Cyber Recovery

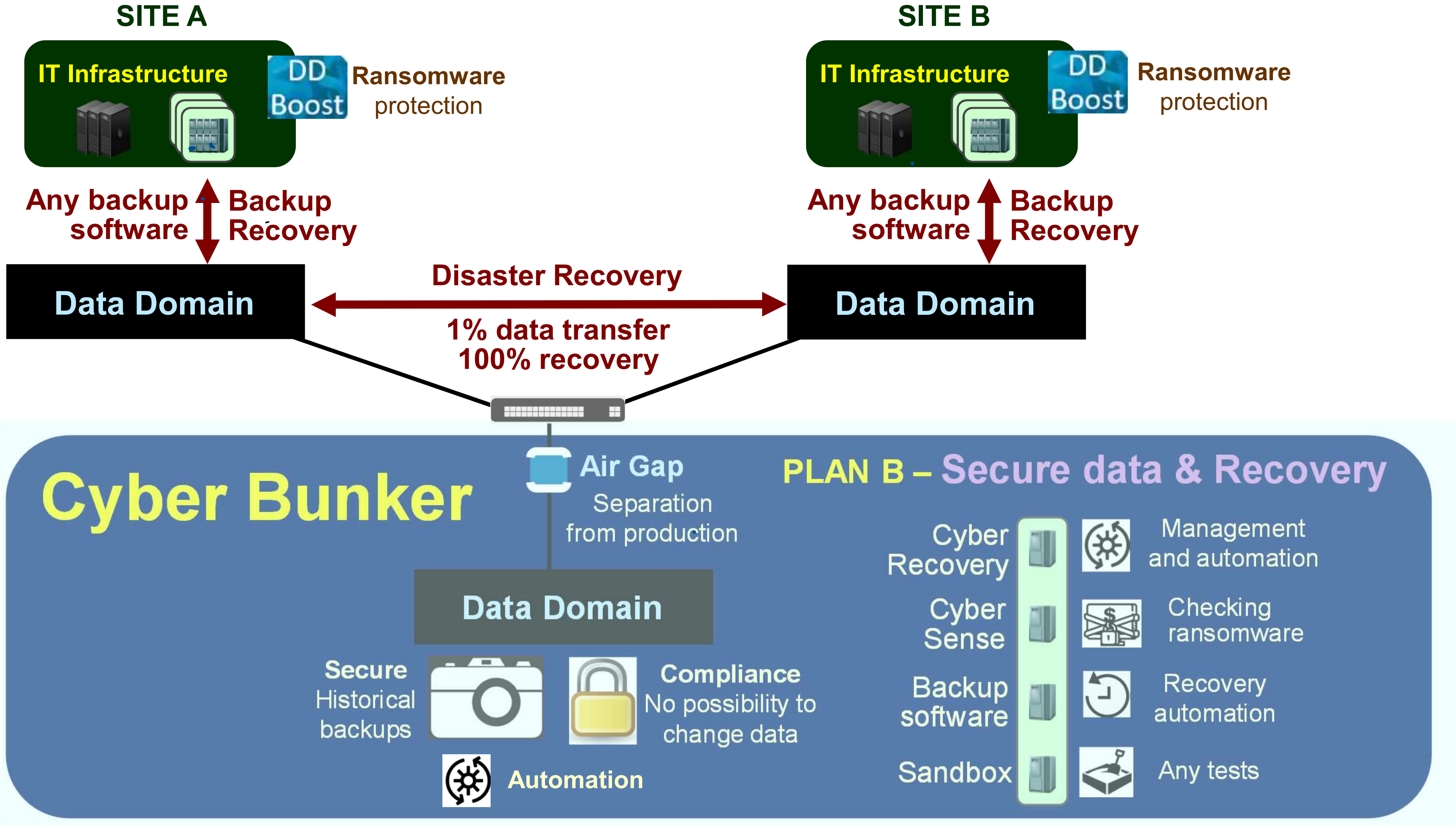
*It is always worth to have trusted **PLAN B***

DELL EMC

Daniel.Olkowski@dell.com

One page

Cyber Security



SITE A

IT Infrastructure

DD Boost

Ransomware protection

Any backup software

Backup Recovery

Data Domain

SITE B

IT Infrastructure

DD Boost

Ransomware protection

Any backup software

Backup Recovery

Data Domain

Disaster Recovery

1% data transfer
100% recovery

Cyber Bunker

Air Gap
Separation from production

Data Domain

Secure Historical backups

Compliance No possibility to change data

Automation

PLAN B – Secure data & Recovery

Cyber Recovery	Management and automation
Cyber Sense	Checking ransomware
Backup software	Recovery automation
Sandbox	Any tests

SITE A SITE B

Cyber Bunker

A complete solution that allows **recovery**
after hacker/ransomware attack.

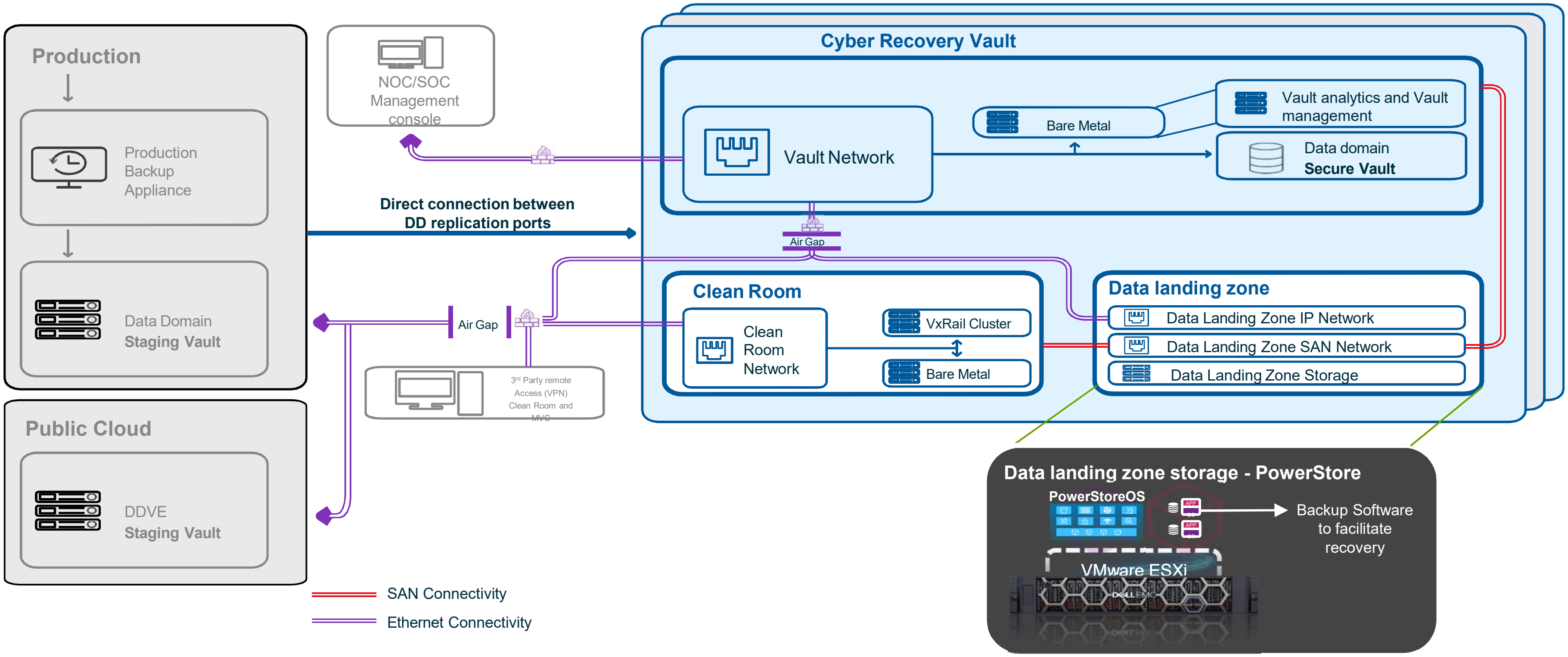
Isolated from production, with any frequency (15min /1h)
Cyber Bunker keeps historical snapshots of all data
with no possibility to remove, change, encrypt by ransomware/hacker.

All the operations in CyberBunker - grabbing data, compliance
protection, checking against virus, recovery – are fully automated.

Be safe!

Cyber Recovery Vault with PowerStore

Secure Landing Zone for recovery of data facilitated by PowerStore


Production
Production Backup Appliance
Data Domain Staging Vault
Public Cloud
DDVE Staging Vault
NOC/SOC Management console
Direct connection between DD replication ports
Air Gap
3rd Party remote Access (VPN) Clean Room and MVC
Cyber Recovery Vault
Vault Network
Bare Metal
Vault analytics and Vault management
Data domain Secure Vault
Air Gap
Clean Room
Clean Room Network
VxRail Cluster
Bare Metal
Data landing zone
Data Landing Zone IP Network
Data Landing Zone SAN Network
Data Landing Zone Storage
Data landing zone storage - PowerStore
PowerStoreOS
APP
APP
Backup Software to facilitate recovery
VMware ESXi
DELL EMC
SAN Connectivity
Ethernet Connectivity

Why PowerStore

- PowerStore X’s built in Hypervisor allows for Cyber Recovery to completely isolate the recovery process outside of the vault and facilitate rebuild on the PowerStore
- PowerStore can then either vMotion recovered hosts or present storage to hosts in the Clean Room, ready for rebuild
- Provides a faster means for data recovery out of the vault
- Only PowerStore, with it’s built in hypervisor, has the ability to do this across the portfolio.

Why Cyber Bunker?

- Full protection
  - No possibility to change / delete data for defined period (*Compliance*) by anyone
    - Ransomware
    - Hacker
    - …
  - Air gap – no access to bunker from the production / world

Why Cyber Bunker?

- Snapshot of production – full image of production
  - In regular intervals (1h / 1 day / …)
  - Protected (as below)
- Automation - All operation in the bunker are automated
  - Snapshots
  - Compliance
  - Checking if snapshots are not compromised

Why Cyber Bunker?

- Checking the production data (snapshots) kept in bunker - add on option
  - Against ransomware
  - Against exploit
  - Against encrypted data

Why Cyber Bunker?

- Automated recovery in case of production encryption
- No influence on the production
- Cyber Recovery solution is included within the price of Data Domain
  - Required Data Domain in bunker and implementation

Agenda

Cyber Security

Maurice: So... Do you have any plan?

Maurice: So... Do you have any plan?

Julian: Better! I have personal charm.

Source: The Penguins of Madagascar, Period 1a, Popcorn Panic

Agenda

- Why backup and cyber security?
- Is Cyber Bunker required?
  - Can backup Solution protect my environment against cyber security?
- Let’s make it easy, cost effective and secure
- Why me?

Cyber Recovery

- Do we need Cyber Recovery?
  - Type of backup media
  - Ease of use
  - Type of backup software
- Any backup software

- Security & Infrastructure department common project
  - Plan B
- Plan
  - Air gap
  - Frequency
  - Data

Cyber Recovery

- Cost
- Out of 10 projects 4 includes Cyber Recovery
- Solution for any environment
- Know-how
- Services
- Materials

Agenda

- Why backup and cyber security?
- Why Dell?
- Hot topic
- Competition

xrem

Cyber Recovery

- How to start?
  - My customers
  - White paper
  - Talking to the market

Why backup person talks about

Cyber Security?

HACKED

CYBER CRIME GETS SOPHISTICATED

Are you staying ahead of the Criminal evolution?

Traditional Threats

Cyber **Theft**

Denial of Service Attacks

Emerging Threats

Cyber **Extortion**

Cyber **Destruction**

Isolated Recovery Solutions Protect Against these Classes of Attacks

Potential attacks

Virus / Ransomware

Hacker

Cyber threats: the facts

A cyber attack occurs

every

39

sec

Source: Security Magazine

verizon√

71%

of breaches are financially motivated

verizon√

43%

of breaches involved small business

accenture

$13M

Avg cost of Cybercrime for an organization

accenture

$5.2T

of global risk over the next 5 years

Avg. cost of cyber attack

by Industry

Industry	Avg Cost
Banking	**$18.4M**
Utilities	**$17.8M**
Software	**$16M**
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**

accenture

Cyberattacks and Financial Impact

SONY

Financial Impact (Loss): $300M
- Business Operations
- Litigation /Legal
- Brand / Reputation

What happened:
- Insider cooperation, ransomware and data destruction

What was reported:
- Destroyed Prod and DR Backup Storage
- Crippled IT networks
- Wiped out 4,100 of 8,300 pcs / servers
- Stole 100TB of data (Equal to 10 times the size of printed Library of Congress)

Aftermath / Impact:
- Reduced to pen, paper, and fax
- IT repairs
- Class –action settlement
- Legal / litigation fees

MAERSK

Financial Impact (Loss): $300M
- Business Operations
- Litigation /Legal
- Brand / Reputation

What happened:
- NotPetya, irrecoverably wiping data

What was reported:
- Reactionary shutdown of global networks
- One-fifth of the world's shipping capacity, rendered useless
- Phone systems were rendered useless

Aftermath / Impact
- Downed 76 shipping ports
- Paralyzed 800 seafaring vessels

MERCK

Financial Impact (Loss): $1,300M
- Business Operations
- Litigation /Legal
- Brand / Reputation

What happened:
- NotPetya, irrecoverably wiping data

What was reported:
- Halted drug production
- Impacted sales, manufacturing, and research units

Aftermath / Impact:
- Halted drug production
- Crippled 30,000 laptops / desktops, and 7,500 servers
- Caused production shortages in the supply chain
- Took 18 months to replenish the cache

FedEx®

Financial Impact (Loss): $300M
- Business Operations
- Litigation /Legal
- Brand / Reputation

What happened:
- NotPetya, irrecoverably wiping data

What was reported:
- FedEx briefly halted trading in its shares
- Subsidiary TNT's delivery system impacted (online, ground and air) globally
- Some systems, unrecoverable

Aftermath / Impact:
- Widespread service and invoice delays
- Forced to move from automated to manual processes for operations and customer service
- Loss of revenue due above contingency plans

Target of the attack

Production data

Production data and security

If we loose our production data…

Production data and security

**If we loose
our production data. . .**

**we have magic button:
RECOVERY**

What if our plan B has gone…

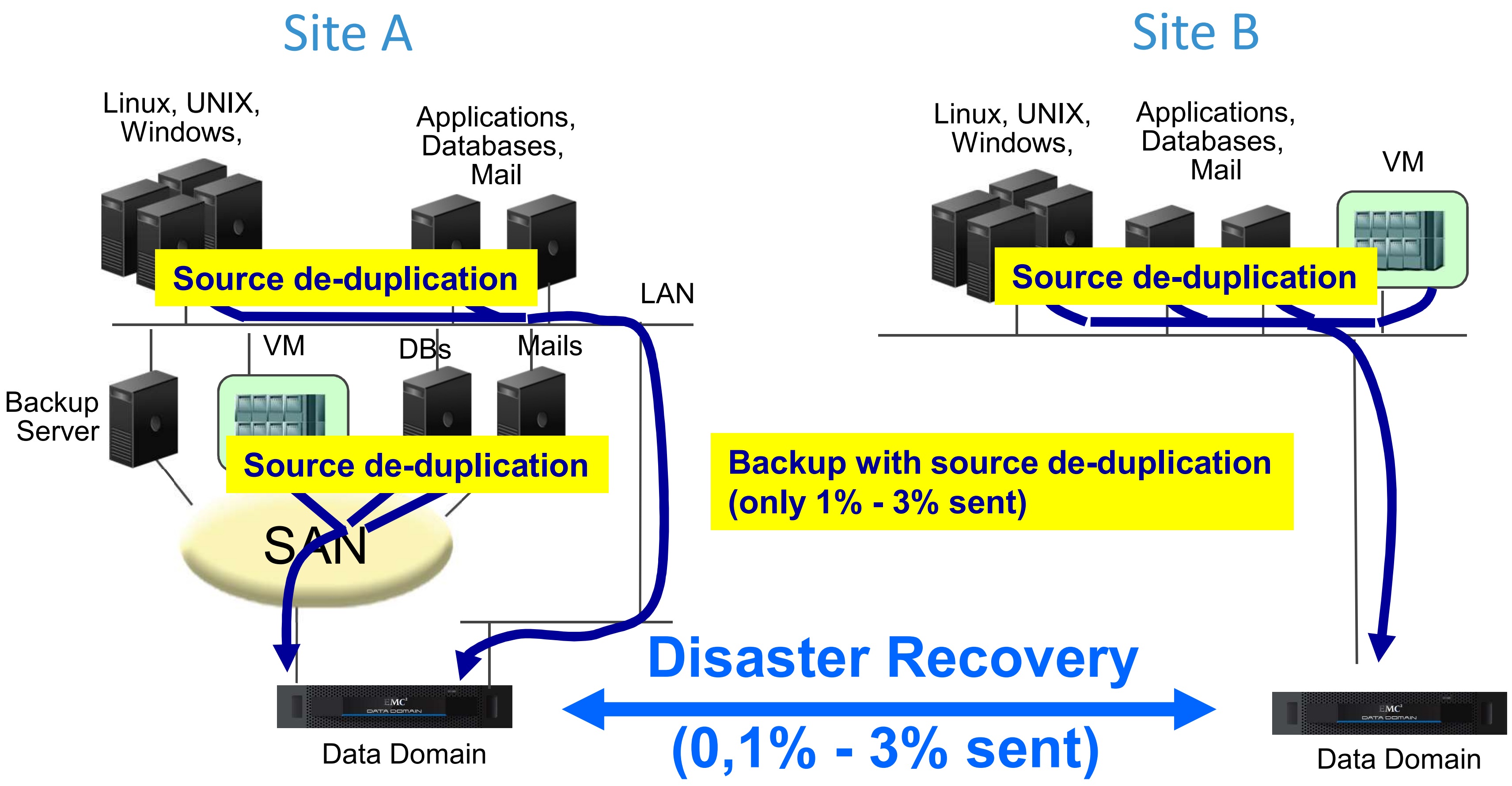
If we loose our production data. . .

we have magic button:
RECOVERY

Can backup system protect us against

Cyberattack?

Data Domain as backup medium



Site A

Linux, UNIX, Windows,

Applications, Databases, Mail

Source de-duplication

LAN

VM

DBs

Mails

Backup Server

Source de-duplication

SAN

Data Domain

Site B

Linux, UNIX, Windows,

Applications, Databases, Mail

VM

Source de-duplication

Backup with source de-duplication (only 1% - 3% sent)

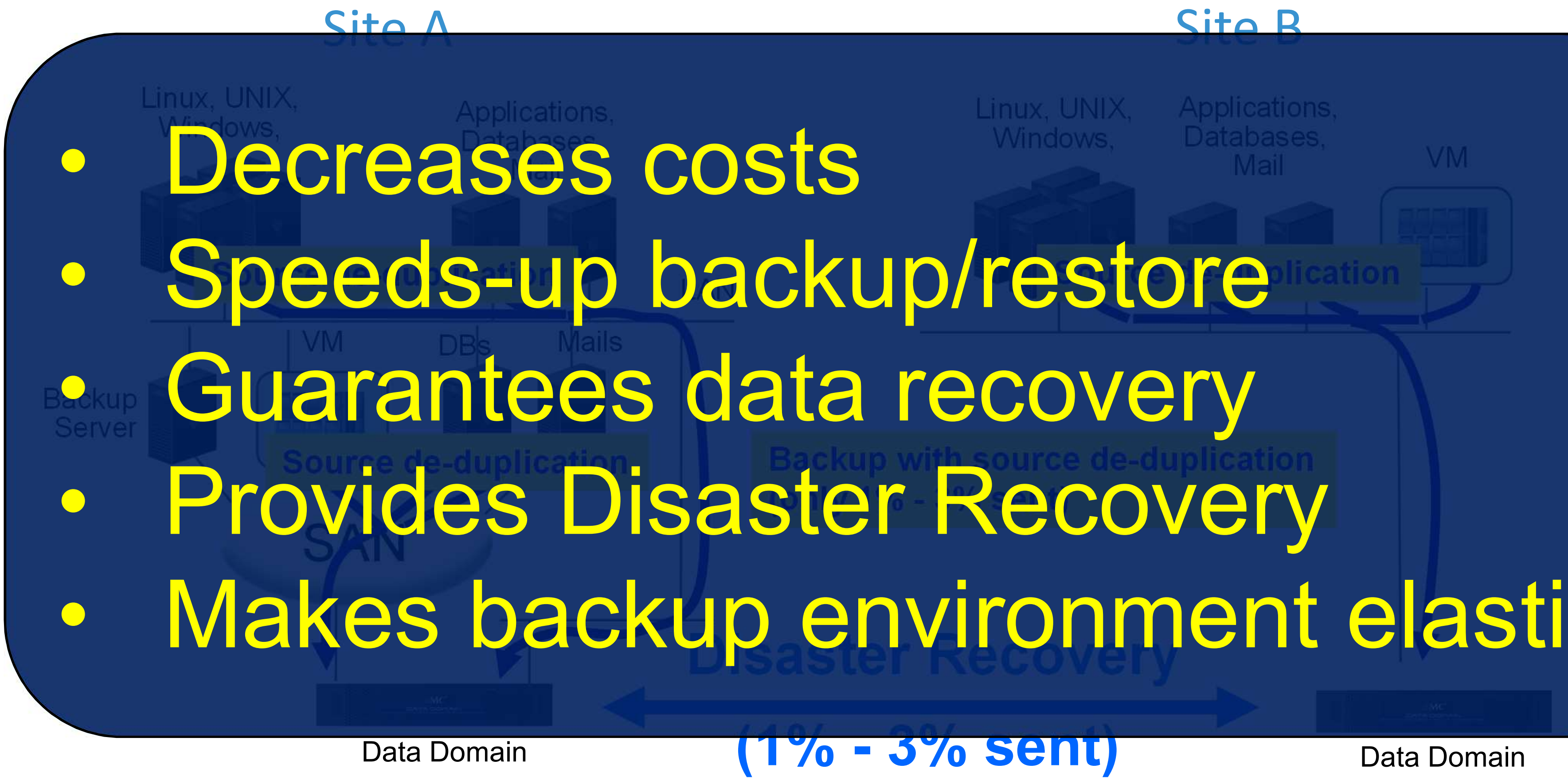
Disaster Recovery

(0,1% - 3% sent)

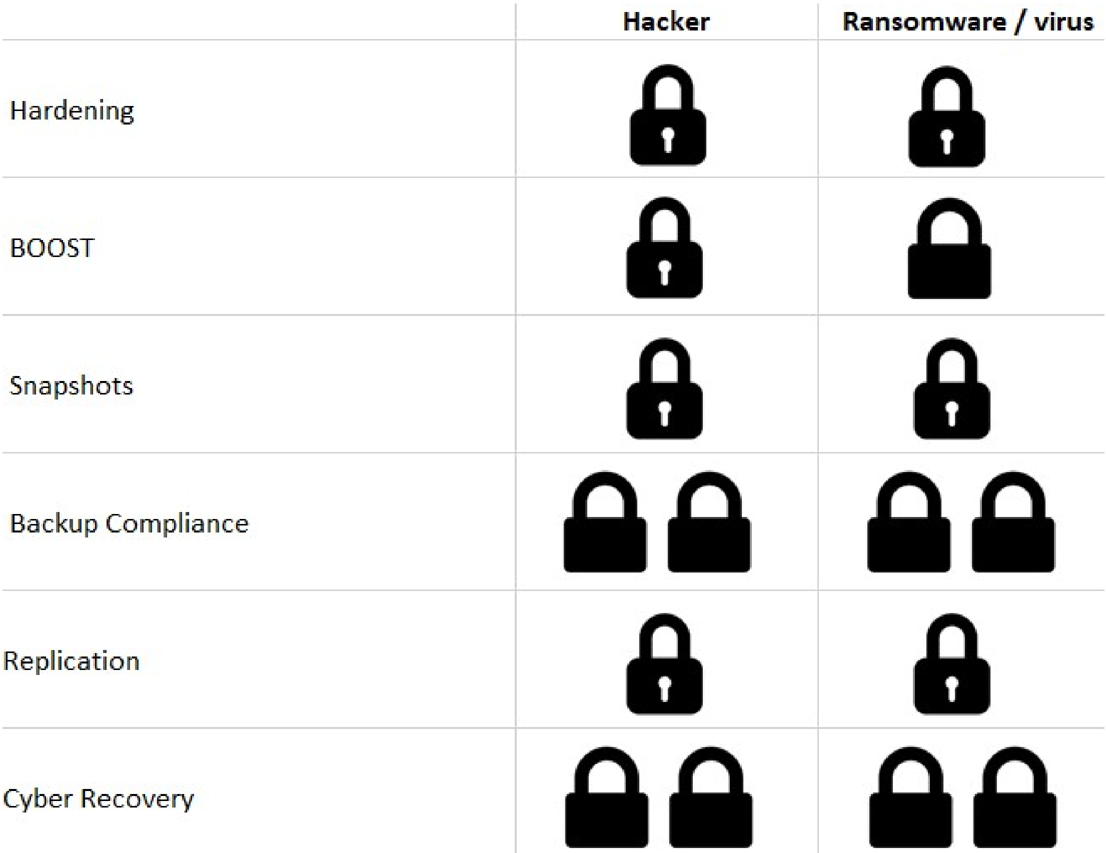
Data Domain

Data Domain as backup medium

- Decreases costs
- Speeds-up backup/restore
- Guarantees data recovery
- Provides Disaster Recovery
- Makes backup environment elastic



Data Domain: Method of protection against cyber attack

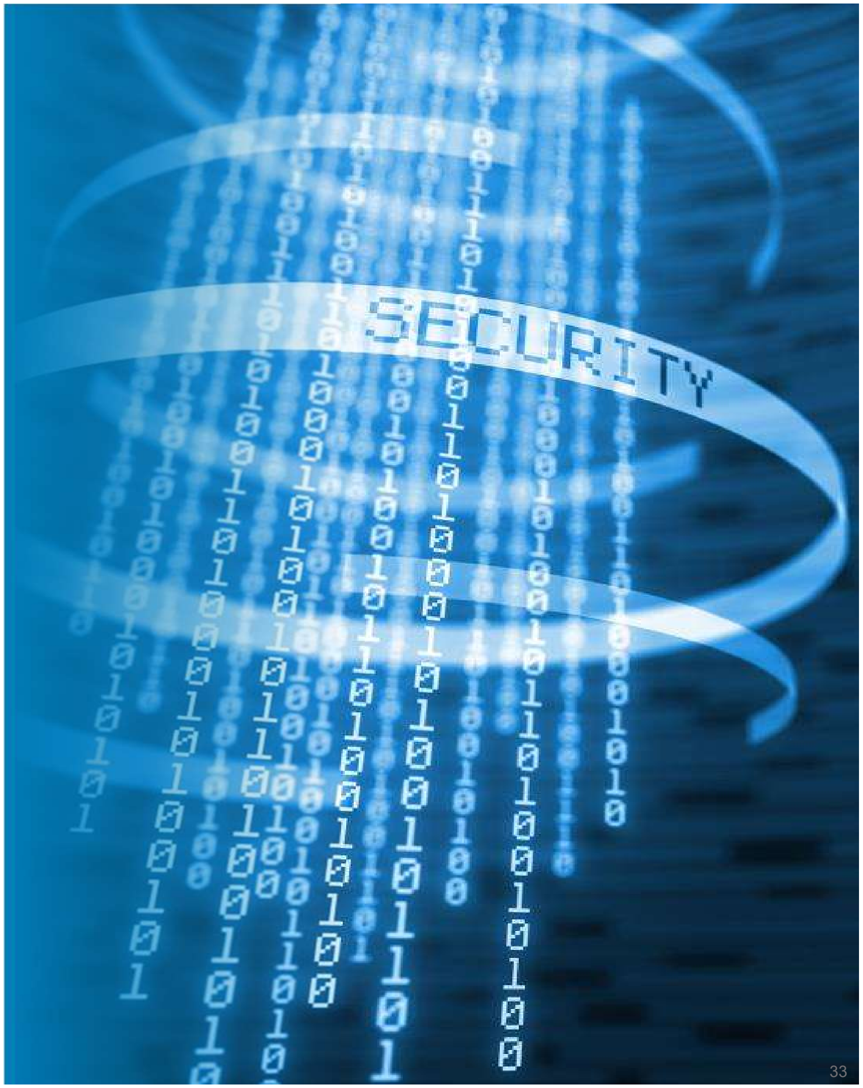


	Hacker	Ransomware / virus
Hardening	🔒	🔒
BOOST	🔒	🔒
Snapshots	🔒	🔒
Backup Compliance	🔒🔒	🔒🔒
Replication	🔒	🔒
Cyber Recovery	🔒🔒	🔒🔒

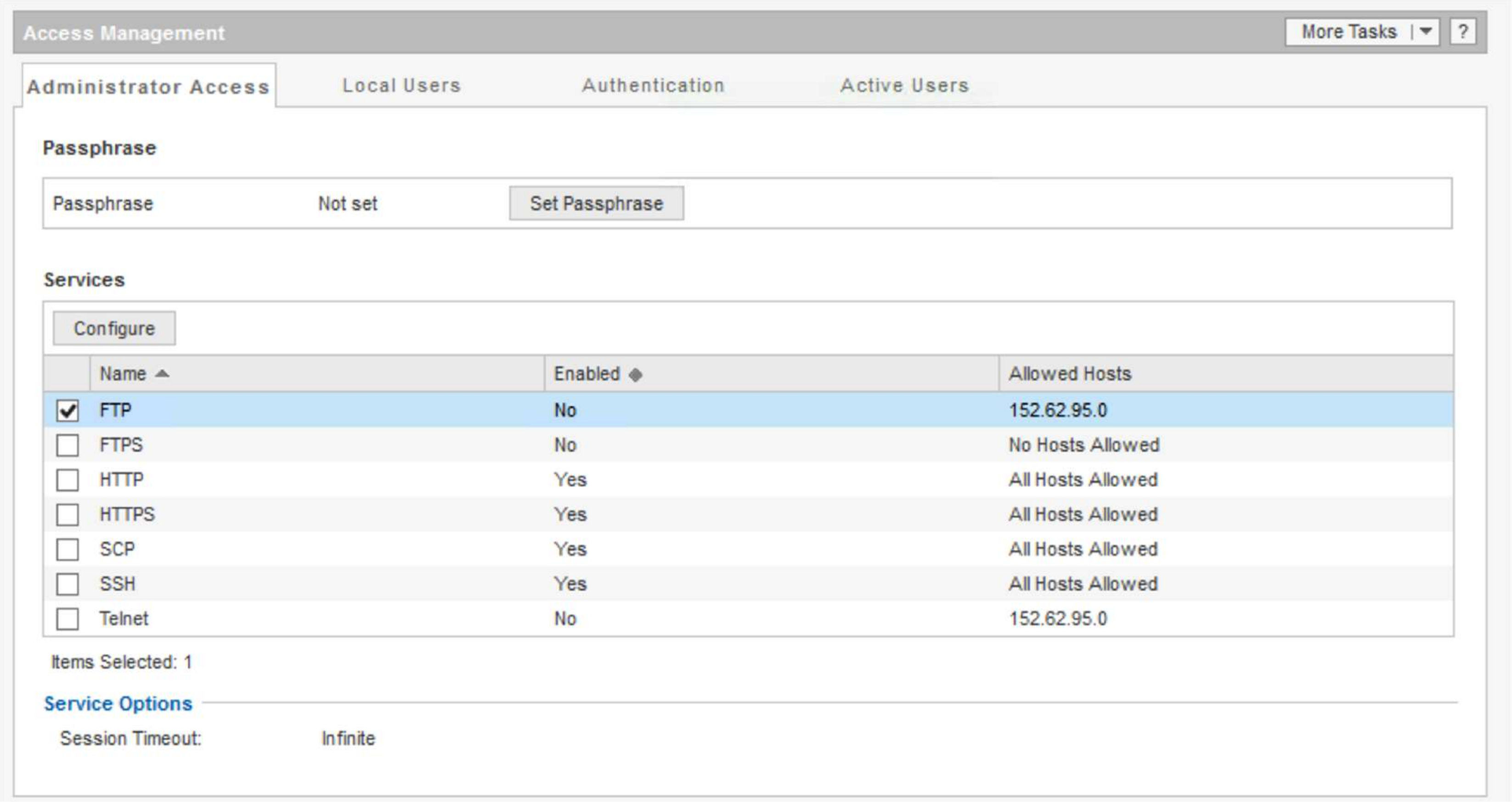
Environment hardening

- Examples:
  - Inactivity Timeout
  - Deny Consecutive Login Attempts
  - Password Aging/Rotation
  - Password Complexity
  - Disable Default Accounts
  - Communication Port Disable / Change
  - Restrict hosts access / IP
  - Use of SSH and Certificates
  - Disable HTTP, FTP, Telnet, etc.
  - Disable unused services
  - Apply Latest Security Patches
  - Use SYSLOG Server / Prevent Audit Log Roll Over

- Review the latest respective Dell EMC Product Security Guides for Hardening Guidelines



Environment hardening



Passphrase

Passphrase Not set

Services

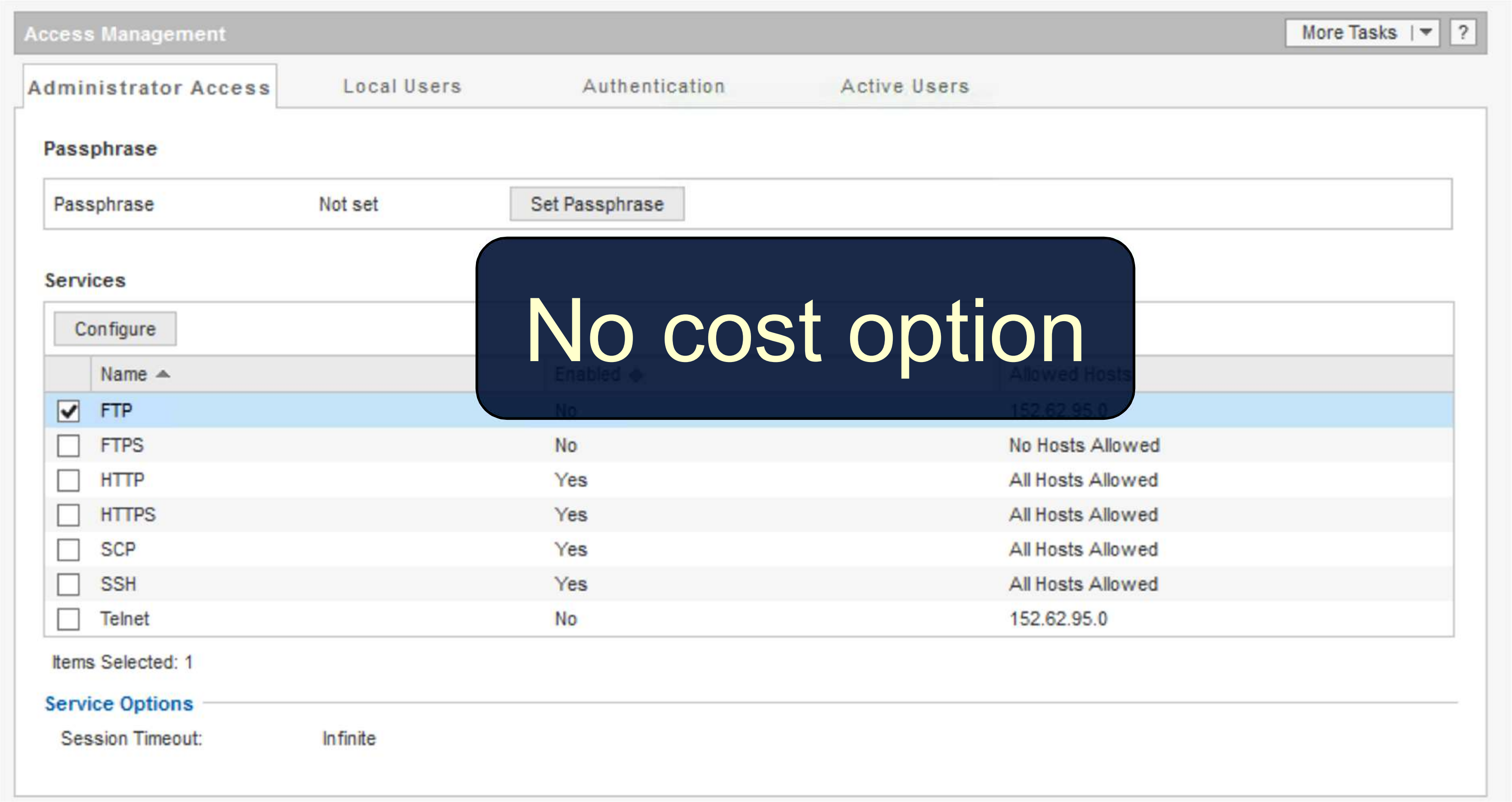
	Name	Enabled	Allowed Hosts
☑	FTP	No	152.62.95.0
☐	FTPS	No	No Hosts Allowed
☐	HTTP	Yes	All Hosts Allowed
☐	HTTPS	Yes	All Hosts Allowed
☐	SCP	Yes	All Hosts Allowed
☐	SSH	Yes	All Hosts Allowed
☐	Telnet	No	152.62.95.0

