DELL EMC CYBER RECOVERY

DATA PROTECTION AND RECOVERY WHEN YOU NEED IT MOST.

GET STARTED

DELL EMC CYBER RECOVERY

DATA PROTECTION AND RECOVERY WHEN YOU NEED IT MOST.

INDUSTRY SNAPSHOT

COMMON VULNERABILITIES

THE SOLUTION

ADDITIONAL RESOURCES

CLICK A BOX TO NAVIGATE

BACK

INDUSTRY SNAPSHOT

39%

of detected malware is ransomware[*]

92%

of organizations can't detect cyberattacks quickly[†]

67%

of organizations had incidents with a negative impact in past 12 months[‡]

Sources

[*] *2018 Verizon Data Breach*

[†] Gartner Research, Shift in Cybersecurity Investment to Detection, January 2016

[‡] RSA Cybersecurity Poverty Index

● ○ ○ NEXT

DELL EMC

INDUSTRY SNAPSHOT

TRUE COST OF RANSOMWARE

Ransom: $30,000

Lost Revenue: $2,500,000
Incident Response: $75,000
Legal Advice: $70,000
Lost Productivity: $250,000
Forensics: $75,000
Recovery & Re-Imaging: $60,000
Data Validation: $25,000
Brand Damage: $500,000
Litigation: $200,000

Total Cost of Attack:

$3,785,000

PREV ○ ● ○ NEXT

INDUSTRY SNAPSHOT

RELIABLE DATA PROTECTION, DELIVERED WHERE YOU NEED IT MOST.

Protecting your organization from the inevitability of cyberattacks – especially ransomware – requires a multi-layered approach. You've got to prevent attacks (of course), but you've also got to be prepared for the worst.

Dell EMC Cyber Recovery protects your organization's most critical data within an isolated secure vault. Through an innovative REST API-based automation approach, your data is removed from the attack surface. Additionally, Cyber Recovery brings flexibility in automating robust analytics by integrating custom or well-known industry tools into your workflow. This facilitates a robust and proactive workflow to help increase cyber resilience throughout your organization.

