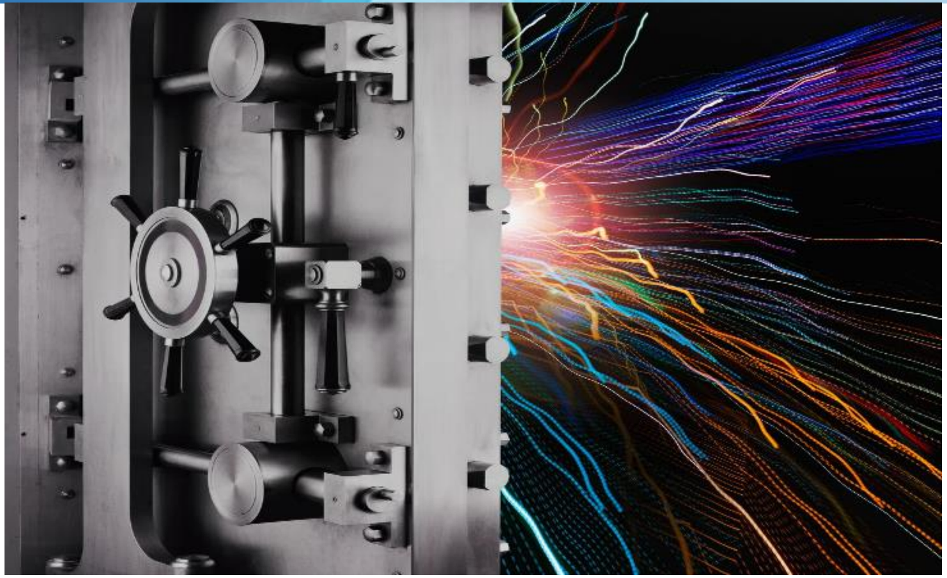
Washington Systems Center - Storage

Accelerate with IBM Storage:

IBM Storage Cyber-Resiliency Solutions
Prepare for WHEN, not IF



Bill Danz
Tape Solutions SME
Washington Systems Center
wddanz@us.ibm.com

Brian Sherman
Distinguished Engineer
Washington Systems Center
bsherman@ca.ibm.com

Dan Thompson
IBM Spectrum Storage Technical Specialist
Washington Systems Center
danthomp@us.ibm.com

Accelerate with IBM Storage Webinars

The Free IBM Storage Technical Webinar Series Continues in 2019...

Washington Systems Center – Storage experts cover a variety of technical topics.

Audience: Clients who have or are considering acquiring IBM Storage solutions. Business Partners and IBMers are also welcome.

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners and IBMers are welcome to send an email request to accelerate-join@hursley.ibm.com.

Located in the Accelerate with IBM Storage Blog:
https://www.ibm.com/developerworks/mydeveloperworks/blogs/accelerate/?lang=en

Also, check out the WSC YouTube Channel here:
https://www.youtube.com/channel/UCNuks0go01_ZrVVF1jgOD6Q

2019 Upcoming Webinars:

August 1 - A Technical Overview and Introductory Demonstration of IBM Spectrum Discover 2.0.1
Register Here: https://ibm.webex.com/ibm/onstage/g.php?MTID=e4de9149ea0838cb7a1383c0c966dd7bb

August 6 – IBM Storage SAN b-type Extension: Native IP vs FCIP
Register Here: https://ibm.webex.com/ibm/onstage/g.php?MTID=eba8b985837a2454480877deb0224114f

August 22 - LinuxONE Servers and IBM Storage Synergies
Register Here: https://ibm.webex.com/ibm/onstage/g.php?MTID=e246d7bbd6b0af257384b0e93c9032eec

Your data can be anywhere

Private cloud

Public cloud

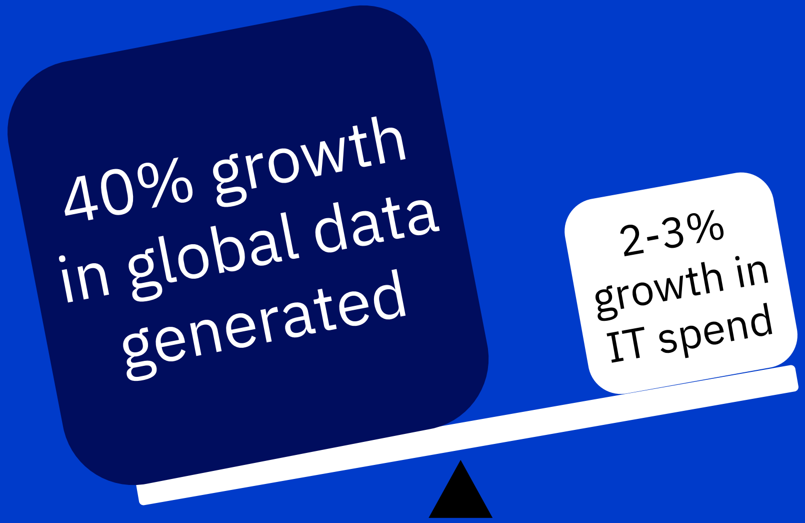
Hybrid cloud

Multicloud

Massive data

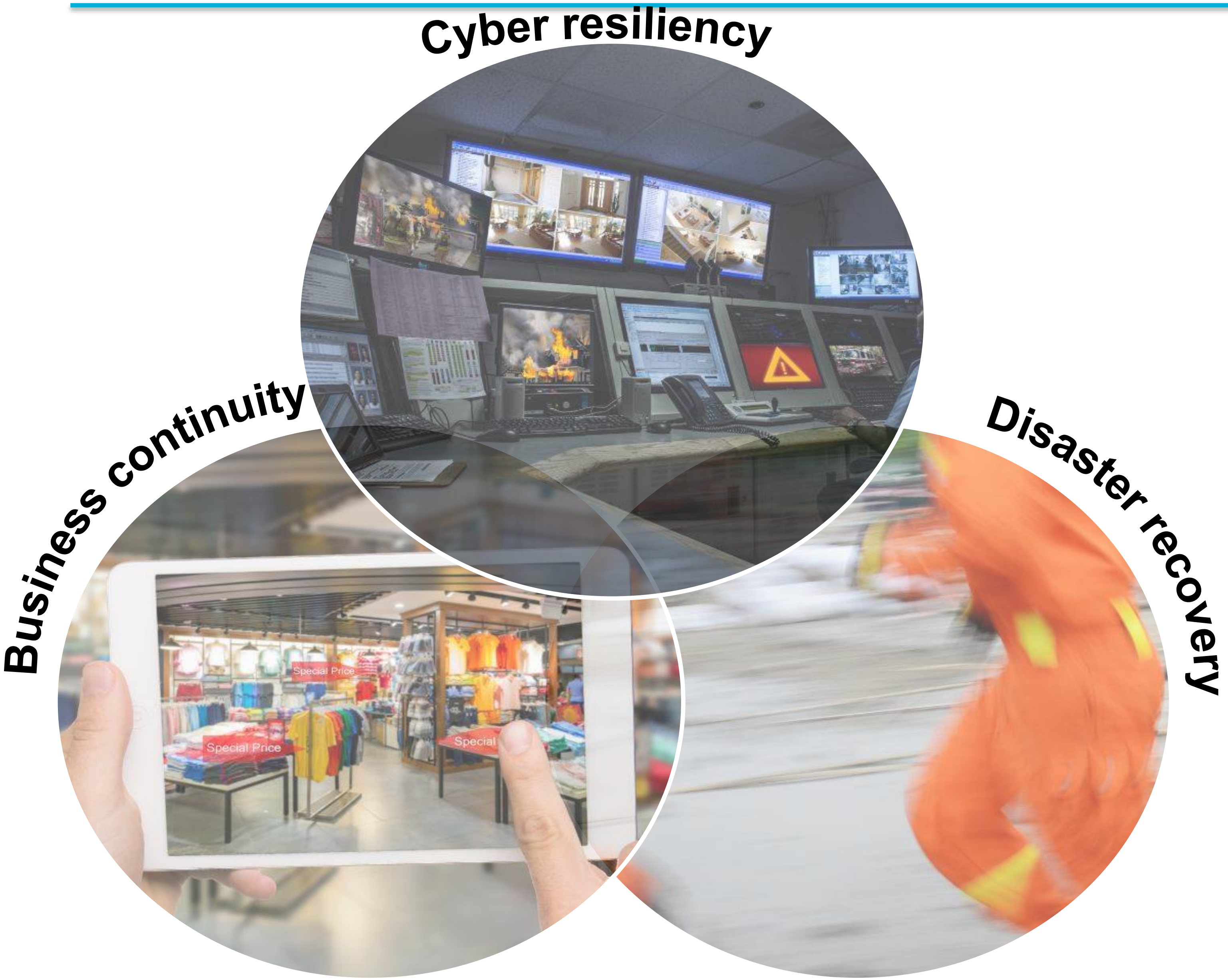
Massive insight

Massive value


40% growth in global data generated

2-3% growth in IT spend

Source: Gartner & McKinsey Global Institute



Current infrastructures focus on BC / DR

- Backups
- Snapshots
- Replication

Add a focus on Cyber Resiliency

- Isolation
- Immutability
- Granularity

Cyber Resiliency

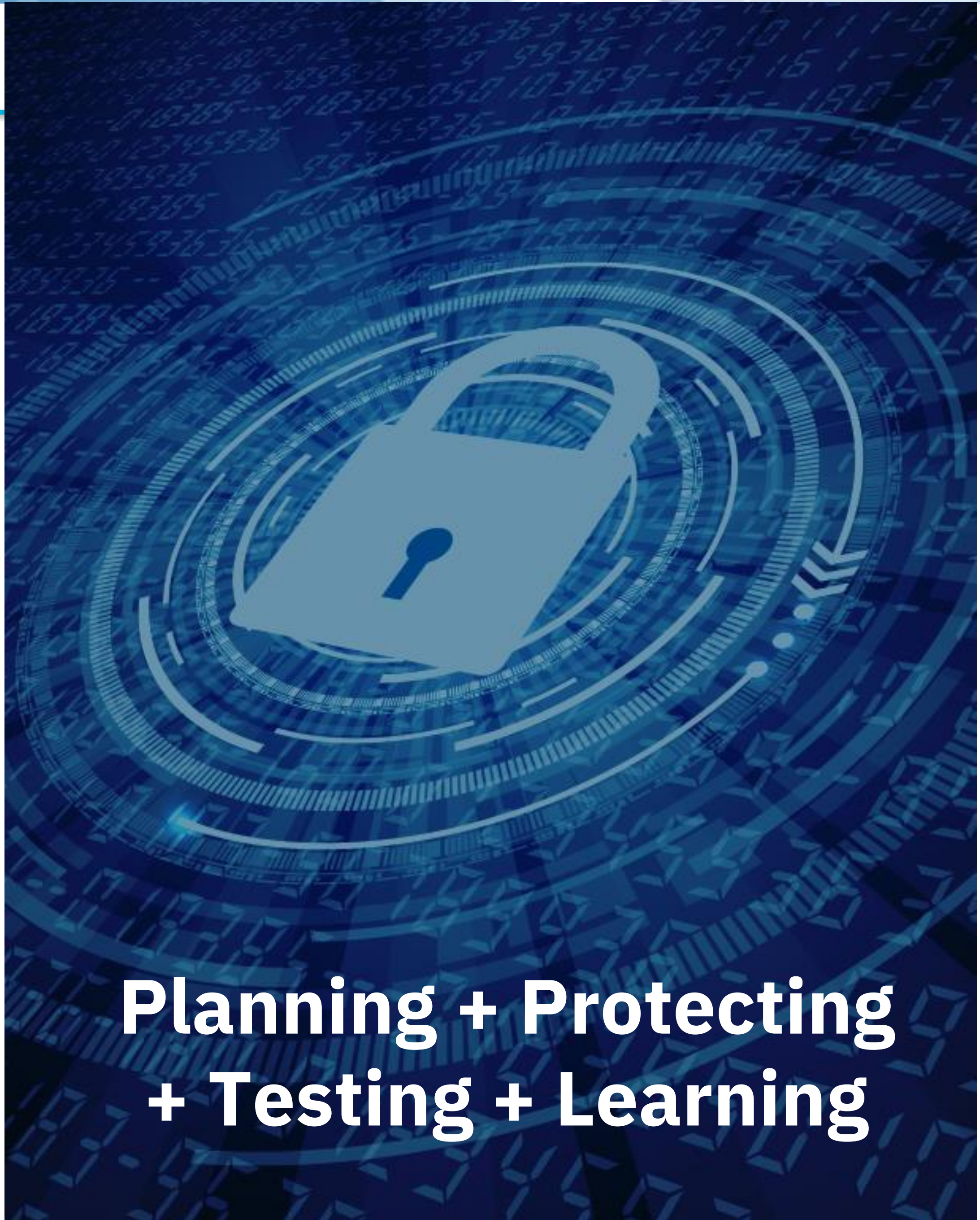
Cyber resiliency is the ability of an organization to continue to function with the least amount of disruption in the face of cyber attacks.

