Protecting from Next Generation Cyber threats

Sidharth Joshi,

Senior Manager, Systems Engineering

4th October 2019, Mongolia

DELL EMC

THREAT LANDSCAPE EVOLVING – BIZ @ RISK

76%
of breaches are financially motivated

39%
of detected malware is Ransomware (#1 variety)

93%
CAGR in Ransomware variants from 2010 to 2016

>100
Average dwell time of a cyber-attack in days

24%
Organizations satisfied with their ability to detect and investigate

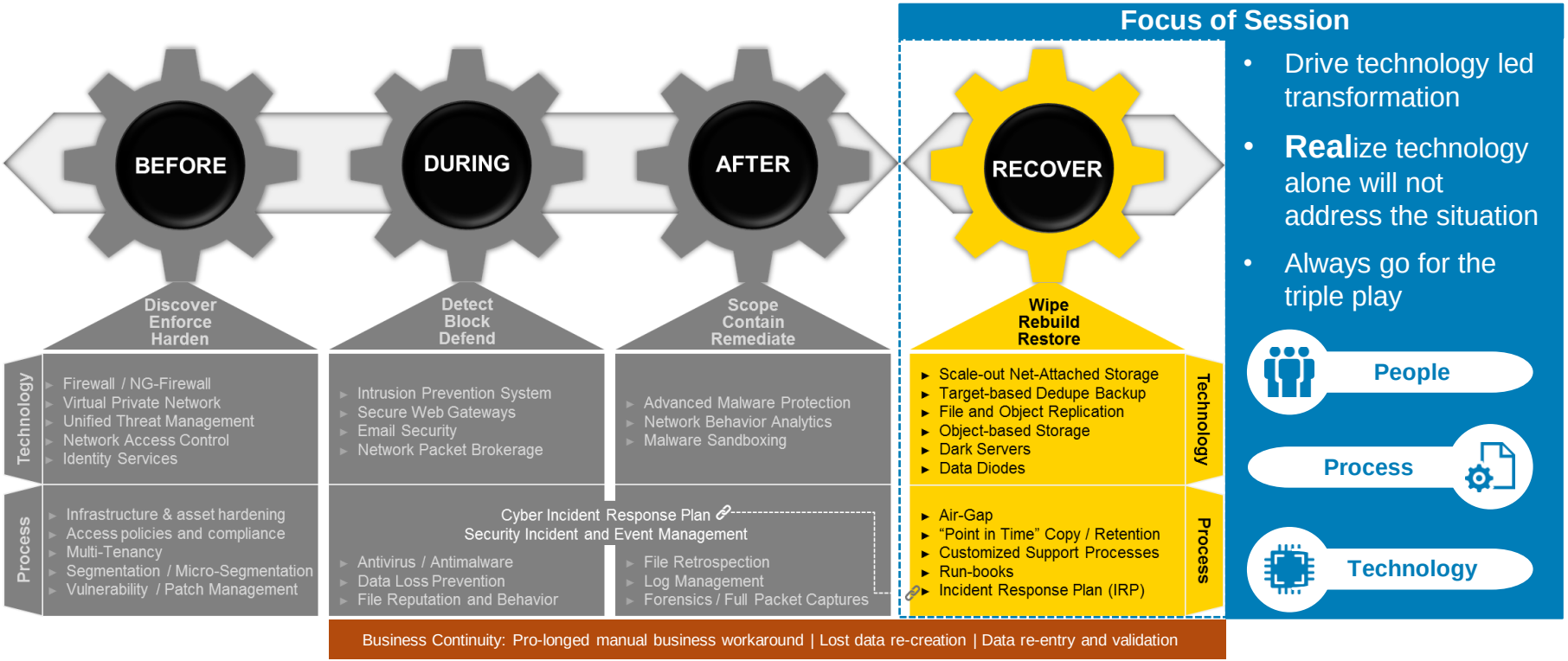
92%
Organizations cannot detect cyber-attacks quickly

59%
Believe that isolating affected systems and recovering from backups should be the response to ransomware

60%
CISOs actively involved in data recovery planning as part of incident response

