Accelerate with IBM Storage: Spectrum Storage, Ransomware and regulations mandating WORM storage

Dan Thompson
Spectrum Storage Specialist
danthomp@us.ibm.com
About this session

This session will discuss how Spectrum software defined storage can help protect you against Ransomware and meet regulations that require non-erasable or non-rewriteable storage.

Topics include
• What is Ransomware and what are its stages of progression?
• How Snapshots can provide a first line of recoverability.
• How networked applications, like a network data-protection solution can be protected.
• How to build air gapped backup solutions using different technologies.
• What is the SEC17a regulation and what does it require?
• How Spectrum software defined storage can help you adhere to SEC17a and similar regulations.

• What this session is NOT about:
• This is not a discussion of the security technology used to prevent and combat Ransomware directly, such as IBM Security Operations and Response.
IBM Spectrum Storage - Changing Nature of Business and Data

Business Pressures

New Applications

Data Growth

Hybrid Cloud

Free data from constraints of hardware and realign with new business processes and applications
IBM Spectrum Storage – Software Defined Storage

Securely ‘unboxing’ storage to revolutionize data economics

Family of Storage Management and Optimization Software

- **IBM Spectrum Control**: Analytics-driven data management to reduce costs by up to 50 percent
- **IBM Spectrum Protect**: Optimized data protection to reduce backup costs by up to 53 percent
- **IBM Spectrum Archive**: Fast data retention that reduces TCO for active archive data by up to 90%
- **IBM Spectrum Virtualize**: Virtualization of mixed environments stores up to 5x more data
- **IBM Spectrum Accelerate**: Enterprise storage for cloud deployed in minutes instead of months
- **IBM Spectrum Scale**: High-performance, highly scalable storage for unstructured data

Software Defined Storage

✓ Runs on commodity hardware
✓ Full suite of storage services
✓ Embraces multiple storage options

Any Storage

FlashSystem

Private, Public or Hybrid Cloud
IT Modernization through “In Place” Copy Data Management

IBM Spectrum CDM

Software-Only Platform

Catalog
• Discover
• Search

Automate
• SLA compliance
• Policy-based

Transform
• Cloud integrated
• DevOps enabled

Use Cases

LEVERAGE

Disaster Recovery

DevOps, Test/Dev

Automated Copy Management by SLA

Hybrid Cloud
Stages of Ransomware

IBM Definition: “As its name implies, ransomware is nefarious malware that holds your data hostage, demanding payment to release it. It takes advantage of leaked exploits, using strong encryption and a modular architecture.”

5 Stages of a Ransomware attack, as defined by the IBM Security Operations and Response team:

- **Break-In stage**
  Employee clicks malicious URL in email and triggers ransomware install

- **Latch-On stage**
  Ransomware probes network seeking vulnerable machines

- **Expand (encrypt) stage**
  Critical servers infected and encrypted with ransomware

- **Shutdown stage**
  Organization is paralyzed, forced to shutdown and pay ransom (the longer you wait, the more expensive it gets).

- **Restore (decrypt) stage**
  Criminals provide decryption keys; decryption can take days. In some documented cases, they fail to provide the keys.
What Does Ransomware mean to storage administrators

• The first and foremost weapons against malware are a sophisticated security infrastructure and user education. Storage can help in the recovery phases and, potentially, in helping identify the Encryption phase has been reached.

• From a recovery perspective, a Ransomware or any Malware infection is treated as a massive data file corruption and, potentially, a large-scale operating system recovery. Ideally, the latter will not be required, if sufficient alternatives have been implemented.

• Many large organizations have begun Ransomware strategy teams, who report to the upper echelons of management, who may then report to a Board of Directors or shareholders. In many cases, the IT teams are just being asked to research what can be done to combat Ransomware with current infrastructure, identify any potential shortcomings and create a plan to address them.
Preventing the Latch-On and Expand Stages

A networked application, like backups over a network, cannot be completely isolated using a true air gap, otherwise they will not be able to provide their needed services. The following steps assume a workstation is infected and trying to spread the Malware.

• The Latch-On stage can be avoided using a concept similar to reducing the radar cross-section of a stealth airplane.
  • For example, do not expose shares or exports, do not advertise a machine’s services unless necessary.
• The Expand Stage can be prevented by protecting the machines themselves.
  • Strong security settings (no insecure or unneeded services; no ssh root access; **stay current on machine, OS and application fixes**, etc.
  • Use firewalls to limit what ports are opened, and limit which addresses can access the opened ports and in which direction.
  • SSL encryption on application sessions; such as backup/archive and command and control sessions for a backup engine.
Note on securing Spectrum Protect as if it were an application

Spectrum Protect, like any other application, can be protected and secured. Since it is critical to recovery of corrupted files, it is extremely important that it be protected effectively.

• Spectrum Protect has disk components, so it can be corrupted.
• Do not expose shares, do not use the machine for any function that requires creating shares/exports or exposing the machine in any way.
• Use firewalls and only expose backup and administrative ports. Separate administrative ports.
• Windows is the primary OS target. Temporarily, *nix may offer benefits due to it not being targeted.
• If using Linux, enable SELinux after install.
• Spectrum Protect supports SSL on data protection, administration and control and command (C&C) functions. SSL can be configured to different levels of security, including FIPs compliance.