Cyber Security

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects organizations from the deliberate exploitation of its assets.

Business Continuity

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for Business continuity address natural catastrophe, accidents and deliberate physical attacks; but **now, they must also support resumption of operations following cyber attack disruptions.**



Planning + Protecting + Testing + Learning

Attacks are becoming more costly and more likely

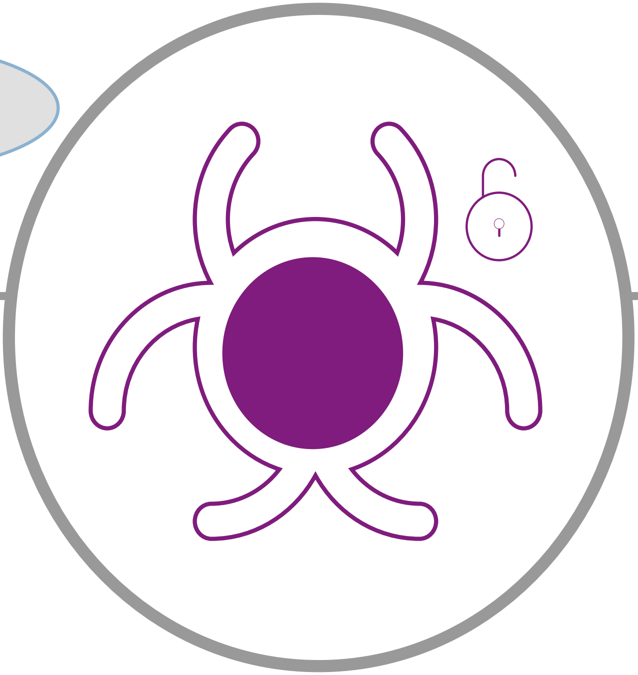
$3.92 million

Average total cost of a data breach in 2019

$200k/hr
Downtime

$8 billion

Estimated global cost of WannaCry attack



$310+ million

Cost impact for one company impacted by NotPetya

1 in 4

Odds of experiencing a data breach over next two years

206 days

Average amount of time hackers spend inside IT environments before discovery

#3
Likely

#6
Impact

* World Economic Forum 2018 Global Risks

Source: Ponemon, 2019 Cost of Data Breach Study - https://w3.ibm.com/w3publisher/ibm-security-internal-community/cost-of-a-data-breach
CBS News WannaCry ransomware attack losses could reach $4 billion - https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Verizon 2019 Data Breaches Report - Summary

Analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches

Who are the victims?

- 16% were breaches of Public sector entities
- 15% were breaches involving Healthcare organizations
- 10% were breaches of the Financial industry

What tactics are utilized?

- 52% of breaches featured Hacking
- 33% included Social attacks
- 28% involved Malware

Who's behind the breaches?

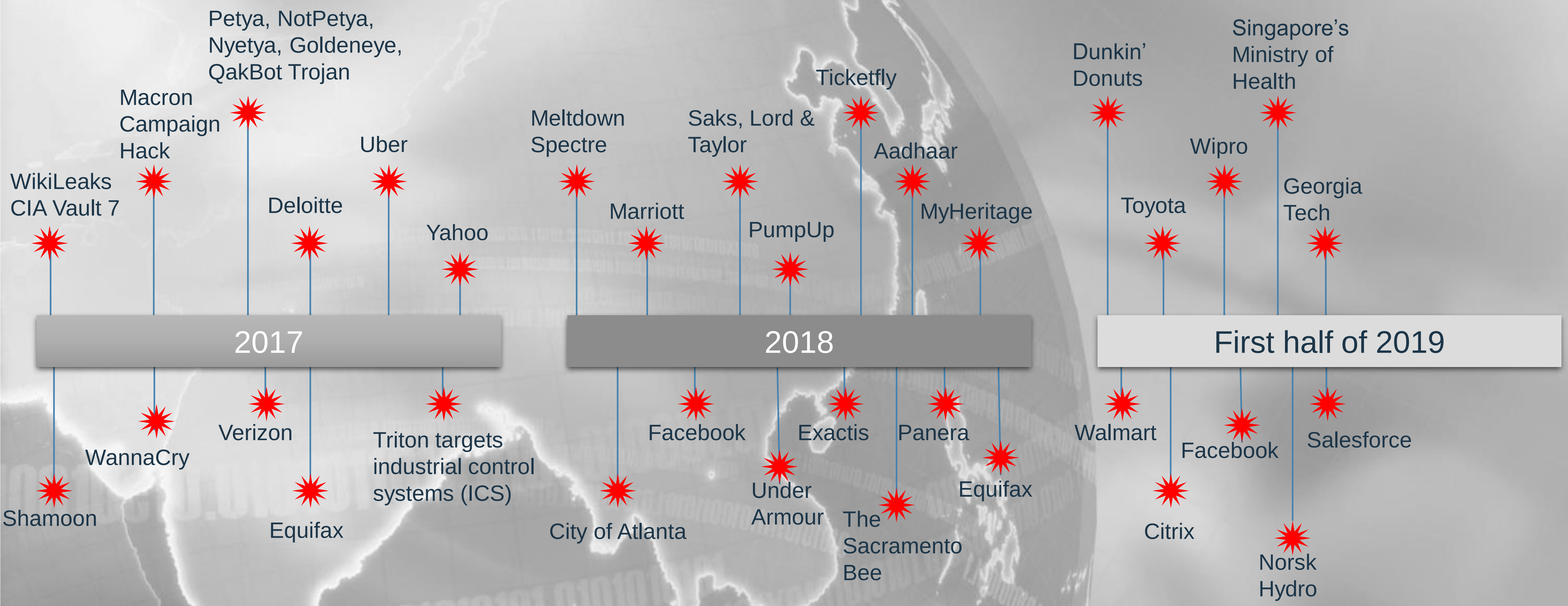
- 69% perpetrated by outsiders
- 34% involved Internal actors

What are other commonalities?

- 71% of breaches were financially motivated
- 25% of breaches were motivated by the gain of strategic advantage (espionage)
- 29% of breaches involved use of stolen credentials

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Cyberattacks happen weekly



2017

WikiLeaks CIA Vault 7

Shamoon

Macron Campaign Hack

WannaCry

Petya, NotPetya, Nyetya, Goldeneye, QakBot Trojan

Verizon

Deloitte

Equifax

Uber

Yahoo

Triton targets industrial control systems (ICS)

2018

Meltdown Spectre

City of Atlanta

Marriott

Facebook

Saks, Lord & Taylor

Under Armour

PumpUp

Exactis

Ticketfly

The Sacramento Bee

Aadhaar

Panera

MyHeritage

Equifax

First half of 2019

Dunkin' Donuts

Walmart

Toyota

Citrix

Wipro

Facebook

Singapore's Ministry of Health

Norsk Hydro

Georgia Tech

Salesforce

2017	2018	First half of 2019
826 million data records	2.3 billion data records	6.7 billion data records

Reported lost or stolen

Pain points evolve as cyber attacks increase and change

- **Need a more precise, immediate response to a cyber event**
- **Eliminate extended business interruptions from more frequent attacks**
- **Retain clean IT and critical business process components to quickly resume company operations**
- **Demonstrable evidence of capability for audit and compliance**

FFIEC
Federal Financial Institutions Examination Council

NAIC
National Association of Insurance Commissioners

EUROPEAN CENTRAL BANK
EUROSYSTEM

FCA
FINANCIAL
CONDUCT
AUTHORITY

Defining a Cyber Resiliency Recovery Service Strategy

- Do not just focus on Ransomware. Other Malware, internal threats and regulations need to be taken into account
- You may have air-gap, encryption at-rest or immutability/WORM requirements. This may apply to all or just a sub-set of data and location of storage and recovery may be different
- You may have much more aggressive requirements for recovering large amounts of corrupted data, from an incorruptible source
- You may have multiple requirements that appear similar, but looking past the superficial similarities shows important details
- We have to look beyond the traditional Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Separate security domains for primary, Disaster Recovery and Cyber Recovery locations

IBM Cyber Resiliency for Storage

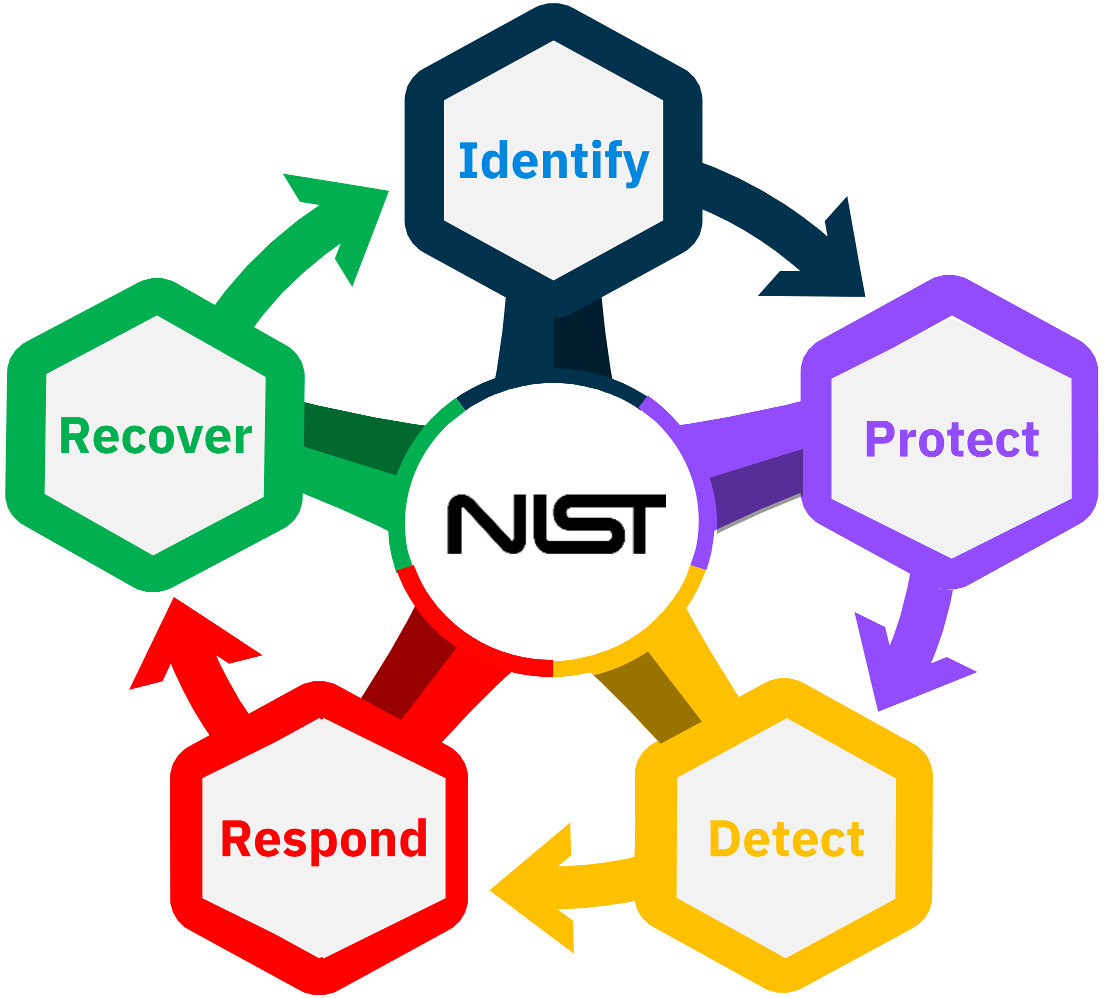
Vision

Deliver a comprehensive storage portfolio that is designed to help organizations reduce the risk of business disruption and financial losses due to Cyber Attack events

