

Washington Systems Center - Storage

Accelerate with IBM Storage: Building a Data Protection Solution for Cyber Resiliency

Dan Thompson

Spectrum Storage Specialist

danthomp@us.ibm.com

Accelerate with IBM Storage Webinars

The Free IBM Storage Technical Webinar Series Continues in 2020...

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 on the Accelerate with IBM Storage Site: <https://www.ibm.com/support/pages/node/1125513>

Also, check out the WSC YouTube Channel here:

https://www.youtube.com/channel/UCNuks0go01_ZrVVF1jgOD6Q

2020 Upcoming Webinars:

May 19 – Spectrum Scale – Stretched Cluster Design

Register Here: <https://ibm.webex.com/ibm/onstage/g.php?MTID=e21d6394be1f4e99e2f28866e7d2b5c88>

May 21 - Storage Insights, Storage Insights Pro or Spectrum Control, which one is right for me?

Register Here: <https://ibm.webex.com/ibm/onstage/g.php?MTID=eeb831096e67ff598348a5bb301d3038d>

June 2 – Spectrum Scale ESS 3000

Register Here: <https://ibm.webex.com/ibm/onstage/g.php?MTID=e6920e411fed595003800af92ecffe68e>

June 4 - TS7700 Systems and zOS - Two Partners Better Together!

Register Here: <https://ibm.webex.com/ibm/onstage/g.php?MTID=efdf15a2fcf8a4582d87a6e73d3ac9544>



WSC Accelerate Survey

Please take a moment to share your feedback with our team.

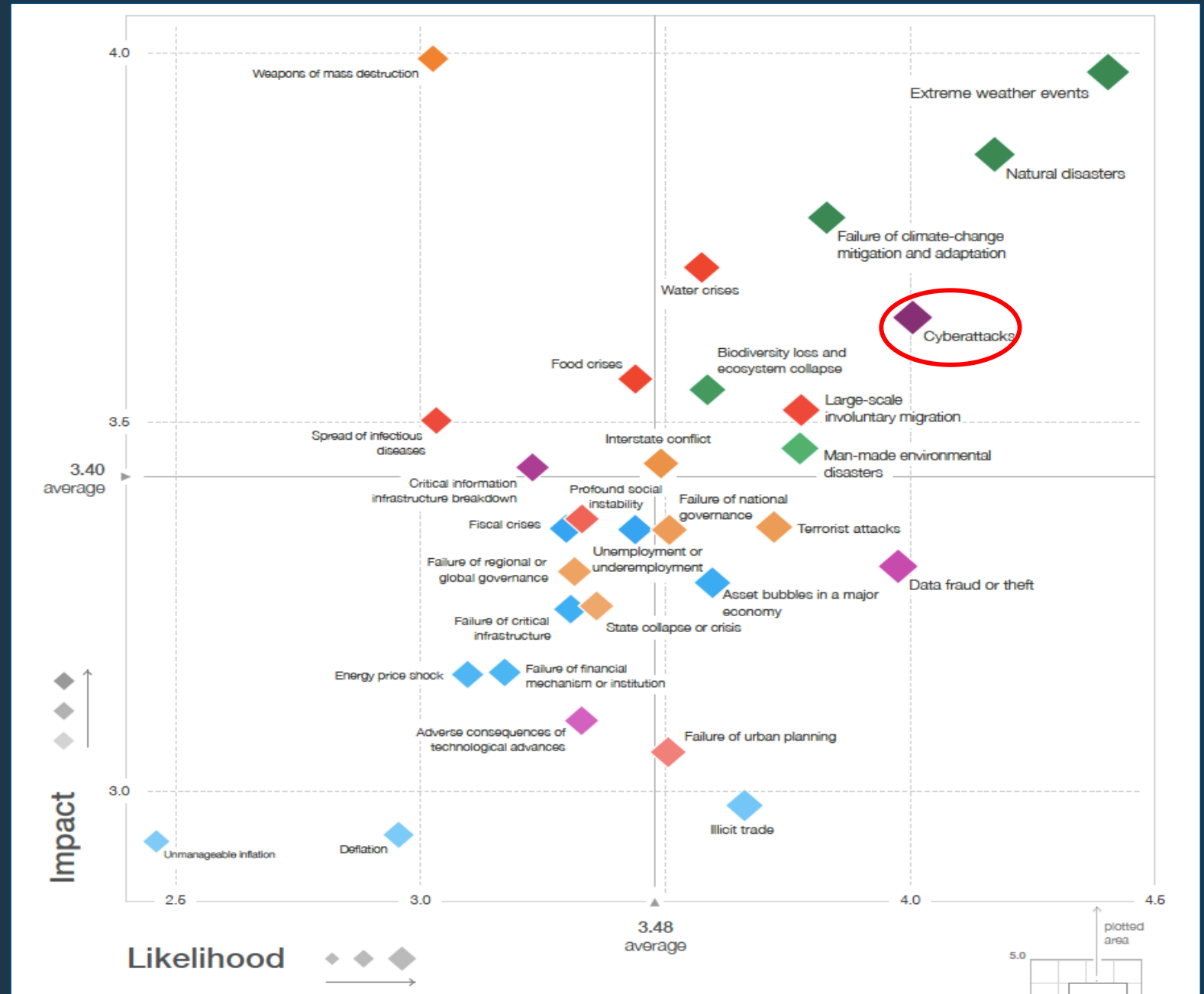
You can access it via

[Menti.com](https://www.menti.com/223747) 22 37 47

World Economic Forum 2018 Global Risks Perception Survey:

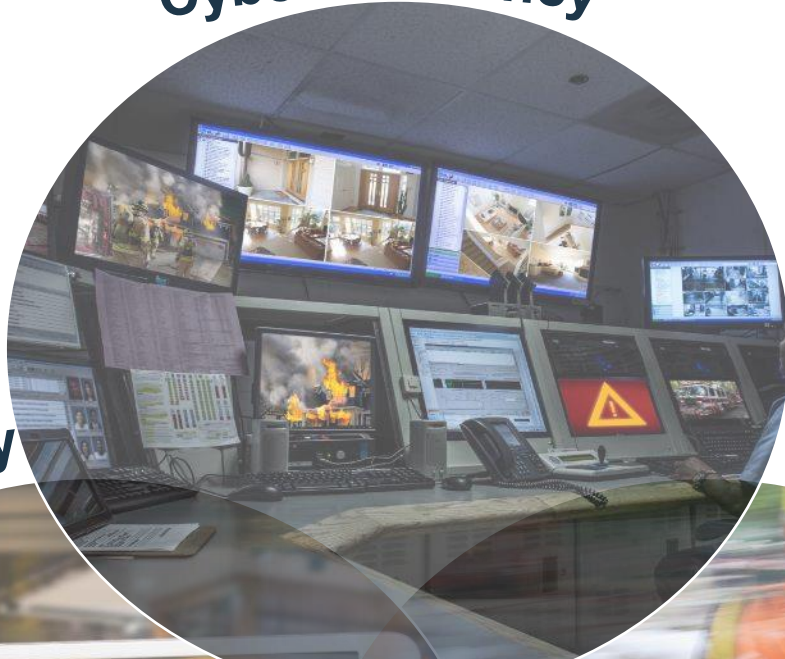
Cyberattacks ranked #3

“Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace.”



Source: World Economic Forum, 2018

Cyber resiliency



Business continuity



Disaster recovery



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

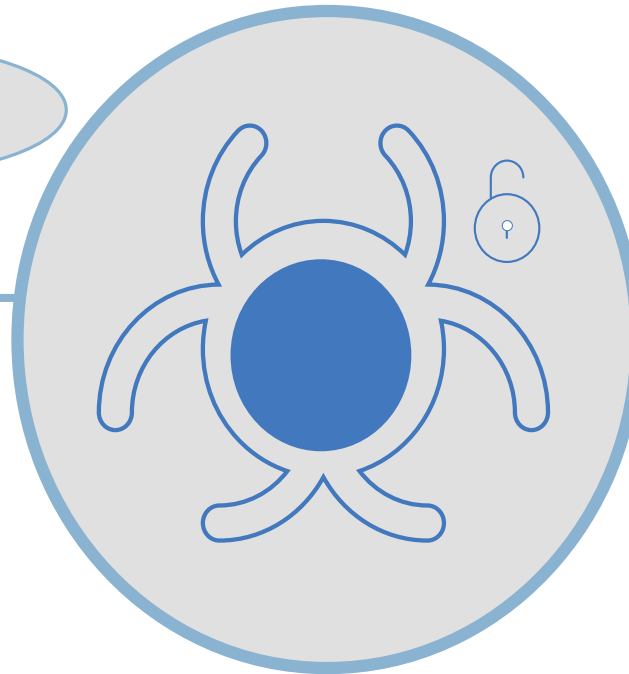
\$3.92 million

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

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



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**



EUROPEAN CENTRAL BANK

EUROSYSTEM



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



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

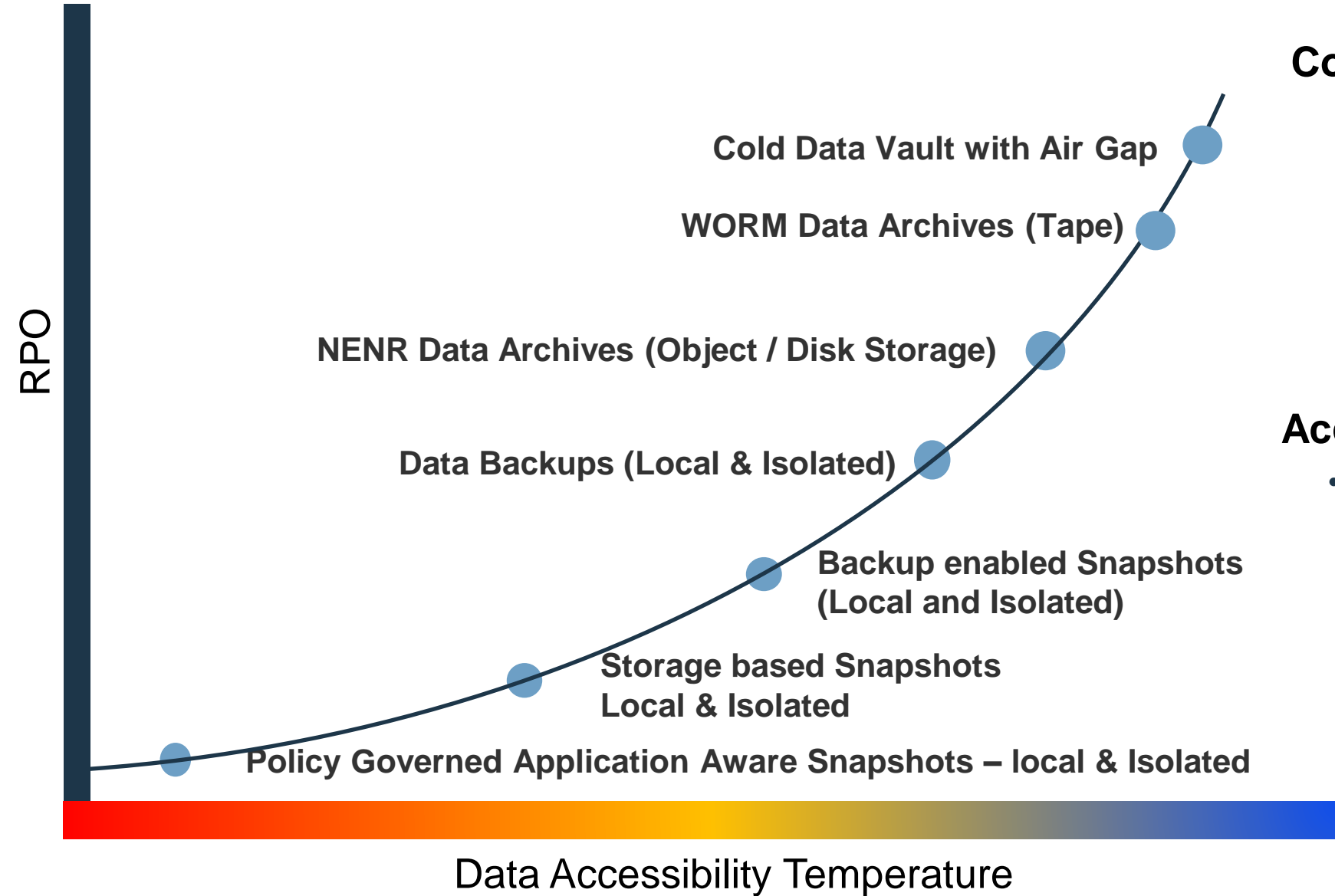
Respond:

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

Recover:

Restore capabilities and services - recovery, improvements, communications

Storage Services and Ransomware



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

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 an 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:

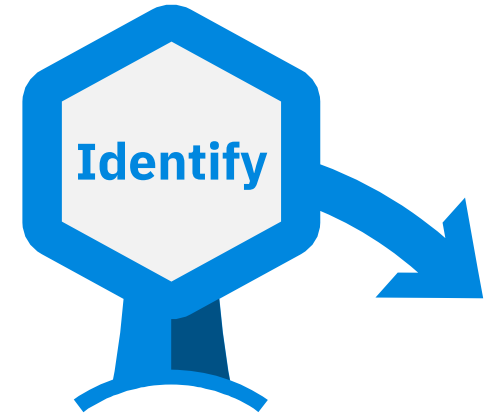
Detecting occurrence of cyber security events – timely, continuous monitoring, detection processes

Respond:

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

Recover:

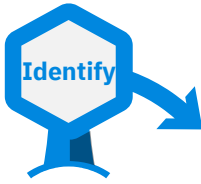
Restore capabilities and services - recovery, improvements, communications



Identify

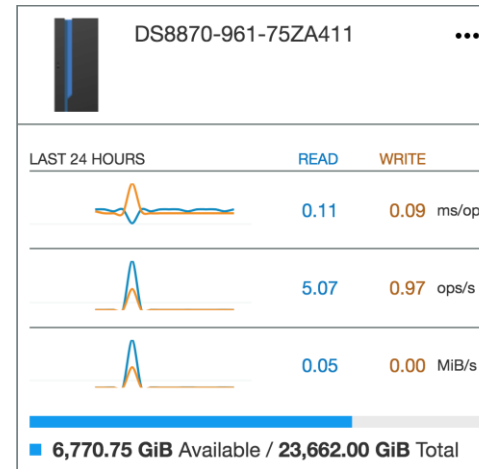
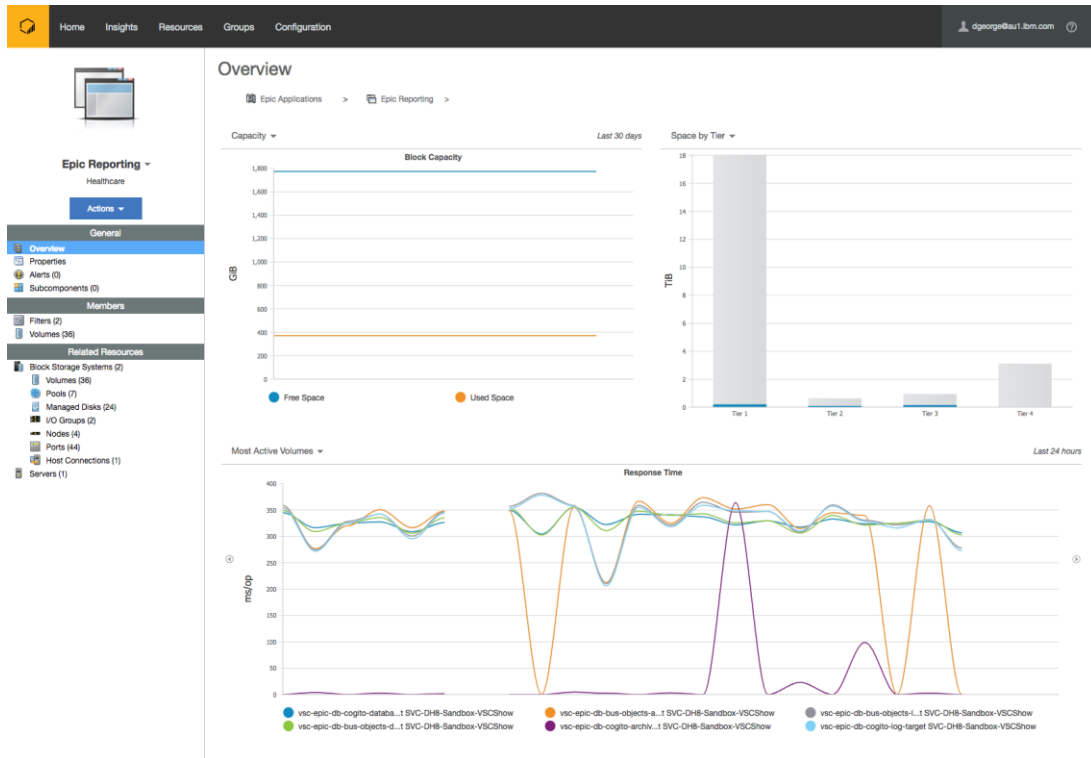
Defining a roadmap and action plan to build or improve Organization's cyber resilience plan

