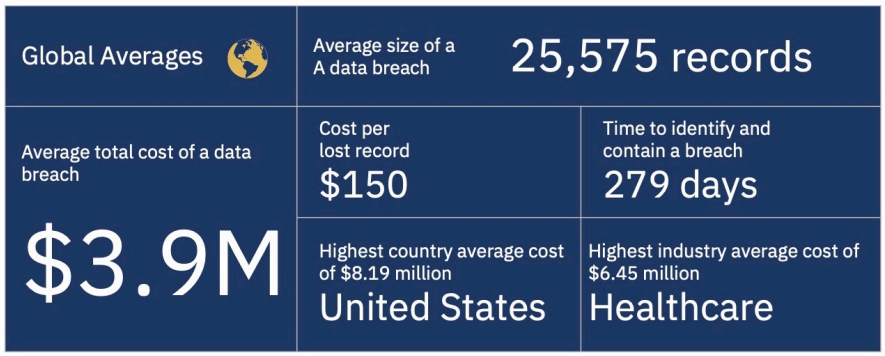
Safeguard against cyberthreats

IBM Safeguarded Copy provides powerful data protection for mission-critical environments

Highlights

- Provides immutable copies of data for Logical Corruption Protection
- Enables hidden, non-addressable backups for additional security
- Offers simple implementation on IBM DS8900F and DS8880/F systems
- Integrates with many disaster-recovery and high-availability environments

Whether they are caused by human error, system glitches, or malicious criminal acts, data breaches are among the gravest and most expensive threats to today's businesses. The annual Cost of a Data Breach Report, conducted by the Ponemon Institute found that the average cost worldwide of a data breach in the preceding 12 months was $3.9M.[1]



The costs of a data breach rise along with the growth in the value of data.

There is also a corresponding human toll. The World Economic Forum's (WEF) 2020 Global Risks Report rated cyberattacks as one of the top risks to human welfare. 75% of those surveyed by the WEF said they expect the risk of theft of data or money from cyberattacks to increase, while 76.1% also saw an increased risk of disruption of operations.[2]

Organizations affected by a breach run the risk of having their normal business operations disrupted, as well as losing valuable data, customers and reputation within their industry. Over the last decades, most organizations have concentrated on developing and implementing high availability (HA) and disaster recovery (DR) solutions to protect their enterprise data against hardware and software failures or data center outages, but these measures may no longer be enough protection against cyberattacks. Today, companies become increasingly concerned about accidental or intentional logical corruption.

Logical Corruption Protection

In this context, logical means that the all-hardware components are working as expected, but data becomes destroyed or corrupted on a content level. This form of corruption can range from deletion, to encryption, to selective manipulation.

Logical corruption cannot be prevented with traditional HA/DR solutions, which are not content-aware. In fact, continuous replication solutions, such as Metro Mirror or Global Mirror, which are often used for DR, would quickly propagate any content level corruption to all copies, because for the storage system, it would just be another I/O.

We need a paradigm shift from a pure availability mindset to cyber resilience (CR). Cyber resilience aims at the ability of an organization to continue to operate with the least amount of disruption despite cyberattacks and outages. Cyber resilience expands the scope of protection, covering both cybersecurity and business continuity. A significant part of cyber resilience is the ability to recover from a logical data corruption event.

Logical Corruption Protection (LCP) is a type of data protection that provides secure, point-in-time copies of production data that can later be used for identification, repair or replacement of data that has 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 is the extraction of specific data from a valid copy and logically restoring it into the production environment. You perform surgical recovery if you only need to restore certain parts of the production data. This may be preferable if only a small portion of the production data is corrupted and if consistency between current production data and the restored parts can be re-established. Another case for this kind of recovery may occur if the latest known-good backup copy is too old to restore the complete environment. It may then be desirable to leave most of the production volumes in their current state and only copy replacement data to correct actually corrupted data.
- Catastrophic recovery is used when you must recover the entire environment back to the point in time of a valid copy, because this is the only recovery option. Catastrophic events are natural or man-made incidents that result in extraordinary levels of damage or disruption, severely affecting production systems and the ability to sustain business operations. If the corruption is extensive, or if the latest known-good protection copy is current enough, the easiest way may be to restore the entire environment to a point in time that is known to be unaffected by the corruption.
- Offline backup provides a second layer of protection by backing up a copy of your environment to offline media. Both virtual and physical isolation of protection copies is possible. With virtual isolation, the protection copies are created in one or more storage systems in the existing high-availability and disaster-recovery topology. These storage systems typically exist in the same storage area network (SAN) or IP network as the production environment. With physical isolation, additional, separate storage systems are used for the protection copies. These systems are typically not on the same SAN or IP network as the production environment, and they have restricted access or even different administrators to provide segregation of duties.