Strategy

- Deliver a consolidated IBM Storage Cyber Resiliency portfolio aligned with client needs
- Collaborate across Brands and disciplines (e.g. Power, IBM Z, aaS, and IBM Security) to meet client requirements
- ✓ Deliver clear deployment guidelines and enablement material in order to highlight existing Cyber Resiliency storage functions
- Expand current IBM Storage Cyber Resiliency portfolio to address essential gaps in accordance with Cyber Resiliency NIST framework

NIST Cyber Resiliency Framework



Framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks:

Identify:

Defining a organizational understanding to build or improve **cyber resiliency plan** – critical assets & strategy

Protect:

Implementing Safeguards to ensure delivery of critical services – protecting against vulnerabilities before they are exploited

Detect:

Detecting occurrence of cyber security events – timely, continuous monitoring, detection processes

Respond:

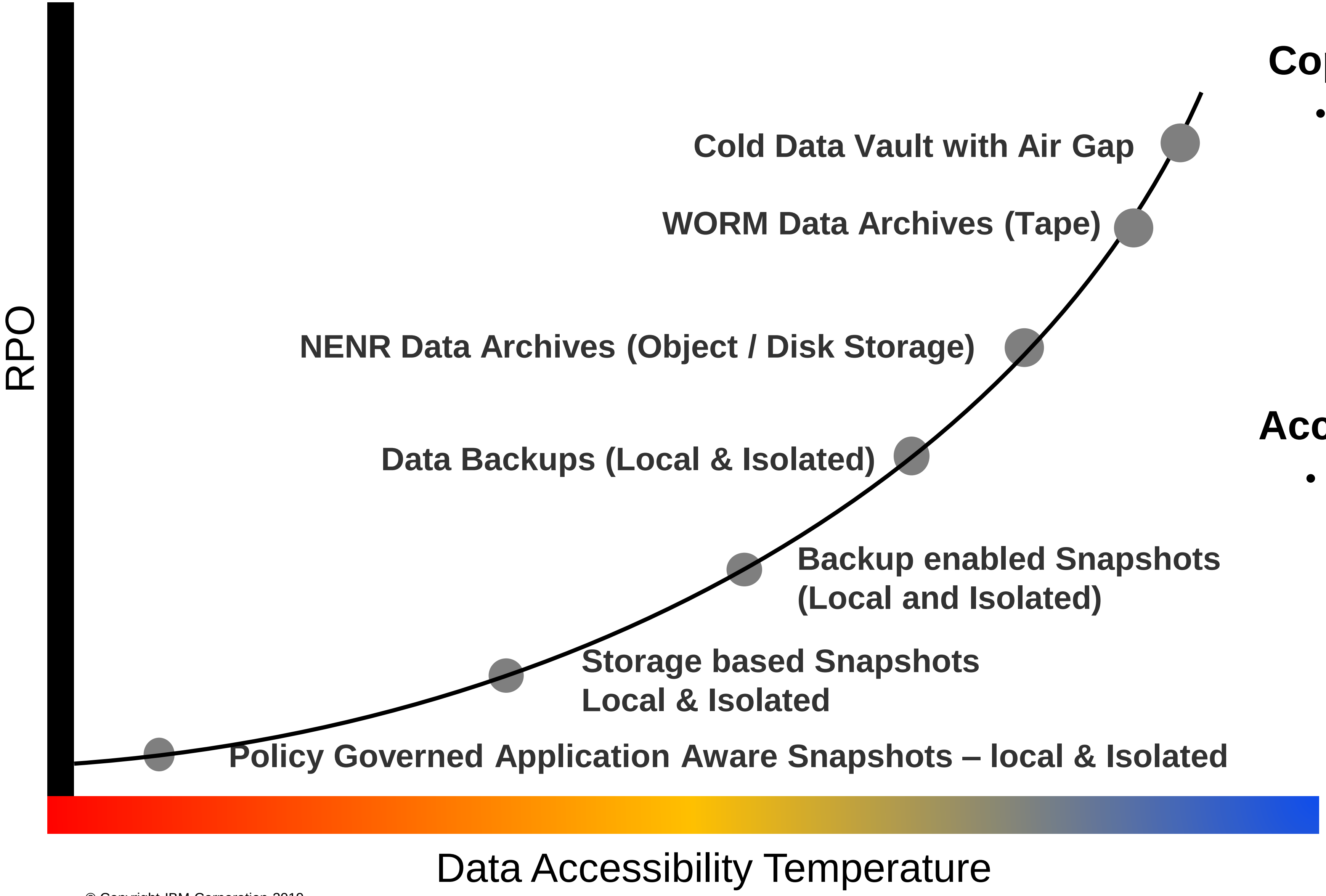
Taking action regarding a detected event – analysis, **contain**, mitigation, & communication

Recover:

Restore capabilities and services - recovery, improvements, communications

IBM Storage Solutions for Cyber Resiliency

Storage Services and Ransomware


RPO
Cold Data Vault with Air Gap
WORM Data Archives (Tape)
NENR Data Archives (Object / Disk Storage)
Data Backups (Local & Isolated)
Backup enabled Snapshots (Local and Isolated)
Storage based Snapshots Local & Isolated
Policy Governed Application Aware Snapshots – local & Isolated
Data Accessibility Temperature

Copy Separation:

- Create a structure of data separation across multiple layers and services including;
  - Copy Services
  - Backup Services

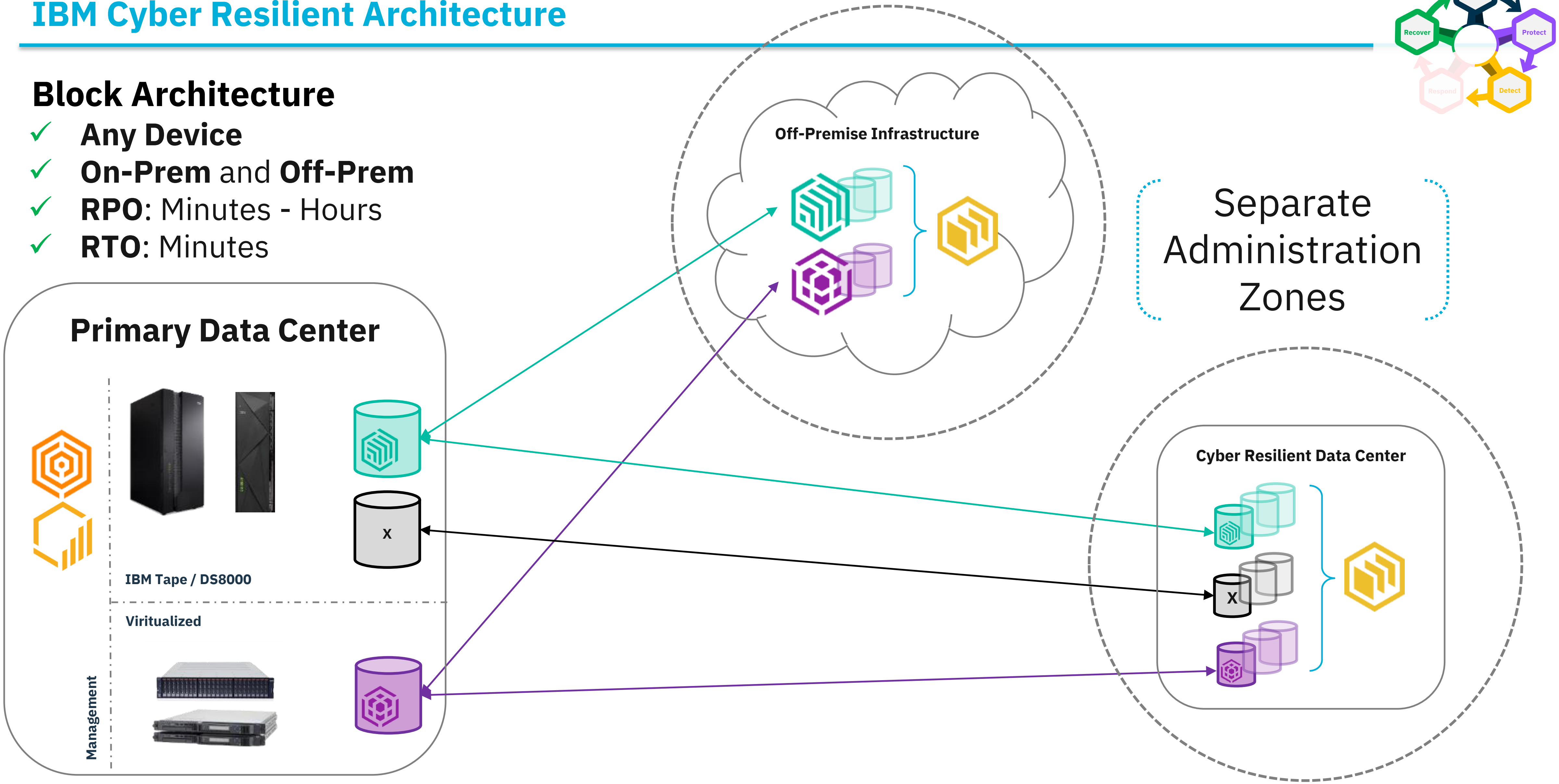
Access Isolation:

- Create a structure of data isolation multiple layers and services including;
  - Air Gap
  - Non-erasable / Non-rewritable Storage
  - Cold Storage / Object Storage
  - Data Vaults
  - Isolated Infrastructure

IBM Cyber Resilient Architecture

Block Architecture

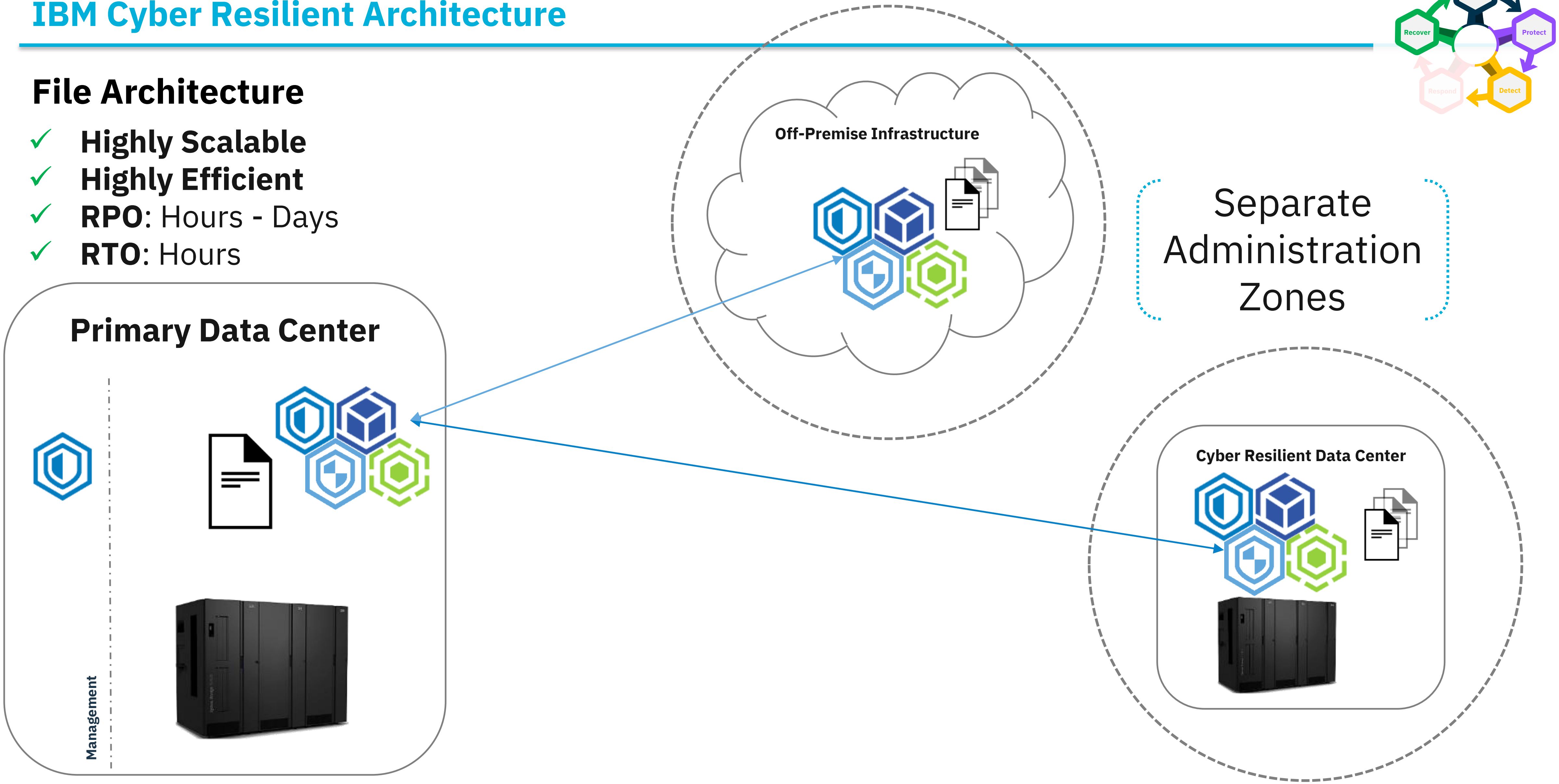
- ✓ **Any Device**
- ✓ **On-Prem** and **Off-Prem**
- ✓ **RPO**: Minutes - Hours
- ✓ **RTO**: Minutes