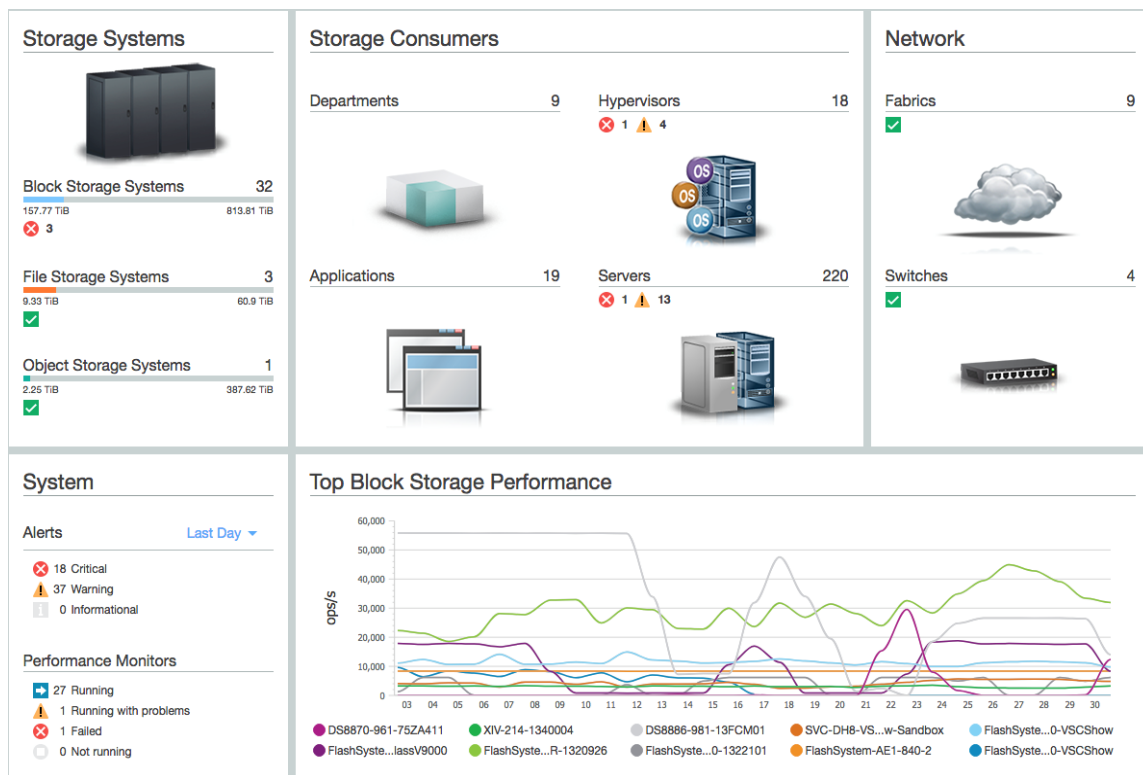
Identify



- IBM Storage Insights Pro
- IBM Spectrum Control
- IBM Spectrum Protect

- Offerings help identify where primary data is located
 - Organize and understand what's critical
- Offerings understand “normal” performance requirements
- Offerings help understand daily changes





Revenue Producing Data

- Intuitive Storage UI
 - Dynamically changing Storage Infrastructure
 - Historical State and Performance information
 - Insight into Block/File/Object/Network
 - Alignment into Business Applications and Units
- Storage Insights Pro
 - Up and running with the cloud in minutes
 - Only maintain simple Collector Agent
- Spectrum Control
 - When cloud is not an option

NIST – Identify

- Develop Organizational Understanding to manage cybersecurity risk
 - Asset Management
 - Business Environment
 - Governance
 - Risk Assessment
 - Risk Management Strategy
- Key IBM Offerings help:
 - Identify where data is located – Insights / Control
 - Understand “normal” performance requirements – Insights / Control
 - Understand daily data changes – Protect
 - Find changes quickly - Discover



IBM
**Spectrum
Discover**



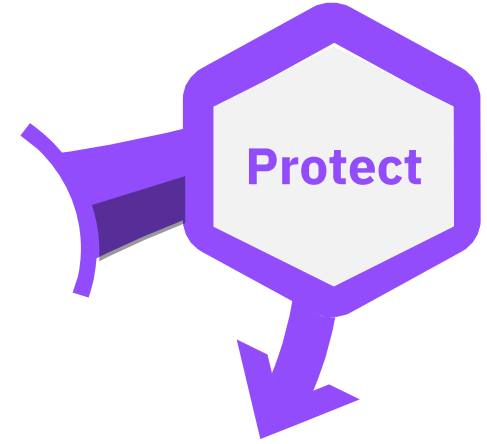
IBM
**Storage
Insights**



IBM
**Spectrum
Control**




IBM
**Spectrum
Protect**



Protect

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

NIST Cyber Resiliency Framework



Protect

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 **Spectrum Protect**



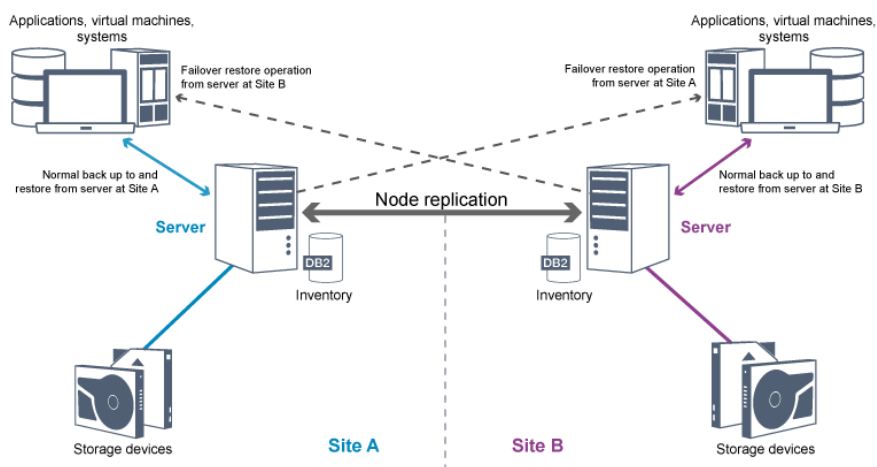
IBM **Spectrum Protect Plus**



IBM Cloud **Object Storage**



IBM **Tape**



Take copies of Revenue Producing Data

- Structured and Unstructured Data
- Flexible Licensing Options
- Flexible Storage Options
- Flexible Policy Configuration
 - Placement
 - Application Classification
- Highly Scalable
 - Single offering to protect enterprise data
- **True Air Gap**
- **Recovery**
 - **RPO 24h (* typical)**
 - **RTO variable**



IBM **Spectrum Scale**



IBM **Spectrum Archive**



IBM **Tape**

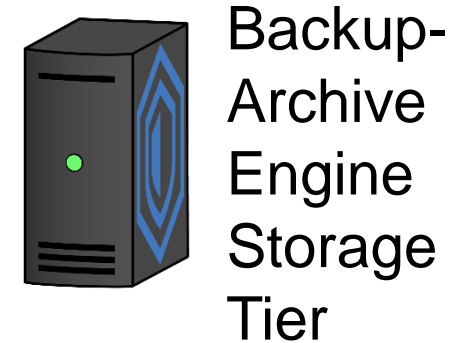
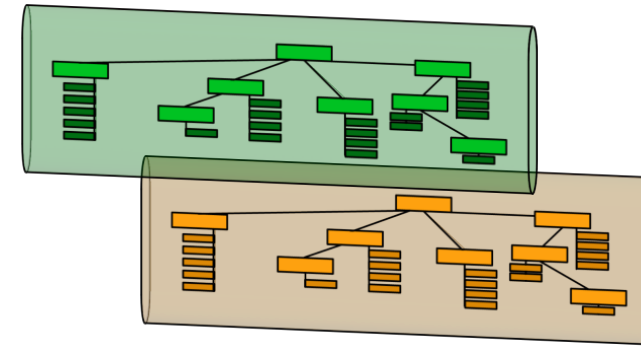


For Primary Data

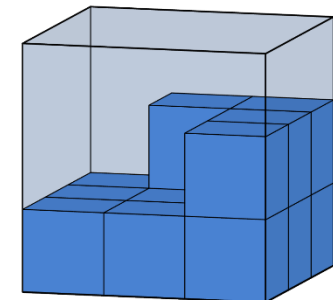
- File Data
- Flexible Licensing Options
- Automatic replication
 - True Air Gap
- Flexible Policy Configuration
 - Placement
 - Application Classification
- Highly Scalable
 - Single offering to hold enterprise data
- Recovery
 - RPO variable (* mins-hrs)
 - RTO variable

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.
- As mentioned earlier, an advanced file system will also support protective snapshots.



Tape Storage Tier



Object Storage Tier

IBM Tape



- Market Leader
- Lowest Cost, Fastest Storage Medium
- Removable Inherent Air Gap
- Works with IBM Spectrum Protect
 - Efficient Copy Management (of copies)
- Environmentally Friendly
- High Automation



IBM **Spectrum CDM**



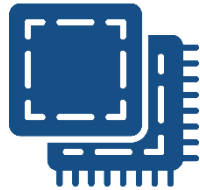
IBM **Spectrum Protect Plus**



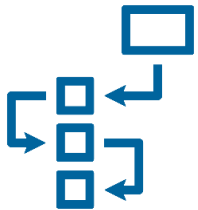
Recovery



Disaster Recovery



Patch Management



Test/Dev Devops



Analytics



Reporting

Take copies of Revenue Producing Data

- Modern Application Protection
- Modern Virtual Machine Protection
- Data stored in native format, immutable
- Simple Configuration
- Easy to use
- Roles based access control
 - End user data access to copies of stored data
- Automation for End to End provisioning
- Recovery
 - RPO 15m - 24h
 - RTO mins



IBM **Spectrum Virtualize**



IBM **Spectrum Accelerate**

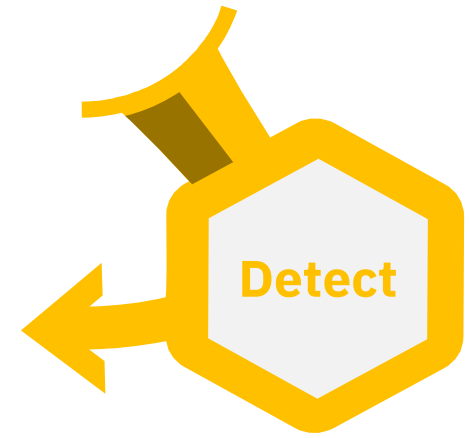


IBM **Spectrum CDM**



Block based replicated data

- Leverage CDM to drive automation
- Replicate Application LUNs to an air-gapped/fenced storage infrastructure
 - Airgap means IP network connectivity is limited
 - Administrative privileges are separated
 - CDM drives snapshots of working systems
 - Sufficient historical snapshots are retained for additional recovery points
- Policy Driven
 - “Snapshot Of Snapshot” used to present data back out when required
 - Separate Administrators
- Recovery
 - RPO 15m - 24h
 - RTO mins



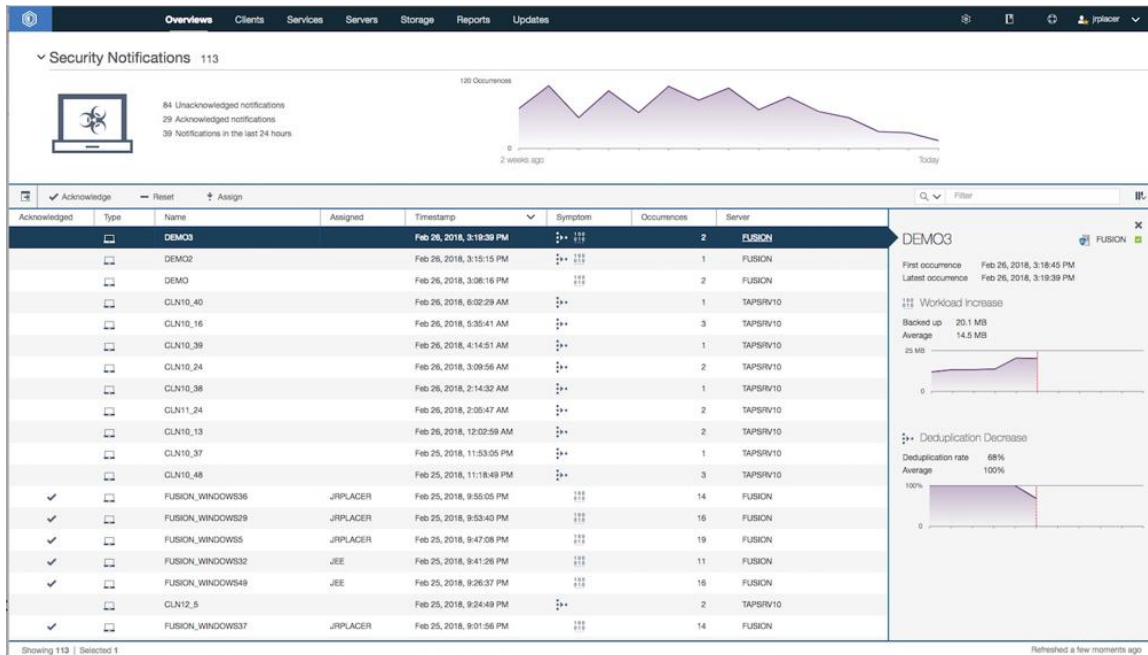
Detect

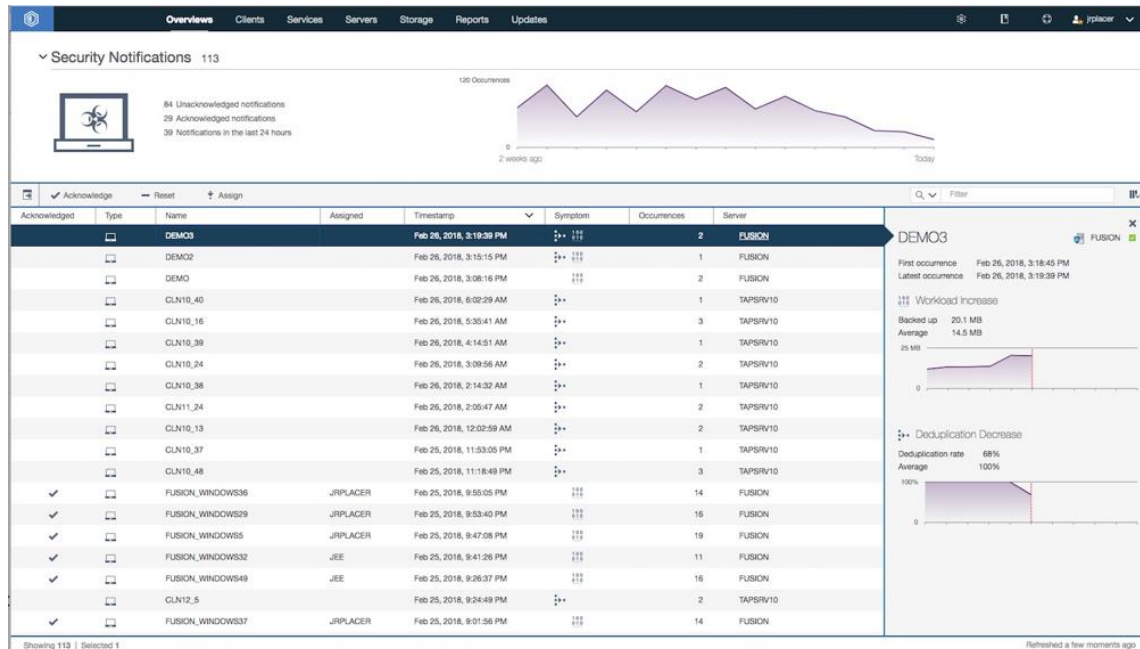
Detecting occurrence of cyber security events
– timely, continuous monitoring, detection
processes