PREV ○ ○ ●

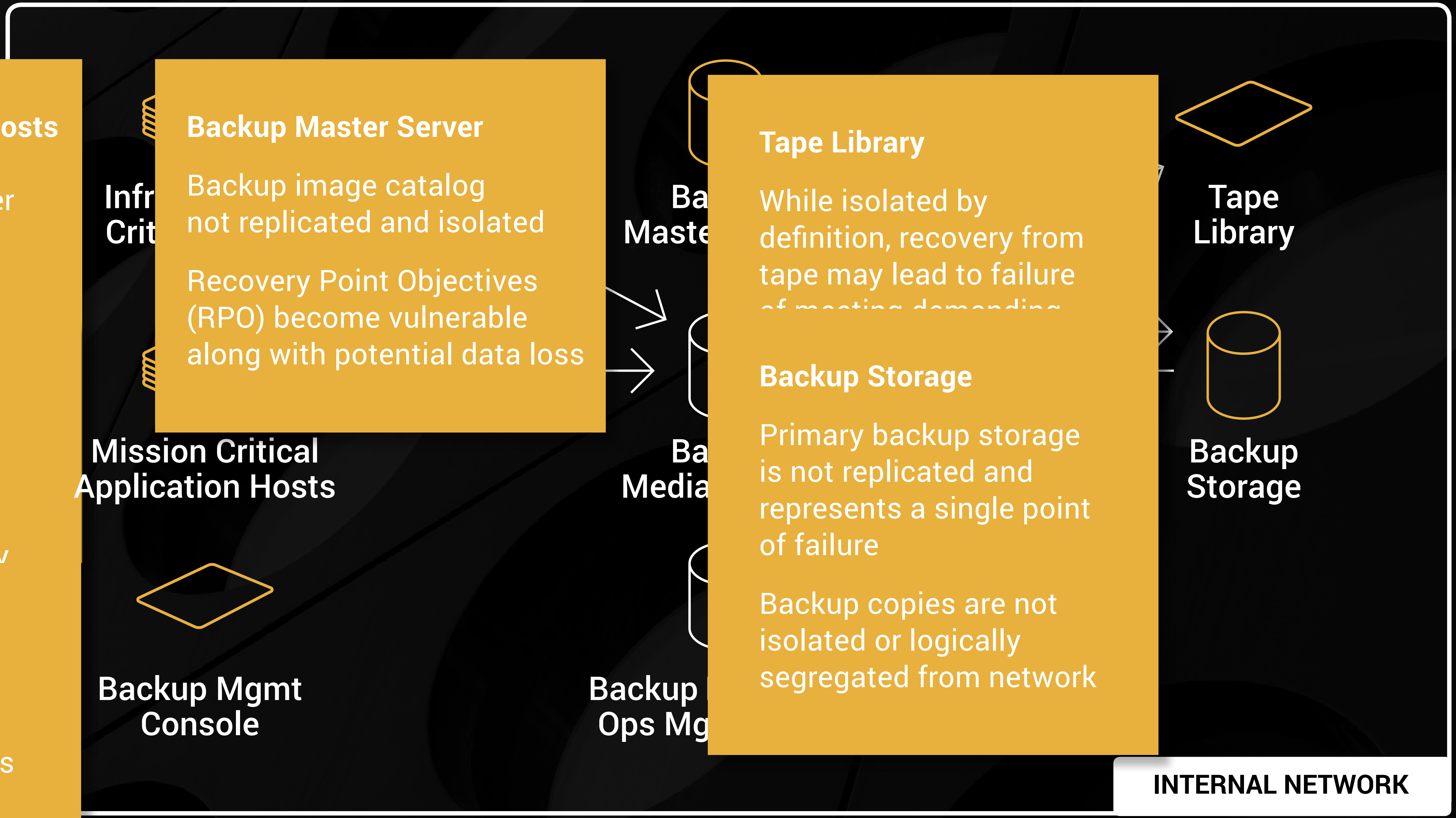
DELL EMC

COMMON VULNERABILITIES →

COMMON VULNERABILIT

ROLL OVER ICONS FOR DETAILS

TECHNICAL



Infrastructure Critical Hosts

Key infrastructure server (i.e., Domain Controller) backup images may be prematurely expired

Mission Critical Application Hosts

Key application data, transactional systems, and intellectual property

Backup Mgmt Console

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

Backup Master Server

Backup image catalog not replicated and isolated

Recovery Point Objectives (RPO) become vulnerable along with potential data loss

Tape Library

While isolated by definition, recovery from tape may lead to failure of meeting demanding

Backup Storage

Primary backup storage is not replicated and represents a single point of failure

Backup copies are not isolated or logically segregated from network

● ○ ○ NEXT

DELL EMC

COMMON VULNERABILIT

ROLL OVER ICONS FOR DETAILS

PEOPLE & PROCESS

Infrastructure Critical Hosts

Bad actors (external or internal) deploy malicious code or circumvent access restrictions to corrupt and destroy configuration and application data

Backup Master Server

Bad Actor prematurely expires backup images from backup infrastructure catalog, or destroys primary

Backup Media Servers

Bad Actor gains access to backup catalog and destroys TBs of critical data backup images