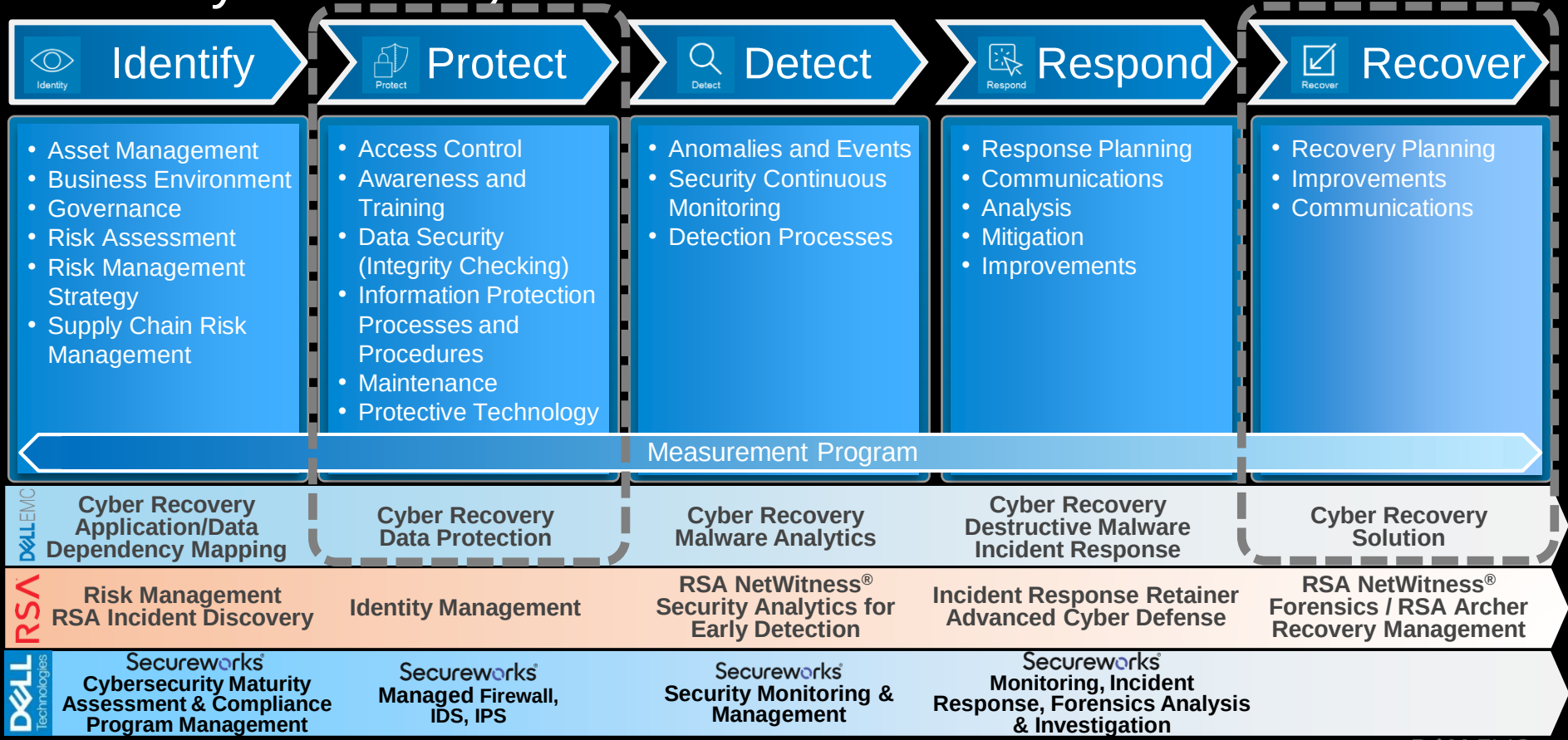
Cyber Resiliency Technology Solution

Enhancing recovery capabilities

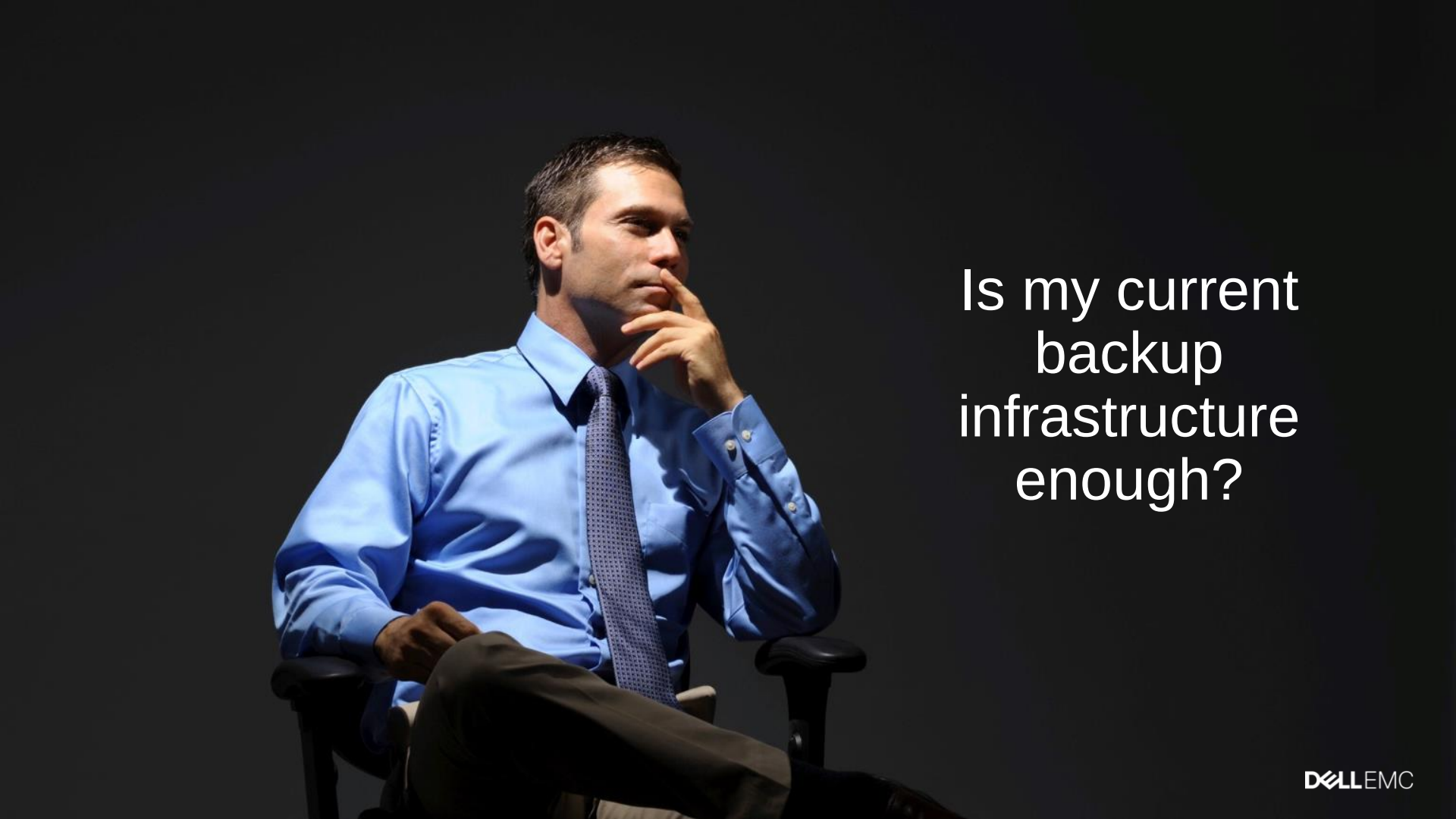


NIST Cybersecurity Framework

Focus



Dell Technologies Aligned Solutions & Services

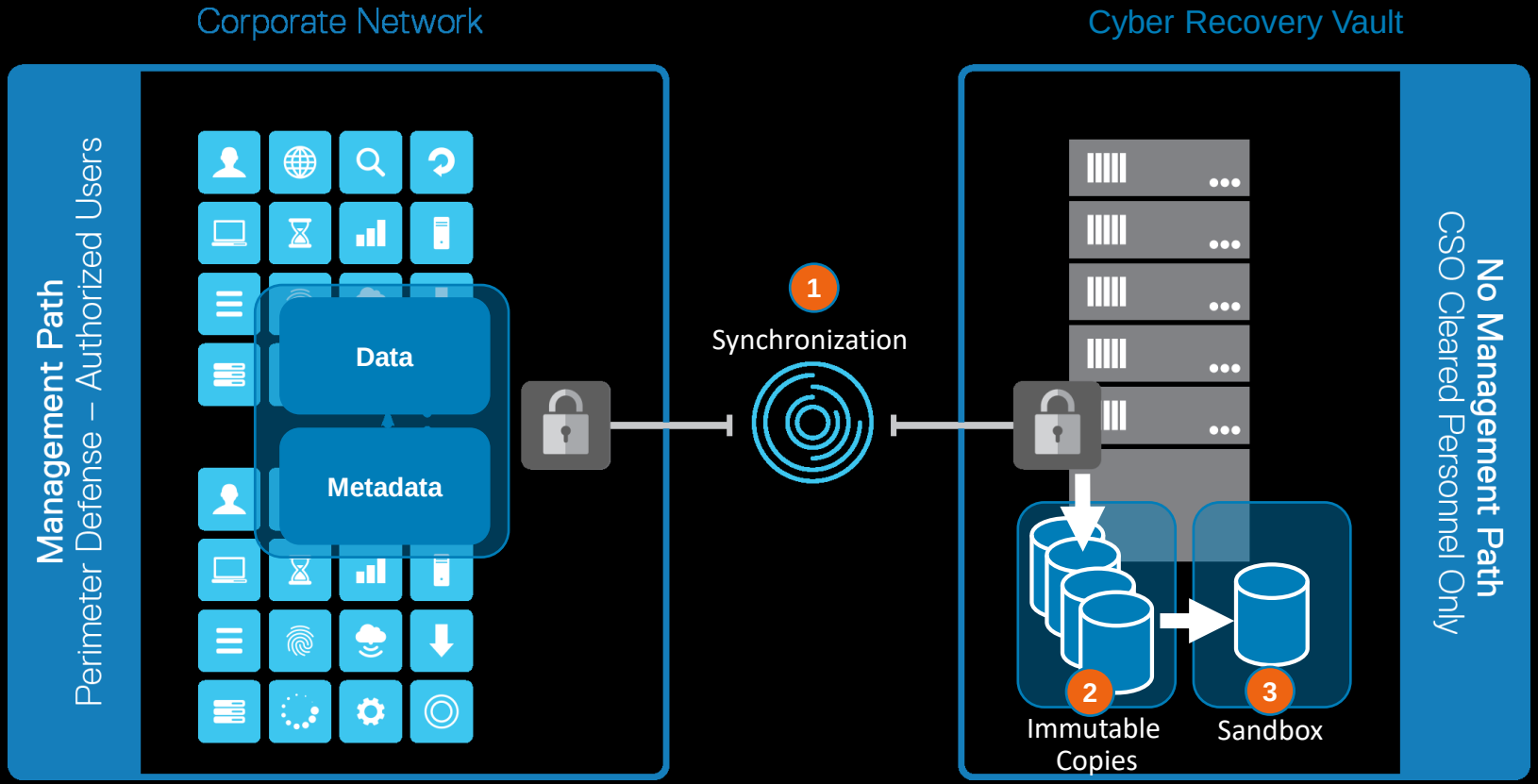

Is my current backup infrastructure enough?

Current State: Risk Profile Summary

Technical	People & Process
All data is currently susceptible to a cyber attack	IT Engineering and Ops have access to most if not all Backup Assets
Primary storage replication can replicate corruption	Security teams not assigned to assets. Bad actors inside the firewall can create havoc.
Backup catalog not replicated	Franchise critical and non-critical data are not segregated
Recovery of backup catalog from tape is slow and failure prone	Backup images can be expired without authorization
Backup copies not isolated from network	