Leverage Tools to Identify Breaches

- Monitor Revenue Producing Data Realtime Performance
- Monitor Copying of Revenue Producing Data Performance
- Understand Changes in Data Reduction Results



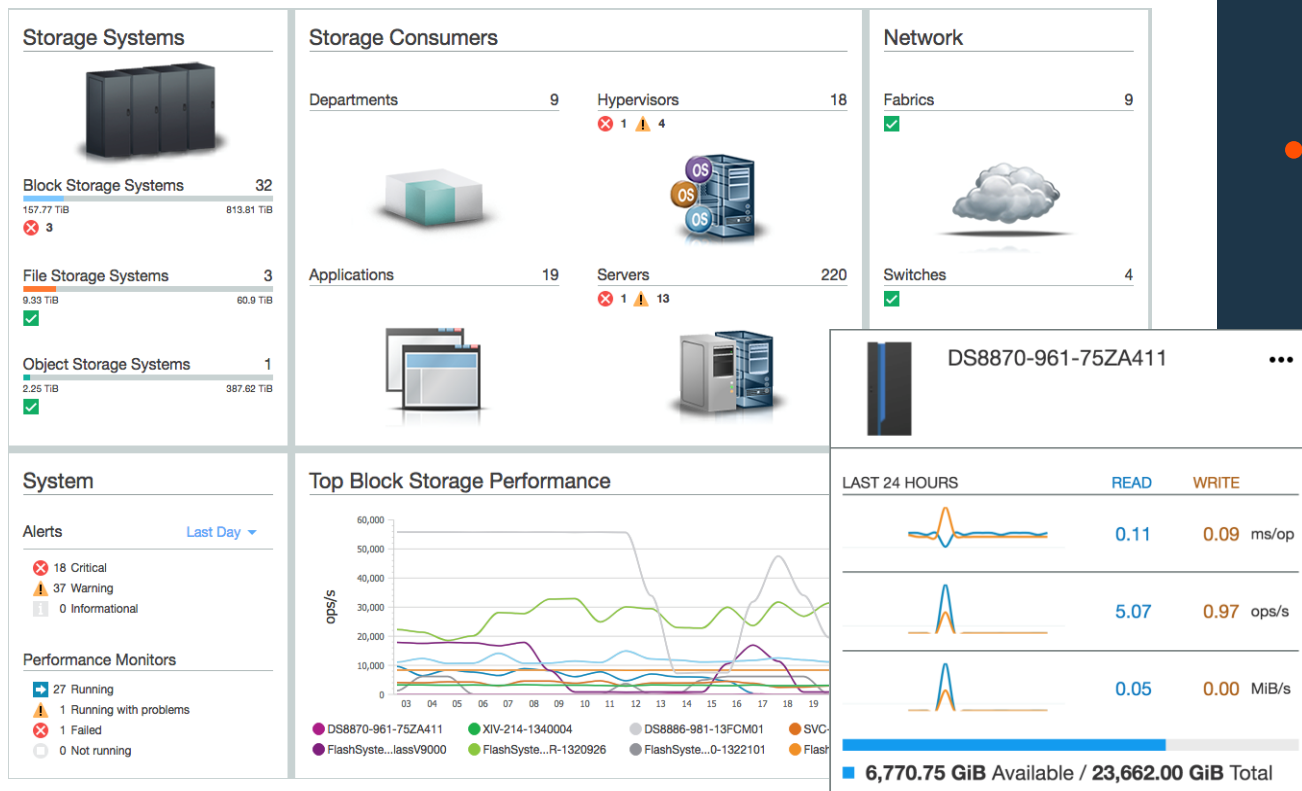


- Proactive
 - Validate protected data (AUDIT *)
- In Action Changes in
 - Number of Files Protected
 - De-duplication Ratio
 - Virtual Machine Block Change Rate
 - HSM Recalls



- Proactive
 - Review historical performance

- In Action Changes in
 - Unusual performance impact alerts



NIST – Detect

- Develop & Implement Activities to identify a cybersecurity threat
 - Anomalies & Events
 - Continuous Security Monitoring
 - Detection Process
- Key IBM Offerings help:
 - Monitor Performance – Insights / Control
 - Understand data changes – Insights / Protect
 - Validate protected data – Protect



IBM
**Storage
Insights**



IBM
**Spectrum
Control**



IBM
**Spectrum
Protect**



Respond

Taking action regarding a detected event –
contain, analysis, mitigation



Disconnect from the threat

- Leverage Storage Infrastructure Management
 - To know where to disconnect
 - What to disconnect
 - What to shutdown

- Validate “Go/No Go” for recovery:
 - Where you able to stop the threat in time from full destruction?
 - Full recovery is destructive
 - Ensure you do need to revert
- Identify IBM Storage Products
 - IBM Storage Insights Pro
 - IBM Spectrum Control
 - IBM Spectrum Protect

NIST – Respond

- Develop & Implement Activities to take action on a cybersecurity incident
 - Response Planning
 - Communications
 - Analysis
 - Mitigation
 - Improvements
- Key IBM Offerings help:
 - Full environment recovery – Protect
 - Instant application / data recovery – Protect Plus / CDM
 - Utilize data copies – Protect Plus / CDM
 - DR Automation – CDM



IBM
**Spectrum
Discover**



IBM
**Storage
Insights**

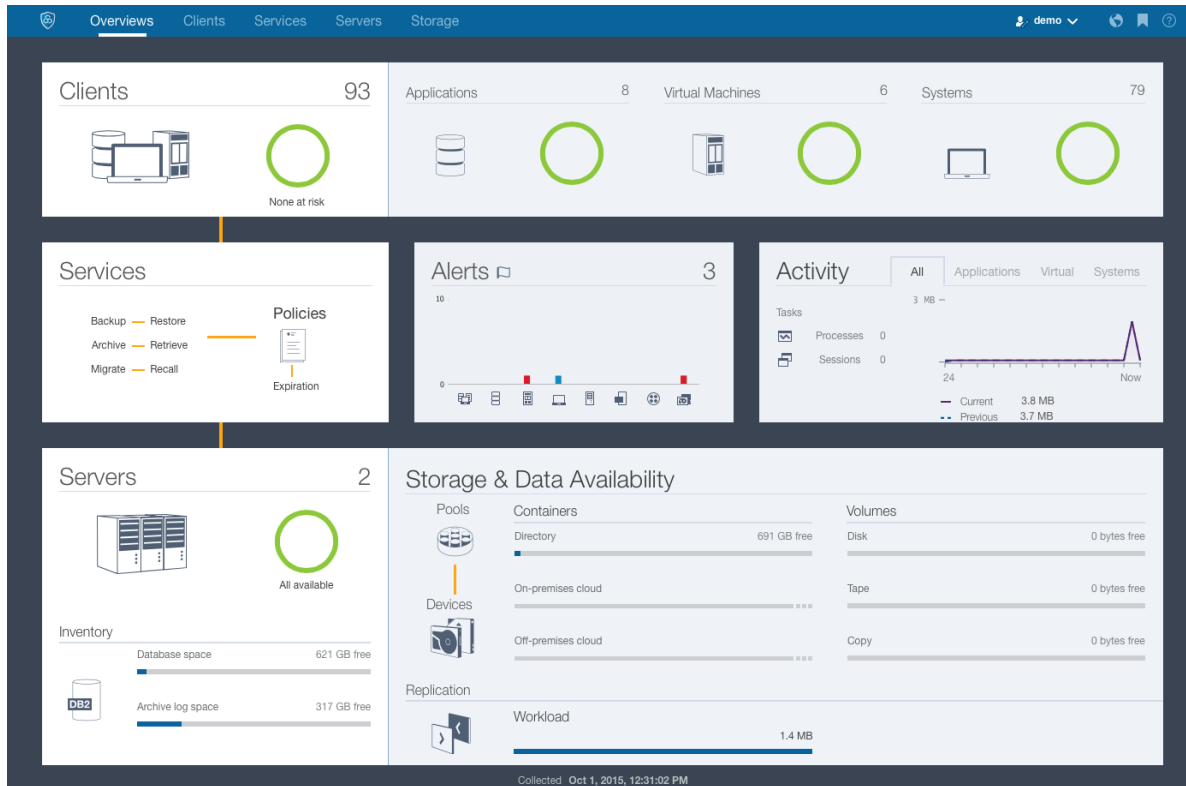


IBM
**Spectrum
Control**



Recover

Restore capabilities and services - recovery, improvements, communications



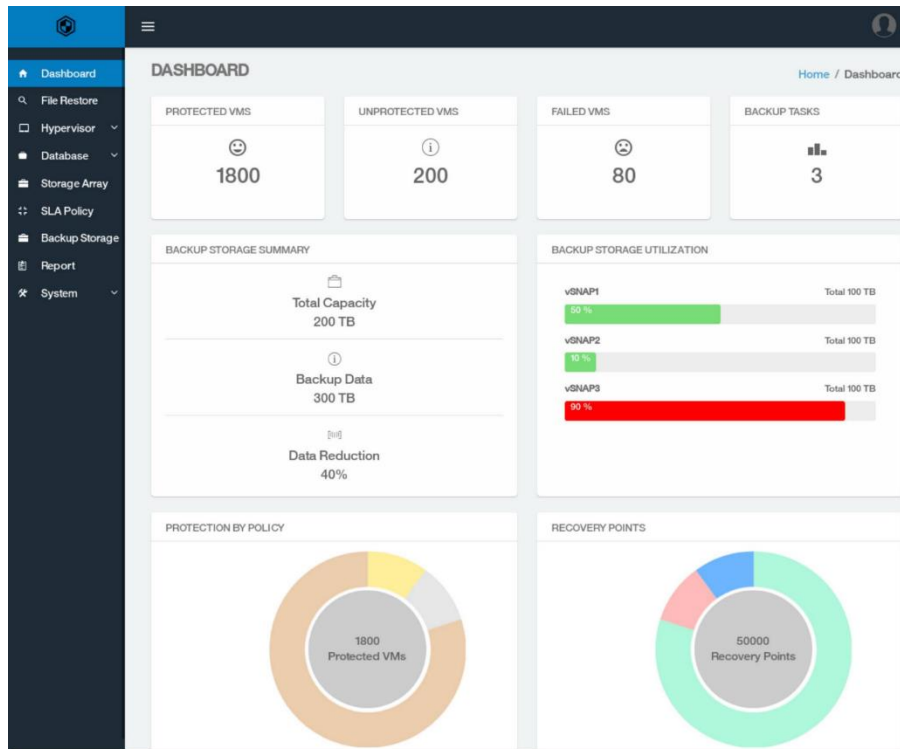
- Disaster Recover Manager
- Fast, Single Pass Recovery
- Leverage Replica for Recovery
- Recover Protect itself from a Replica



IBM Spectrum Copy Data Management

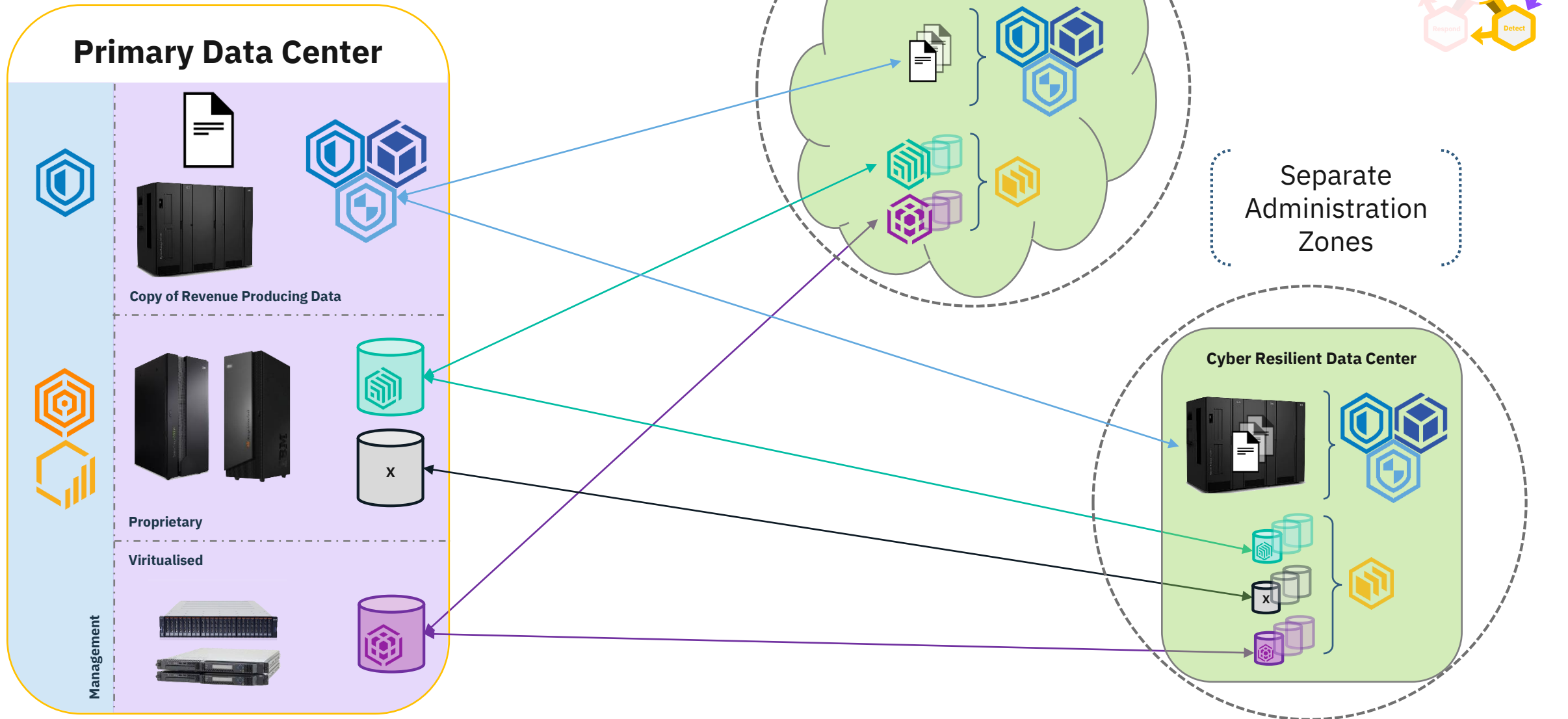


IBM Spectrum Protect Plus



- Instant Recovery
 - Test before commit
- Application End to End Recovery
 - Automation
 - Skills
- Automation with RESTful APIs
- Leverage Replica for Recovery

IBM Cyber Resilient Architecture



Spectrum Protect Family and WORM/Immutable Storage

- Spectrum Protect provides logical, software-based protection of backup/archives, but a Protect Admin can delete data as part of normal operations. Clients can be authorized to delete or expire backups, as well.
- Spectrum Protect for Data Retention/System Storage Archive Manager provides software WORM for archives (administrator cannot delete or obfuscate the archive data).
- Spectrum Protect supports many WORM/Immutable storage devices (physical WORM such as optical or Firmware-based WORM like tape).
- Spectrum Protect **Plus** supported IBM Cloud Object Storage retention vaults starting v10.1.3 (released 02-2019).
- Spectrum Protect will support creation of recovery points based upon existing backups, starting in v8.1.7 (released 02-2019).

