IBM Spectrum Sentinel

Automated Recovery from Ransomware and Other Threats

Highlights

- Data resilience for SAP HANA and Epic
- Protects against ransomware and other threats
- Creates immutable application-specific primary storage snapshots
- Uses anomaly detection and machine learning to identify potential threats
- Orchestrates recovery from verified and validated backup copies

Organizations of all sizes, in every industry, are now threatened by increasingly malevolent ransomware and other cyber threats. Even with the strongest defensive measures, there is always the risk that some threats might circumvent every barrier and penetrate an organizations's information supply chain. Beyond the financial cost and operational chaos, these attacks can severely damage a company's brand, especially in critical areas such as financial services, healthcare, and manufacturing.

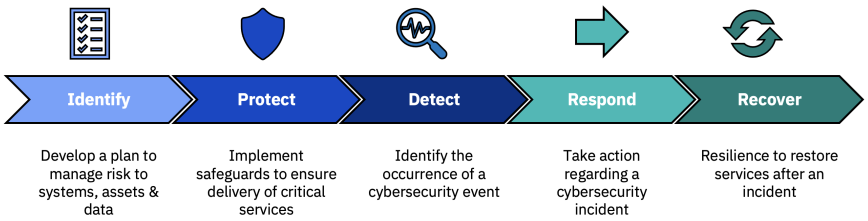
One alarming trend is that some criminal gangs now exploit the fact that many organizations use a “30-60-90” policy for backing up data – snapshots are captured hourly and daily, with full backups generated every 30, 60, and 90 days. In response, these bad actors have come up with a new twist – they install malware and leave it dormant for 100 days or more before springing the trap. At that point, the malicious code has infected not only the target’s production data systems and snapshots, but every single one of their backup copies. The victims have few alternatives other than paying up.

IBM Spectrum Sentinel is a cyber resiliency solution for SAP HANA and Epic healthcare systems, designed to help organizations enhance ransomware detection and incident recovery. IBM Spectrum Sentinel automates the creation of immutable backup copies of your data, then uses machine learning to detect signs of possible corruption and generate forensic reports that help you quickly diagnose and identify the source of the attack. Because IBM Spectrum Sentinel can intelligently isolate infected backups, your organization can identify the most recent verified and validated backup copies, greatly accelerating your time to recovery.

IBM Spectrum Sentinel, a workload-specific turn-key solution, is based on the IBM FlashSystem Cyber Vault architecture, a set of blueprints that can be customized to provide advanced data protection and recovery capabilities for a variety of workloads and use cases.

Comprehensive Data Protection

Defending against today's emergent threats requires an end-to-end framework for data security and protection.

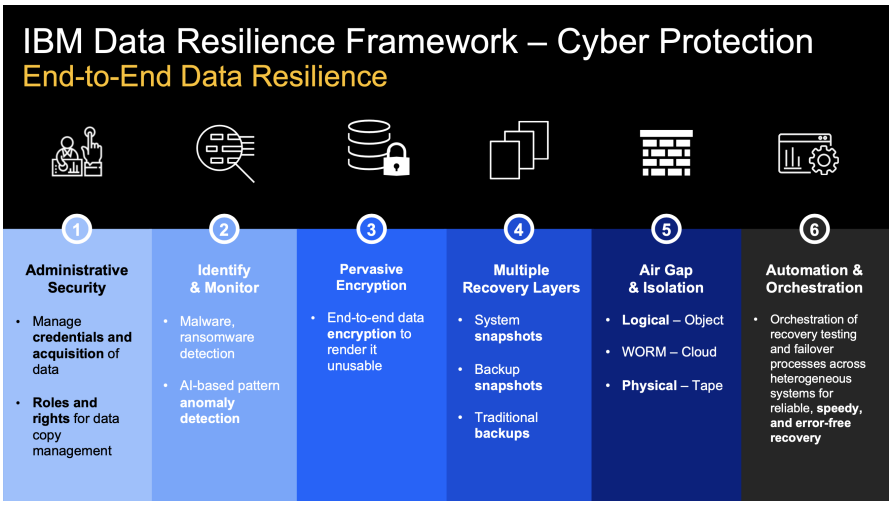


The NIST Cyber Security Framework establishes a baseline for data protection best practices.