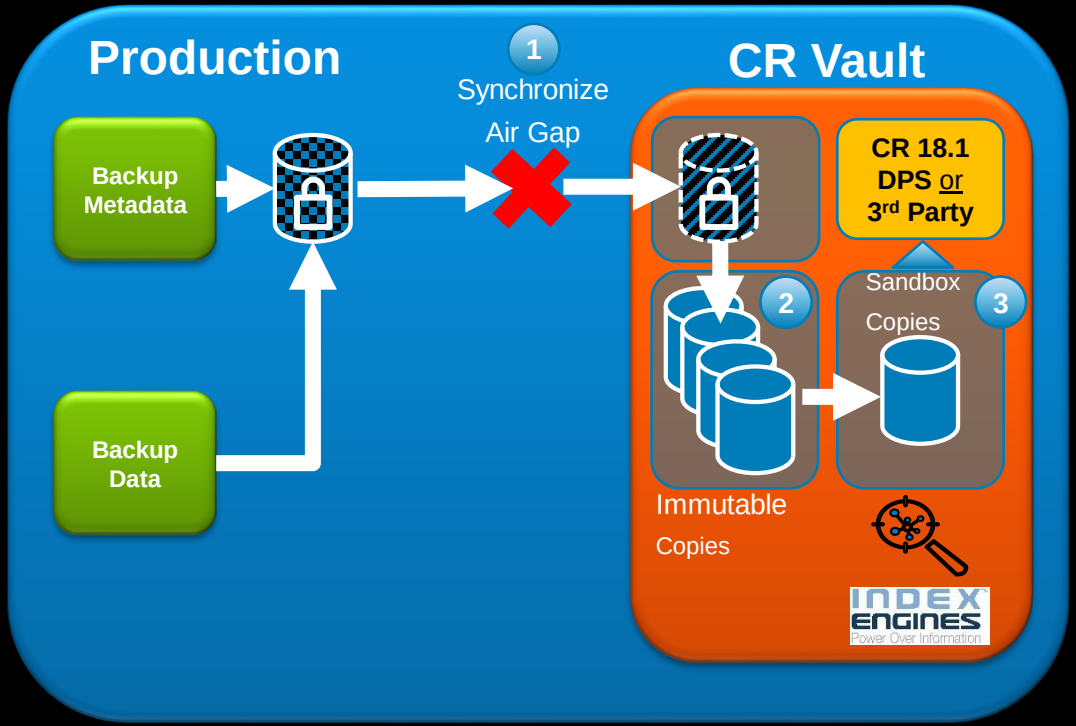
- These risks are consistent with traditional Prod/DR models.
- This is a different challenge and requires a different architecture.

Dell EMC Cyber Recovery



Cyber Recovery Benefits

- End-to-End workflow automation SW including automated recovery
- 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

