# IBM FlashSystem Cyber Vault

## Highlights

- Detect cyberattacks early to minimize damage
- Speed recovery from an attack
- Reduce recovery time from days or weeks to just hours
- Enable forensic analysis of attack

The busines and financial effect of cyberattacks continue to rise. Cyberattacks can occur in various ways: they can take many different forms and continue to evolve. Whether the attacker's goal is targeted at stealing confidential customer data or holding valuable information for ransom, organizations must have an overall cyber security strategy in place.

Storage has a fundamental role to play in both helping to detect attacks and helping to recover quickly.

IBM® Safeguarded Copy creates isolated immutable snapshots of data to help protect against cyberattacks, malware, acts of disgruntled employees, and other data corruption. And since Safeguarded Copy snapshots are on the same FlashSystem storage as operational data, recovery is designed to be faster than restoring from copies stored separately.

The IBM FlashSystem® Cyber Vault solution complements IBM Safeguarded Copy. FlashSystem Cyber Vault automatically scans the copies created regularly by Safeguarded Copy looking for signs of data corruption introduced by malware or ransomware. This scan serves two purposes. First, it can help identify a classic ransomware attack rapidly once it has started. Second, it is designed to help identify which data copies have not been affected by an attack. Armed with this information, customers are positioned to more quickly identify that an attack is underway and to more rapidly identify and recover a clean copy of their data.

## Overview

Cybercrime continues to be a major concern for business. Almost every day we see reports of new attacks. The average cost is $4.24 million and recovery can take days or weeks. Cyberattacks have both an immediate impact on business but can also have a lasting reputational impact if the business is unavailable for a long time.[1]

Unfortunately, cyberattacks are very likely to remain a significant threat for 2022 and beyond. It's not a matter of *if* you are breached, it's a matter of *when.*

When a cyberattack occurs, your organization's response will be the difference between permanent financial and reputational damage or comparatively short-term disturbance.

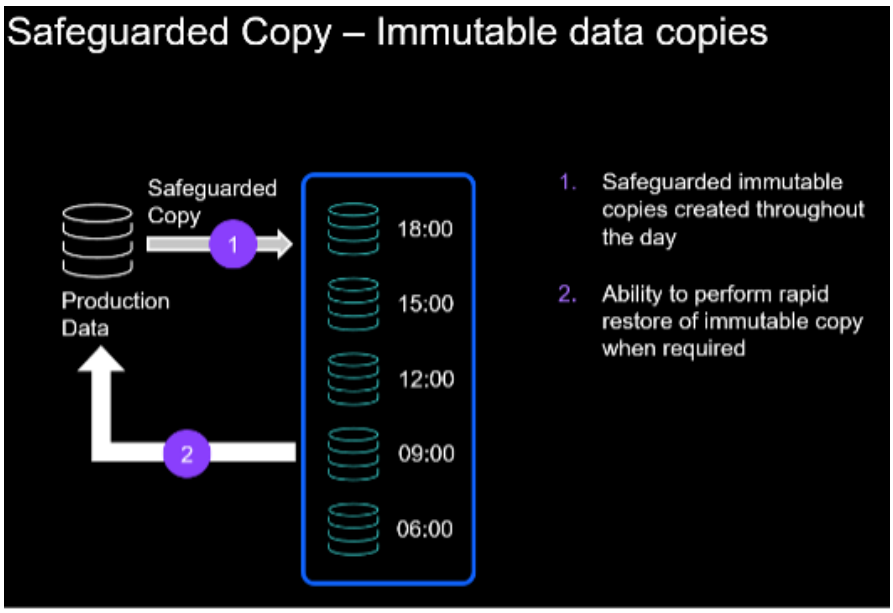
Traditional business continuity solutions that most organizations develop and implement are high availability (HA) and disaster recovery (DR) to protect their data against conventional (but still relevant) threats to data. Unfortunately, these solutions are unable to protect against the increasing range of cyberattacks.

The only solution is to invest in updated technology and automated processes that help protect against a cyber event and also help quickly recover mission critical business operations. During a cyber event, fast recovery is the highest priority for any organizations. Whether large or small,and regardless of industry, every organization must have a well-defined data resilience strategy, including cyber resilience, in place to enable them to recover quickly from a data breach and similar attacks.