Requirements for logical corruption protection

As already stated, traditional HA/DR solutions cannot provide complete protection against content-level destruction of data. Different approaches to data protection are required to provide this kind of protection. The major design requirements for logical corruption protection include the following characteristics:

- **Granularity:** we must be able to create many protection copies in order to minimize data loss in case of a corruption incident
- **Isolation:** the protection copies must be isolated from the active production data so that it cannot be corrupted by a compromised host system (this is also known as air gap)

- **Immutability:** the copies must be protected against unauthorized manipulation.

The IBM DS8000 storage systems provide a wide range of data protection capabilities, mostly based on the proven IBM FlashCopy and Peer to Peer Remote Copy (PPRC) technologies. They were, however, not designed for today's logical corruption protection demands. IBM Safeguarded Copy functionality is introduced to fill this gap.

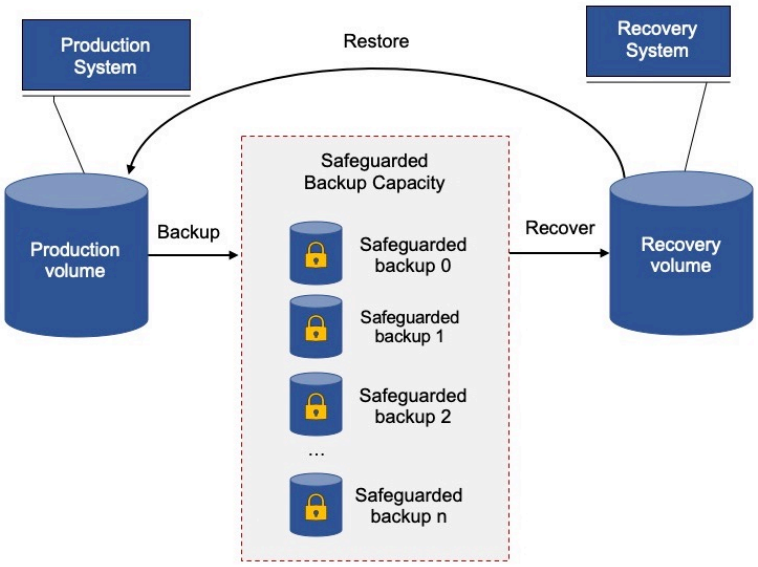
IBM Safeguarded Copy

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

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.



IBM DS8000 Safeguarded Copy

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:

- 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 small number of less frequent copies (such as weekly copies maintained for 1-2 weeks).

Safeguards that perform

Perhaps no combination of data protection strategies will ever achieve 100 percent effectiveness. But aggressive innovation from IBM ensures that IBM systems such as the DS8000 family of proven, market-leading storage solutions offers leading-edge data security capabilities and options. IBM 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. This is what data security means in the 21st century, and this is what IBM delivers.

[1] "2019 Cost of a Data Breach Study: Global Overview." Ponemon Institute, July 2019
https://www.ibm.com/security/data-breach

[2] "Global Risks Report 2020." World Economic Forum, Geneva, Switzerland, January 2020
https://www.weforum.org/reports/the-global-risks-report-2020

Why IBM?

IBM storage solutions do more than provide a trusted resting place for data; they help meet the needs of IT administrators for storage solutions that offer them more value from their data and are built with disaster response in mind, not simply day-to-day operations. IBM innovations in modern data protection are well suited for today's demanding high-volume data staging, archiving and analysis environments, and are designed to address ease of use, interoperability, reliability, security and capacity needs.

For more information

To learn more about the IBM Safeguarded Copy functionality for IBM DS8000, please contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/us-en/marketplace/ds8000f

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM®, DS8000®, FlashCopy®

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.