Items Selected: 1

Service Options

Session Timeout: Infinite

Environment hardening



Access Management

Passphrase

Passphrase: Not set

Services

	Name ▲	Enabled	Allowed Hosts
☑	FTP	No	152.62.95.0
□	FTPS	No	No Hosts Allowed
□	HTTP	Yes	All Hosts Allowed
□	HTTPS	Yes	All Hosts Allowed
□	SCP	Yes	All Hosts Allowed
□	SSH	Yes	All Hosts Allowed
□	Telnet	No	152.62.95.0

Items Selected: 1

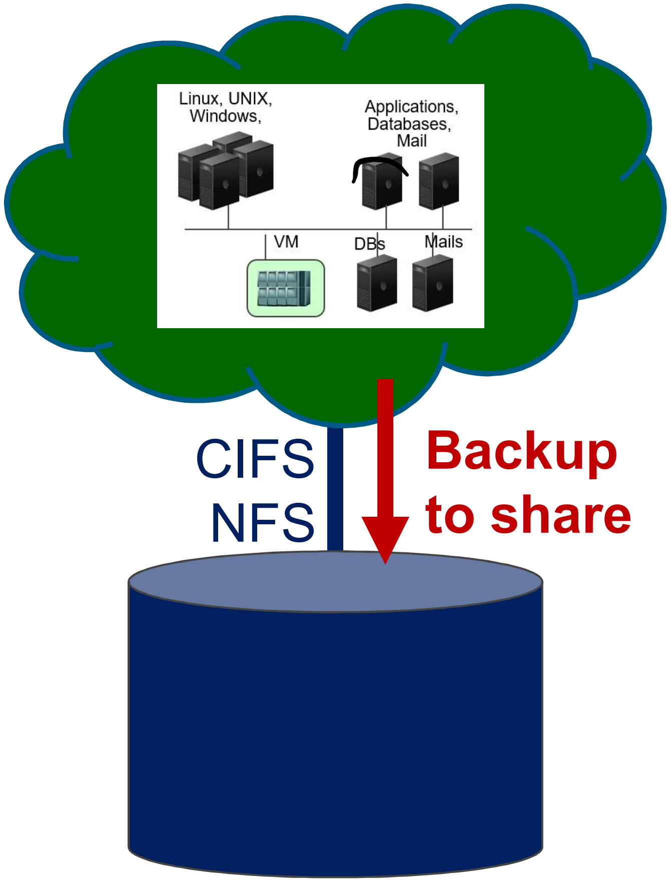
Service Options

Session Timeout: Infinite

No cost option

Snapshots

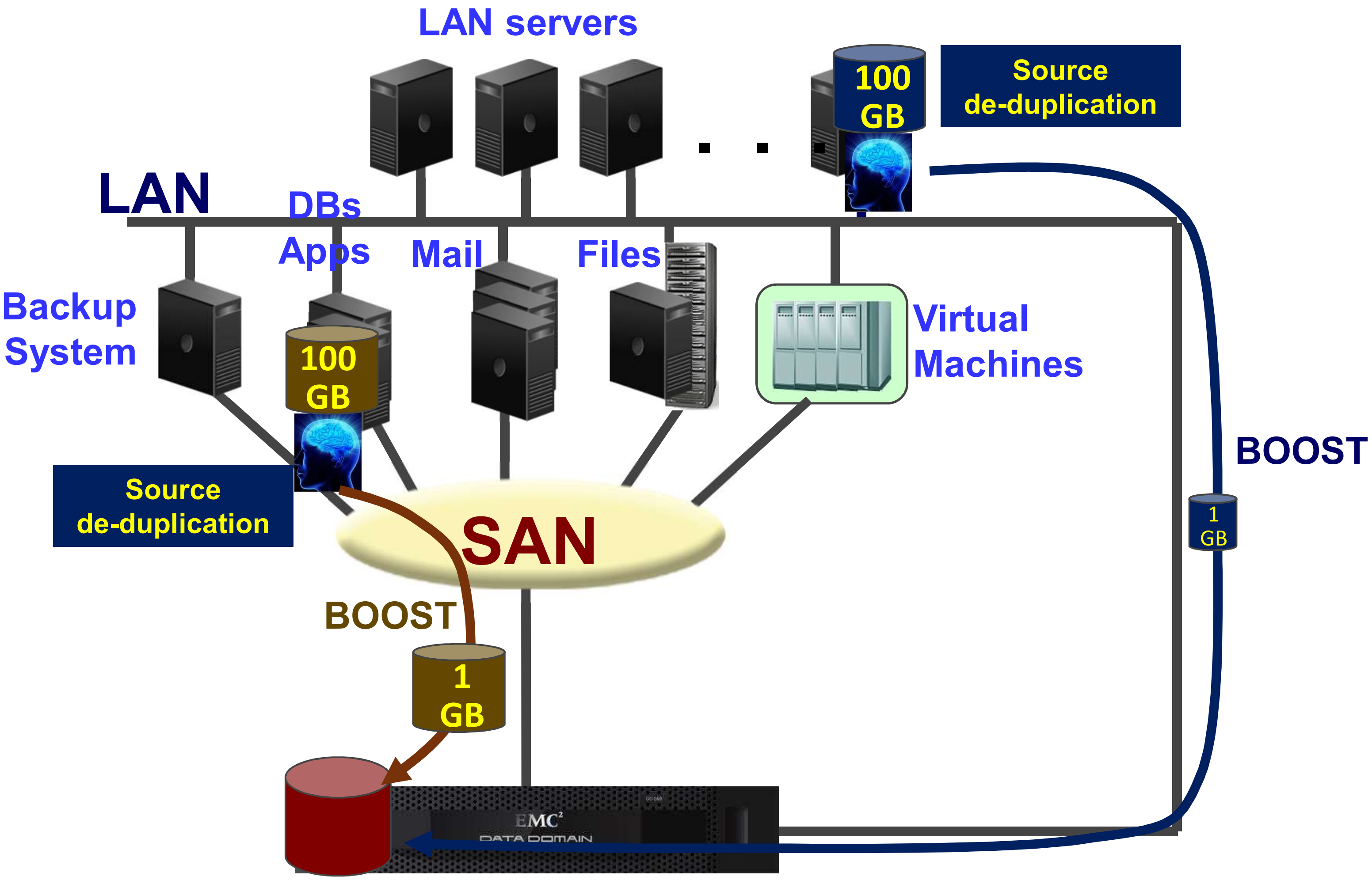
CIFS / NFS technology are easy to be hacked



CIFS / NFS backups

a. Easy to be encrypted by ransomware

b. Easy to be deleted by hackers

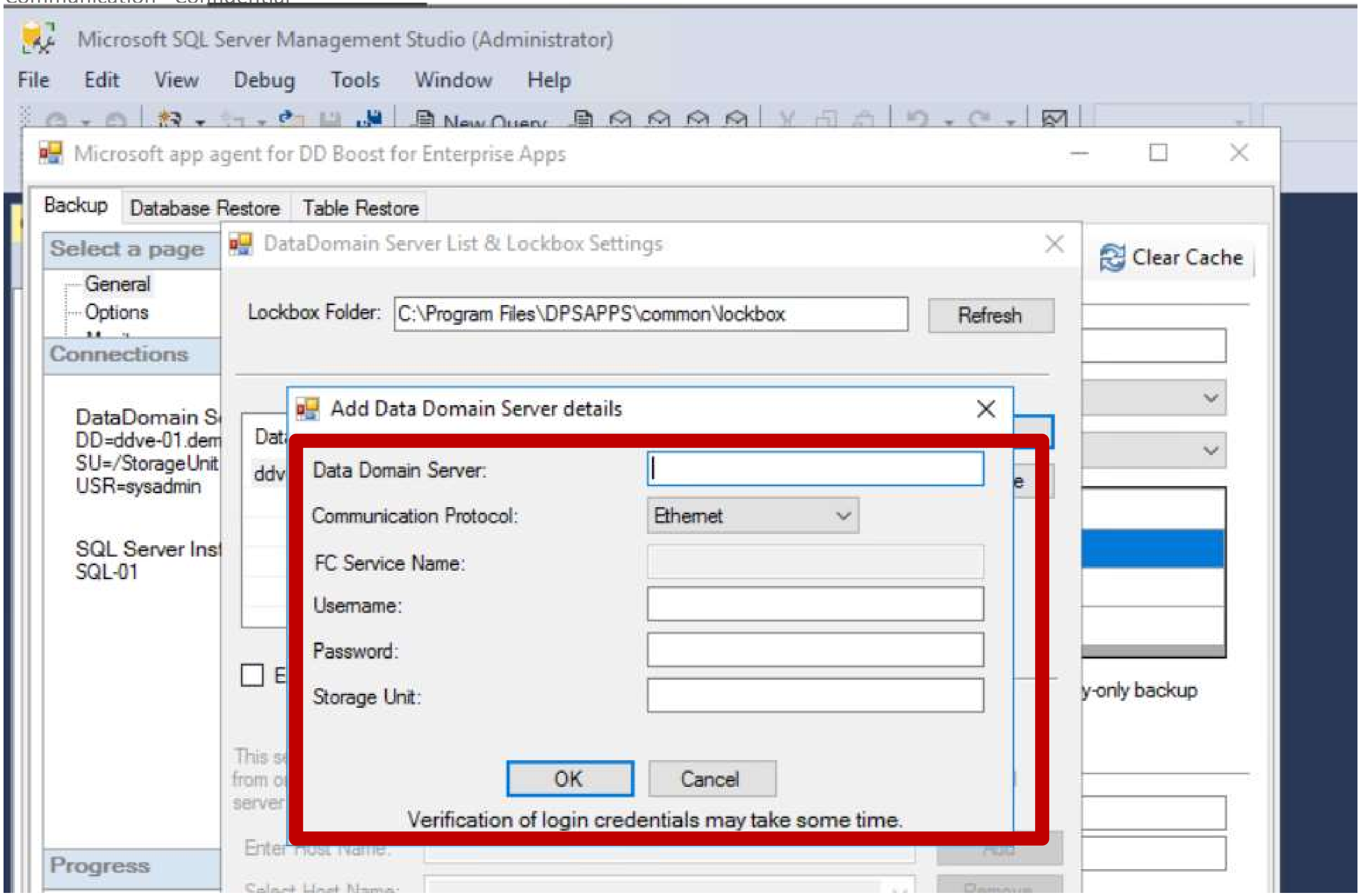

LAN servers
100
GB
Source
de-duplication
LAN
DBs
Apps
Mail
Files
Backup
System
100
GB
Virtual
Machines
BOOST
1
GB
Source
de-duplication
SAN
BOOST
1
GB
EMC²
DATA DOMAIN

LAN servers

BOOST for apps as backup method

Ransomware is not able to infect BOOST resources

A number of customers recovered data from BOOST backups after ransomware attacks



Microsoft SQL Server Management Studio (Administrator)

Microsoft app agent for DD Boost for Enterprise Apps

DataDomain Server List & Lockbox Settings

Lockbox Folder: C:\Program Files\DPSAPPS\common\lockbox

Add Data Domain Server details

Data Domain Server:

Communication Protocol: Ethernet

FC Service Name:

Username:

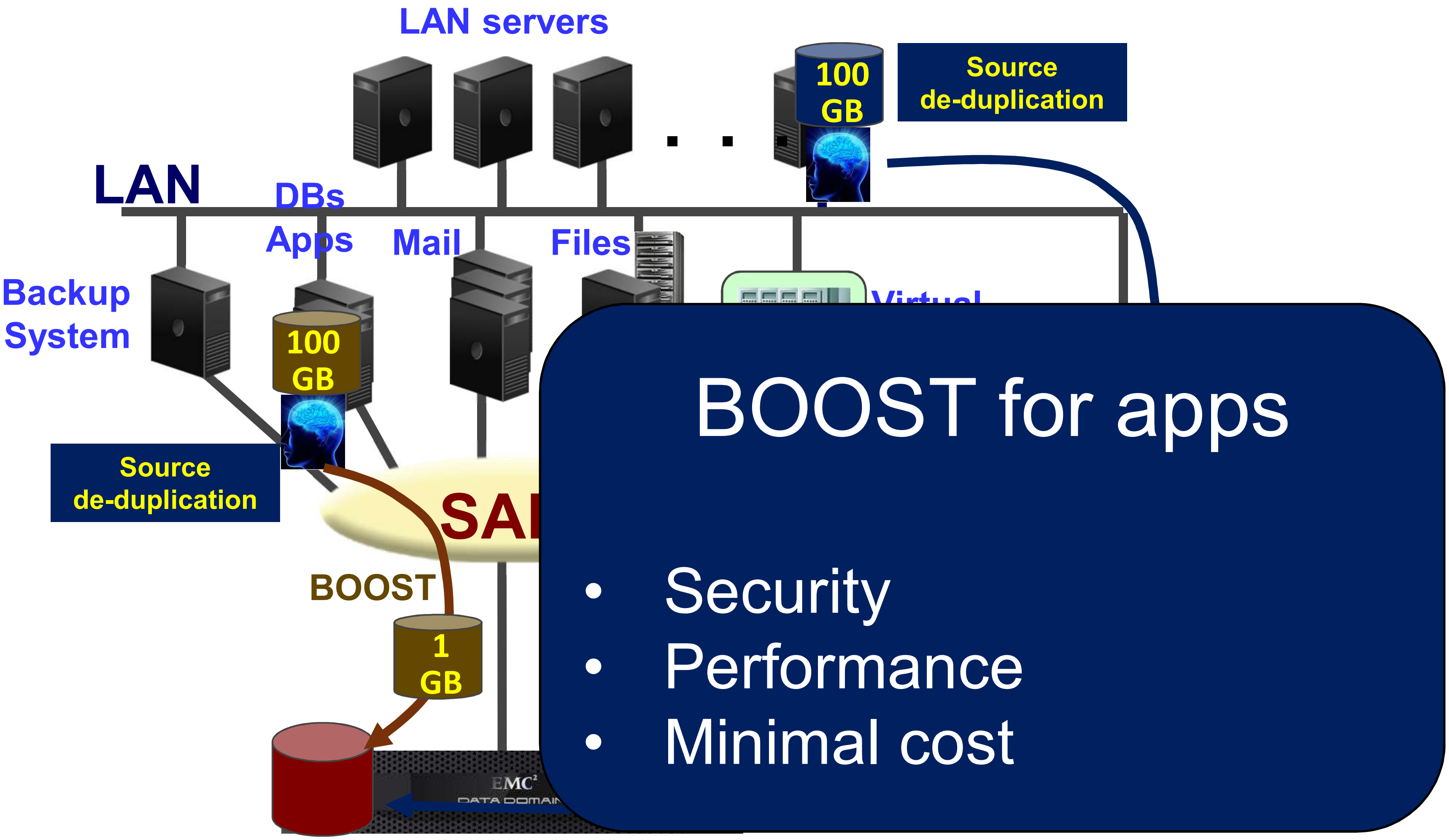
Password:

Storage Unit:

Verification of login credentials may take some time.

DataDomain S
DD=ddve-01.dem
SU=/StorageUnit
USR=sysadmin

SQL Server Inst
SQL-01



BOOST for apps

- Security
- Performance
- Minimal cost

Ransomware: your company can be next

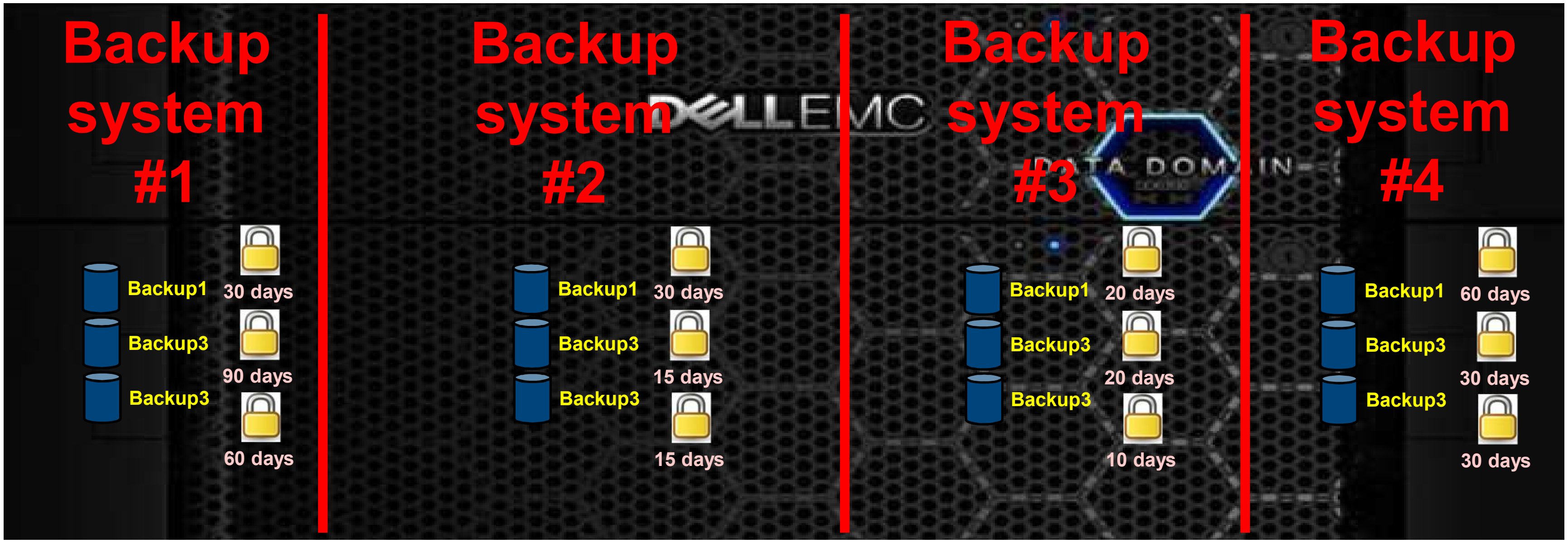
Beiersdorf

NIVEA

- In July 2017 Beiersdorf suffered a serious ransomware attack
- During the attack every Windows Client went down (not only in the HQ in Hamburg, but worldwide!)
- The customer was able to recover only thanks to Data Domain that they are using!

Data Domain allows to lock (compliance) backup files for certain amount of time.

During lock time no one can modify / delete file



Backup system #1

Backup1 30 days

Backup3 90 days

Backup3 60 days

Backup system #2

Backup1 30 days

Backup3 15 days

Backup3 15 days

Backup system #3

Backup1 20 days

Backup3 20 days

Backup3 10 days

Backup system #4

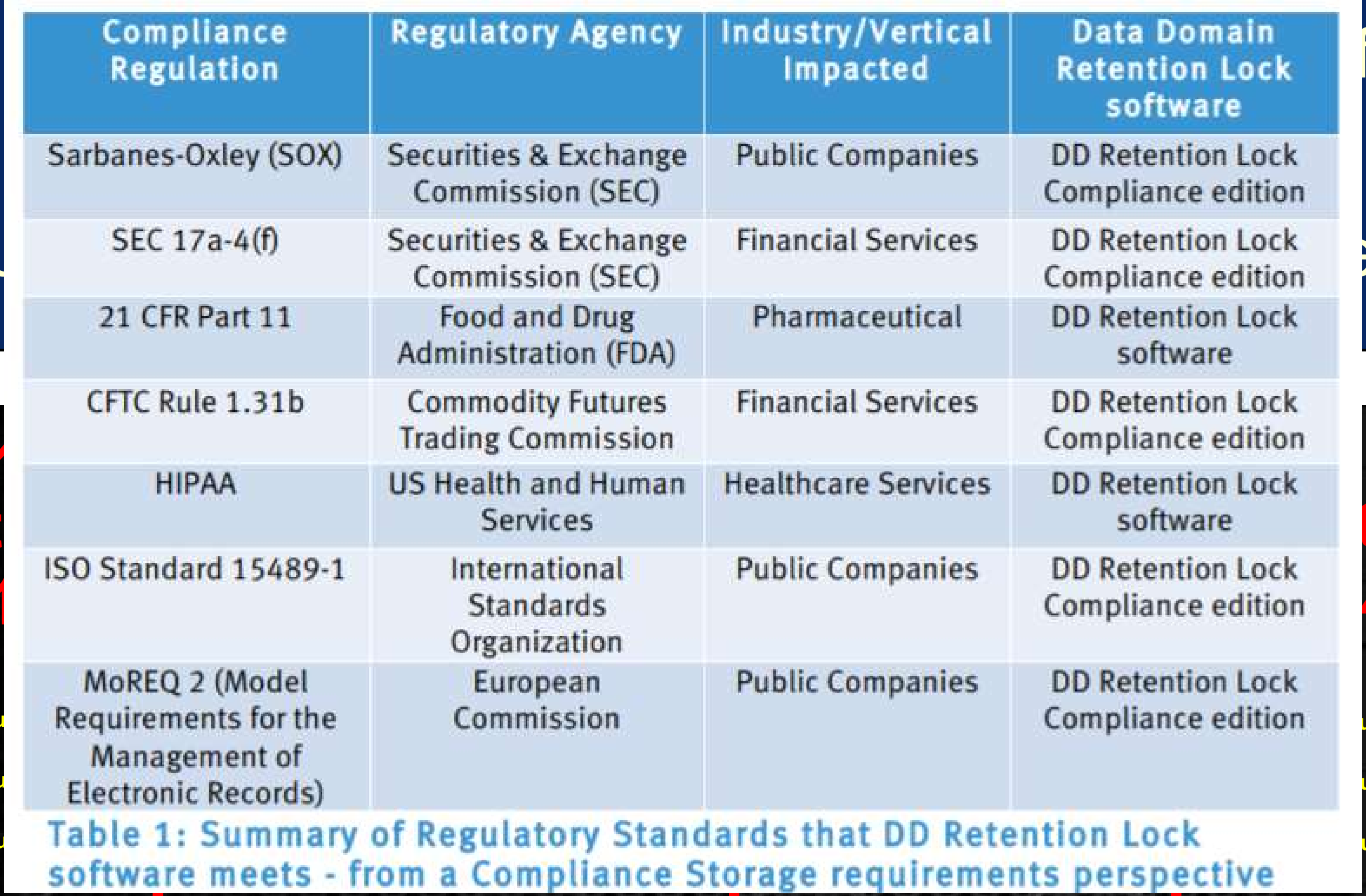
Backup1 60 days

Backup3 30 days

Backup3 30 days

Data files

Du e



Compliance Regulation	Regulatory Agency	Industry/Vertical Impacted	Data Domain Retention Lock software
Sarbanes-Oxley (SOX)	Securities & Exchange Commission (SEC)	Public Companies	DD Retention Lock Compliance edition
SEC 17a-4(f)	Securities & Exchange Commission (SEC)	Financial Services	DD Retention Lock Compliance edition
21 CFR Part 11	Food and Drug Administration (FDA)	Pharmaceutical	DD Retention Lock software
CFTC Rule 1.31b	Commodity Futures Trading Commission	Financial Services	DD Retention Lock Compliance edition
HIPAA	US Health and Human Services	Healthcare Services	DD Retention Lock software
ISO Standard 15489-1	International Standards Organization	Public Companies	DD Retention Lock Compliance edition
MoREQ 2 (Model Requirements for the Management of Electronic Records)	European Commission	Public Companies	DD Retention Lock Compliance edition

Table 1: Summary of Regulatory Standards that DD Retention Lock software meets - from a Compliance Storage requirements perspective

Back syst #1

kup tem 4

Backu

Backu

Backu

up1 60 days

up3 30 days

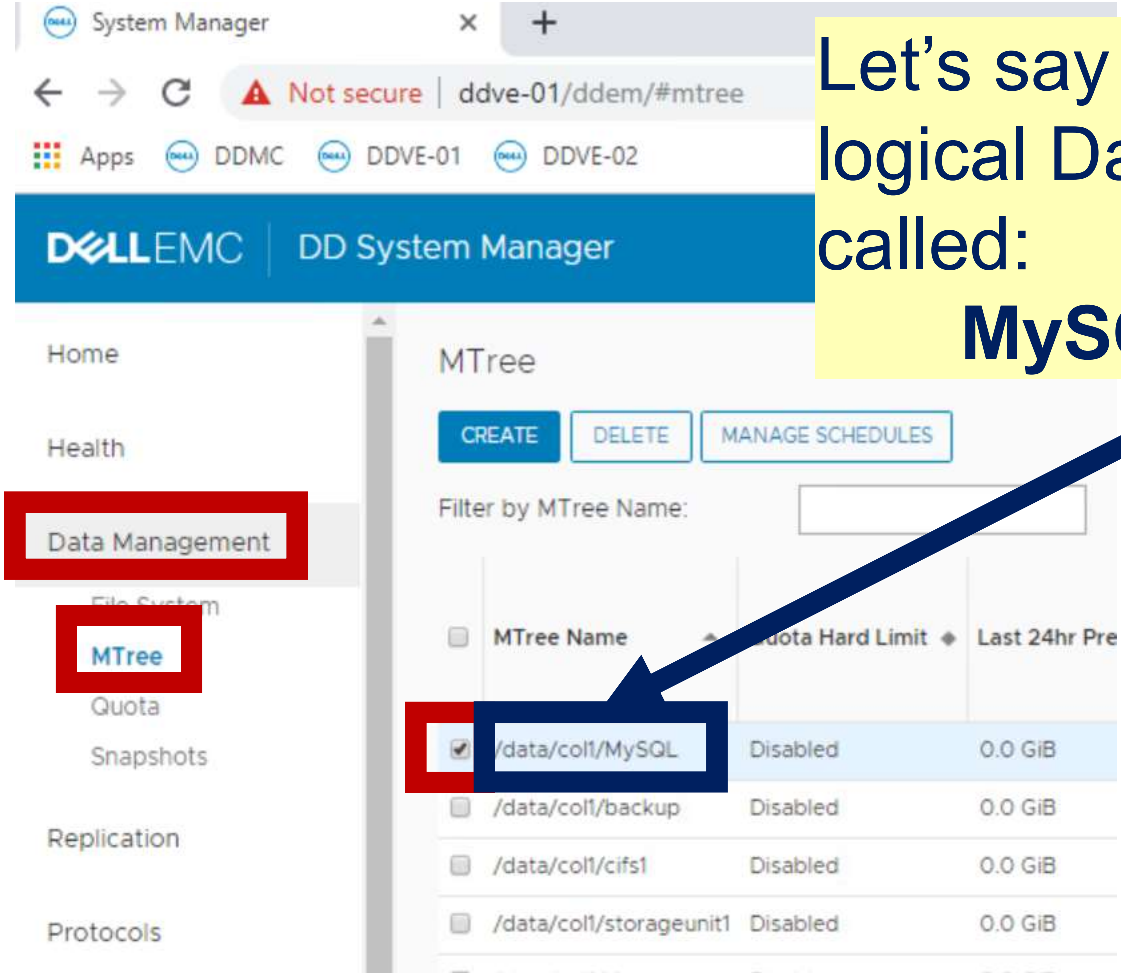
up3 30 days

60 days

15 days

10 days

How to do it?



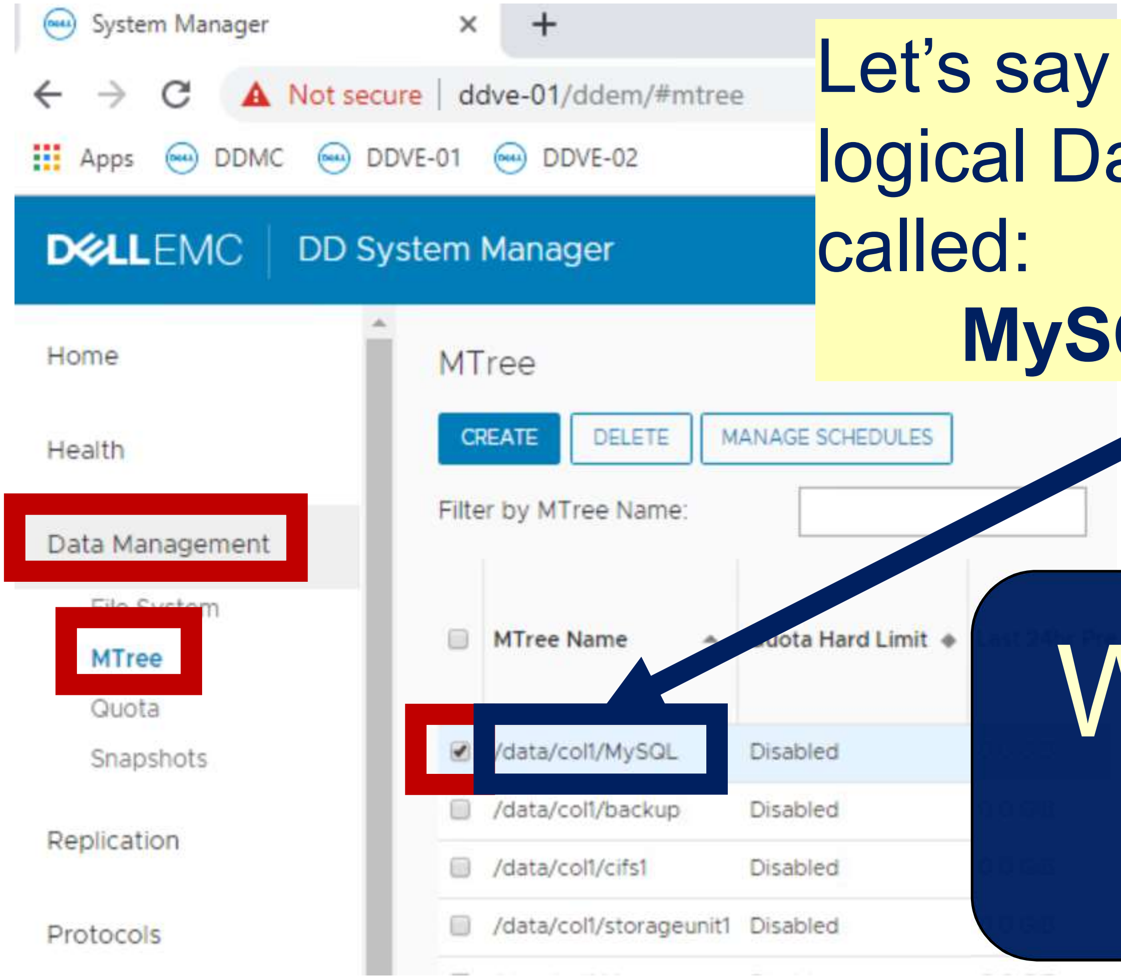
MTree

Filter by MTree Name:

☐	MTree Name	uota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
☐	/data/col1/backup	Disabled	0.0 GiB
☐	/data/col1/cifs1	Disabled	0.0 GiB
☐	/data/col1/storageunit1	Disabled	0.0 GiB

Let’s say we have created logical Data Domain (mtree) called:

MySQL



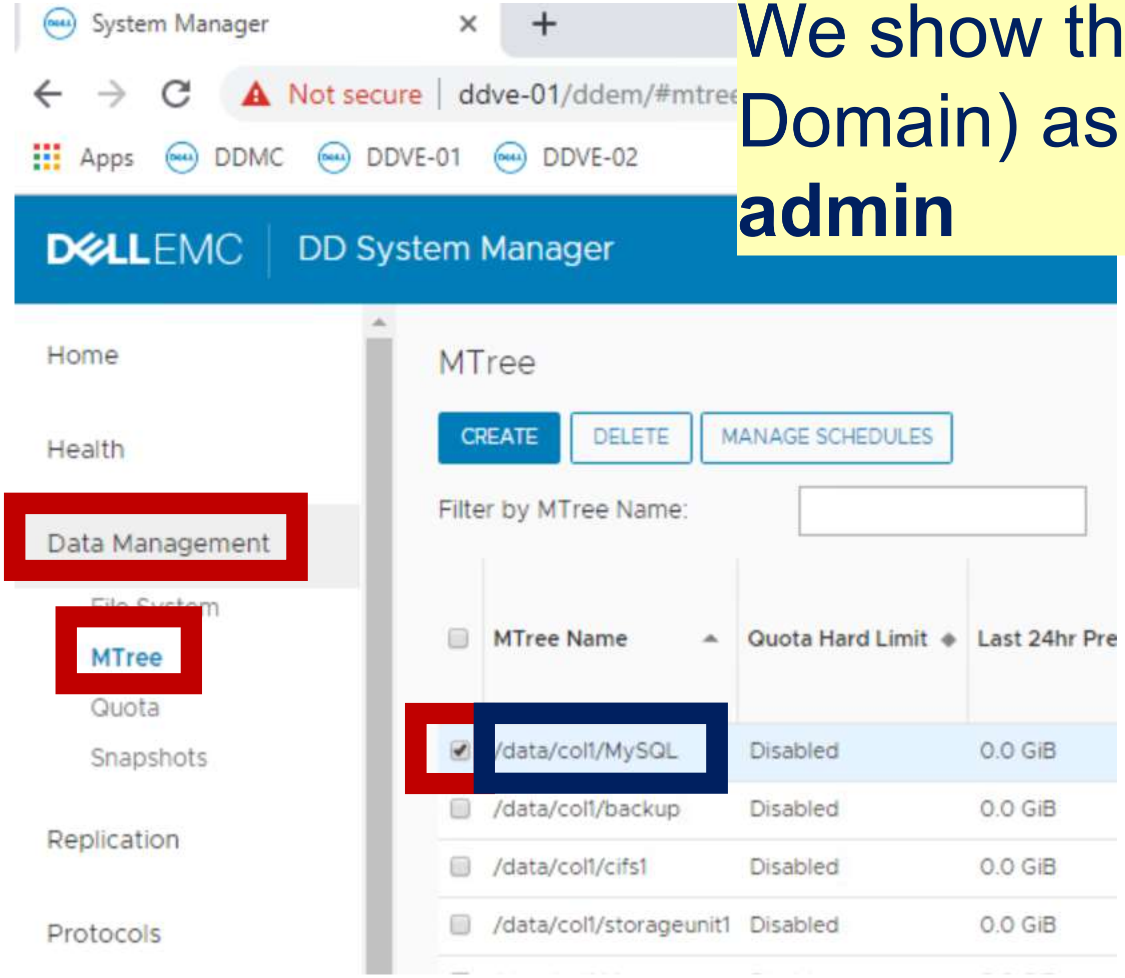
□	MTree Name	uota Hard Limit
☑	/data/col1/MySQL	Disabled
□	/data/col1/backup	Disabled
□	/data/col1/cifs1	Disabled
□	/data/col1/storageunit1	Disabled

Let’s say we have created logical Data Domain (mtree) called:

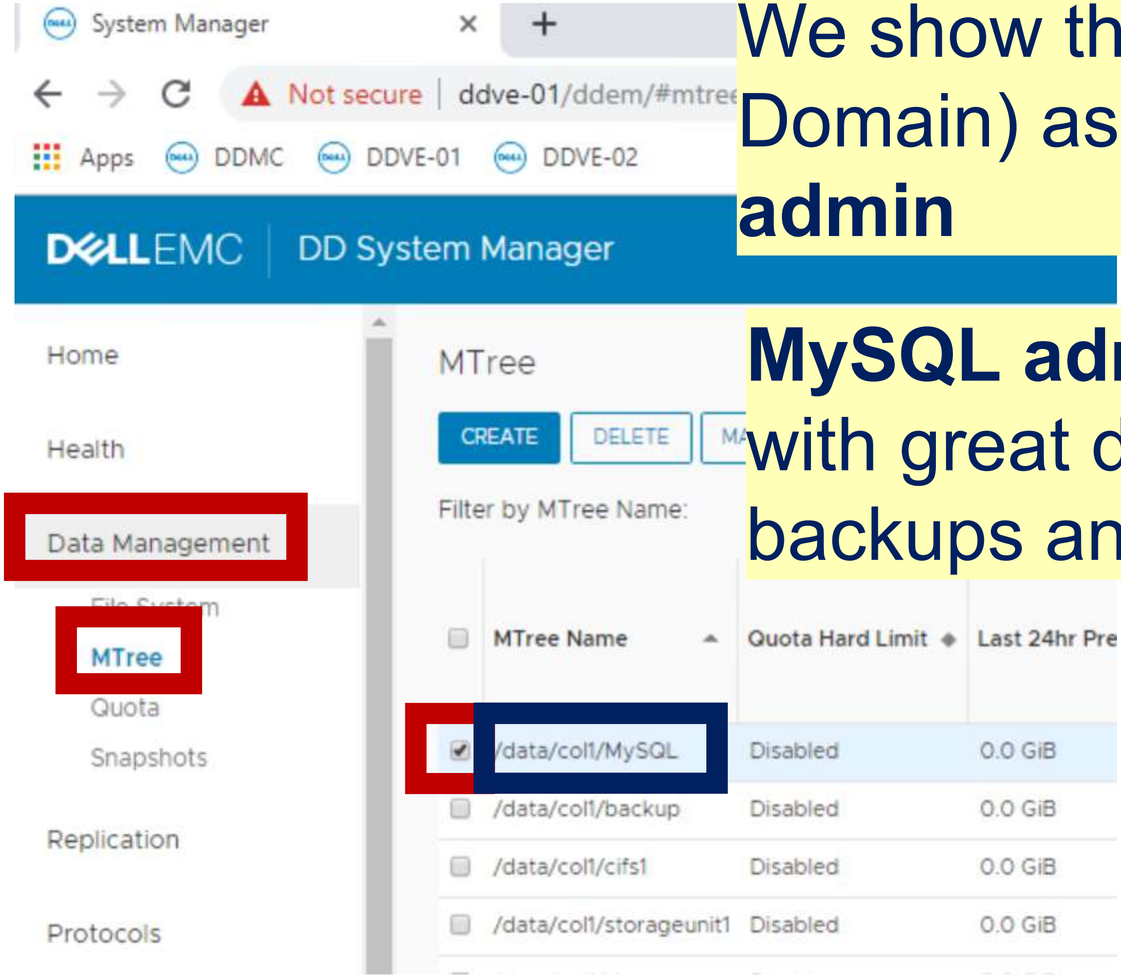
MySQL

Why do we need it?

