Accelerating Ransomware Detection and Response

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

Highlights

- Deploy IBM Security QRadar for powerful AI-enhanced cyber threat detection
- Leverage IBM Safeguarded Copy to add extra layer of protection
- Take preventive action based on threat detection
- Speed recovery from an attack with IBM FlashSystem Cyber Vault

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 could exceed $6 trillion in in 2021 alone.[1] 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 confidential data to cripple organizations. Surprisingly, 34% of data breaches involve internal actors.[2]

Traditional approaches to data protection work well for their intended purposes but are not sufficient to protect against cyber-attacks, which can encrypt or otherwise corrupt your 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 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®,[4] 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. 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.

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[5]. 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. Now IBM QRadar can proactively invoke Safeguarded Copy to create a protected backup at the first sign of a threat.

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.

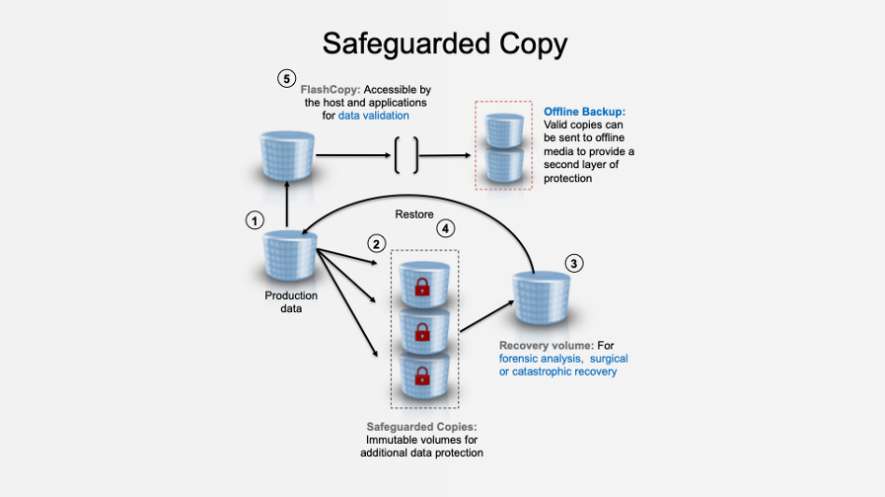
IBM Safeguarded Copy helps you recover quickly and with confidence if you should encounter one of the most pressing IT threats in the industry today, and since it’s available at no additional charge, start planning for Safeguarded Copy now.

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. It provides secure, point-in-time copies or snapshots of

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.

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.



IBM Safeguarded Copy architecture

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. 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.

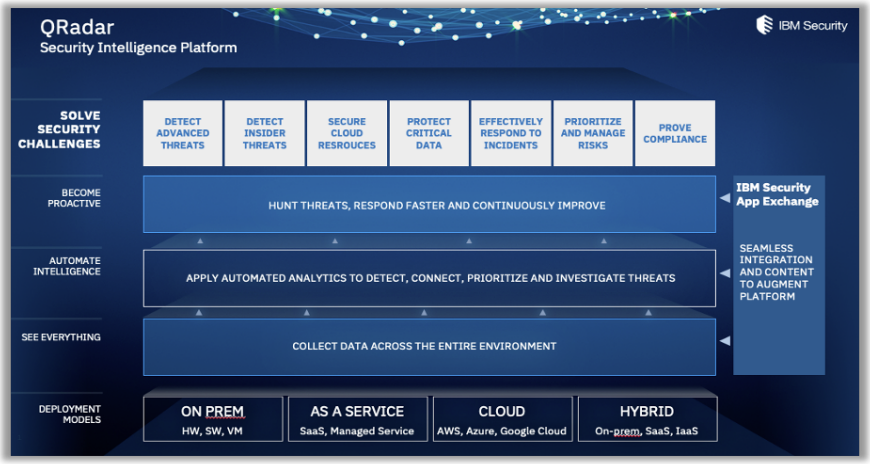
The data management and storage features of IBM FlashSystem and IBM Spectrum Virtualize combined with log analysis, deep inspection, and detection of threats provided by IBM QRadar offer an excellent platform for hosting unstructured business data, reducing the impact of cyber

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

IBM QRadar can be deployed:

- On-premises as hardware, software, or a virtual machine
- In your cloud of choice – 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 or any of our Managed Services Provider partners.



IBM QRadar Security Information and 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, organizations 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

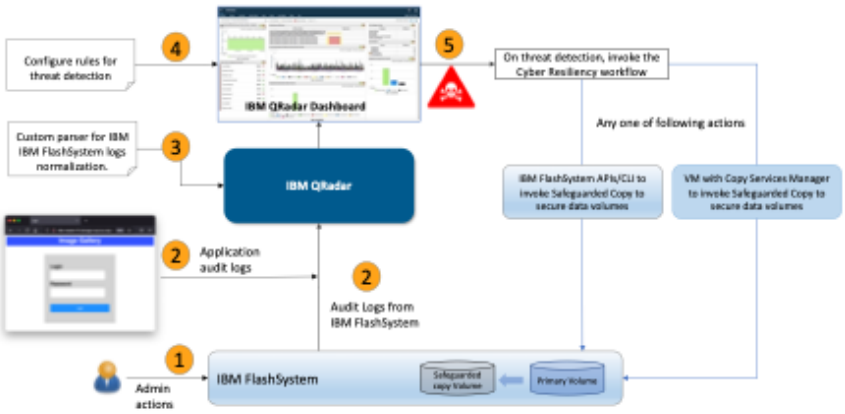
By combining IBM FlashSystem access logs, application logs, network or server logs, flow and packet data, and discovering unknown threat vectors using IBM Watson, IBM QRadar can provide 360-degree protection to enterprise data.

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

The combined solution is easy 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, normalize 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 and IBM FlashSystem cyber resilience solution overview

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.

Cyber resilience assessments

In addition to the capabilities of IBM Spectrum Virtualize, IBM FlashSystem and IBM QRadar. IBM Lab Services offers a Cyber Incident Response Assessment a multi-phase approach that includes a workshop, implementation services, and health checks that help organizations assess their needs, develop strategies, and 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 your organization's current data protection state, identify gaps, strengths, weaknesses, and provide recommendations to build an effective cyber resilience plan.

1. Morgam S. Nov 13, 2020. “Cybercrime To Cost The World $10.5 Trillion Annually By 2025”. Cybercrime magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2. Verizon: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

3. 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/

4. FlashSystem 5100, 5200, 7200, 9100/R, 9200/R.

5. Redbook: Enhanced Cyber Resilience Threat Detection with IBM FlashSystem Safeguarded Copy and IBM QRadar, https://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/redp5655.html?Open

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 representative or IBM Business Partner. If you need to be connected, fill out this form to schedule a consult with an IBM storage expert.

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, please contact your IBM Business Partner:

Horizon Computer Solutions