Off-Premise Infrastructure
Separate Administration Zones
Primary Data Center
IBM Tape / DS8000
X
Viritualized
Management
Cyber Resilient Data Center
X

IBM Cyber Resilient Architecture

File Architecture

- ✓ **Highly Scalable**
- ✓ **Highly Efficient**
- ✓ **RPO**: Hours - Days
- ✓ **RTO**: Hours



Separate Administration Zones

Identify

NIST – Identify - Know your Systems and Data

- **Develop organizational understanding to manage cybersecurity risk**
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy

- **Key IBM Offerings:**
  - Identify where data is located – Storage Insights / Spectrum Control / Spectrum Discover
  - Understand “normal” performance requirements – Storage Insights / Spectrum Control
  - Understand daily data changes – Spectrum Protect
  - Find changes quickly – Spectrum Discover

IBM
Storage
Insights

IBM
Spectrum
Discover

IBM
Spectrum
Control

IBM
Spectrum
Protect

Protect

NIST – Protect - Protect your Systems and Data

- **Develop and Implement safeguards to ensure delivery of critical services**
  - Identity Management
  - Access Control
  - Awareness / Training
  - Data Security
  - Information Protection Process
  - Maintenance
  - Proactive Technology

- **Key IBM Offerings:**
  - Store data on separate infrastructure – Tape / Archive
  - Replicate to a remote location – DS8000 / Spectrum Virtualize/ Spectrum Scale / Cloud Object Storage
  - Limit administrative access – DS8000 / Spectrum Protect Plus / Spectrum CDM
  - Exploit data copies in your DR environment – DS8000 / Spectrum Protect Plus / Spectrum CDM

IBM Spectrum Protect

IBM Spectrum CDM

IBM Spectrum Archive

IBM Spectrum Scale

IBM Spectrum Virtualize

IBM Cloud Object Storage

IBM Spectrum Protect Plus

IBM Tape

NIST – Detect - Leverage Tools to Identify Breaches

Detect

- **Develop and Implement activities to identify a cybersecurity threat**
  - Anomalies & Events
  - Continuous Security Monitoring
  - Detection Process

- **Key IBM Offerings:**
  - Monitor Performance – Storage Insights / Spectrum Control
  - Understand data changes – Storage Insights / Spectrum Protect / Spectrum Protect Plus / Spectrum Discover
  - Validate protected data– Spectrum Protect / Spectrum Protect Plus

IBM
Storage
Insights

IBM
Spectrum
Discover

IBM
Spectrum
Control

IBM
Spectrum
Protect Plus

IBM
Spectrum
Protect

Respond

NIST – Respond - Disconnect from the threat

- **Develop and Implement activities to take action on a cybersecurity incident**
  - Response Planning
  - Communications Planning
  - Analysis
  - Mitigation
  - Improvements

- **Key IBM Offerings help:**
  - Scope Analysis – Spectrum Protect, Spectrum Protect Plus / Spectrum Discover / Storage Insights / Spectrum Control

IBM
Storage Insights

IBM
Spectrum Discover

IBM
Spectrum Control

IBM
Spectrum Protect

IBM
Spectrum Protect Plus

Recover

NIST – Recover - Restore capabilities and services

- **Develop and Implement activities to maintain plans for resilience and restore**
  - Recovery Planning
  - Improvements
  - Communications

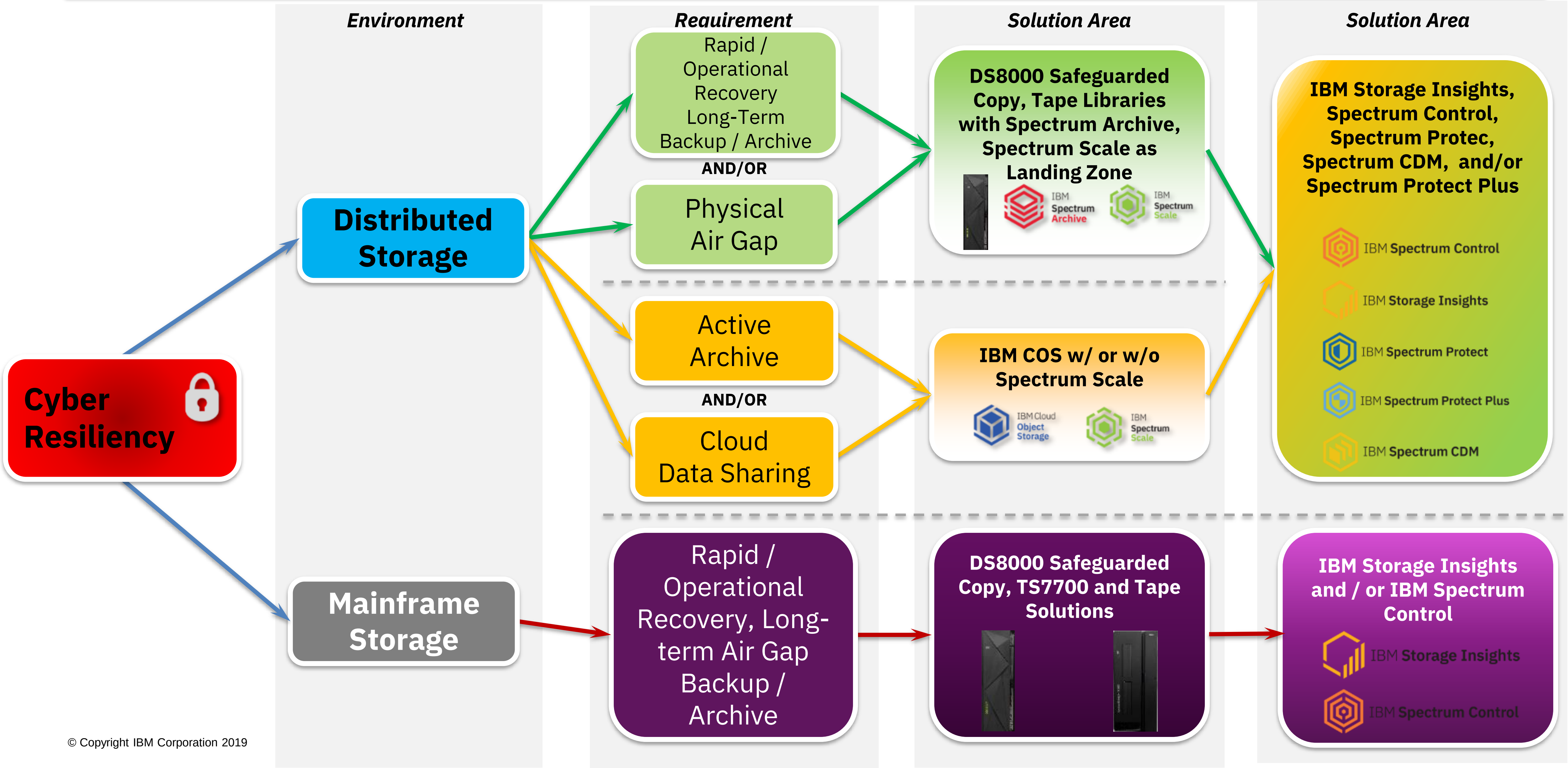
- **Key IBM Offerings:**
  - Full environment recovery – DS8000 / Spectrum Virtualize / Spectrum Protect
  - Instant application / data recovery – DS8000 / Spectrum Protect Plus / Spectrum CDM
  - Utilize data copies – DS8000 / Spectrum Protect Plus / Spectrum CDM
  - DR Automation – Copy Services Manager / GDPS / Spectrum CDM

IBM **Spectrum Virtualize**

IBM
Spectrum
Protect

IBM
Spectrum
Protect Plus

IBM Storage Cyber Resiliency Solutions



Environment

Requirement

Solution Area

Solution Area

Cyber Resiliency

Distributed Storage

Rapid / Operational Recovery Long-Term Backup / Archive

AND/OR

Physical Air Gap

DS8000 Safeguarded Copy, Tape Libraries with Spectrum Archive, Spectrum Scale as Landing Zone

IBM Spectrum Archive

IBM Spectrum Scale

Active Archive

AND/OR

Cloud Data Sharing

IBM COS w/ or w/o Spectrum Scale

IBM Cloud Object Storage

IBM Spectrum Scale

IBM Storage Insights, Spectrum Control, Spectrum Protec, Spectrum CDM, and/or Spectrum Protect Plus

IBM Spectrum Control

IBM Storage Insights

IBM Spectrum Protect

IBM Spectrum Protect Plus

IBM Spectrum CDM

Mainframe Storage

Rapid / Operational Recovery, Long-term Air Gap Backup / Archive

DS8000 Safeguarded Copy, TS7700 and Tape Solutions

IBM Storage Insights and / or IBM Spectrum Control

IBM Storage Insights

IBM Spectrum Control

Rapid Recovery & Long term Air Gap archive

DS8880 Safeguarded Copy

IBM's unique, host independent, proven new data protection solution that allows you to recover faster than traditional methods

☑ **IBM z Robustness**

☑ **Highest Possible Resiliency**

☑ **Always Offline By Design**

Tape WORM

Air Gap copies that cannot be modified or deleted

IBM Tape / Virtualization

Delivering long term air gap tape archival for your most mission-critical data

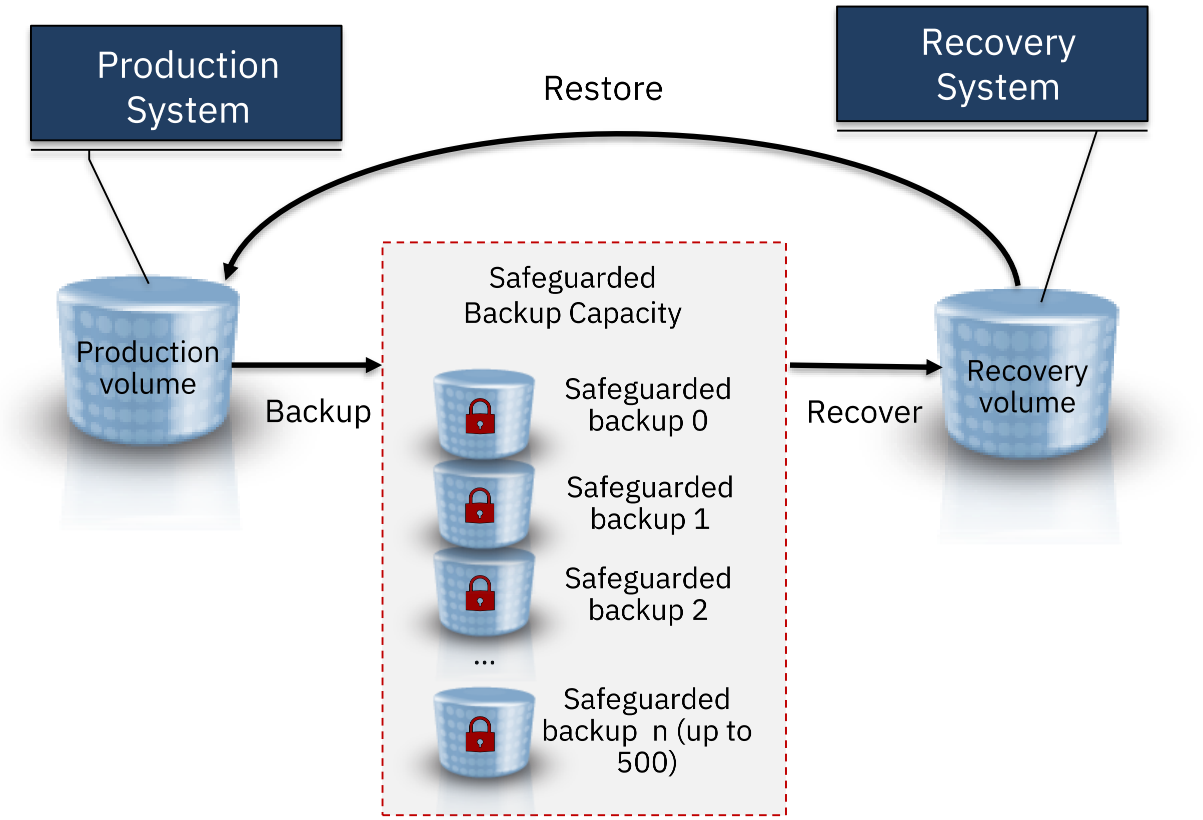
DS8880 Safeguarded Copy for logical corruption protection

