Technical Validation

IBM Storage Delivers Effective and Efficient Cyber Resilience

Cyber Resilience Features and Capabilities of IBM Spectrum Storage Software-defined Solutions and IBM Storage Systems

By Jack Poller, ESG Senior Analyst

March 2021

This ESG Technical Validation was commissioned by IBM and is distributed under license from ESG.

Contents

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

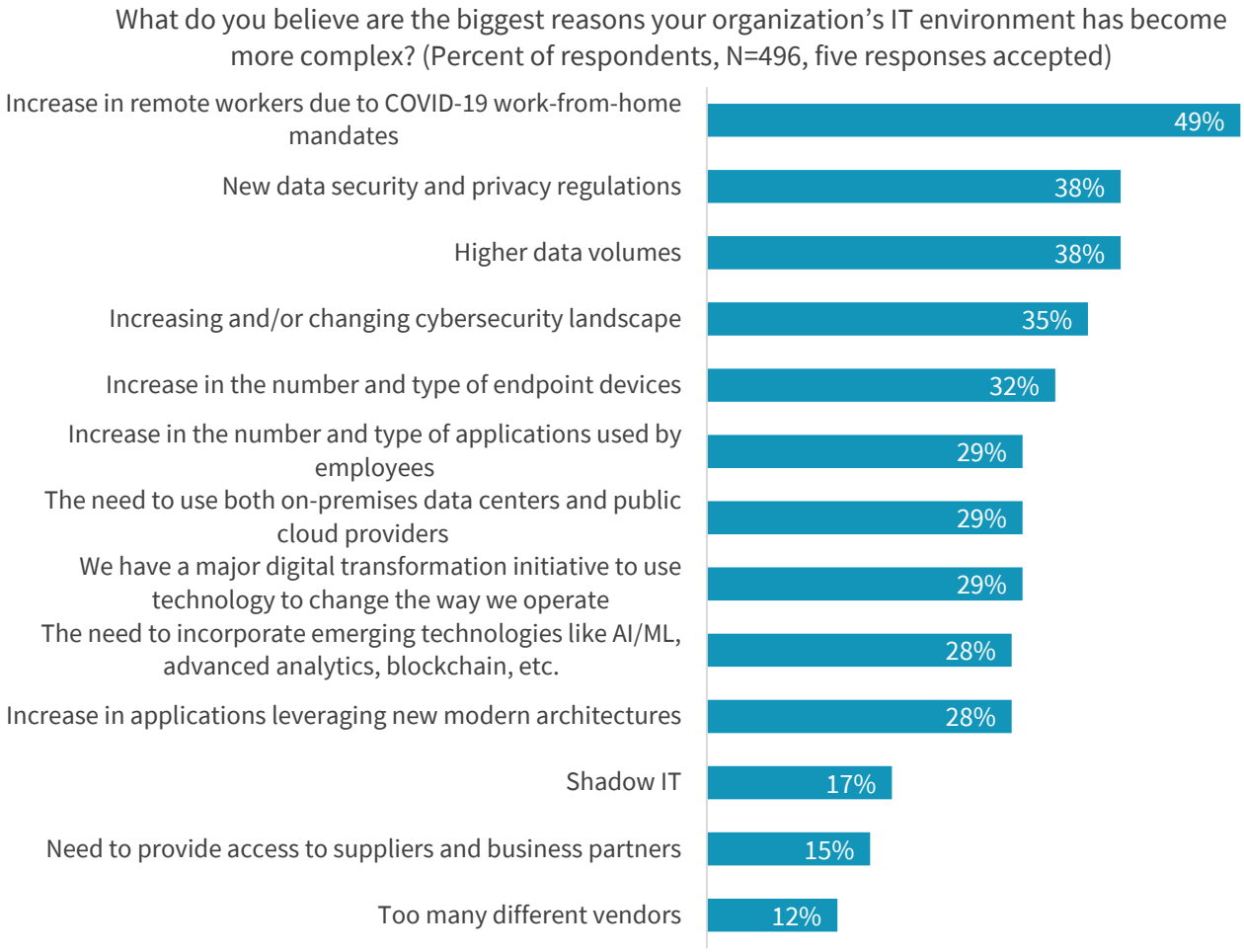
Introduction

This ESG Lab Report documents evaluation of the cyber resilience features and capabilities of selected IBM Storage products. We focused on how IBM Storage products help organizations address each of the five key elements of an effective cyber resilience strategy.

Background

When it comes to implementing effective cyber resilience, one of the biggest hurdles turns out to be IT complexity. In fact, according to ESG research, three-quarters (75%) of IT decision makers believe that their IT environments have grown more complex in the last two years. This perspective is very understandable, as data and applications extend from traditional architectures constructed behind data center firewalls out to include multiple public cloud resources and providers, more employees work from home or from any location around the globe using multiple devices and collaboration platforms, and a barrage of new technologies such as containers and artificial intelligence (AI) sweep across the technology landscape. As illustrated in Figure 1, add to these drivers of IT complexity the increasing volume and sophistication of cyber-attacks and the relentless increase in data volumes—and it's no wonder that IT appears more complicated than ever. [1]

Figure 1. Drivers of IT Complexity



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

Modern hybrid multi-cloud IT environments dramatically increase the attack surface of exposure to cyber threats. IT complexity tends to exacerbate the shortage of IT skills that currently plagues organizations and amplifies data breach costs. For example, according to Ponemon Institute research sponsored by IBM, system complexity adds $290K while third-party involvement in IT infrastructures increases the cost of a data breach by $207K.[2]

To help guide planning and implementation of effective modern cyber resilient solutions, organizations can adapt the cybersecurity framework provided by the National Institute of Standards and Technology (NIST) into a framework for the five elements of cyber resiliency:

- 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 and Recover—In the Respond and Recover stages, organizations should develop and implement appropriate activities to mitigate attacks and restore any capabilities or services that were impaired due to a cybersecurity incident.

