covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

COVENCO GUIDE

Accelerating Ransomware Detection and Response.

Deploying IBM FlashSystem storage and Safeguarded Copy with IBM Security QRadar can enhance threat detection capabilities.

Version 1.0 March 2024

Introduction

The financial impact of cyberattacks continues to rise. According to recent estimates, a company is likely to be the target of a cyber-attack in the next 11 seconds, and the total cost of these attacks has already exceeded $6 trillion in 2023.

There are reports of new attacks almost every day. Cyberattacks can take place in different ways. They can take the form of malware - or ransomware, which aims to steal confidential data or keep valuable information for ransom. Sometimes these attacks are designed to destroy or exfiltrate confidential data to cripple the organisation.

Traditional approaches to data protection work well for their intended purposes but are not sufficient to protect against cyberattacks, which can encrypt or otherwise corrupt business-critical data. Remote replication for disaster recovery will replicate all changes - malicious or not - to the remote site. And data stored on offline media or the cloud can take far too long to recover from a widespread attack.

Recovery operations can take some businesses days or weeks of downtime. Therefore, a solution is needed that combines the protection of offline copies with the speed of local copies.

Improving cyber resilience and business agility with IBM Storage

The IBM® Safeguarded Copy function for IBM FlashSystem®, IBM SAN Volume Controller, and IBM Spectrum® Virtualize for Public Cloud is designed to help businesses recover quickly and safely from a cyber-attack, reducing the recovery from days to hours.

IBM Safeguarded Copy automatically creates efficient immutable snapshots according to a schedule. These snapshots are specially stored by the system and cannot be connected to servers, creating a logical “air gap” from malware or other threats.

The snapshots also cannot be modified or deleted except according to pre-planned schedule policies, which helps protect against unhappy employees’ errors or actions. In other words, Safeguarded Copy is another weapon within the IBM Storage arsenal to fight back cyber threats of all kinds.

Detecting a threat before it starts can help speed recovery even more. IBM Security® QRadar® software uses AI and other technologies to monitor and inspect IT system-generated data to detect potential cyber threats. It is one of the most popular SIEM solutions on the market today.

However, in order to detect malicious patterns most effectively, IBM QRadar must process very large amounts of data from a variety of sources, including access logs, network and server logs, and even network flow and packet data. To obtain the best results, these large data streams require fast, cost-effective, and highly scalable data storage.

IBM QRadar can now pro-actively invoke Safeguarded Copy to create a protected backup at the first sign of a threat.

> “ If you need a copy of your production data that is hidden, non-addressable, cannot be altered or deleted, and can only be used after recovery, Safeguarded Copy has you covered. “

In the event of an attack, our orchestration software, IBM Copy Services Manager, can identify the Safeguarded backup to use and automates the process to restore data to online volumes. Because a recovery action uses the same snapshot technology, it is almost instantaneous: much faster than using offline copies or copies stored in the cloud.

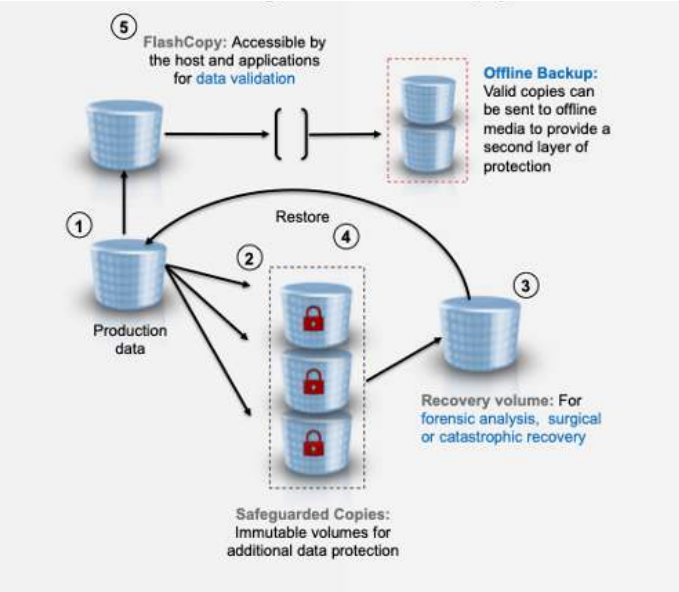
IBM Safeguarded Copy helps you recover quickly and with confidence if you should encounter one of the most pressing IT threats in the industry today, and since it’s available at no additional charge, start planning for Safeguarded Copy now.

