Bolstering cyber resilience with threat detection

Highlights

- Deploy IBM Spectrum Scale for innovative data management and protection
- Integrate IBM QRadar to add powerful AI-enhanced cyberthreat detection
- Include additional IBM Spectrum Storage solutions for enhanced protection
- Rely on validated solutions in IBM Redbooks to lower costs and risk

Build cyber resilience solutions that includes threat detection, as well as data protection and recovery

The financial impact of cyberattacks continues to rise. According to cybersecurity analyst firm Ponemon, the average cost of a data breach in 2019 was a staggering 3.92 million dollars per incident. Moreover, the chance of experiencing a data breach over the next two years has risen to 29.6%.[1]

For enterprises in the 21st century, the question of cyberattack is not if – but when.

Cyberattacks can happen in various ways. They may take the form of malware or ransomware targeted at stealing confidential data or holding valuable information for ransom. Sometimes these attacks are designed to destroy confidential data in order to cripple organizations. Surprisingly, 34% of data breaches involve internal actors.[2]

Cybersecurity is the discipline involved in protecting organizations from threats such as data fraud and cyberattacks. But what happens when cybersecurity efforts fail and digital systems are compromised, either accidentally or intentionally? This is the domain of *cyber resilience*, which refers to the preparation organizations make to deal with threats and vulnerabilities, the defenses that have been developed, and the resources available for mitigating security failures after the fact. Cyber resilience capabilities are essential in IT systems, critical infrastructure, business processes, organizations, societies, and nation-states.[3]

IBM Spectrum Scale is a state-of-the-art software-defined storage (SDS) solution that offers a long list of leading-edge data protection and security features. This massively parallel data management system with roots in the high-performance computing (HPC) world is currently deployed in high performance and computationally demanding environments such as the banking, financial, healthcare, oil and gas, and automotive industries and even in two of the fastest research-oriented supercomputers on the planet right now – Summit and Sierra – plus the fastest commercial supercomputer, Pangea III.[4]

Artificial intelligence (AI) is a powerful new technology being used to enhance cyber resilience. IBM has developed cyber resilience solutions that utilize the wide-ranging data management features of IBM Spectrum Scale, leverage other IBM Spectrum Storage solutions as needed to bolster specific capabilities, and add powerful AI capabilities through a new solution called IBM QRadar.

When combined, this suite of IBM SDS solutions with IBM Spectrum Scale as the foundational component offers great flexibility to address the full range of cyber resilience requirements using proven enterprise-grade components and powerful AI-driven capabilities.

Standards-driven cyber resilience

Organizations are discovering that traditional data security measures fail to provide desired levels of cyber resilience. More holistic approaches are being explored that integrate data, applications, and entire IT infrastructures to not only recover, but prevent – or at least minimize – the effects of security breaches. As part of this new trend toward more effective cyber resilience, the National Institution of Standards and Technology (NIST) has developed a policy framework providing guidance regarding how organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. This framework has become an industry-accepted methodology for building plans to develop and implement safeguards to ensure delivery of critical business services.

Among other aspects, the NIST framework offers a set of five cybersecurity functions:

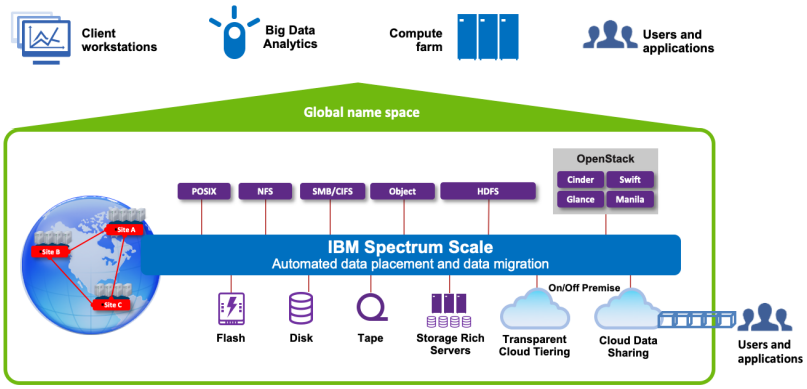
- Identify: In order to confidently restore business IT systems to their operational state after a security breach, organizations should clearly identify what must be protected, then develop and prioritize a protection plan.
- Protect: During the Protect stage, organizations should implement various safeguards such as identity management, access control, awareness and training, data security, code currency procedures, and data protection technology to ensure delivery of critical services.
- Detect: The best way to reduce impacts during a security breach is to detect it early, so business services can recover more rapidly.