The IBM Storage solutions for Cyber Resilience

IBM provides a comprehensive portfolio of end-to-end cyber resilient software-defined and hardware storage solutions that help organizations efficiently identify, detect, protect, respond, and recover from cyber-attacks. By providing multi-layered security and highly resilient functionality, this portfolio maximizes data resilience capabilities to help organizations significantly reduce the risk of business disruption and financial losses due to user errors, malicious destruction, or ransomware attacks. IBM solutions, as well as their cyber resiliency capabilities, are listed below.

[2] Source: *2020 IBM Cost of a Data Breach Report.*

Table 1. IBM Solutions

IBM Solution	Description	Cyber Resiliency Capabilities	Identify	Protect	Detect	Respond	Recover
IBM FlashSystem Storage	All-flash and hybrid storage based on Spectrum Virtualize with encryption, replication, and IBM FlashCopy snapshots for space-efficient immutable copies of data. Enables quick restores and accelerates recovery from unauthorized data modification.	Encryption; Immutable		✓		✓	✓
IBM DS8900F Storage	High-capacity, high-performance all-flash storage, supporting continuous operations, immutable storage, and recovery using many immutable recovery copies across multiple volumes or storage systems, with the ability to prevent ransomware attempts to delete or modify data. Provides secure authentication and encryption in flight for IBM Z environments.	Encryption; Immutable		✓	✓	✓	✓
IBM Cloud Object Storage and IBM Spectrum Discover	Cloud-based object storage for archiving and data protection, providing immutable storage using WORM technology with the ability to specify legal holds and retention periods at an object level. The IBM Spectrum Discover description is below.	Encryption; Immutable	✓	✓		✓	✓
IBM Tape Storage	Tape cartridges physically air gap data because they are offline. Virtual tape libraries can provide logical WORM storage.	Encryption; Immutable; Air gap		✓		✓	✓
IBM Spectrum Archive	Features the IBM Linear Tape File System (LTFS) format standard to provide direct, intuitive, and graphical access to data stored on tape cartridges.	Encryption; Immutable; Air gap		✓		✓	✓
IBM Spectrum Copy Data Management	Identifies and manages multiple data copies, provides data protection for hybrid cloud environments, and can recover data in an isolated network.	Discovery; Data management; Encryption	✓	✓		✓	✓

IBM Solution	Description	Cyber Resiliency Capabilities	Identify	Protect	Detect	Respond	Recover
IBM Spectrum Protect Portfolio	Leveraging IBM's long history with data protection, including inventing tape and other removable media solutions, IBM Spectrum Protect supports physical systems, VMs, containers, applications, and multiple cloud services. The software-defined storage solution can store data on flash, disk, cloud object storage, and physical tape and can detect malware and ransomware activity by identifying large deviations from typical backup workload patterns.	Detection Access control; Backups; Data management; Encryption; Immutable; Air gap	✓	✓	✓	✓	✓
IBM Spectrum Scale	Data recovery using snapshots and synchronous and asynchronous replication. IBM Spectrum Scale can work in combination with IBM QRadar to detect potential threats using AI-enhanced capabilities. The IBM Spectrum Discover description is below, and the IBM Spectrum Archive description is above.	Encryption; Immutable; Threat detection	✓	✓	✓	✓	✓
IBM Transparent Cloud Tiering (TCT)	Enables hybrid clouds as an additional storage tier and provides logical air gapping for data protection and recovery.	Encryption; Air gap		✓		✓	✓
IBM Spectrum Discover	Enables companies to rapidly identify and categorize large-scale, heterogeneous data repositories using metadata management.		✓				
IBM Cyber Resiliency Services	Helps organizations assess their needs and develop and implement cyber resilience strategies and integrated solutions across storage and security.		✓	✓	✓	✓	✓

Source: Enterprise Strategy Group

ESG Technical Validation

ESG evaluated the cyber resiliency capabilities of the IBM Storage portfolio. We focused on product features and capabilities related to discovering and managing sensitive data (Identify), protecting applications and valuable organizational data (Protect), detecting cyber intrusions and threats (Detect), and responding to and recovering from various cyber incidents (Respond and Recover).

Identify

Modern IT environments have grown so complex that discovering and cataloging all the data sets, application instances, and IT infrastructure components have become substantial challenges. Many companies have been deluged by so much business-generated data that they can't keep track of it all—or they don't know as much about their data assets as they

should in order to protect these valuable assets. Where does any particular data asset reside? What specifically is contained in each of those thousands or millions of files? How old is it? Who has access to it—and should they? Is it compliant with the latest regulations? Thus, we started with the ***Identify*** element of the cyber resiliency framework.

The IBM Spectrum Protect Plus proactive catalog and global search enables administrators to ensure they are protecting all the right data and quickly identify the data they want to recover across multiple VM hosts, file systems, hypervisors, applications, and containers.