IBM has embraced and extended the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST), which identifies five key steps toward comprehensive data resiliency:

- Identify: Develop a plan to manage risk to systems, assets & data
- Protect: Implement safeguards to ensure delivery of critical services
- Detect: Identify the occurrence of a cybersecurity event
- Respond: Take action regarding a cybersecurity incident.
- Recover: Resilience to restore after an incident

The IBM data resilience framework identifies six key capabilities that organizations can implement to help minimize their exposure to potential data breaches, keep the business operational, and control costs.



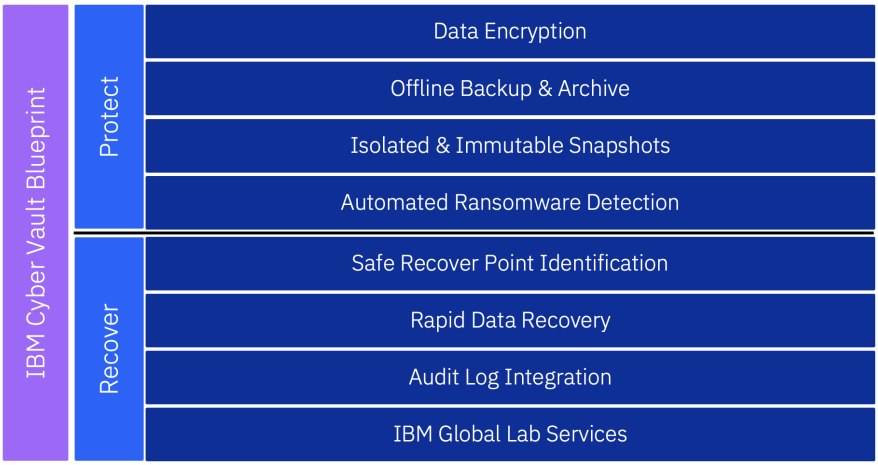
The IBM data resilience framework encompasses the NIST framework and identifies key elements in a comprehensive data protection solution.

These capabilities include:

- Ensuring applications in the environment have identity and administrative security that can help manage credentials and data access. This capability can protect against the biggest of the threat vectors; compromised credentials and the malicious insider, together accounting for 26% of data breaches.
- Monitoring and identifying data in the data protection environment for ransomware or malware and taking advantage of machine learning capabilities to determine data pattern anomalies and contain a threat before it can harm all the data.
- Ensuring the business has pervasive encryption, starting at the primary storage layer all the way thought backups in flight to where it is stored on backup devices.
- Having multiple layers of backup and utilizing the 3-2-1-1 methodology for protecting data to help ensure the business can be back up and running quickly.
- Protecting information in an isolated environment and using a physical or logical air gap to ensure data can't be compromised.
- Putting capabilities in place to automate recovery so the recovery process is effective, rapid, and accurate.

IBM FlashSystem Cyber Vault

IBM FlashSystem® Cyber Vault is a data security framework that provides blueprints for designing and deploying a robust set of data protection and recovery capabilities.



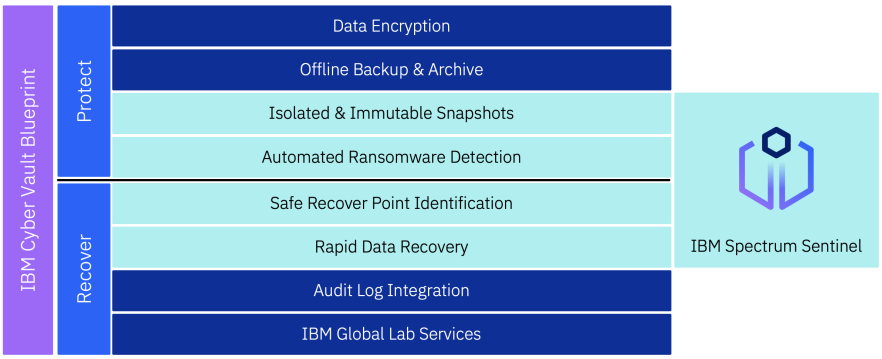
IBM FlashSystem Cyber Vault provides blueprints for effective data protection and recovery.