- Respond: Refers to the development and implementation of the appropriate activities needed to contain the impact of a potential cybersecurity incident.
- Recover: In the Recover stage, organizations should develop and implement appropriate activities to restore any capabilities or services that were impaired due to a cybersecurity incident.

IBM cyber resilience solutions are designed using a standards-driven approach based on the NIST framework. IBM Spectrum Scale provides the features and functionality that organizations can use to address both the Protect function of the NIST cybersecurity framework and the Recover function. IBM QRadar, a leading intelligent security platform, easily integrates into IBM Spectrum Scale environments and provides AI-enhanced capabilities to address the Detect function of the NIST framework. Together, IBM Spectrum Scale and IBM QRadar can help organizations of all types and sizes build much more effective cyber resilience solutions.

Innovative data protection and recovery

Part of the IBM Spectrum Storage family of SDS solutions, IBM Spectrum Scale is an enterprise-grade parallel file system that provides superior resiliency, scalability, and control. It delivers scalable capacity and performance to handle demanding data analytics, content repositories, and technical computing workloads. Storage administrators can combine flash, disk, object, cloud, and tape storage into a unified system with higher performance and lower cost than traditional approaches.



IBM Spectrum Scale simplifies data management with integrated tools designed to help organizations manage petabytes of data and billions of files. It offers a full-featured set of file data management tools, including advanced storage virtualization, global collaboration for data-anywhere access that spans storage systems and geographic locations, and intelligent storage tiering. IBM Spectrum Scale is designed to support a wide range of application workloads at scale using a variety of access protocols and has been proven extremely effective in large, demanding environments. Today, it is installed in clusters supporting enterprise and HPC applications ranging from climate modeling and tornado simulation to big data MapReduce analytics, gene sequencing, digital media, and scalable file serving. It is deployed across environments as diverse as the financial, retail, digital media, and biotechnology industries, as well as in many science and government use cases.

As organizations move to multicloud environments and begin to adopt AI applications, the flexibility and data sharing capabilities of IBM Spectrum Scale have increased its popularity. For example, innovative transparent cloud tiering enables non-disruptive, intelligent data migration between flash, disk, tape, object, and even cloud storage tiers, helping enterprises more easily bridge data silos on-premises plus add the benefits of cloud storage to their overall data solutions. Adding IBM tape-based storage offers highly secure, cost-effective backup and archive WORM (write once, read many times) storage, with a true physical air gap for the ultimate protection against ransomware and cyberattacks.

IBM Spectrum Scale provides conventional cyber resilience and business continuity features such as snapshots, replication, encryption, and data immutability. In addition, its seamless integration with IBM Spectrum Storage SDS solutions such as IBM Spectrum Protect and IBM Spectrum Archive enables the implementation of wide-ranging backup and restore mechanisms for organizations that want to improve cyberthreat resolution, reduce costs, and deliver quick business systems recovery.