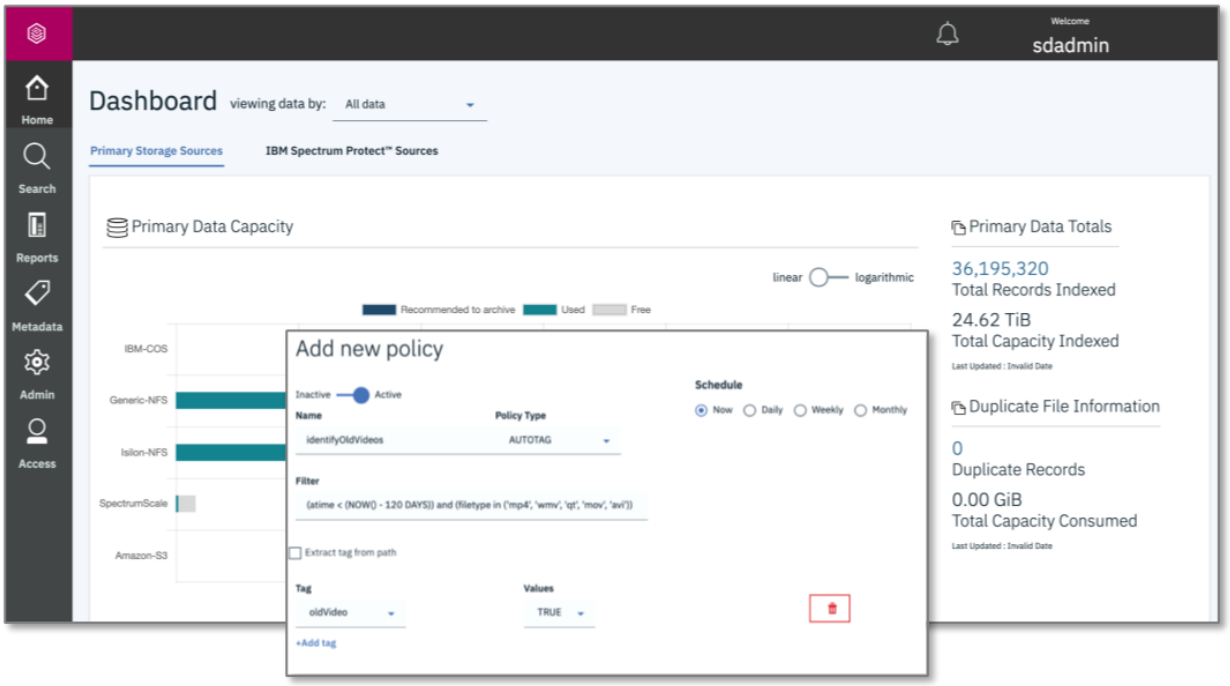
IBM designed IBM Spectrum Discover to be an extensible platform providing exabyte-scale data ingestion, identification, visualization, activation, and business-oriented data mapping from across the enterprise. The solution provides a precise view of the "who, what, where, when, and why" aspects of an organization's data across all data storage systems.

IBM Spectrum Discover is an on-premises interactive data management catalog that offers a detailed, real-time view of data. It's non-disruptive to existing storage and applications and provides the ability to create custom indexes and reports for identifying and optimizing enterprise data. IBM Spectrum Discover works across file, object, backup, and archival systems and synchronizes with related members of the IBM Spectrum Storage family, such as IBM Spectrum Scale in massive file systems; IBM Cloud Object Storage where substantial portions of modern unstructured data is stored on-premises and in the cloud; IBM Spectrum Protect, which manages data backups and other cyber resilience functions; and IBM Spectrum Archive in tape systems used to create air-gapped data protection schemes.

IBM Spectrum Discover can analyze backed up/archived data from IBM Spectrum Protect, extracting metadata from the IBM Spectrum Protect catalog to drive analytics of the back data, improving overall data protection storage utilization.

IBM Spectrum Discover automatically captures system metadata from source storage systems, creates custom metadata based on user-defined policies, and enables more advanced use cases such as deep content inspection and extraction of metadata from file headers and content using its Action Agent API. The result is a rich layer of file and object metadata that is managed using one centralized solution. Available as a VMware virtual appliance, IBM Spectrum Discover can be easily deployed to perform large-scale data analytics, enable better data governance, and help optimize the value and management of nonstructured data assets.

Figure 2. IBM Spectrum Discover Data Identification



Source: Enterprise Strategy Group

IBM engineered IBM Spectrum Discover to export metadata gathered on-premises to the cloud-based IBM Watson Knowledge Catalog and leverage IBM Watson AI solutions. IBM Watson Knowledge Catalog is an open, AI-driven data catalog for managing enterprise data and AI model governance, quality, and collaboration. The Catalog provides a gateway to other tools, such as Watson Studio and Watson Machine Learning, that together provide wide-ranging data identification, security, research, governance, self-service, and data lake management services.

Why This Matters

Because IT ecosystems have grown so complex, discovering and identifying every element in these environments has become a crucial ongoing endeavor at the core of any effective cyber resilience strategy. You can't protect what you don't know exists.

ESG found that IBM Spectrum Discover enables organizations to automatically find and classify corporate data assets. IBM Spectrum Copy Data Management increases organizational efficiency by identifying and cataloging information from local, hybrid cloud, and off-site cloud infrastructure, providing comprehensive visibility of objects, object copies, and their locations. By deploying these IBM solutions, organizations can leverage data mapping, data discovery, data set identification, duplicate data removal, data inspection, and data classification to effectively implement the Identify element of the cyber resilience framework.

Protect

IBM has enhanced and adapted its traditionally architected data protection solutions to adopt a new data resilience approach that provides continuous access to data no matter where that data resides, protecting critical information in the event of a system failure, human error, malicious behavior, or a natural disaster.

The data resilience portfolio includes IBM Spectrum Protect, IBM Spectrum Protect Plus, and IBM Spectrum Copy Data Management (CDM). Each can be deployed as a standalone solution, and together, this data resilience portfolio unifies data protection, backup, recovery, retention, and reuse for physical, virtual, and container workloads in multiple different environments.

IBM Spectrum Protect helps admins protect traditional, cloud, and virtualized environments and systems of all sizes from a single point of control. It can recover a myriad of applications, databases, files, and file systems. IBM Spectrum Protect Snapshot, a component of IBM Spectrum Protect, uses storage system snapshots to backup and restore data, including DB2 and Oracle databases.

