Comprehensive Data Storage Solutions

Fortifying Your Business

LRS®
IT SOLUTIONS

Data protection has continued to morph over the last 20+ years. Today we are seeing a new evolution as to what it means to ensure data is safe and protected.

It used to be that when businesses thought about data protection, they thought about replication, backup and recovery. Today's data protection, is now all about ensuring that your business is resilient, and since data is the lifeblood of business, is your data resilient?

Cyber resilience refers to an entity's ability to continuously deliver the intended outcome, despite adverse cyber events. The concept essentially brings the areas of information security, business continuity, and organizational resilience together.

Cyber Attacks:

- Phishing (spear, whale, zombie)
- Malware (ransom, drive by, trojan)
- Web Attacks (sql inject, xss)
- Eavesdropping / Man in the middle
- Denial of Service
- Password and Brute Force Login
- Insider Threats

Data Breaches:

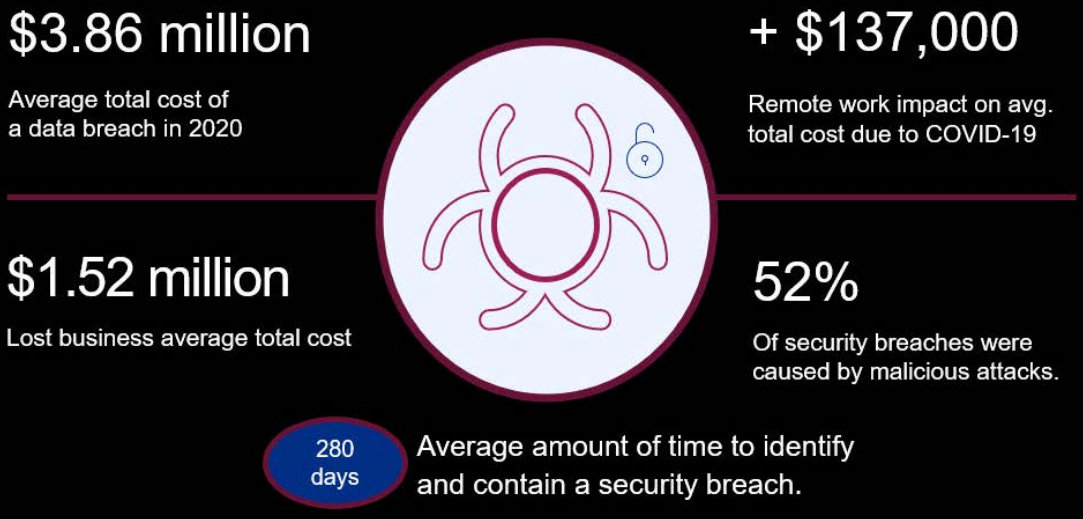
- Physical Theft
- User Error
- Unauthorized Access

Historically, we protect data from accidental loss or corruption, and from catastrophic physical events

- Backup and archive, with various granularity of recovery
- Offsite transport of backup media, network copies of backup data
- Replication of active data by storage layer, middleware, or application since late 1990's
- Methods for continuous operation

Protection of enterprise data from cyberattack is another dimension of the data custodian role. New threats from increased societal role of technology, distributed IT, and increased risk from bad actors

- More than just securing passwords and running firewalls. Threats now include 'trusted' employees, mobile devices etc.
- More sophisticated attacks, including state actors
- More complex environments, including mobile devices, external data feeds, information ecosystems, all presenting larger attack surfaces



Source: IBM security, 2020 Cost of Data Breach Study

Every business is on a cyber security journey

Most businesses today at least 'think' they have some solutions in place, and they are likely focused on Business Continuity or Disaster Recovery (BC/DR). However, a focus on cyber resiliency adds another dimension.

Cyber resiliency, Business Continuity and Disaster Recovery share a common goal of protecting your data. When you add a focus on cyber resiliency, you will then have confidence that the copy of your revenue producing data has not been modified since it was ingested and that it can be reliably used to restore your business should a cyber incident occur.