We show this mtree (logical Data Domain) as CIFS to **MySQL admin**



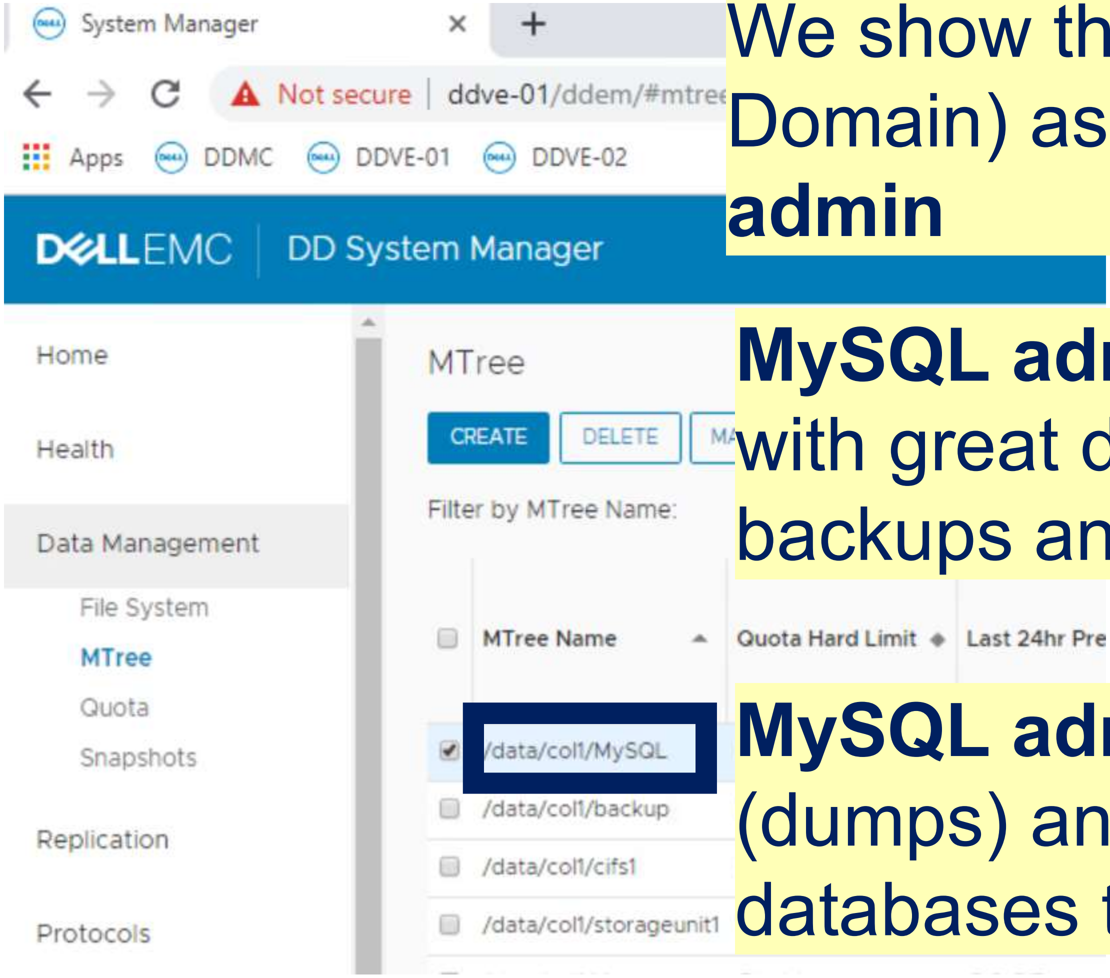
☐	MTree Name	Quota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
☐	/data/col1/backup	Disabled	0.0 GiB
☐	/data/col1/cifs1	Disabled	0.0 GiB
☐	/data/col1/storageunit1	Disabled	0.0 GiB



☐	MTree Name	Quota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
☐	/data/col1/backup	Disabled	0.0 GiB
☐	/data/col1/cifs1	Disabled	0.0 GiB
☐	/data/col1/storageunit1	Disabled	0.0 GiB

We show this mtree (logical Data Domain) as CIFS to **MySQL admin**

MySQL admin has its own disk with great de-duplication, fast backups and fast restores.



MTree

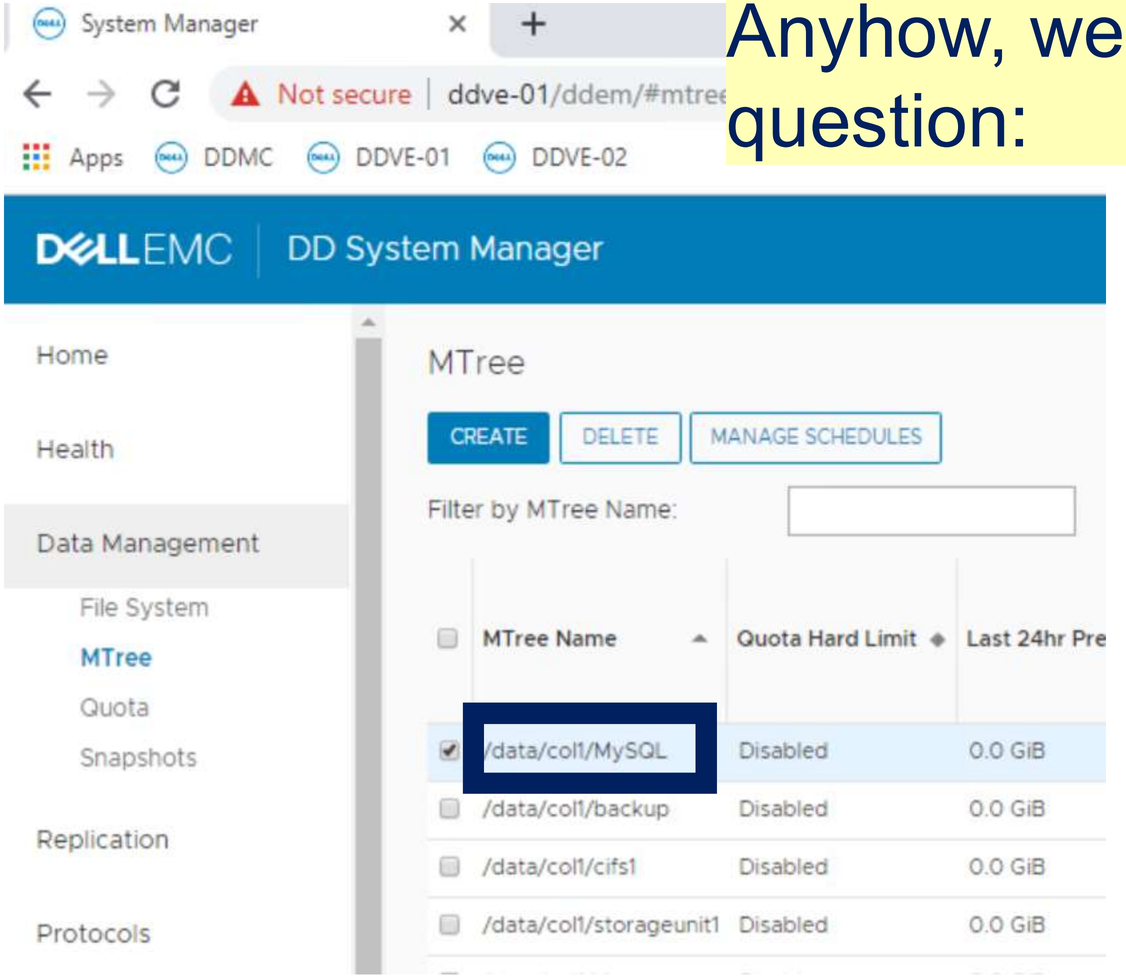
□	MTree Name	Quota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL		
□	/data/col1/backup		
□	/data/col1/cifs1		
□	/data/col1/storageunit1		

We show this mtree (logical Data Domain) as CIFS to **MySQL admin**

MySQL admin has its own disk with great de-duplication, fast backups and fast restores.

MySQL admin can backup (dumps) and restore his databases to this disk

Anyhow, we can ask ourselves question:

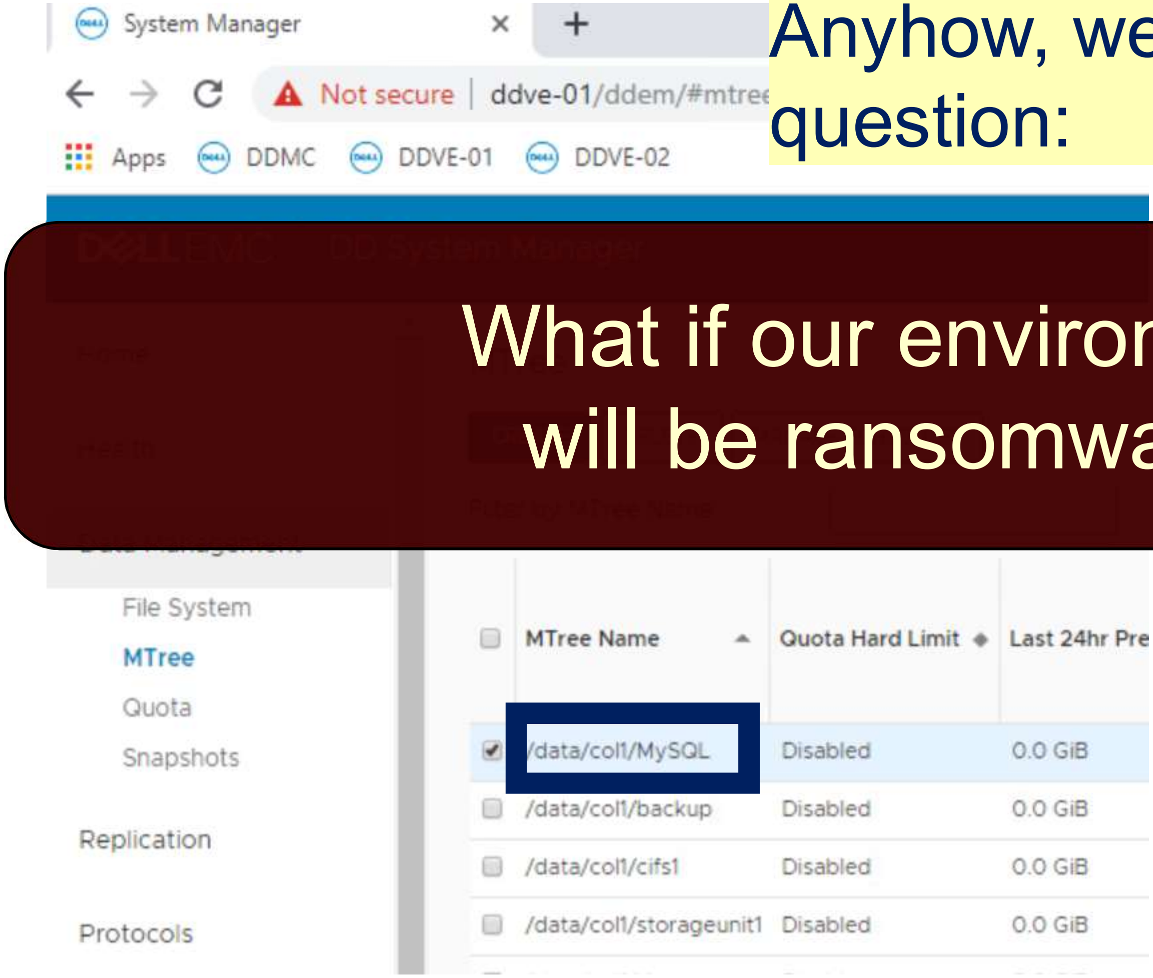


MTree

Filter by MTree Name:

☐	MTree Name	Quota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
☐	/data/col1/backup	Disabled	0.0 GiB
☐	/data/col1/cifs1	Disabled	0.0 GiB
☐	/data/col1/storageunit1	Disabled	0.0 GiB

Anyhow, we can ask ourselves question:



☐	MTree Name	Quota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
☐	/data/col1/backup	Disabled	0.0 GiB
☐	/data/col1/cifs1	Disabled	0.0 GiB
☐	/data/col1/storageunit1	Disabled	0.0 GiB

What if our environments will be ransomwared?

MTree Name	Quota Hard Limit	Last 24hr Pre
/data/col1/storageunit1	Disabled	0.0 GiB

Anyhow, we can ask ourselves question:

What if our environments will be ransomwared?

Will this MySQL disk on Data Domain be encrypted as well?

/data/col1/storageunit1 Disabled 0.0 GiB

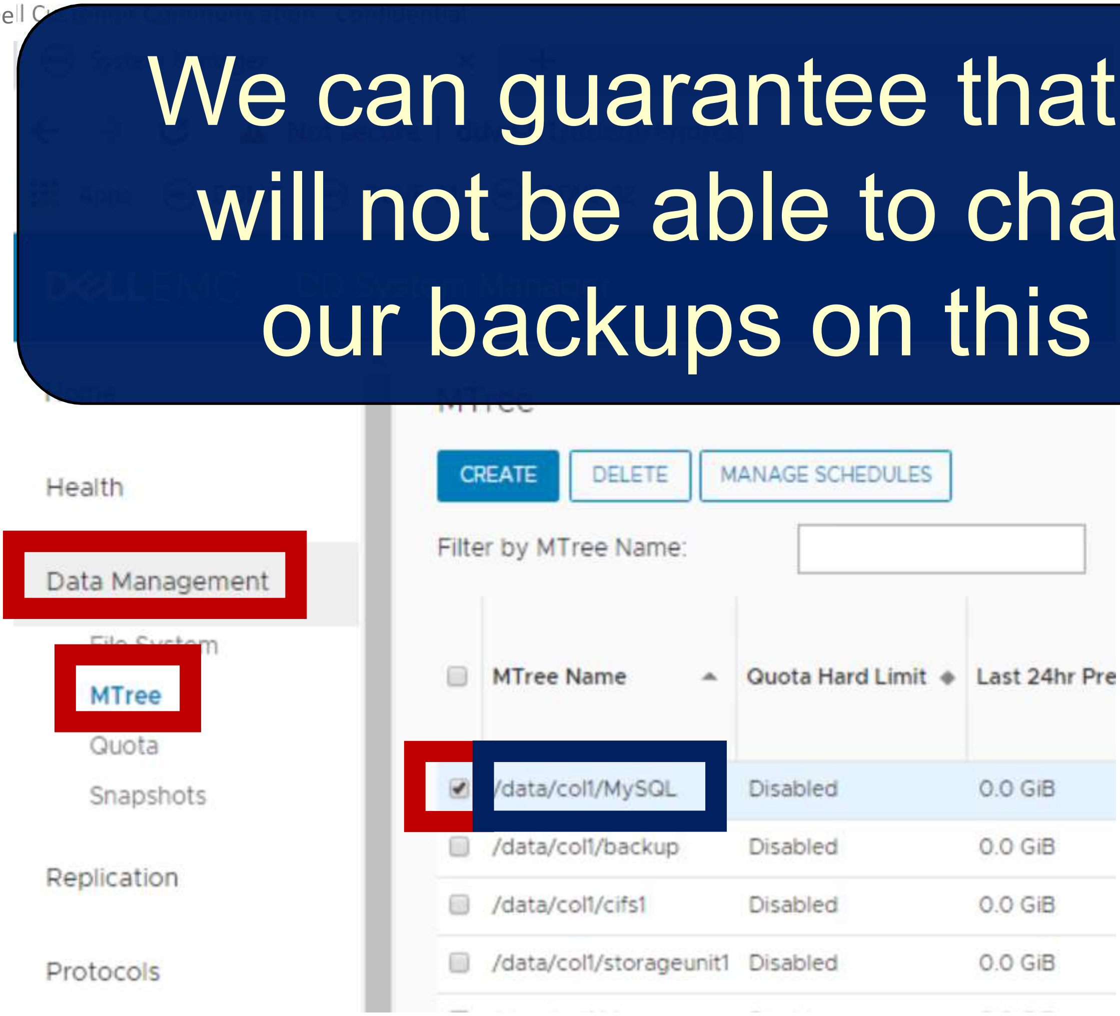
Anyhow, we can ask ourselves question:

What if our environments will be ransomwared?

Will this MySQL disk on Data Domain be encrypted as well?

This would be the real **DISASTER**!

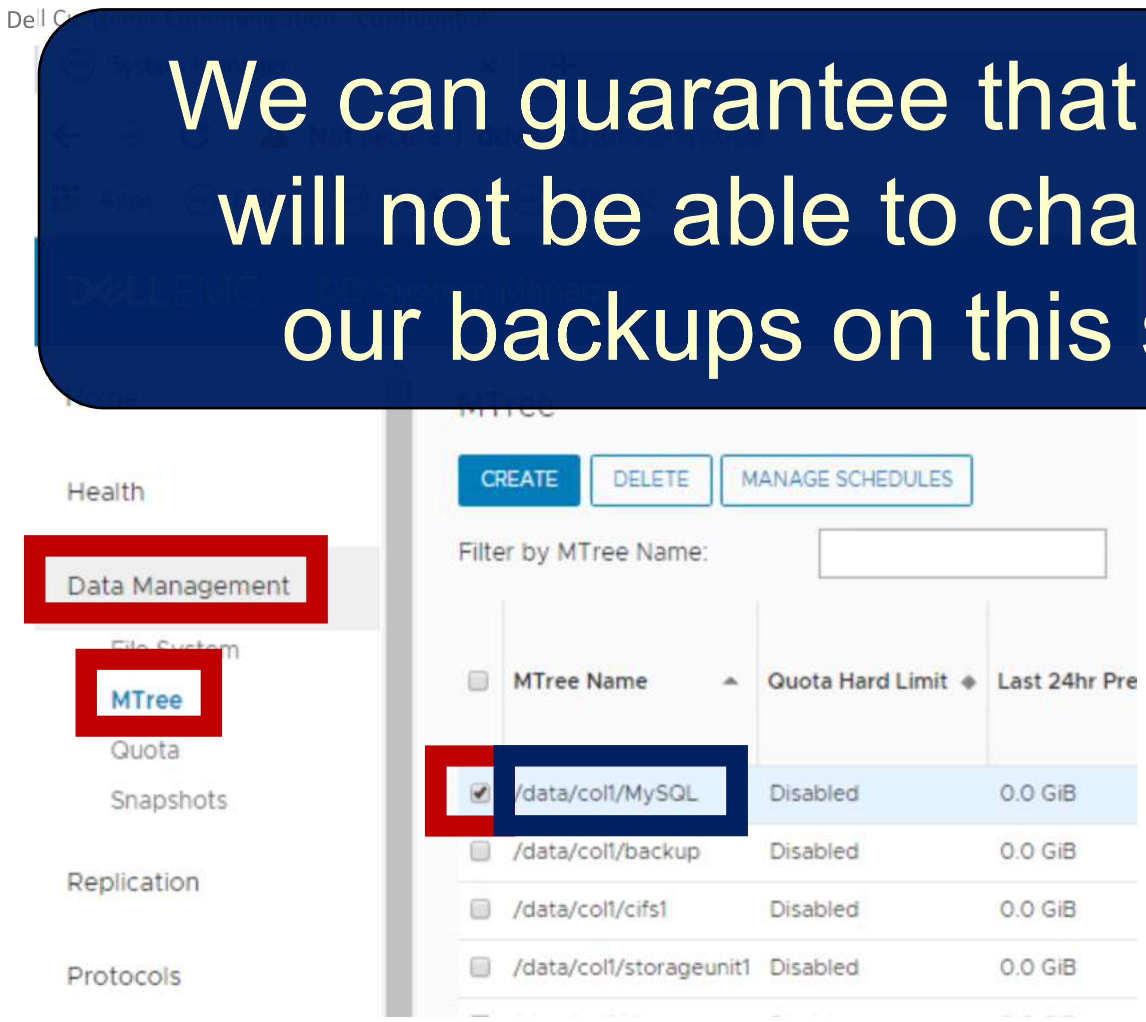
We can guarantee that ransomware will not be able to change / delete our backups on this share disk



Filter by MTree Name:

☐	MTree Name ▲	Quota Hard Limit ◆	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
☐	/data/col1/backup	Disabled	0.0 GiB
☐	/data/col1/cifs1	Disabled	0.0 GiB
☐	/data/col1/storageunit1	Disabled	0.0 GiB

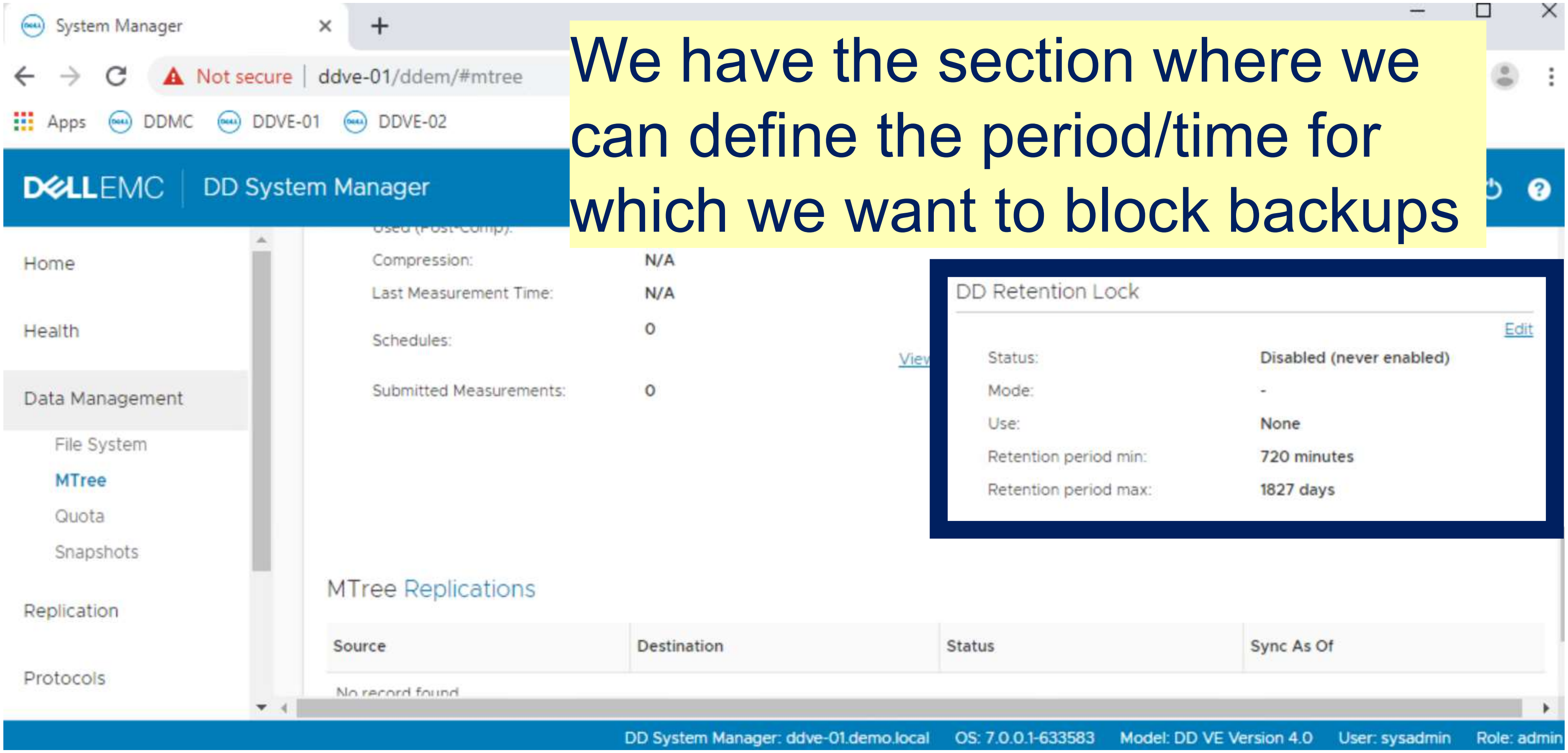
We can guarantee that ransomware will not be able to change / delete our backups on this share disk



Filter by MTree Name:

□	MTree Name	Quota Hard Limit	Last 24hr Pre
☑	/data/col1/MySQL	Disabled	0.0 GiB
□	/data/col1/backup	Disabled	0.0 GiB
□	/data/col1/cifs1	Disabled	0.0 GiB
□	/data/col1/storageunit1	Disabled	0.0 GiB

Let’s go down with the page



We have the section where we can define the period/time for which we want to block backups

Compression:	N/A
Last Measurement Time:	N/A
Schedules:	0
Submitted Measurements:	0

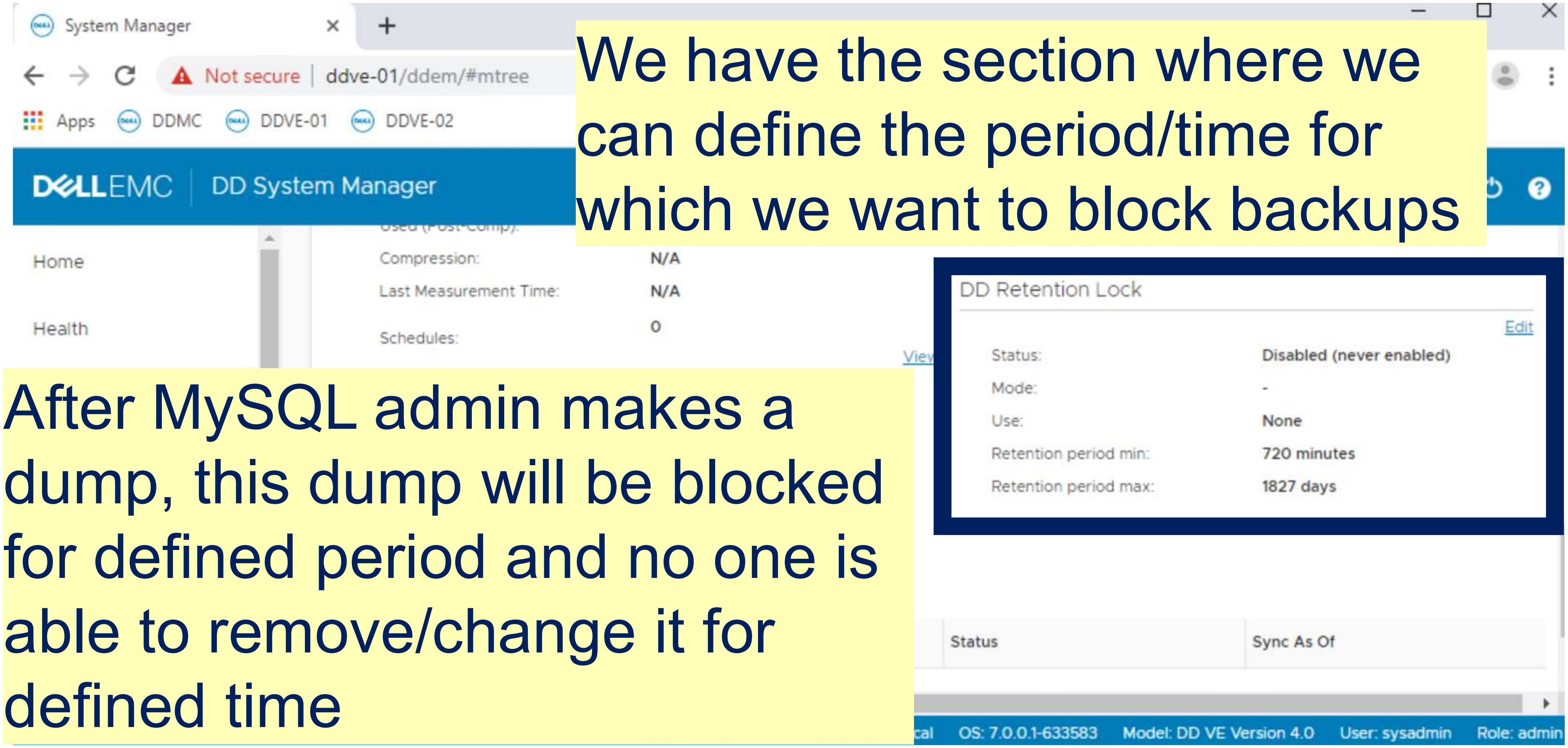
DD Retention Lock

Status:	Disabled (never enabled)
Mode:	-
Use:	None
Retention period min:	720 minutes
Retention period max:	1827 days

MTree Replications

Source	Destination	Status	Sync As Of
No record found			

DD System Manager: ddve-01.demo.local OS: 7.0.0.1-633583 Model: DD VE Version 4.0 User: sysadmin Role: admin



We have the section where we can define the period/time for which we want to block backups

After MySQL admin makes a dump, this dump will be blocked for defined period and no one is able to remove/change it for defined time

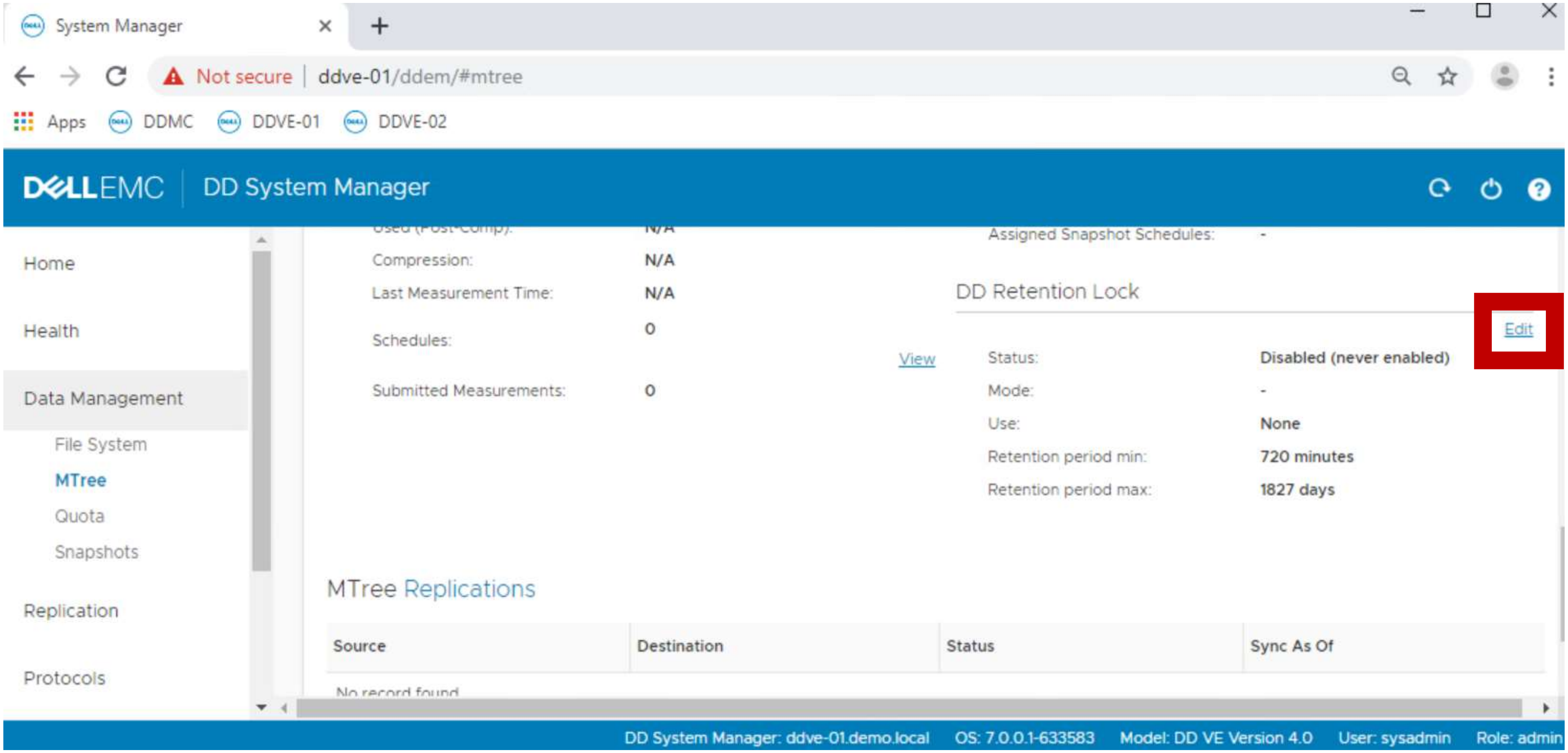
Compression:	N/A
Last Measurement Time:	N/A
Schedules:	0

DD Retention Lock

Status:	Disabled (never enabled)
Mode:	-
Use:	None
Retention period min:	720 minutes
Retention period max:	1827 days

Status	Sync As Of

OS: 7.0.0.1-633583 Model: DD VE Version 4.0 User: sysadmin Role: admin



Used (Post-Comp): N/A

Compression: N/A

Last Measurement Time: N/A

Schedules: 0

Submitted Measurements: 0

Assigned Snapshot Schedules: -

DD Retention Lock

Status: Disabled (never enabled)