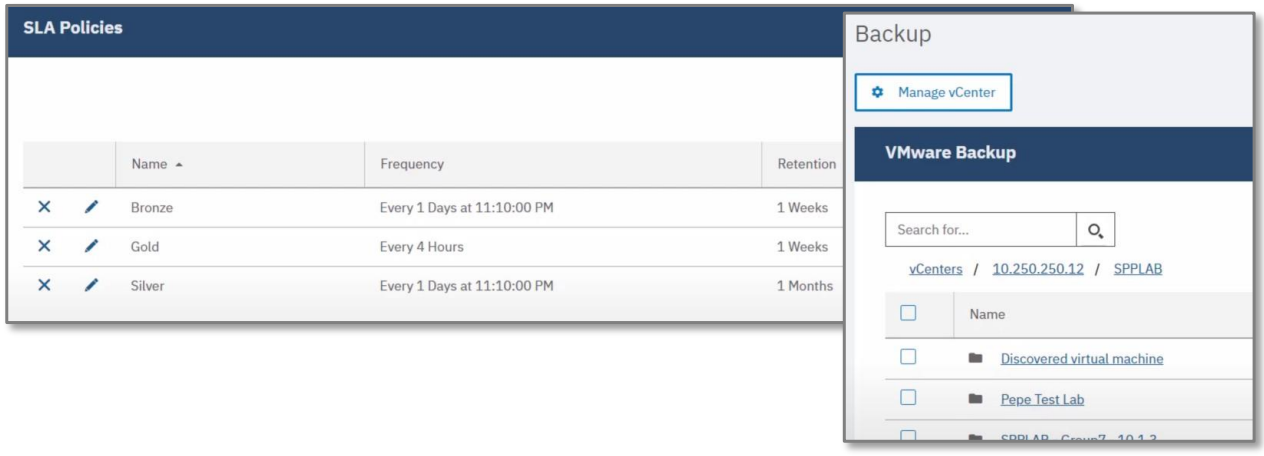
IBM Spectrum Protect container storage pools leverages cloud object storage without additional hardware or cloud gateways and supports IBM Cloud, IBM Cloud Object Storage, Amazon S3, Microsoft Azure Blob Storage, Google Cloud Storage, and other validated S3 object storage devices and services. These storage pools include high-performance in-line data deduplication and compression for efficient use of storage and network capacity, as well as encryption to secure data in transit and at rest. For maximum cost flexibility, IBM Spectrum Protect supports a broad choice of options for backup data storage including flash, disk, tape, public cloud services, and on-premises object storage.

IBM Spectrum Protect Plus provides near-instant recovery, replication, reuse, and retention for VMs, databases, file systems, SaaS workloads, applications, and containers in hybrid cloud environments. The solution is easy to deploy as a virtual appliance and the agentless architecture is easy to maintain. SLA-based policies automate data protection processes, including operational backups, data replication, and data retention. Role-based access control (RBAC) and application integration enable self-service data reuse to improve the speed and efficacy of data protection.

The entire data protection lifecycle—backups, data reuse, replication, and data offload—are all managed using SLA policies. This single, easy-to-use, common user interface provides end-to-end policies that automate backup processes, including operational data recovery, data replication, and data retention.

IBM Spectrum Protect Plus increases data protection and retention efficiency for cyber incident recovery by leveraging snapshots and incremental forever technologies, along with data encryption, compression and deduplication. Data is stored in native formats so administrators can rapidly restore data, while data owners have quick access to copies. Using write-once-read-many (WORM) object storage technology and the ability to air-gap data on physical tape via integration with other IBM Spectrum Protect offerings enhances cyber resilience data protection.

Figure 3. IBM Spectrum Protect Plus Data Protection SLAs



Source: Enterprise Strategy Group

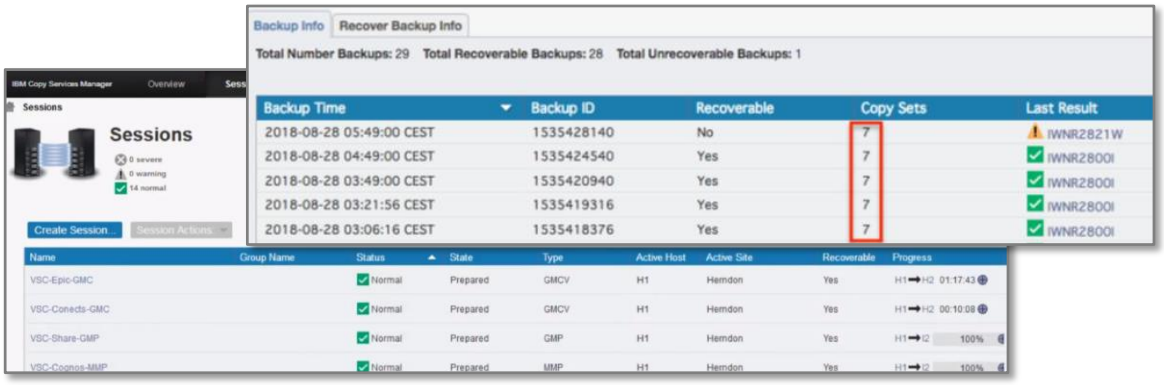
IBM designed IBM Spectrum Protect Plus to simplify protection for containerized workloads. Organizations can easily back up, recover, and retain persistent container volumes by utilizing pre-defined policies, and container storage interface (CSI) snapshots. Admins can create policies to schedule persistent volume snapshots, backups, replication to secondary sites, and copying data to object storage or IBM Spectrum Protect for secure long-term data retention.

Logical Corruption Protection

Logical Corruption means that the all-hardware components are working as expected, but data becomes destroyed or corrupted on a content level. Logical corruption cannot be prevented with traditional high availability or disaster recovery solutions, which are not content-aware. In fact, continuous replication solutions, such as Metro Mirror or Global Mirror, would quickly propagate any content-level corruption to all copies. To combat logical corruption, organizations need a paradigm shift from a pure availability mindset to cyber resilience.