## IBM Safeguarded Copy

IBM Safeguarded Copy regularly creates isolated (separated from servers) immutable (unable to be changed) snapshots of data to help protect against cyberattacks, malware, acts of disgruntled employees, and other data corruption. And since Safeguarded Copy snapshots are on the same FlashSystem storage as operational data, recovery is designed to be faster than restoring from copies stored separately.

In this example, a Safeguarded Copy policy automatically takes immutable snapshot copies every three hours.




*IBM Safeguarded Copy operation*

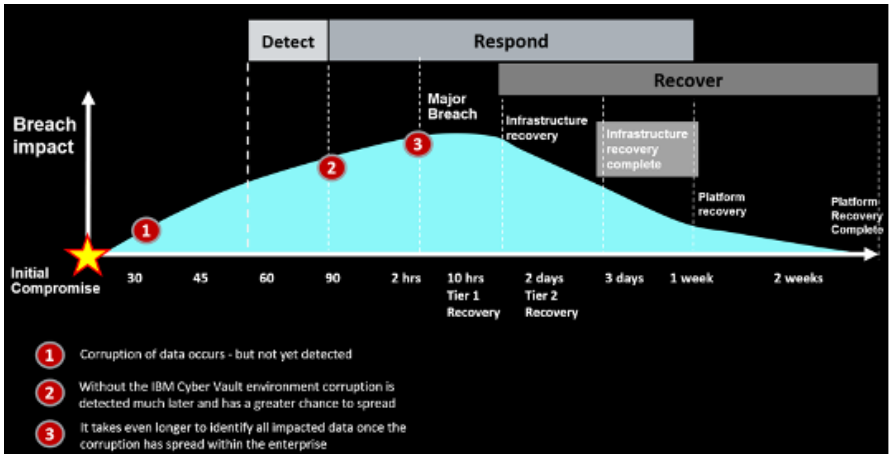
## IBM FlashSystem Cyber Vault

Full cyber resiliency requires intrusion detection and monitoring for unusual behavior at all levels of your infrastructure including individuals, programs, and inter-connected systems, including external vendors and cloud resources. Critical to detection is timely reporting and dashboards to alert teams to unusual activities and behaviors.

All employees, contractors, and other people working with IT tools or systems must regularly refresh their awareness and training on how to prevent common attack points, such as phishing, smishing, vishing, or social engineering. They must also feel engaged and recognize events to report unusual behavior, as this is truly a team effort.

Simply put, it is too late, if the first detection of a ransomware attack is after it has occurred. Investment, utilization, and dedication to proper technologies, tools, processes, monitoring, education, and communication are critical before an incident has occurred. These items are key to achieving enterprise-grade cybersecurity and resiliency.

The following diagram depicts the industry averages in how long it takes an organization to recover business operations. You'll notice 2-3 weeks is very typical.




*Typical duration of cyber recovery*

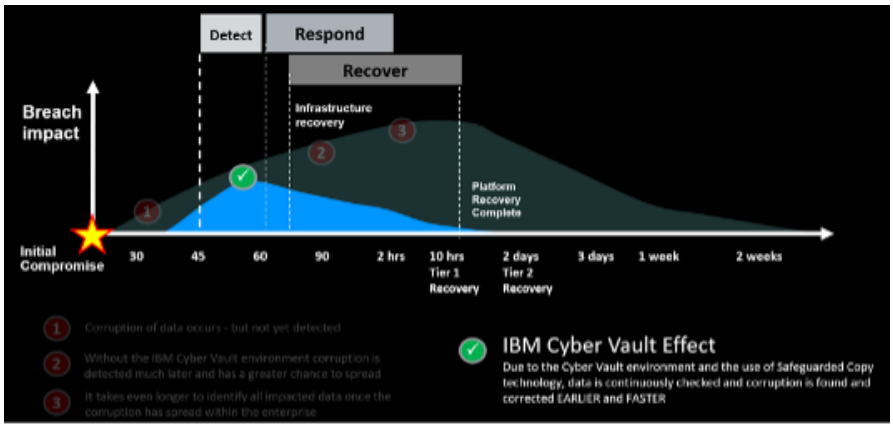
Even so, according to a study, while 41 per cent of business hit with a ransomware attack were able to recover within a month, more than half (58 per cent) said it took more than a month to recover, 29 per cent said it took more than three months, and *nine per cent said it took more than five to six months.*[2]

A cyber resiliency storage solution must provide capabilities to protect against the unique challenges of a cyberattack. First is the absolute need for logical or physical isolation; immutable copies of data that cannot be corrupted or erased by a cyber attacker.