Defining a 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.

Quantifying the concepts of Air Gap and Immutability

- The term air gap initially referred to a computer truly disconnected from the network. From a networked application or networked backup perspective, this term is somewhat incongruous.
- When discussing air gapped storage, it is better to consider some key characteristics:
- **Logical and Physical Separation:** Is the recovery point a read-only logical snapshot within the same file system? Is the recovery point a space-efficient snapshot within the same disk subsystem? Is the recovery point a traditional backup of data on a different disk subsystem within the same datacenter? Is the recovery point on tape, ejected from the library and shipped to a vault?
- **Ease of Corruption or Destruction:** Is the recovery point offline or immutable from automatic encryption attacks? Is the recovery point stored within the same file system or disk subsystem and therefore susceptible to insider attacks? Is the recovery point retained for a short enough period such that it will be corrupted if the corruption of the primary data is not detected in a timely manner? Is the recovery point a file system snapshot, disk snapshot or backup stored in a location secured such that a single infiltrator/insider cannot attack multiple copies of the data.
- **Note:** since the greater the degree of separation may also mean the slower the recovery, it is not uncommon to need a multi-level/multi-copy solution. So, we cannot ignore performance characteristics to meet RTO/RPO requirements in different scenarios. We are beginning to see more requirements for Cyber Recovery (CR) in addition to traditional backup/restore and DR requirements.

Third Characteristic Important to Cyber Recovery

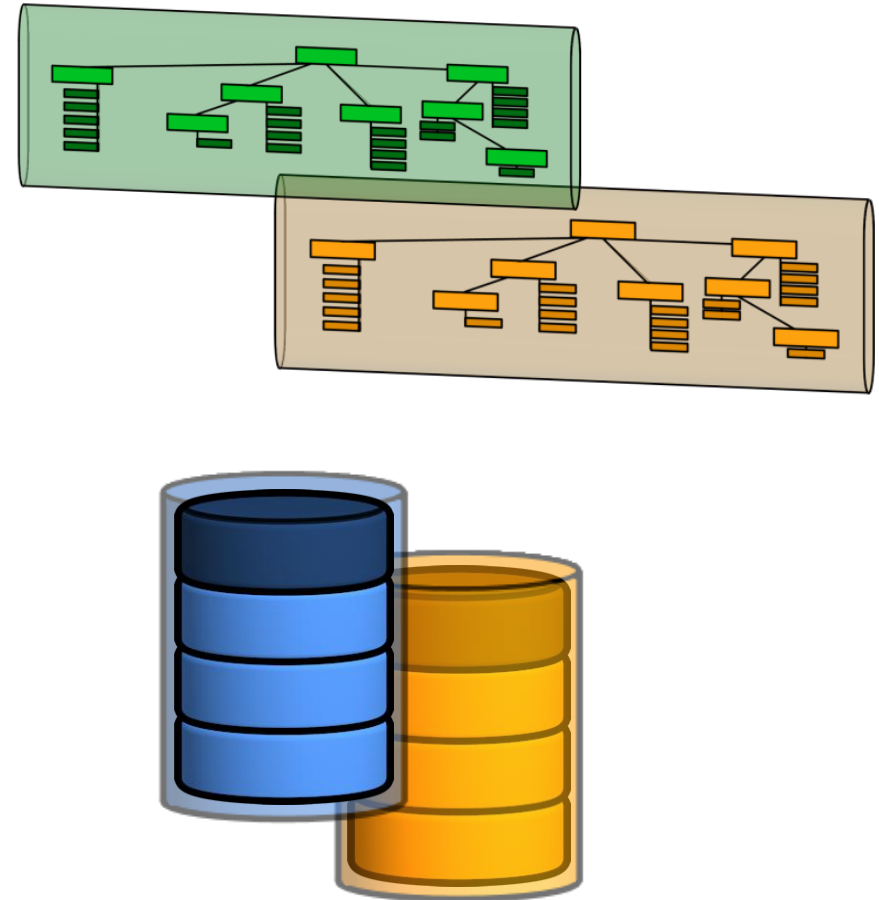
- In addition to the 2 characteristics related to Air Gapped storage, a third is important to other Cyber Incident Recovery:
- **Ease of Reuse:** Can the storage in question easily be recovered or otherwise accessed for use by automatic validation software? Such capabilities are key to advanced cyber incident recovery tools, which evaluate whether backups contain infected or otherwise compromised data.

Recap: Four Main Criteria to Compare Air Gap or Immutable Storage

- Logical and Physical Separation (Isolation)
- Ease of Corruption or Destruction (Immutability)
- Performance (Speed to meet RTO/RPO in different scenarios)
- Ease of Reuse

Recovering from a large malware encryption event

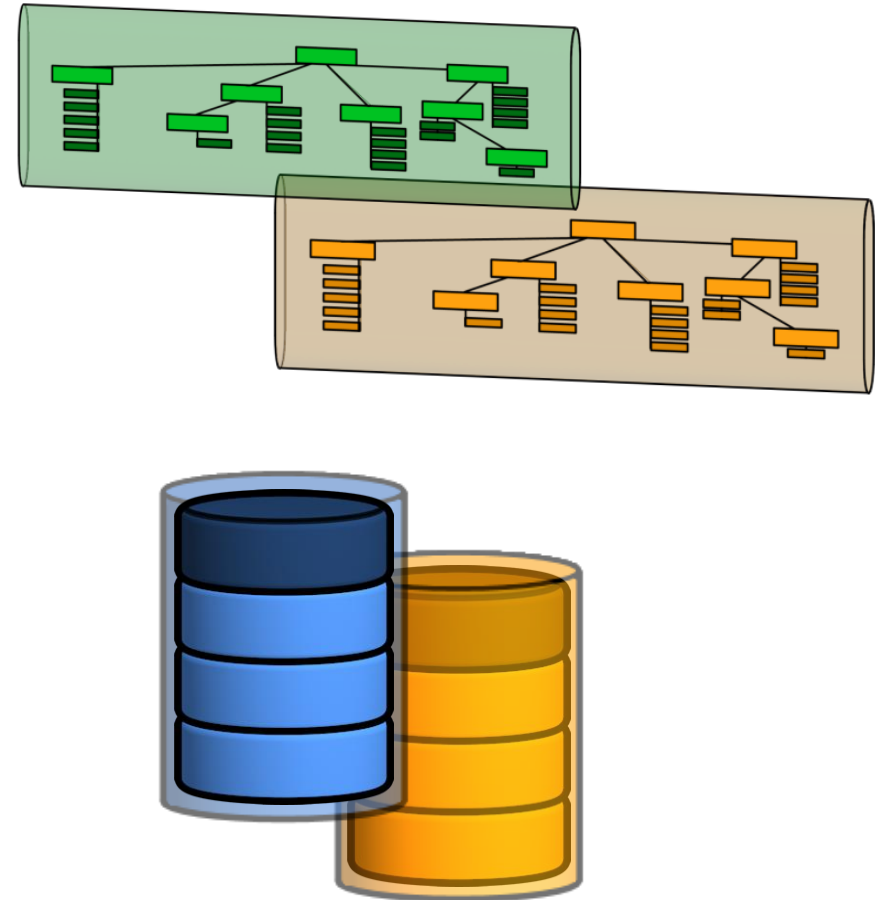
- Ransomware works by targeting a user machine, but it does not damage that machine at first. After it has infected a machine, it attempt to encrypt data on any share that it can locate from that machine (Latch-On and Expand). In other words, it is targeting files on a file system, which can be documents, databases, etc.
- After following good security practices and eliminating unneeded shares or exports, there may still need data that needs more protection to prevent having to pay the ransom in the Restore (decrypt) stage.
- One good first step is to create read-only snapshots of file systems or, for applications, disk snapshots not exposed to the machine's operating system. These snapshots can be used as a quick recovery.
- It will be necessary to keep a sufficient number of snapshots to give you time to detect and stop the Expand (encryption) stage.



Recovering from a large malware encryption event

While Snapshots provide:

- Very fast Recovery Time and Recovery Point
- They are either read-only (file system snapshots) or offline to the physical machine (disk subsystem snapshots or logical snapshots in backup repository)
- Local Snapshots can be attacked by infiltrator/insider with access to the file system or subsystem.
- Replicated copies can exist on remote systems with different security settings.
- Sophisticated workflows may exist (create snapshot and replicate to another location; create replicas which are then snapshotted at remote location and mounted for reuse/validation, etc.)
- IBM DS8000 family provides for SafeGuarded snapshots created by Copy Services Manager or GDPS, for protection against infiltrator/insider. CSM provides advanced support for SafeGuarded copies.



Evaluating Snapshots using the 4 Criteria

Logical and Physical Separation (Isolation): Snapshots are not visible to automatic or simple malware attacks, but typically reside within the same file system or controller. Replicating snapshots to DR/CR locations may create greater separation, and newer technology DS8000 hidden snapshots can help create greater isolation.

Ease of Corruption or Destruction (Immutability): If a snapshot resides within the same file system or controller, they may not be protected from infiltrator/insider attack, or simple human error. Depending upon the technology, a snapshot may or may not be truly read only. Replicating snapshots to DR/CR locations may create greater isolation, and newer technology DS8000 hidden snapshots can help create greater levels of protection.

Performance (Speed to meet RTO/RPO in different scenarios): Snapshots typically offer the greatest level of recovery performance, so are a good candidate for the first level of recovery from large data corruption/encryption attacks.

Ease of Reuse: Snapshots are typically very easy to Reuse, as they are copies of the natively formatted data. They are also easily replicated to DR/CR locations, which allows the location of this reuse to be flexible.

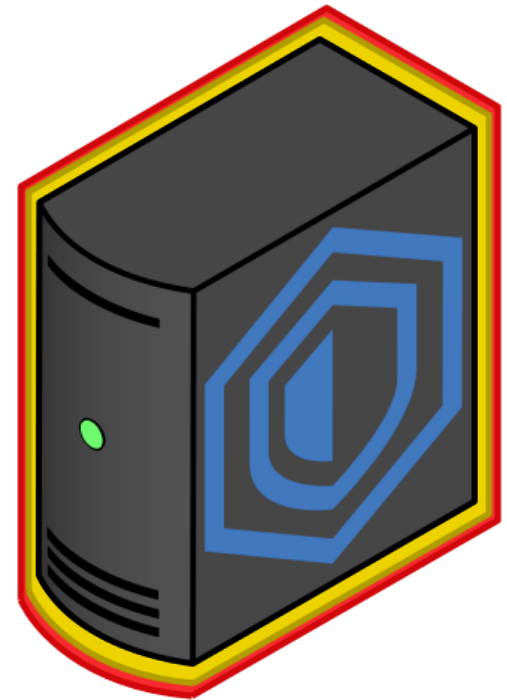
Backup Solution Design with Immutability, Air Gap and Cyber Vaulting



Spectrum Protect for Data Retention

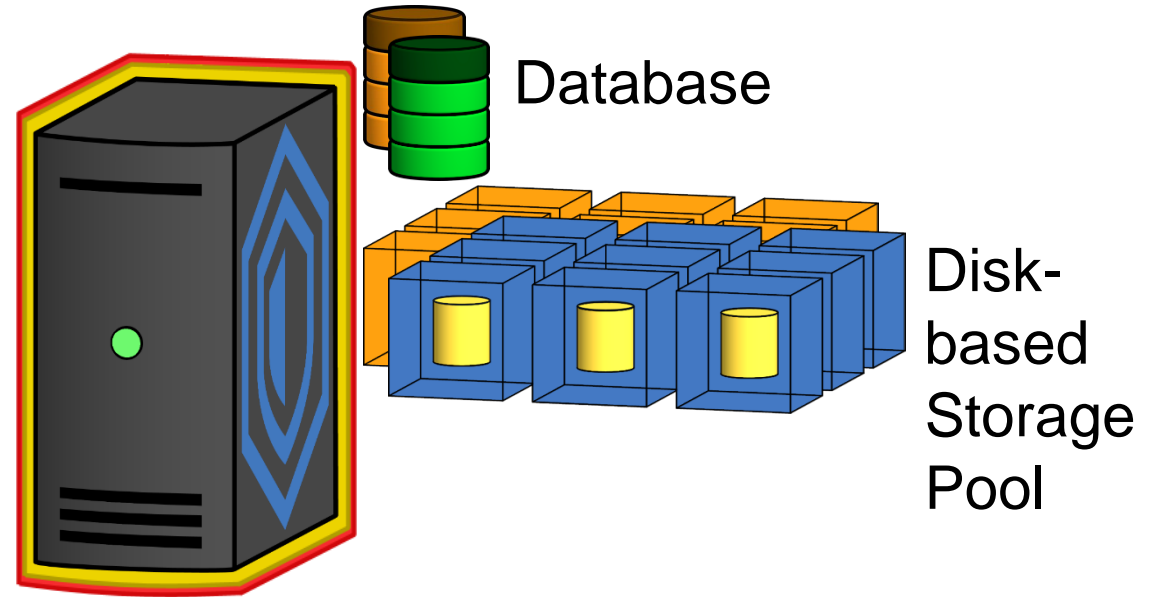
Spectrum Protect for Data Retention is a special-use version of Spectrum Protect. This allows the following features:

- 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.