IBM DS8900F storage solutions include Safeguarded Copy, a technology IBM designed for logical corruption protection (LCP) by enabling immutable points of data recovery that are hidden and protected from being modified or deleted due to user errors, malicious destruction, or ransomware attacks. These immutable copies are a secure source of data that organizations can use for forensic analysis and recovery from either surgical or catastrophic events.

Figure 4. IBM DS8900F Safeguarded Copy



Source: Enterprise Strategy Group

Safeguarded Copy supports up to 500 backup copies per production volume for data restoration in case of logical corruption or destruction of primary data. Copies can be maintained at either production or recovery sites. Safeguarded Copy protects storage targets from malicious actions with additional security provided through different user roles and authority levels. Admins can integrate Safeguarded Copy with multiple cyber incident recovery and high availability configurations. Safeguarded Copy also prevents backup data from being compromised, either intentionally or deliberately, such as accidentally deleting volumes.

IBM's Z mainframe solutions integrate with IBM DS8900F storage to implement pervasive encryption, which encrypts data at the host, in-flight, at rest in the storage system, and in the hybrid cloud.

Why This Matters

Data protection is a key element of cyber resiliency, and is so critical to maintaining business operations that, despite the pandemic, 50% of organizations plan to increase their investment in data protection in 2021.[3]

ESG found that organizations can use the IBM Spectrum Protect Portfolio to protect critical data assets in traditional data storage, databases, applications, and containers. An easy-to-use interface and SLA-based policies help organizations continuously protect data and store backups using WORM technologies, providing an additional layer of protection. In addition, IBM DS8000's features such as pervasive encryption and safeguarded copy ensure data and backups are hidden from prying eyes.

ESG validated that IBM Safeguarded Copy for DS8900F can protect data from logical corruption by creating immutable and hidden copies of data. This content-aware protection prevents logical corruptions from propagating to replicated storage or backups.

ESG validated that organizations can deploy the IBM suite of data protection to implement the Protect element of the cyber resiliency framework.

Detect

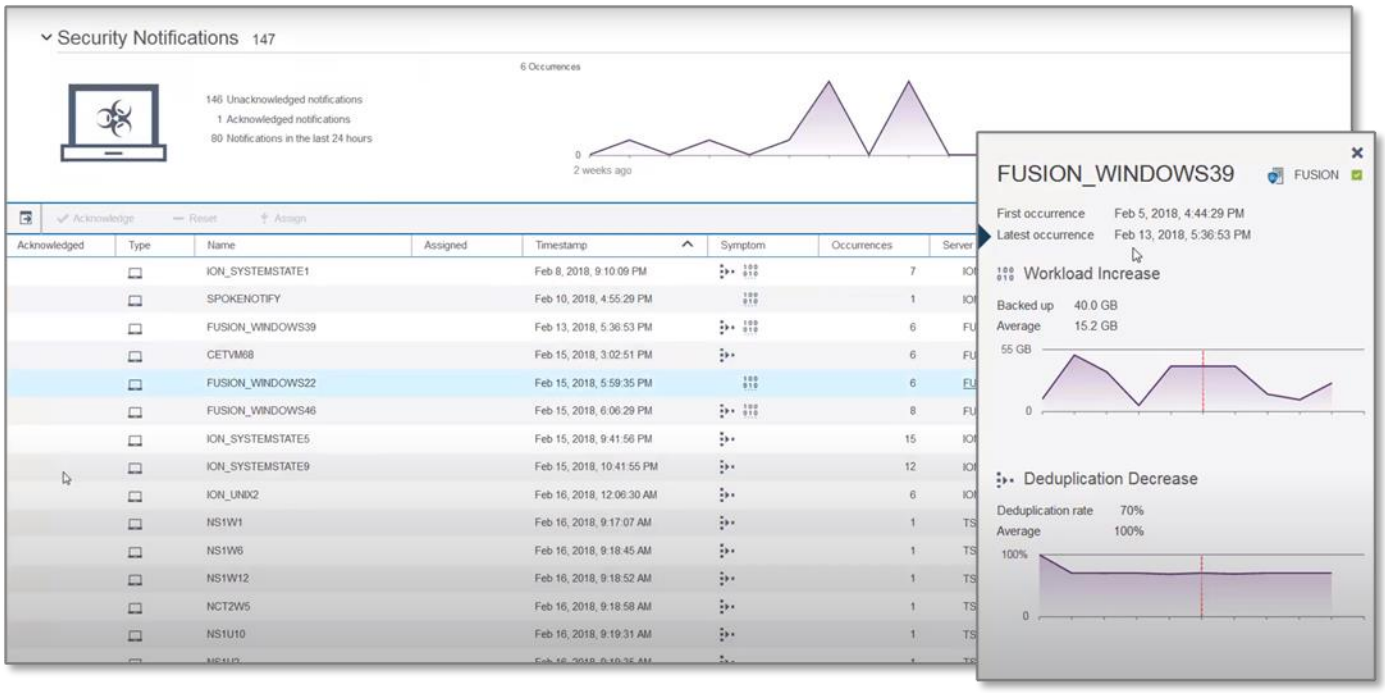
Even with the best security, data breaches—via attack or negligence—still occur. And when they do, organizations must detect them as quickly as possible to limit damage and data exfiltration. Both IBM Spectrum Protect and IBM QRadar provide threat detection capabilities.

IBM Spectrum Protect detects anomalies in data protection workload patterns to alert administrators of potential ransomware infections. As a result of ransomware encrypting data, many, if not all, files are modified and will be copied during the next backup. Similarly, these newly encrypted files cannot be deduplicated or compressed. Thus, IBM Spectrum protect alerts administrators whenever a systems backup volume increases by a large amount or the deduplication rate decreases by a large amount (25% by default).

The IBM Spectrum Protect Security Notifications dashboard, shown in Figure 5, provides an at-a-glance summary of potential ransomware infections along with a detailed list of each affected system. Clicking on a system drills down for more information, showing the actual workload increase and deduplication decrease. Administrators can use the alerts to trigger forensic investigation and remediation efforts.