IBM FlashSystem Cyber Vault builds upon IBM Safeguarded Copy, which creates isolated immutable snapshots of data to help protect against cyberattacks, malware, acts of disgruntled employees, and other data corruption. 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.

IBM Spectrum Sentinel

IBM Spectrum Sentinel was developed in response to challenges experienced by organizations that had successfully weathered a ransomware attack or other cyber threat and wanted to accelerate how quickly they could get back up and running. It is not intended as a replacement for existing real-time security applications but instead provides a last line of defense against corruption when an attack occurs.



IBM Spectrum Sentinel leverages Safeguarded Copy snapshots to accelerate your organization's recovery after a cyber-attack.

Building on the capabilities of IBM Safeguarded Copy, IBM Spectrum Sentinel frequently checks data copies for evidence of data damage caused by malware or ransomware. IBM Spectrum Sentinel then uses Safeguarded Copy snapshots to create a secure and isolated backup. Ransomware cannot remove, alter, or encrypt Safeguarded Copy snapshots, even with administrator capabilities. In the event of a cyber-attack, these authenticated restore points aid in a speedy recovery.

How it Works

There are six key points on the timeline as IBM Spectrum Sentinel responds to a cyber-attack.

The data protection and recovery process for IBM Spectrum Sentinel addresses six key points in the cyber-attack timeline.

1. Pre-attack – IBM Safeguarded Copy creates a series of immutable snapshots, which are proactively scanned for malware by IBM Spectrum Sentinel.

2. During an attack – Ransomware begins infecting production files / databases / systems with Safeguarded Copy, and those snapshots are protected and scanned proactively by Spectrum Sentinel.
3. Scanning initiated – Even as the attack is taking place, IBM Spectrum Sentinel is scanning snapshots and analyzing entropy changes, file extension mismatch, and other signs of data corruption.
4. Integrity review – Snapshots can now be assessed to confirm which have been verified to be free of malware and data corruption.
5. Determine good snapshot – The most viable snapshot to restore from is identified.
6. Restore – The most viable snapshot is used to restore data to the production environment so the organization can resume normal business operations.

IBM Spectrum Sentinel for SAP HANA

Key capabilities for IBM Spectrum Sentinel for SAP HANA include:

Backup

Backup Types

– FlashCopy NoCopy
– FlashCopy Incremental
– Global Mirror with Change volumes
– Safeguarded Copy

There is also a log backup option.

Restore

SCDM will create a temporary volume from a backup and mount it to the original server for recovery unless the user enables the revert option.

Restore Types

– Instant Disk Recovery
– Instant Database Recovery
Restore Options
– Make Permanent - Will initiate a background copy from the source volume to the new cloned volume and make the new clone volume a permanent volume.

– Revert (Reverse FlashCopy)

IBM Spectrum Sentinel for Epic

The integrated EHR software from Epic covers all aspects of healthcare operations, including patient engagement, patient record access, clinical data, specialties, distance care, mobile, managed care, billing and revenue, interoperability, and government regulations.

Epic software implementations employ the following two main database technologies:

– Operational database – The online transaction processing (OLTP) database runs Caché from InterSystems Corporation as the main database engine.
– Analytical database – The analytical databases typically run on Microsoft SQL Server or Oracle database software.

IBM Spectrum Sentinel for Epic supports both the Caché and Iris databases used by the Epic.

1. GigaOm Radar for Hybrid Cloud Data Protection for the Enterprise, June 2021

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.

For more information

NA

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Spectrum Sentinel™