Mode: -

Use: None

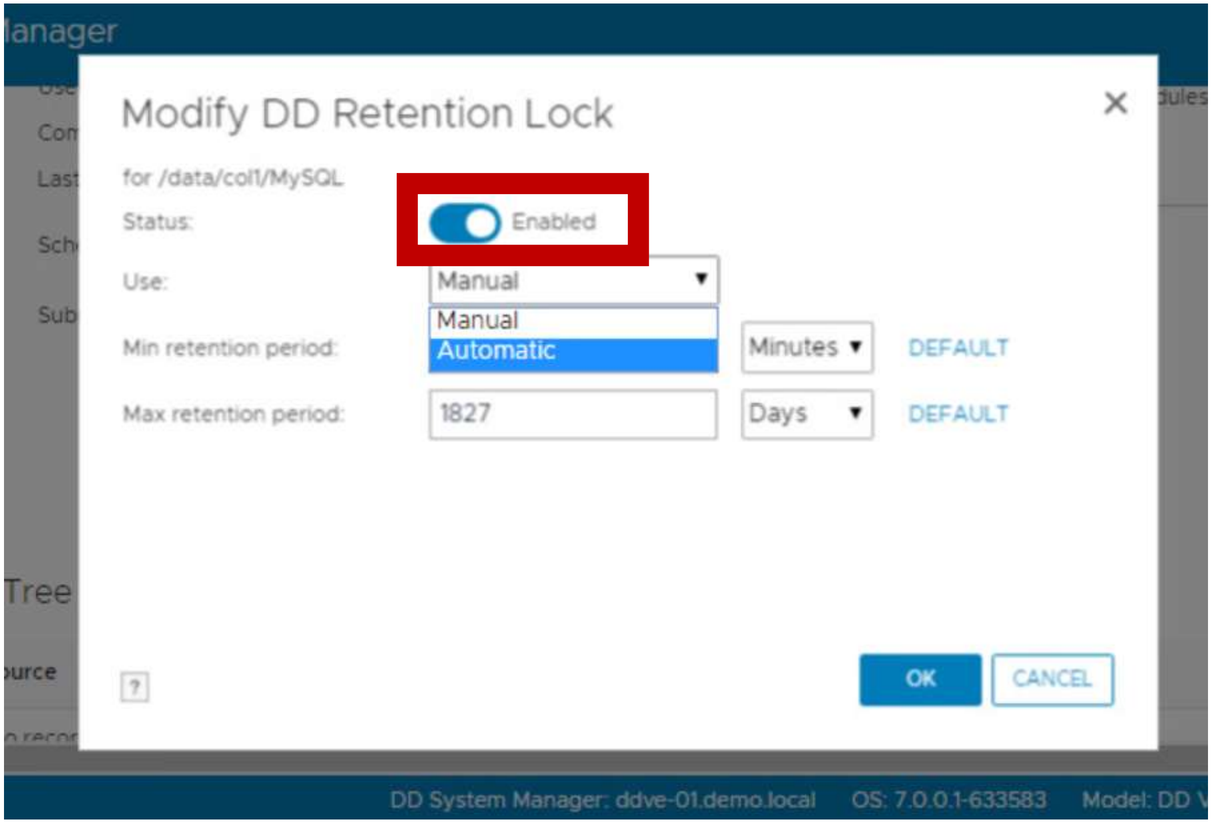
Retention period min: 720 minutes

Retention period max: 1827 days

MTree Replications

Source	Destination	Status	Sync As Of
No record found			

DD System Manager: ddve-01.demo.local OS: 7.0.0.1-633583 Model: DD VE Version 4.0 User: sysadmin Role: admin



Modify DD Retention Lock

for /data/col1/MySQL

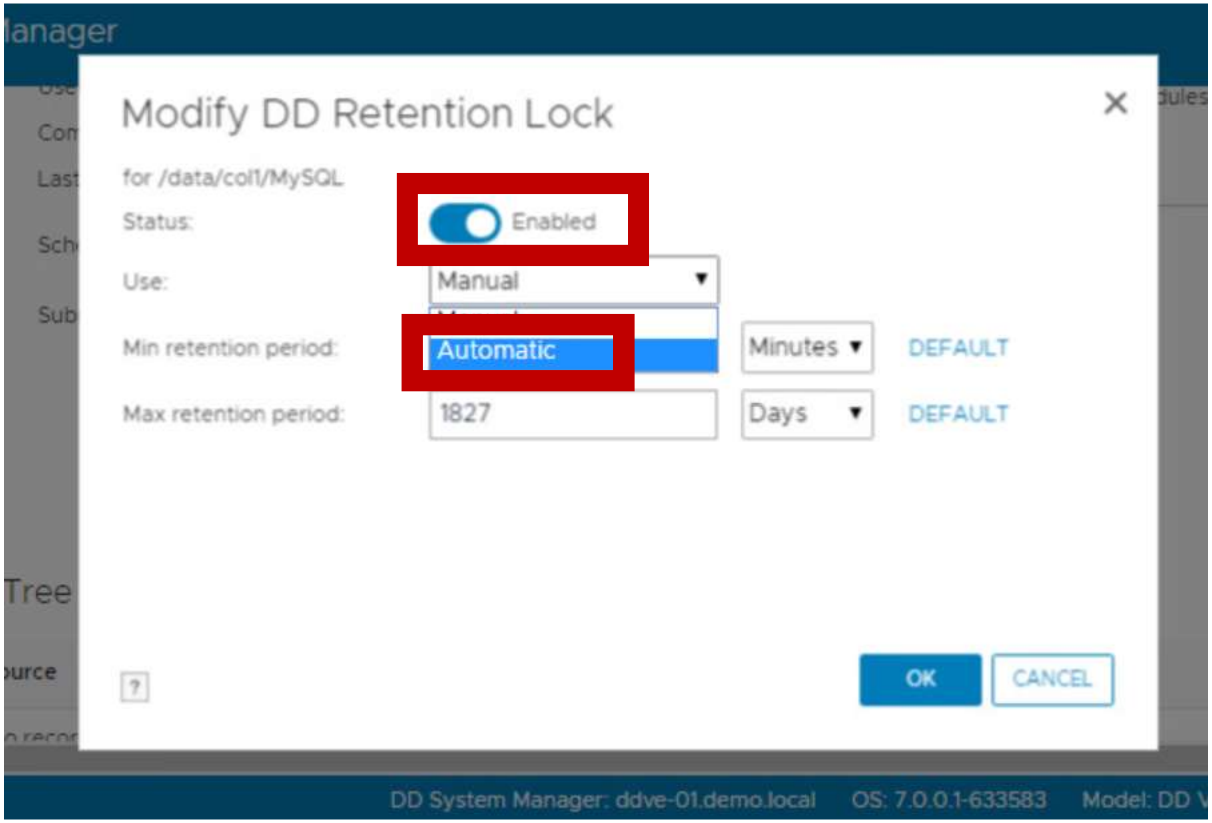
Status: Enabled

Use: Manual

Min retention period: Minutes

Max retention period: 1827 Days

DD System Manager: ddve-01.demo.local OS: 7.0.0.1-633583 Model: DD V



Modify DD Retention Lock

for /data/col1/MySQL

Status: Enabled

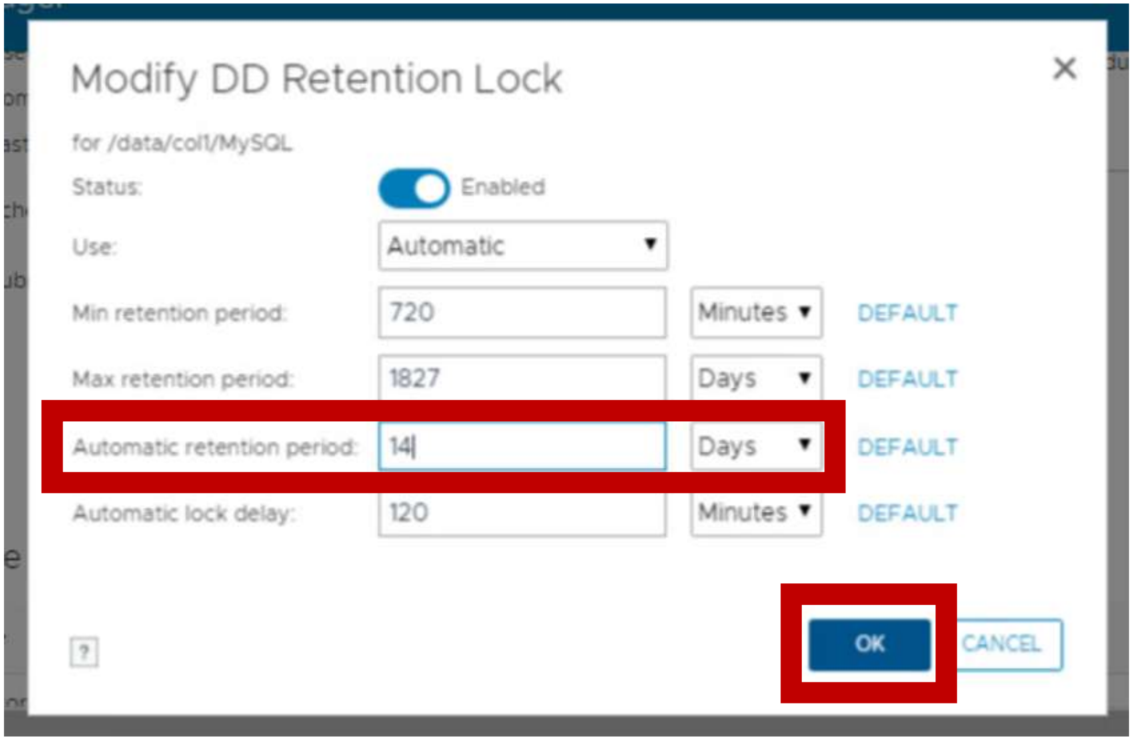
Use: Manual

Automatic

Min retention period: Minutes

Max retention period: 1827 Days

We can define period for how long we want Data Domain to block against deletion or change any backups written to this MySQL shared disk



Modify DD Retention Lock

for /data/col1/MySQL

Status: Enabled

Use: Automatic

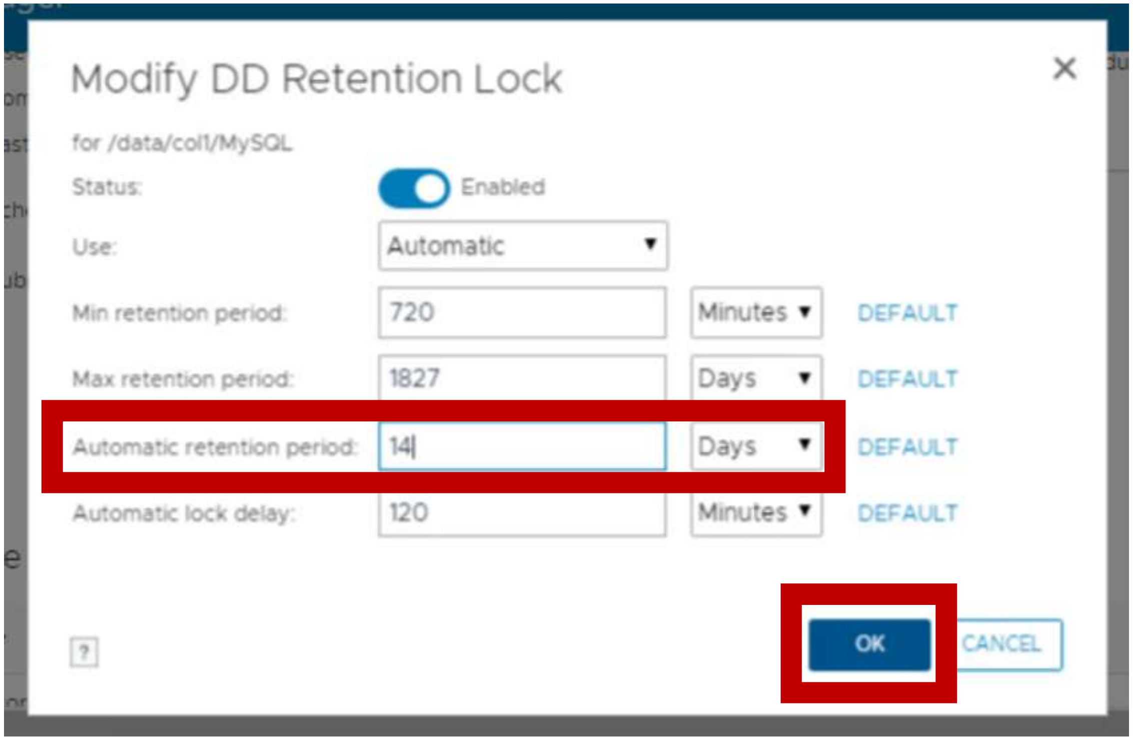
Min retention period: 720 Minutes

Max retention period: 1827 Days

Automatic retention period: 14 Days

Automatic lock delay: 120 Minutes

We can define period for how long we want Data Domain to block against deletion or change any backups written to this MySQL shared disk



Modify DD Retention Lock

for /data/col1/MySQL

Status: Enabled

Use: Automatic

Min retention period: 720 Minutes

Max retention period: 1827 Days

Automatic retention period: 14 Days

Automatic lock delay: 120 Minutes

Here we see block for 14 days.

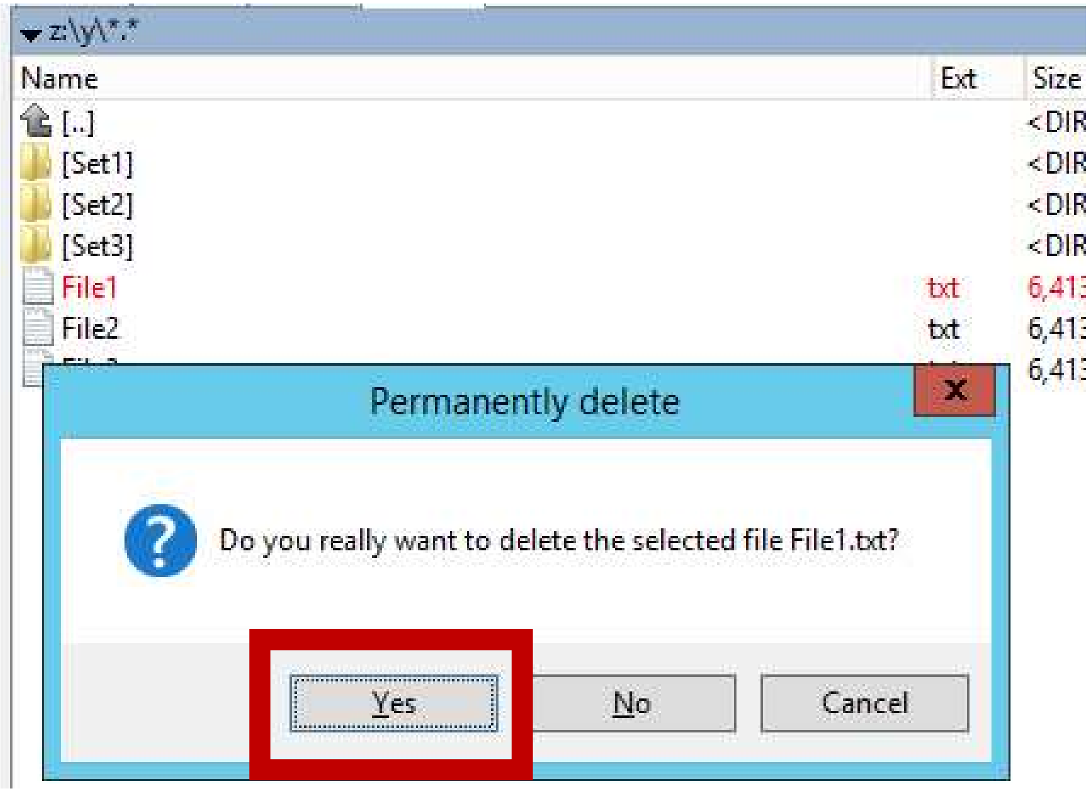
Anyhow 30 days for our security shall be setup

And that it all!

And that it all!

If there is ransomware attack, MySQL admin can restore his databases from Data Domain

Ransomware is not able
to destroy backups on this share
laying on **Data Domain**
with **Retention Lock**

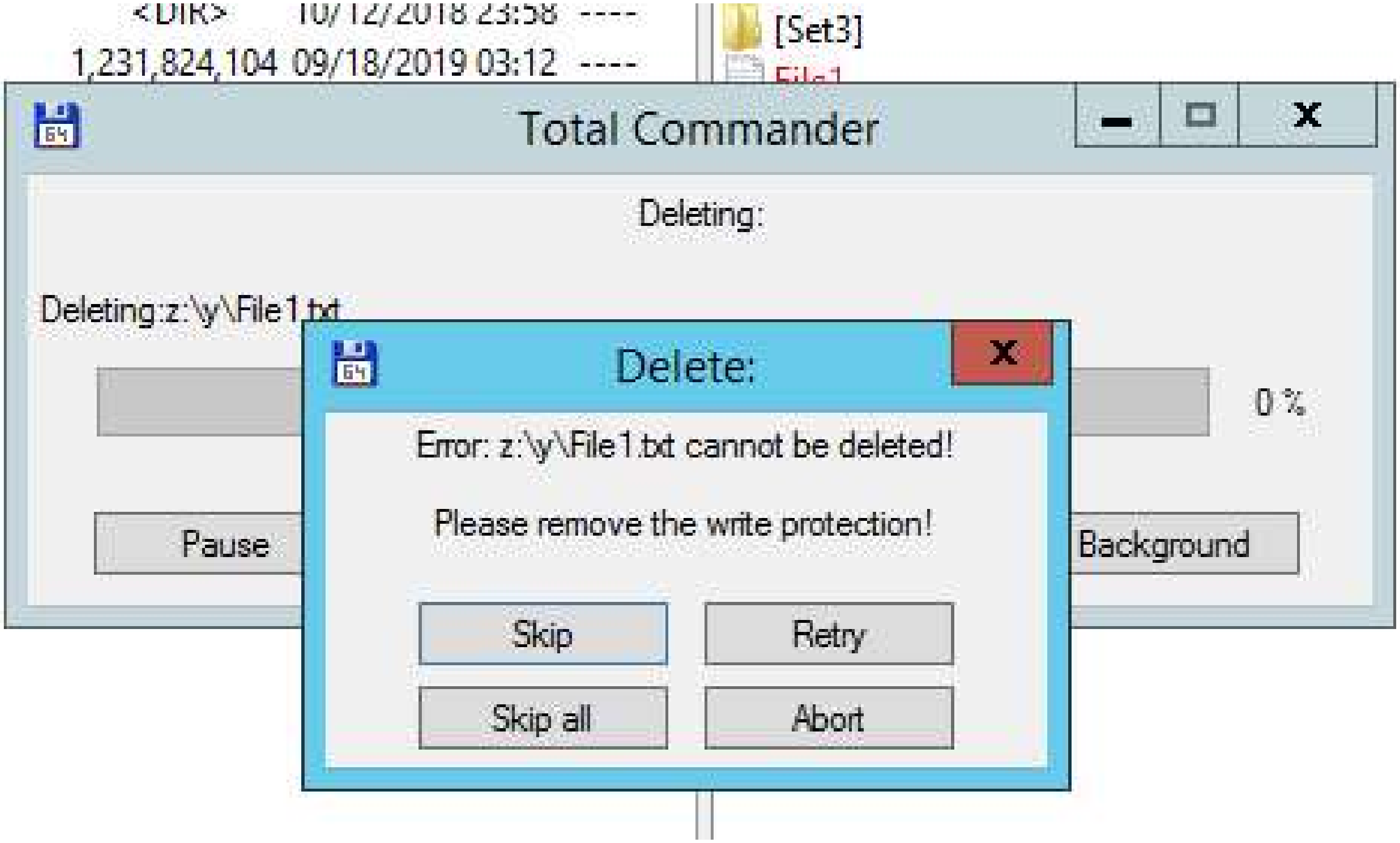


z:\y\*.*

Name	Ext	Size
[..]		<DIR
[Set1]		<DIR
[Set2]		<DIR
[Set3]		<DIR
File1	txt	6,41
File2	txt	6,41
		6,41

Permanently delete

Do you really want to delete the selected file File1.txt?



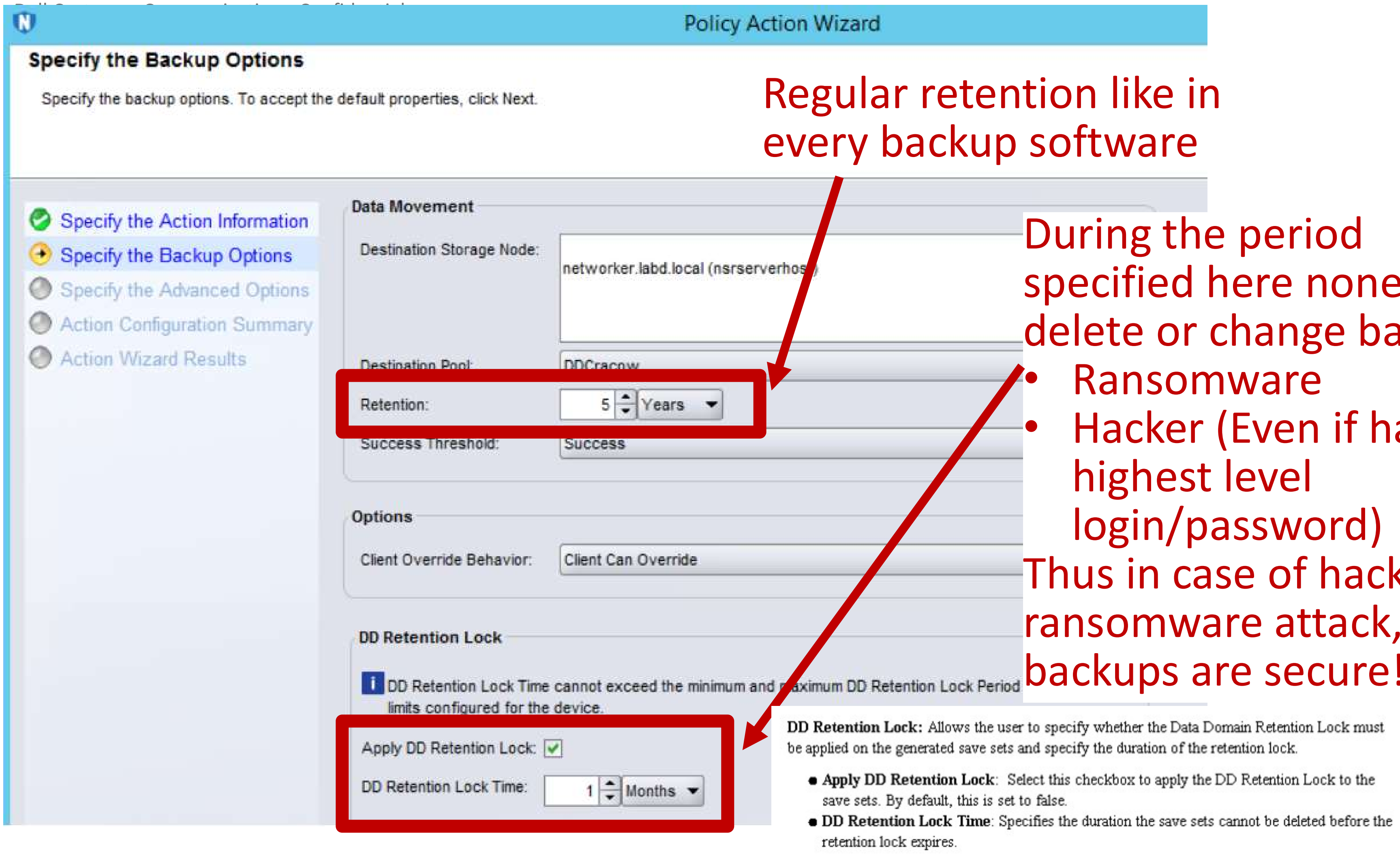
```
<DIR>       10/12/2018 23:58 ----
1,231,824,104 09/18/2019 03:12 ----
```

Deleting:z:\y\File1.txt

Error: z:\y\File1.txt cannot be deleted!

Please remove the write protection!

The best approach is to setup
Retention Lock from backup software level



Policy Action Wizard

Specify the Backup Options

Specify the backup options. To accept the default properties, click Next.

Specify the Action Information
Specify the Backup Options
Specify the Advanced Options
Action Configuration Summary
Action Wizard Results

Data Movement

Destination Storage Node: networker.labd.local (nsrserverhos

Destination Pool: DDCracow

Retention: 5 Years

Success Threshold: Success

Options

Client Override Behavior: Client Can Override

DD Retention Lock

DD Retention Lock Time cannot exceed the minimum and maximum DD Retention Lock Period limits configured for the device.

Apply DD Retention Lock: ☑

DD Retention Lock Time: 1 Months

Regular retention like in every backup software

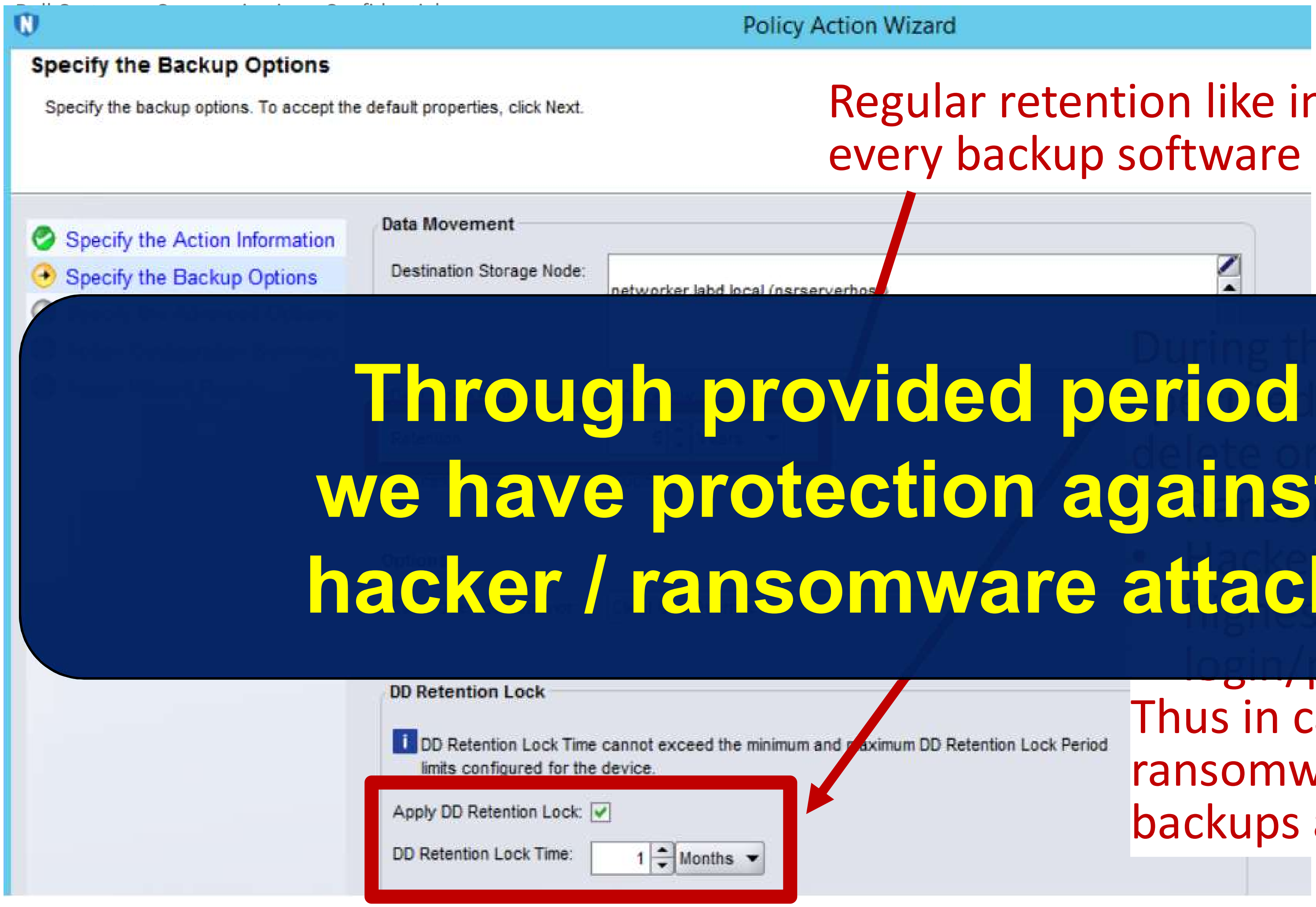
During the period specified here none can delete or change backups

- Ransomware
- Hacker (Even if has highest level login/password)

Thus in case of hacker / ransomware attack, our backups are secure!

DD Retention Lock: Allows the user to specify whether the Data Domain Retention Lock must be applied on the generated save sets and specify the duration of the retention lock.

- **Apply DD Retention Lock**: Select this checkbox to apply the DD Retention Lock to the save sets. By default, this is set to false.
- **DD Retention Lock Time**: Specifies the duration the save sets cannot be deleted before the retention lock expires.



Policy Action Wizard

Specify the Backup Options

Specify the backup options. To accept the default properties, click Next.

✓ Specify the Action Information
➔ Specify the Backup Options

Data Movement

Destination Storage Node: networker.labd.local (nsrserverhos

DD Retention Lock

DD Retention Lock Time cannot exceed the minimum and maximum DD Retention Lock Period limits configured for the device.

Apply DD Retention Lock: ☑

DD Retention Lock Time: 1 Months

Regular retention like in every backup software

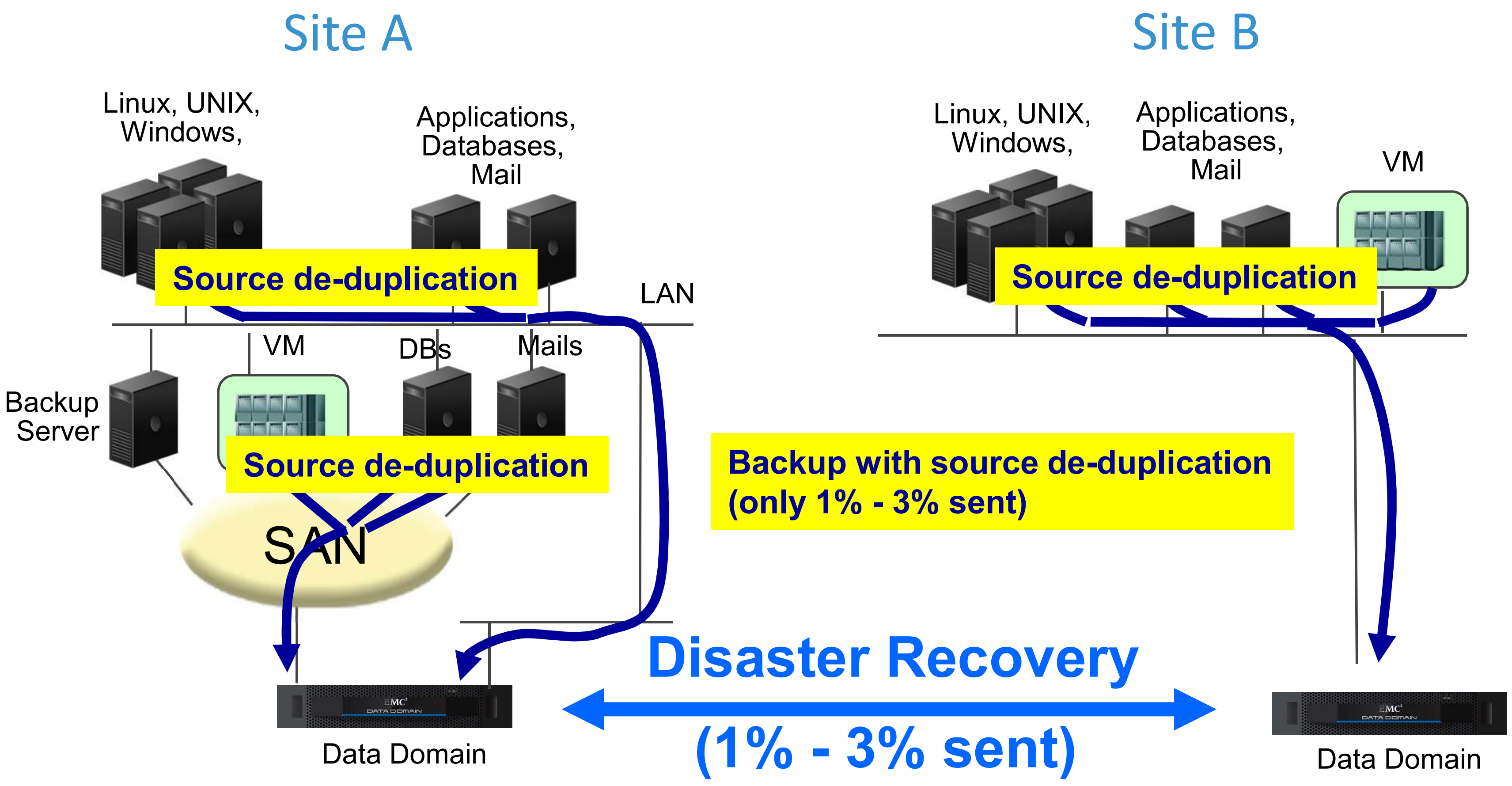
During the period specified here none can delete or change backups

- Ransomware
- Hacker (Even if has highest level login/password)

Thus in case of hacker / ransomware attack, our backups are secure!

Through provided period we have protection against hacker / ransomware attack

Replication



Backup with source de-duplication (only 1% - 3% sent)

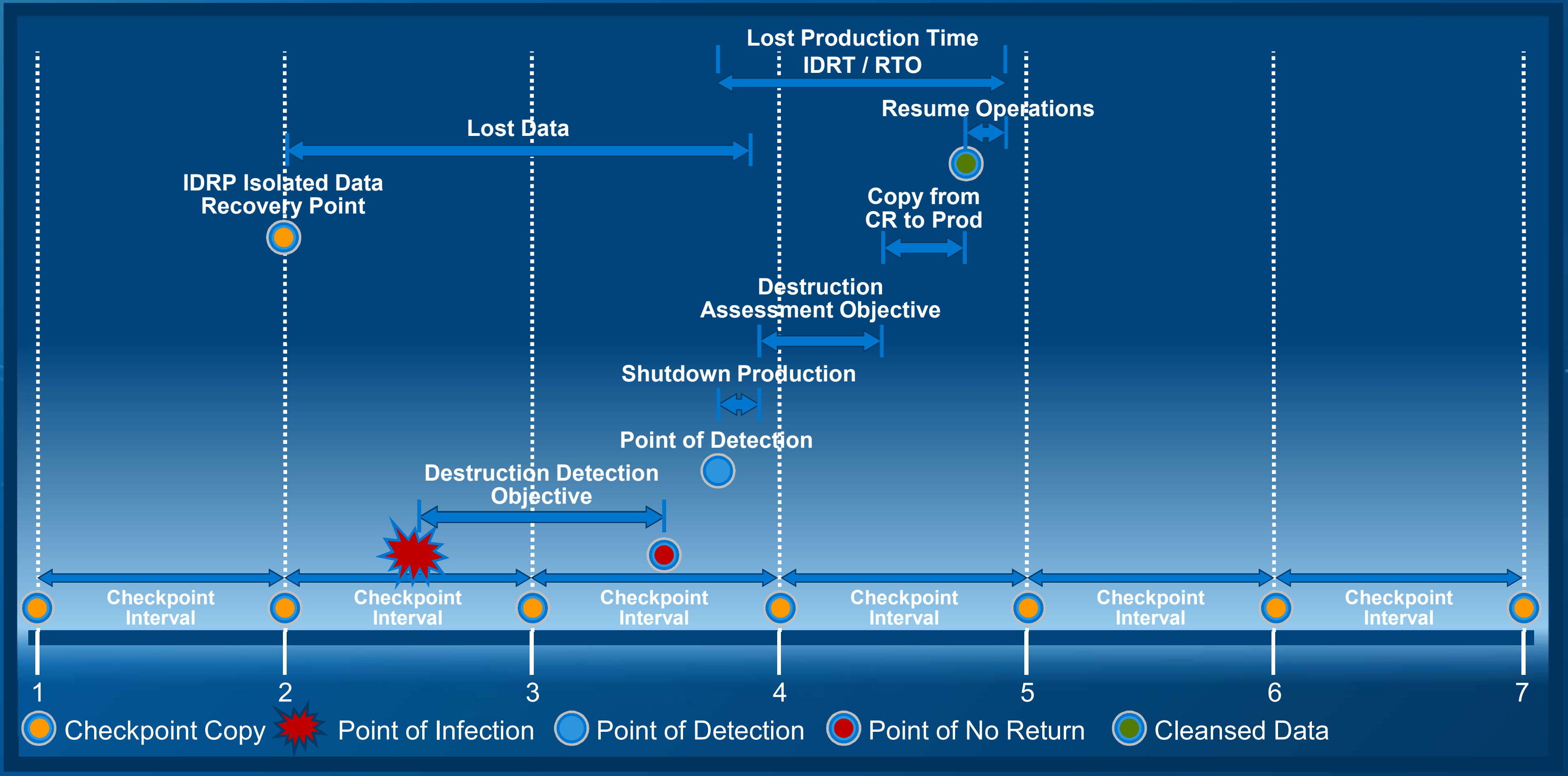
Disaster Recovery

(1% - 3% sent)

Cyber Recovery

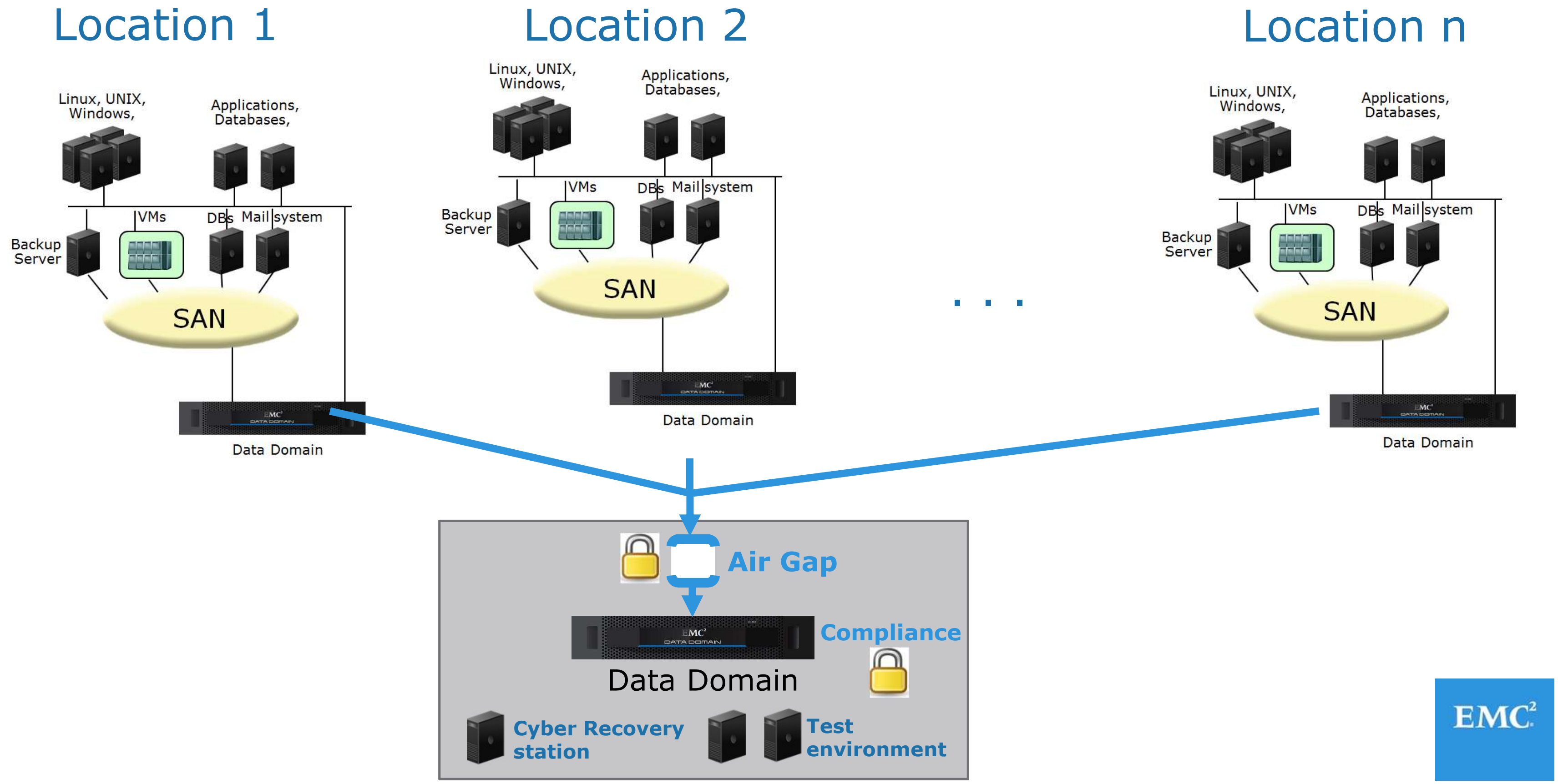
What? Why? How?

