

SNIA COMPUTE + MEMORY
+ STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Cyber Recovery & Resilience

Jim Shook

Director, Cybersecurity & Compliance
Practice

Dell Technologies



Actively licensed attorney
Litigator and General Counsel for 10+ years
BS, Computer Science (Programming)
CISSP, CIPP/US

Founded Cyber & Compliance Practice in 2015
Joint Steering Committee, Sheltered Harbor
Sedona Conference Think Tank - WG11 Leadership



Cyber Security, Cyber Recovery, and Cyber Crime

75%

of IT organizations will face one or more **RANSOMWARE THREATS** by 2025

Gartner, 2021

72%

of IT organizations **REPORT NEEDING EXTERNAL HELP** making sure they cover all the IT Security and Risk requirements

Forrester Consulting, 2020

24
days

The **AVERAGE DOWNTIME** after a Ransomware attack

Coveware 2022

2
hours

breakout time – the **TIME** it takes intruder to begin **MOVING Laterally** into other systems in the network after compromising a machine

CrowdStrike 2022

71%

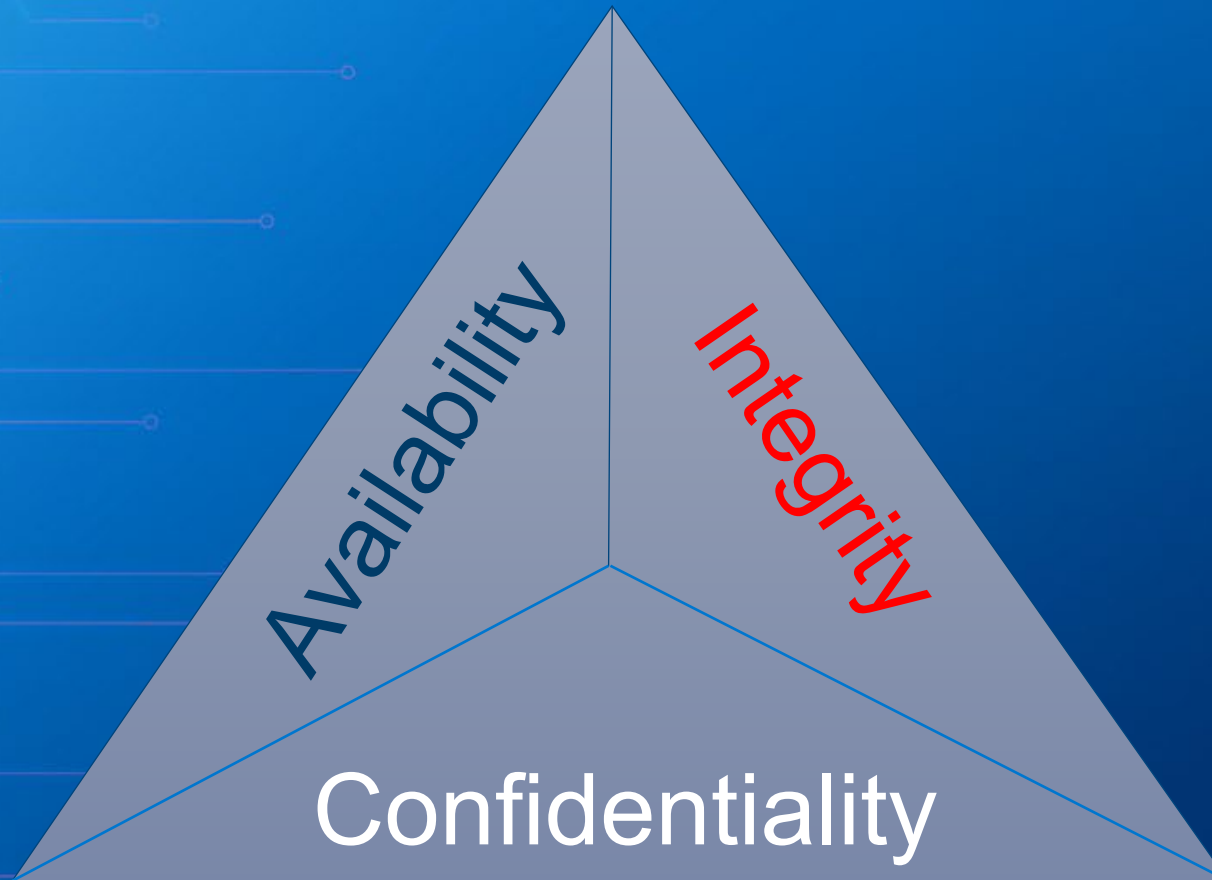
of attacks comprise use of **NON-MALWARE, HANDS-ON-KEYBOARD ACTIVITY**