[3] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

Figure 5. IBM Spectrum Protect Security Notifications



Source: Enterprise Strategy Group

IBM designed IBM QRadar as a security information and event management (SIEM) system to monitor, inspect, detect, and derive insights for identifying potential threats to the data stored on IBM Spectrum Scale and IBM Spectrum Virtualize-based storage systems. IBM QRadar provides centralized visibility, flexible deployment, automated intelligence, machine learning, proactive threat hunting, and more, and these features improve an organization's cyber resilience.

IBM QRadar applies heuristics and artificial intelligence (AI) across a variety of data sources, including access logs, network logs, server logs, network flow, packet data, user behavioral records, and more, to detect potentially malicious behavior. Security analysts can perform complex queries to correlate and aggregate disparate data spanning long time frames, which aids hunting of advanced persistent threats, forensic investigations, and identification of root causes.

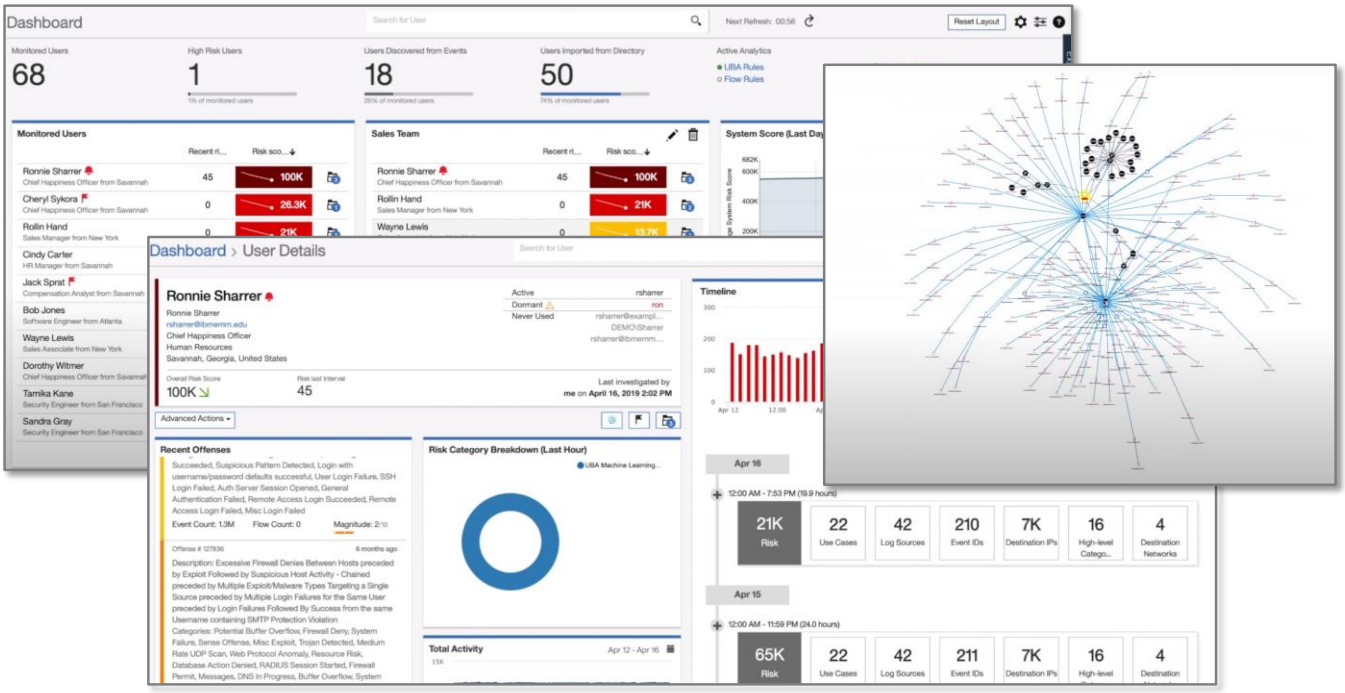
The benefits of cross-correlation and analysis of data, assets, and activity across the entire infrastructure include real-time and historical threat detection based on rules, exposing hidden indicators of attack (IOA) and indicators of compromise (IOC). IBM QRadar establishes a known baseline of network and user activity. Network analysis identifies changes in network traffic that indicate new and possibly unauthorized network entities along with abnormal communications between existing hosts, which may be a sign of lateral movement of malware across the infrastructure. User behavior anomaly detection identifies deviations from baseline that are indicative of suspicious activities.

Most cybersecurity threat detection and prevention tools and techniques are focused on threats emanating from outside the organization. Cyber resilience requires that organizations also detect insider threats—risks to the organization's infrastructure and data caused by inadvertent or malicious employee and contractor behavior.

IBM QRadar's user behavioral analysis (UBA) helps detect these insider threats. The UBA dashboard provides an at-a-glance overview of high-risk and monitored users, along with the list of users ordered by risk. This enables security analysts to triage and prioritize their activities. Clicking on a user drills down for the key details of the user's risky behavior, showing the timeline, recent offenses, and more.

To aid the threat detection and forensic investigation, IBM QRadar creates a navigable map of the user's activity, showing all the entities the user has communicated with, the direction of the data flow, documents exchanged, and more. Analysts can zoom into event of interest to get more information and gain an understanding. Using IBM QRadar, the analyst can quickly determine whether anomalous behavior is malicious or benign.

Figure 6. IBM QRadar User Behavioral Analysis



Source: Enterprise Strategy Group

Why This Matters

Ransomware represents a small portion of the large volume of sophisticated threats targeting businesses, and more than one quarter (29%) of organizations experience weekly or daily ransomware attacks. And while most security tools focus on external threats, organizations must not lose sight of the potential damage caused by insiders.[4]

ESG validated that IBM Spectrum Protect can detect ransomware by identifying a rapid increase in backup volume with a concomitant decrease in deduplication. These two metrics are good indicators that ransomware is encrypting data, and IBM Spectrum Protect alerts administrators, enabling rapid investigation and mitigation.