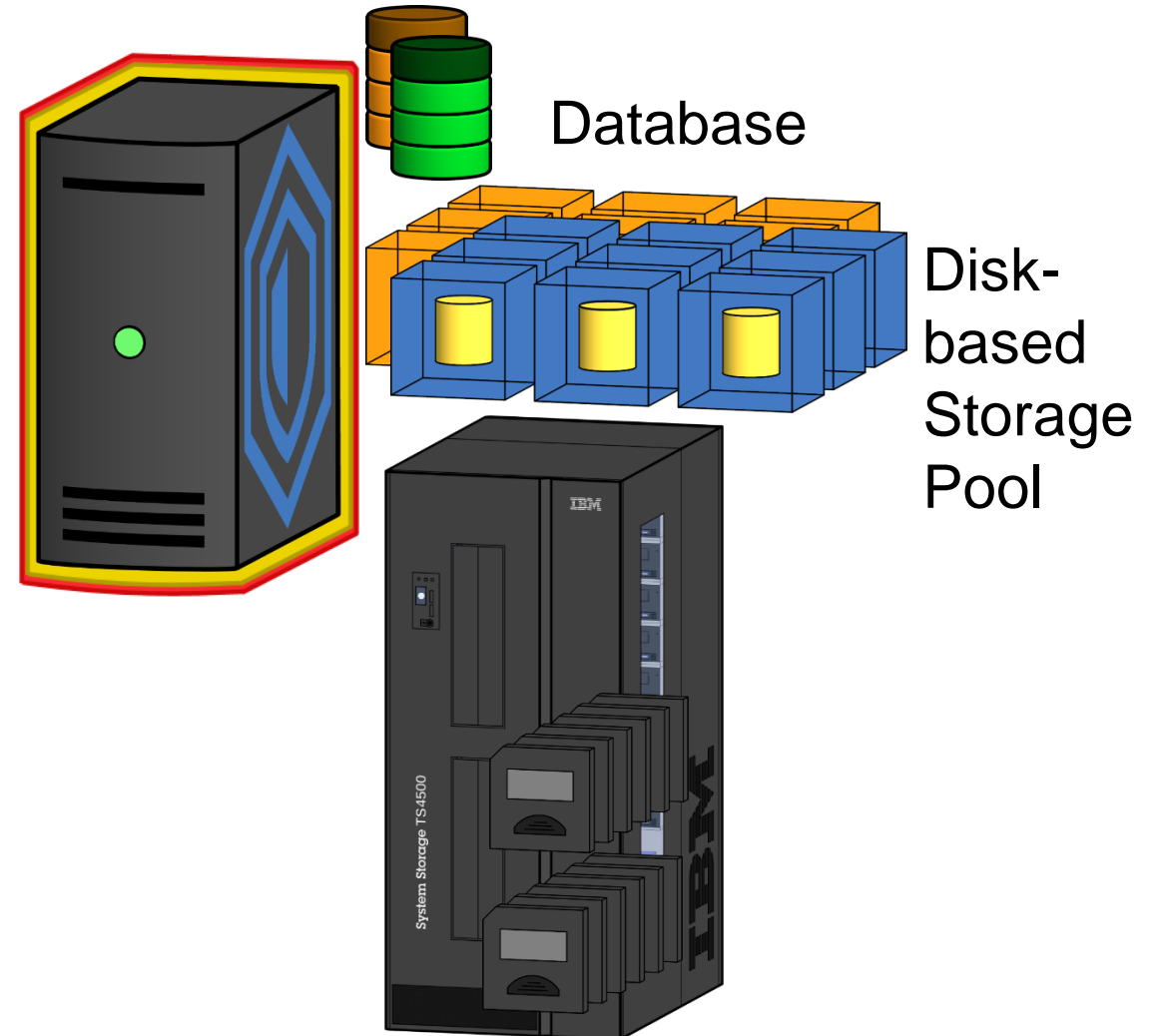
Ease of Corruption or Destruction (Immutability): Node Replication/Protect Stgpool can create a single replica (multiples possible with custom scripting or future features), and the DR target(s) can have different security to help control infiltrator/insider destruction. One can also keep more versions 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.

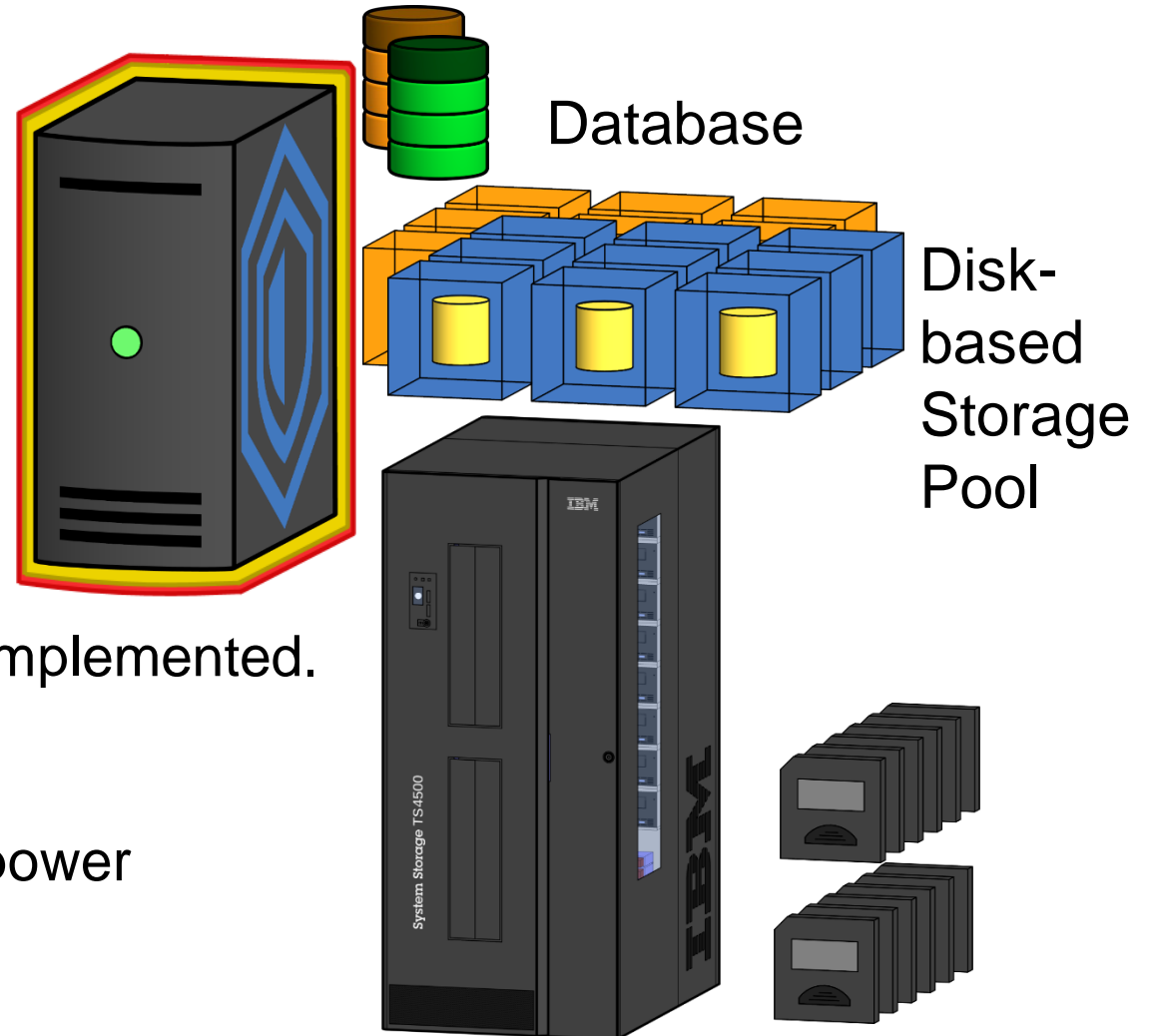
How to add air gapped solutions to a backup hierarchy

- 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.

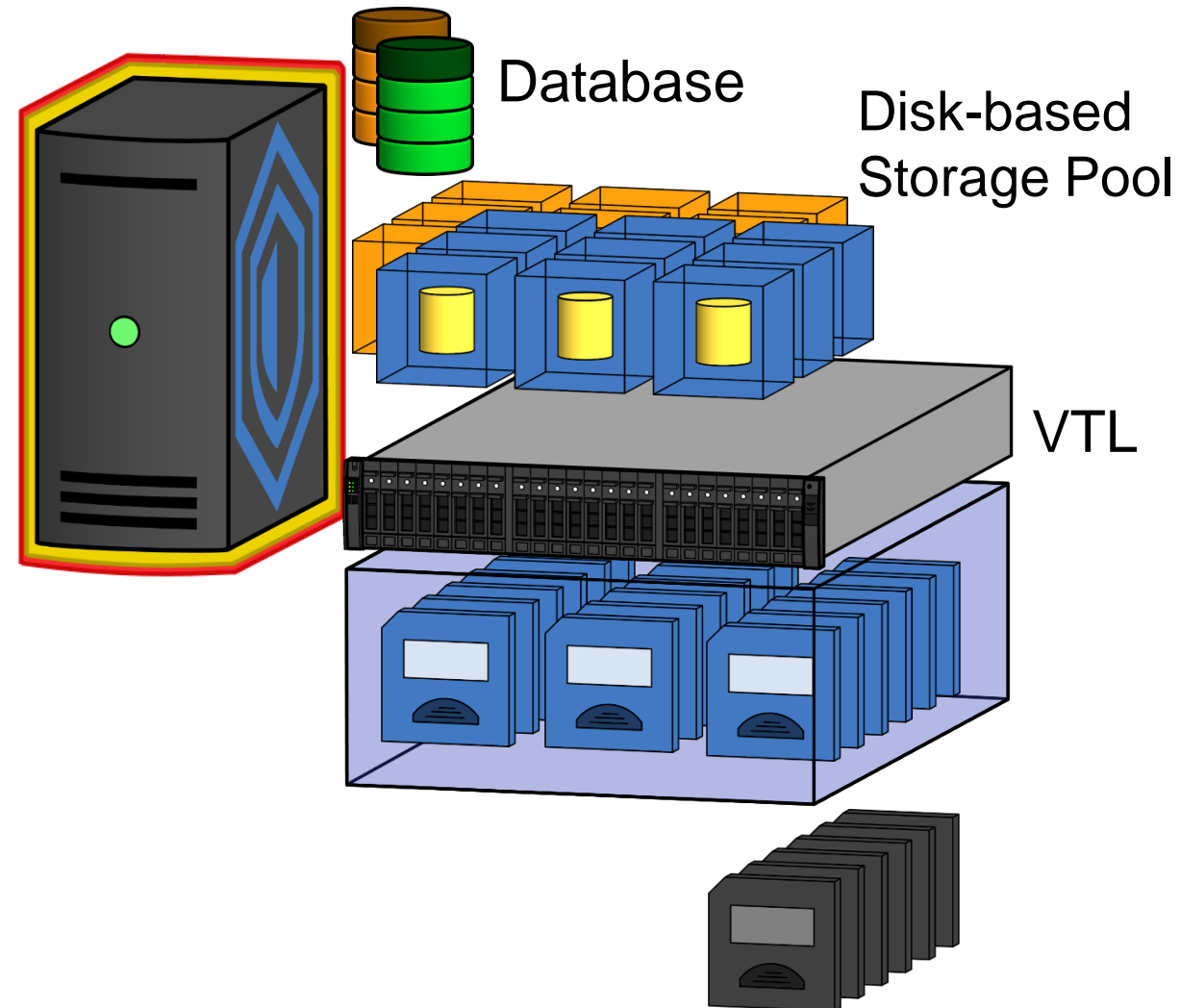
Ease of Corruption or Destruction (Immutability): Tape is inherently harder to corrupt due to its greater isolation. It also offers encryption capabilities as well as WORM media options. Due to the nature of physical tape media, an infiltrator/insider may not be able to logically delete/corrupt the media 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.

How to add air gapped solutions to a backup hierarchy

- A Virtual Tape Library can be added (Ransomware does not currently target serial scsi/fcp device and the underlying disk is not exposed).
- Some VTLs also support moving virtual tape volumes to virtual storage shelves, so malware cannot direct data to those volumes.
- Some VTLs also provide additional cyber-recovery capabilities such as immutability.



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.

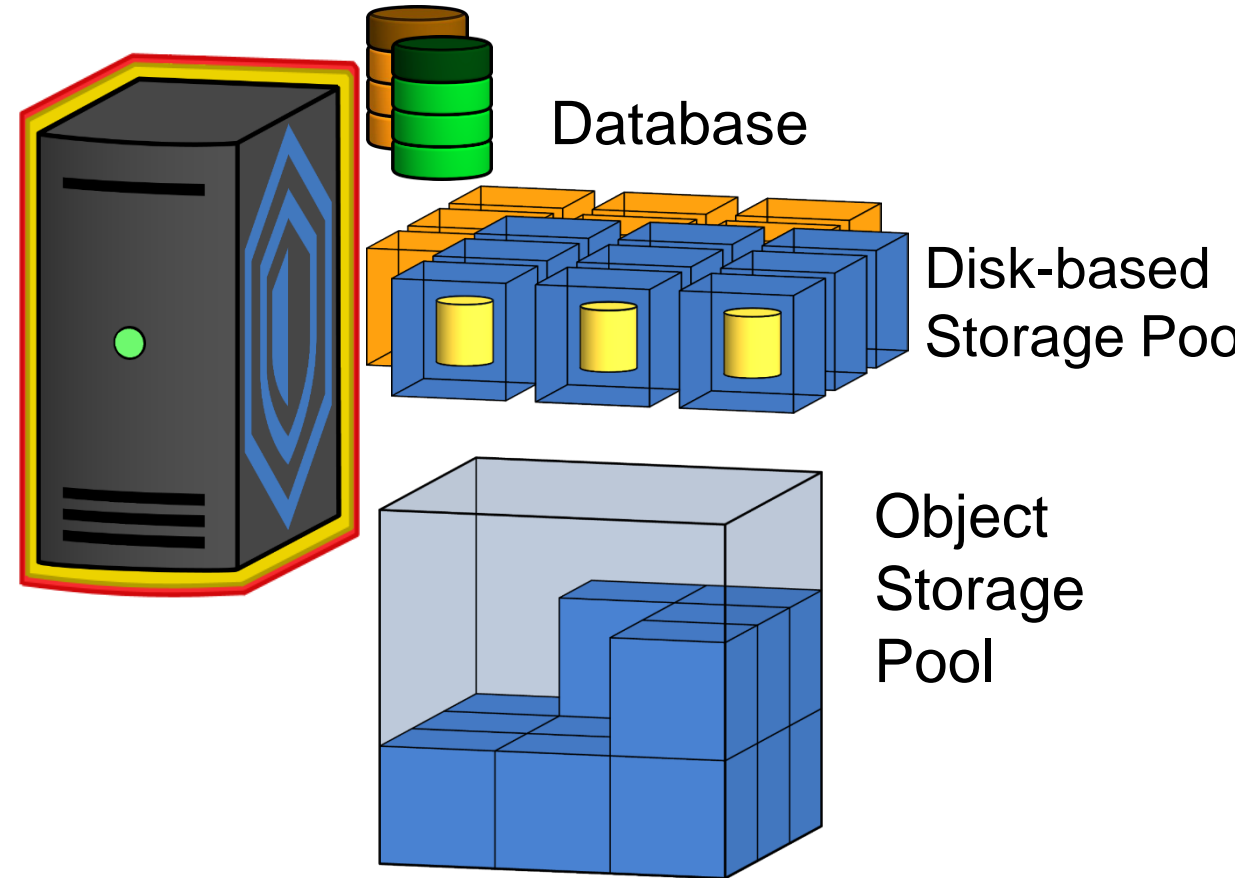
Ease of Corruption or Destruction (Immutability): Virtual Tape is more protected than disk storage pools that reside on file systems but not as protected as physical tape. Support for emulating tape WORM or Encryption will vary, but given the nature of virtual tape it may not be valid. Some VTL vendors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