Recovery Timeline

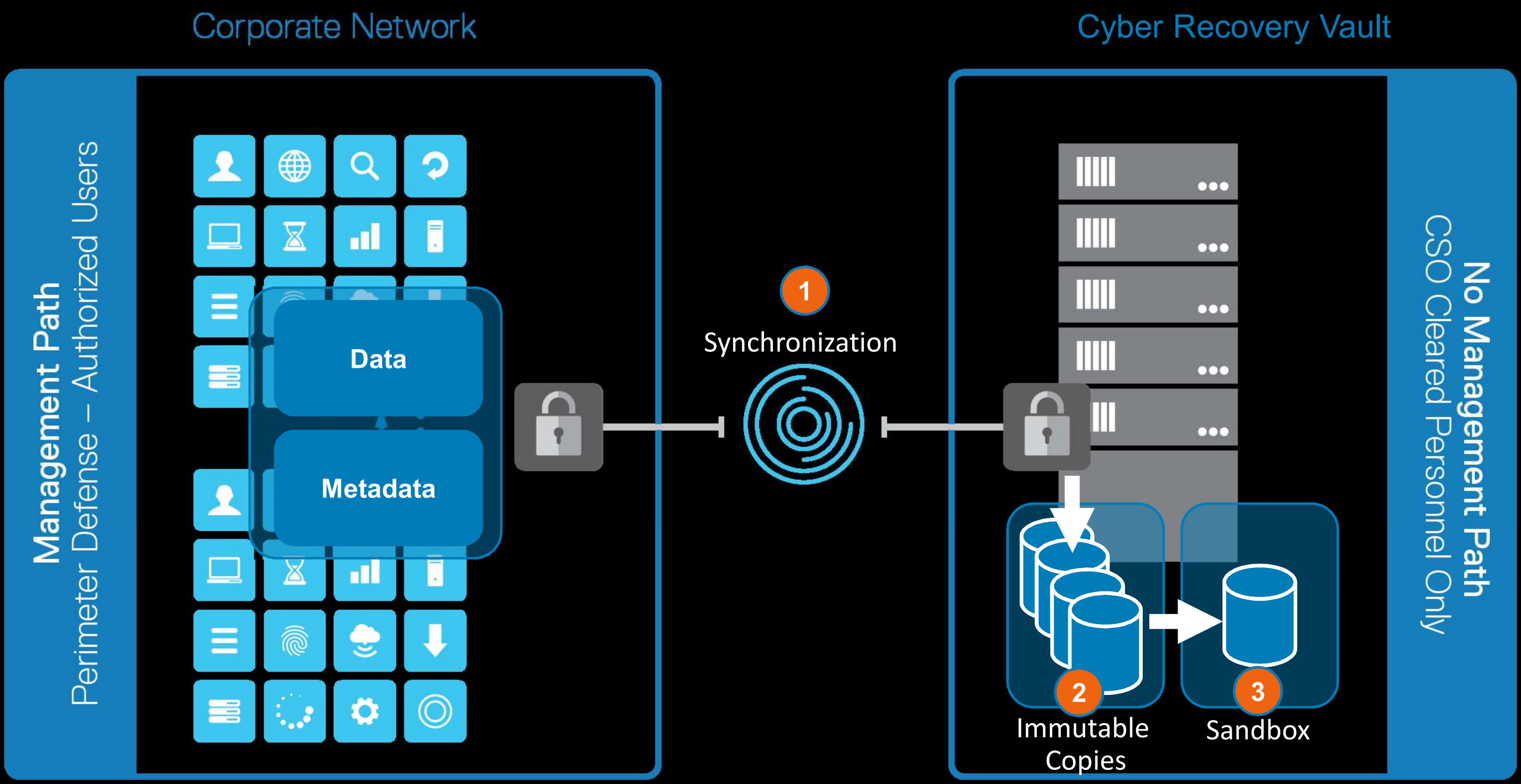


MUTLI-SITE ENVIRONMENT

ARCHITECTURE OF CYBER RECOVERY SOLUTION



Dell EMC Cyber Recovery



Corporate Network

Cyber Recovery Vault

Management Path

Perimeter Defense – Authorized Users

Data

Metadata

1

Synchronization

2

Immutable Copies

3

Sandbox

No Management Path

CSO Cleared Personnel Only

Proposed: Exposures Resolved and Remaining

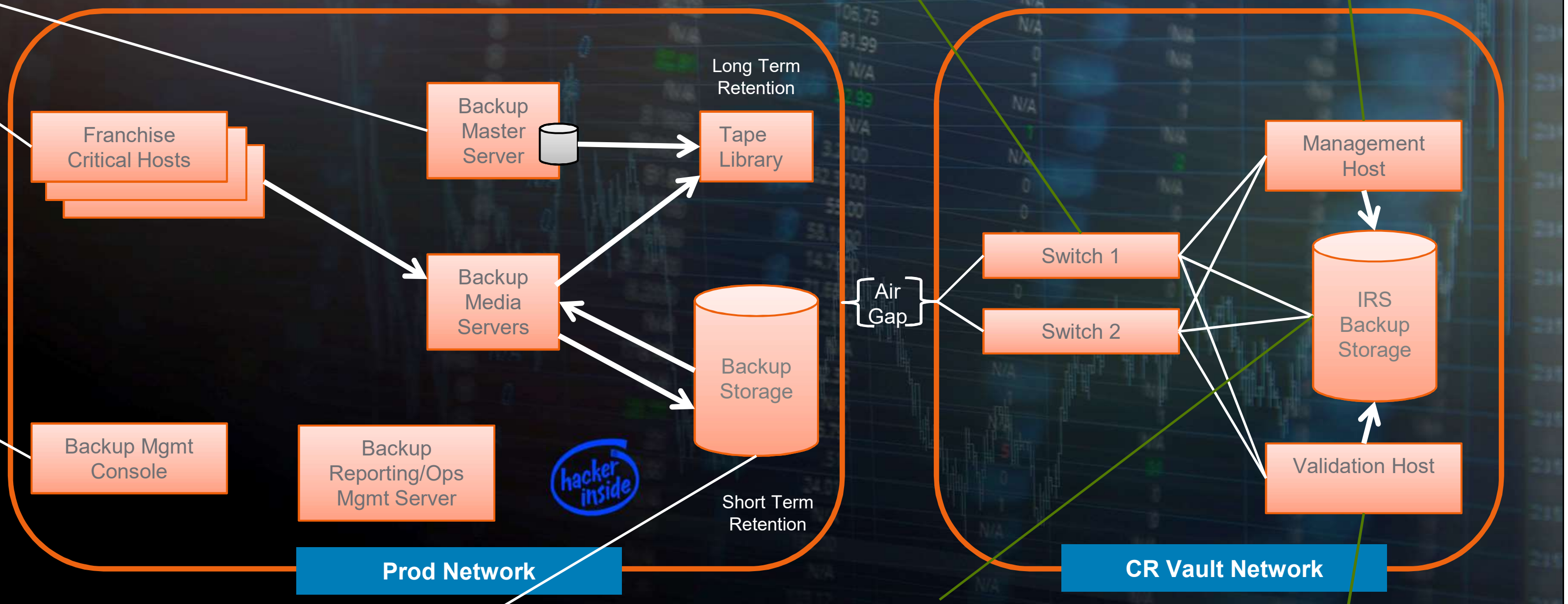
Non-HA backup server represents single point of failure

Backup images may be prematurely expired without authorization

Ineffective role-based access controls may allow unintended access to backup data

Switches are only logical point of entry and open only ports required for scheduled replication and alerting

Management host opens/closes ports based on schedule and DD probes. Applies Retention Lock on DD.



Franchise Critical Hosts

Backup Master Server

Long Term Retention

Tape Library

Backup Media Servers

Backup Storage

Short Term Retention

Backup Mgmt Console

Backup Reporting/Ops Mgmt Server

hacker inside

Prod Network

Air Gap

Switch 1

Switch 2

Management Host

IRS Backup Storage

Validation Host

CR Vault Network

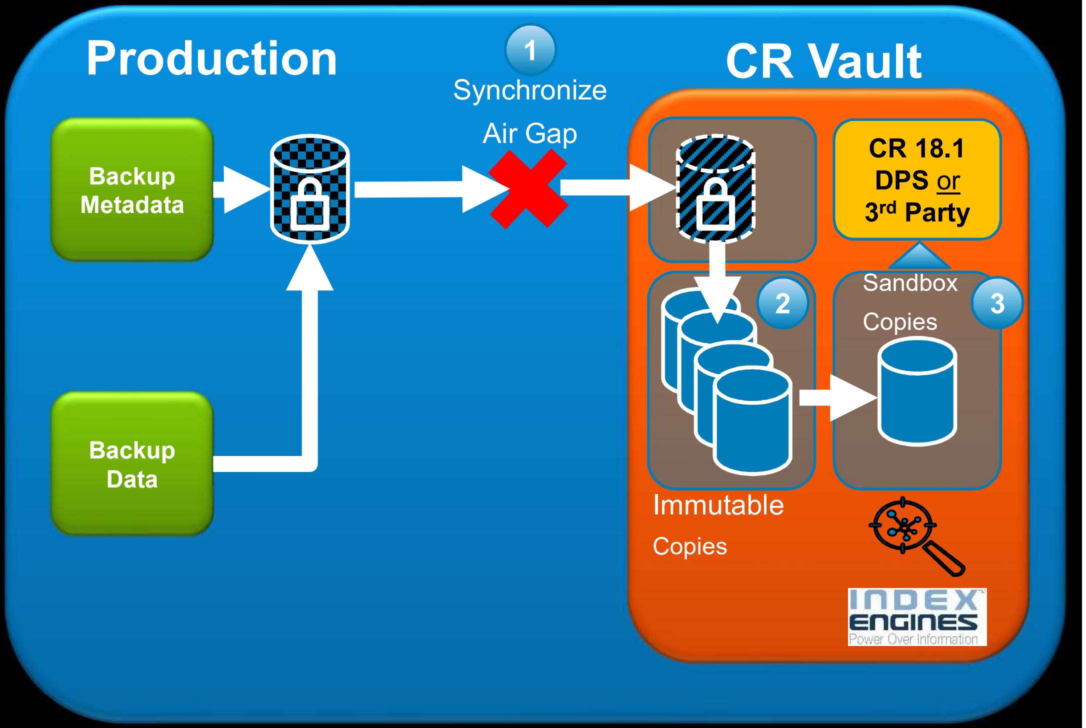
Backup copies are not isolated or logically segregated from network

CR copies are isolated and Compliance/WORM locked. No destructive actions without dual role authentication

Validation host ensures usability of CR copies and alerting of corruption

Cyber Recovery

- End-to-End workflow automation SW
- Runs only in CR Vault
- Create isolated gold copies
- Robust REST API framework enables analytics with AI/ML for malware (incl. Ransomware)
- Modern UI / UX experience
- Easy to deploy and maintain



Production

Backup Metadata

Backup Data

1 Synchronize Air Gap

CR Vault

CR 18.1 DPS or 3rd Party

2

Immutable Copies

Sandbox Copies 3

INDEX ENGINES Power Over Information

Cyber Sense

Check!

Why CyberSense?

- We need to protect against insiders and advanced threat actors, not just basic ransomware

Why CyberSense?

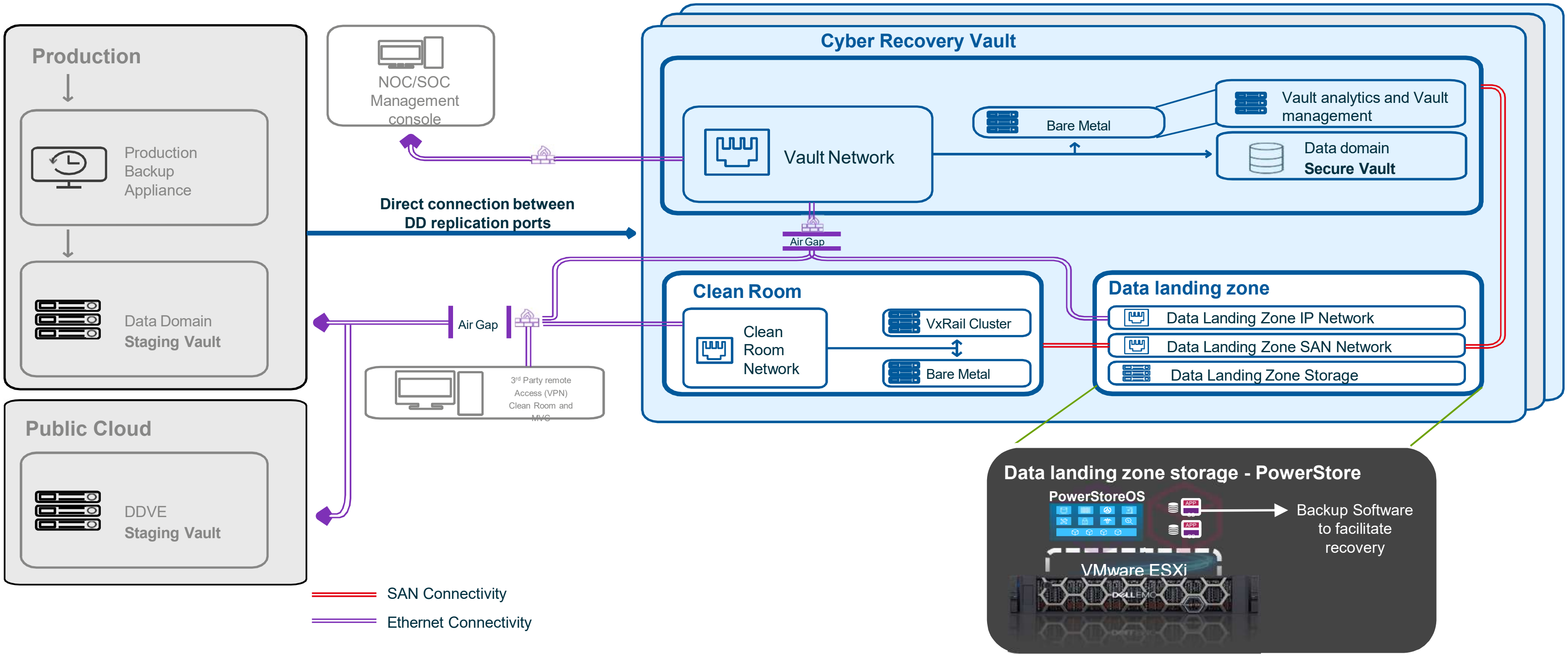
- The only approach that will deliver a high level of confidence in detecting hidden and sophisticated corruption techniques is to deploy comprehensive content-based analytics right from the start.
  - *Most solutions use metadata-only analytics and only look at basic information about a file or database.*
  - *Some solutions use a multi-pass approach that uses metadata analytics on the first pass and then sends the suspect files for content-based analytics on a second cloud-based pass. This workflow is flawed and will miss most sophisticated attack vectors, providing a false sense of confidence.*

Cyber Recovery

Real Architecture

Cyber Recovery Vault with PowerStore

Secure Landing Zone for recovery of data facilitated by PowerStore



Production

Production Backup Appliance

Data Domain **Staging Vault**

Public Cloud

DDVE **Staging Vault**

NOC/SOC Management console

Direct connection between DD replication ports

Air Gap

3rd Party remote Access (VPN) Clean Room and MVC

Cyber Recovery Vault

Vault Network

Bare Metal

Vault analytics and Vault management

Data domain **Secure Vault**

Air Gap

Clean Room

Clean Room Network

VxRail Cluster

Bare Metal

Data landing zone

Data Landing Zone IP Network

Data Landing Zone SAN Network

Data Landing Zone Storage

Data landing zone storage - PowerStore

PowerStoreOS

VMware ESXi

Backup Software to facilitate recovery

🟥 SAN Connectivity

🟪 Ethernet Connectivity

Why PowerStore

- PowerStore X’s built in Hypervisor allows for Cyber Recovery to completely isolate the recovery process outside of the vault and facilitate rebuild on the PowerStore
- PowerStore can then either vMotion recovered hosts or present storage to hosts in the Clean Room, ready for rebuild
- Provides a faster means for data recovery out of the vault
- Only PowerStore, with it’s built in hypervisor, has the ability to do this across the portfolio.

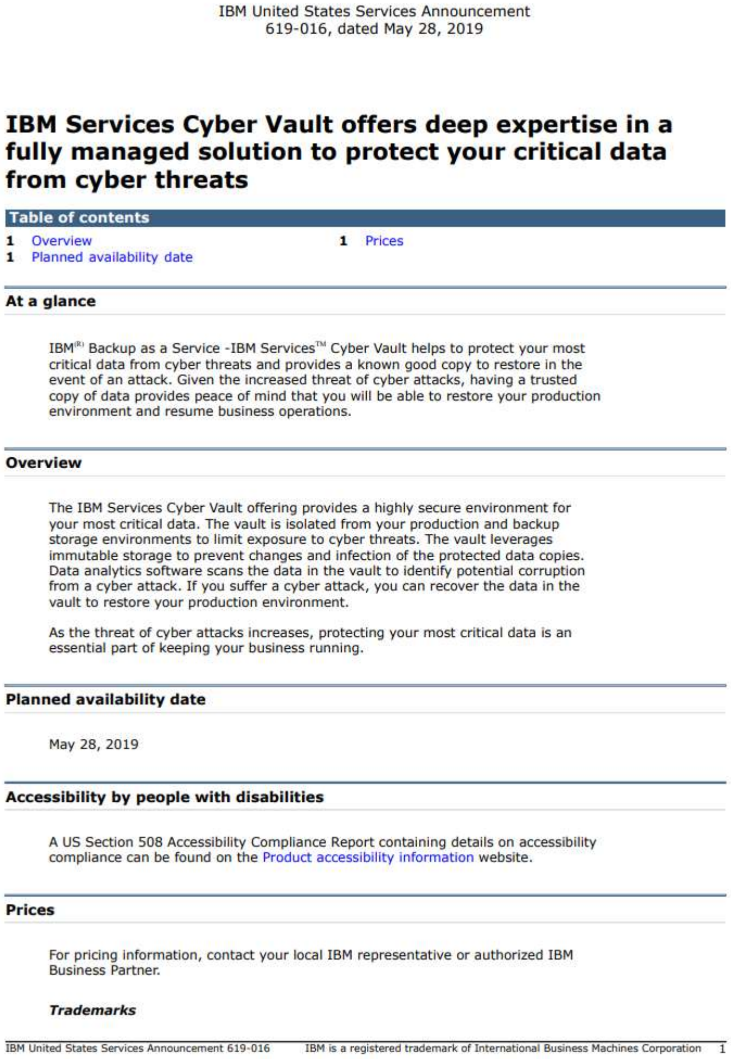
Cyber Recovery

Reality

IBM Cyber Recovery offering

IBM offering is based on Cyber Recovery solution

https://www.ibm.com/downloads/cas/US-ENUS619-016-CA



IBM United States Services Announcement
619-016, dated May 28, 2019

IBM Services Cyber Vault offers deep expertise in a fully managed solution to protect your critical data from cyber threats

Table of contents

At a glance

IBM[(R)] Backup as a Service -IBM Services[TM] Cyber Vault helps to protect your most critical data from cyber threats and provides a known good copy to restore in the event of an attack. Given the increased threat of cyber attacks, having a trusted copy of data provides peace of mind that you will be able to restore your production environment and resume business operations.

Overview

The IBM Services Cyber Vault offering provides a highly secure environment for your most critical data. The vault is isolated from your production and backup storage environments to limit exposure to cyber threats. The vault leverages immutable storage to prevent changes and infection of the protected data copies. Data analytics software scans the data in the vault to identify potential corruption from a cyber attack. If you suffer a cyber attack, you can recover the data in the vault to restore your production environment.

As the threat of cyber attacks increases, protecting your most critical data is an essential part of keeping your business running.

Planned availability date

May 28, 2019

Accessibility by people with disabilities

A US Section 508 Accessibility Compliance Report containing details on accessibility compliance can be found on the Product accessibility information website.

Prices

For pricing information, contact your local IBM representative or authorized IBM Business Partner.

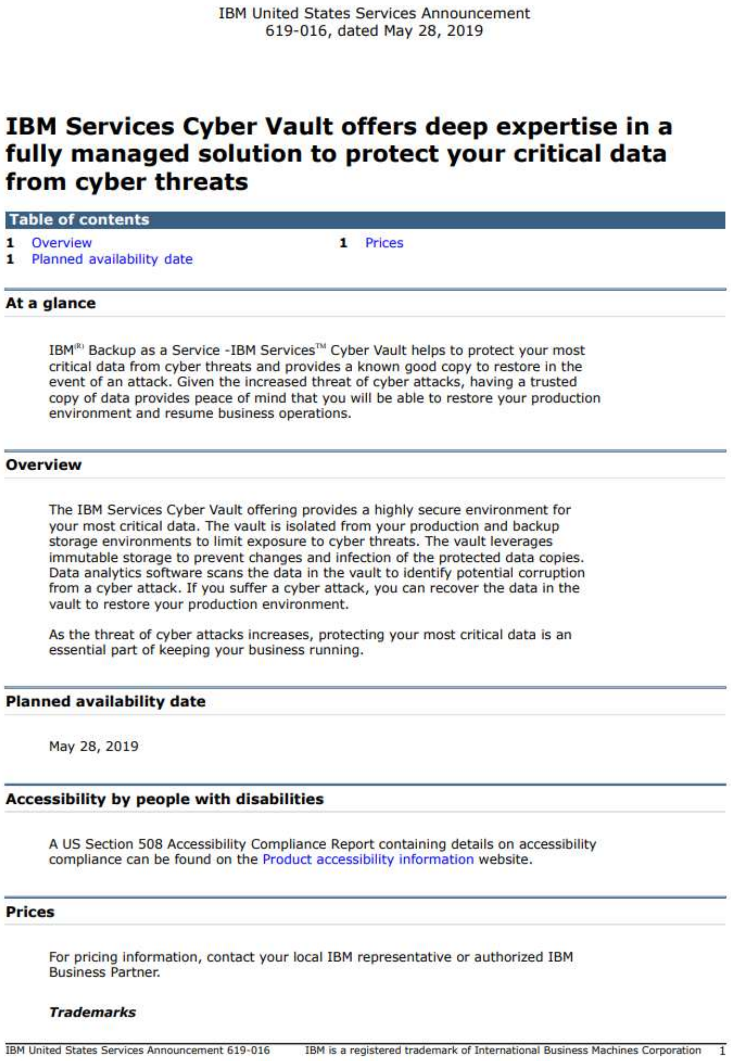
Trademarks

IBM United States Services Announcement 619-016 IBM is a registered trademark of International Business Machines Corporation 1

IBM utilizes the Cyber Vault solution using Dell Cyber Recovery technology. IBM adds-on the maintenance, incident response services and additional automation capabilities via Resiliency Orchestration.

Cyber Vault can be housed anywhere it is required – IBM, client or 3rd party site.

In addition, IBM has the ability to provide the additional WAN services that should be located at IBM or 3rd party site.



IBM United States Services Announcement
619-016, dated May 28, 2019

IBM Services Cyber Vault offers deep expertise in a fully managed solution to protect your critical data from cyber threats

Table of contents

At a glance

IBM(R) Backup as a Service -IBM Services™ Cyber Vault helps to protect your most critical data from cyber threats and provides a known good copy to restore in the event of an attack. Given the increased threat of cyber attacks, having a trusted copy of data provides peace of mind that you will be able to restore your production environment and resume business operations.

Overview

The IBM Services Cyber Vault offering provides a highly secure environment for your most critical data. The vault is isolated from your production and backup storage environments to limit exposure to cyber threats. The vault leverages immutable storage to prevent changes and infection of the protected data copies. Data analytics software scans the data in the vault to identify potential corruption from a cyber attack. If you suffer a cyber attack, you can recover the data in the vault to restore your production environment.

As the threat of cyber attacks increases, protecting your most critical data is an essential part of keeping your business running.

Planned availability date

May 28, 2019

Accessibility by people with disabilities

A US Section 508 Accessibility Compliance Report containing details on accessibility compliance can be found on the Product accessibility information website.

Prices

For pricing information, contact your local IBM representative or authorized IBM Business Partner.

Trademarks

IBM United States Services Announcement 619-016 IBM is a registered trademark of International Business Machines Corporation 1

The technology is based on Data Domain, CyberRecovery, … components provided as a service.
There are IBM value added features such as Global managed services on or off premises, Resiliency Orchestration tools, etc
Apart from security, one of the reasons IBM picked CR is because it is totally RESTAPI based, so they don't use the CR GUI, but make calls down to Cyber Recovery RESTAPIs from their single pane of glass for their admins.
Also IBM has tons of Data Domains at their Resiliency sites for test and development.

Dell Customer Communication - Confidential

Most of finfancial Customer expirience several cyber attacks per day

So far, every Customer that was using BOOST technology (secured login/password connection to media) were able to recover after Cyber Attack thanks to Data Domain.

Customer A
Having just Data Domain

Customer had 3 sites – 10TB each.
DD2200 was at one site, just backup to disk at 2 others

After Cyber Attack Customer was able to restore only from the site with DD2200.

Currently there is project for Data Domain in all 3 sites (DD2200 will be renewed in 1st site).

Customer B
Wise after issue

Customer called me and wanted to buy Data Domain.
He lost data because of ransmoware.

He knew this is for future.

Customer C
Having Cyber Recovery

The customer is a leading provider for the insurance industry of various digital services. It has ~4K VMs in many sites globally.

On April 17th the company was hit by a ransomware that shut down the entire IT ops.

The virus knew exactly how the network is constructed – sites, subnets, virtual centers etc., and attacked it in a very precise and coordinated manner.

Leaving the spy conspiracies aside, there is no doubt that some internal work was involved at some level.

The extortion attempt was for millions of dollars, so this is clearly a planned, targeted attack, rather than random pervasive hacking.

The malware disconnected all NICS and HBAs on every one of the 4,000 VMs, destroyed its GUI and shell, and encrypted all attached disks. Therefore, upon discovery, there was no way to approach the servers but manually, and run a fix (developed in the day after) on each server by the IT staff, no central deployment or anything similar. Furthermore, there was not even a template to start deploying new servers. It was the mere definition of a total loss disaster.

The customer is using Veeam for backup. They also have few DDs, one of them is a DDVE with CloudTier to AWS. Upon the encryption storm all the servers were damaged, and also all Veaam servers naturally, being on windows. In sites where the customer didn't invest in DD, all data was totally corrupted.

In the 2nd day, after realizing the scale of the hit, they immediately setup new Veeam servers to start restoring. Veeam server wasn’t installed correctly (too little resources), customer fixed it.
DD kept its integrity 100% !! please notice, that not only that there is no cyber recovery on these systems, but they didn’t even employ RL. The native hardening of DDOS and DDboost was enough to push back the attack.
Anyhow the attacked destroyed all backups where it was on a JBOD.

This company is giving services to the financial sector, where there is lots of regulation and a heavy weight for reputation. This company was in a serious risk to be closed if it weren’t for DD. I actually have a whatsapp saying "DD saved the day".

Cyber Recovery

Cost

10TB CyberSense: 32K Euro

xrem

Cyber Recovery

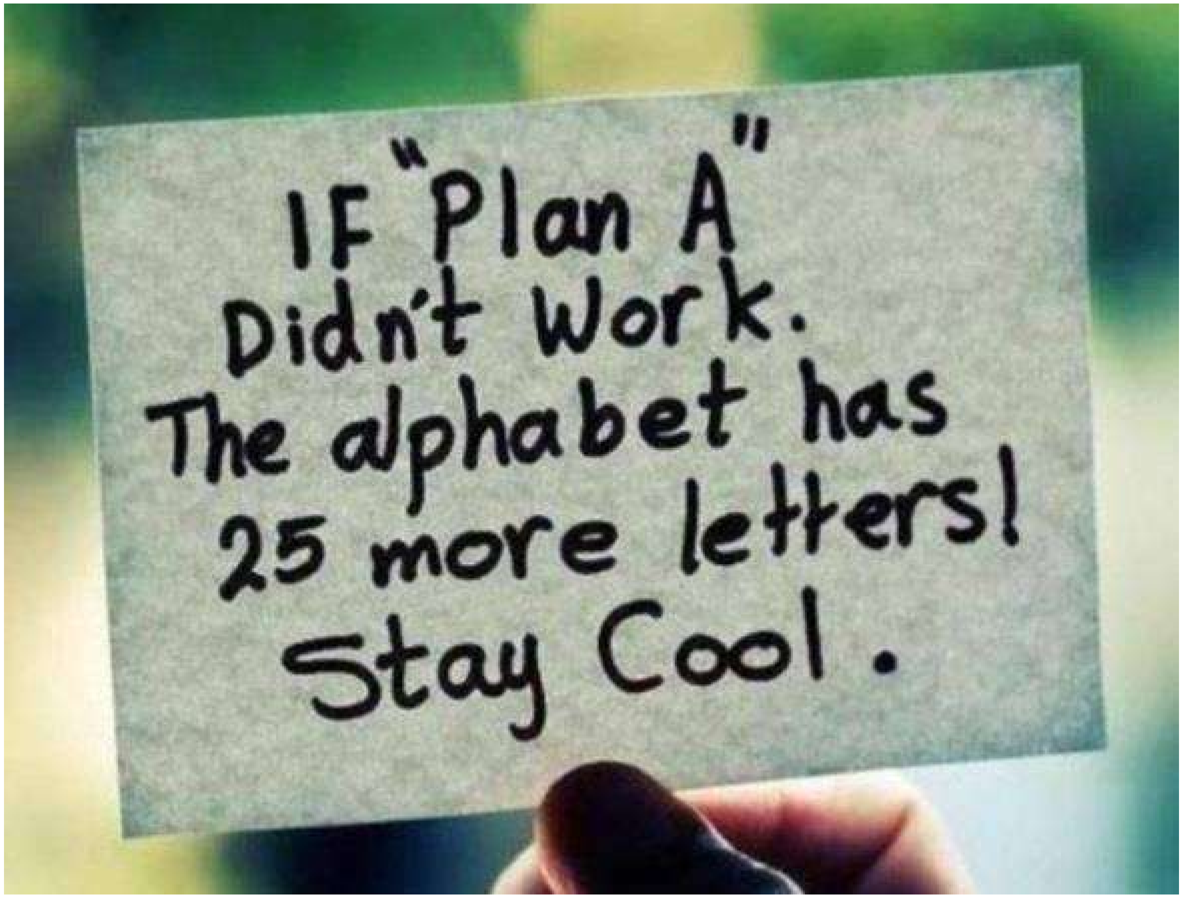
Materials

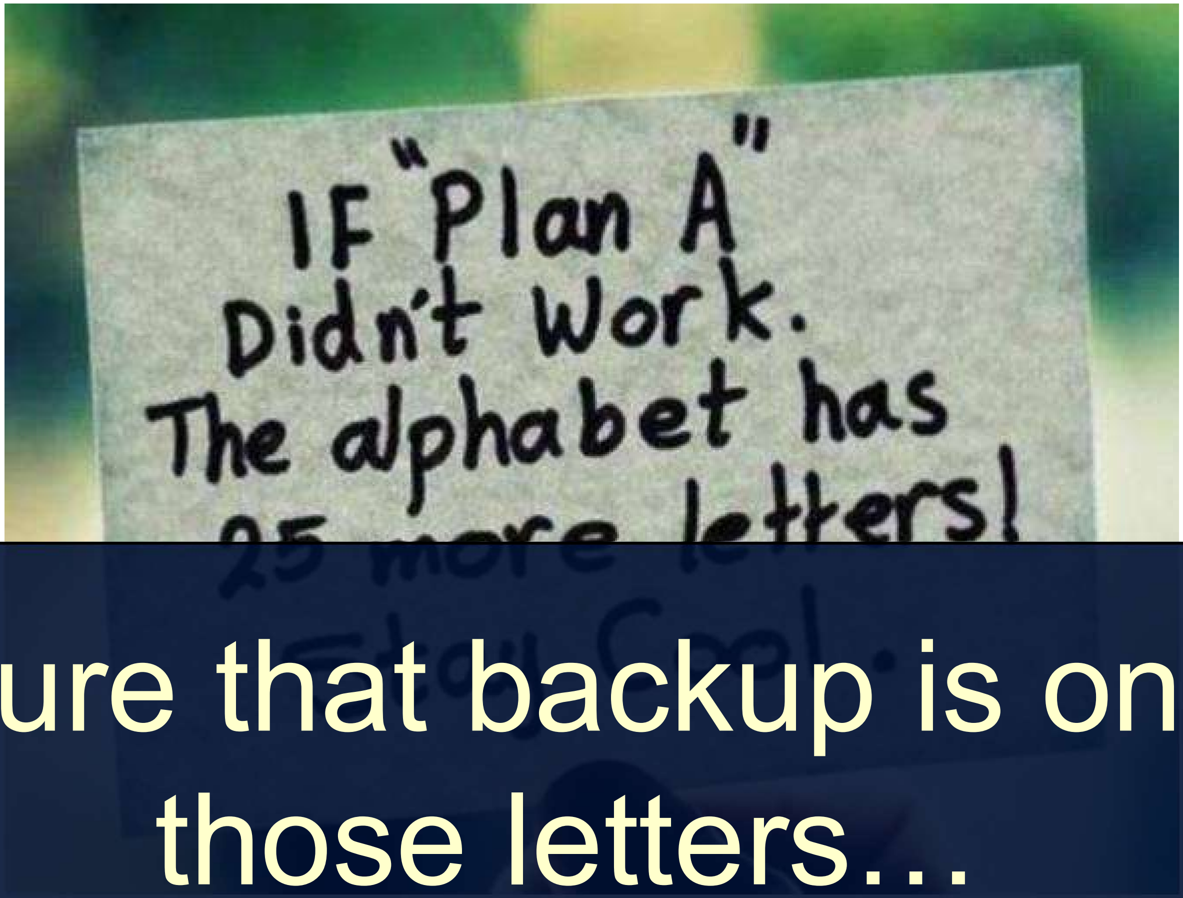
Public video in **English** describing **Cyber Recovery**

- Public video describing **Cyber Bunker**:
  - https://youtu.be/jtgm2WHpFPk
- All topics covered in the above video – includes this presentation:
  - http://backuprecoveryguy.blogspot.com/2020/01/ransomware-attack-how-can-we-recover.html

Cyber Recovery

Summary


IF "Plan A"
Didn't Work.
The alphabet has
25 more letters!
Stay Cool.



