Safeguard against cyber threats

IBM DS8880 Safeguarded Copy functionality provides powerful new data protection for mainframe and other mission-critical environments

Today, we increasingly witness cyberattacks and breaches with devastating and far-reaching consequences. Cybercrime costs enterprises around the globe nearly two trillion dollars a year, with an estimated 4,000 ransomware attacks occurring each day. In 2018, the average cost of a data security breach approached USD3.9 million. With attacks becoming more malicious and techniques more advanced, businesses need new technologies and practices to survive and adapt to today’s cyber threat scenarios.

Mainframe utilization has remained robust as these high-performance processors move from being simply transactional machines to becoming drivers of revenue growth and business innovation. Today, mainframes are as important to business as ever before, if not more so. 87 percent of all credit card transactions and nearly USD8 trillion in payments a year are processed on mainframes. These systems manage 29 billion ATM transactions each year, equivalent to nearly USD5 billion per day.
The costs of a data breach rise along with the growth in the value of data.

The enduring value and popularity of mainframes and other high-performance data processing environments means that the supporting storage infrastructure must continue to evolve and innovate in unison with these systems order to ensure the most effective data protection and security possible. DS8880 data systems continue to be a powerful complement to both mainframe and distributed computing environments. Not only is DS8880 the leader in the external storage market for mainframe environments, but family members offer an additional advantage—deep integration with IBM Z.

Cybersecurity is not a new concept for DS8880. Thanks to its highly resilient architecture, DS8880 solutions have helped protect data from malware, ransomware, cyberattacks and many other threats for decades. At the same time, DS8880 systems have more than kept up with the pace of mainframe innovation. This is reflected in the recent introduction of new Safeguarded Copy functionality that provides logical corruption protection (LCP) to help mainframe-based enterprises stay one step ahead of cyber threats.

Proven data security strategies

Cyber threats to enterprise data are increasing from a range of different sources, including external malware infection and external hacking, as well as threats from inside organizations. In fact, for core systems running on IBM Z or IBM Power Systems, many organizations believe cyber threats from privileged insiders pose the greatest risks, though loss or corruption of data also results from other causes such as application and operational errors. This means that truly effective data protection solutions designed to reduce the risk of financial losses from security breaches must handle a wide range of possible scenarios.
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.

The question becomes, How do enterprises most efficiently and effectively implement these data protection strategies and processes? DS8880 data systems, with their new Safeguarded Copy functionality, offer a compelling answer.

The leader in mainframe storage

For data sets and business use cases requiring the highest performance and availability, DS8880 is the number-one family of storage systems supporting both mainframe-based and distributed IT infrastructure. The storage systems and their predecessors have been deployed to support business-critical environments for nearly two decades. Just last year, DS8880F was named a Product of the Year finalist by Storage Magazine.

The DS8880 family is designed to manage the full spectrum of storage workloads that exist in today's complex data infrastructure and do it while offering very high performance and system availability, with industry-leading data protection and disaster-recovery features.
The IBM DS8000 family has continually increased not only in storage capacity, but in its ability to avoid or disrupt security threats to enterprise data.

The DS8880 family currently includes four members—the new IBM DS8882F, plus IBM DS8884F, IBM DS8886F and IBM DS8888F—that together provide a broad range of options for addressing business-critical application workloads. These proven, award-winning systems would not have maintained a leadership position in a rapidly evolving IT marketplace without considerable ongoing evolution and innovation. The true difference between DS8880 and other enterprise storage systems lies in this combination of maturity and innovation. For example, DS8880 leverages innovations such as new Gen2 High Performance Flash Enclosures (HPFE) for increased storage density and lower storage costs, transparent cloud tiering to enable agile integration with cloud resources, and a suite of features to enhance support for Blockchain implementations. Today, DS8880 can be deployed in next-generation IT and business environments with as much confidence and trust as ever.

The practice of pervasive encryption can also:

- Protect data associated with applications, databases or cloud services
- Reduce risk with undiscovered or misclassified sensitive data
- Make it more difficult for attackers to identify sensitive data
- Significantly reduce the cost of compliance
- Encrypt data without requiring time- and cost-intensive application changes
Not only is DS8880 the leader in the external storage market for mainframe environments in general, but family members offer an additional advantage in particular—deep integration with IBM Z. Innovation and new engineering is planned and developed in conjunction with the IBM Z team and released in a coordinated manner. This unique IBM relationship helps maximize the potential of mainframe environments by delivering mission-critical acceleration, uncompromising availability and transformational efficiency through industry-leading capabilities.

Perhaps most importantly, DS8800F systems complement the IBM Z suite of data protection technologies collectively labeled “pervasive encryption,” which essentially enables extensive encryption of data in-flight and at-rest to simplify encryption and reduce costs associated with data protection.\(^\text{11}\)

**Additional data protection through Safeguarded Copy**

In addition to support for IBM Z pervasive encryption, plus a long list of data protection and high-availability features, DS8880 data systems now offer Safeguarded Copy functionality.

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 to restore data in case of logical corruption or destruction of primary data.
- The backup volume is a hidden, non-addressable volume that does not consume any of the regular DS8880 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.

---

The Safeguarded Copy feature for IBM DS8880 allows production data to be quickly and reliably backed up for disaster recovery, but also for analytics, testing and other uses.

Safeguarded Copy helps prevent data from being compromised, deliberately or not, by events such as deletion or corruption of archived data:

• Different user roles and authority levels can be used to manage production source volumes, backup capacity and recovery volumes.

• Administrators need at least two interfaces in order to create, enable and manage Safeguarded Copy:
  - The DS8880 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.

• Production volumes in a Safeguarded Copy relationship cannot be deleted from the DS8880 GUI or CLI, even with the force command.
IBM Copy Services Manager provides highly secure and efficient capabilities to manage Safeguarded Copy tasks, such as creating, monitoring and terminating Safeguarded Copy sessions and creating, expiring or recovering Safeguarded Copy backups.

Safeguarded Copy does not replace IBM FlashCopy functionality, which is also offered with DS8880 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 DS8880 family of proven, market-leading storage solutions offer leading-edge data security capabilities and options. 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.


7 Based on IBM DS8000 data system history and common use cases and IBM experience in real customer environments using high-availability features to improve security and resiliency.


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 backup storage 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 Safeguarded Copy feature for IBM DS8880, please contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/us-en/marketplace/ds8000f