Second, tools are needed to continually validate this data to help detect an attack and build confidence in the quality and validity, of a backup to recover from once a cyber-attack has taken place. These tools will also help IT staff perform the forensic analysis that is needed to assess the incident; formulate optimal recovery strategies and options; and determine the scope of recovery, files, databases, or entire systems.

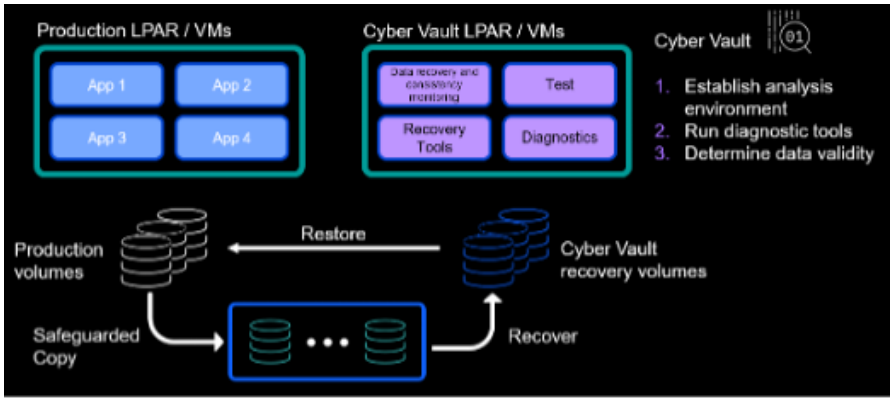
The IBM FlashSystem Cyber Vault solution is a blueprint implemented by IBM Lab Services or IBM Business Partners that is designed to help speed cyberattack detection and recovery. The Cyber Vault solution runs continuously and monitors snapshots as they are created by Safeguarded Copy. Using standard database tools and automation software, FlashSystem Cyber Vault checks Safeguarded Copy snapshots for corruption.

If FlashSystem Cyber Vault finds such changes, that is an immediate indication an attack may be occurring. When preparing a response, knowing the last snapshots with no evidence of an attack can speed the determination of which snapshot to use. And since Safeguarded Copy snapshots are on the same FlashSystem storage as operational data, recovery is designed to be faster than restoring from copies stored separately. With these advantages, FlashSystem Cyber Vault is designed to help reduce cyberattack recovery time from days to just hours.