ESG also validated that IBM QRadar aggregates and correlates security information and event data. Heuristics and AI algorithms enabled detection of multiple threats. User behavioral analysis established a baseline for known good activities and identified anomalies representing suspicious behavior. Using IBM QRadar, we could drill down to get details of user activity including which files were transferred to which systems. This enabled us to determine whether suspicious activity was malicious or benign.

[4] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, February 2020.

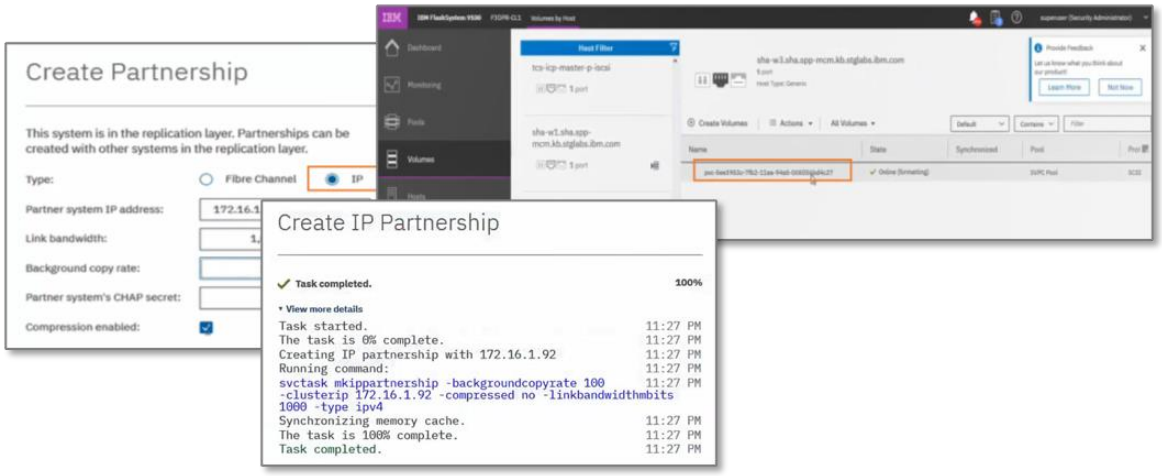
Respond and Recover

IT architects and decision makers may think that responding and recovering from a cyber incident requires an investment in a panoply of bolt-on tools and extra technologies. However, organizations can achieve efficient effectiveness by deploying IT storage infrastructure solutions that inherently provide response and recovery across their environment.

IBM Spectrum Virtualize enables administrators to deploy consistent replication services across all systems regardless of the type of storage being used. IBM Spectrum Virtualize and IBM Spectrum Virtualize for Public Cloud together support mirroring data between on-premises and cloud or between cloud data centers. Admins can use these features to ensure consistent data management between on-premises and public cloud storage, implement real-time disaster recovery strategies, and ensure the integrity of cloud-resident data using AWS "air-gap" snapshots to S3.

Using IBM Spectrum Virtualize and IBM Spectrum Virtualize for Public Clouds, admins can create partnerships and data replication between on-premises and hybrid cloud environments. Once configured, organizations can use these partnerships to replicate and migrate data, implementing recovery strategies to ensure operations continue during and after a cyber incident.

Figure 7. IBM Spectrum Virtualize Partnerships and Data Replication for Cyber Incident Recovery



Source: Enterprise Strategy Group

The FlashCopy feature creates almost-instant snapshots of active data that admins can use to further increase efficiency and run multiple backup and restore operations in parallel. Admins can also leverage FlashCopy with two IBM Spectrum Virtualize systems using a Metro Mirror connection to synchronously replicate data across metro-area-wide distances with automatic failover and no data loss. In this configuration, IBM Spectrum Virtualize writes data to both systems before sending an I/O acknowledgement to the issuing host.

The Global Mirror feature enables data replication over greater distances without affecting overall performance. Global Mirror periodically creates a point-in-time FlashCopy snapshot at the recovery site without disrupting the I/O to the source, thus providing a continuously updating, nearly up-to-date data backup. Global Mirror provides support for virtually unlimited distances between the sites, enabling organizations to locate sites based on business needs.

Using the IBM HyperSwap feature, servers in two or three data centers can concurrently access data with automated switch-over in case of failure. When combined with server data mobility functions such as VMware vMotion or IBM PowerVM Live Partition Mobility, HyperSwap technology enables non-disruptive storage and VM mobility between data centers that can be up to 300 km (186 miles) apart.