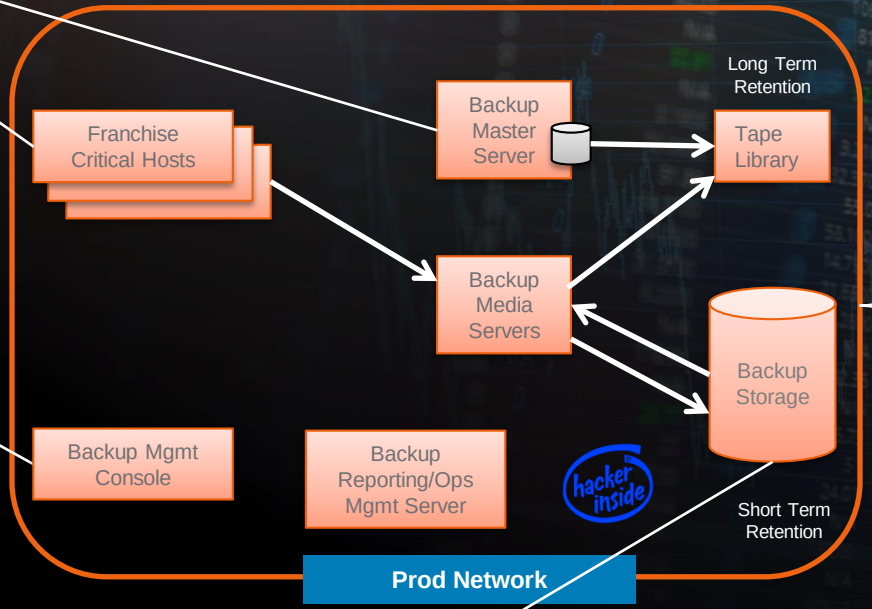


Proposed: Exposures Resolved and Remaining

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

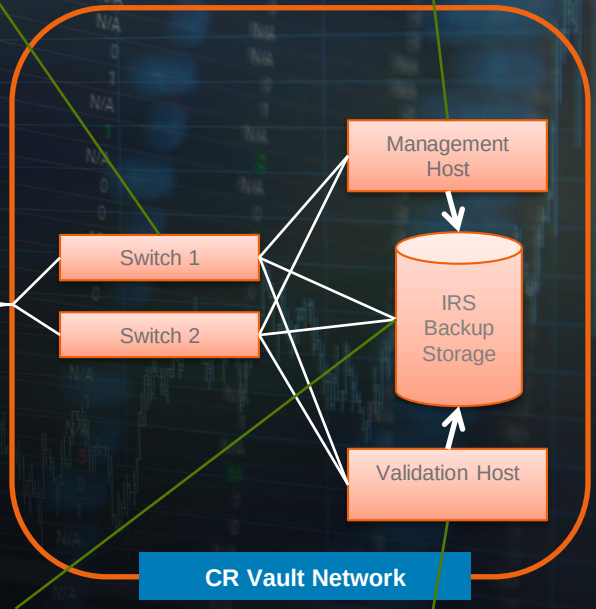


Backup copies are not isolated or logically segregated from network

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

Air Gap

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



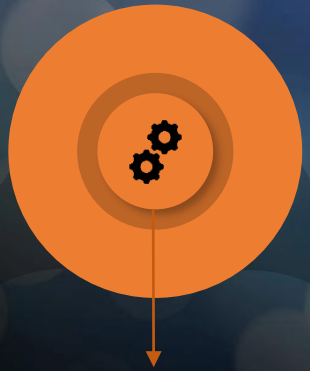
CR copies are isolated and Compliance/WORM locked.
No destructive actions without dual role authentication

Validation host ensures usability of CR copies and alerting of corruption

Finding Indicators of Compromise in Your Backup

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.

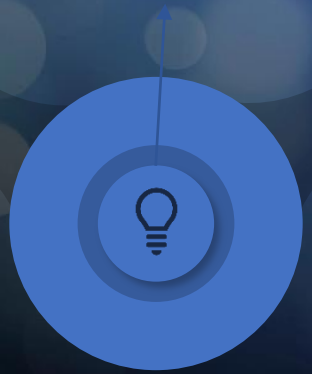


Analytics

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.

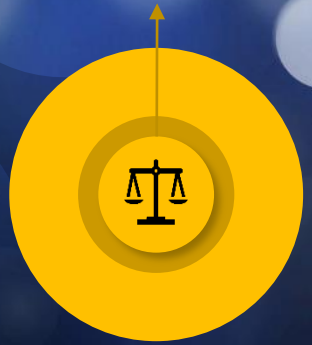


Repeat

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.



INDEX ENGINES Power Over Information

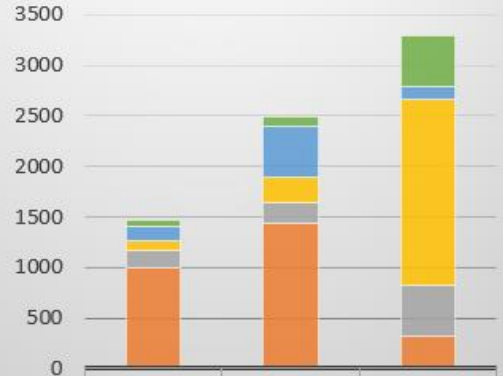
DELL EMC

Data Integrity Check

Assessment of Data Quality on Initial Scan

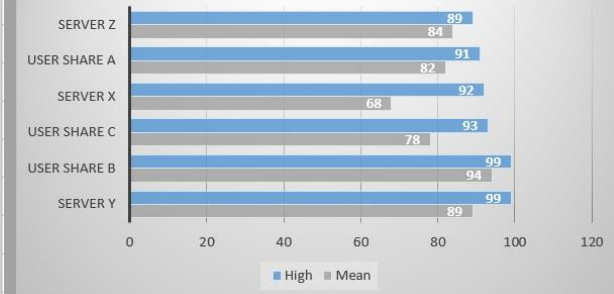
File Count/by Type

(Thousands)