Tape Library

Backup tapes are stolen, lost or maliciously destroyed

Backup Storage

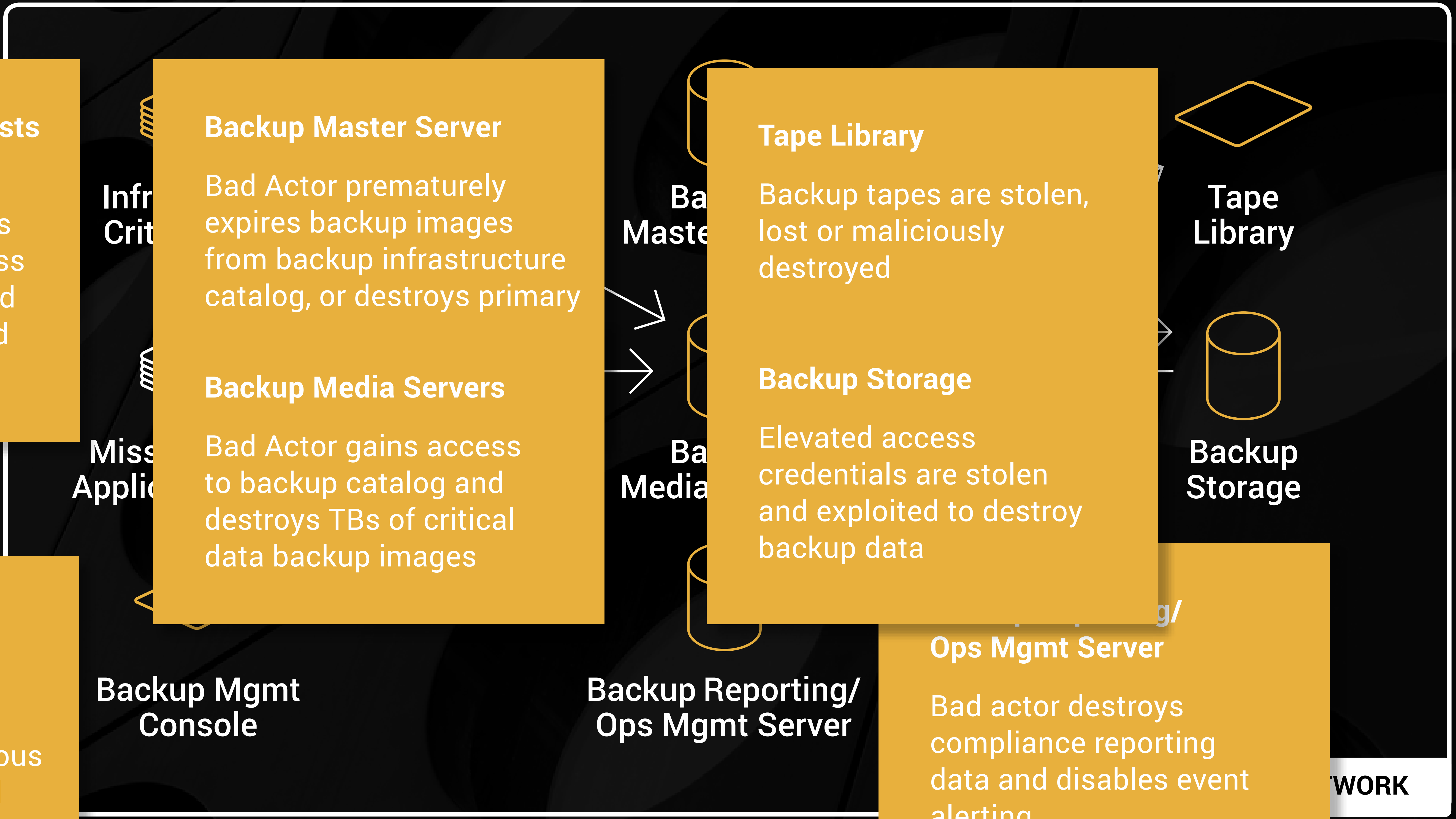
Elevated access credentials are stolen and exploited to destroy backup data

