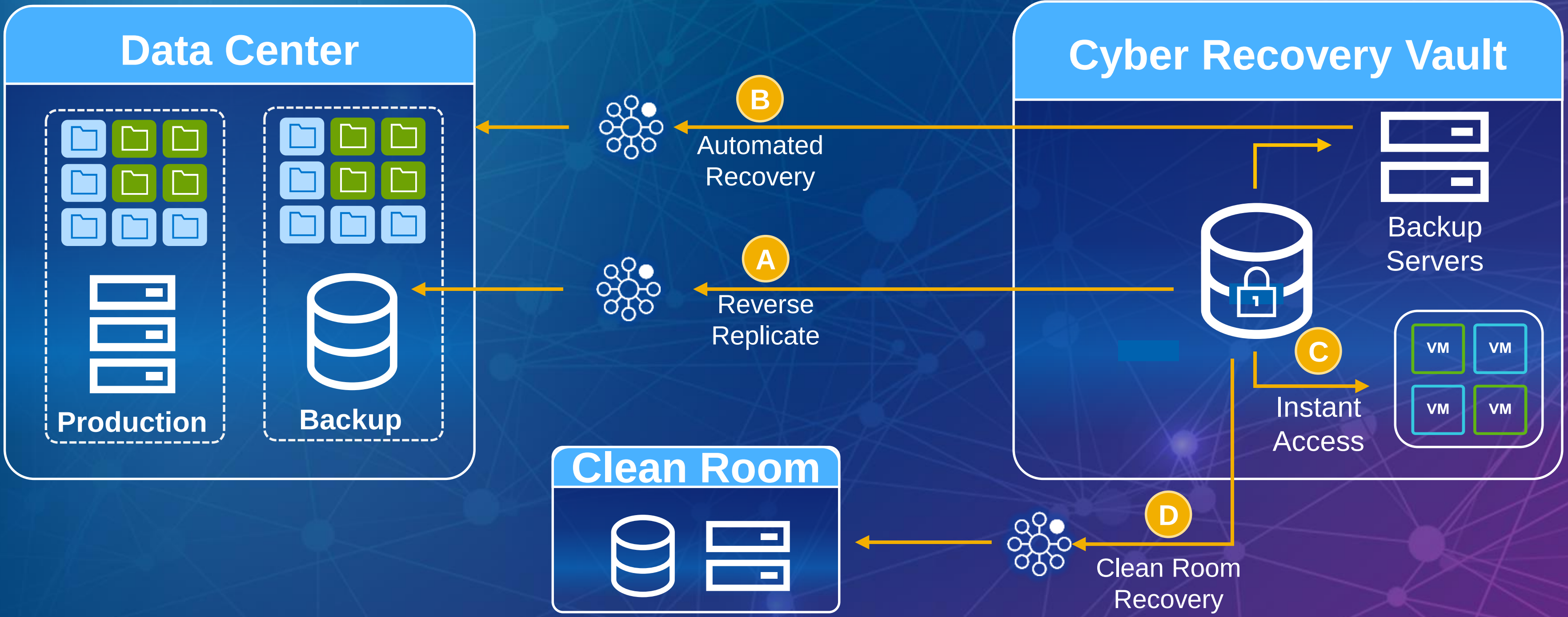
PowerProtect Cyber Recovery

Data Vaulting and Recovery Processes



PowerProtect Cyber Recovery

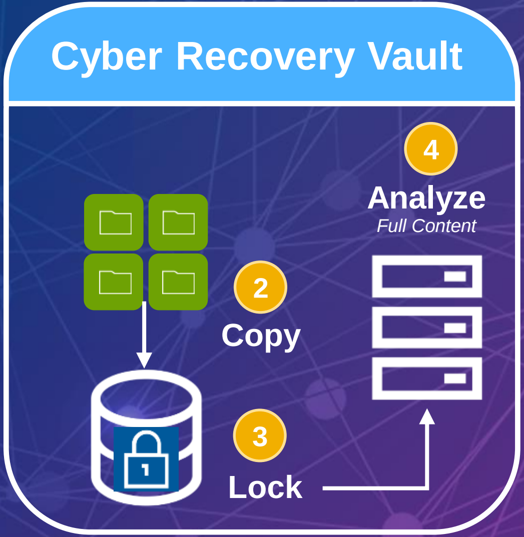
Flexible Recovery Options



DELLTechnologies

The Cyber Recovery Vault – Summary

- Vault is segmented off of the Production Network
- Air Gap is the protected, hardened *“single point of Entry”*
- Everything is managed from within the Vault with CR Software
- Firewall for *“single point of Exit”* for messaging (e.g. Alerts/Alarms)