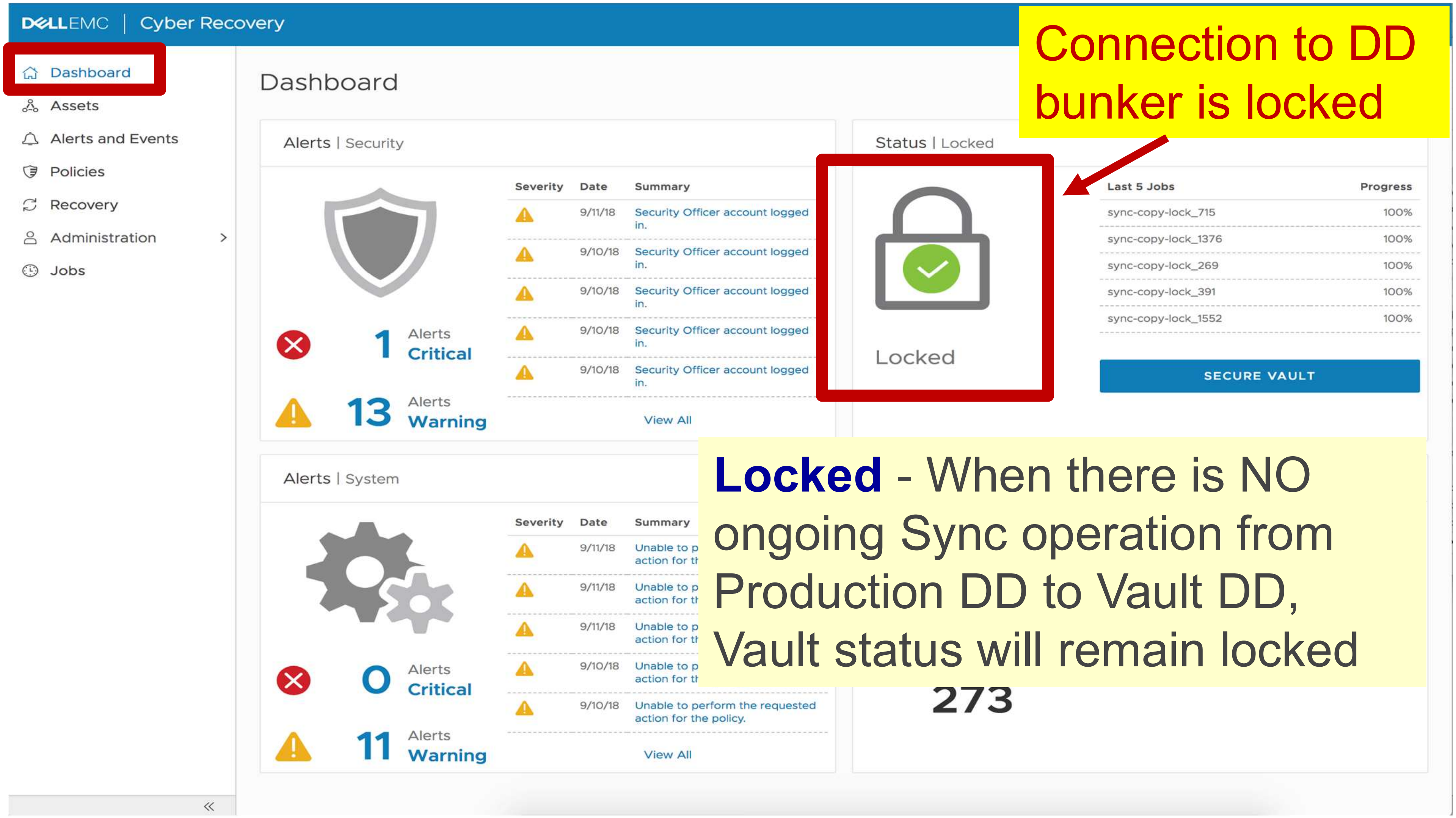
Be sure that backup is one of those letters…

Cyber Recovery

Demo

Cyber Recovery

GUI overview



Dashboard

Alerts | Security

1 Alerts Critical

13 Alerts Warning

Severity	Date	Summary
⚠	9/11/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.

View All

Status | Locked

Locked

Last 5 Jobs	Progress
sync-copy-lock_715	100%
sync-copy-lock_1376	100%
sync-copy-lock_269	100%
sync-copy-lock_391	100%
sync-copy-lock_1552	100%

SECURE VAULT

Alerts | System

0 Alerts Critical

11 Alerts Warning

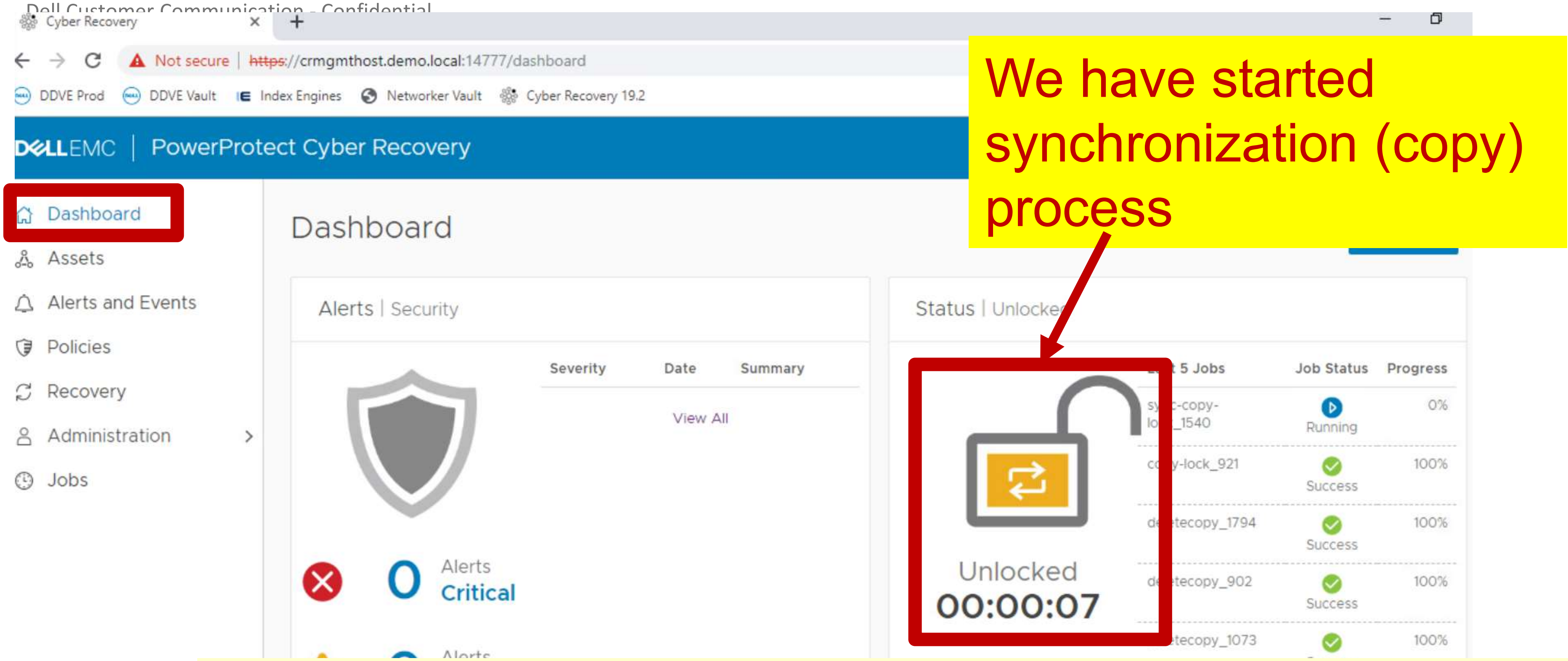
Severity	Date	Summary
⚠	9/11/18	Unable to p action for th
⚠	9/11/18	Unable to p action for th
⚠	9/11/18	Unable to p action for th
⚠	9/10/18	Unable to p action for th
⚠	9/10/18	Unable to perform the requested action for the policy.

View All

273

Connection to DD bunker is locked

Locked - When there is NO ongoing Sync operation from Production DD to Vault DD, Vault status will remain locked

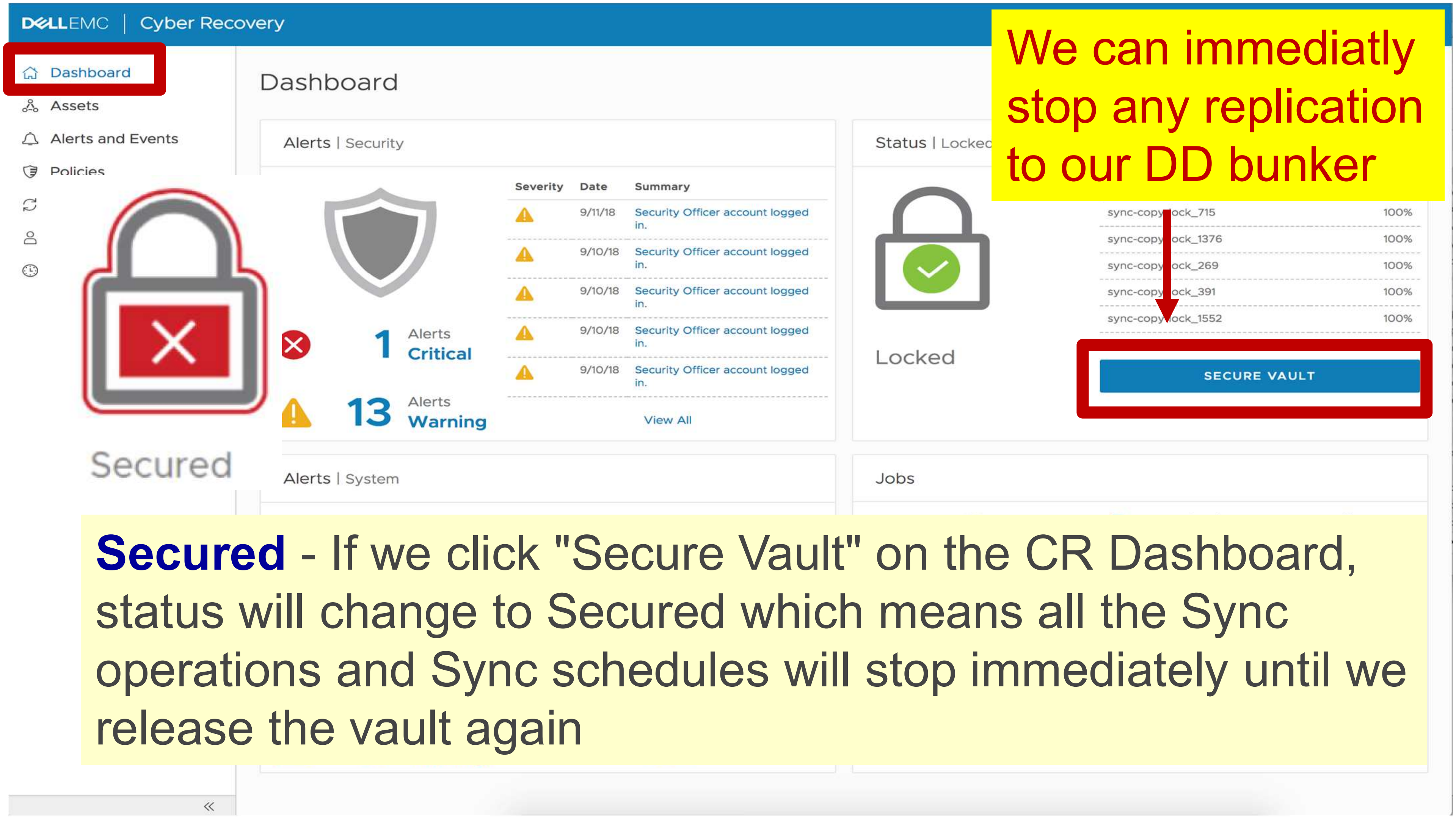


Severity	Date	Summary

...t 5 Jobs	Job Status	Progress
sy...c-copy-lo..._1540	Running	0%
co...y-lock_921	Success	100%
de...tecopy_1794	Success	100%
de...tecopy_902	Success	100%
...tecopy_1073		100%

We have started synchronization (copy) process

Unlocked - When there is Sync Operation going on and data is getting replicated from Production DD to Vault DD, Vault status will remain Unlocked during that time



Severity	Date	Summary
⚠	9/11/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.
⚠	9/10/18	Security Officer account logged in.

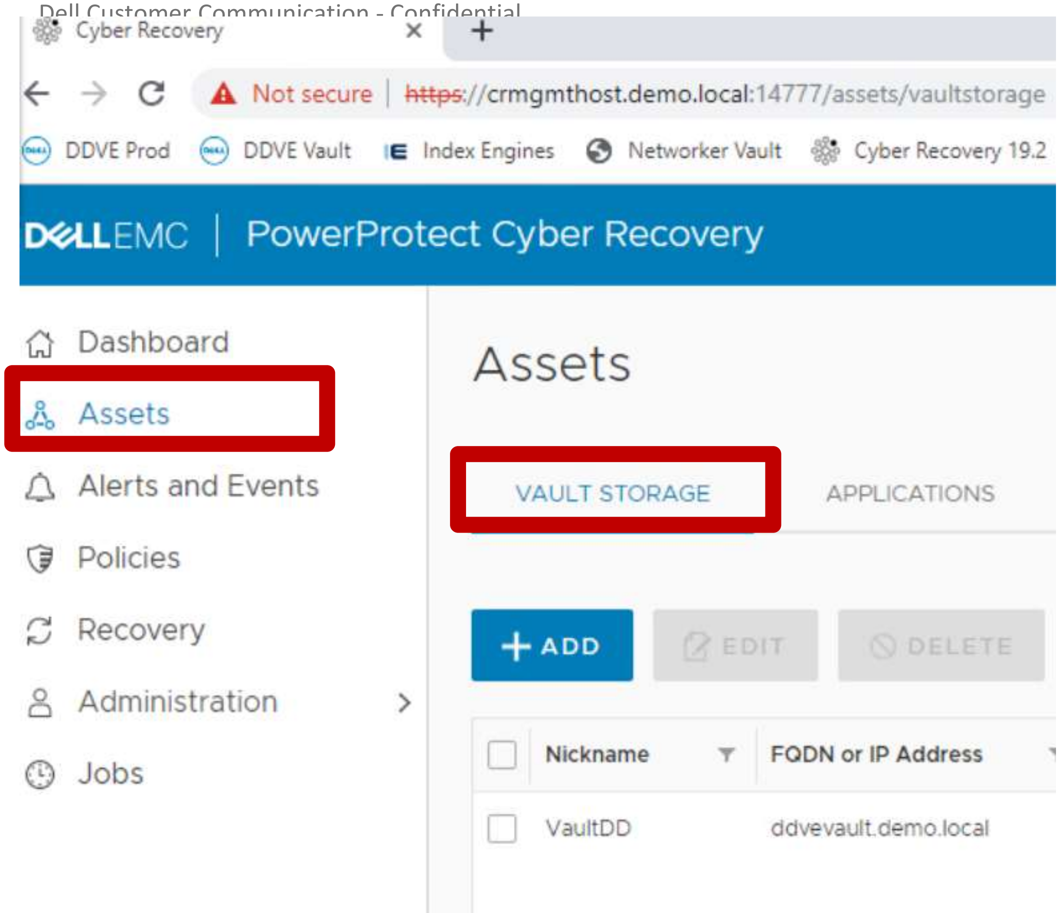
sync-copy ock_715	100%
sync-copy ock_1376	100%
sync-copy ock_269	100%
sync-copy ock_391	100%
sync-copy ock_1552	100%

We can immediatly stop any replication to our DD bunker

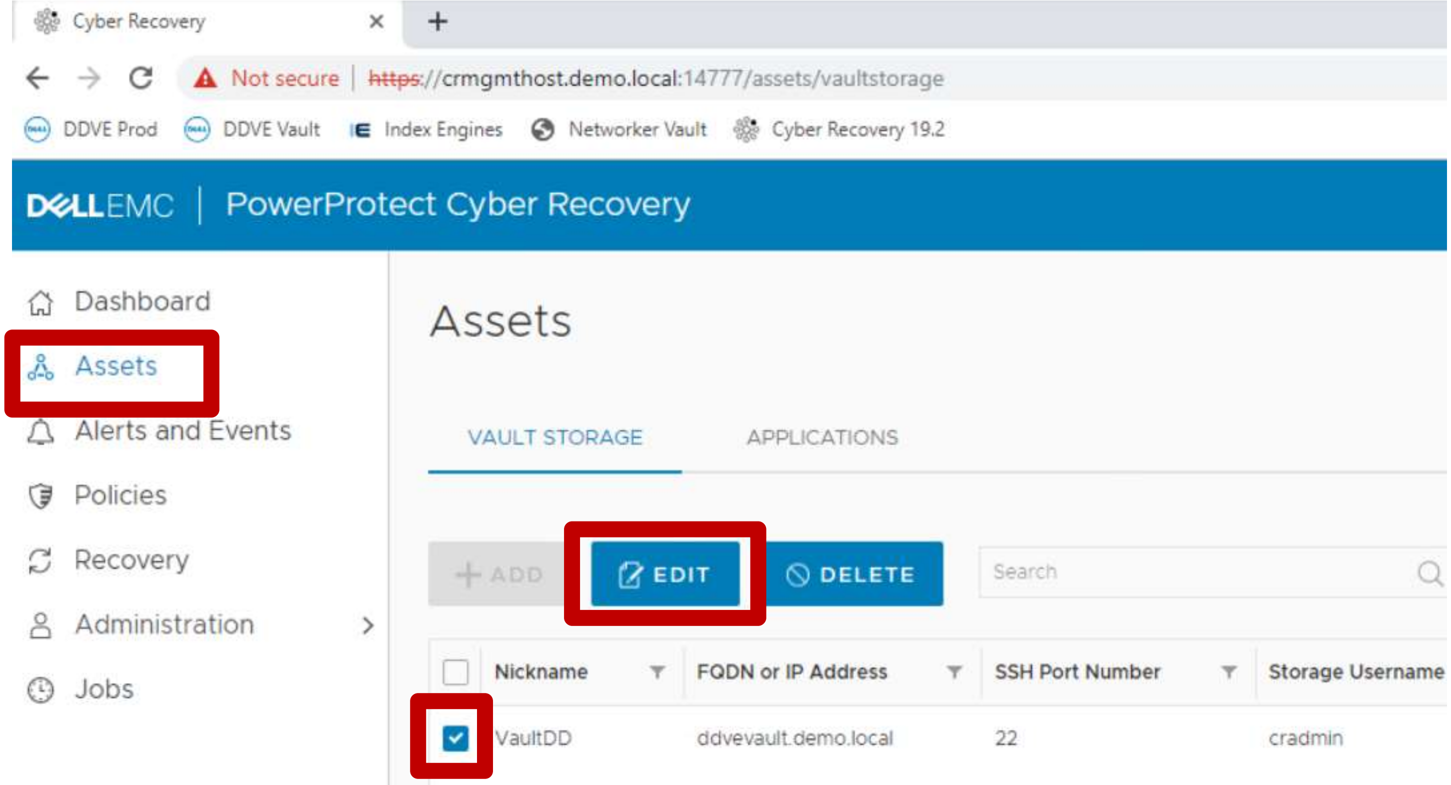
Secured - If we click "Secure Vault" on the CR Dashboard, status will change to Secured which means all the Sync operations and Sync schedules will stop immediately until we release the vault again

Cyber Recovery

Assets



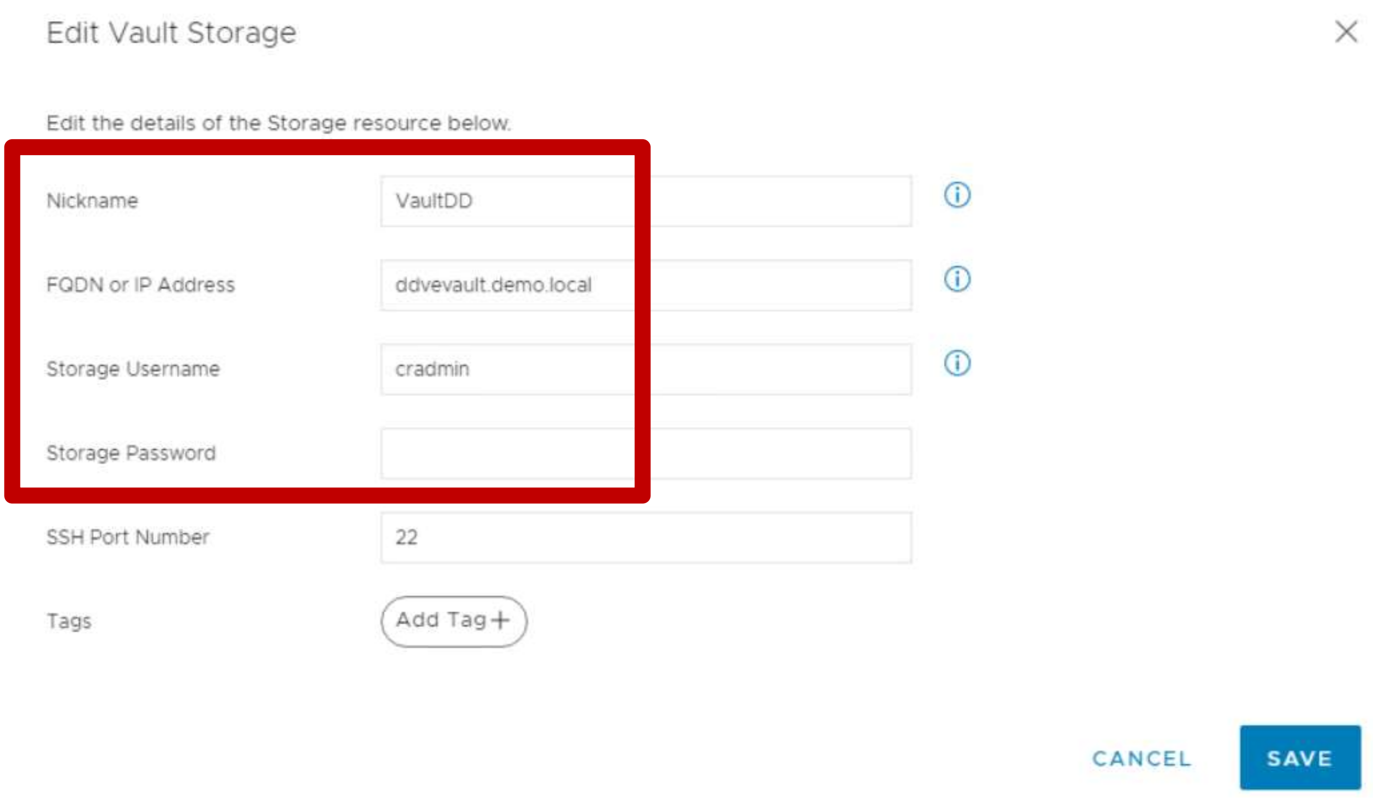
□	Nickname	FQDN or IP Address
□	VaultDD	ddvevault.demo.local



Assets

VAULT STORAGE | APPLICATIONS

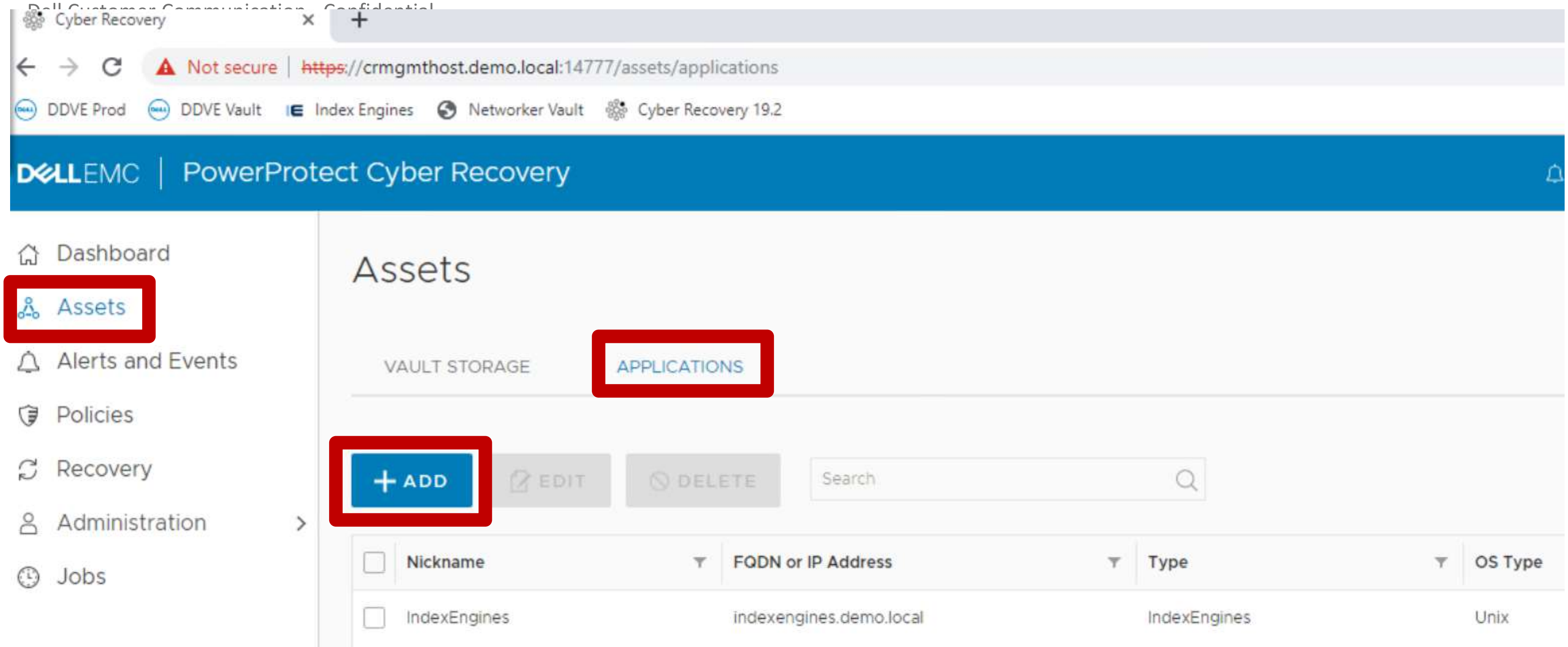
☐	Nickname	FQDN or IP Address	SSH Port Number	Storage Username
☑	VaultDD	ddvevault.demo.local	22	cradmin



Edit Vault Storage

Edit the details of the Storage resource below.

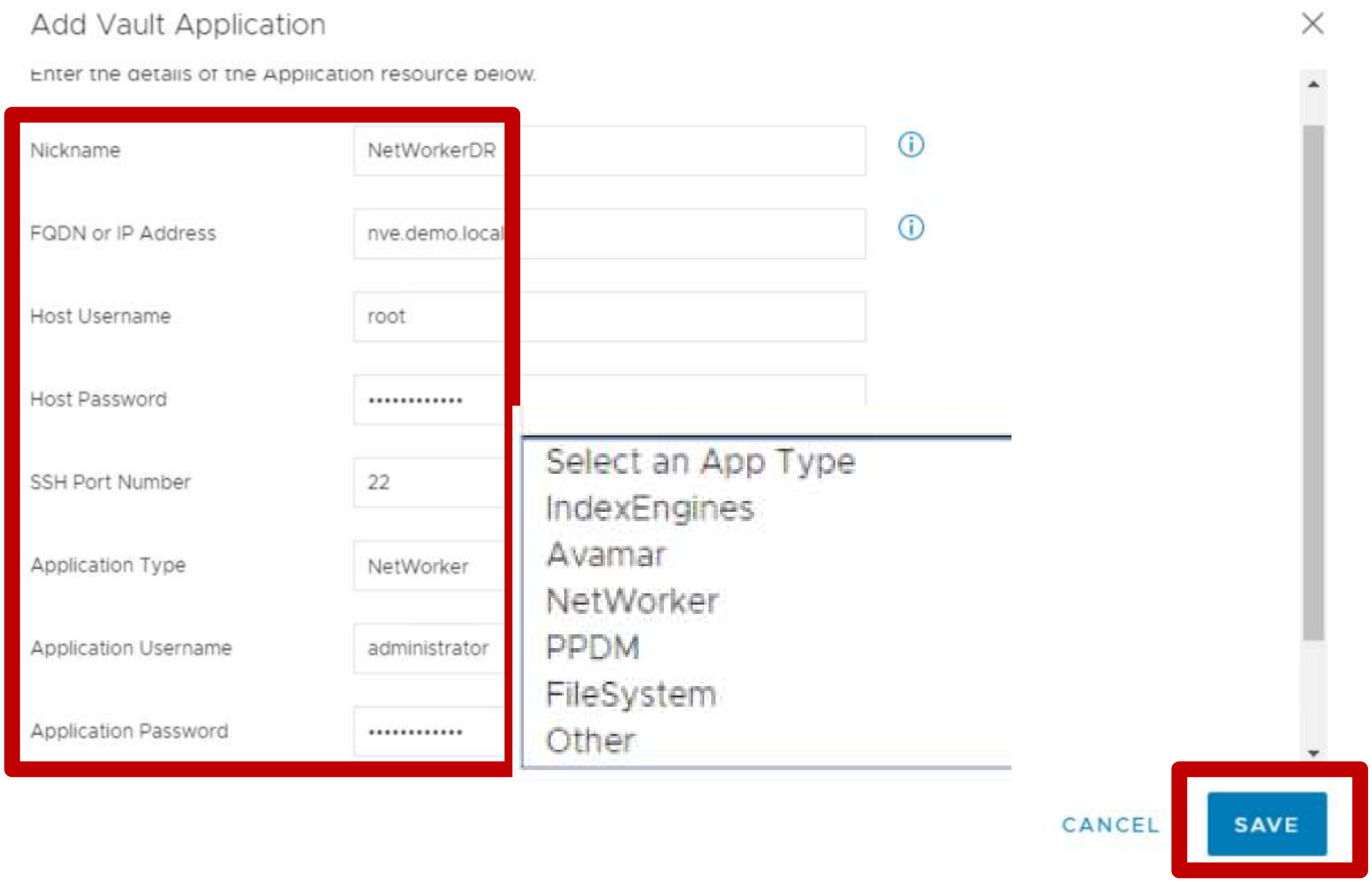
Nickname	VaultDD
FQDN or IP Address	ddvevault.demo.local
Storage Username	cradmin
Storage Password	
SSH Port Number	22
Tags	Add Tag +



https://crmgmthost.demo.local:14777/assets/applications

Assets

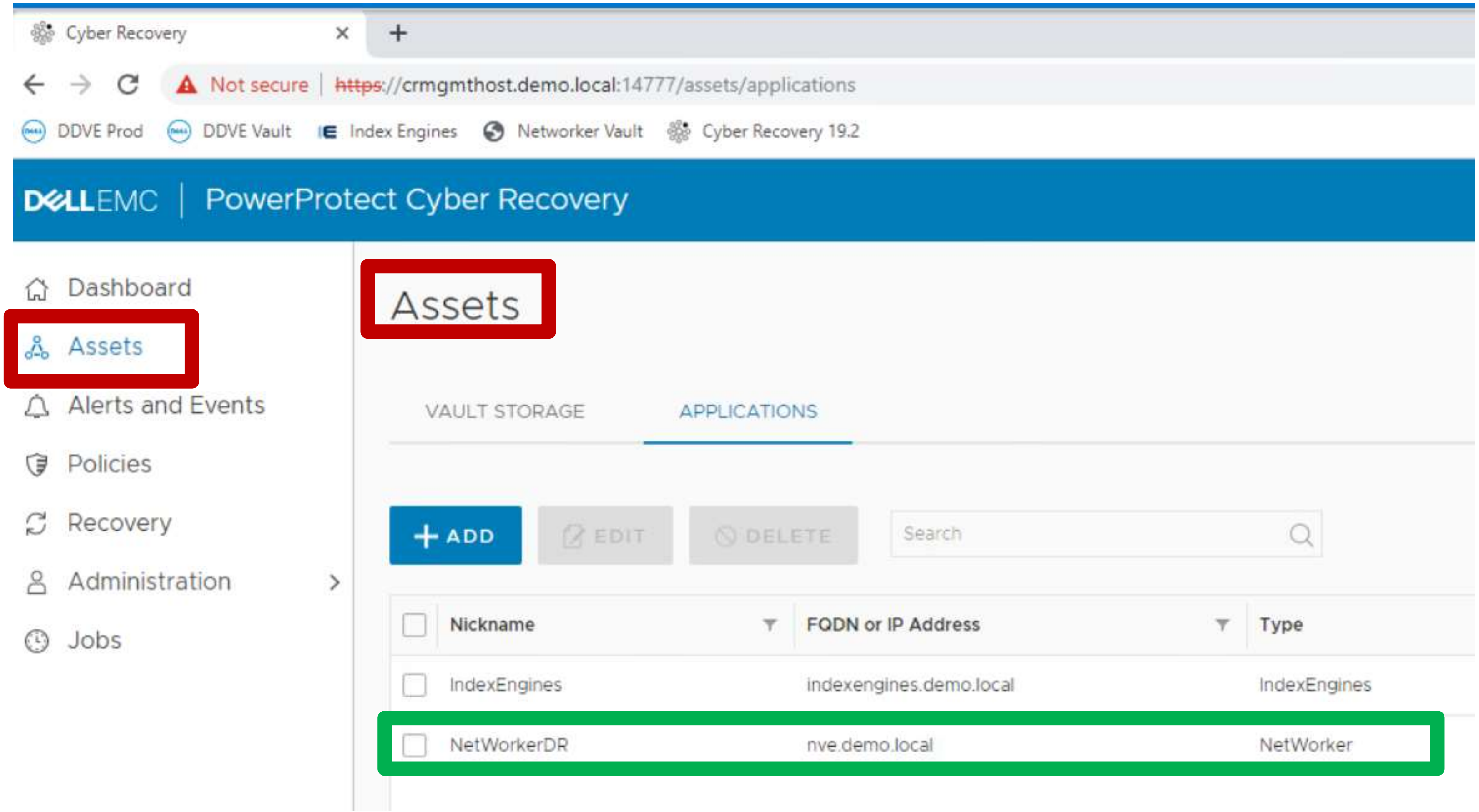
□	Nickname	FQDN or IP Address	Type	OS Type
□	IndexEngines	indexengines.demo.local	IndexEngines	Unix



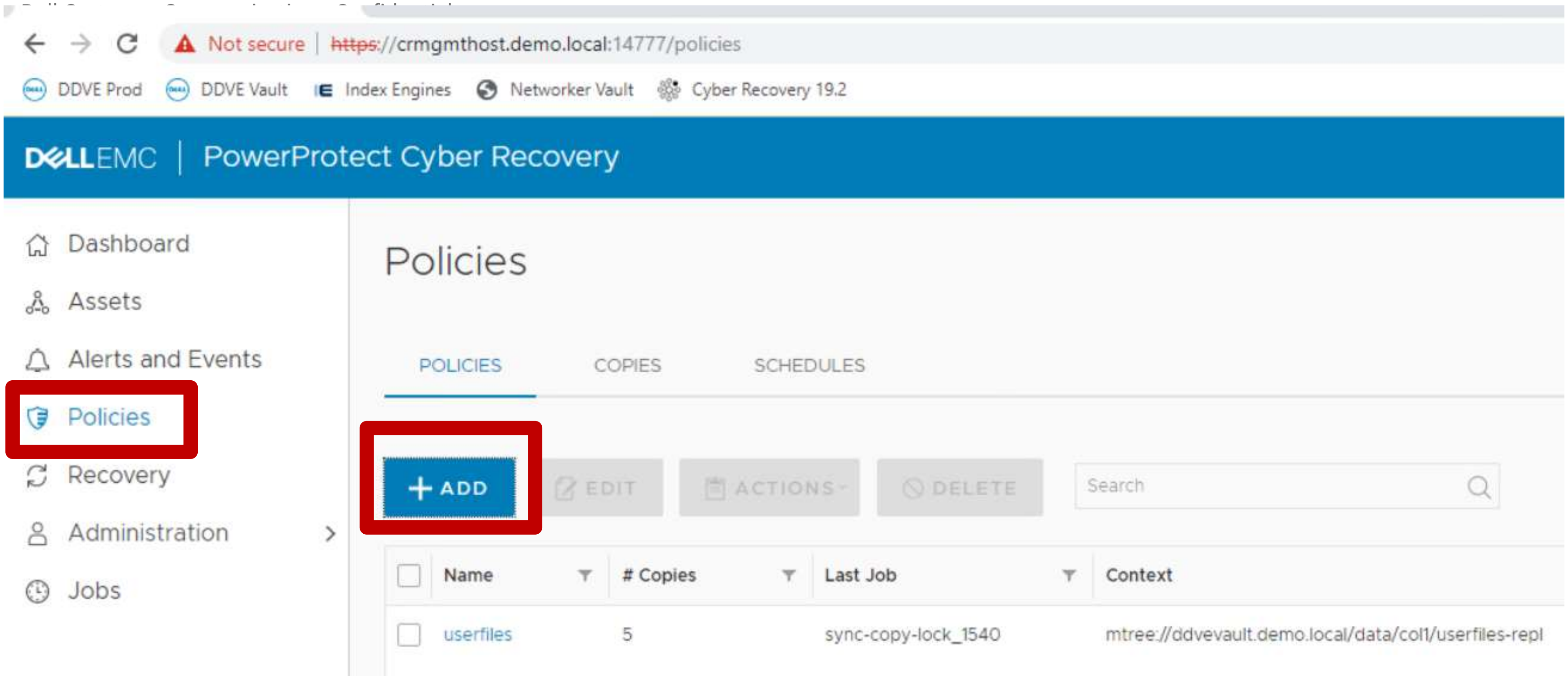
Add Vault Application

Enter the details of the Application resource below.