The Case for Safeguarded Copy

In previous years, businesses have focused on the development and execution of solutions bordering on high availability (HA) and disaster recovery (DR). These solutions are typically based on the need to protect enterprise data from data center outage-based hardware and software compromises. However, cyberattacks have advanced almost at the same systematized rate as business technology; hence organizations are vulnerable to cyberattacks.

Currently, companies that encounter cyber-breach are still exposed to risks like loss of vital data and market share and industry reputation. And in the context of modern times, accidental or intentional logical corruption have become a new scare and for a legitimate reason.

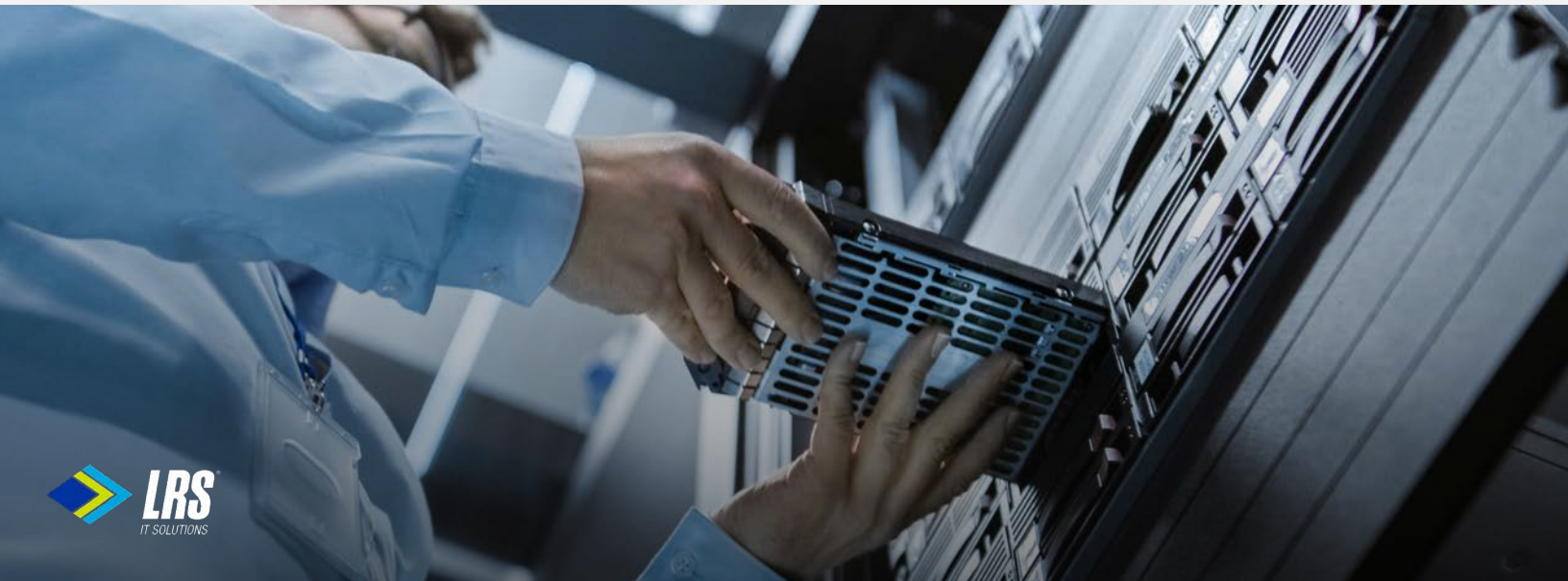
The Need for Logical Corruption Protection

Logical Corruption Protection (LCP) is a data protection approach that provides secure, point-in-time copies of production data, which factor in the future identification, repair, or replacement of corrupted data. This data may have been compromised by either cyber or internal attack or corrupted by system failures or human error. LCP facilitates a number of data analysis and system restoration processes that can prove invaluable for achieving effective and efficient data protection:

Data validation is the process of executing regular analytics to identify data corruption and determine the most convenient recovery actions. Performing corruption detection and validation processes against data copies may prove more practical than performing these actions in a live production environment.

