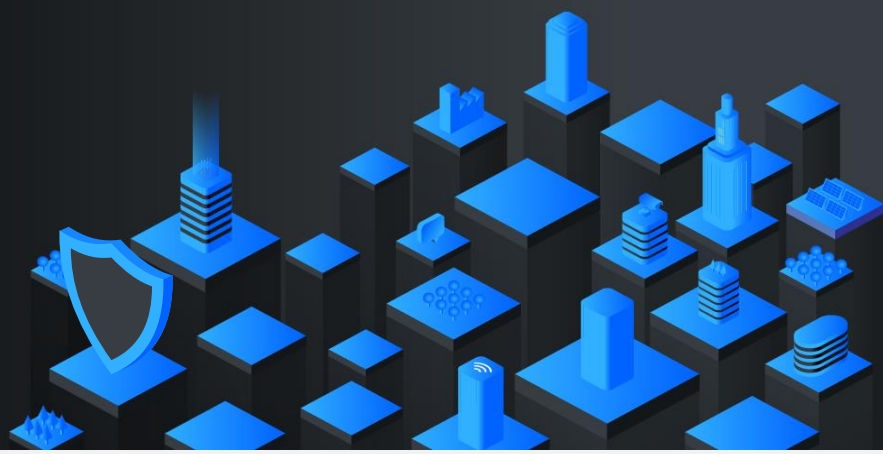
Protect your data against malware and ransomware attacks



Every 11 seconds
a company will likely become a victim of a cyber-attack

2x more attacks
during the CODIV-19 pandemic.

A further increase
in cybercrime is highly likely in the near future.

Building an effective line of defense against cyber threats

As the world evolves and the IT industry becomes more complex due to the nature of multi-cloud environments exposes critical data to higher levels of risk than ever before, the likelihood of a successful cyberattack has become an absolute certainty.
Data Resilience emerges as a modern concept that encompasses two key elements:

- **Data**: It has become the lifeblood of business. It drives what we do, how we do it, and our competitive edge.
- **Resilience**: The capacity to recover quickly from difficulties; toughness.

Data Resilience is defined as "the capability to recover data quickly from any data destructive event and be flexible enough to provide proper accessibility."

Whether they are caused by human error, system glitches, or malicious acts, data breaches including natural disasters are among the gravest and most expensive threats to today's businesses. Organizations affected by a catastrophic event run the risk of having normal business operations disrupted, as well as losing valuable data, customers, and reputation within their industry.

Attacks to national security targets demonstrate that a single attack against critical infrastructure could impact a wide section of society. In response, the **White house** signed an executive order calling for tighter security requirements for hardware and software[1]. IT organizations require a systematic approach to security today, in order to meet new challenges posed by pervasive security threats

Understanding full life cycle of your data

To establish and maintain a robust data resilience strategy, a procedural approach should be employed to understand what data and system assets you have, what their value is, and what risks apply to them.

Adopting the principles of risk management to profile the current and desired data resilience state of your organization enables you to consider a range of possible tiers of implementation
An essential step to set up your environment for proper recovery to ensure the business meets its SLAs is to make sure that clients classify the data in their environment. To do this, the business should:

- **Identify** the objective for classifying their data: is it to better meet its protection objectives or its recovery objectives?
- **Categorize** the types of data they have in their environment by level of importance to the organization
- Create protection and **recovery** workflows based on the data class and tools available
- **Monitor** and maintain new data as it comes into the environment to make sure it is falling into the right protection or recovery bucket
- **Test,** the recovery capabilities for the most important data

Design for recovery: Recover more data quickly
Don't architect for "backup" but architect for fast recovery. This may mean that having environments separated out by important applications or grouping specific data sets together and deciding which technology can provide the best RTO and using that technology for these data sets can be the difference between getting your business up and running quickly or not at all.

The role of storage infrastructure

The System Storage layer has traditionally provided protection functions that help organizations recover from unusual events. Shifting from general data recovery functions to data resilience-related ones specifically, there are four key considerations to ensure a data resilient environment.