Backup Mgmt Console

Admin’s laptop is compromised and exploited to host malicious code, destroying normal backup operations and configuration information

g/
Ops Mgmt Server

Bad actor destroys compliance reporting data and disables event alerting



PREV ○ ● ○ NE

DELL EMC

COMMON VULNERABILITIES

RISK PROFILE SUMMARY

TECHNICAL

- All data is currently susceptible to a cyberattack
- Primary storage replication can replicate corruption
- Backup catalog not replicated
- Recovery of backup catalog from tape is slow and failure-prone
- Backup copies not isolated from network

PEOPLE & PROCESS

- IT Engineering and Ops have access to most if not all Backup Assets
- Security teams not assigned to assets. Bad actors inside the firewall can create havoc.
- Franchise critical and non-critical data are not segregated
- Backup images can be expired without authorization

These risks are consistent with traditional disaster recovery models. This is a different challenge and requires a different architecture.

PREV ○ ○ ●

DELL EMC

THE SOLUTION →

THE SOLUTION

DISASTER RECOVERY VS. CYBER RECOVERY

Traditional disaster recovery solutions are ill-equipped to recover from a cyberattack.

	DR	CR
Recovery Time	Close to Instant	Reliable & Fast
Recovery Point	Ideally Continuous	1 Day Average
Nature of Disaster	Flood, Power Outage, Weather	Cyberattack, 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 Foundation SVCs
Recovery	Standard DR (e.g., failback)	Iterative, selective recovery; part of IR