Forensic analysis identifies the cause and scope of a problem before you decide on a recovery action. If the data validation process detects a data corruption event, then the next step is to carry out a forensic analysis, which determines what data is corrupted, when the corruption occurred and which of the available protection copies is the most recent uncorrupted one. Based on this analysis, you can determine whether to:

- Fix the corruption from within the production environment
- Extract and recover certain parts of the data from a valid backup copy (surgical recovery)
- Restore the entire environment to a point in time that is known to be unaffected (catastrophic recovery)



Surgical recovery

In this process, you extract particular data from a valid copy, after which you logically restore it into its production environment. This process becomes necessary if you restore certain production data parts. In essence, you can use it if the larger part of the data is uncorrupted and, on the condition, that the current production data can re-establish the corrupted portions. Furthermore, you can use the surgical recovery when it is not feasible to restore the complement environment because the last-known-good backup copy is confirmed too old. Then, you may have to leave the larger share of the production volumes in the existing state so that you copy replacement data for correcting corrupted data.

Catastrophic recovery

This method will be used when you have to recover the whole environment to a valid copy and as the only option for recovery. They follow a trend of natural or human errors that set large-scale damage or disruption in motion. The chain of cause and effect also severely impacts both the business operations and production systems. In the case of a far-reaching corruption, or where can confirm that the latest known-good protection copy is current, the most feasible recovery strategy is whole environment restoration. Gradually, the process will reverse the situation such that there is a time the corruption has not been affected.

Offline backup

If you seek a second layer of protection by backing up a copy of your environment to offline media, the offline backup will prove most effective. This is possible in either virtual or physical isolation methods, both of which exist in the same storage area network (SAN) or Internet Protocol (IP) network as the environment of production. In virtual isolation, you can create more than one storage system in the current high availability, whereas under physical isolation, you can achieve copy protection using additional/separate storage systems. However, this does not mean they are on the same SAN or IP network as the production environment. Moreover, there are different administrators to define the duties even as access is limited.

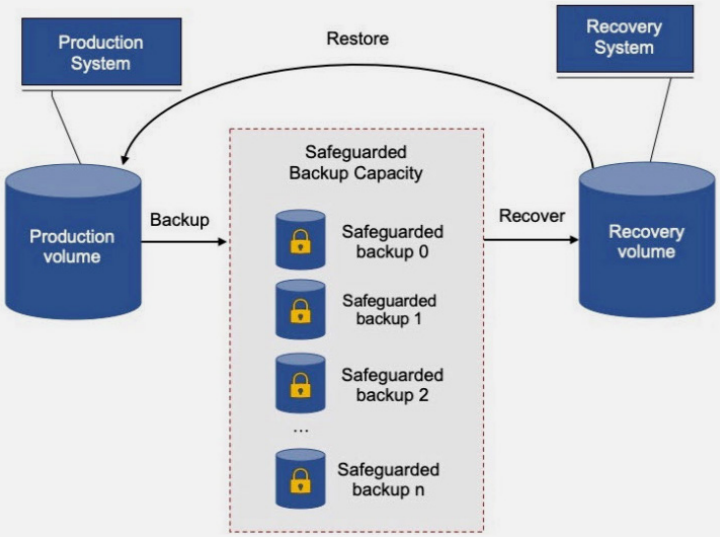
Logical Corruption Protection Requirements

Since the high availability and disaster recovery solutions fall short of content-level data damages, engineers usually need to innovate new protection solutions. Now, some requisite characteristics and standard design requirements to address logical corruption protection are discussed below:

- Granularity: Must be able to create many protection copies in order to minimize the loss of data if a corruption event takes place.
- Isolation: Protection copies must be isolated from active production data to prevent post event corruption coming from a host system that has been compromised.
- Immutability: Copies must be protection against unauthorized manipulation.

Advanced data protection capabilities with Safeguarded Copy

After a cyberattack occurs, you don't want to discover that your sensitive point-in-time copies are corrupted or missing. Safeguarded Copy provides immutable points of data recovery that are hidden and protected from being modified or deleted due to user errors, malicious destruction or ransomware attacks. These immutable copies are a secure source of data that can be used for a forensic analysis, or a surgical or catastrophic recovery.