Safeguarded Copy provides functionality to create up to 500 recovery points for a production volume

- These recovery points are called Safeguarded Backups
- The Safeguarded Backups are stored in a storage space that is called Safeguarded Backup Capacity (SGBC)
- The Safeguarded Backups are hidden and non-addressable by a host
- The data can only be used after a Safeguarded Backup is recovered to a separate recovery volume
- Recovery volumes can be accessed using a recovery system and used to restore production data

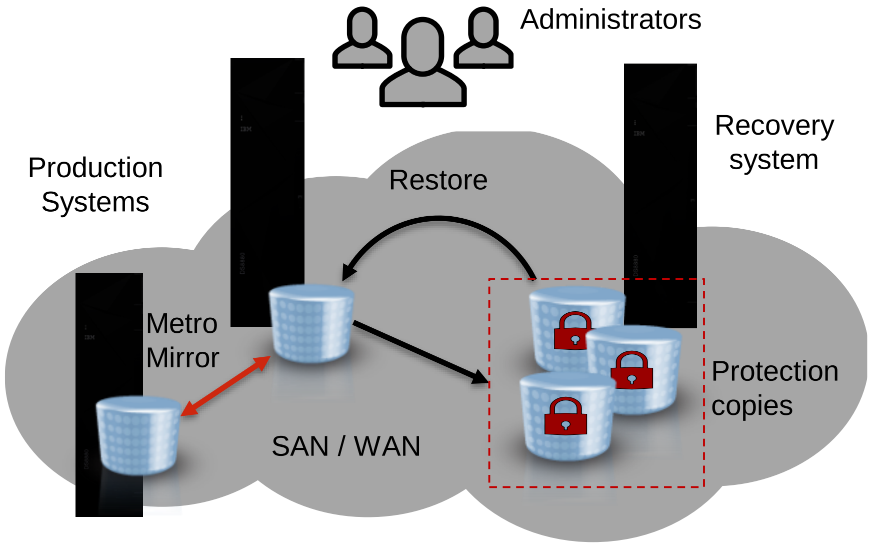
Automation provided via CSM or GDPS

IBM DS8880 Safeguarded Copy prevents sensitive point in time copies of data from being modified or deleted due to user errors, malicious destruction or ransomware attacks



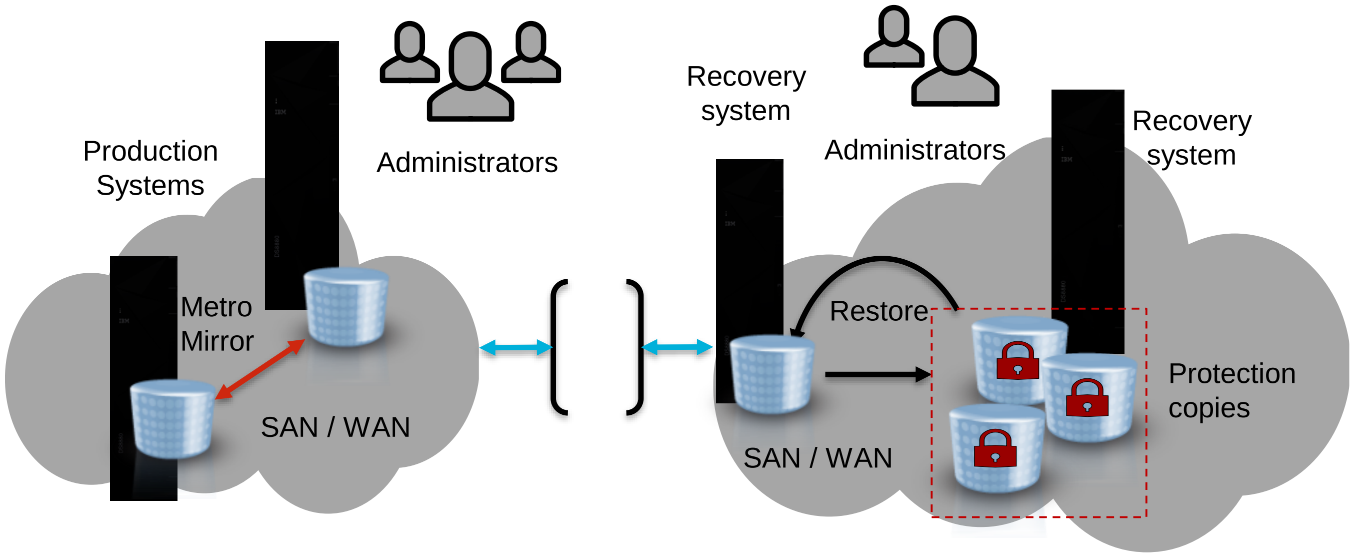
Virtual and physical isolation of protection copies

Virtual isolation



- The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- The storage systems are typically in the same SAN or IP network as the production environment

Physical isolation



- Additional storage systems are used for the protection copies
- The storage systems are typically not on the same SAN or IP network as the production environment
- The storage systems have restricted access and even different administrators to provide separation of duties

Automation: Critical for successful rapid recovery and continuity

The benefits of automation:

- Allows business continuity processes to be built on a reliable, consistent recovery time
- Recovery times can remain consistent as the system scales to provide a flexible solution designed to meet changing business needs
- Reduces infrastructure management cost and staffing skills
- Reduces or eliminates human error during the recovery process at time of disaster
- Facilitates regular testing to help ensure repeatable, reliable, scalable business continuity
- Helps maintain recovery readiness by managing and monitoring the server, data replication, workload and the network along with the notification of events that occur within the environment

Automate - Automate - Automate

DS8880 Business Continuity and Safeguarded Copy made easy with Copy Services Manager

IBM Copy Services Manager (CSM) ensures business continuity with Multi-site replication and disaster recovery management for IBM Storage Systems and Safeguarded Copy support for DS8880

Protect

Keeps your production environment always on, with 2, 3 & 4 site remote replication for higher performance and **maximum availability**

Dual Authentication Control for additional security with Safeguarded Copy

Simplify

Provides a single point of control to automate and simplify the DS8880 recovery process in **just one step**

Monitor

Provides a measurement of the amount of replication and the amount of time that is required to **complete the replication operations**

IBM Copy Services Manager protects your most valuable data and ensures 24x7 business operations

GDPS Support for Logical Corruption Protection (LCP)

GDPS 4.1 in March 2018 introduced a new Logical Corruption Protection feature enabled via IFAPRDxx

- Enables up to 10 LCP FlashCopies plus a single Recovery Copy
  - No UCB required for these copies in the system taking the Point-in-Time copy
  - UCB required in recovery systems to address the Recovery Copy

- Users must decide between Logical or Physical Isolation topology for their LCP copies
  - First Logical (virtual) Isolation topology delivered for GDPS Metro
  - First Physical Isolation topology delivered for GDPS Metro Global – GM 4-site solution
    - PROCEDUREs provided to manage the actions required to create PiT copy

- Physical Isolation topologies defined within the GDPS GEOGROUP definition

GDPS Metro R4.2 – LCP RESTORE and LCP RECOVER

New Logical Corruption Protection script statements available in GDPS Metro

- Will be extended to further solutions, including SGC via SPE’s

Requires the LCP production registration feature to be enabled:

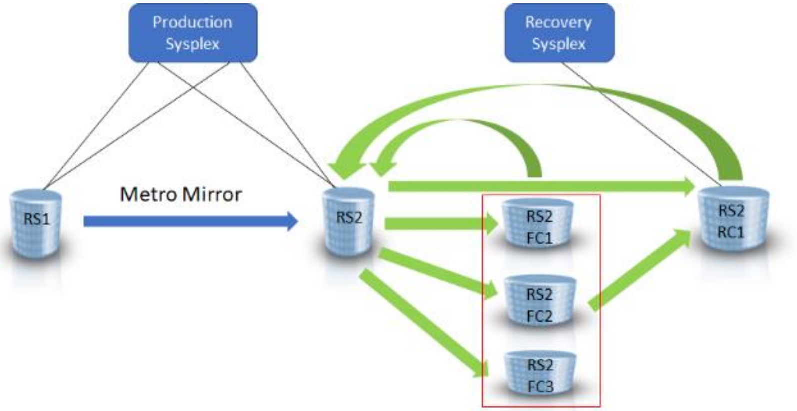
- FeatureName(‘LCP_MGR’)

LCP=RESTORE

- Restore a captured FlashCopy volume set to an RS(n) volume set
- Supports up to 10 FlashCopy volume sets
  - LCP ‘RESTORE FC(n) RS(n)’
  - LCP ‘RESTORE RC(1) RS(n)’

LCP=RECOVER

- Recover a captured FlashCopy volume set to an RC(n) Recovery volume set
- Supports 1 Recovery volume set
  - LCP ‘RECOVER RS(n) FC(n) RC(1) NOCOPY’
  - LCP ‘RECOVER RS(n) FC(n) RC(1) COPY’
  - LCP ‘RECOVER RS(n) FC(n) RC(1) NOCOPY2COPY’
  - LCP ‘RECOVER RS(n) RC(n) END’



Instant Recovery, Long term Backup/Archive & Physical Air Gap

Tape Library

IBM Spectrum Protect

IBM Spectrum Scale

IBM Spectrum Archive

IBM Cloud Object Storage

IBM Tape Virtualization

Delivering long term air gap tape archival for your most mission-critical data

☑ Reduced TCO

☑ Maximum Security

☑ Always Offline By Design

Spectrum Scale

Provides resilient, high performance, and simultaneous access to shared data

IBM Spectrum Protect

Instant recovery options and alerts

IBM Cloud Object Storage

Immutable Storage for data copies

Protecting Primary data on IBM Virtual Tape

- **Implement Logical WORM on TS7700 and configure Retention Hold for scratch retention to prevent immediate overwrite of data on tape**

- **Evaluate increasing retention of data on ML0 to prevent HSM thrashing which can also increase space requirements for protection copies**

- **Implement Copy Export from TS7700 to remove physical tape volumes from TS7700 control. Can move tapes to a separate logical library while maintaining them in the physical tape library to avoid manual tape handling.**

THE WALL STREET JOURNAL.

Companies Look to an Old Technology to Protect Against New Threats

Companies are once again storing data on tape, just in case

Companies are returning to tape as a medium for storing data as hackers get smarter about penetrating defenses. ILLUSTRATION: KEVIN VAN AELST FOR THE WALL STREET JOURNAL

“Storing data on tape seems impossibly inconvenient in an age of easy-access cloud computing. But that is the big security advantage of this vintage technology, since hackers have no way to get at the information.”