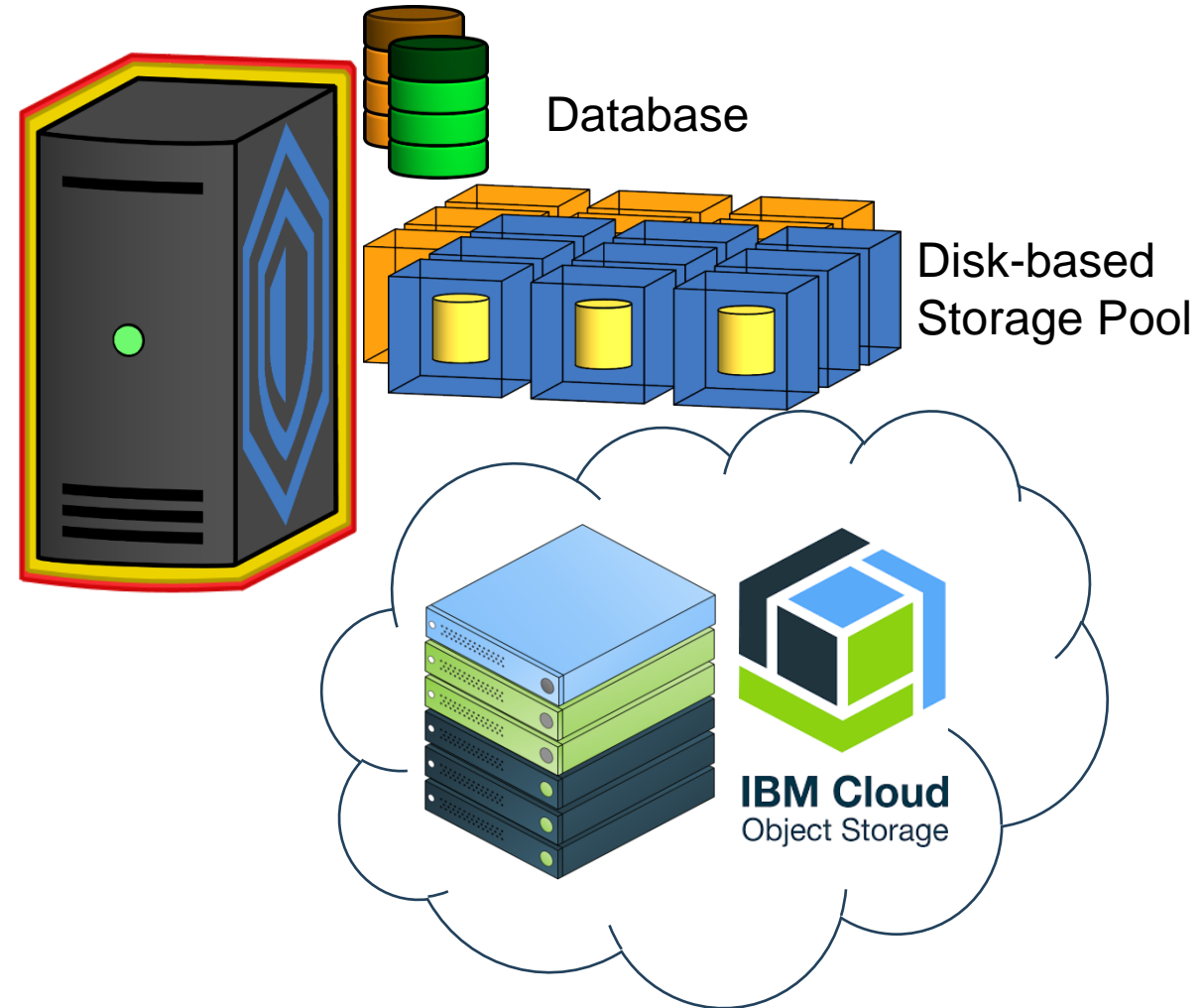
How to add air gapped solutions to a backup hierarchy

- 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.

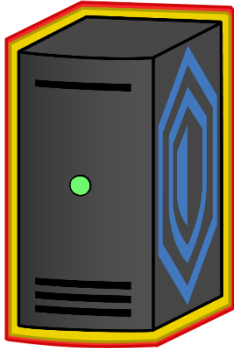
Performance (Speed to meet RTO/RPO in different scenarios): Object storage, especially cloud-based object storage, is not intended to provide the performance of block or file storage. In other words, it is not meant to be used for high-speed operational recovery.

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.

Recommendations Overview

1 Harden the protection of existing backup systems

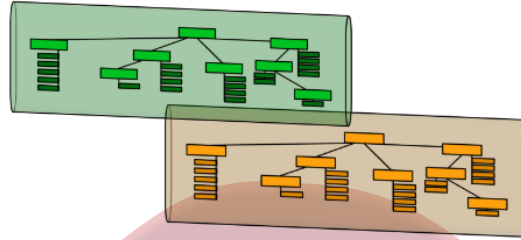
- Having a backup is the prerequisite for recovery.
- Audit capability and ensure success....



- 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.



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

3 Ensure Critical Backups are stored on other non-disk storage

- 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

NIST – Recover

- Develop & Implement Activities to maintain plans for resilience and restore
 - Recovery Planning
 - Improvements
 - Communications
- Key IBM Offerings help:
 - Full environment recovery – Protect
 - Instant application / data recovery – Protect Plus / CDM
 - Utilize data copies – Protect Plus / CDM
 - DR Automation – CDM



IBM
**Spectrum
Protect**



IBM
**Spectrum
CDM**



IBM
**Spectrum
Protect Plus**



Hardening Your Backup Infrastructure



NIST Cyber Resiliency Framework



Protect



Respond

This presentation is about hardening your data protection infrastructure so you can continue to offer recovery services after a cyber attack.

A second presentation discusses use of air-gapped storage, immutable storage and snapshots for enhanced recovery

You will need to account for:

- Automated Ransomware Attacks
- Infiltrator Attacks, can be extended, deep infiltration
- Insider Attacks
- Combination of deep infiltrator and compromised insider.

Top Ten Security/Reliability Topics (and a Bonus Topic)

- Harden the Spectrum Protect server hosts/machines
- Protect Spectrum Protect servers against RansomWare and other Malware
- Secure the communication pathways **(details on 8.1.2+)**
- Secure Spectrum Protect administration
- Secure Spectrum Protect client nodes
- Use all support and alerting tools available to you and apply Flashes
- Follow strong testing and currency policies
- Validate Data Protection and DR Services
- Make the Protect Server infrastructure easier to manage reliably
- Make the Protect Clients easier to manage reliably
- Bonus Topic: Data Spill Recovery (Data Sanitization)

How Many TSM and Spectrum Protect Infrastructures are Operated Today

- Standard Password for Admin account (Admin/Admin123)
- Every administrator uses the same account (Admin)
- Firewall turned off on TSM/Spectrum Protect server, component servers and protected machines.
- Client Node Password the same on all servers (same text or based upon machine name/cluster name)
- Communication sessions are not encrypted
- Very limited test infrastructure (if any)
- Mismatched versions of software
- Flashes not being received, so emergency fixes not applied
- Flood of messages causing important messages being missed
- Chaotic client options due to years of setting them manually in local client options
- Testing of recoveries done solely by actually performing recoveries
- DR Testing stops day-to-day DR protection

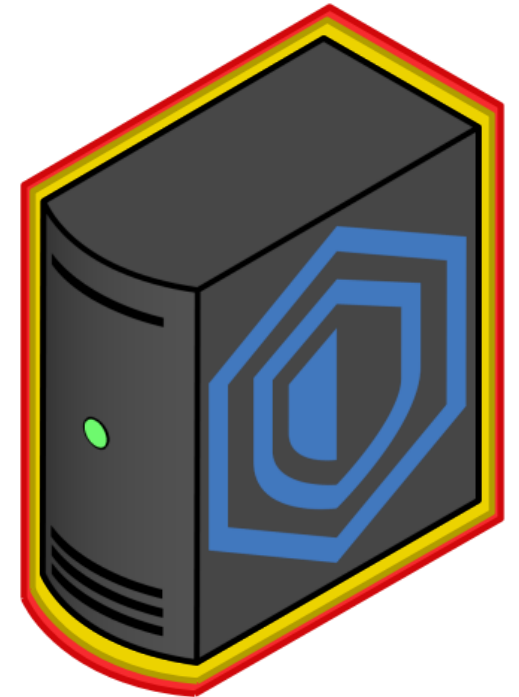
Spectrum Protect Security Model

Please endure a quick Recap of the Spectrum Protect Security Model

- Each Spectrum Protect Client Node has its own password. Will auto-generate upon expiration, if client scheduler is used. If client scheduler is not used, expiration is often deactivated.
- Only that Node can access its own data. No other node can do so, unless explicitly permitted to do so (by Set Access command or Grant Proxynode).
- Spectrum Protect Administrators each authenticate with their own password.
- An administrator has no authority other than read-only (used to be called Analyst authority), unless explicitly granted.
- Rough role-based authority levels exist for admins, and admins can have their scope limited to specific domains, storage pools, nodes, etc.
- Complex password rules for nodes and admins can be enforced by an external LDAP or AD.

1 - Harden the Spectrum Protect server machines

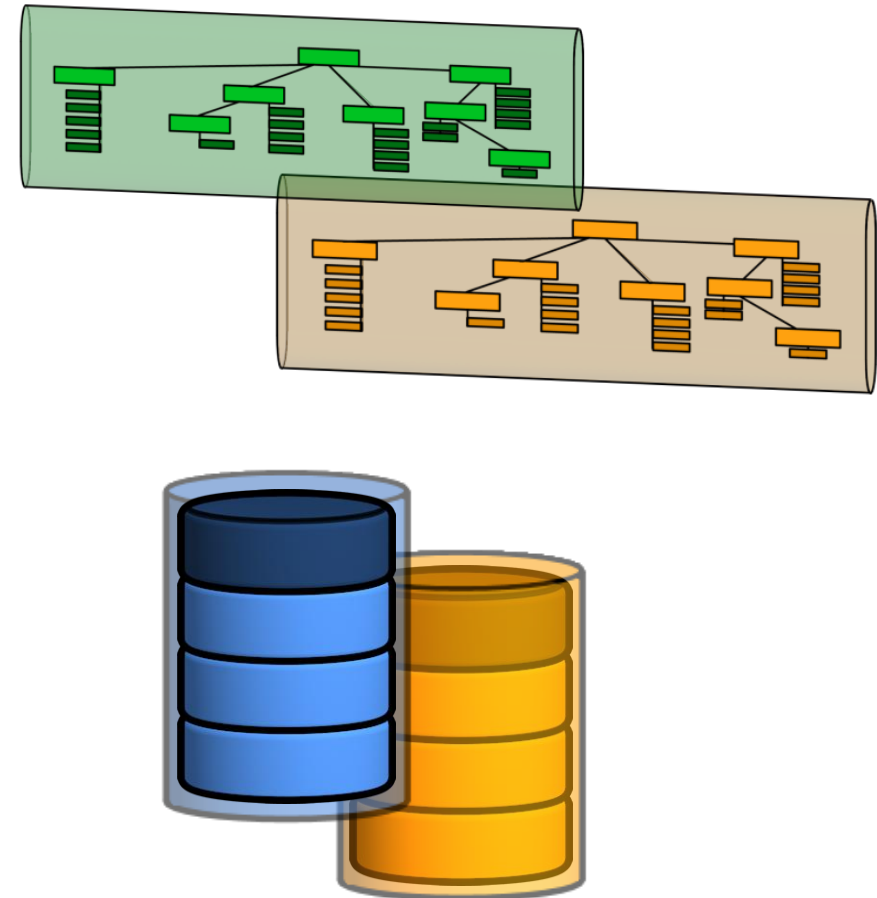
- A networked application, like backups over a network, cannot be completely isolated using an air gap.
- The application machine can be protected using a concept similar to reducing the radar cross-section of a stealth plane.
- Do not expose shares or exports, use strong security settings, etc.
- The server can be further protected by using firewalls to limit what ports are opened, as well as which addresses can access the opened ports, and in which direction.
- 8.1.2 introduced encryption at rest using software native features (directory container pools, this already exists in cloud container pools). Protect also supports self-encrypting disk and tape.
- At OS installation time, you can select advanced security settings (on *nix, keep an eye on nosuid on /home dir).
- SELinux, Trusted Execution, etc. Activate after installation.



2 – Harden Spectrum Protect servers against RansomWare and other Malware

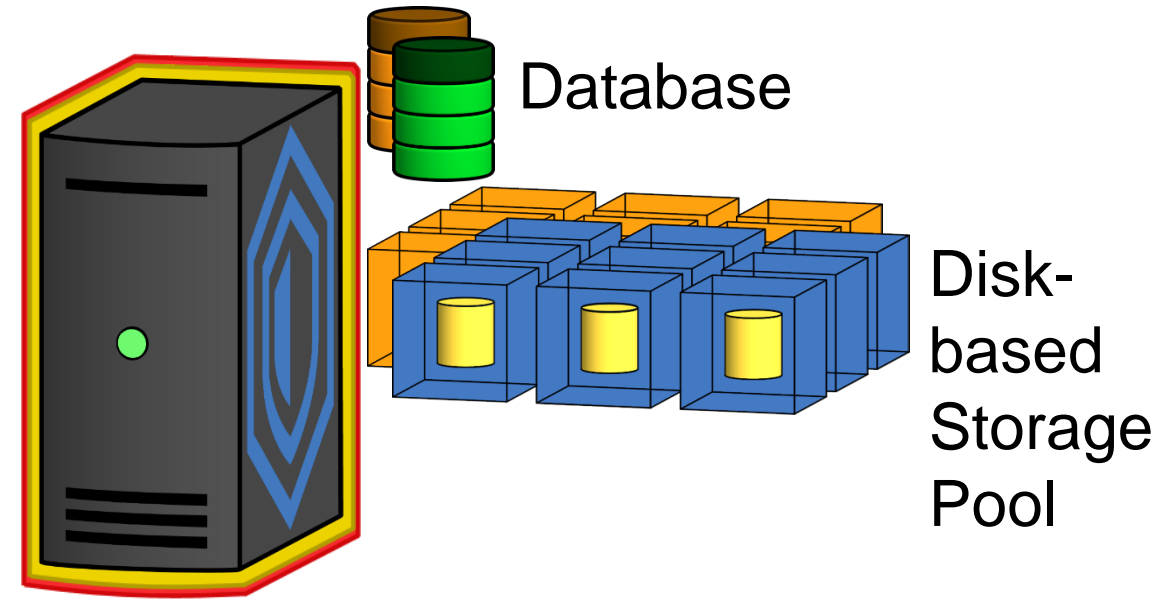
You can protect client data before you begin addressing the protection of the backup engine.

- Ransomware works by targeting a user machine, but it does not damage that machine at first. After it has infected a machine, it attempts to encrypt data on any share that it can locate from that machine. In other words, it is targeting files on a file system, which can be documents, databases, etc.
- After following good security practices and eliminating unneeded shares or exports, there may still need data that needs more protection.
- One good first step is to create read-only snapshots of file systems or, for applications, disk snapshots not exposed to the machine's operating system.