See “Top 10 Ways of Securing Data Protection” for more information.
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 sufficient numbers of snapshots to give you time to detect and stop the Expand (encryption) stage.
Protecting Spectrum Scale

Spectrum Scale has unique functions to provide recovery from massive file corruption.

• Spectrum Scale Snapshots

• Integration into Spectrum Protect backups via MMBackup. This includes massively parallel backup of Petascale environments. Backups can target disk or non-disk storage pools.

• Integration into external storage pools such as Spectrum Protect, Spectrum Archive and IBM Cloud Object Storage. HSM/ILM functions include pre-migration (but not purged/deleted) each day, similar to a backup, rather than wait until data age policies trigger a migration.

• Sophisticated DR replication options allow site-level protection.

• Petascale backup support allows file system recreation. Details on DeveloperWorks: Petascale Data Protection
Near-Universal Snapshot (Copy Services)

- When asked to design a perfect “end-to-end” data protection and DR solution, I often include Spectrum Virtualize as a way to provide “universal snapshot” capabilities (keeping in mind nothing in this space is truly universal).

- Common copy services regardless of underlying disk infrastructure.

- Too many advanced features to discuss in this presentation:
  - Largest install base, most mature yet modern solution.
  - Only solution with end-to-end management, including the virtualization layer (Spectrum Control).
  - Storage Tiering, Easy Tier, Flash support, scale large and small, real-time compression, space efficient and incremental snapshots, stretch cluster and hyperswap.
  - Can be exploited by backup only snapshots (Spectrum Protect Snapshot) or multi-use-case snapshots (Spectrum Copy Data Manager).
  - Multi-site DR replication management with IBM Copy Services Manager.
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.
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

- 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.
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

- 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.

Backup-Archive Engine Storage Tier
Tape Storage Tier
Object Storage Tier
Where else can a Backup Solution Fit to Protect from Ransomware?

- A system that has the bulk of its data encrypted will have an unusually large amount of activity and encrypted data will deduplicate poorly. Large deviations in activity can be identified and reported upon. Theoretically, you can run a pre-backup script to look for obvious changes in the file system (create date, modify date, archive bit, etc.) and if it exceeds a threshold, fail and skip the backup.

- 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.

- As discussed earlier, managing multiple backup types, including snapshots, can provide faster recovery or superior protection.

- Storage pools can be configured to not reuse storage for X days after expiration. This Reuse Delay allows a safety buffer to if bad backups have been sent.
Providing WORM and WORM-Like Features
Regulatory Requirements for non-erasable, non-rewriteable storage

There are many regulations that require non-erasable or non-rewritable storage (WORM, immutable, etc.)

- SEC17a-4: According to the rule, records of numerous types of transactions must be retained and indexed on indelible media with immediate accessibility for a period of two years, and with non-immediate access for a period of at least six years. Duplicate records must also be kept within the same time frame at an off-site location. Source: Wikipedia

- Many others, from different governmental organizations in different governments.

- Like many government regulations, the governmental agencies do not, themselves, certify any solution directly. Some organizations, like KPMG, will evaluate a solution and document an opinion that it does or does not meet the regulations (an assessment document).
Regulatory Requirements for non-erasable, non-rewriteable storage

- KPMG evaluated Spectrum Scale immutability and how it complies with SEC17a and other regulations:

- KPMG has previously assessed SSAM 6.3 to be SEC 17a-4 compliant:

- KPMG has recently assessed Spectrum Protect for Data Retention v8.1 to be SEC 17a-4 compliant:
  http://www.kpmg.de/bescheinigungen/RequestReport.aspx?56B00E998BA14B31AF2E0F0FB63F0034

- Combining Spectrum Scale immutability with external pools will extend the immutability to IBM Cloud Object Storage, Spectrum Scale and Spectrum Protect.
  Note: no combination with Scale and external storage pools have been assessed by KPMG at the current time.

- Spectrum Protect supports many types of WORM media (WORM tape, software-worm content addressable storage, etc.) BUT an administrator can delete backups and archives. Spectrum Protect for Data Retention will not allow archive data to be deleted early, thus providing software-based WORM. IBM documents using SP for Data Retention to comply with these types of regulations: https://www.ibm.com/dev.../media
Spectrum Scale and Integrated Archive Manager Features

• Spectrum Scale, a.k.a. is a global shared file system, which can be broken down into sub-sets called FileSets.

• Spectrum Scale supports setting the Immutable (WORM) or Append-Only characteristics on a file, but in older versions those settings could be deactivated by an admin with sufficient authority. Starting in Spectrum Scale, file-sets can have Integrated Archive Manager (IAM) features enabled, which prevent deactivating these features once they are activated.

• These IAM features are as follows (when running in Compliant mode):
  • Immutable: A file cannot be modified, renamed or relocated once this is set, until an expiration period is reached. Once it has expired, it can be deleted, but not otherwise modified.
  • Append-Only: A file can only be appended to once this is set, but previously written data cannot be modified and the file cannot be renamed, moved, etc. Once an expiration period is reached, the file can be deleted, but not otherwise modified.
  • Immutable and Append-Only flags can be set with Scale command mmchattr or OS command chmod.
  • Retention date can be set using Scale command mmchattr or the OS command touch
  • Immutability is compatible with external storage pools, which may in turn exploit WORM storage technologies.
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.