With Safeguarded Copy, storage administrators can ensure that data is kept safe, secure and recoverable in a way that is transparent and easy to manage. Safeguarded Copy is secure and efficient, and offers a number of important advantages:

- It provides up to 500 backup copies per volume to restore data in case of logical corruption or destruction of production data.
- The backup volume is a hidden, non-addressable volume that does not consume any of the regular volume addresses.
- Copies can be maintained at either production or recovery sites.
- Storage targets are protected against malicious actions with additional security provided through unique user roles.
- Safeguarded Copy capacity is allocated in the best performing storage tier available, minimizing performance impacts from writing backup data.
- For capacity optimization, safeguarded backup uses thin provisioning and may also use thin provisioned Extent Space Efficient (ESE) recovery volumes.
- Safeguarded Copy can be integrated with different disaster-recovery and high-availability configurations.
- Different user roles and authority levels can be used to manage production source volumes, backup capacity and recovery volumes.
- For maximum security, administrators need at least two interfaces in order to create, enable and manage Safeguarded Copy:
    - The DS8000 DS command line interface (CLI) or graphical user interface (GUI) is needed to IBM Systems Solution Brief create backup capacity.
    - IBM Copy Services Manager is needed to enable and manage Safeguarded Copy tasks.
    - Access to one or the other interface can be limited and restricted to specific storage administrators.

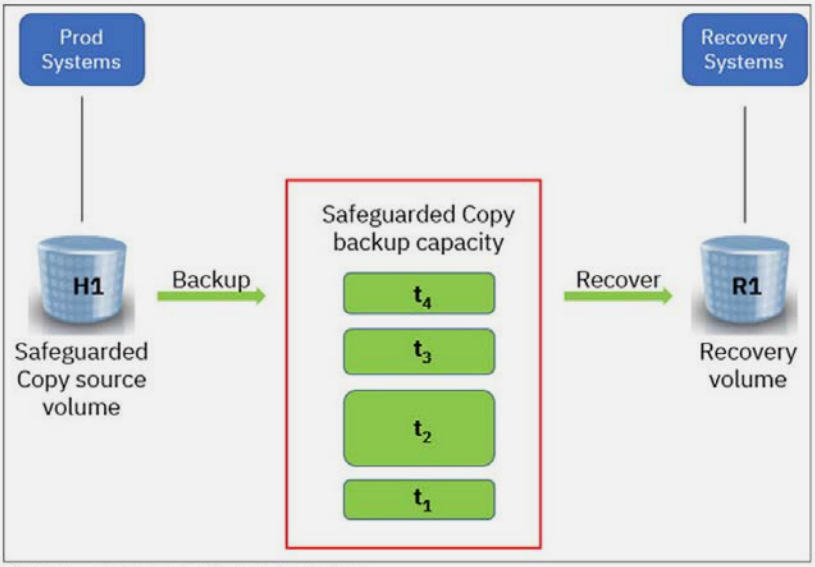


Figure 1— Safeguarded Copy basic relations

IBM Copy Services Manager (CSM) provides highly secure and efficient capabilities to manage Safeguarded Copy tasks including:

- Create and monitor Safeguarded Copy sessions.
- Create manual or automatic Safeguarded Copy Backups
- Expire Safeguarded Copy Backups
- Recover a Safeguarded Copy Backup
- Display Volumes of a Safeguarded Copy Backup
- Terminate a Safeguarded Copy session

Safeguarded Copy does not replace IBM FlashCopy functionality, which is also offered with DS8000 systems. Both technologies remain relevant in LCP scenarios:

- IBM Systems Solution Brief FlashCopy provides an instantly accessible copy of a production volume or data set, and each copy is independent from the others from a data perspective.
- Safeguarded copies could be used to take many frequent copies of a production environment (such as hourly copies maintained for a number of days) while FlashCopy continues to be used to take a a small number of less frequent copies (such as weekly copies maintained for 1-2 weeks).

Safeguards That Perform

Safeguarded Copy functionality substantially expands the repertoire of data protection strategies that enterprises can deploy to keep their businesses in the ballgame and their customers coming back.

You may not be able to choose when an enterprise cyberattack will occur – however, you can ready your business for when it happens.

Are you ready to tackle continually growing cyber security threats? Contact LRS to learn more about the IBM Safeguarded Copy functionality