CrowdStrike 2022 Global Threat Report

76%

EXPERIENCED REINFECTION following the initial cyber attack

IDC by Druva



NIST Cyber Security Framework



IDENTIFY

Identify an organization's critical functions, assets, and processes and how cyber security risks could disrupt them



PROTECT

Define safeguards necessary to protect critical infrastructure services



DETECT

Implement the right measures to identify threats and cyber risks promptly



RESPOND

Define the measures necessary to react to an identified threat



RECOVER

Strategic plans to **restore** and **recover** any capabilities damaged during a cyber security incident

The Time for Resilience is Now!

The Gartner logo is displayed in a large, bold, dark blue font on a white rectangular background. The logo consists of the word "Gartner" followed by a registered trademark symbol (®).

"Transforming cybersecurity into cyber-resilience involves prioritizing resilience over defense, and elevating the native disciplines and skills used by the business continuity management office above cybersecurity teams' traditionally defensive strategies."

Gartner, *You Will Be Hacked, So Embrace the Breach!*

"Implement at least an immutable backup copy by selecting write lock or WORM media before starting any other initiative, as having an immutable copy of the backup is the most important item to start protecting backup data."

Gartner, *Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults*

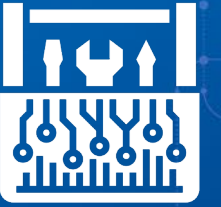
Cyber Resilience

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.



Tools for Your Resilience Journey

Your Data Protection Toolbox



Backup



Continuous
Data
Protection



Immutable
Primary
Storage



Immutability
for backups
(2-copy resilience)