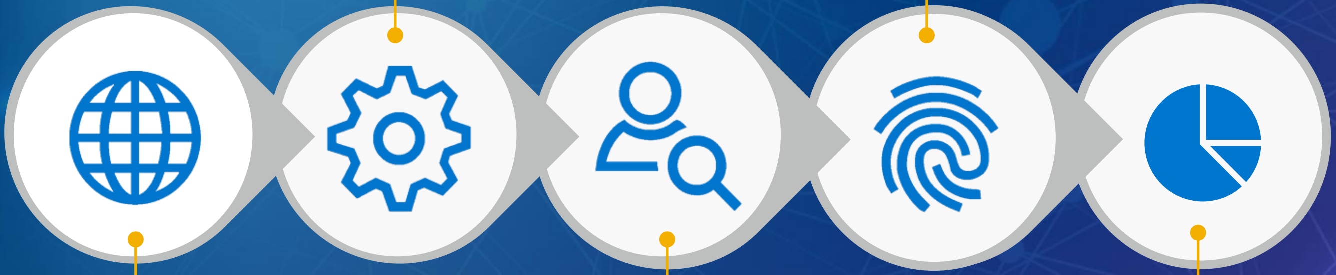


DELL Technologies

CyberSense

How CyberSense Works

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



SECURITY ANALYTICS
100+ 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

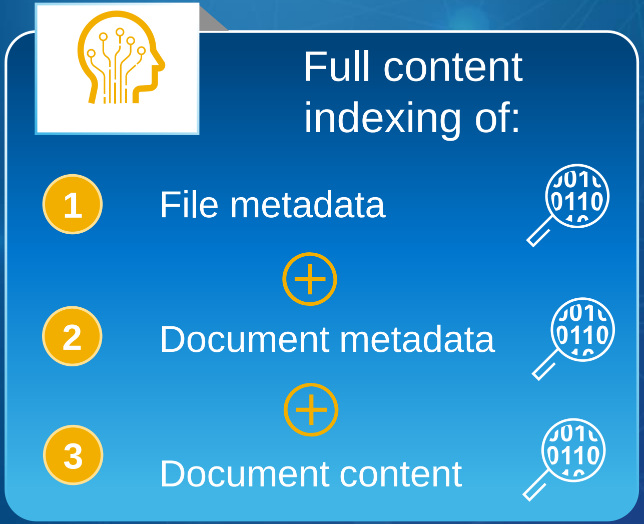
CyberSense Provides

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

Compare: CyberSense vs. “Basic” Analytics

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

CyberSense:



Full content indexing of:

1 File metadata

⊕

2 Document metadata

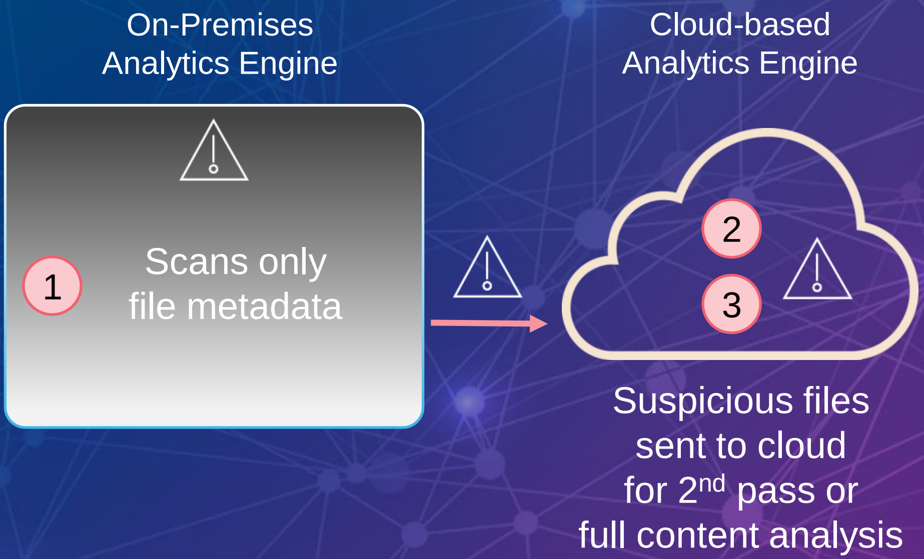
⊕

3 Document content

- Data not sent to cloud for analysis

VS.