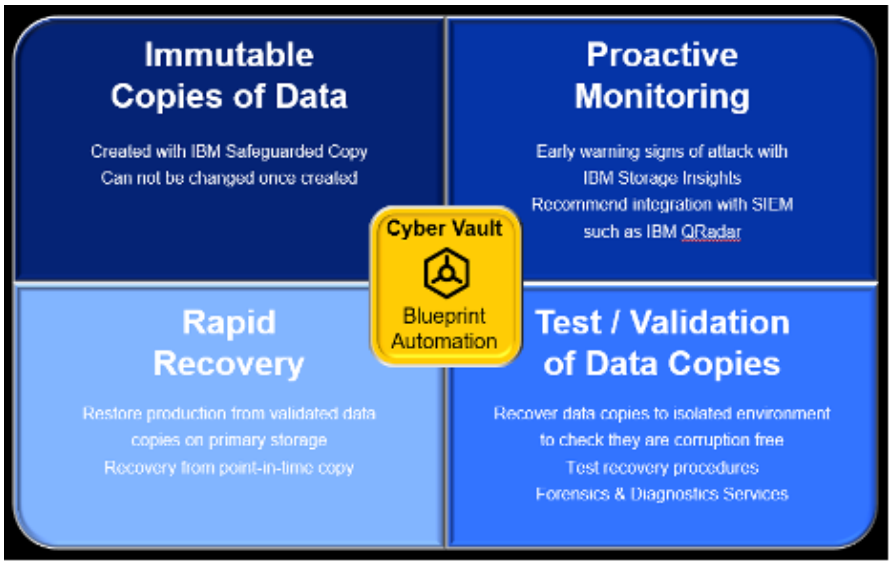

*IBM Cyber Vault effect*

The IBM FlashSystem Cyber Vault solution provides for a safe, isolated environment where a replica of the production environment is maintained. The IBM FlashSystem Cyber Vault environment does not impact the production environment as it leverages a sandbox/clean room environment (logical partitions or VMs) to run data validation processes without affecting production workloads. This sandbox environment is also the place to train your teams, conduct forensic analysis after data corruption is detected, and—based on the analysis—exercise surgical recovery procedures with peace of mind that if something goes wrong with any step of recovery, your teams can always go back to the original Safeguarded Copy point-in-time copy.




*IBM Cyber Vault Environment*

IBM FlashSystem Cyber Vault is comprised of the following four key elements:




*IBM Cyber Vault Operations*

Let's briefly look at these elements in turn.

## Immutable Copies of Data

IBM Safeguarded Copy is the latest protection mechanism for data on IBM FlashSystem family and IBM SAN Volume Controller storage systems. As on IBM DS8000® systems, Safeguarded Copy helps secure data to prevent it from being compromised accidentally or deliberately. It also allows for fast recovery from protected point-in-time copies when a cyberattack occurs.

Safeguarded Copy provides secure, point-in-time copies or snapshots of active production data that cannot be altered or deleted (known as immutable copies). These Safeguarded Copies are typically created in a separate storage environment from production and only accessed by the IBM FlashSystem Cyber Vault recovery system.

## Proactive Monitoring

Detecting a threat before it starts is critical to accelerate recovery time and operational availability.

IBM Security® QRadar® is a Security Information and Event Management (SIEM) solution that can monitor, inspect, detect, and derive insights for identifying potential threats to the data stored on IBM FlashSystem and IBM Spectrum® Virtualize. It provides powerful cyber resilience and threat detection features such as centralized visibility, flexible deployment, automated intelligence, machine learning, proactive threat hunting, and much more.

IBM QRadar can detect malicious patterns leveraging a number of data sources and analysis tools and techniques, including access logs, heuristics, correlation with logs from other systems such as network logs or server logs, network flow, and packet data, and even unknown threat vector detection using IBM Watson® for Security resources. IBM QRadar has integration with IBM Safeguarded Copy to take a protected snapshot of data at the first sign of a possible attack.

IBM Security Guardium® Data Protection automatically discovers and classifies sensitive data from across the enterprise, providing real-time data activity monitoring. It is enhanced by Guardium Vulnerability Assessment, which detects behavioral vulnerabilities such as account xcsharing, eessive administrative logins and unusual after-hours activity, and identifies threats and security gaps in databases that could be exploited by hackers. And to help security principals understand where the threats are to the business, Guardium Data Risk Manager has an executive dashboard to help visualize data-related business risks so both executives and management can take immediate actions to protect the business.

IBM Storage Insights and IBM Spectrum Control monitor IBM flash storage. They provide the ability to both view a current I/O workload against a previous base line and help provide an indication of an attack in progress.

Alerts can be set to be triggered if a storage system is under many types of stresses. For example, if the data reduction ratio suddenly changes radically, that could indicate a cyberattack is now encrypting data. An attack could also cause a significant change in performance. Likewise, deviations or anomalies in write change rate may be an indicator that a cyberattack is occurring.