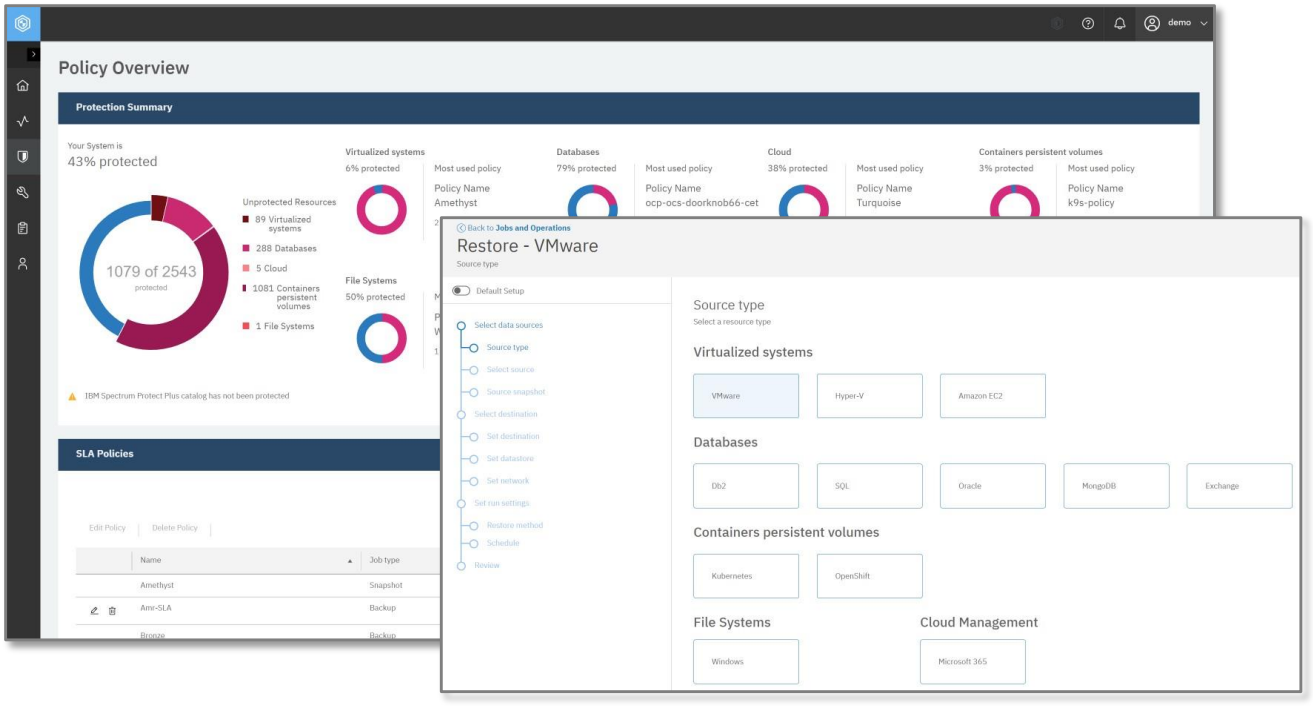
IBM Spectrum Protect enables advanced data protection for cloud, virtualized, and software-defined environments; core applications; and remote facilities. Data managed by IBM Spectrum Protect is replicated to offsite recovery facilities for safekeeping, enabling fast, flexible restores from primary and remote recovery sites to help recover individual items, complex systems, and entire data centers.

IBM Spectrum Protect can also be a data copy target for IBM Spectrum Protect Plus, enabling clients to leverage existing investments for long-term data retention and disaster recovery. Data encryption and native support for tape and immutable object storage enhance protection and ensure cyber resilience. Key administration commands offer tighter security and require dual authorization to prevent data loss.

IBM Spectrum Protect Plus provides near-instant recovery, replication, retention, and reuse for VMs, databases, and containers in hybrid cloud environments. The solution is distributed as a virtual appliance that simplifies deployment and maintenance. Organizations can recover from a cyber incident through restoring archival data copies stored in cloud object storage or on IBM virtual or physical tape (via IBM Spectrum Protect) with air gapping or WORM technology, which prevents inadvertent or malicious corruption of archival data copies.

The dashboard ensures that admins have up-to-date status information and can determine which systems, databases, containers, and cloud storage systems are unprotected. Admins control protection and recovery through SLA policies. IBM Spectrum Protect Plus simplifies recovery through a wizard interface that proceeds step-by-step through the recovery process. Using the Wizard, admins select data source type, location, and specific snapshot to be recovered. Next, the admins select the destination system, data store, and network and schedule the recovery operation.

Figure 8. IBM Spectrum Protect Plus Policy Dashboard and Recovery Jobs



Source: Enterprise Strategy Group

Why This Matters

Organizations invest efforts to identify and protect data and detect threats and attacks to facilitate and improve the recovery of business operations after a cyber incident. The success of the Respond and Recover elements are the measure of all other phases of the cyber resilience framework. When designing and building solutions for response and recovery, rather than bolting on additional components that may add cost, complexity, and risk, organizations can increase efficiency and effectiveness by leveraging the inherent capabilities of existing infrastructure.

ESG found that deploying IBM Spectrum Virtualize enables organizations to replicate data between on-premises data centers and the cloud. Features such as FlashCopy, Global Mirror, and HyperSwap enable organizations to shrink RPO, minimizing data loss and accelerating resumption of business operations during cyber incidents. We also found that IBM Spectrum Protect Plus simplified the backup and recovery process, increasing efficiency and enabling us to easily restore operations by restoring systems, VMs, containers, databases, and applications from local or remote archival data copies.

The Bigger Truth

It's clear that a strong correlation exists between IT complexity and vulnerability to cyberattacks. And as IT grows more complex, cyberattacks will increase in frequency and cost. The truth is, given enough time and effort, anything can be breached. This explains why organizations are shifting focus and resources to moving beyond cybersecurity toward a more comprehensive data and business security posture called cyber resilience.

Protection of valuable data assets is an important goal—but ensuring the overall cyber resilience of the organization is now becoming more important, as more than half (53%) of organizations say they are spending more now to implement long-term technology strategies that will give them a more flexible and resilient IT infrastructure in the event of future major business disruptions.[5]

IBM has developed an extensive suite of storage and data protection solutions to help proactive organizations implement comprehensive cyber resiliency. The IBM solutions incorporate all facets of a complete cyber resilience storage strategy—data discovery, ransomware detection, encryption, immutable storage, air gapping, and multiple recovery options to enable organizations of any size to increase their cyber resilience and improve their ability to identify, protect against, detect, respond to, and recover from cyber incidents.

The results that are presented in this document are based on demos and evaluation of products in controlled environments. Due to the many variables in each production data center, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

If your organization is looking to implement a cyber resilience strategy, then ESG believes you should consider how IBM storage solutions can help you efficiently and effectively achieve your cyber resilience goals.

[5] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.