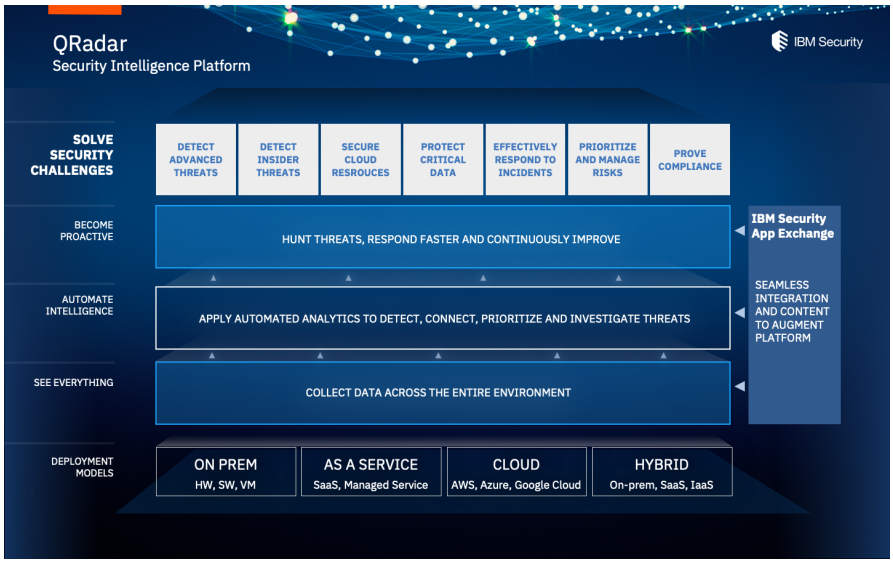
IBM Spectrum Scale also offers a number of innovative cyber resilience capabilities not found in other file management solutions. For example, it offers synchronous replication that optimizes data access and performance when replicas are separated across a wide area network (WAN). When WAN connections are not high-performance or are unreliable, an asynchronous approach to data replication is required. For this type of environment, you can use an IBM Spectrum Scale feature called Active File Management (AFM). AFM is a distributed caching technology developed by IBM Research that allows the expansion of the IBM Spectrum Scale global namespace across long geographical distances. It can be used to provide high availability between sites or provide local “copies” of data distributed to one or more IBM Spectrum Scale clusters and to provide policy management for increased business resiliency.

Another important cyber resilience capability is IBM Spectrum Scale File Audit Logging, which logs all access to the file system with required audit information. IBM Spectrum Scale file access logs can be securely directed to IBM QRadar in order to implement powerful capabilities for identifying and detecting potential malicious data access.

Powerful threat detection

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 Spectrum Scale-managed systems. It is one of the most popular SIEM solutions on the market today.[5] 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 Spectrum Scale combined with the 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 cyberthreats, 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, which makes it even more scalable and robust.



IBM QRadar

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.

And at each layer of the platform, applications from the IBM Security App Exchange can be added to augment threat detection and cyber resilience capabilities.

IBM QRadar is part of a new breed of SIEM solutions designed to address scenarios where people cannot analyze advanced threats using the normal monitoring tools. It collects events from different assets present in the environment, even picking up raw packets of data from the network for correlation. Furthermore, it provides session rebuilding capabilities for forensic analysis. IBM QRadar also integrates with IBM Watson for Security and multiple other third-party security feeds, further helping users orchestrate responses to unknown threat vectors.

Simple to deploy solutions

Combining the capabilities of IBM Spectrum Scale and IBM QRadar enables enterprises to build comprehensive cyber resilience solutions that address not only the Protect and Recover functions of the NIST framework, but also the Detect function as well. IBM has produced a solution Redbook that provides detailed descriptions and configuration guidance for designing and implementing powerful cyber resilience solutions based on IBM Spectrum Scale and IBM QRadar.