## Test and Validation of Data Copies

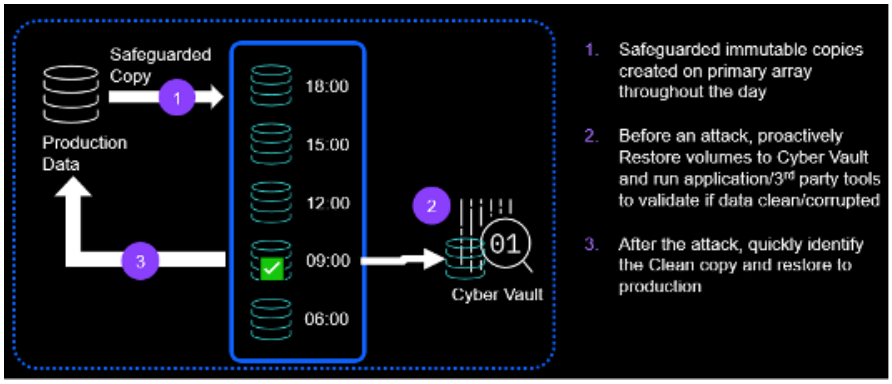
The IBM FlashSystem Cyber Vault solution provides the following distinct cyber resiliency capabilities:

- **Data validation**: Regular operational validation of the Safeguarded Copy point-in-time copies to provide proactive detection of data corruption or reassurance that the copy is validated clean before any further actions.
- **Forensic analysis**: Start a copy of the production system and use it to investigate a problem and determine the recovery action. Plan what tools and procedures would be used to identify the cause and scope of an attack.
- **Surgical recovery**: Extract data from the Safeguarded Copy and logically restore it into the production environment. This operation is critical to restoring data, files, or systems back into production use if there has been an intended or unintended data loss.
- **Catastrophic recovery**: This option is the last option that everyone hopes will never be used. The IBM FlashSystem Cyber Vault solution provides this capability, and it is a best practice to regularly perform a full catastrophic recovery exercise against a test or development system so you can be confident in recovery should an attack occur.
- **Offline backup**: Take a fresh backup with your traditional backup solution of the successfully validated environment to add an additional protection layer and long-term data retention.

## Rapid Recovery

IBM FlashSystem Cyber Vault is designed to provide rapid dependable recovery, in minutes to hours, of your mission critical applications, to protect your organization's reputation and brand value. After a cyberattack, the old saying holds even more true: *time is money!*

As we've seen, the combination of IBM Safeguarded Copy snapshots, Cyber Vault validation, and automation together deliver the ability to rapidly restore a production environment following an attack.




*IBM Cyber Vault Rapid Data Recovery*

## Frameworks for IT Cyber Resiliency

Specific regulations and frameworks vary by country or region of the world. One commonly cited framework was released in 2013 and updated in 2018 by the National Institute for Standards and Technology (NIST).

The NIST Cyber Security Framework provides a policy Framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. This basic framework is an industry accepted methodology for building a plan to develop and implement safeguards to ensure delivery of critical business services. The following diagram outlines the five categories of the NIST Framework:


*NIST Framework*

**Identify** – is about preparing a plan so that when you are attacked, you are prepared and confident in your ability o restore business IT systems back to their prior state, which calls for a detailed awareness of the scope of your critical business assets required to continue operations and a strategy for rapid recovery.

**Protect** – is focused around discovering weaknesses before attackers can, and ensuring your data is stored on infrastructure that cannot be compromised by any malicious activity. This involves topics from ID management, access control, awareness, data security, and data protection as well as proactive protective technology.

**Detect** – find unknown threats with monitoring and advanced analytics to rapidly uncover when threats exist.

**Respond** – Covers coordinating your response: analysis, containment, mitigation, and communication

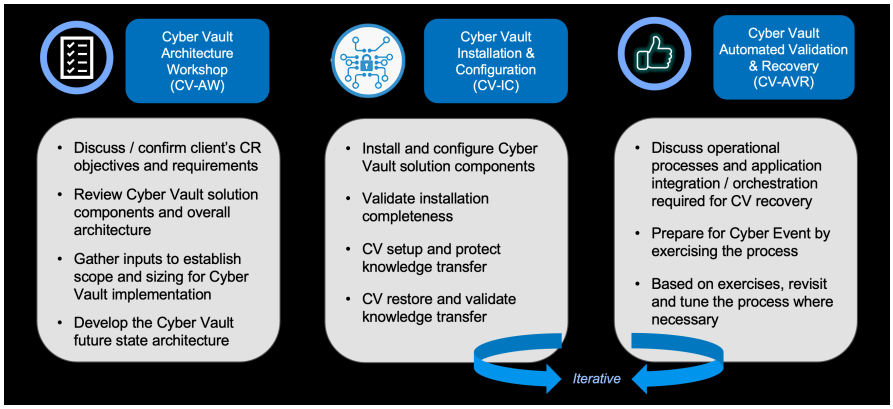
**Recover** – Get back up and running quickly and efficiently. This involves orchestrating many moving parts and once the actions required are analyzed, automating as much of the recovery as possible.