Basic Analytics:



On-Premises Analytics Engine

1 Scans only file metadata

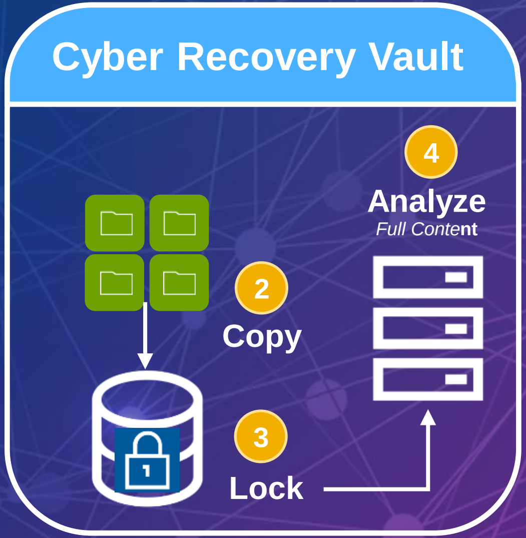
Cloud-based Analytics Engine

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

Cyber Recovery Analytics – Summary

Analyzing and Validating Backup Files in the Vault

- CyberSense is Integrated with the Cyber Recovery Application
- Scans for changes in data not typical of user behavior
- Analytics looks for signs of a Cyber Attack
  - Corruption/Encryption/Mass Deletion
- Full content analytics vs metadata only