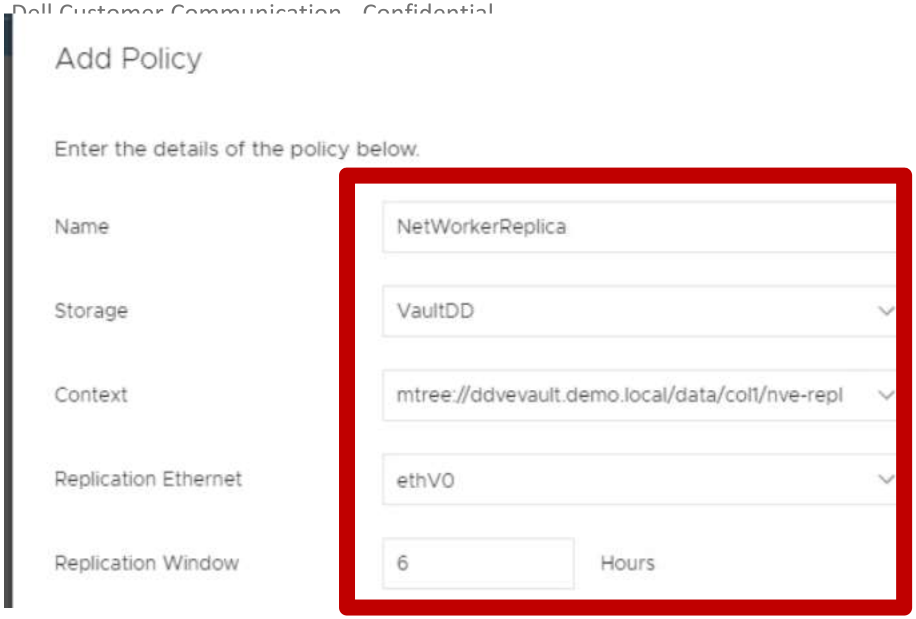
Nickname	NetWorkerDR
FQDN or IP Address	nve.demo.local
Host Username	root
Host Password	•••••••••••••
SSH Port Number	22
Application Type	NetWorker
Application Username	administrator
Application Password	•••••••••••••



□	Nickname	FQDN or IP Address	Type
□	IndexEngines	indexengines.demo.local	IndexEngines
□	NetWorkerDR	nve.demo.local	NetWorker



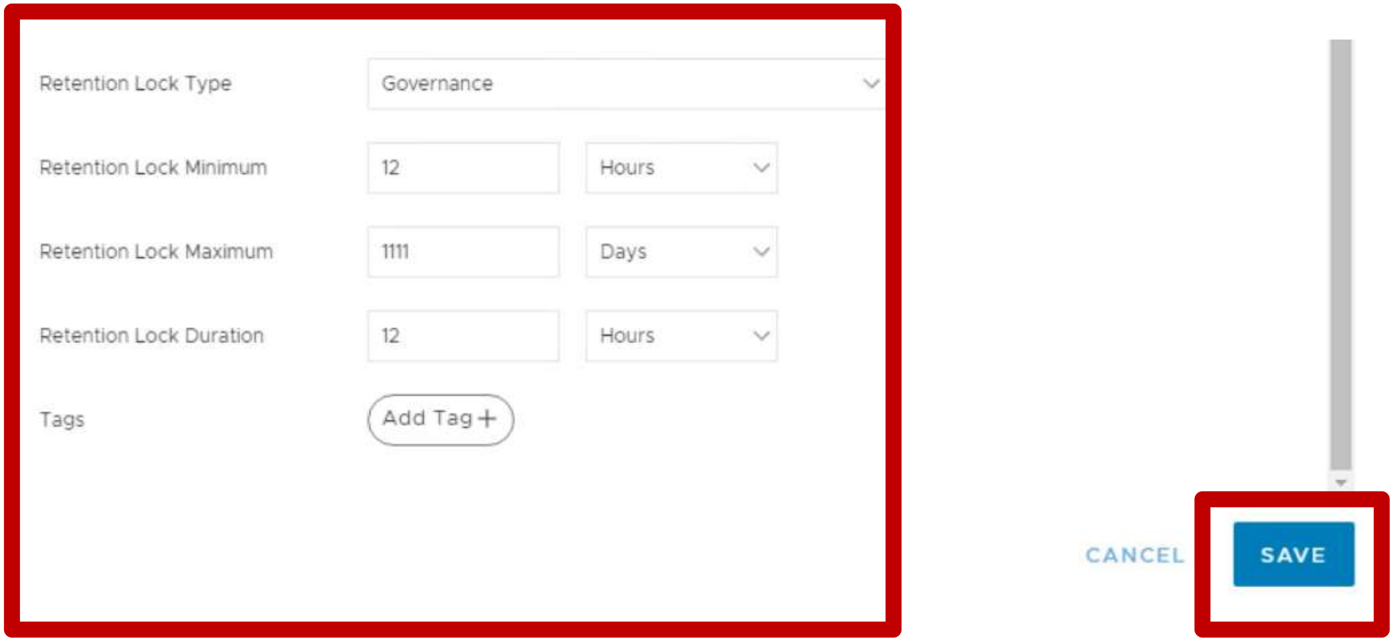
□	Name	# Copies	Last Job	Context
□	userfiles	5	sync-copy-lock_1540	mtree://ddvevault.demo.local/data/col1/userfiles-repl



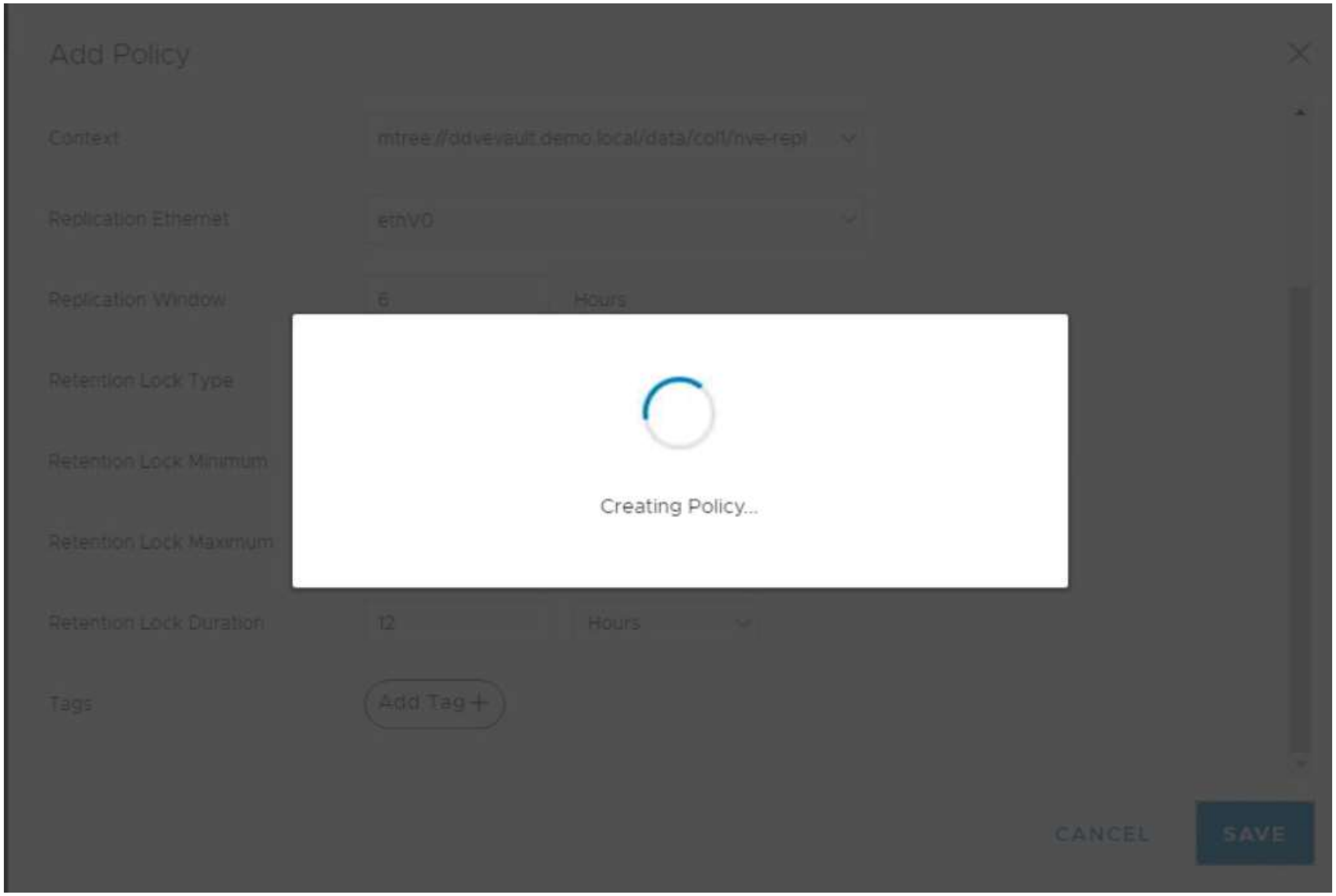
Add Policy

Enter the details of the policy below.

Name	NetWorkerReplica
Storage	VaultDD
Context	mtree://ddvevault.demo.local/data/col1/nve-repl
Replication Ethernet	ethV0
Replication Window	6 Hours



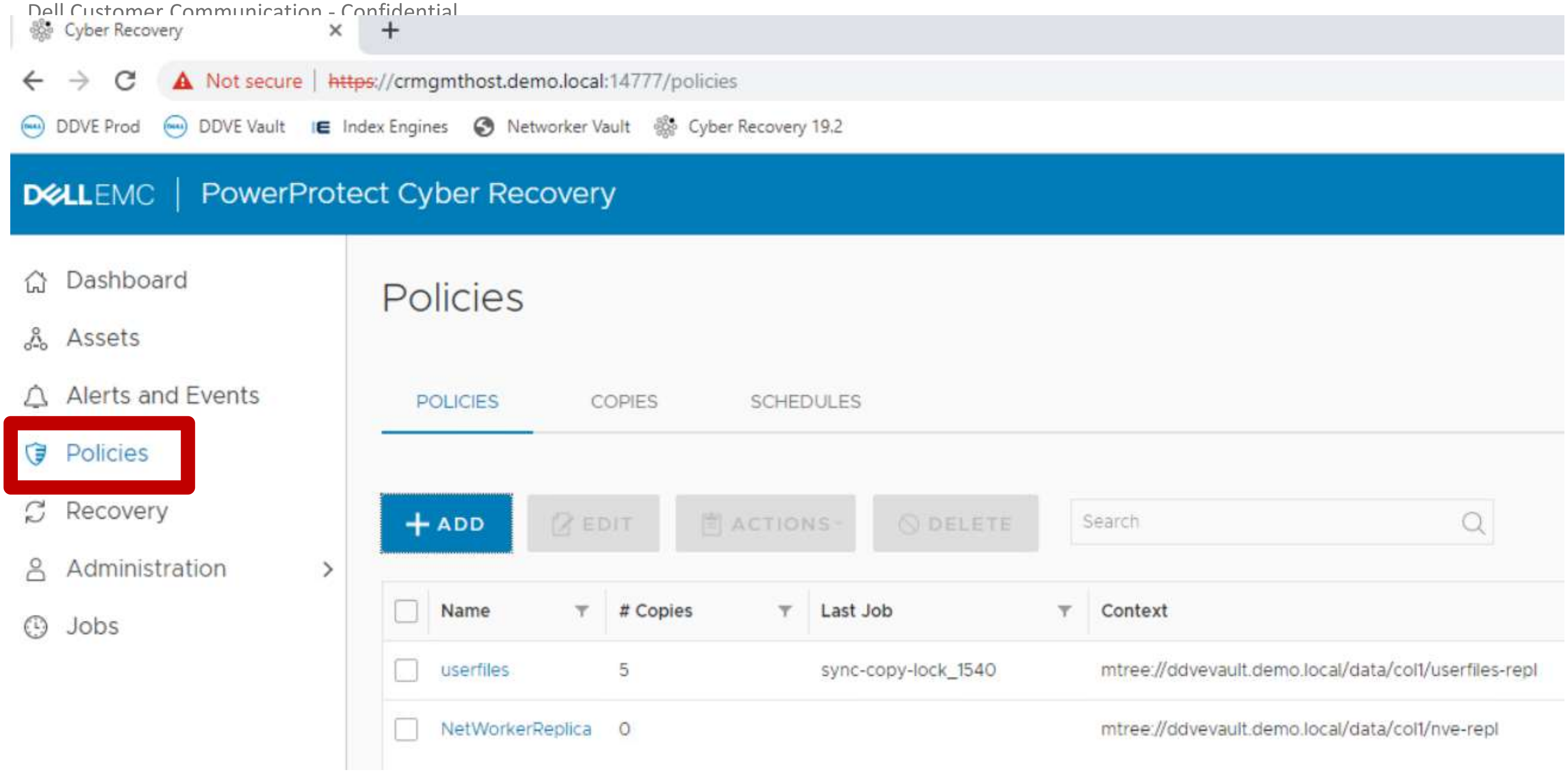
Retention Lock Type	Governance	
Retention Lock Minimum	12	Hours
Retention Lock Maximum	1111	Days
Retention Lock Duration	12	Hours
Tags	Add Tag +	



Add Policy

Context	mtree://ddvevault.demo.local/data/col1/nve-repl	
Replication Ethernet	ethV0	
Replication Window	6	Hours
Retention Lock Type		
Retention Lock Minimum		
Retention Lock Maximum		
Retention Lock Duration	12	Hours
Tags		

Creating Policy...



Policies

□	Name	# Copies	Last Job	Context
□	userfiles	5	sync-copy-lock_1540	mtree://ddvevault.demo.local/data/col1/userfiles-repl
□	NetWorkerReplica	0		mtree://ddvevault.demo.local/data/col1/nve-repl

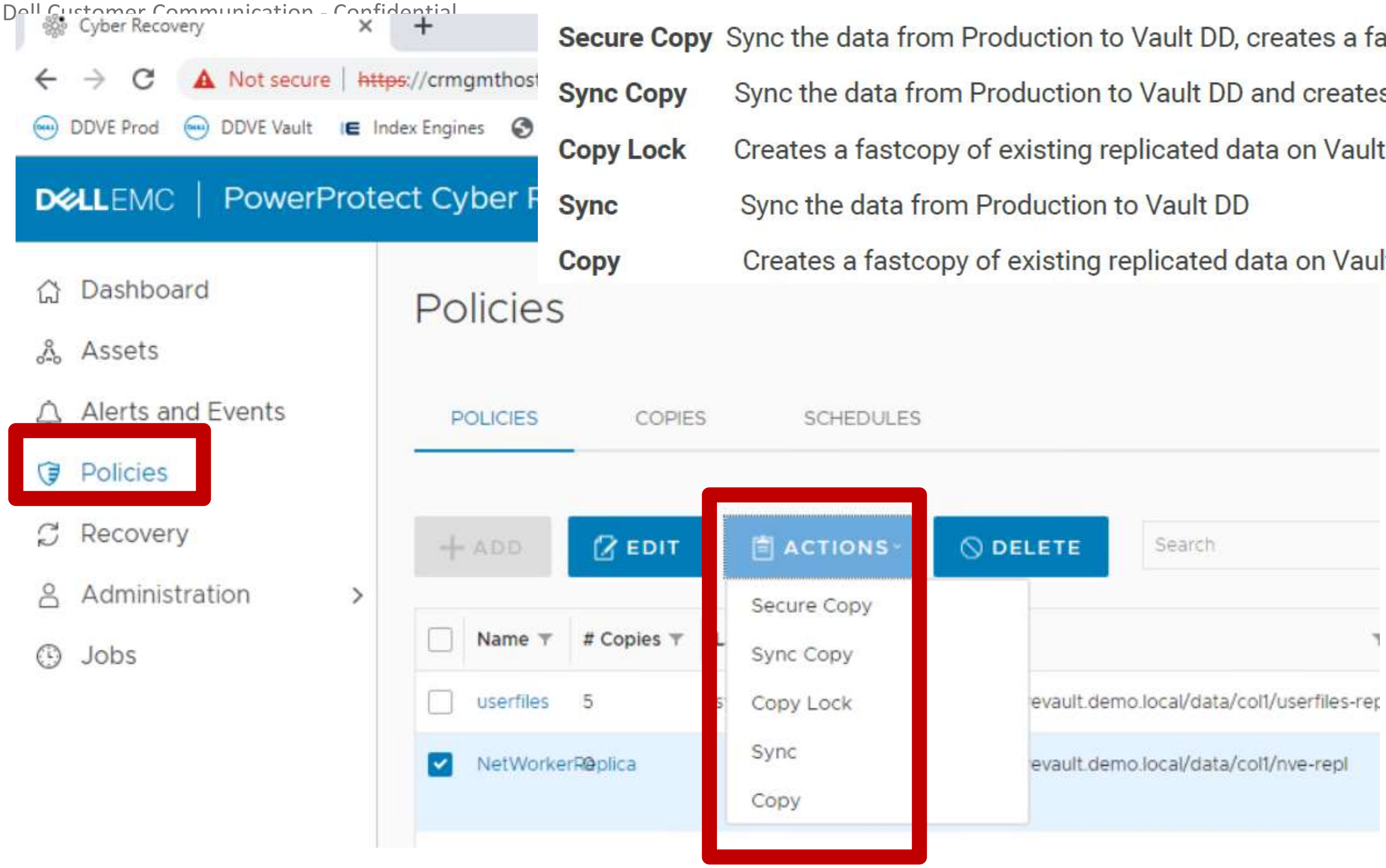
Secure Copy Sync the data from Production to Vault DD, creates a fastcopy and retention lock it

Sync Copy Sync the data from Production to Vault DD and creates a fastcopy

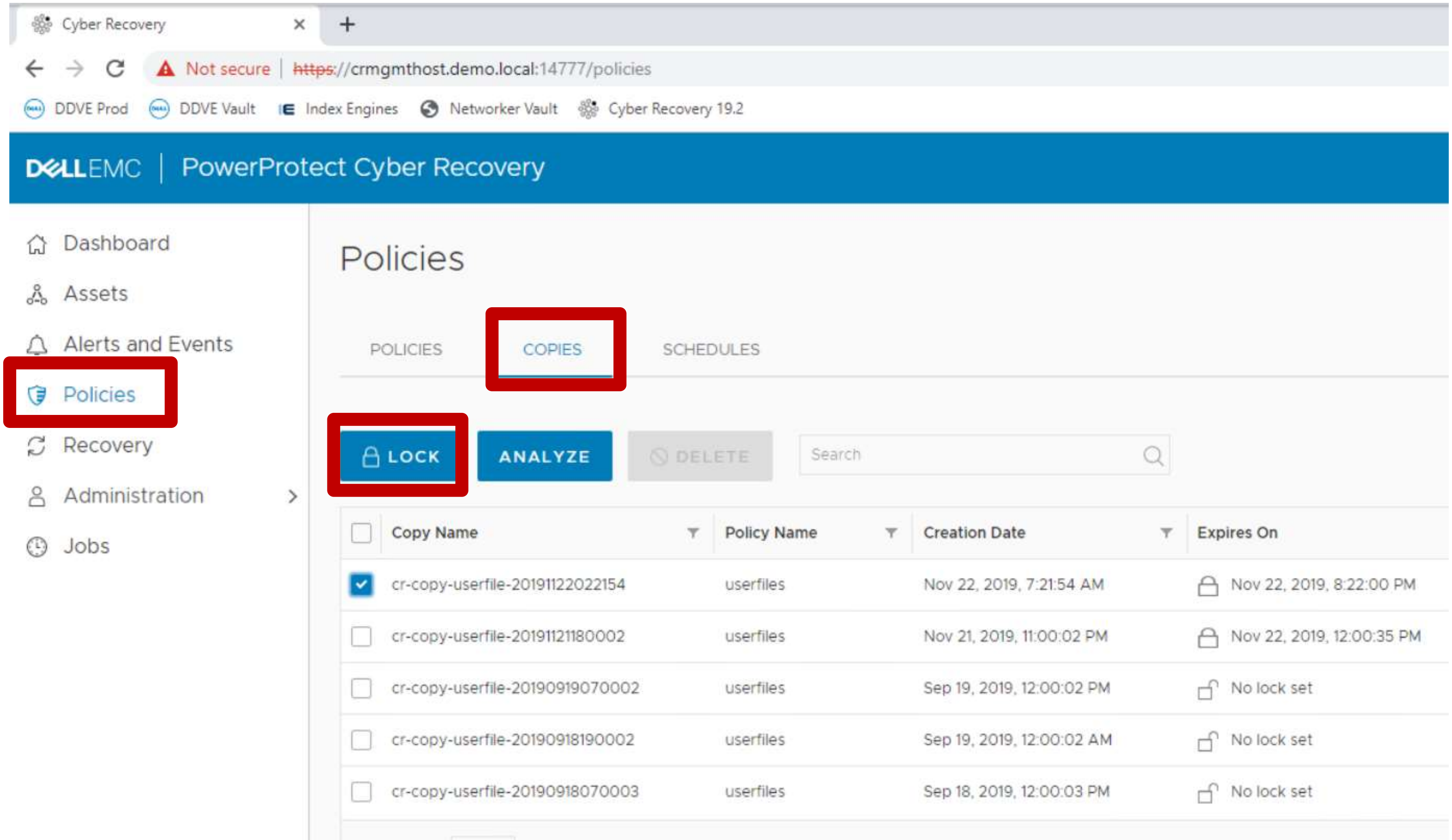
Copy Lock Creates a fastcopy of existing replicated data on Vault DD and retention lock it

Sync Sync the data from Production to Vault DD

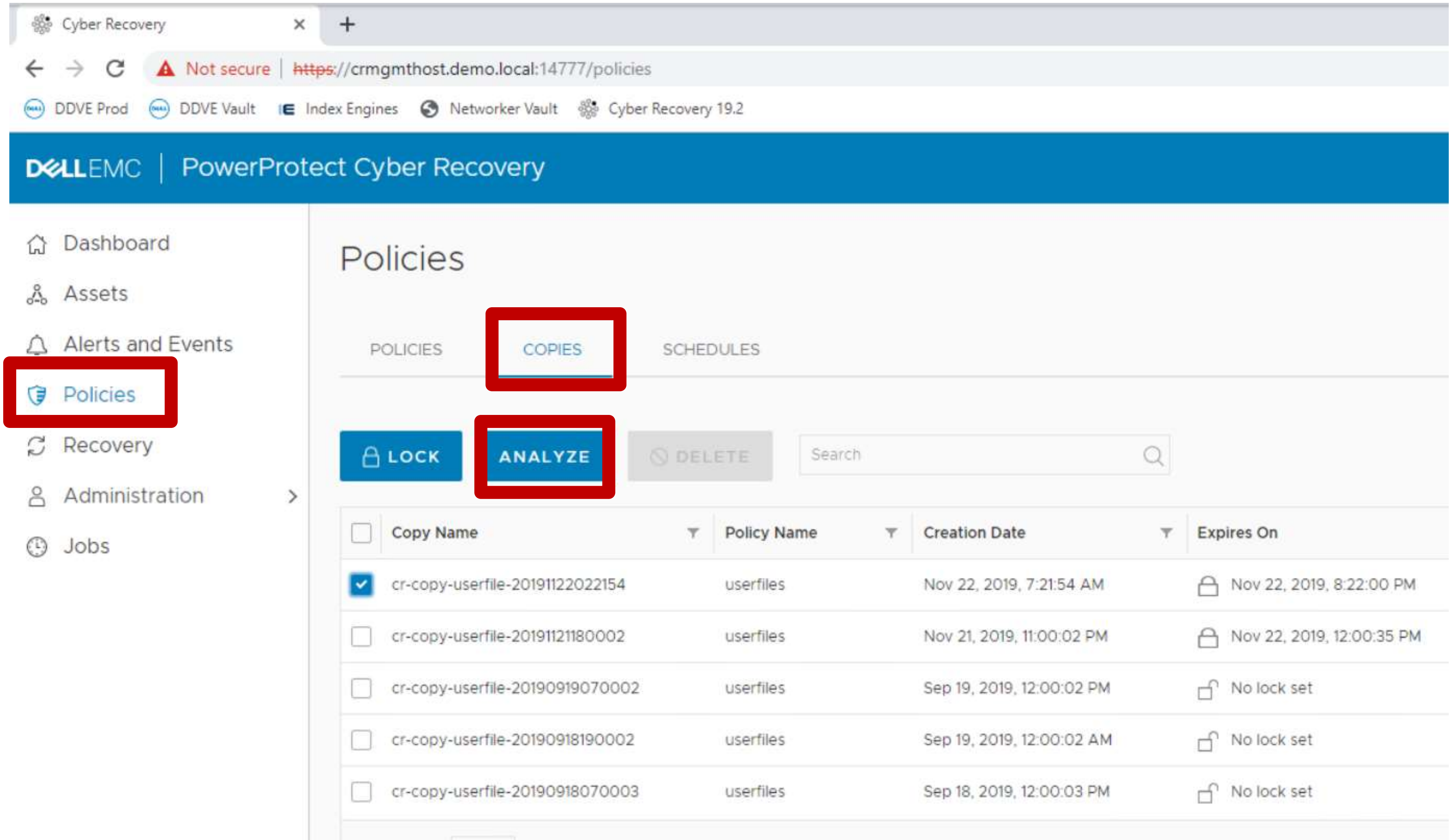
Copy Creates a fastcopy of existing replicated data on Vault DD



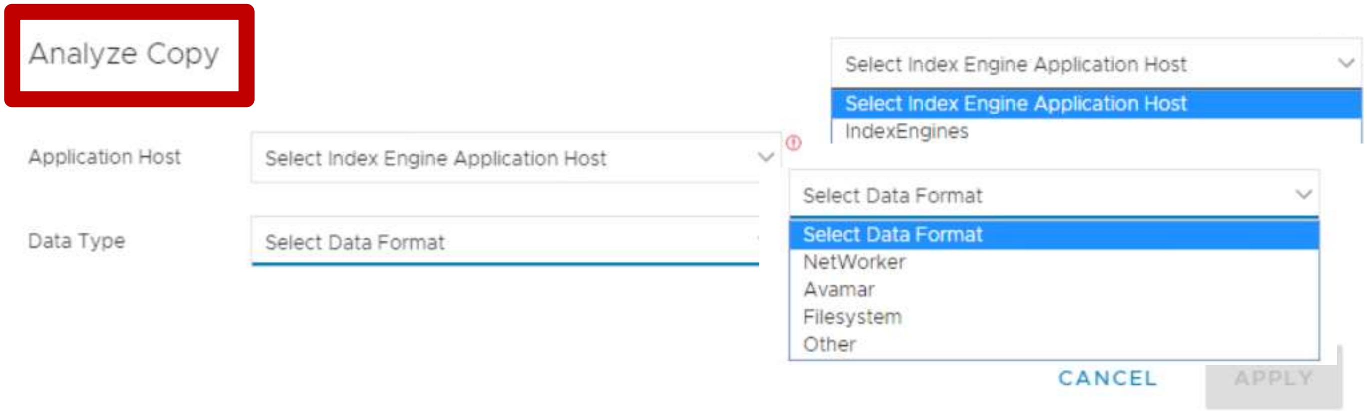
	Name	# Copies	
□	userfiles	5	evault.demo.local/data/col1/userfiles-rep
☑	NetWorkerReplica	0	evault.demo.local/data/col1/nve-repl



☐	Copy Name	Policy Name	Creation Date	Expires On
☑	cr-copy-userfile-20191122022154	userfiles	Nov 22, 2019, 7:21:54 AM	🔒 Nov 22, 2019, 8:22:00 PM
☐	cr-copy-userfile-20191121180002	userfiles	Nov 21, 2019, 11:00:02 PM	🔒 Nov 22, 2019, 12:00:35 PM
☐	cr-copy-userfile-20190919070002	userfiles	Sep 19, 2019, 12:00:02 PM	🔓 No lock set
☐	cr-copy-userfile-20190918190002	userfiles	Sep 19, 2019, 12:00:02 AM	🔓 No lock set
☐	cr-copy-userfile-20190918070003	userfiles	Sep 18, 2019, 12:00:03 PM	🔓 No lock set



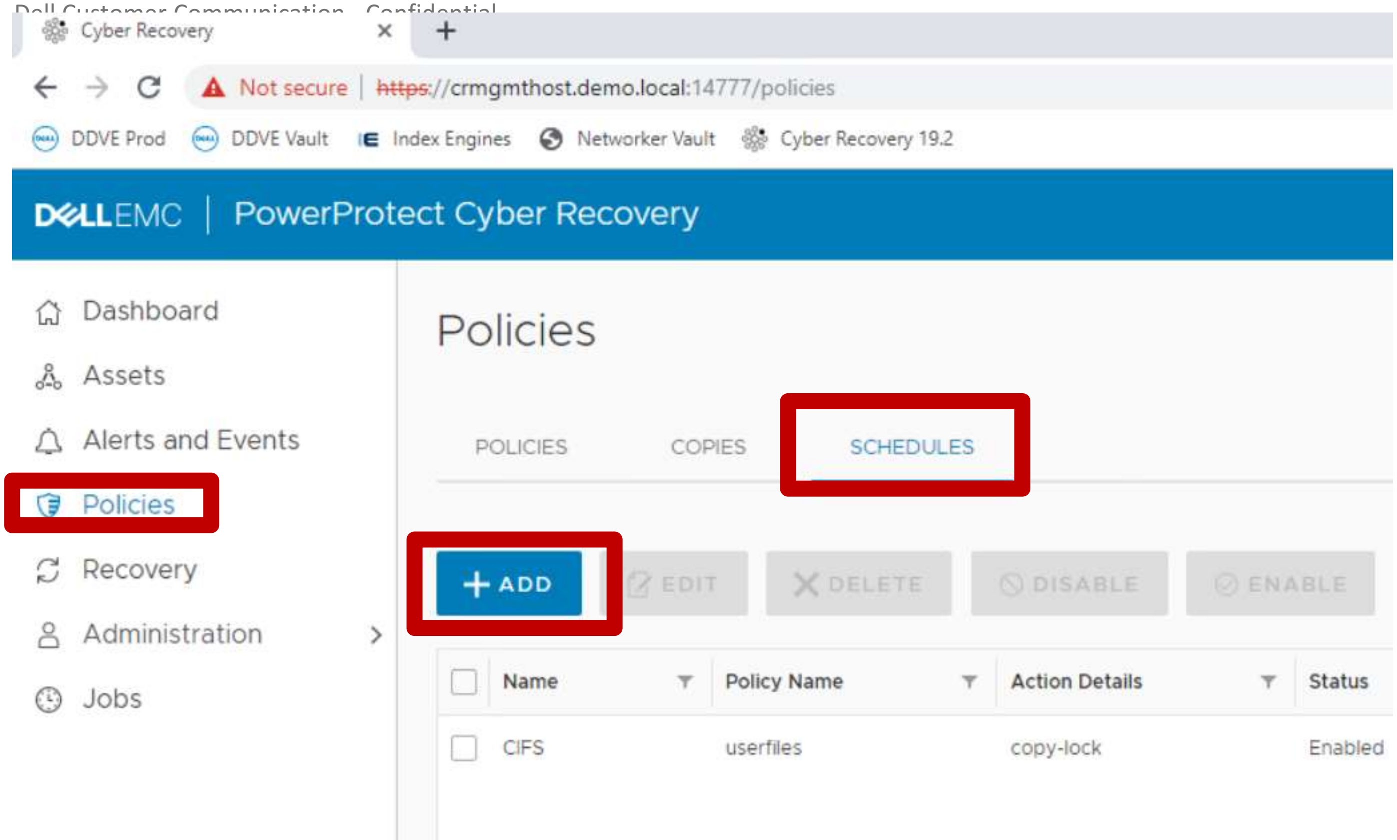
□	Copy Name	Policy Name	Creation Date	Expires On
☑	cr-copy-userfile-20191122022154	userfiles	Nov 22, 2019, 7:21:54 AM	Nov 22, 2019, 8:22:00 PM
□	cr-copy-userfile-20191121180002	userfiles	Nov 21, 2019, 11:00:02 PM	Nov 22, 2019, 12:00:35 PM
□	cr-copy-userfile-20190919070002	userfiles	Sep 19, 2019, 12:00:02 PM	No lock set
□	cr-copy-userfile-20190918190002	userfiles	Sep 19, 2019, 12:00:02 AM	No lock set
□	cr-copy-userfile-20190918070003	userfiles	Sep 18, 2019, 12:00:03 PM	No lock set