Cyber Resiliency with TS7700 Virtual Tape

- **Proactive Functions**
  - **Copy Export** – Dual physical tape data copies, one can be isolated. True “air gap” solution; no access to exported volumes from z/OS or Web
  - **Physical Tape** – Single physical tape data copy not directly accessible from IBM Z hosts. Partial “air gap” solution; manipulation of DFSMS, tape management system and TS7700 settings required to delete virtual tape volumes
  - **Delete Expired** – Delay (from 1 to 32,767 hours) the actual deletion of data (in disk cache or physical) for any logical volume moved to scratch status. Transparent protection from accidental or malicious volume deletion
  - **Logical Write Once Read Many (LWORM)** – TS7700 enforced preservation of data stored on private logical volumes. Immutability (i.e. no change once created) assured

- **Reactive Function**
  - **FlashCopy with Write Protect** – “Freeze” the contents of production TS7700 systems during an emergency situation (such as with an active cyber intruder). Read activity can continue

Cyber Resiliency with IBM Physical Tape

- **Market Leader for both mainframe and distributed systems**
- **Cost effective long-term backup and archive**
- **Ability to move cartridges from library to storage racks or vaults**
  - Inherent Air Gap
- **WORM / Immutable storage**
- **Encryption capabilities**
- **Works with IBM Spectrum Protect**
  - Efficient Copy Management (of copies)
- **Environmentally Friendly**
- **High Automation**
  - For tapes in the library

How to add air gapped solutions to Cloud Object Storage

IBM Cloud Object Storage

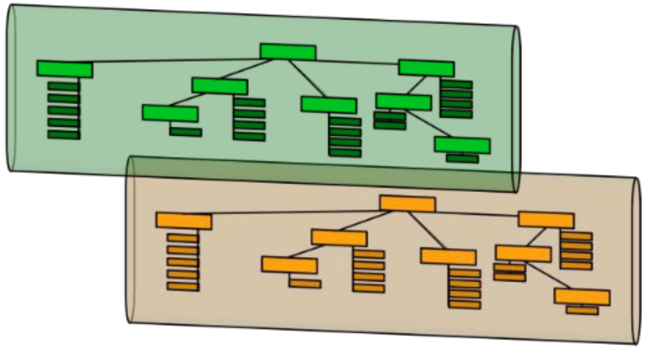
- Flexible, high availability, scalable, dispersed storage for unstructured data
- Hybrid Cloud and Transparent Cloud Tiering solutions
- Create policies for data that guarantee no deletion for a customer defined period
- Active Archive and Long Term backup
- Immutable storage vaults
- Encryption for data at rest and data in motion

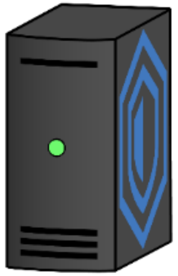
How to add air gapped solutions to a Spectrum Scale storage hierarchy

- **Spectrum Scale's Information Lifecycle Management data tiers allows targeting object storage, tape storage or backup/archive engines as external storage tiers**

- **Each of those options supports multiple copies of data**

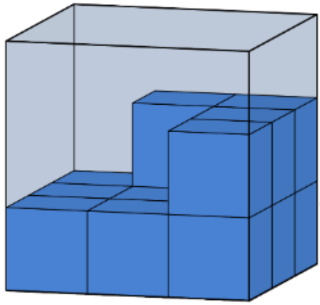
- **Also support protective snapshots**





Backup-Archive Engine Storage Tier

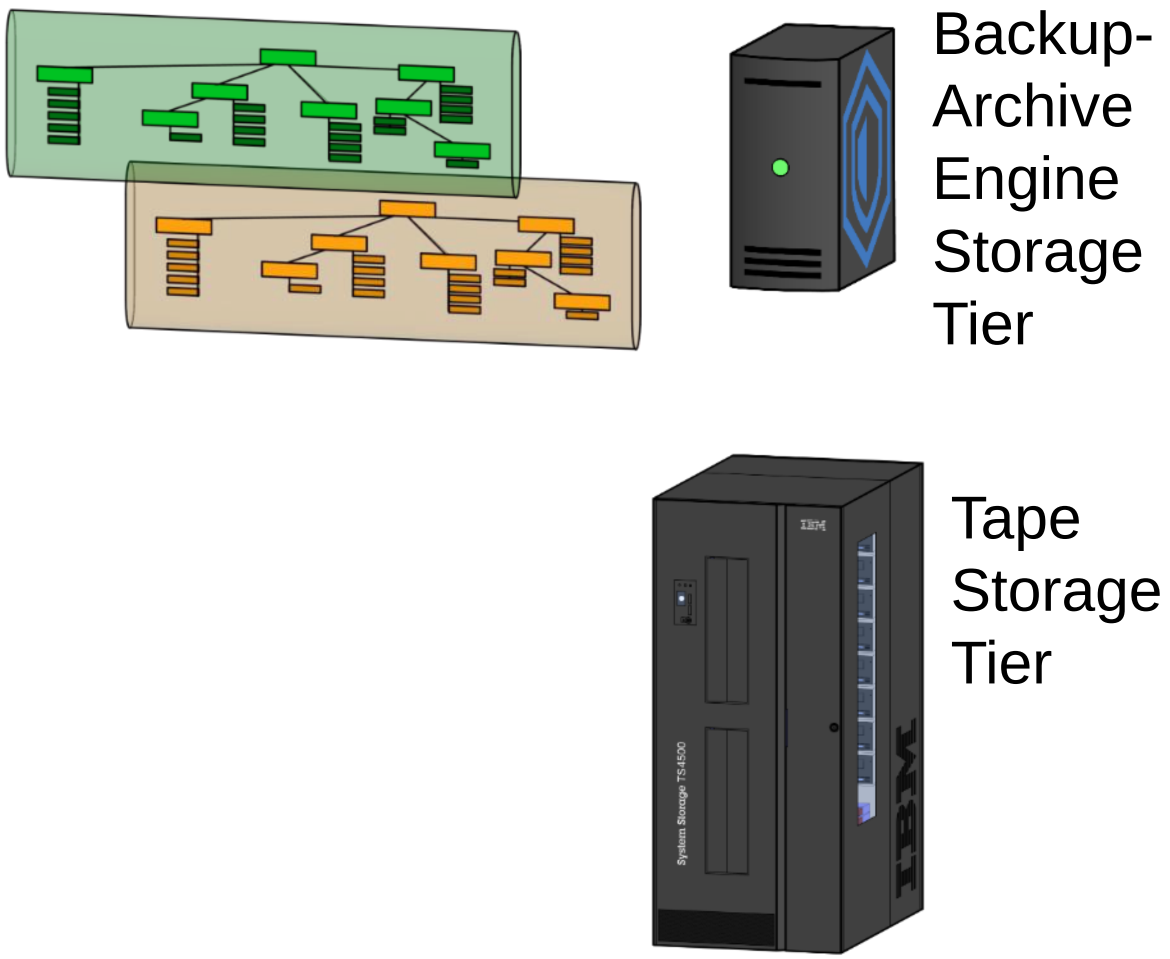
Tape Storage Tier



Object Storage Tier

Using immutable files in a Spectrum Scale and Archive storage hierarchy

- **IBM Spectrum Archive EE version 1.2 has been assessed for compliance**
  - According to German, Swiss and US regulation
  - Report from independent auditor: link
- **Relies on Spectrum Scale immutable fileset (whitepaper)**
  - Spectrum Archive has been assessed for archiving immutable files from Spectrum Scale immutable fileset to WORM tape managed by Spectrum Archive EE



Backup-Archive Engine Storage Tier

Tape Storage Tier

Backup Solution Design with Immutability, Air Gap and Cyber Vaulting

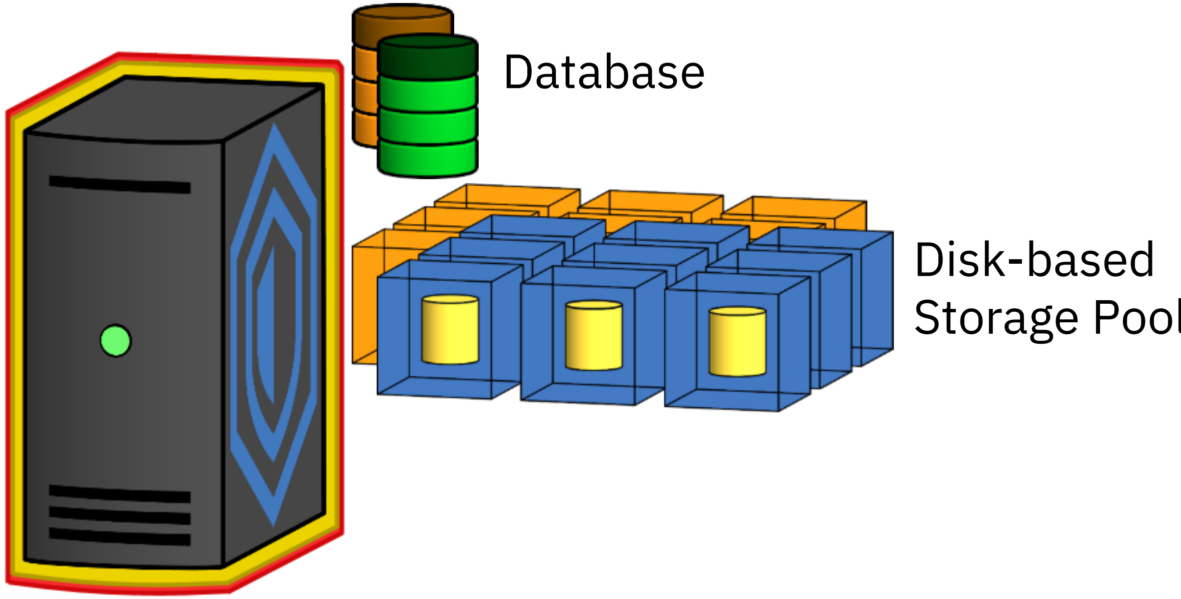
Spectrum Protect for Data Retention

Spectrum Protect for Data Retention is a special-use version of Spectrum Protect. This allows the following features:

- Spectrum Protect administrators cannot delete data as part of normal administrative tasks such as data cleanup, host decommissioning, etc.
- Data archives are protected with software-based WORM controlled by data management policies.
- Extra capabilities to place data holds on archives, including interacting with external content management software.
- Both normal Spectrum Protect and Spectrum Protect for Data Retention support multiple storage pool types such as WORM tape.
- Some content addressable storage features such as NetApp Snaplock, Hitachi Content Platform, etc. are supported by Spectrum Protect for Data Retention.

How to add air gapped solutions to a backup hierarchy

- **A modern backup engine with a disk-only storage pool layout will need to have its profile reduced and protective layers enabled, as outlined earlier.**
- **If desired to provide faster recovery of a backup engine, should it be attacked successfully, disk-based components can be snapshotted.**
- **If greater levels of protection on its storage pool is desired, a copy of data can be taken to different storage types.**
- **Spectrum Protect container pools support encryption at-rest for both disk and object.**



Evaluating Spectrum Protect Directory Container Pools using the 4 Criteria

Logical and Physical Separation (Isolation): The directory container pools themselves are part of the data protection engine, and stored on a file system on that host (or networked file system). While the data protection engine can be secured, the storage cannot be considered isolated. DR Replicas can be created which can potentially increase isolation.

Ease of Corruption or Destruction (Immutability): Node Replication/Protect Stgpool can create a single replica (multiples possible with custom scripting or future features), and the DR target(s) can have different security to help control infiltrator/insider destruction. One can also keep more versions at the replication target(s). But, if the original data is corrupted or destroyed, the replicas can be compromised.