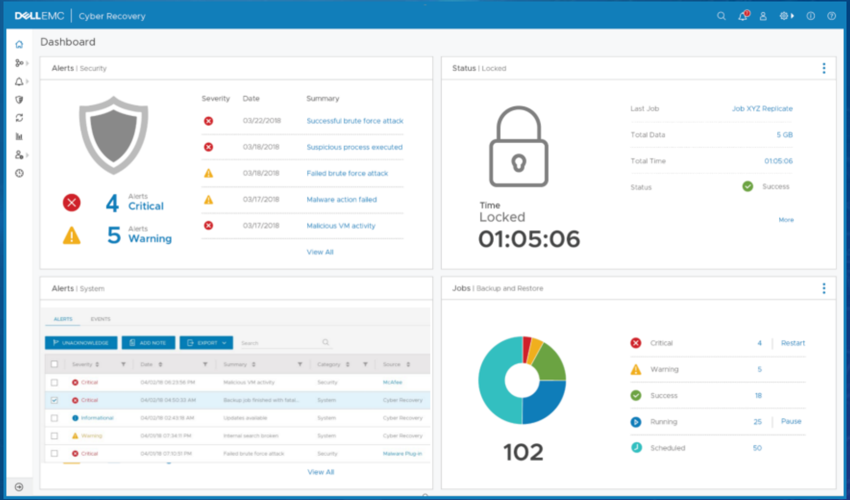


DELL Technologies

CyberSense UI & Alerting

Machine Learning Enables Early Detection & Rapid Recovery from a Cyber Attack

Dell EMC Cyber Recovery w/ CyberSense



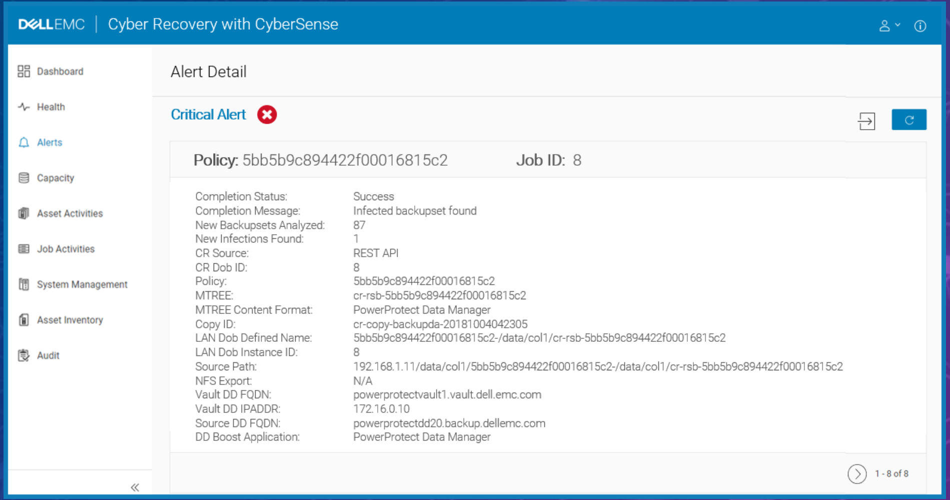
Severity	Date	Summary
☒	03/22/2018	Successful brute force attack
☒	03/18/2018	Suspicious process executed
⚠	03/18/2018	Failed brute force attack
⚠	03/17/2018	Malware action failed
☒	03/17/2018	Malicious VM activity

Last Job	Job XYZ Replicate
Total Data	5 GB
Total Time	01:05:06
Status	✓ Success

	Severity	Date	Summary	Category	Source
□	Critical	04/02/18 06:23:56 PM	Malicious VM activity	Security	McAfee
☑	Critical	04/02/18 04:50:33 AM	Backup job finished with fatal...	System	Cyber Recovery
□	Informational	04/02/18 02:43:18 AM	Updates available	System	Cyber Recovery
□	Warning	04/01/18 07:34:11 PM	Internal search broken	System	Cyber Recovery
□	Critical	04/01/18 07:10:51 PM	Failed brute force attack	Security	Malware Plug-in

Critical	4	Restart
Warning	5	
Success	18	
Running	25	Pause
Scheduled	50	

CyberSense Alert Example



Alert Detail

Critical Alert

Policy: 5bb5b9c894422f00016815c2 Job ID: 8

Completion Status:	Success
Completion Message:	Infected backupset found
New Backupsets Analyzed:	87
New Infections Found:	1
CR Source:	REST API
CR Dob ID:	8
Policy:	5bb5b9c894422f00016815c2
MTREE:	cr-rsb-5bb5b9c894422f00016815c2
MTREE Content Format:	PowerProtect Data Manager
Copy ID:	cr-copy-backupda-20181004042305
LAN Dob Defined Name:	5bb5b9c894422f00016815c2-/data/col1/cr-rsb-5bb5b9c894422f00016815c2
LAN Dob Instance ID:	8
Source Path:	192.168.1.11/data/col1/5bb5b9c894422f00016815c2-/data/col1/cr-rsb-5bb5b9c894422f00016815c2
NFS Export:	N/A
Vault DD FQDN:	powerprotectvault1.vault.dell.emc.com
Vault DD IPADDR:	172.16.0.10
Source DD FQDN:	powerprotectdd20.backup.dellemc.com
DD Boost Application:	PowerProtect Data Manager

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 Technologies

Cyber Recovery & data protection leadership

2015	First “Isolated” recovery solution with custom deployment
2018	Introduced PowerProtect Cyber Recovery solution
2019	First technology vendor in Sheltered Harbor Alliance Partner Program
2020	First Endorsed Sheltered Harbor Solution – PowerProtect Cyber Recovery
2021	Introduced Cyber Recovery with Multi-Cloud Data Services for Dell PowerProtect
2021	Introduced PowerProtect Cyber Recovery for AWS
2022	Introduced PowerProtect Cyber Recovery for Azure
2022	Introduced PowerProtect Cyber Recovery for Google Cloud

1300+ Cyber Recovery Customers[1]

#1

Data Protection Appliances & Software[2]

[1] Based on Dell Technologies analysis, October 2022

[2] Based on combined revenue from the IDC 2Q22 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 2Q22 Storage Software and Cloud Services Tracker

Q&A

Disaster Recovery is not Cyber Recovery

Disaster Recovery / Business Continuity is not enough to address modern cyber threats