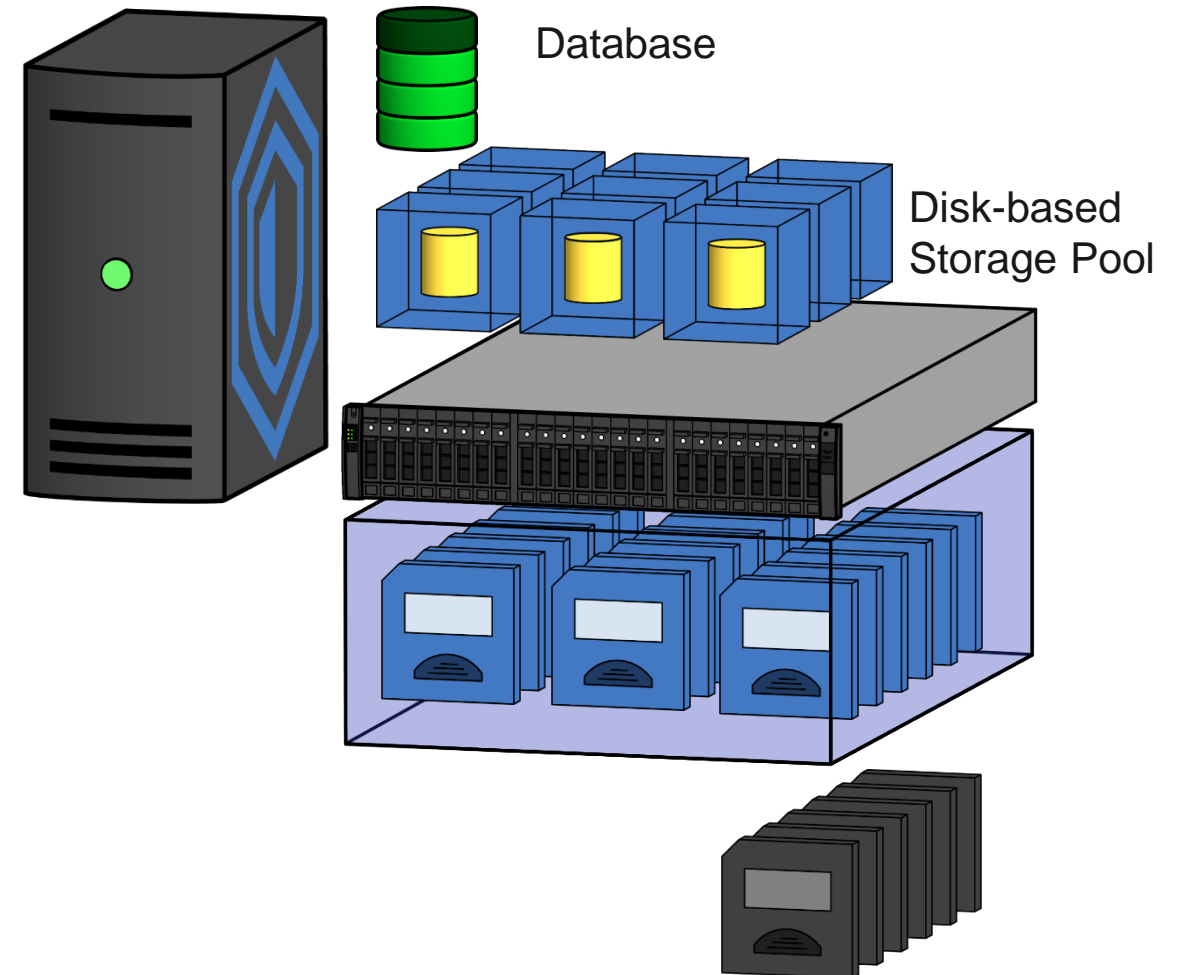
2 – Harden Spectrum Protect servers against RansomWare and other Malware

- Consider same techniques used on protected clients on Spectrum Protect Server.
- A modern backup engine with a disk-only storage pool layout will need to have its profile reduced, as outlined earlier.
- Disk-based components can be protected with storage snapshots.
- Use of reuse delay settings discussed in a few slides.



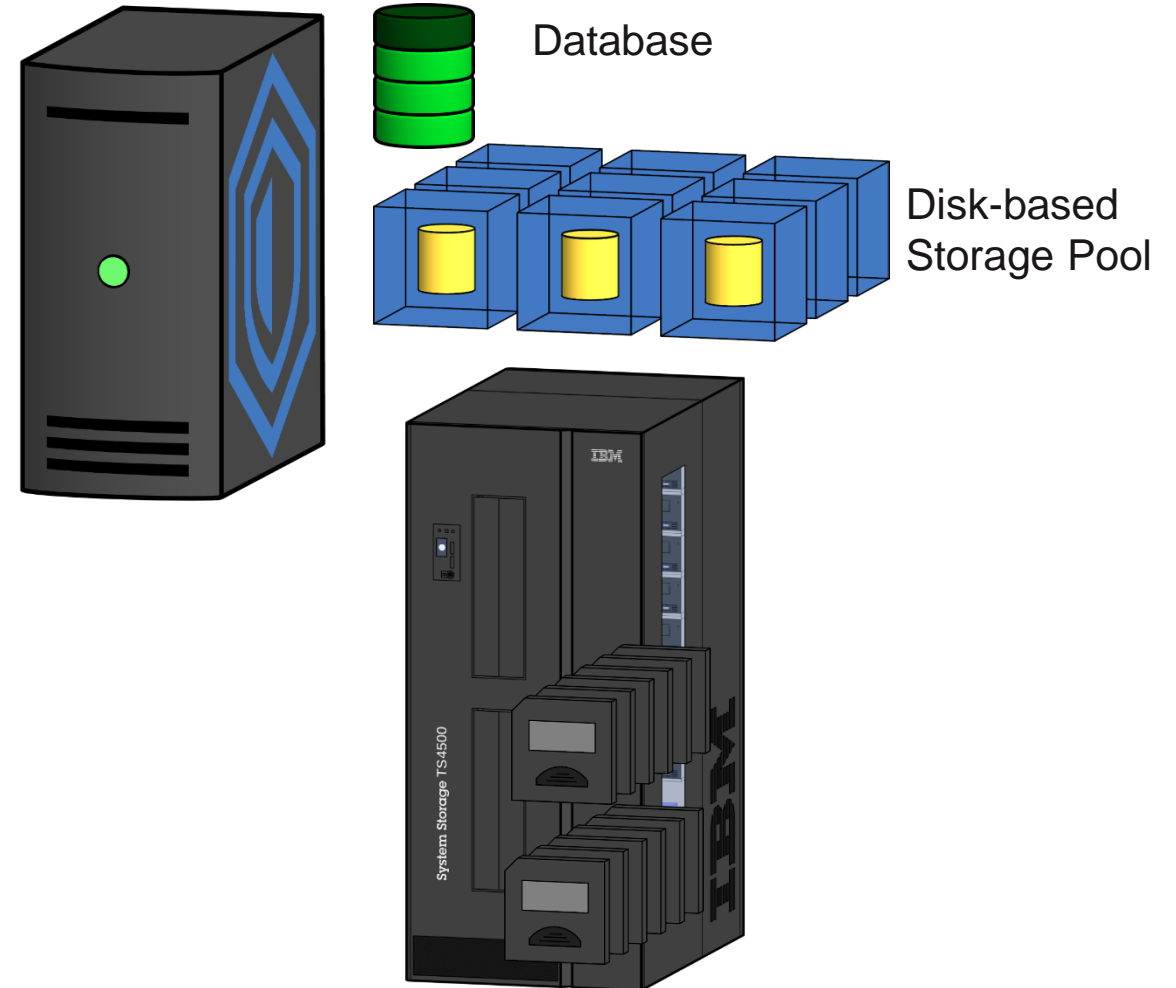
2 – Harden Spectrum Protect servers against RansomWare and other Malware

- A Virtual Tape Library can be added (Ransomware does not currently target serial scsi/fcp device and the underlying disk is not exposed).
- Some VTLs also support moving virtual tape volumes to virtual storage shelves, so malware cannot direct data to those volumes.



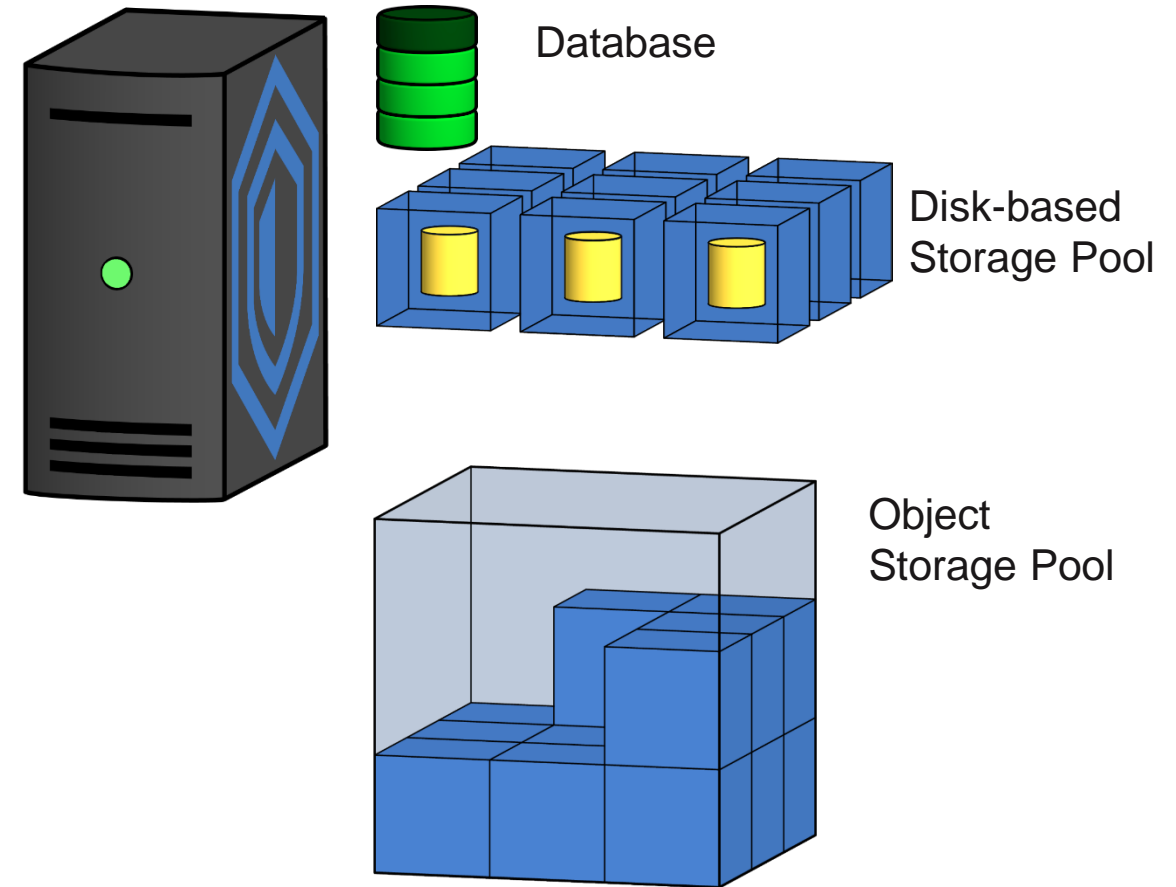
2 – Harden Spectrum Protect servers against RansomWare and other Malware

- 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.



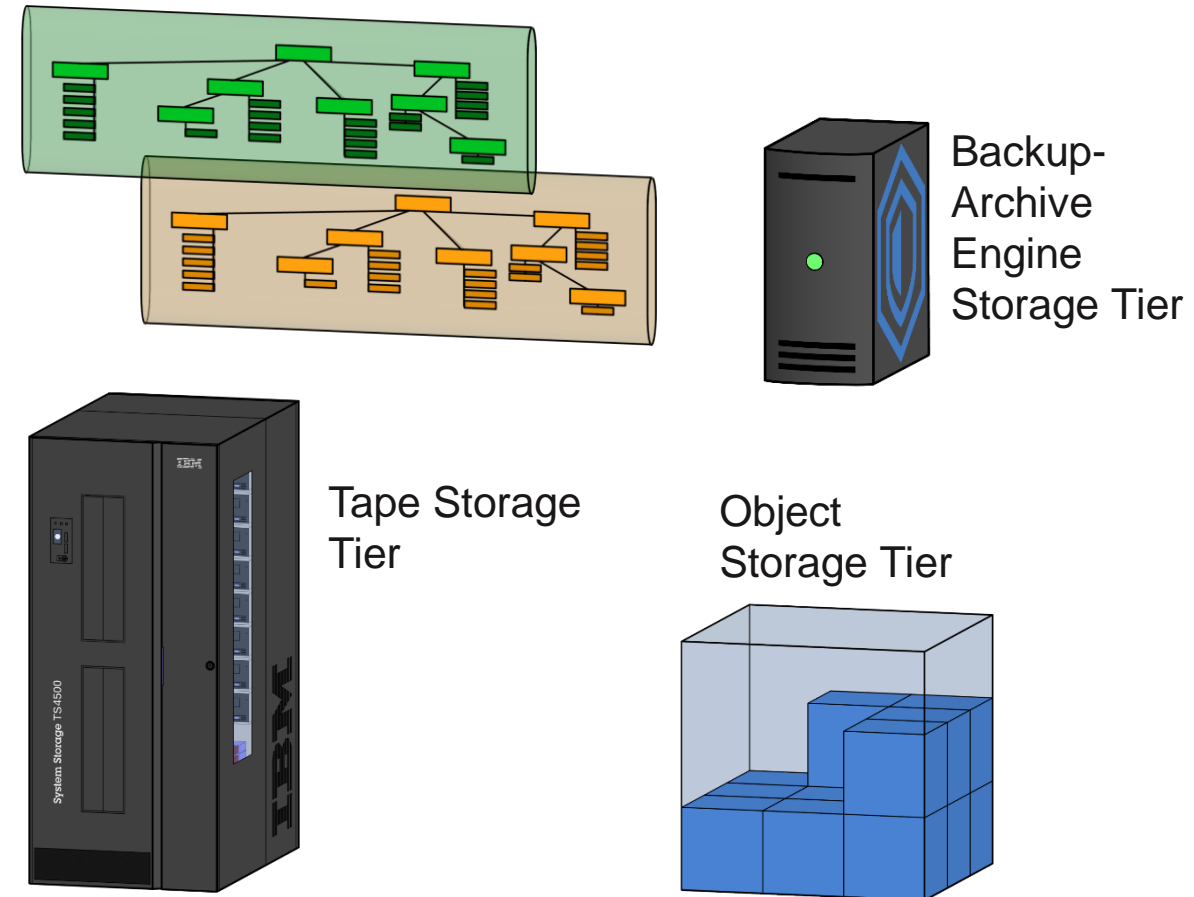
2 – Harden Spectrum Protect servers against RansomWare and other Malware

- 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.
- Some object storage technologies are adding features for greater no-erasable, no-rewriteable protection.



2 – Harden Spectrum Protect servers against RansomWare and other Malware

- Advanced file systems will also support protective snapshots, which can be used if containing a storage pool.
- More than a single storage pool type can be used in different ways (local protect stgpool, node replication target pools, etc.).



What else can you do?


- Monitor and report upon changes in volume, dedup and compression efficiency (8.1.5+ security alerts)
- Use reuse delay to allow environment to be reverted back to previous state. This is not granular, the entire backup engine will be reverted to a previous DB backup, and reuse delay ensures space maintenance has not caused data to be expired, which would render the DB backup partially obsolete. If a node replica target has been written to, it may be corrupted and need to be reverted as well. If the replication target is not corrupted, it can be used to bring the reverted primary up to date.

Remember, your backup infrastructure should not be the first line of defense of protecting clients from cyber attacks, so alerts and activity monitoring report upon corrupted clients, it does not prevent corruption.