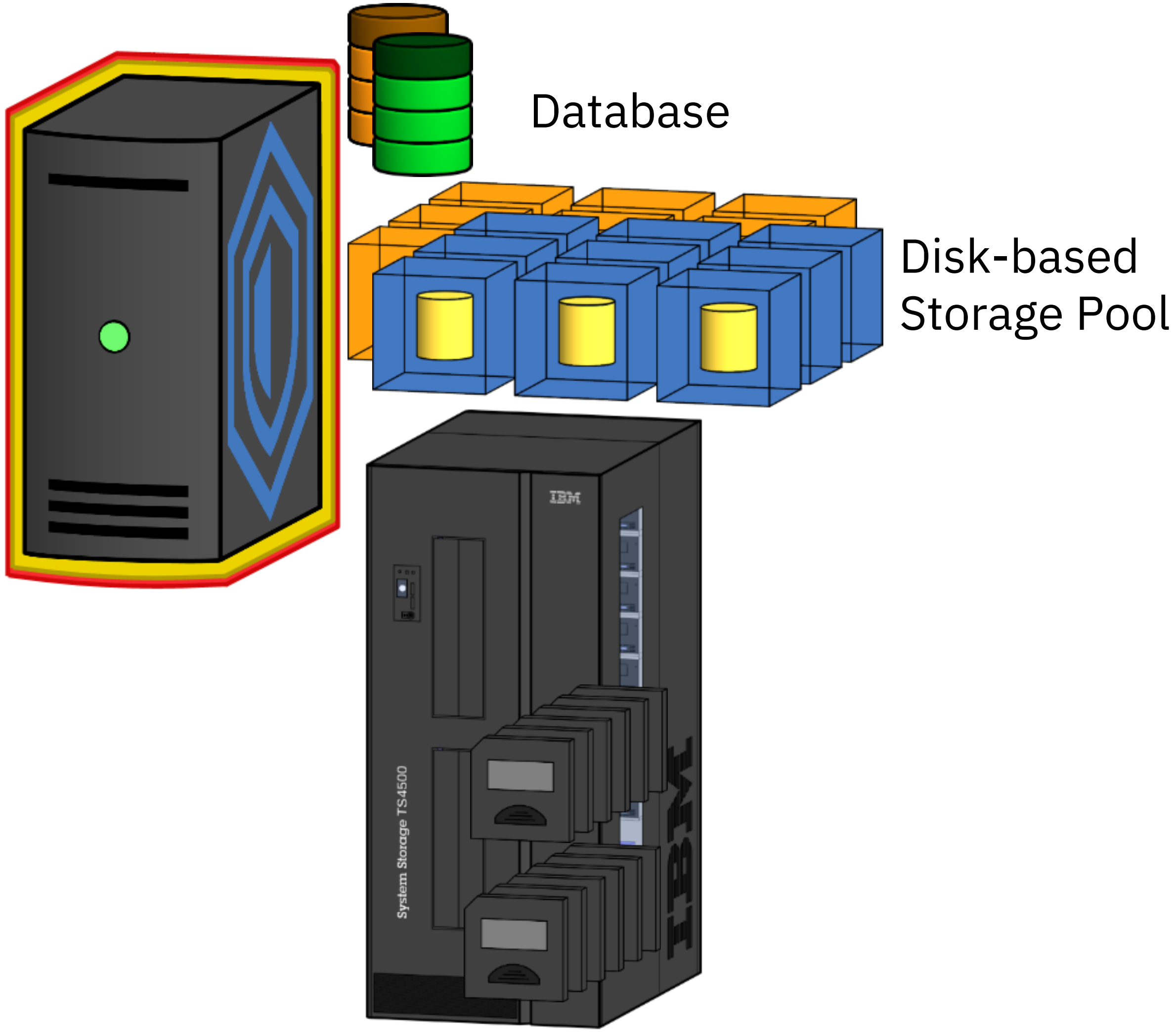
Performance (Speed to meet RTO/RPO in different scenarios): Directory container pools generally provide good recovery performance for traditional backup/restore.

Ease of Reuse: Directory container pools are traditional backup repositories (which are deduplicated and optionally compressed and/or encrypted). This does not yield itself to simple reuse scenarios, although automatic restores can be performed at DR/CR locations.

How to add air gapped solutions to a backup hierarchy

- **A physical tape infrastructure can also provide true air gap (media is not mounted on drive at all times).**

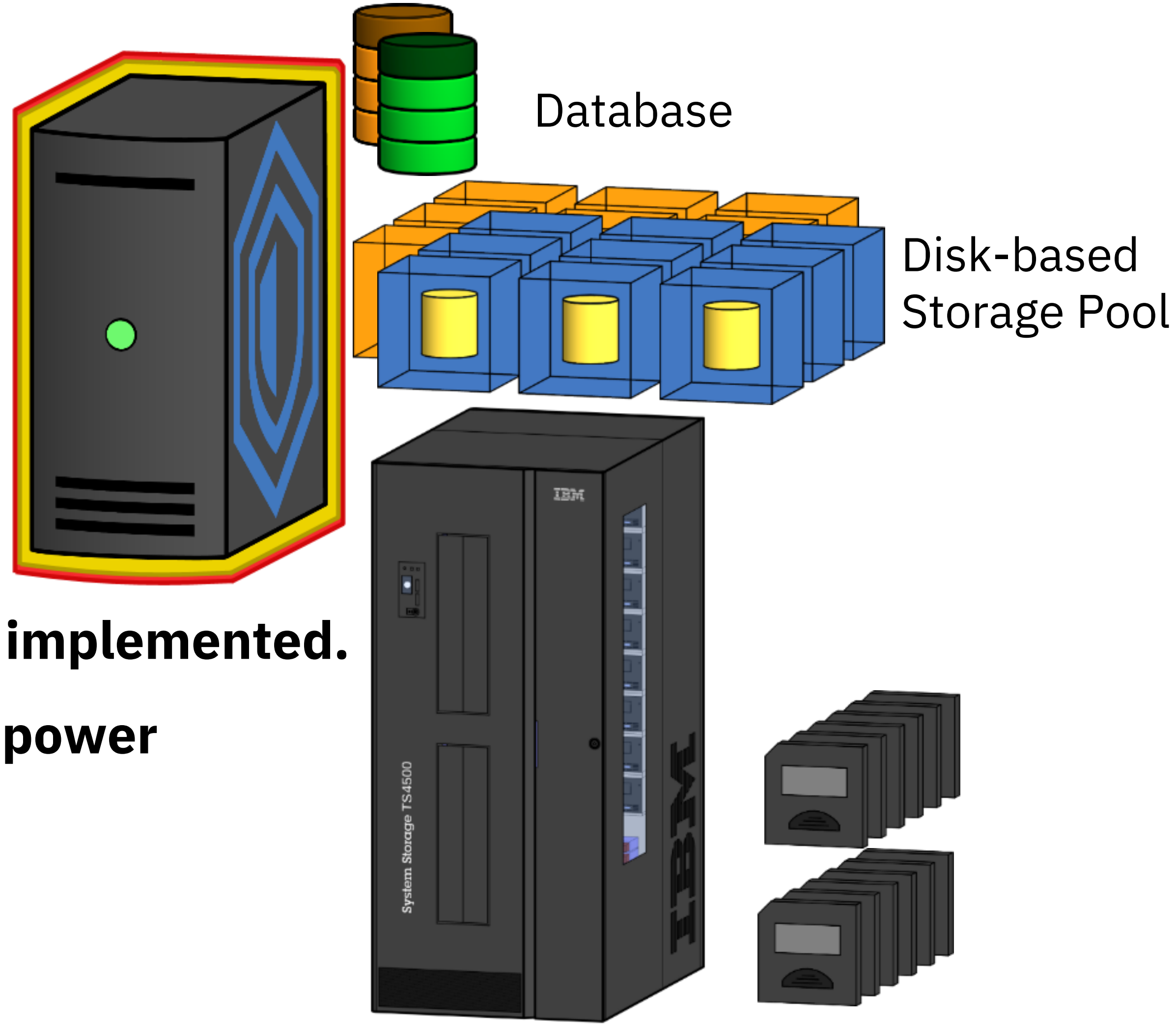
- **For the greatest possible amount of air gap, a copy of the data can be made and ejected from the tape library. This can be combined with media rotation, to provide both air gap and DR protection.**



How to add air gapped solutions to a backup hierarchy

Tape provides a great deal of logical isolation:

- For backups, it is not a file system targeted by ransomware
- Encryption/WORM features
- Physically offline, perhaps ejected from library and stored in vault.



Tape can be very fast, if sufficient tape drives are implemented.

Other benefits (low cost per TB, high density, low power consumption.

Evaluating Tape using the 4 Criteria

Logical and Physical Separation (Isolation): Tape offers the greatest level of isolation. Serial storage devices are not targeted by automatic malware. The media is not automatically online, you can eject the on-site copy from the library, you can create multiple copies and physically rotate those to DR/CR locations. The Vaulting options are more flexible with tape (it can be rotated to any secure location). Due to the nature of physical tape media, an infiltrator/insider may not be able to logically delete/corrupt the media without physical access to it.

Ease of Corruption or Destruction (Immutability): Tape is inherently harder to corrupt due to its greater isolation. It also offers encryption capabilities as well as WORM media options. Due to the nature of physical tape media, an infiltrator/insider may not be able to logically delete/corrupt the media without physical access to it.

Performance (Speed to meet RTO/RPO in different scenarios): Tape read/write performance makes it a very fast option for traditional backups (non-snapshot). But, if you wish high performance across multiple tasks, you must have sufficient numbers of tape drives in the location(s) that requires this performance.

Ease of Reuse: Since tape is exclusively used for traditional streaming backups, it is not particularly effective for simple data reuse. Automatic recovery of data at a DR/CR location can certainly be done, but that will be slower and more complex than exploiting snapshots or disk replicas.

Evaluating Virtual Tape using the 4 Criteria

Logical and Physical Separation (Isolation): Virtual Tape is somewhat isolated as serial storage devices are not currently targeted by automatic malware attacks. The use of native replication and its underlying constructs typically mean the media is logically offline, but an infiltrator/insider can destroy the backups without physical access.

Ease of Corruption or Destruction (Immutability): Virtual Tape is more protected than disk storage pools that reside on file systems but not as protected as physical tape. Support for emulating tape WORM or Encryption will vary, but given the nature of virtual tape it may not be valid. Some VTL vendors have begun offering proprietary, software-based immutability/WORM.

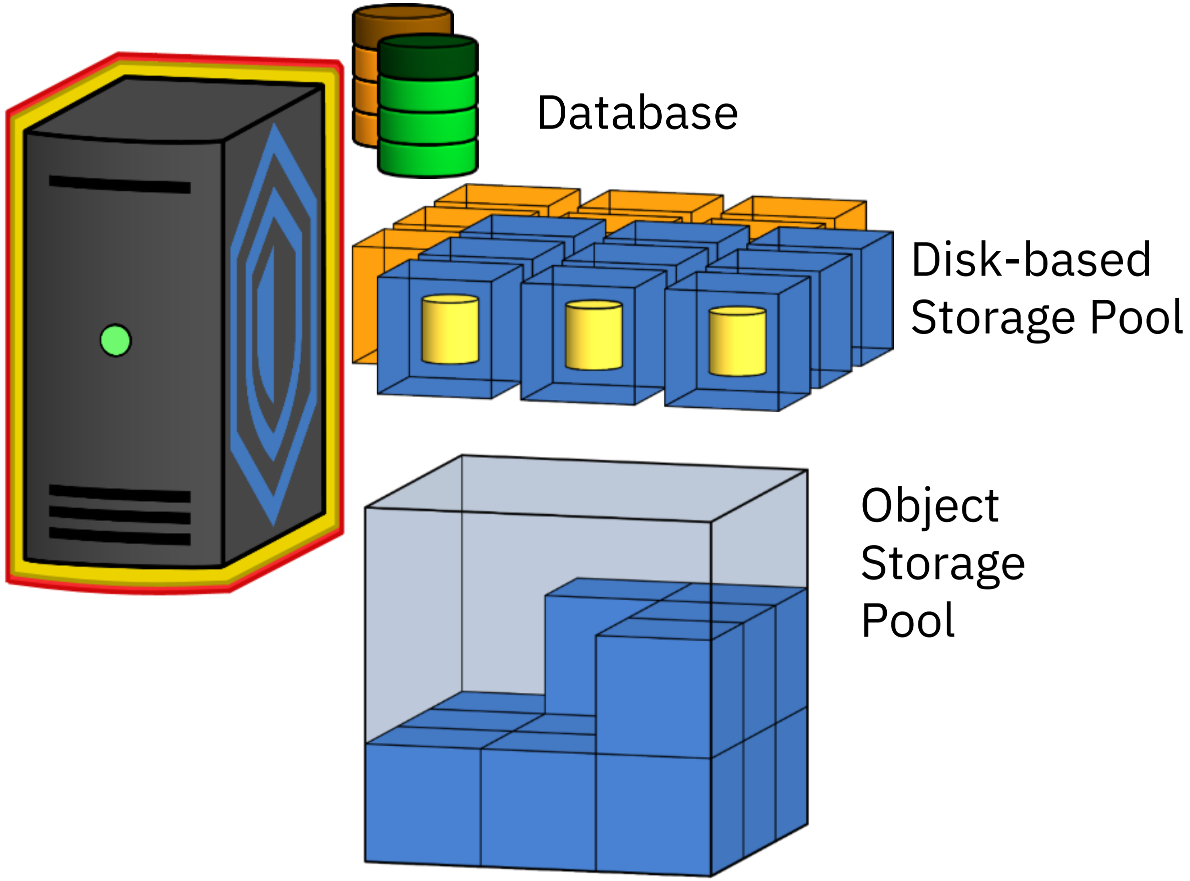
Performance (Speed to meet RTO/RPO in different scenarios): Virtual Tape libraries can typically be a fast storage option for traditional backups, depending upon the VTL model Generally, VTL cannot be scaled to be as fast as physical tape (if sufficient tape drives are implemented).