Clean Rooms
& Mature
Recovery



Replication
to DR



Snapshots



Immutable
Snapshots

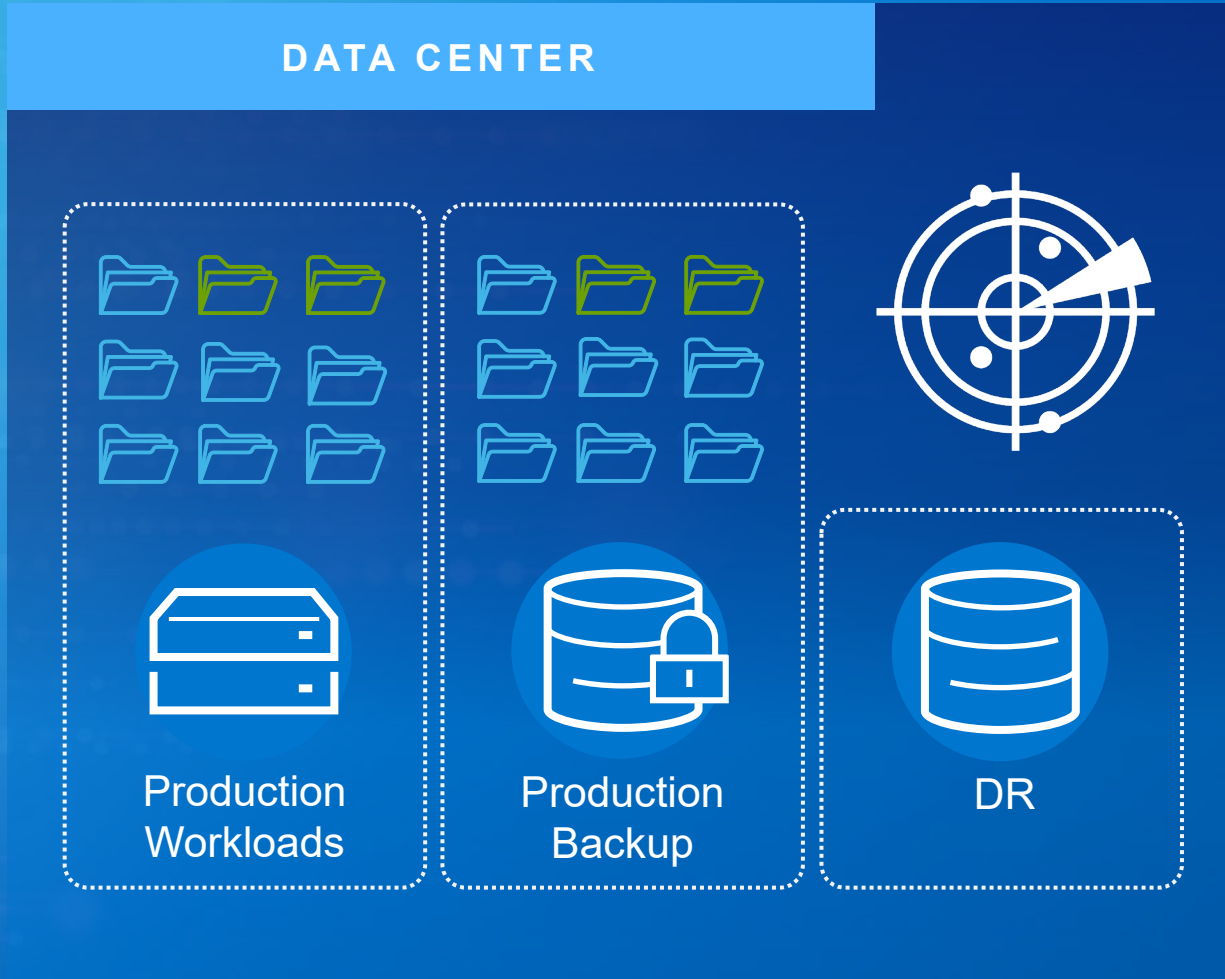


Isolated Vault
for Critical
Rebuild



Vault for Key
Applications
(3rd copy)

Data Resilience In the Production Environment



Anomaly Alerting



Alert for anomalous
behavior in the backup
environment



Monitor selected
appliance and systems
with suitable set of
rules











Supplement /
complement standard
cybersecurity tools



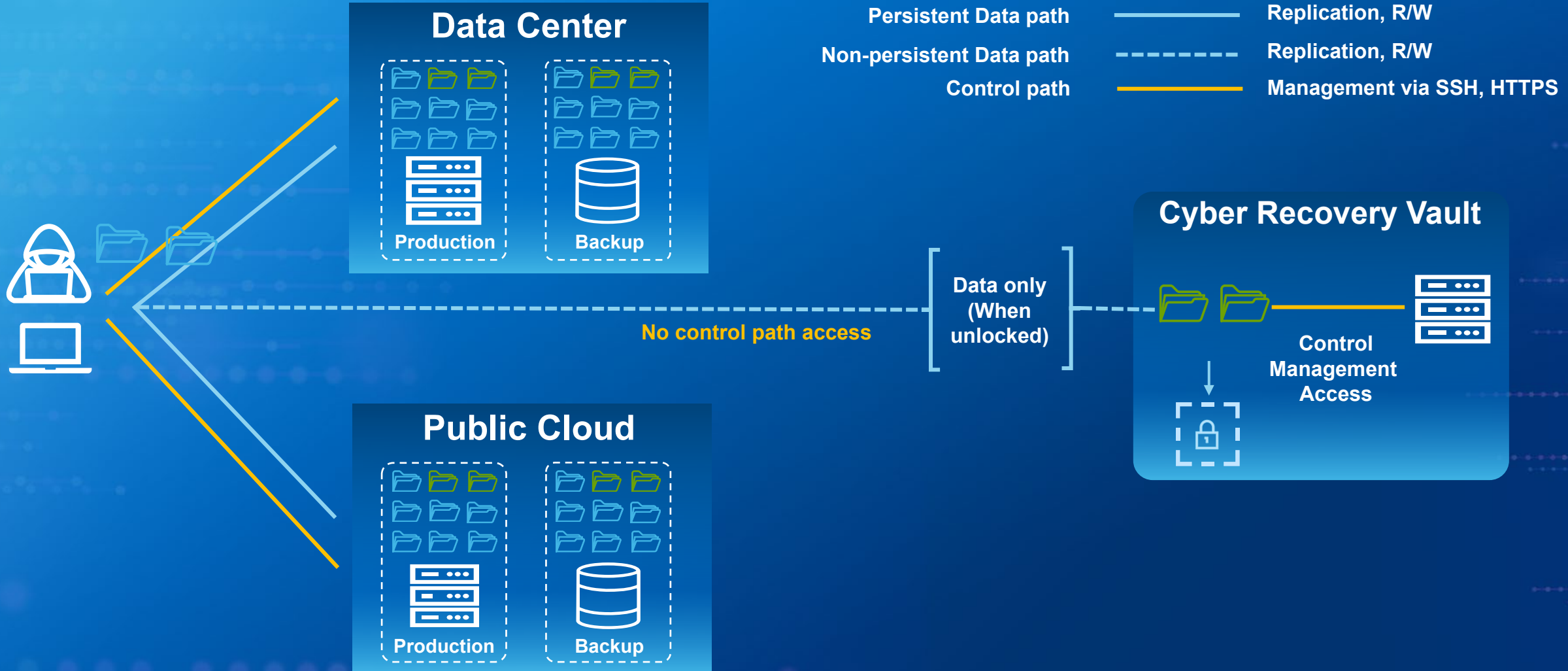
Adversarial and non-
adversarial

Worldwide Guidance

		 Hong Kong Monetary Authority	 Singapore Computer Emergency Response Team
“Create an isolated recovery environment ..”	“Ensure that backups are not connected to the business network ”	“Secure tertiary data backup should be disconnected ... [to] withstand targeted cyber attacks ... or ... malicious insiders.”	“It is important that the backup data is stored offline and not connected to your network.”
			 Australian Cyber Security Centre
“It is critical to maintain offline , encrypted backups of data”	“Data Vault requirement: ‘Air gapped’ ”	“Ensure backups are not connected to the networks they back up.”	“Daily backups of important data, software and settings, stored disconnected.... ”

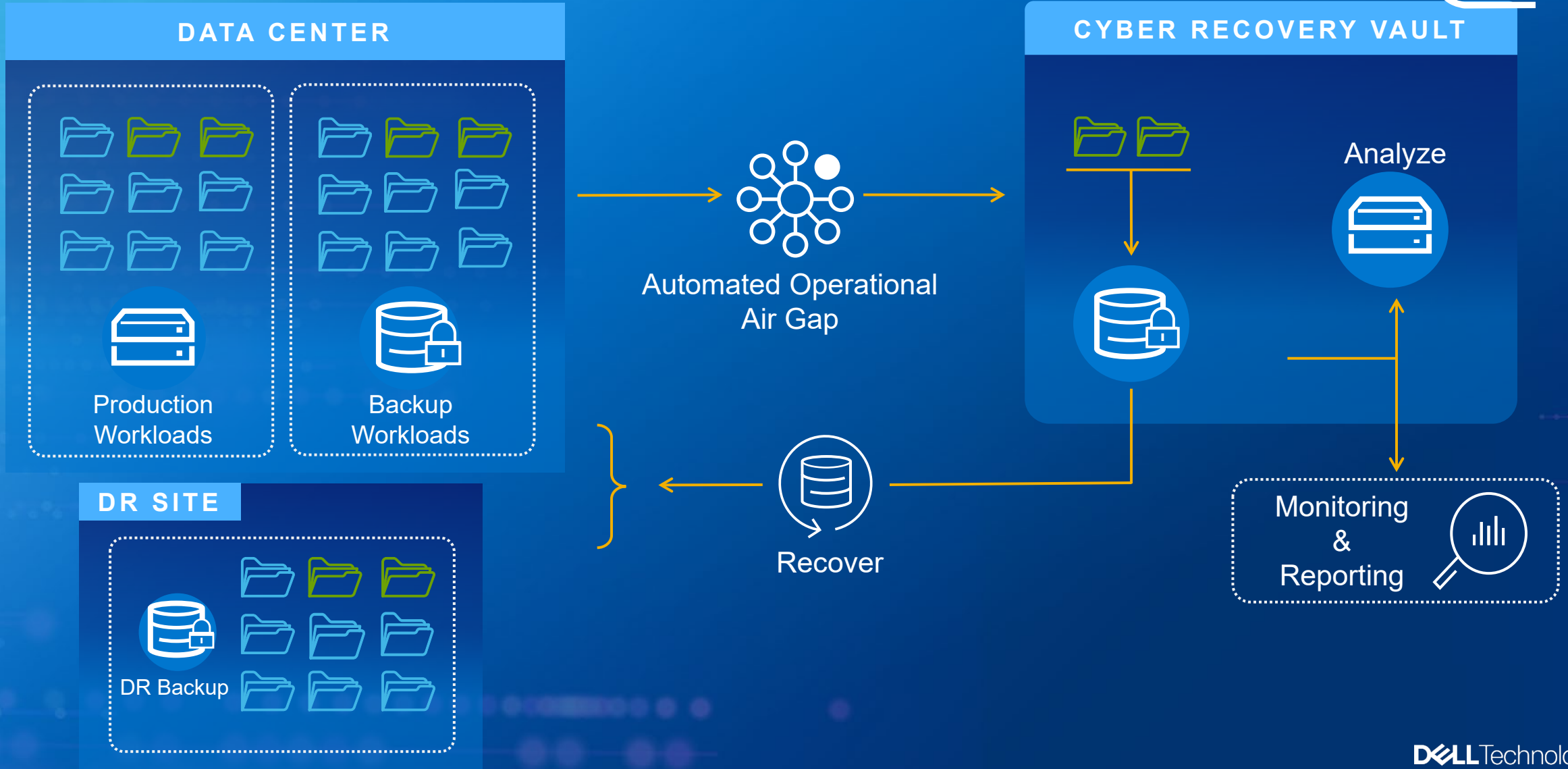
The Importance of Isolation

Improve On Immutability By Denying Access



Cyber Vaulting Capabilities

Ensuring Recovery After A Cyber Disruption



Cyber-attack recovery

Requiring data copies that are hardened, locked, and kept in isolation.

The design should strive to achieve a state where these copies could not be impacted by anything, including scenarios wherein production volumes or other types of copies they are linked to have been compromised.

NIST 800-209, Section 4.7

Anomaly Alerting or Integrity Validation?

Use Both For Better Outcomes

Anomaly Alerting

- Identifies and alerts on abnormal activities
- Can help determine if threat actors are targeting the backup environment



Integrity Validation

- Validates the integrity of the data to use in recovery operations
- "Last known good copy"

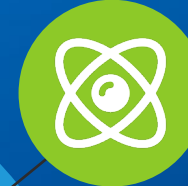
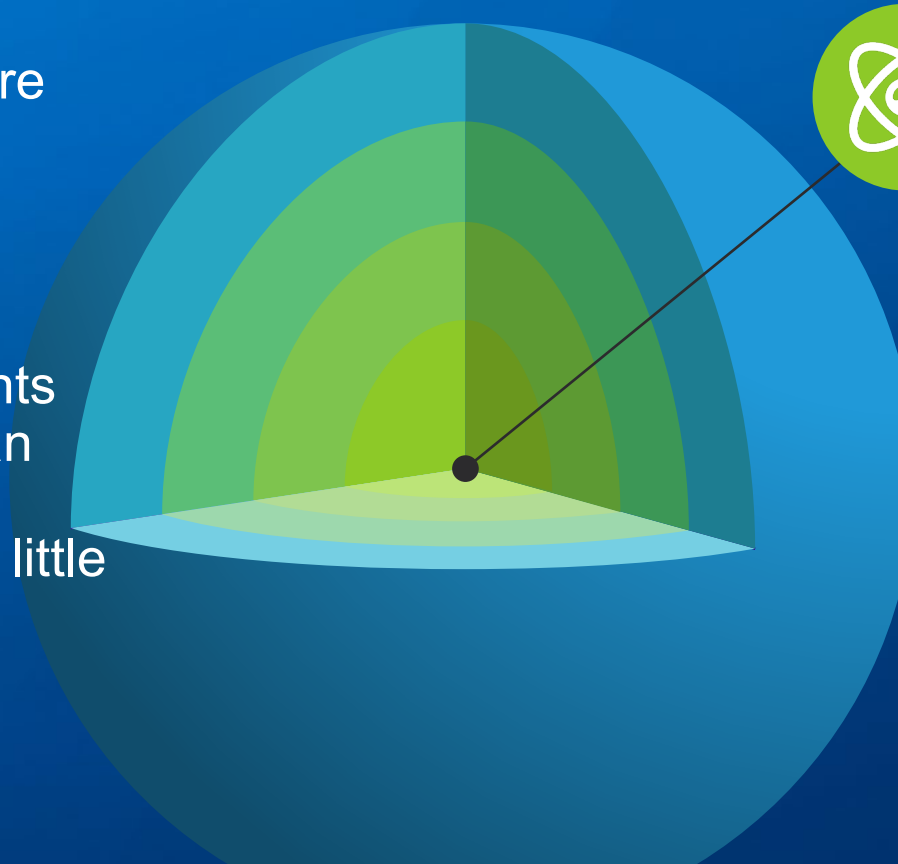


Critical Rebuilds Start at the Core

Deploy A Vault with Basic Recovery Building Blocks



- Critical Rebuild Materials are **"Tier 0"** infrastructure needed before business applications can run.
- Protecting Tier 0 components such as Active Directory can substantially speed and improve recovery with very little complexity or overhead requirements.



Tier 0

Protect the critical data needed to begin the rebuild of your environment first. Some examples are:

- Active Directory / LDAP
- DNS
- Switch / router / IP configurations
- Firewall rules
- Gold copy images / binaries
- Configurations and settings

Why Deploy a Critical Rebuild Materials Vault?

- Fast deployment and low complexity
- Enhanced resilience
- Provide a foundation for future vault contents such as databases and business applications

Continue Your Data Recovery Journey

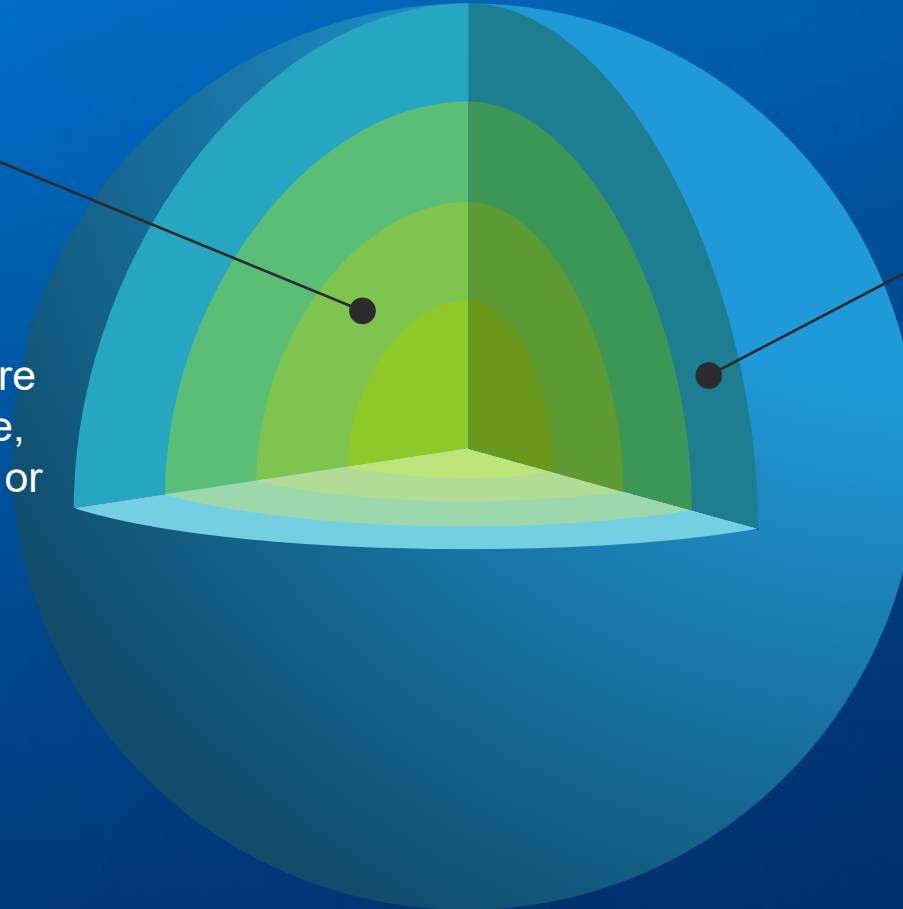


Understand the data in your environment and how it impacts the business



Tier 1 Applications

Progress to the top 2 or 3 applications that are most important to keeping the business running. These are typically aligned to revenue, reputation, systematic risk or safety.



Tier 2 Applications

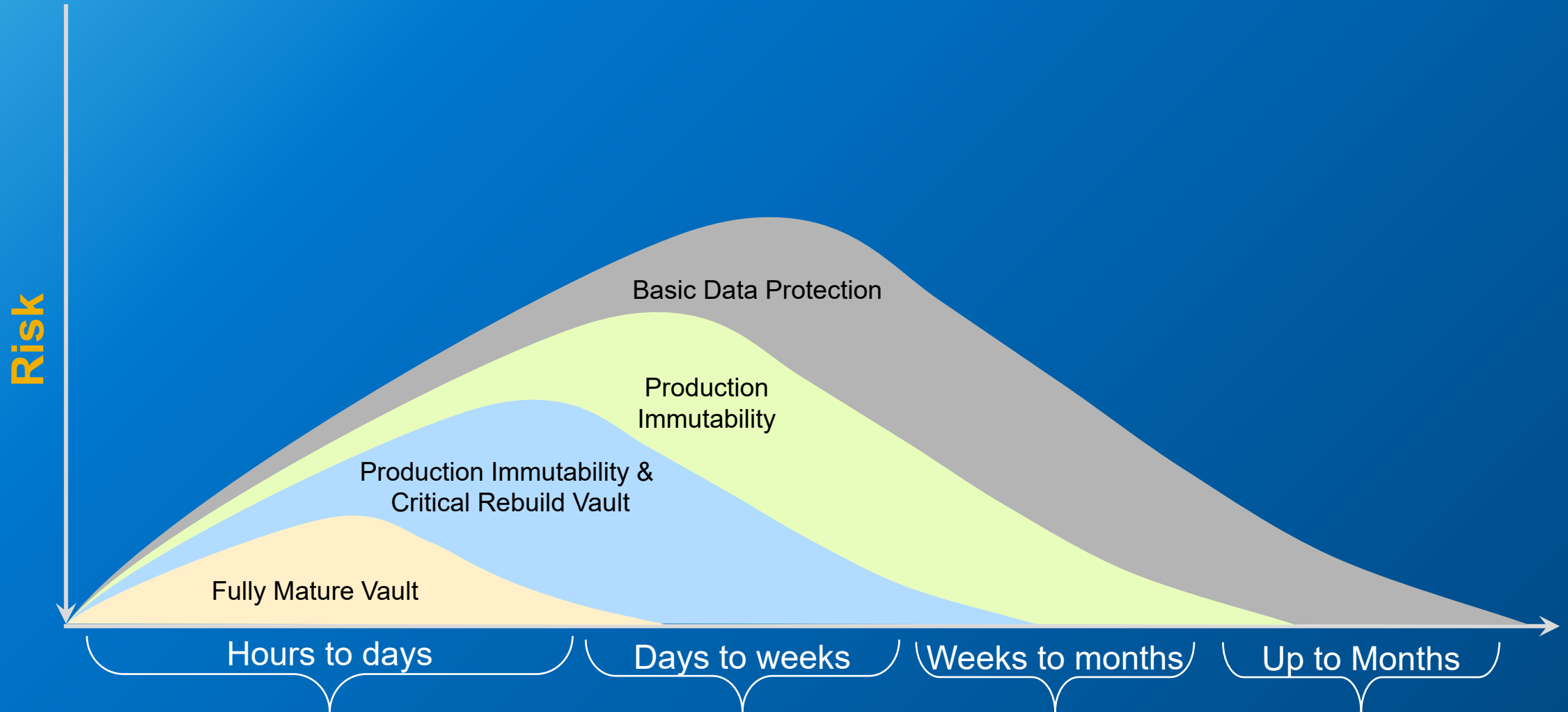
Protect additional applications and data that are important to the business. This will enable more of the business to be quickly recovered. Grow, as needed, over time.

Recovery Maturity

Consider advanced capabilities such as clean rooms and landing zones to speed and further enhance the recovery process.

Stronger Resilience. Better Outcomes.

Reduce Risk, Speed Recovery, and Lower Costs



Full Time to Recover



COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023



Please take a moment to rate this session.

Your feedback is important to us.