IBM Safeguarded Copy

IBM Safeguarded Copy, which is available with IBM Spectrum Virtualize 8.4.2 and later software, is the latest protection mechanism for data on IBM FlashSystem family, SAN Volume Controller (SVC), and IBM Spectrum Virtualize for Public Cloud storage.

IBM FlashSystem Safeguarded Copy, similar to IBM DS8000® Safeguarded Copy, helps prevent data from being compromised, either accidentally or deliberately and allows for recovery from protected backups, in the event of a cyber-attack.

Safeguarded Copy provides secure, point-in-time copies or snapshots of IBM Storage active production data that cannot be altered or deleted (immutable copies), and 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.



IBM Safeguarded Copy Architecture

The safeguarded backups or copies of data are protected with additional security provided through unique user roles with dual management control (separation of duties).

Safeguarded Copy on IBM FlashSystem family and IBM SAN Volume Controller integrates with IBM Copy Services Manager software, starting with Copy Services Manager version 6.3.0.1, leveraging its automated, built-in copy and retention scheduling, testing and ease of recovery capabilities.

IBM Copy Services Manager also coordinates the Safeguarded Copy function across multiple systems to configure, manage, and monitor data-copy functions.

Copy Services Manager runs on Windows, AIX, Linux, Linux on z Systems, and z/OS operating systems, and can be used to plan for replication when provisioning storage, keep data consistent across storage systems if there is a planned or unplanned outage and monitor and track replication operations.

IBM Security QRadar

IBM 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 is one of the most popular SIEM solutions on the market today.

QRadar provides powerful cyber resilience and threat detection features such as centralised visibility, flexible deployment, automated intelligence, machine learning, proactive threat hunting, and much more.

The data management and storage features of IBM FlashSystem and IBM Spectrum Virtualize combined with log analysis, deep inspection, and detection of threats provided by IBM QRadar offer an excellent platform for hosting unstructured business data, reducing the impact of cyber threats, and increasing cyber resilience.

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.

And QRadar's open architecture enables third-party interoperability so that many solutions can be integrated, making it even more scalable and robust.

Additionally, QRadar's Network Insights delivers real-time scanning of network communications and deep analysis of network data to detect threat activity that could otherwise go unnoticed. The included custom rule engine focuses on providing deep analysis, alerts, and invaluable threat reports.

IBM QRadar can be deployed:

- On-premises as hardware, software, or a virtual machine.
- In your cloud of choice, including; AWS, Azure, IBM Cloud, or Google Cloud.
- As SaaS, with the backend infrastructure managed by IBM.
- Or as a managed service, with help from either IBM Managed Security Services and Covenco.

IBM QRadar Security Information & Event Management

IBM FlashSystem Cyber Vault

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.

When preparing a response to an attack, 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.

Solution use cases

By combining the capabilities of IBM Safeguarded Copy and IBM QRadar, organisations can develop comprehensive cyber resilience solutions that cover the Protect, Recover, and Detect functions of the NIST framework.

IBM FlashSystem can log all object activity in the access logs that contain all access information from storage objects. In order to identify and detect potential malicious access and for compliance auditing purposes, such access logs should be integrated with the SIEM solution

By combining IBM FlashSystem access logs, application logs, network or server logs, flow and packet data, and discovering unknown threat vectors using IBM Watson, IBM QRadar can provide 360-degree protection to enterprise data.

This solution addresses the following IT business security and resiliency challenges:

- Availability of immutable copies of data (safeguarded backups) that cannot be altered or deleted, or mapped to host
- Early threat detection for proactive data protection with logically, air-gapped immutable snapshots/backups
- Active monitoring for anomalies in user login activity, patterns, and operations (control and data path)
- Alerting IBM Spectrum Virtualize in the event of a detected threat to take a cyber resilience action to generate a safeguarded backup or prevent further user action.
- Timely identification and action to recover from your protected safeguarded backups

> "FlashSystem Cyber Vault is designed to help reduce cyberattack recovery time from days to just hours."