Ease of Reuse: Since VTL is emulating physical tape it is not particularly effective for simple data reuse. Automatic recovery of data at a DR/CR location can certainly be done, but that will be slower and more complex than exploiting snapshots or disk replicas.

How to add air gapped solutions to a backup hierarchy

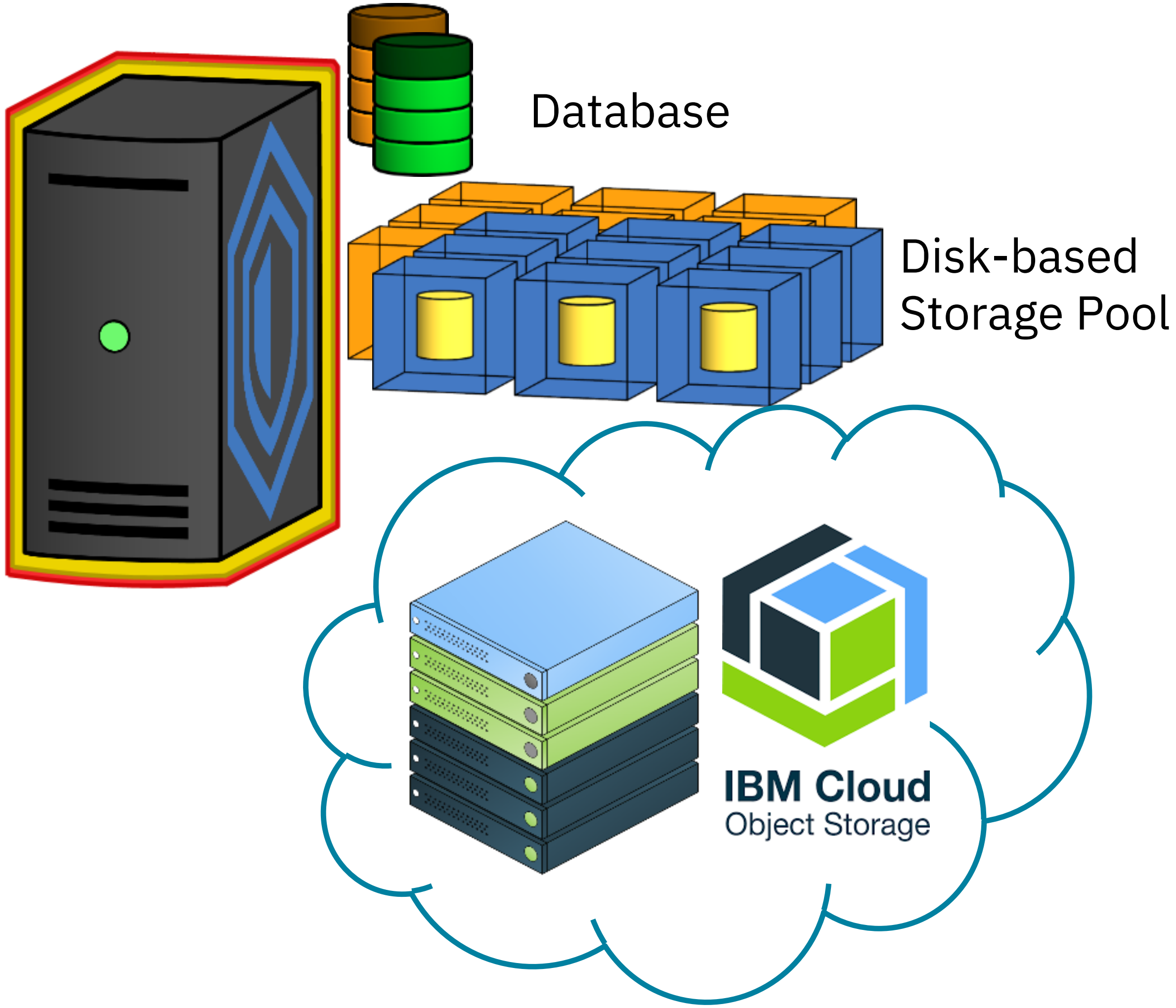
- **An Object Storage tier can also be exploited, as Ransomware does not target object storage devices.**

- **Many Object Storage solutions have built-in replication with multiple copies of data retained by the underlying object storage application.**



How to add air gapped solutions to a backup hierarchy

- **IBM Cloud Object Storage can be used to provide a powerful Object Storage solution, with capabilities including Disaster Recovery protection and Retention protected vaults ideal for use in Cyber Recovery capabilities.**



Evaluating Object Storage using the 4 Criteria

Logical and Physical Separation (Isolation): Object Storage is somewhat isolated as object storage layers devices are not currently targeted by automatic malware attacks. The use of native replication may mean there are dispersed or replicated copies in different locations.

Ease of Corruption or Destruction (Immutability): Object storage may have immutability features that prevent simple data destruction or corruption (such as COS retention vaults). An infiltrator/insider cannot perform surgical data destruction, but large scale destruction of the backup infrastructure or COS itself may be possible.

Performance (Speed to meet RTO/RPO in different scenarios): Object storage, especially cloud-based object storage, is not intended to provide the performance of block or file storage. In other words, it is not meant to be used for high-speed operational recovery.

Ease of Reuse: Object Storage can be used as a repository for traditional backups, native file system tiering or snapshot backup offload. Reuse from traditional backup is not simple, but can be done with automatic restore of the data prior to reuse. Reuse from a file system or snapshot offload may be much easier, depending upon the implementation.

How to add change data protection services to limit Ransomware damage

- **Enable security notifications.**
- **Spectrum Protect policy can control how often a backup takes place. The default is “however often you want”, but you can limit backups of files to once a day, once every 2 days, etc. If Ransomware attempts to corrupt multiple backups, this can limit how much damage to backups the malware can cause.**
- **For critical data, multiple backup or archive targets can be created.**
- **WORM media, such as LTO or TS11XX tape and other technologies are supported by Spectrum Protect. Spectrum Protect for Data Retention allows archive data to be protected with software-WORM.**
- **Snapshots, Snapshots, Snapshots.**
- **Storage pools can be configured to not reuse storage for X days after expiration. This Reuse Delay allows a safety buffer to give you time to react if bad backups have been sent.**

IBM
Spectrum
Protect

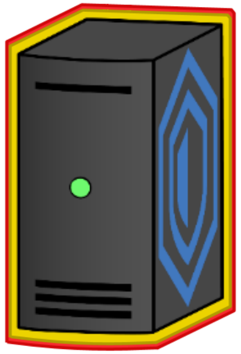
Recommendations Overview

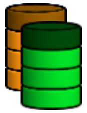
1

Harden the protection of existing backup systems

Having a backup is the pre-requisite for recovery.

Audit capability and ensure success….

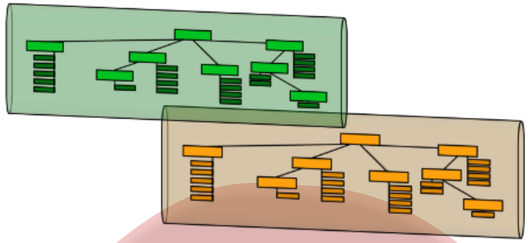




Protect the backup system and database with snapshots

2

Apply Read-only Point-in-Time (PiT) Copies (aka Snapshots) for filesystems or disk volumes supporting core data servers.



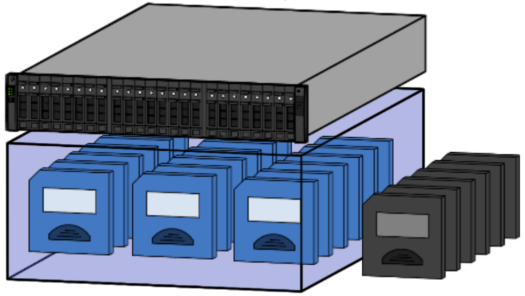
Snapshots are offline to operational servers … Can be Filesystem (e.g. IBM Spectrum Scale) or Disk Controller Based

Harden protection of disk snapshot management for increased air-gap

Allocate recovery server infrastructure on isolated networks to allow audit/analysis/recovery of snapshots or backups.

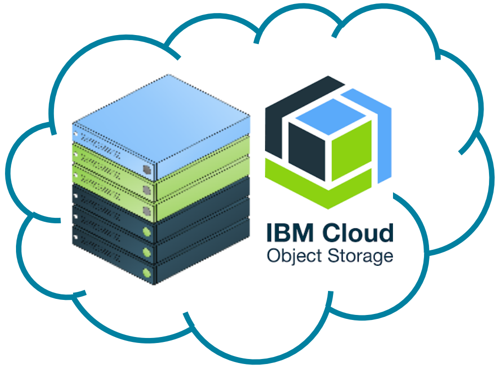
3

Ensure Critical Backups are stored on other non-disk storage



Virtual and Real Tape Libraries offer ability to partition access or physically export.

Cloud object stores can provide vaulting and policy based protection



Logical/Virtual "air-gap" *Increasing "air-gap"* Physical "air-gap"

Increasing Recovery Time

Incremental Costs Curve

The IBM difference

Enterprise data protection

High-throughput air gap

WORM immutable storage

Safeguarded copy

Transparent cloud Tiering supporting hybrid multicloud

Cyber attack preparation

FIPS 140-2 certification

Pervasive encryption

Ransomware detection

Exceeds SLA

100TB/day per server

Restore 2.5 TB VM in < 3 mins

Restart business operations

12x faster with a variety of 3 or 4-site DR configurations

IBM Storage for Cyber Resiliency

Useful DS8000 References

IBM DS8000 Safeguarded Copy, REDP-5506

- http://www.redbooks.ibm.com/redpieces/abstracts/redp5506.html?Open

IBM DS8880 Architecture and Implementation – SG24-8323

- http://www.redbooks.ibm.com/abstracts/sg248323.html?Open

IBM DS8880 Copy Services – SG24-8367

- http://www.redbooks.ibm.com/abstracts/sg248367.html?Open

Useful TS7700 Reference Documents

- **(Redbook) TS7700 Release 4.2 Guide (SG24-8366-02)**
  http://www.redbooks.ibm.com/redbooks/pdfs/sg248366.pdf

- **(Knowledge Center) TS7700 – Customer Documentation 4.2.0**
  https://www.ibm.com/support/knowledgecenter/STFS69_4.2.0/hydra_c_ichome.html

- **(White Paper) IBM TS7700 Full Disk Encryption (FDE)**
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102200

- **(White Paper) IBM TS7700 Series z/OS Host Command Line Request User's Guide**
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101091

- **(White Paper) IBM TS7700 Tape Encryption Overview**
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101000

- **(White Paper) IBM TS7700 Best Practices - FlashCopy for DR Testing V1.5**
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102415

Accelerate with IBM Storage – Cyber Resiliency

Previous Cyber Resiliency Accelerate with IBM Storage Sessions

- WSC - Accelerate with IBM Storage: Copy Services Manager Update and DS8880 Safeguarded Copy Demo
- WSC - Accelerate with IBM Storage: Copy Services Manager / Safeguarded Copy Update
- WSC - Accelerate with IBM Storage: Modern Data Protection
- WSC - Accelerate with IBM Storage: Discover New Features of IBM Cloud Object Storage
- WSC - Accelerate with IBM Storage: TS7760 Best Practices (A View from the Field)