The IBM FlashSystem Cyber Vault solution addresses key components of the NIST Cybersecurity Framework.

## IBM Lab Services

IBM Systems Lab Services offers infrastructure services to help you build enterprise IT and hybrid cloud solutions. Lab Services consultants collaborate with organizations, offering deep technical expertise, valuable tools and successful methodologies. Experts help customers solve business challenges, train IT departments with new skills and how to apply best practices. IBM Lab Services offers deep technical expertise for a wide range of IT infrastructure services including storage.

IBM Lab Services offers a full set of services to help customers accelerate their adoption and use of the Cyber Vault solution. These services for Cyber Vault can include preparation, planning, and implementation of the Cyber Vault solution and, if needed, assistance with cyber incident recovery.




*Deployment Services for IBM FlashSystem Cyber Vault*

## Summary

The busines and financial effects of cyberattacks continue to rise. Cyberattacks can occur in various ways. They can take many different forms and continue to evolve. Whether the cyber attacker's goal is targeted at stealing confidential customer data or holding valuable information for ransom, organizations must have an overall Cyber Security strategy in place.

Traditional HA/DR approaches to data protection work well for their intended purposes, but they are inadequate to protect against cyberattacks. Storage-based remote replication for high availability or disaster recovery replicates all changes (malicious or not) to the remote copy.

Data that is stored on offline media or the cloud can take too long to recover a widespread attack. Large-scale recovery can take anywhere between days to weeks, which can lead to substantial downtime for businesses.

The Safeguarded Copy capability in IBM FlashSystem and IBM SAN Volume Controller is designed to automatically create efficient immutable snapshots according to a schedule. These snapshots are stored specifically by the system and cannot be connected to servers, which creates a virtual isolation environment from malware or other threats. They also cannot be changed and or deleted, except according to a planned schedule, which helps protect against errors or actions committed by staff.

The IBM FlashSystem Cyber Vault solution builds on Safeguarded Copy to help speed cyberattack detection and recovery. Using standard database tools and automation software, FlashSystem Cyber Vault checks Safeguarded Copy snapshots for corruption.

If FlashSystem Cyber Vault finds such changes, that is an immediate indication an attack may be occurring so recovery using the last snapshots with no evidence of an attack can start quickly. And since Safeguarded Copy snapshots are on the same FlashSystem storage as operational data, recovery is designed to be faster than restoring from copies stored separately. With these advantages, FlashSystem Cyber Vault is designed to help reduce cyberattack recovery time from days to just hours.

1. Source: IBM Institute for Business Value 2021 Cost of a Data Breach report, https://www.ibm.com/security/data-breach

2. IT World Canada, "Average ransomware payment for Canadian firms hits $450,000", https://www.itworldcanada.com/article/average-ransomware-payment-for-canadian-firms-hits-450000/467792

## Why IBM?

IBM offers a vast portfolio of hardware, software and services to help organizations cost-effectively address their IT infrastructure needs. These include robust data-storage solutions to enable always-on, trustworthy storage and recovery from disaster. Because business needs shift, IBM solutions emphasize interoperability and the integration of new use cases or approaches, from analytics to multi-site backup to near-instant recovery. With IBM, organizations can create flexible, robust and resilient storage infrastructure to support critical operations for smooth operations and regulatory compliance.

IBM Storage and IBM Security offerings are designed to work together to provide a comprehensive solution for cyberattack prevention, detection, and recovery.

## For more information

Visit our solutions page to learn more about the FlashSystem family of data systems, or contact your IBM Business Partner.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. Visit: https://www.ibm.com/financing/flash

To learn more, contact your IBM Business Partner:

System Analysis Services, INC.
6176316946 | carl@sysgbs.com
http://systemsanalysisservices.com/