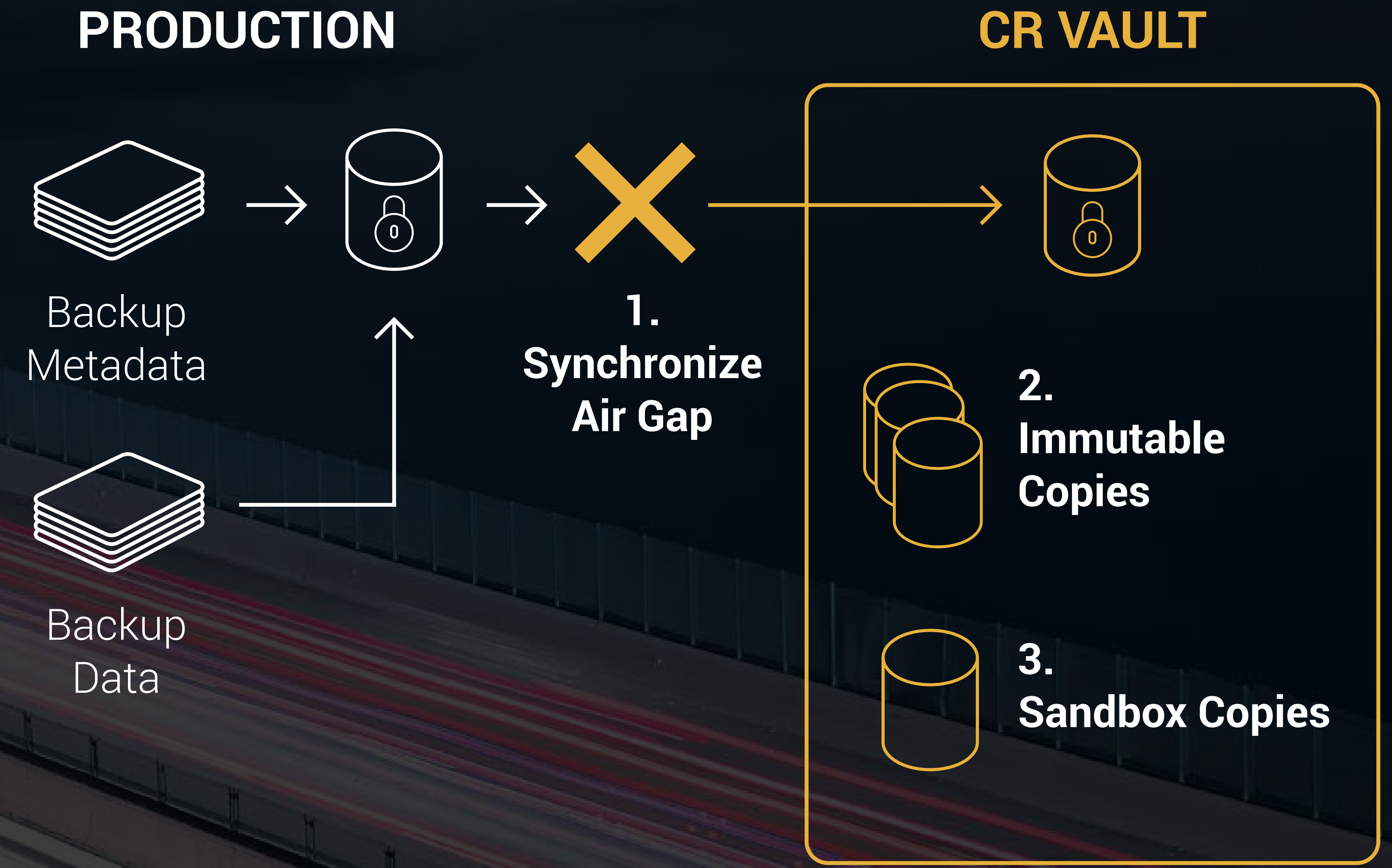
● ○ ○ ○ NEXT

DELLEMC

THE SOLUTION

CYBER RECOVERY SOFTWARE

- End-to-end workflow automation
- Runs only in CR Vault
- Creates 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