- **Isolation** which is the degree of separation of a backup or snapshot from the rest of the network. Isolation can be achieved though logical means or can also be achieved through a physical air gap with Tape infrastructure.
- **Immutability**, or tamper-proof storage that prevents any attacker, external or internal, from changing or deleting data. IBM offers multiple WORM (Write Once, Read Many) storage solutions.

- **Performance** is also an important capability of the data resilience framework. How fast can your organization recover from data corruption, data loss, a natural disaster, or a cyber-attack?
- **Ease of reuse** or the ease of access to data that lives in the backup is important for testing recovery procedures, validating backups, and restoring data into an isolated environment to find a valid recovery point in the event of a ransomware incident. You should be looking for capacities that provide instant restore capabilities, into fenced environments, to get your organization back on its feet quickly and securely.

The solution: Enhanced Data Resilience with IBM

In domains such as data security and business resilience, the multi-cloud business world creates unique challenges that require new solutions tailored specifically to these complex architectures. IBM Storage has responded with wide- ranging innovations designed to meet the unique challenges of keeping data and applications secure in multi-cloud environments.

Two members of the IBM Storage family complementing with Data Resilience technology partner, joined forces to address the unique business resilience challenges – IBM Spectrum Protect Plus, IBM Cloud Object Storage and Predatar.

With an unmatched AI/ML analytics engine, rely on intelligent automation and proactive monitoring to keep your data safe, you don't need to scan everything again before restoration process at high impact to your RTO.

Together, these capabilities provide a modern, comprehensive approach to business resilience that can function effectively with almost any legacy distributed storage systems including Distributed Storage (FlashSystem/Disk), Tape and On-prem COS/Cloud; supporting all kind of data protection workloads: container, bare metal, virtual or application level.

IBM Spectrum Protect Plus, IBM Cloud Object Storage, and Predatar are engineered to leverage all the benefits the multicloud has to offer, while taming its complexity. When it comes to keeping data safe and revenue flowing, these are the solutions that smart businesses choose

Key benefits:

- Strategic partnership with Predatar to increase Data Resilience leveraging automated testing & ransom recovery orchestration using AI/ML.
- Immutable storage to protect data against Cyber Attacks.
- Copies of data stored across hybrid- cloud for better protection against cyber events.

Benefits of IBM Storage-driven Data Resilience

SafeGuarded Copy is yet another weapon within the IBM storage arsenal to fight back cyber threats of all kinds. When you need a copy of your production data that is hidden, non-addressable, cannot be altered or deleted, and is only usable after recovery Safeguarded Copy has you covered.