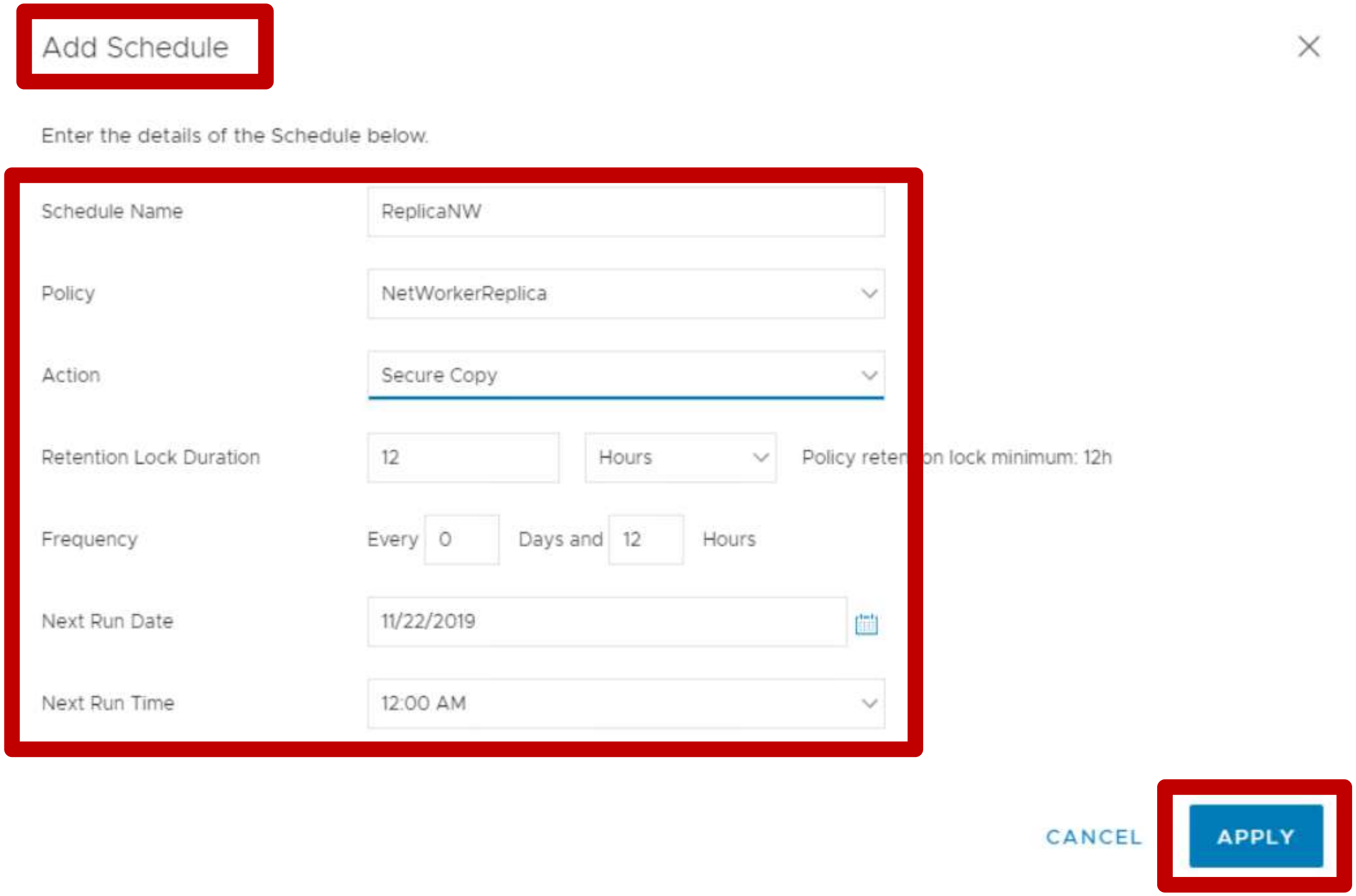
Analyze Copy

Application Host: Select Index Engine Application Host

Data Type: Select Data Format



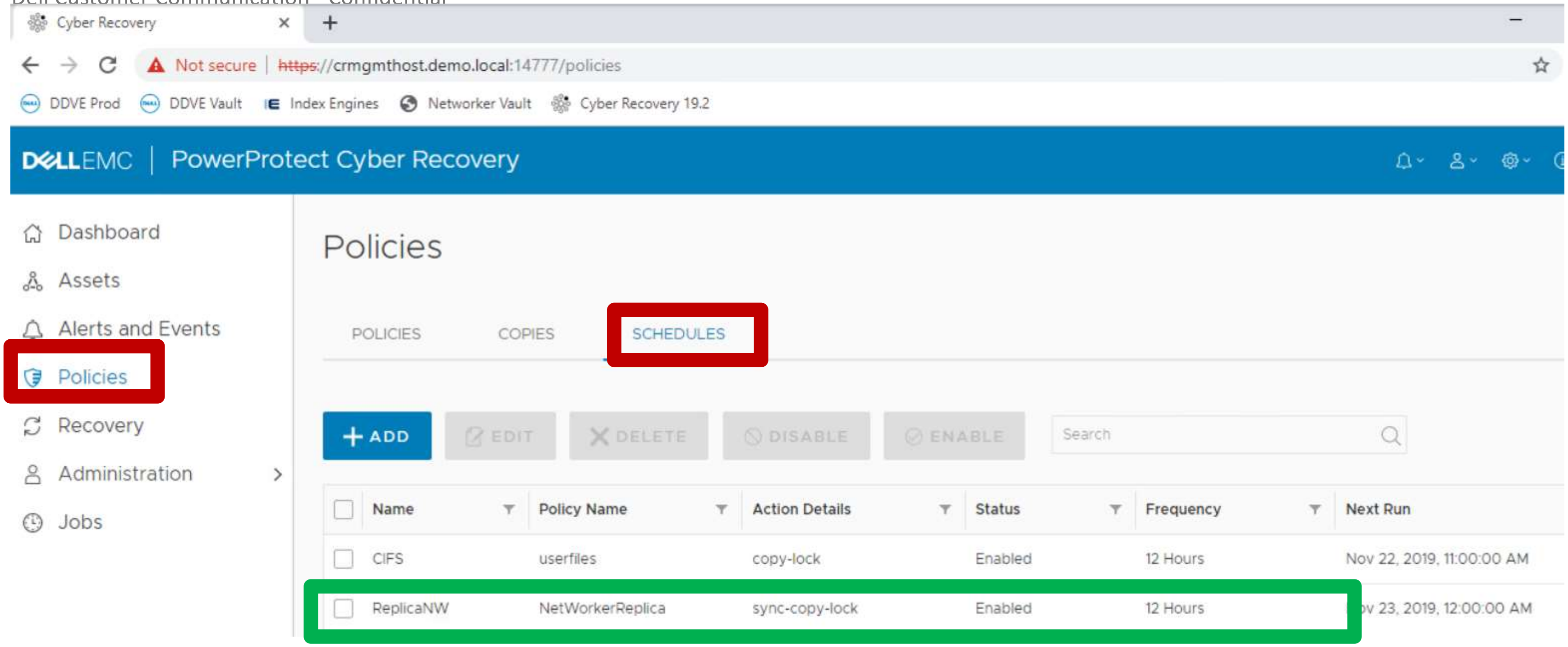
□	Name	Policy Name	Action Details	Status
□	CIFS	userfiles	copy-lock	Enabled



Add Schedule

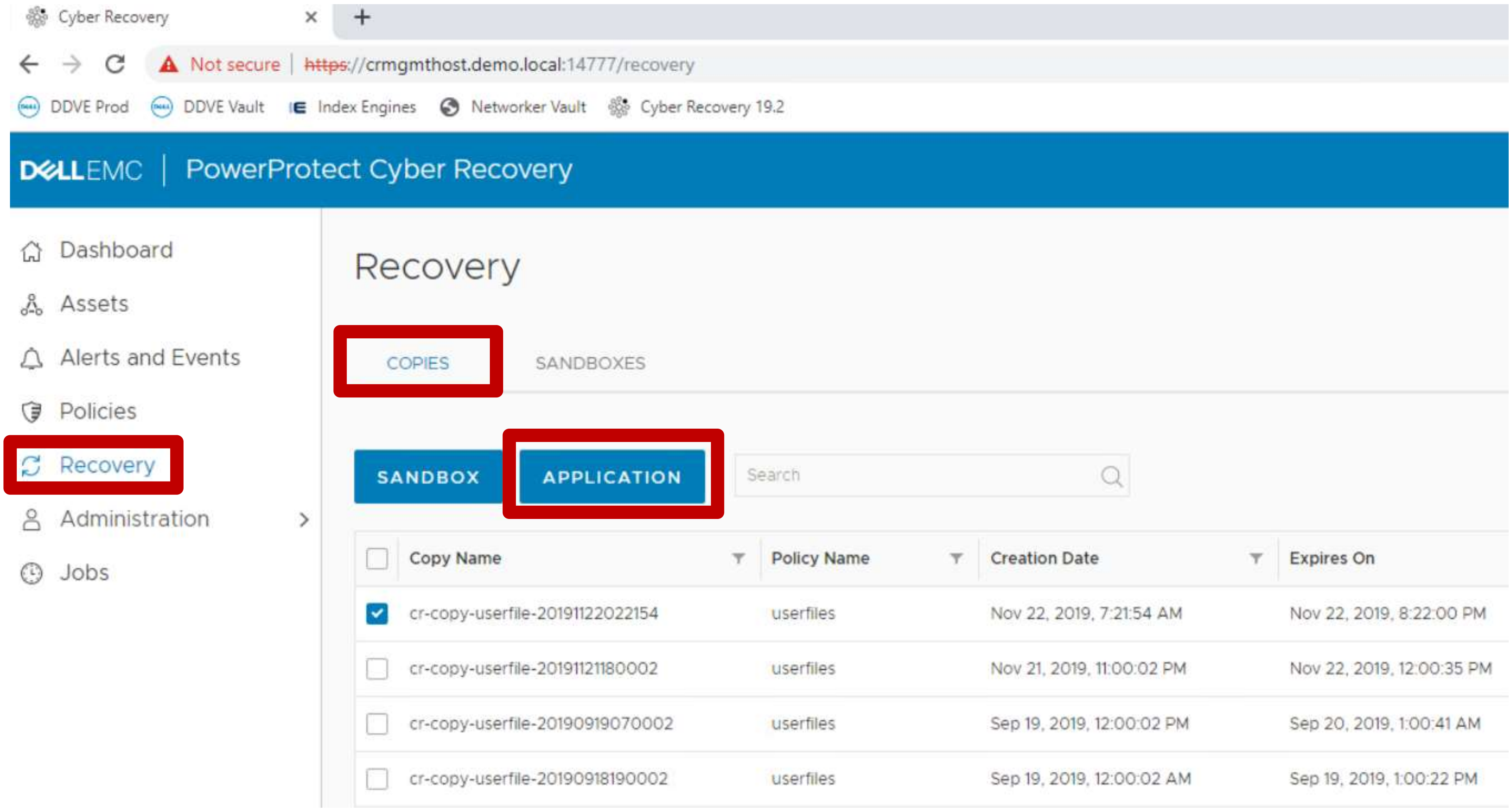
Enter the details of the Schedule below.

Schedule Name	ReplicaNW
Policy	NetWorkerReplica
Action	Secure Copy
Retention Lock Duration	12 Hours — Policy retention lock minimum: 12h
Frequency	Every 0 Days and 12 Hours
Next Run Date	11/22/2019
Next Run Time	12:00 AM



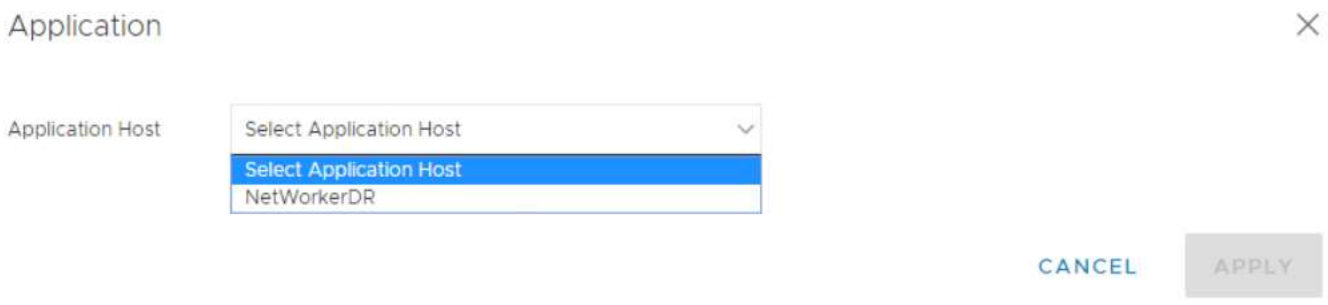
Policies

□	Name	Policy Name	Action Details	Status	Frequency	Next Run
□	CIFS	userfiles	copy-lock	Enabled	12 Hours	Nov 22, 2019, 11:00:00 AM
□	ReplicaNW	NetWorkerReplica	sync-copy-lock	Enabled	12 Hours	ov 23, 2019, 12:00:00 AM



Recovery

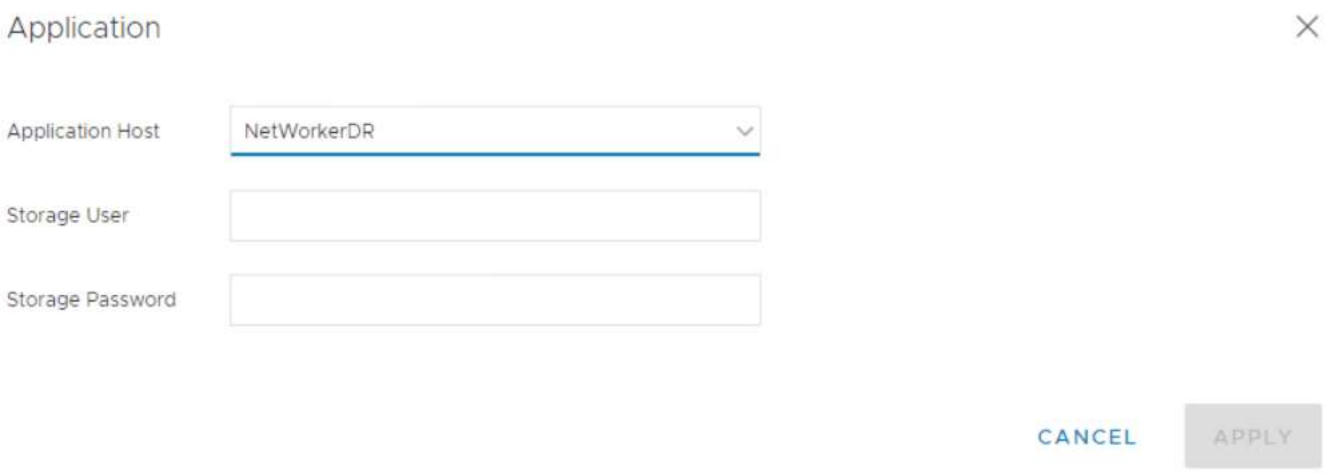
□	Copy Name	Policy Name	Creation Date	Expires On
☑	cr-copy-userfile-20191122022154	userfiles	Nov 22, 2019, 7:21:54 AM	Nov 22, 2019, 8:22:00 PM
□	cr-copy-userfile-20191121180002	userfiles	Nov 21, 2019, 11:00:02 PM	Nov 22, 2019, 12:00:35 PM
□	cr-copy-userfile-20190919070002	userfiles	Sep 19, 2019, 12:00:02 PM	Sep 20, 2019, 1:00:41 AM
□	cr-copy-userfile-20190918190002	userfiles	Sep 19, 2019, 12:00:02 AM	Sep 19, 2019, 1:00:22 PM



Application

Application Host: Select Application Host

Select Application Host
NetWorkerDR

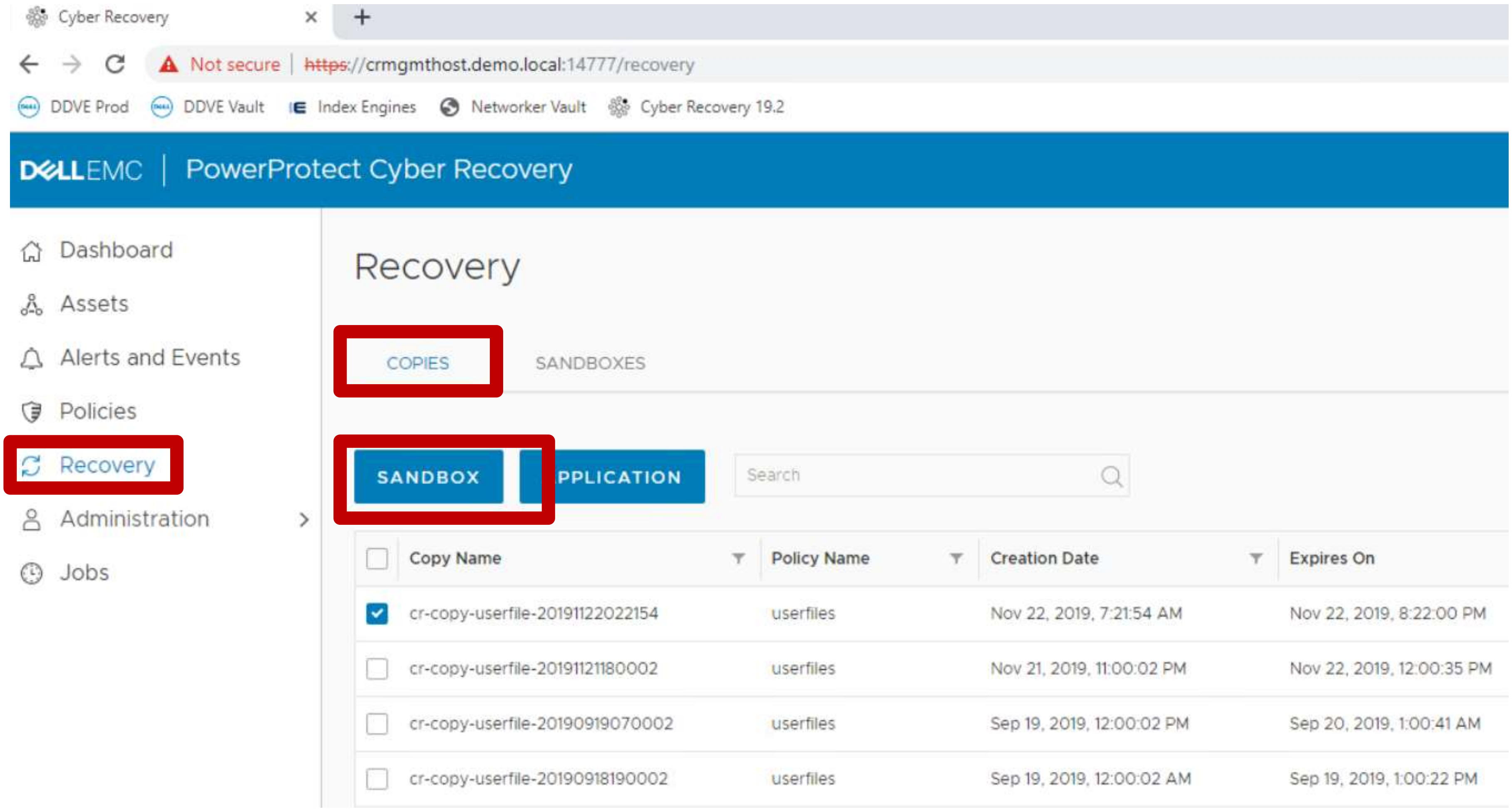


Application

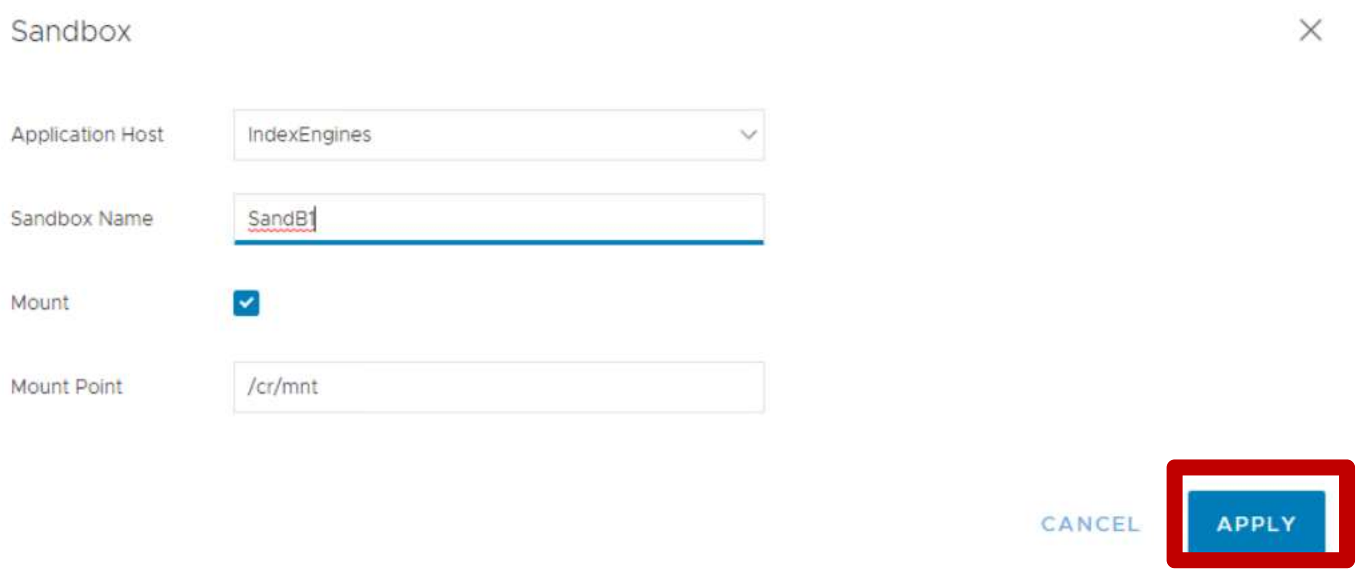
Application Host: NetWorkerDR

Storage User:

Storage Password:



□	Copy Name	Policy Name	Creation Date	Expires On
☑	cr-copy-userfile-20191122022154	userfiles	Nov 22, 2019, 7:21:54 AM	Nov 22, 2019, 8:22:00 PM
□	cr-copy-userfile-20191121180002	userfiles	Nov 21, 2019, 11:00:02 PM	Nov 22, 2019, 12:00:35 PM
□	cr-copy-userfile-20190919070002	userfiles	Sep 19, 2019, 12:00:02 PM	Sep 20, 2019, 1:00:41 AM
□	cr-copy-userfile-20190918190002	userfiles	Sep 19, 2019, 12:00:02 AM	Sep 19, 2019, 1:00:22 PM



Sandbox

Application Host: IndexEngines

Sandbox Name: SandB1

Mount: ☑

Mount Point: /cr/mnt

Proactive Analytics in the CR Vault

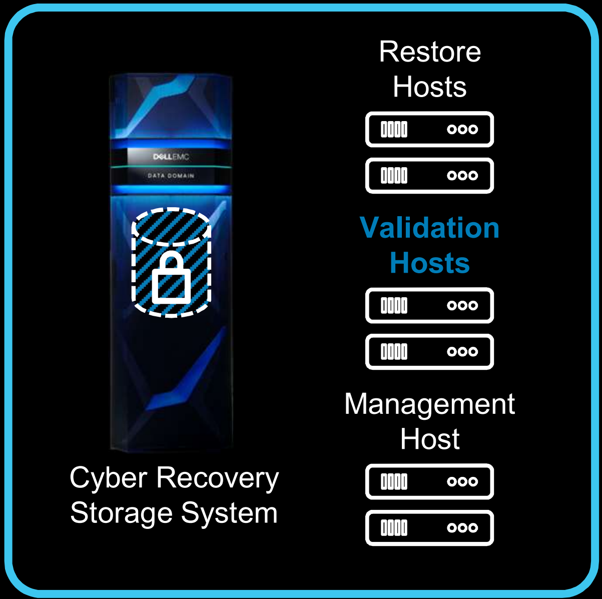
Why Analytics in the Vault?

- Increase effectiveness of Prevent/Detect cybersecurity when performed in protected environment.
- Diagnosis of attack vectors can take place within an isolated workbench.
- App restart activities can detect attacks that only occur when application is initially brought up.

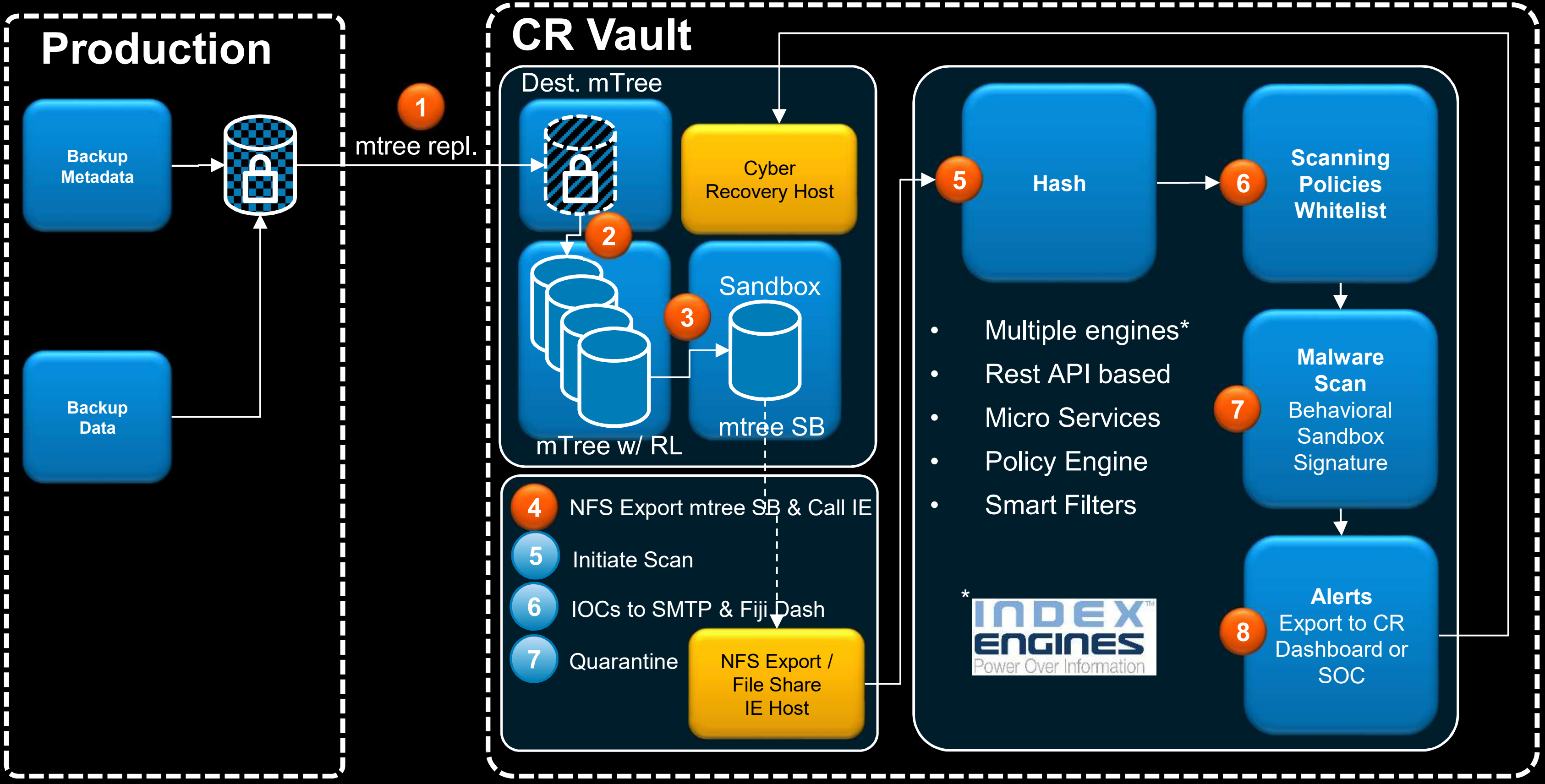
Categories of Data

- Transactional Data – dynamic/large (log variances, sentinel records, etc.)
- Intellectual Property – static/large (checkums, file entropy)
- Executables / Config. Files – static/small (checksums, malware scans)

CYBER RECOVERY VAULT



FLEXIBLE IN-VAULT SECURITY ANALYTICS



Production

Backup Metadata

Backup Data

1 mtree repl.

CR Vault

Dest. mTree

Cyber Recovery Host

2

mTree w/ RL

3

Sandbox

mtree SB

4 NFS Export mtree SB & Call IE

5 Initiate Scan

6 IOCs to SMTP & Fiji Dash

7 Quarantine

NFS Export / File Share IE Host

5 Hash

6 Scanning Policies Whitelist

- Multiple engines*
- Rest API based
- Micro Services
- Policy Engine
- Smart Filters

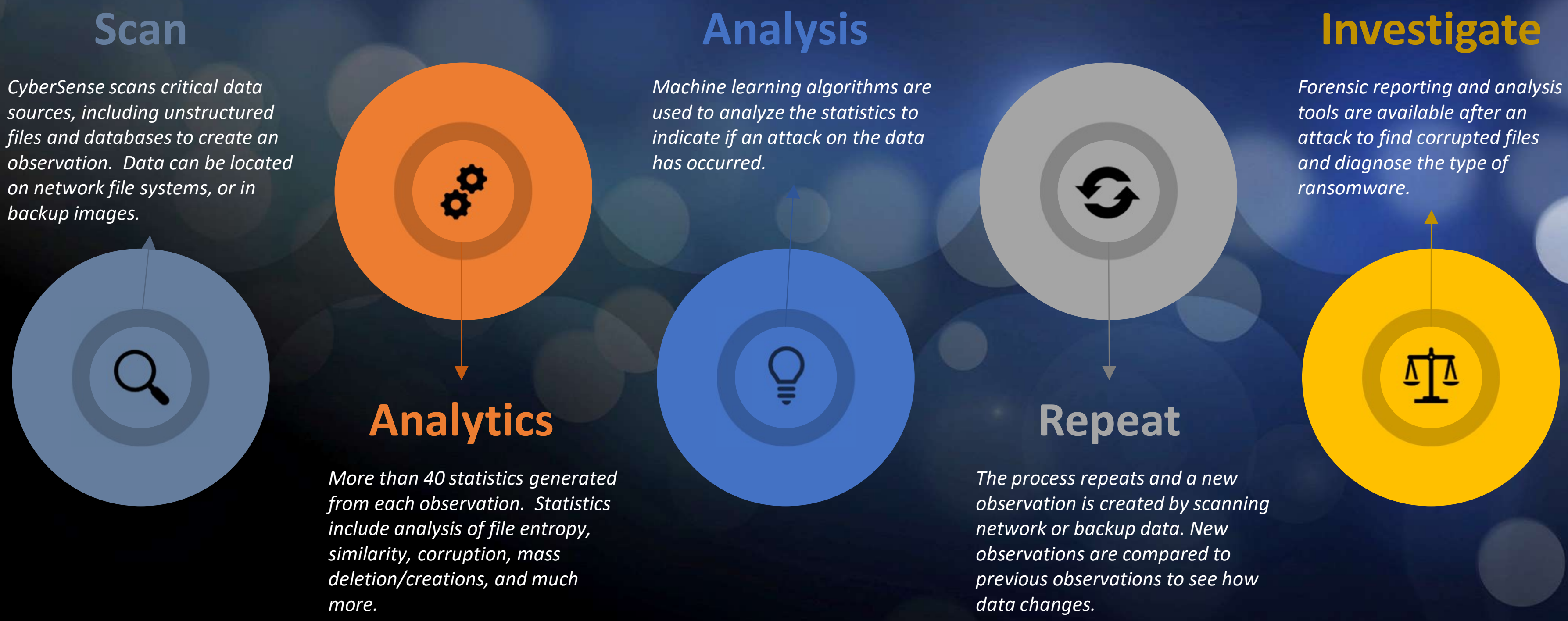
7 Malware Scan Behavioral Sandbox Signature

8 Alerts Export to CR Dashboard or SOC

* INDEX ENGINES Power Over Information

Finding Indicators of Compromise in Your Backup

Index Engines CyberSense^{TM}



Scan

CyberSense scans critical data sources, including unstructured files and databases to create an observation. Data can be located on network file systems, or in backup images.

Analytics

More than 40 statistics generated from each observation. Statistics include analysis of file entropy, similarity, corruption, mass deletion/creations, and much more.

Analysis

Machine learning algorithms are used to analyze the statistics to indicate if an attack on the data has occurred.

Repeat

The process repeats and a new observation is created by scanning network or backup data. New observations are compared to previous observations to see how data changes.

Investigate

Forensic reporting and analysis tools are available after an attack to find corrupted files and diagnose the type of ransomware.

Dell EMC Services for Cyber Recovery Solution

Deployment

New deployment services from Dell EMC Services accelerates the value of Data Domain based Cyber Recovery Solution. These implementation services are available in two sizes to fit customer needs based on number of MTrees and data subsets

Workshop

Dell EMC Consulting leads a facilitated Business Resiliency workshop with key stakeholders to share Dell EMC best practices for resiliency including IT Continuity, data protection, with an emphasis cyber recovery

Advisory Services

Dell EMC Consulting Advisory services include the workshop and provide customers with a deeper understanding of the solution, specific data to contain in the vault, and advises on roadmap and custom solution design. These offers scale based on the customer’s specific needs.

For More information: https://www.dellemc.com/resources/en-us/auth/services/consulting/it-transformation/resiliency.htm

Cyber Recovery

The Last Line of Data Protection Defense Against Cyber-Attacks

The Challenge

93%

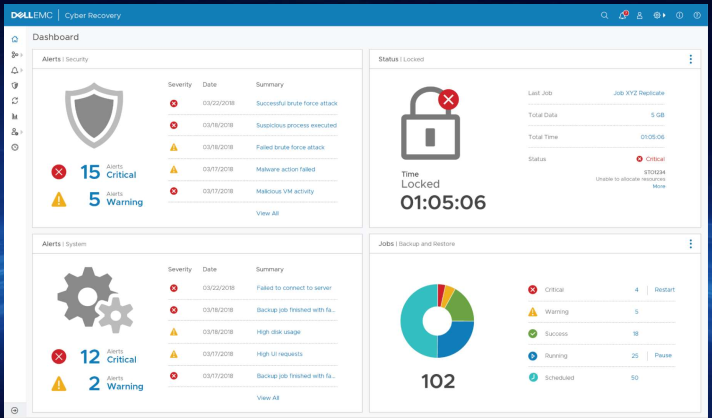
CAGR in Ransomware variants from 2010 to 2016

92%

Organizations cannot detect cyber-attacks quickly

59%

Believe that isolating affected systems and recovering from backups should be the response to ransomware



DELLEMC | Cyber Recovery

Dashboard

Alerts | Security

15 Alerts Critical

5 Alerts Warning

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

View All

Status | Locked

Time Locked 01:05:06

Last Job	Job XYZ Replicate
Total Data	5 GB
Total Time	01:05:06
Status	⊗ Critical

STO1234
Unable to allocate resources
More

Alerts | System

12 Alerts Critical

2 Alerts Warning

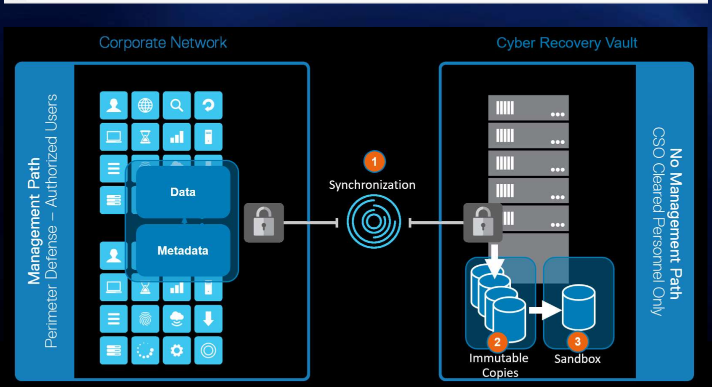
Severity	Date	Summary
⊗	03/22/2018	Failed to connect to server
⊗	03/18/2018	Backup job finished with fa...
⚠	03/18/2018	High disk usage
⚠	03/17/2018	High UI requests
⊗	03/17/2018	Backup job finished with fa...

View All

Jobs | Backup and Restore

102

⊗	Critical	4	Restart
⚠	Warning	5	
✓	Success	18	
▶	Running	25	Pause
●	Scheduled	50	



Cyber Recovery

- End-to-End Automated Workflow
- Modern & Simple UI/UX
- Flexible Rest API
- Fully Supported
- Enables Vault Analytics*

Consulting Services Available!!!

- Seamless ProDeploy Packages
- L1 CyberAdvisory Services

* INDEX ENGINES Power Over Information

Questions…

Daniel.Olkowski@dell.com