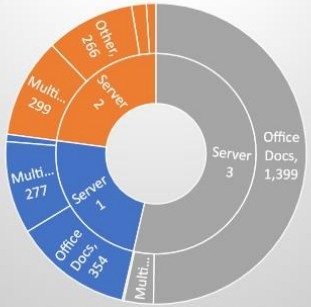


	Server X	Server Y	Server Z
Other	59	100	493
Email	147	498	131
Multimedia	88	249	1841
Text	176	199	493
Office Docs	998	1444	329

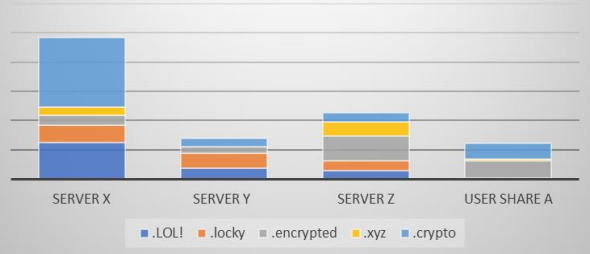
Mean/High Entropy Server Score



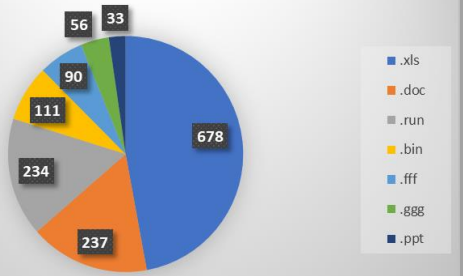
Corrupt Files by Server/Type



Known Ransomware Extension by Location



File Types Entropy Score of 99



Cyber Recovery

The Last Line of Data Protection Defense Against Cyber-Attacks

The Challenge

93%

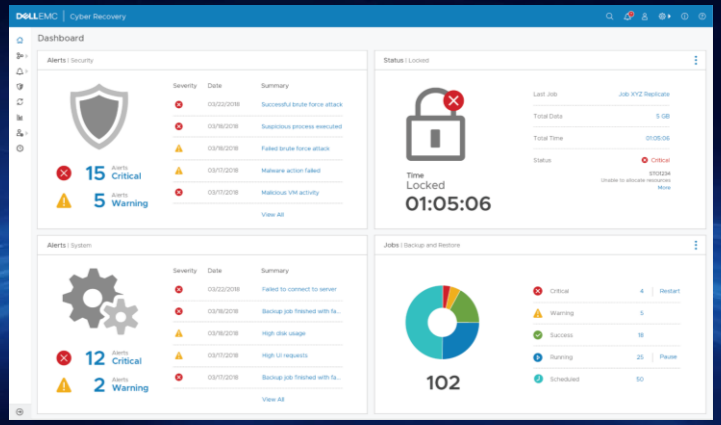
CAGR in Ransomware variants from 2010 to 2016

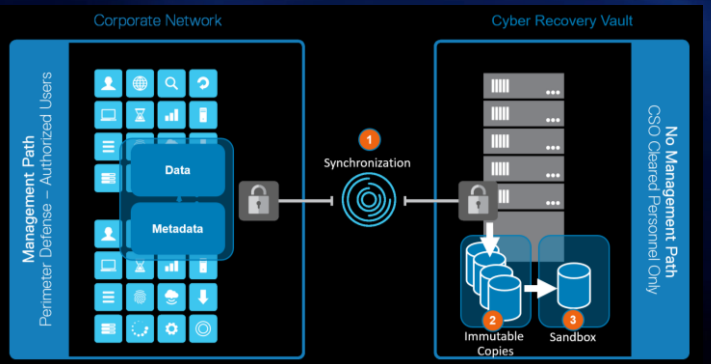
92%

Organizations cannot detect cyber-attacks quickly

59%

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





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


DELL EMC