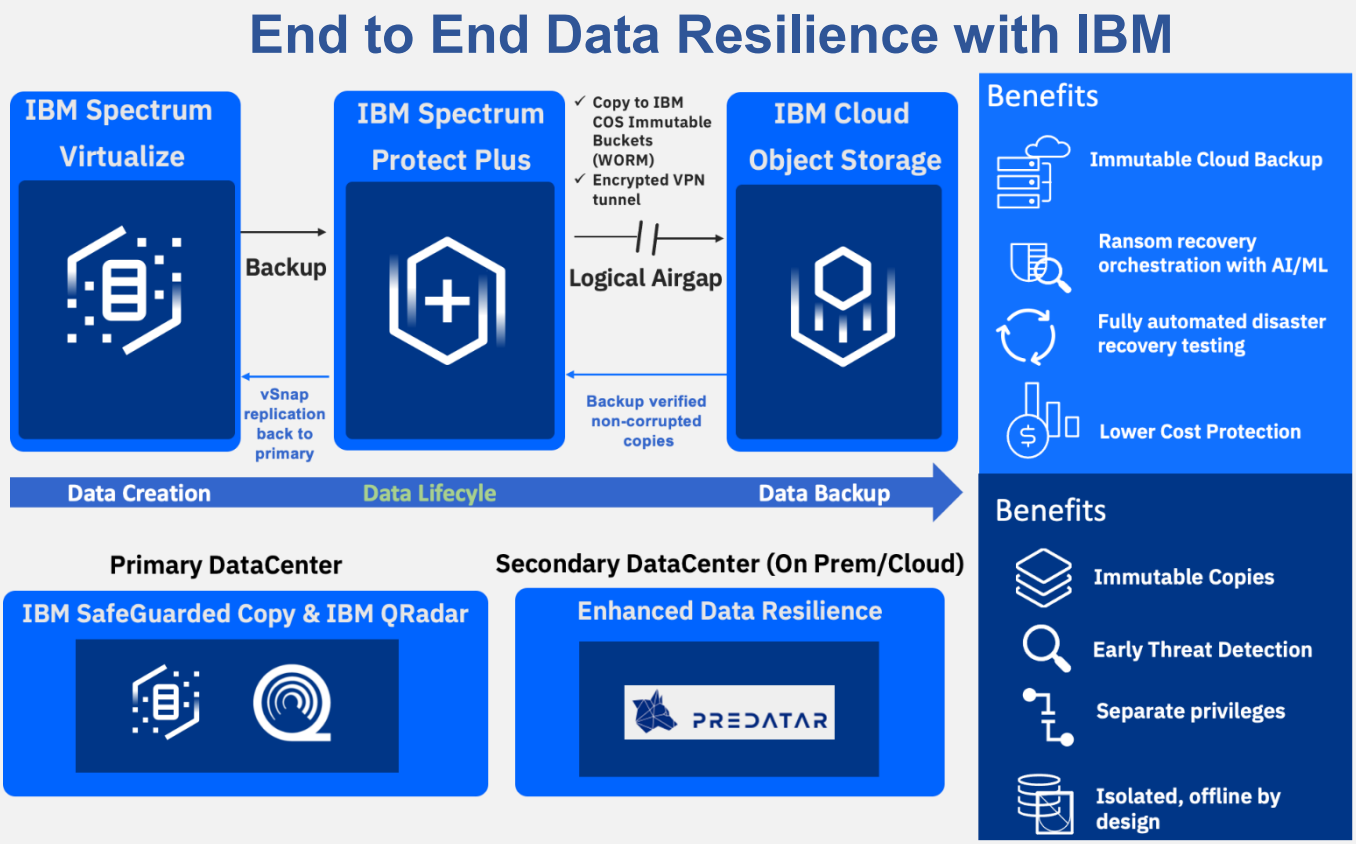


Figure 1 End to End Data Resilience with IBM

These are point-in-time copies that leverage all the same APIs and automation as regular snapshots, only with unique characteristics that make them an ideal place to protect your most important data. First, a Safeguarded copy is offline by design creating a logical airgap between your production data and the copy. IBM intends to deliver the same Safeguarded Copy utilized today in our Enterprise Class DS8000 systems in IBM Spectrum Virtualize for the IBM FlashSystem distributed storage family and IBM SAN Volume Controller [2].

As an added layer of protection supported by the team, in an industry first-of-its-kind integration for block storage, SafeGuarded Copy is integrated with IBM QRadar – the Security Information and Event Management (SIEM) system that helps security teams accurately detect and prioritize threats across the enterprise [3].

Why IBM?

IBM Storage for data resilience provides end-to-end solutions that can efficiently prevent, detect, and respond to cyberattacks as a result of a deep integration between innovative technology and a comprehensive portfolio of software and hardware offerings. By providing multi-layered security and high resilient functionality, this portfolio can maximize the data protection capabilities to help organizations significantly reduce the risk of business disruption and financial losses due to user errors, malicious destruction, or ransomware attacks.

Cyber resilience assessments:

In addition to the capabilities of IBM Spectrum Protect Plus, IBM Cloud Object Storage, and Predatar's orchestration, IBM Lab Services offers a Cyber Incident Response Assessment which is a multi-phase approach that includes a workshop, implementation services, and health checks that help organizations assess their needs, develop strategies, deploy and configure solutions to support cyber resilience.

Also, based on the NIST Security Framework, the Storage Cyber Resiliency Assessment Tool (CRAT) provides a bridge mechanism to evaluate the current data protection state of your organization, identify gaps, strengths, weaknesses, and provides recommendations to build an effective cyber resiliency plan.

1. Executive Order on Improving the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2 (Source: March 23,2021 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS221-137&appname=USN)
3. Available by the time SafeGuarded Copy becomes general available
4. Detect, Protect, Recover: How modern backup applications can protect you from ransomware, Gartner 2021, Nik Simpson, Ron Blair