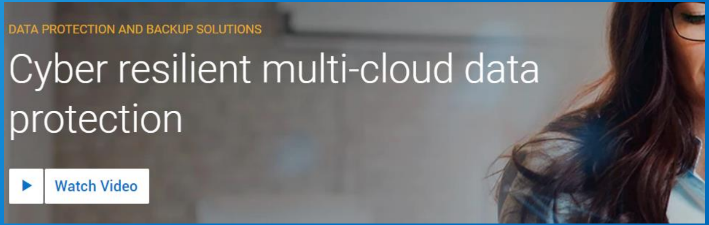
CATEGORY	DISASTER RECOVERY	CYBER RECOVERY
Recovery Time	Close to instant	Reliable & fast
Recovery Point	Ideally continuous	1 day average
Nature of Disaster	Flood, power outage, weather	Cyber attack, targeted
Impact of Disaster	Regional; typically contained	Global; spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR
Data Volume	Comprehensive, all data	Selective, includes foundational services
Recovery	Standard DR (e.g., failback)	Iterative, selective recovery; part of CR

Learn More

Dell PowerProtect Cyber Recovery

Intel® Innovation Built-in intel.

delltechnologies.com/cyberrecovery

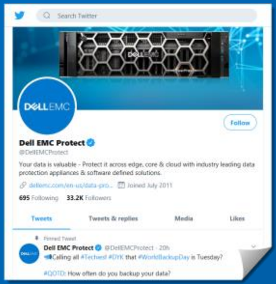


DATA PROTECTION AND BACKUP SOLUTIONS

Cyber resilient multi-cloud data protection

▶ Watch Video

delltechnologies.com/dataprotection



Search Twitter

Dell EMC Protect
@DellEMCProtect

Your data is valuable - Protect it across edge, core & cloud with industry leading data protection appliances & software defined solutions.

dellemc.com/en-us/data-pro... Joined July 2011

695 Following 33.2K Followers

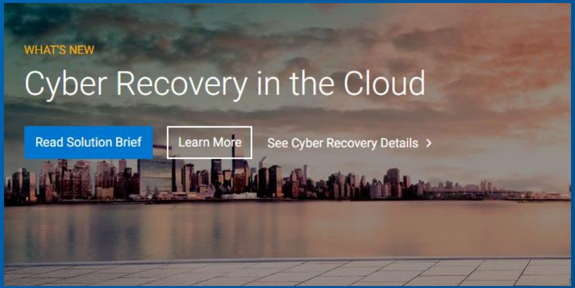
Tweets | Tweets & replies | Media | Likes

Pinned Tweet

Dell EMC Protect @DellEMCProtect · 20h
Calling all #Techies! #DYK that #WorldBackupDay is Tuesday?

#QOTD: How often do you backup your data?

@DellProtect



WHAT'S NEW

Cyber Recovery in the Cloud

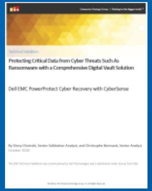
Read Solution Brief | Learn More | See Cyber Recovery Details >

delltechnologies.com/cloudprotection

Managing Cyber Risk As A Business Issue

Business Cyber Risk Bulletin

Case Study: Founder’s Federal Credit Union



Technical Validation

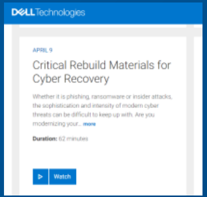
Protecting Critical Data from Cyber Threats Such As Ransomware with a Comprehensive Digital Vault Solution

Dell EMC PowerProtect Cyber Recovery with CyberSense

By Vinny Choinski, Senior Validation Analyst; and Christophe Bertrand, Senior Analyst
October 2020

ESG Analyst Validation: Cyber Recovery & CyberSense

ESG Analyst Video Cyber Recovery & CyberSense



DELL Technologies

APRIL 9

Critical Rebuild Materials for Cyber Recovery

Whether it is phishing, ransomware or insider attacks, the sophistication and intensity of modern cyber threats can be difficult to keep up with. Are you modernizing your... more

Duration: 62 minutes

▷ Watch

dellemc.com/webinars

DELL Technologies

DELL Technologies