PREV ○ ● ○ ○ NEXT

DELL EMC

THE SOLUTION

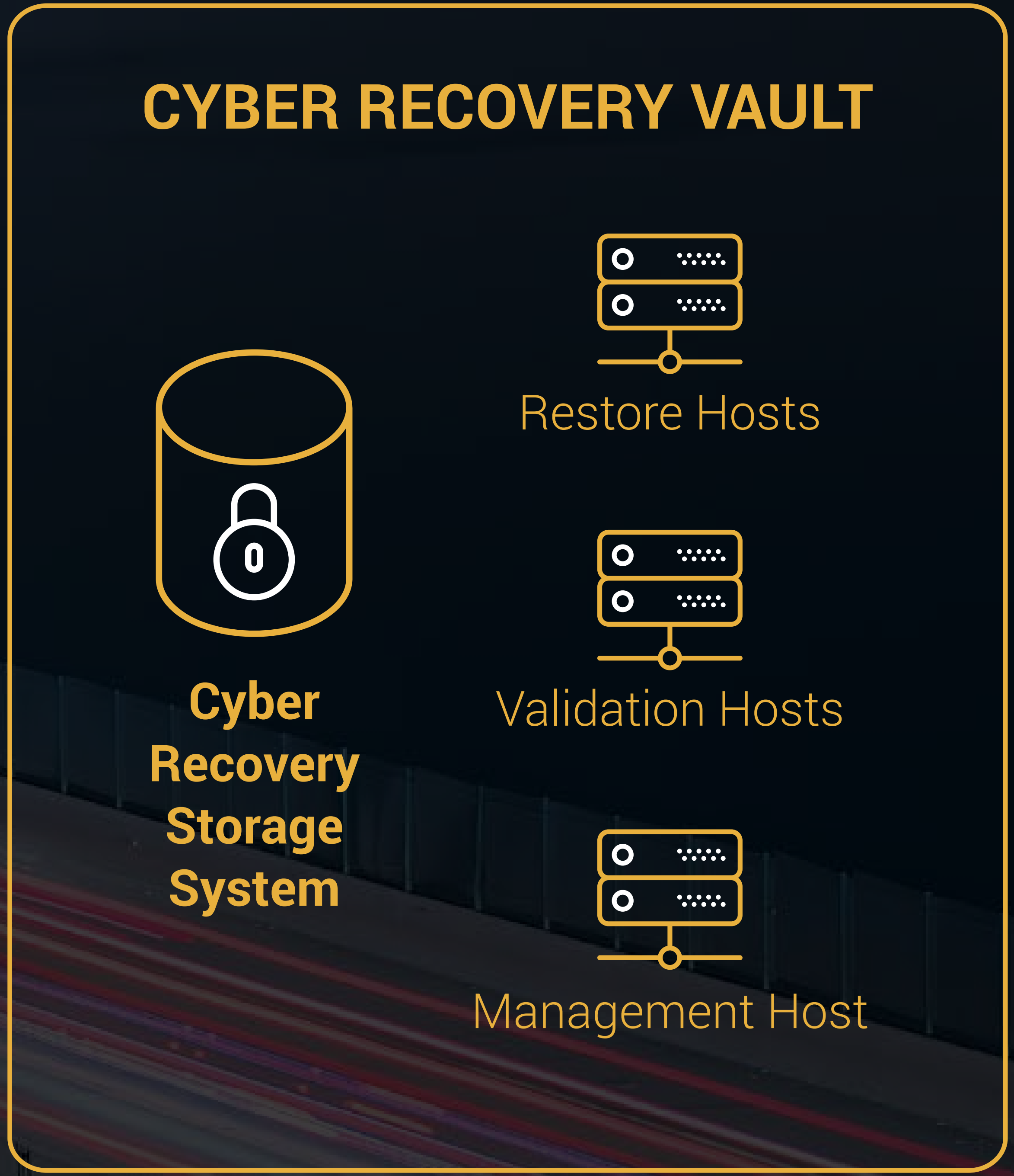
PROACTIVE ANALYTICS IN THE CR VAULT

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 (checksums, file entropy)
- Executables / Config. Files – static/small (checksums, malware scans)



CYBER RECOVERY VAULT

Cyber Recovery Storage System

Restore Hosts

Validation Hosts

Management Host

PREV ○ ○ ● ○ NEXT

DELLEMC

THE SOLUTION

ADDITIONAL CYBER RECOVERY SERVICES

DEPLOYMENT

New deployment services from Dell EMC Services accelerate the value of Data Domain based Cyber Recovery Solution. These implementation services are available in two sizes to fit your 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 and data protection, with an emphasis on cyber recovery.

ADVISORY SERVICES

Dell EMC Consulting Advisory services include the workshop and provide you 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 your specific needs.

PREV ○ ○ ○ ●

DELL EMC

ADDITIONAL RESOURCES →

ADDITIONAL RESOURCES

Case Study: Founder's Federal Credit Union

▷ WATCH VIDEO

Managing Cyber Risk As A Business Issue

Business Cyber Risk Bulletin

DOWNLOAD PDF

DELL EMC
ASSESS YOUR SYSTEM
ADVISE YOU ON AIR GAPPED VAULT
DESIGN YOUR RECOVERY PROCESSES

Learn more about our Cyber Recovery Solution

▷ WATCH VIDEO

DELL EMC

CYBER RECOVERY

Cyber Recovery Solution Overview

DOWNLOAD PDF

● ○ NEXT

DELL EMC

ADDITIONAL RESOURCES

Enterprise Strategy Group | Getting to the bigger truth.™

White Paper

Cyber Resiliency with the Dell EMC Cyber Recovery Solution

Dell EMC Cyber Recovery and its Data Isolation Architecture Provide Technologies and Services to Protect Data Assets Effectively

By Christophe Bertrand, ESG Senior Analyst
Doug Cahill, ESG Group Director and Senior Analyst
and Monya Keane, ESG Senior Research Analyst
November 2018

[illegible]

Analyst Report:
Cyber Recovery

DOWNLOAD PDF

78% of organizations have a formal/documented incident response plan in place, or are currently developing one.

ESG Video:
Cyber Recovery

WATCH VIDEO

PREV ○ ●

DELL EMC