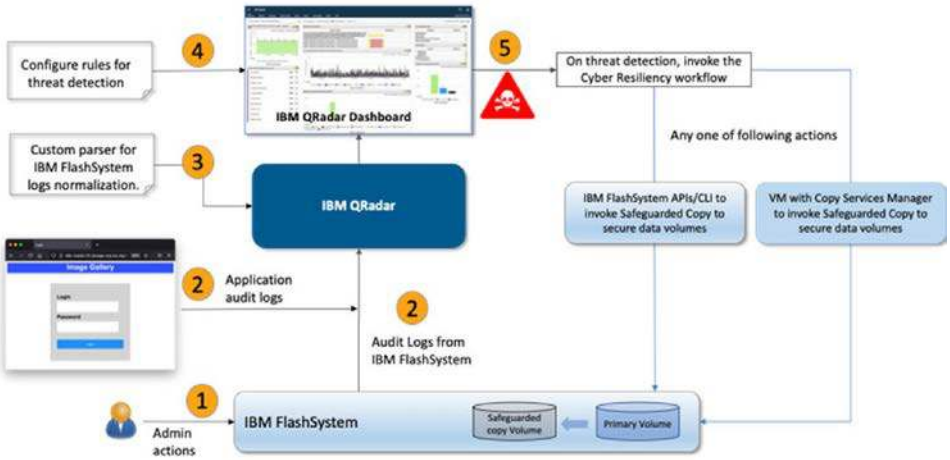
Deployment as a combined solution

The combined solution is straight forward to deploy:

- IBM FlashSystem is configured to forward audit logs to IBM QRadar. These logs contain information about every control path action including but is not limited to volume creation, deletion, resize, or user creation executed using both CLI or GUI.
- Similar to IBM FlashSystem, applications are also configured to log application-related events and forward them using the operating system's standard log forwarding mechanism.
- IBM QRadar is configured to receive any forwarded events, normalise them and persistently store them.
- When the logs are in IBM QRadar, an administrator can set various rules, map log relationships, and configure additional parameters to detect potential malicious data access.
- Based on analysis and threat detection, IBM QRadar can invoke custom scripts or cyber resilience workflow such as Safeguarded Copy invocation to protect the data.

IBM QRadar collects data from extensive data sources, then applies correlation and deep inspection to gain exceptionally accurate and actionable insights.

Once threats are identified, administrators can respond quickly to mitigate or reduce the impact of incidents and increase cyber resilience across the entire business application environment.



IBM QRadar and IBM FlashSystem cyber resilience solution overview

Cyber resilience assessments

In addition to the capabilities of IBM Spectrum Virtualize, IBM FlashSystem and IBM QRadar. Covenco and IBM Lab Services offer a Cyber Incident Response Assessment, consisting of a multi-phase approach that includes a workshop, implementation services, and health checks that help organisations assess their needs, develop strategies, and deploy and configure solutions to support cyber resilience.

Also, based on the NIST Security Framework, our Storage Cyber Resiliency Assessment Tool provides a bridge mechanism to evaluate your organisation's current data protection state, identify gaps, strengths, weaknesses, and provide recommendations to build an effective cyber resilience plan.

Call the Covenco team today to book your FREE Cyber Assessment: 01753 732 000

Email: sales@covenco.com

About Covenco

Covenco connects data management services with IT hardware supply and support. With over 34 years of experience in the IT industry, our team offers a reliable source of expertise for data centre administrators.

Covenco supports businesses with world-class data protection, backup, and disaster recovery services.

Our UK data centres have over two Petabytes of customer data under management at any time, and we are fully ISO27001 accredited for data security.

Contact Covenco

Covenco UK Ltd Head Office
Unit 3, MXL Centre, Lombard Way,
Banbury, Oxfordshire. OX16 4TJ
United Kingdom

Telephone: 01753 732000
Email: sales@covenco.com

https://covenco.com

covenco
DATA MANAGEMENT & INFRASTRUCTURE 365