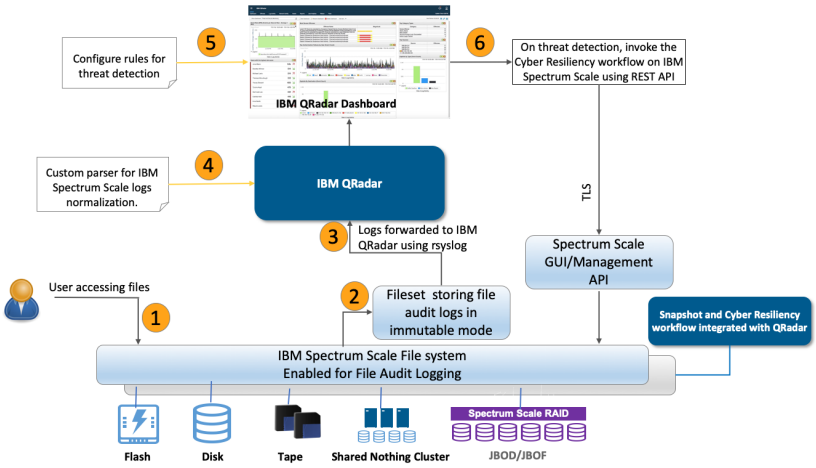
Enabling the IBM Spectrum Scale File Audit Logging function and directing the log data to QRadar allows it to run analyses to detect potential threats using its AI-enhanced capabilities. Then, based on predefined rules, QRadar can invoke cyber resilience workflows within IBM Spectrum Scale.

The combined solution is simple to deploy:

- IBM Spectrum Scale is configured and enabled for file audit logging for any given file system. This will generate file access audit logs that are stored on a dedicated, immutable IBM Spectrum Scale fileset.
- A dedicated IBM Spectrum Scale client node, part of the IBM Spectrum Scale network, is configured to forward the IBM Spectrum Scale file audit logs to IBM QRadar, which is then configured with parsing logic to interpret the log format, parse the logs, and persistently store the logs.

- 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 resiliency workflow on IBM Spectrum Scale

IBM QRadar compiles data from extensive data sources, then applies correlation and deep inspection to derive exceptionally accurate and actionable insights. Once threats are identified, administrators can quickly act on them to mitigate or reduce the impact of incidents and increase cyber resilience across the entire business application environment.



Cyber resilience with IBM Spectrum Scale and IBM QRadar

IBM Cyber Incident Response Services offers a broad spectrum of cyber resilience solutions, expertise, and resources, including setup and configuration of IBM Spectrum Scale and IBM QRadar-based solutions. IBM cyber resilience solutions leverage the capabilities of market-leading IBM Spectrum Storage software-defined infrastructure, along with IBM FlashSystem and IBM DS8900F storage systems. Together, these solutions can be used to build IT environments that are extremely resilient in the face of both cyberattacks and natural disasters.

Comprehensive Cyber Incident Response

Today, cyber resilience has become a crucial element in the design of successful business application environments. IBM offers a broad spectrum of cyber resilience solutions detailed in solution Redbooks and based on standards such as the NIST security frameworks. IBM Spectrum Scale is a popular high-performance data management system that offers many data protection and cyber resilience features. When IBM QRadar is integrated with IBM Spectrum Scale, enterprise cyber resilience expands from simply protecting data and recovering from cyber incidents to proactively detecting cyberthreats and reducing their impacts. Comprehensive cyber resilience approaches such as those offered by IBM Spectrum Scale and IBM QRadar are how modern business can thrive in a world of constantly evolving digital hazards.

[1] Ponemon: Cost of a Data Breach Report 2019 https://www.ibm.com/security/data-breach?lnk=ushpv18l1

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

[3] TechTarget, WhatIs.com: cyber resilience: https://whatis.techtarget.com/definition/cyber-resilience

[4] IBM Infrastructure website: The world's most powerful supercomputers https://www.ibm.com/it-infrastructure/power/supercomputing

[5] IBM Redbooks: Enhanced Cyber Security with IBM Spectrum Scale and IBM QRadar, 2019 ISBN 0738458015

Why IBM?

IBM Storage for cyber resiliency 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.

For more information

Certified BP Business Partners and IBM Storage Lab Services have the expertise and technical consultants to help you turn your business into a cyber resilient organization.

Contact your IBM Business Partner or IBM Representative to learn more.