Spectrum Protect 8.1.5 Security Notifications Panel

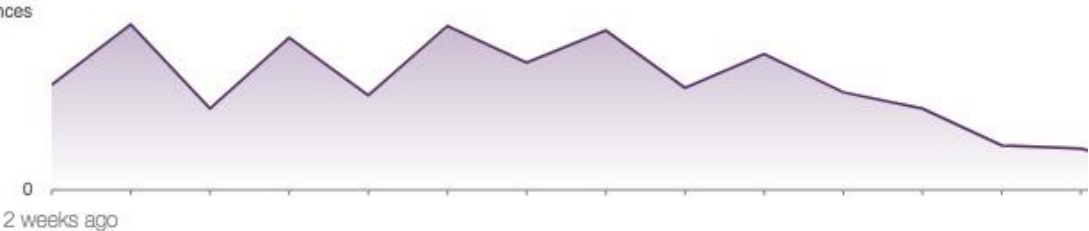
i
Overviews
Clients
Services
Servers
Storage
Reports
Updates

Security Notifications 113



84 Unacknowledged notifications
29 Acknowledged notifications
39 Notifications in the last 24 hours

120 Occurrences



0
2 weeks ago

+ Acknowledge - Reset + Assign

Acknowledged	Type	Name	Assigned	Timestamp	Symptom	Occurrences	Server
		DEMO3		Feb 26, 2018, 3:19:39 PM		2	FUSION
		DEMO2		Feb 26, 2018, 3:15:15 PM		1	FUSION
		DEMO		Feb 26, 2018, 3:08:16 PM		2	FUSION
		CLN10_40		Feb 26, 2018, 6:02:29 AM		1	TAPSRV10
		CLN10_16		Feb 26, 2018, 5:35:41 AM		3	TAPSRV10
		CLN10_39		Feb 26, 2018, 4:14:51 AM		1	TAPSRV10
		CLN10_24		Feb 26, 2018, 3:09:56 AM		2	TAPSRV10
		CLN10_38		Feb 26, 2018, 2:14:32 AM		1	TAPSRV10
		CLN11_24		Feb 26, 2018, 2:05:47 AM		2	TAPSRV10
		CLN10_13		Feb 26, 2018, 12:02:59 AM		2	TAPSRV10

3 - Secure the communication pathways

- Exploit Spectrum Protect's SSL support for data and control pathways. Spectrum Protect SSL support can:
 - Use Spectrum Protect self-generated keys or import keys from an internal or external CA.
 - You can lock out non-SSL communication.
 - You can use current SSL (TLS 1.2).
 - You can lock out older SSL (from back-level clients).
 - You can enforce FIPS compliance.
- Exploit Firewalls on both server and client.
- Spectrum Protect can separate backup and administrative ports, to eliminate the possibility of non-administrative machines logging into Spectrum Protect and attempting to penetrate administrative functions (with use of necessary firewall port blocking). Note: You may wish to exploit administrative access when doing an automated client install, and this will limit that capability.
- If you have a DMZ, isolate the Spectrum Protect server from other parts of the Protect infrastructure.
- If you have clients outside the DMZ that cannot initiate a session into the Spectrum Protect server, you can allow Spectrum Protect to initiate from the server side.

Spectrum Protect V8.1.2, 7.1.8

What was Changed?

- Product wide adoption and exploitation of TLS to secure point to point communication
- Changes to how local “credentials” are stored and managed

Why?

- Skills and tools to “craft” successful attacks improve year to year as a byproduct of:
 - Increased compute power being available
 - Sharing of tools and exploits (dark web, ...)
 - Improved skill and “access” by people that want to “attack”
- Attacks from many vectors
 - Computational: Bots, worms, etc...
 - People, internal threats from disgruntled/disillusioned...

Spectrum Protect V8.1.2, 7.1.8

How?

- Spectrum Protect will rely on Global Security Kit (GSKit) (where appropriate)
 - Where GSKIT does not support/cover a platform, Openssl is used...
 - Java uses native libraries, other examples of “code” using other tools for TLS and cryptographic support...
- Already being used for encryption (AES128, AES256) and hashes (SHA-1, ...)
- GSKit is “best of breed”...
 - Other SW companies have approached IBM and requested to “license” or OEM GSKIT
 - Has not been done as GSKIT is viewed as a competitive advantage with the skill and effort IBM has invested in it

4 - Secure Spectrum Protect administration

- Do not share administrative accounts, give every administrator their own account (also allows alerts to be assigned to specific personnel for resolution).
- Do not give administrative account more access than they need for daily work.
- If necessary have individual or group accounts with higher level of access and very short password expiration.
- If ongoing automation needs admin account, create dedicated account for each purpose.
- Store automation administrative passwords in secure location and obfuscate password (don't put in the clear in a script).
- Store scripts in secure location (they will have commands to un-obfuscate the password).
- If one-time setup scripts need administrative account, delete, lock or change password after initial run.
- Audit and report upon administrative activity. Validate that the special accounts only issue commands associated with their functions. Validate the system-level accounts only issue specific commands your policies limit them to. Check for invalid password counts, etc.
- Exploit LDAP or AD integration to enforce complex password rules.
- Secure Object storage credentials.
- Decommission accounts as employees move jobs or leave company.

5 - Secure Spectrum Protect client nodes

- Do not use simple, well known passwords.
- Create a complex random password and store locally.
- Limit who can read the random password file or registry key.
- Audit for password exceptions.
- Encourage Protect file-level restores or ad hoc backups be done with Web client and administrative password. Old web client disabled in 7.1.8 and 8.1.2. New web client 2.0 introduced in v8.1.7.
- Use client-side auditing (Audit Logging).
- Use server-side client auditing (ReportRetrieve):
ANR041 11 Session 8 for administrator COLIND-TUC logged in as node COLIND-TUC restored or retrieved Backup object: node COLIND-TUC, filespace \\colind-tuc\c\$, object\CODE\TESTDATA\ XXX.OUT
- Use Client Management Service to show logs for clients within the Operations Center.
- Stay on top of misc. warning and error messages (excluding files that cannot be backed up, etc.).

6- Use all support and alerting tools available to you and apply critical fixes

- Sign up with IBM to receive Spectrum Protect Flash e-mails.
- Install critical Spectrum Protect fixes as quickly as possible, within your change control rules (more on those later).
- Validate your organization receives OS and hardware flashes as well, and installs critical fixes within change control rules.
- Adopt Spectrum Protect Operations Center alerting model to assign and close issues (documenting them according to your organizations problem management rules).
- You will need to manage your client-side and server-side messages to avoid hiding real problems in alert storms.
- Proactively open support tickets even for minor issues to keep the problems under control.

7 - Follow strong testing and currency policies

- Have documented currency rules. For example, run software no more than 18 months past GA, but no earlier than 6 months after GA. Highly critical fixes will have their own emergency rules.
- Have corresponding testing rules. For example, run new code in a small isolated environment within a month of GA, for 2 months. If all tests are passed, run in larger environment with actual testing workloads of different client types. Then move to Dev/QA environment and finally production environment.
- Have reasonable testing criteria, for pure “It does not blow up my machine” testing, functional testing, integration testing with protected clients, validating policies, procedures and installation scripts do not have to be modified.
- This is made greatly more cost effective if customers share testing procedures and results with one another.
- Testing and software currency management is just part of standard ITIL processes. Others include:
 - Enterprise workload management (scheduling backups and maintenance with enterprise scheduler).
 - Software distribution (using software distribution tools and automated installation packages)
 - Problem Management with feedback loop into Change Control
 - Others.

8 - Validate Data Protection and DR Services

- Monitor the performance of backup streams to project the estimated performance of restores
- Plan out implications of multi-stream backup to different stgpools/copygroups if you want multi-session restores.
- Test restores of different client scenarios periodically (ideally as part of testing policies). Note: there are third party products from Cristie and TSMWorks for this purpose.
- Define different classes of service and monitor appropriately.
- Most organizations have DR testing procedures. Plan whether you wish to stop DR replication during that test (Spectrum Protect Node Replication can continue operation in parallel with DR testing).
- Monitor ingest workload and managed data of Spectrum Protect servers to validate they are within specs for a given instance design.

9 - Make the Protect Server infrastructure easier to manage reliably

- Standardize on a platform and configuration for a given workload (cookie-cutter methodology). Spectrum Protect Blueprints greatly assist with this effort.
- Standardize on naming conventions for admins, nodes, domains, devclass, stgpools, etc. Take into account different servers may have the same policy names with different rules, so you can include retention/version in names. The Blueprints have examples of these.
- For managed objects that you want to be identical across servers, use Spectrum Protect Enterprise Management (put objects in managed profiles on one server, subscribe to that profile on the other servers).
- Monitor the workload for given Protect instance (ingest, back end) and validate against intended capability of design.
- Leave a spare amount of workload capabilities to account for ad hoc spikes and adding client workloads with time to burn in.
- Decouple OC and Hub server versions from backup engine versions

10 - Make the Protect Clients easier to manage reliably

- Use currency rules to have limited number of versions to manage.
- Use server-side client options sets (Clopts) to store configuration settings in sets on the server and have client nodes subscribe.
- Allow Clopts to override client-side settings for key parameters, to eliminate unreliable chaos of different client-side options files parameters across the enterprise.
- Exploit the Client Management Service.
- Register the client-side instrumentation trace (performance tracing, on by default starting in 7.1.6, but can be run in earlier versions) with the Client Management Service.
- Use auto-configuring installation packages to maintain consistency, avoid human error and greatly speed up the process of installing and upgrading software.

Bonus Topic: Data Spill Recovery (Data Sanitization)

A Data Spill occurs when secret or confidential data is stored on a protected client in violation of policy, but then is backed up before the violation is found.

- If it is not considered secret data that has to be sanitized, you can simply delete the backup or archive object from Spectrum Protect using the appropriate client software and then running Expiration (specifying the node name).
- If needing to sanitize the data, before the data is deleted using the client software, find its volume by querying the Contents pool (if using a volume-based storage pool) or the container tables if using a new Container pools.
- Set the reusedelay on the target storage pool (to prevent volume from being deleted or reused or the container from being deleted).
- After data is deleted and expiration is run, issue Move Container or Move Volume to move the good data out of the container or volume.
- After volume and container is emptied, destroy it. If a file on a file system, you can issue the OS Shred or SDelete commands. If a tape, physically de-gause and/or destroy.
- Note: NIST Publication 800-88 discusses both Shredding (multiple overwrite passes) and Cryptographic Erase as valid data sanitization techniques.
- Encryption features added in 8.1.5 for Directory Container Pools (already existing in Cloud Container Pools), which means if data is deleted, expiration run and then the container emptied, the data will be cryptographically erased.



Real World Experiences



Real World Experiences

- Recovery is a Long Process (one month or even multi-month process).
- One challenge is a reluctance to hit the alert button and start taking action, even with compelling information that an attack is underway.
- Windows is the main target (damaged backup engines are predominantly on Windows).
- Active Directory is targeted and used as a vector to spread infection, then corrupted (which is propagated).
- Backup engines are targets.
- The design of the recovery process is paramount.

Recovery Steps – Part 1

- Figure out what has happened (or is currently happening)
 - Malware may have multiple vectors/actors
 - Do not assume a single attack. Compromised infrastructure (immune system) may have opened to other infections/attacks, accidentally or by intent.
 - Do not assume automated attacks stopped at datacenter boundaries, if there is a network connection, there is a potential vector
- Plan recovery
 - Prioritize data to be recovered.
 - clean-room procedure? Who authorizes moving from clean room to production? What is the process to restore, validate, promote, confirm?
 - What about infrastructure? AD, Network, switch configs, etc.
 - What components are part of key applications (db servers, app servers, ancillary servers, AD, DNS, etc.)
 - Where are you recovering (where is clean room, where is production)?
 - Is it necessary to back up data between cleaning/validating and promoting? To where?

Recovery Steps – Part 2

— Pre-recovery steps:

- Do you need to fix your backup infrastructure?
- Do you need to bring in offsite media?
- Do you need to stage data from slower storage to faster storage to facilitate restore?
- Can you add resources to backup infrastructure to make it faster?

— Perform recovery

- Do you need to maintain backups during the process?
- Do you need to re-introduce backups as clients are returned to service?

Specific Lessons Learned

- No such a thing as an app that does not need backups - backup AD
- Inventory management is critical
 - Application components and relationships
- Pre-incident recovery planning can be very valuable (including end-to-end scenarios mass recovery).
- Pre-incident acquisition of recovery tooling - for all steps. Automation, testing, orchestration.
- Assembly line processing model for recovery is ideal
- Have clean room environment available, or able to be deployed quickly. Pre-designed.
- Advanced logging infrastructure is key to detecting what was attacked and when.
 - QRadar, splunk, other
- Currently 3 big areas of defense/detection
 - - perimeter defense
 - - signature scanning
 - - anomaly detection

Specific Lessons Learned

- Should feed detected anomaly information back into logging/security tools.
- MS Windows is a main target:
 - Decide if it is an option for backup engine. Even if a standard, consider an alternative, if only to avoid a mono-culture.
 - Is a non-Windows backup an option (traditional *nix DNS as backup for Windows, etc.)
- Backup infrastructure design:
 - Design backups with air gap, immutability, encryption, etc. in mind
 - Isolate resources to cover different failure scenarios (don't put backup engine DB on same controller as production data it protects)
 - Follow other hardening practices
- Customers have resistance to acting to call a disaster/pulling the switch. Ideally, set up procedure and criteria first so it is not a debate (or debate is reduced).
- AD recovery is complex, don't wait until the incident to begin building your WinPE environment. Make certain AD restore scenario is documented (and tested)

Specific Lessons Learned

- Expect a post-incident recovery to have stricter security settings, at least during recovery:
 - From trusted to zero-trust
 - May need to support some initial detection of whodunnit before you can start recovering.
- Set up tiger/incident response teams pre-incident, including contact and responsibility information. Include backup personnel.
- A business has a large number of teams that need to be involved after a Cyber Incident, many of which have little to do with recovery
 - CEO/CIO/CTO/CISO
 - Legal
 - Marketing/communication
- Consider more active DR testing, actual simulated Cyber attacks and recoveries.
- During the recovery, we may need to be responsible for sending the malware signatures to IBM research, anti-virus companies, regulatory boards, etc.
- A good CCMDB and backups of system configs (switches, SAN components, etc.) is ideal.

Useful links for DR Automation

- **IBM Cloud Resiliency Orchestration**

<https://ibm.biz/Bd2dDu>

- **Cyber Resiliency Lifecycle**

<https://ibm.biz/Bd2dD9>

- **Cyber Incident Recovery**

<https://ibm.biz/Bd2dDQ>

- **Cyber Incident Recovery Demo**

<https://ibm.biz/Bd2dD3>

Accelerate with IBM Storage Survey

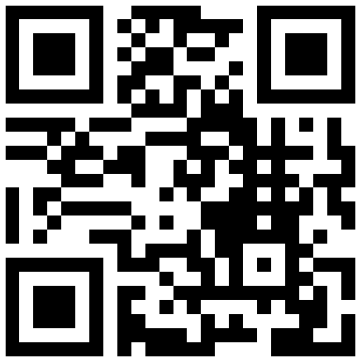
Please take a moment to share your feedback with our team!

You can access this 5 question survey via [Menti.com](https://www.menti.com) with code 22 37 47 or

Direct link <https://www.menti.com/mkg7a2x6q8>

Or

QR Code



Notices and disclaimers

- © 2019 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights – use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml