COHESITY & AWS PRESENT

Innovations

LEARNING SERIES

Protect, Recover, and Get More from Your AWS Data

A guide to selecting an AI-powered data security and management platform

Lawrence Miller

COHESITY | aws

POWERED BY ActualTech MEDIA

Innovations

LEARNING SERIES

Protect, Recover, and Get More from Your AWS Data

A guide to selecting an AI-powered data security and management platform

By Lawrence Miller

POWERED BY ActualTech MEDIA

www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

GRAPHIC DESIGNER

Olivia Thomson

HEAD OF SMARTSTUDIO

Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM COHESITY

Genny Gordon
SENIOR PRODUCT MARKETING MANAGER

Chris Hoff
SENIOR PRODUCT MARKETING MANAGER

Marc Mombourquette
SENIOR PRODUCT MARKETING MANAGER

Nikitha Omkar
SENIOR PRODUCT MARKETING MANAGER

Diana Salazar
SENIOR PRODUCT MARKETING MANAGER

ABOUT THE AUTHOR

Lawrence Miller, CISSP, CISM, has worked in information technology in various industries including military, telecommunications, legal, retail, and professional services for more than 30 years. He earned an MBA in Supply Chain Management from Indiana University and has written numerous books on technology and security topics.

TABLE OF CONTENTS

CALLOUTS USED IN THIS BOOK

THE 101

This is where we turn when we want to provide foundational knowledge for the subject at hand.

OFF THE BEATEN PATH

This is a special place where you go to discover insight into topics that may be outside the main subject but that are still important and relevant.

BRIGHT IDEA

When we have incredible thoughts (at least in our heads!), we express them through eloquent phrasing in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

It's not all tech all the time! This is where we discuss items of strategic interest to business leaders.

DEFINITION

Defines a word, phrase, or concept.

GPS

We'll help you navigate your knowledge to the right place.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

WATCH OUT!

Make sure you read this so you don't make a critical error!

PAY ATTENTION

We want to make sure you see this!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

As modern organizations adopt cloud workloads and face increasingly sophisticated cyber threats, their legacy on-premises technology solutions are no longer effective. One of the most significant roadblocks to digital transformation today is data sprawl. Effective data management—including data protection, data security, and data insights—is key to unlocking the full value of your organization's data.

This Innovations Learning Series Guide, "Protect, Recover, and Get More from Your AWS Data" explores common data management and security challenges organizations face and how they can solve them to remain resilient as threats evolve.

CHAPTER 1

Cloud Data Protection and Recovery

Data is the lifeblood of every modern business, but what happens when your data is gone? Whether it's ransomware, a denial-of-service (DoS) attack, a malicious insider, a hardware malfunction, or an honest mistake, when your data is gone your business can't function. Given the business-critical nature of data today, you need to ensure you can quickly and effectively back up and recover your data.

In this chapter, you'll learn about data management challenges, cloud data protection and recovery use cases, and the capabilities and features you need in a modern data protection and recovery solution.

Modern Data Management Challenges

Despite knowing how important protecting their data is, organizations struggle to do so because of complex IT infrastructures, data silos, and explosive data growth. Part of this is due to organizations

developing a patchwork of data protection tools and products to address different use cases. It is also driven by legacy solutions that have grown expensive to maintain and aren't always interoperable with new technologies. Instead, many companies are adopting cloud-first strategies with hybrid infrastructures spread across on-premises and the public cloud.

However, hybrid cloud architectures are not without their challenges. Sometimes, hybrid cloud architectures have emerged unintentionally as a result of decentralized IT management and pervasive shadow IT, rather than a deliberate strategy. For example, your human resources department may be using a Software-as-a-Service (SaaS) application for payroll, your DevOps teams may prefer to build applications on Amazon Web Services (AWS), and your IT department may be managing your core infrastructure on-premises or in a private cloud. Other times, they are deliberate, but by nature, hybrid cloud strategies result in data in separate locations. Regardless of whether they were intentional or not, data is everywhere. This increases IT complexity, leading to data protection and security challenges.

Another source of data growth and complexity is data democratization—that is, making all data and data types readily available to all business users, rather than adopting the least privilege security principle—which creates more data management challenges. As organizations quickly move to launch their own artificial intelligence (AI) initiatives, data volumes will continue to grow exponentially, and putting data everywhere in disparate point products deployed across multicloud and hybrid architectures, will continue to be increasingly problematic.

What organizations need is a modern data protection and recovery solution that protects systems and AWS workloads, such as S3, RDS, and EC2, across on-premises and hybrid cloud environments that is fully integrated, provides granular backup and instant recovery capabilities, strengthens cyber resilience, detects threats, and

enables rapid recovery from cyberattacks. It's a single unified solution for data management and protection that will service business use cases today and in the future.

Cloud Data Protection and Recovery Use Cases

Cloud data protection and recovery supports many use cases. Some of the most common include:

- **Backup and recovery.** You can lose data in a variety of ways, malicious and not, which is why a critical first step to recovery is backing up your data. It is important to have a process and a tool that create and store copies of data in a secure location to protect against loss or damage.
- **Data security and compliance.** Different industries have different rules for how you can handle data. For example, General Data Protection Regulation (GDPR) applies to any business controlling or processing the personally identifiable information (PII) of European Union residents. Businesses who fail to manage their data in accordance with their industry's regulations could face legal, monetary, and financial repercussions.
- **Ransomware protection, detection, and recovery.** The most effective defense against ransomware is a good, immutable backup of your data that enables rapid recovery—without paying a ransom. However, you should also put a strategy in place to ensure an effective response. Align your strategy with a framework, like NIST, to ensure you're following cybersecurity best practices and have robust protection, detection, and recovery capabilities for your data.

- **Long-term retention and archival.** For businesses that generate new data regularly, but need to retain existing data, data archiving is critical because it enables organizations to quickly retrieve both types. In certain industries, retaining data for longer periods of time is required for compliance and regulatory reasons.

- **Disaster recovery and business continuity.** In our fast-moving, "always-on" business world, downtime hurts both your reputation and bottom line. Organizations must be able to meet increasingly stringent maximum tolerable downtime (MTD) requirements, recovery time objectives (RTOs), and recovery point objectives (RPOs), to ensure their business can quickly and fully recover from an outage or other major event.

RTO is the maximum time that a system can be down before causing harm to the business, while RPO represents how much data can be lost. RTO and RPO are both calculated in time: seconds (or sub-seconds), minutes, hours, or even days.

Requirements for a Cloud Data Protection and Recovery Solution

As data becomes more valuable to organizations, a modern cloud data protection and recovery solution is essential. Key requirements include:

- **Unified management.** A single unified solution enables global management across multicloud, hybrid, and on-premises environments at scale. It should act as an

intelligent global assistant, detecting potential ransomware attacks, helping you identify anomalies and making corresponding remediation recommendations, such as for additional capacity planning.

- **Protection for on-premises, cloud, and SaaS data.** Data is everywhere today. Modern data protection and recovery must protect your data wherever it exists, whether it is on-premises, spanning multicloud and hybrid environments, or in SaaS applications. Look for flexible on-premises and cloud deployment options that can be self-managed or managed "as-a-Service."
- **Instant mass data restore.** Threat actors attempt to exfiltrate or destroy as much of our data as possible, so you need a way to quickly recover all your data. Look for a solution that keeps snapshots fully hydrated to improve recovery times so it can provide the ability to restore hundreds of VMs, large databases, and large volumes of unstructured data instantly, at scale, to any point in time and location.
- **Cyber recovery.** Verify the integrity of your backups to identify a "clean" recovery point, for example, in the event of a ransomware attack that targets backups. Look for a solution that can enable you to confidently restore data at a granular level.
- **Unlimited scalability.** Eliminate complex, risky, and costly on-premises forklift upgrades and easily scale your solution without disruption. Look for a scale-out, hyperscale architecture and distributed file system that provides global search capabilities and helps reduce your data and storage footprint with global variable-length deduplication and compression.

CUSTOMER STORY

InfraServ Wiesbaden Picks Cohesity and AWS for Faster Recovery, Lower Costs, and Scalability

Service provider InfraServ Wiesbaden offers a variety of infrastructure and technology services to tenants of the Kalle-Albert industrial park in Wiesbaden, Germany. It employs 850 people to support the many businesses that use its 96 hectare site. The core processes managed by InfraServ are the supply of energies and wastewater disposal, but the business can also aid with the development of premises, with procurement and logistics, as well as with services in human resources.

CHALLENGE

InfraServ Wiesbaden offers Backup as a Service (BaaS) to its customers, but this was based on legacy tape technology and required three data centers for production, disaster recovery, and backup environments. It also required staff to physically take tapes to an offsite storage facility—and on occasions—go and retrieve them to restore systems.

The process consumed up to 30 hours of time in manual tasks per month. In addition, the on-premises hardware was reaching its end of life and was increasingly expensive to maintain. Expanding capacity was a slow and manual process that delayed the onboarding of new services or workloads.

InfraServ Wiesbaden's real challenge was that it struggled to adequately back up Microsoft 365 files, which its customers increasingly required. Granular restoration of Microsoft 365 files, especially Microsoft Teams data, is difficult because its data and

files come from a variety of sources. Customers also wanted backups that would work across their on-premises and cloud workloads with minimal need for management or oversight.

SOLUTION

InfraServ Wiesbaden looked at a variety of solutions for its backup challenges before deciding to work with AWS partner Cohesity. Cohesity's BaaS offering on AWS—which is managed by Cohesity and hosted on AWS—was the only solution that provided a single platform to satisfy all its requirements, while needing minimal oversight or management.

Cohesity and AWS worked together closely to provide the right solution for InfraServ Wiesbaden. "Cohesity has been a true partner," says Steffen Mauer, head of IT and Operations at InfraServ Wiesbaden. "We needed someone we could look in the eye when there was a problem—not deal with through a call center. They've been there when we needed them, but also proactively warned us about upcoming issues like malware."

Cohesity BaaS offers hybrid cloud flexibility with connectors to on-premises workloads and backs up cloud workloads through direct, read-only access. Each snapshot is replicated three times and stored in the AWS data center in Frankfurt. Cohesity's BaaS uses Amazon Cloud Compute (Amazon EC2), which gives access to reliable, scalable infrastructure on demand, and Amazon Simple Storage Service (Amazon S3) object storage to retrieve any amount of data from anywhere.

OUTCOME

Once the decision was made to go with Cohesity's solution on AWS, and backup strategies and processes had been agreed, the team had a pilot system ready for testing in a few days.

Optimizing bandwidth and trialing different processes took a little longer. But the team is already saving up to 30 hours a month in staff time and is no longer physically driving tapes to the storage facility. Regular backups used to take all night to complete and full backups typically took a weekend. The Cohesity solution runs in hours and works incrementally so there's no need to run full backups.

Restoring files is also much easier. "I'd say the difference between old and new is 100 to one," says Mauer. "The old system meant we had to physically find the old tape or even go to the offsite storage vault and find it there. Now it takes seconds, and we can restore files very selectively." All backed up files are checked for malware and not even the InfraServ team can delete files less than four weeks old.

The team can constantly monitor files and systems and quickly perform restoration if needed, while Cohesity has responsibility for the integrity of the backups. The system handles about 100TB of on-premises data but can scale almost instantly as required.

The company is still in the process of closing down its on-premises systems, which will provide additional cost savings. But it's already saving the team a great deal of time previously spent on manual tasks.

Migrating to AWS has also opened up access to other services. InfraServ Wiesbaden is talking to Cohesity about a more comprehensive disaster recovery system and what kind of emergency infrastructure would be required to restore systems from AWS in the event of a serious incident.

But saving money was never the main driver for this project. "We've gotten rid of a ton of technical debt," says Mauer. "The project itself was so straightforward. It's not just saving us time and money, we now have faster, better backups for customers—it just doesn't compare to what we had before."

While a hybrid cloud strategy delivers many benefits, it can also be a modern data management challenge—adding more clouds to manage increases complexity across the environment. In Chapter 2, you'll learn how a modern data management solution helps organizations address their data security and management use cases.

CHAPTER 2

Intelligent Data Security and Management

In the digital economy, data is the most important asset for modern enterprises and a lucrative target for cybercriminals. While the rate of ransomware attacks dropped slightly in the past two years (59% of organizations being hit by ransomware in 2023), it's no time to let down your guard. Cybercriminals and ransomware gangs are increasingly targeting backups with an alarming 75% success rate and, in the absence of a secure, immutable backup, 56% of organizations are paying a ransom to recover their data.

What Will You Do When Ransomware Hits You?

The enterprise data footprint—that is, your attack surface—is growing rapidly and becoming increasingly complex as organizations innovate, add more tools to their tech stack, and pursue multicloud strategies. Larger attack surface areas are more difficult to protect and leave organizations more vulnerable to attacks. That's why in our previous brief, we talk about the importance of

data management and how it is the foundation for any effective security strategy. At the same time, cyberattacks are occurring more frequently. This is in part due to Ransomware-as-a-Service (RaaS) offerings, which have made it easy for anyone to launch an attack and use AI to gain intelligence and repeatedly attempt to compromise your last line of ransomware defense, your backups. Ransomware attacks are also becoming more complex with double- and triple-extortion attacks becoming more pervasive.

TYPES OF RANSOMWARE ATTACKS

Double Extortion: Attackers exfiltrate a copy of your sensitive data, encrypt it, and threaten to expose it.

Triple Extortion: An advanced cyberattack strategy that adds layers of increased pressure to a victim, such as attackers launching a denial-of-service (DOS) attack or directly targeting individuals whose data they have stolen.

Data Security and Management Use Cases

An intelligent data security and management solution supports many enterprise use cases, including:

- **Cyber resilience.** A cyber resilient solution requires the foundational layer of backup and recovery with enhanced, built-in ransomware defenses to protect your data.

- **Ransomware protection, detection, and recovery.** Robust ransomware defense requires comprehensive data security and management capabilities, including immutable backup snapshots, AI-powered threat detection and user behavior analysis, and rapid recovery at scale.

- **Clean room recovery.** A clean room isolates compromised systems in a controlled environment where security operations teams can perform forensics to understand how an attack happened while completely separated from the network. Building a timeline of the incident allows them to devise a recovery plan that eradicates the threat and helps prevent reinfection in the future.

- **Data compliance.** Governance, risk, and compliance (GRC) establishes the data archival, retention, and sovereignty requirements that an organization must follow to align with regulations. An intelligent data security and management solution provides granular controls to help ensure compliance.

- **Data privacy laws.** Data privacy laws, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), are driving organizations to accurately identify and manage sensitive data containing personally identifiable information (PII), and prove compliance. EU regulations such as the Digital Operational Resilience Act (DORA) are creating additional penalties for organizations that don't comply.

Ransomware Data Protection and Recovery

An intelligent data security and management solution helps organizations strengthen their security posture, reduce the risk of unauthorized access, and minimize the impact of a ransomware attack. Key capabilities for ransomware data protection and recovery include:

- **Cyber vaulting and data isolation.** A cyber vault creates an isolated copy of production data. With a clean, separate, and protected copy of data always ready, organizations can rapidly recover data back to its original source, or alternate backup locations, in case of a ransomware attack or other incident that compromises production or primary backup systems.

- **Unlimited immutable snapshots.** Software-based, native immutable backup snapshots effectively throw up a wall against ransomware attacks because they can't be encrypted, modified, or deleted. Unlimited snapshots enable precise point-in-time recovery to a known good backup.

- **WORM lock.** Write once, read many (WORM) mechanisms provide another layer of protection against a ransomware attack, allowing IT teams to create and apply a time-bound lock to enhance immutability for protected data.

- **AI/machine learning (ML) threat detection.** A modern data security and management solution powered by AI/ML can accurately detect patterns and anomalies that may be indicative of an imminent cyberattack, while reducing alert fatigue and "noise" due to false positives.

- **At-rest and in-flight encryption.** Secure at-rest and in-flight backup data with robust Advanced Encryption Standard (AES)-256 encryption that is U.S. Federal Information Processing Standards (FIPS)-validated.

- **Granular role-based access control (RBAC).** Least-privilege access is key to reducing ransomware and insider threats. Granular RBAC provides an efficient and effective means to reduce the risk of unauthorized access to data while granting authorized users the minimum privileges required to do their work.

- **Strong authentication with multi factor authentication (MFA).** MFA has become a de facto standard for strong authentication. To protect your backup data from ransomware and other threats, ensure phishing-resistant asymmetric key cryptographic challenge-response authentication protocols (not text-based) MFA is enforced for access.

- **Separation of duties.** An administrative control (also known as Quorum Approval) used by organizations to prevent fraud, sabotage, theft, and other security compromises. It's the principle that no person, role, or group should be able to execute all parts of a transaction or process.

- **Data classification.** Intelligent data management helps organizations proactively identify, classify, and protect their most sensitive and valuable data, and prioritize their recovery efforts.

- **Automation.** The ability to configure regular backup schedules, policies, and reporting, as well as to perform automated testing to verify the integrity of backups. This automation helps ensure that backups are reliable and can be restored quickly when needed.

- **Actionable alerts.** Customizable, real-time alerts ensure that IT and security teams receive prompt notification of important events. Alerts allow you to build custom playbooks to streamline response operations.
- **Extensible application programming interfaces (APIs) and third-party integrations.** Customizable management APIs, pre-built workflows, and third-party integrations provide an extensible, future-proof solution that helps streamline operations and enhance data security.

CUSTOMER STORY

Beckman Coulter Streamlines Operations with Backup Solutions from Cohesity on AWS

Beckman Coulter develops, manufactures, and markets products for biomedical testing. However, without a standard backup solution in place, it was challenging for Beckman Coulter to monitor global backups and protect against ransomware. With Amazon Web Services (AWS) partner Cohesity, Beckman Coulter simplified data management and strengthened its security posture for both on-premises infrastructure and Backup as a Service in the cloud. Now the company is bringing smaller sites into the fold, using the Cohesity DataProtect Delivered as a Service hosted on AWS. Cohesity's single interface for self-managed and Software-as-a-Service (SaaS) environments simplifies management and eliminates upgrade downtimes, while its immutable backups enhance ransomware protection.

CHALLENGE

Hospitals, labs, and doctors' offices around the world rely on Beckman Coulter's diagnostic equipment to enhance patient care and improve outcomes. This makes secure, reliable data management especially critical to prevent business disruptions and bring new products to market quickly. Historically, Beckman Coulter didn't have a standard backup solution in place, making it complicated to monitor global backups and ensure it was meeting the service level agreements (SLAs) in place. Consequently, each Beckman Coulter office needed an engineering specialist familiar with that location's backup solution, increasing costs. Additionally, the existing solutions didn't protect against ransomware, a growing business risk. As part of Beckman's cloud-first initiative to reduce on-premises infrastructure costs and management overhead, it sought to switch to a SaaS model for backups and archiving.

SOLUTION

When establishing a company-wide standard for its data management platforms, Beckman Coulter conducted a comprehensive evaluation of its existing solutions, comparing them with Cohesity. "Cohesity's platform stood out because of its simple management interface and ransomware protection with immutable backups," says Kevin Chi, IT systems engineer at Beckman Coulter Life Sciences. "We also liked that we could order an appliance with the right configuration for each location instead of hassling with a complex configuration process."

The company's nine major data center locations on three continents use Cohesity DataProtect, hosted on AWS. Local Cohesity clusters that are stored in Amazon Simple Storage Service (Amazon S3) provide backup and recovery for Beckman Coulter's NetApp files, Nutanix AHV, and Oracle ERP data.

To further its cloud-first initiative, Beckman Coulter also deployed Cohesity's Backup-as-a-Service (BaaS) solution, eliminating the need for on-premises infrastructure for its smaller locations. "We have a unified view of all backups—on-premises or in the cloud—helping us meet SLAs. And now we don't need to worry about complying with long-term retention requirements because Cohesity does it automatically," explains Chi.

OUTCOME

Today, Beckman Coulter uses Cohesity to back up 330TB of data in 11 locations in North America, France, Ireland, and India—183TB in Phoenix alone. With the simple management interface, a central operations team can now manage backups and restores, avoiding the need for engineering specialists in each location, reducing overall costs. Beckman Coulter's security posture is stronger now because of Cohesity's immutable backups. In the event of a ransomware incident, the company can restore clean data, avoiding added costs and business interruptions.

Moreover, the Cohesity dashboard alerts the operations team to anomalous activity that could signal a cyberattack—such as a big change in the number of files from one backup to the next. "Recently we received an alert on the Cohesity dashboard that hundreds of application files had been deleted," Chi recalls. "The application team let us know they were doing updates, so there was no cause for alarm. If it had been an attack, we had the comfort of knowing we could have restored the files from an immutable backup."

Finally, Beckman Coulter can futureproof its data with timely updates and zero downtime. As soon as updates are available, Beckman Coulter seamlessly and easily installs software releases featuring security enhancements, while Cohesity manages BaaS

updates. “With our old backup solution, we sometimes postponed software upgrades because they required downtime,” Chi says. “With the Cohesity non-disruptive upgrades we update regularly every quarter, making sure we have the latest security features.” Chi concludes, “With Cohesity and AWS we have great technology—and also great partners. Our Cohesity team is invested in making sure we’re successful with deployment and support, and that we have the features we need to protect the business today and into the future.”

In Chapter 3, you discover how to unlock the value of your organization’s data with AI-driven data insights to fuel growth and stay competitive, detect threats in real-time, improve decision-making speed and accuracy, and streamline compliance and risk management with AI-driven insights.

CHAPTER 3

AI-Driven Data Insights

Artificial intelligence (AI) has ushered in a new era where deep insights can be unlocked from your data. Much like cloud adoption a decade ago, AI has quickly become the hottest technology driving new innovation and digital transformation initiatives in enterprises everywhere. And like the early days of cloud computing, there is often a great deal of confusion and misinformation about AI that makes it challenging for leaders to know where and how to get started.

Recognizing AI Adoption Challenges

AI models are already being used for a wide variety of applications, such as predictive maintenance in manufacturing, individualized treatment plans in healthcare, and sentiment analysis in marketing and customer service. Today, AI is being used to bolster cybersecurity capabilities, for example, to detect anomalies and automate response and recovery actions. Rapid advancements in AI-powered conversational applications leveraging high-quality backup data enable

organizations to improve decision-making speed and accuracy using natural language questions instead of complex data queries, and receive responses that go far beyond traditional data analytics.

IT leaders must ensure a working understanding of AI technologies and partner with vendors that promote "responsible AI" principles including transparency, governance, accountability, fairness, and privacy. Other common AI adoption challenges include:

- **Difficulties making sense of large amounts of data.** AI feeds itself on massive amounts of data. However, poor data quality—that is, outdated, incomplete, or inaccurate data—can quickly derail an AI project. For example, when data is not properly deduplicated or doesn't have metadata that can improve data retrieval and response generation, the quality of large language model (LLM) responses suffers—"garbage in, garbage out."
- **Harnessing siloed data to maximize business value.** Enterprise data is literally everywhere, and discovering, identifying, and accessing massive volumes of data in disparate systems spanning hybrid and multicloud environments is a significant challenge to AI adoption. A modern AI-powered data platform consolidates data in a single place, where it can be used to readily identify and resolve security issues faster and support AI initiatives.
- **Aligning expectations on what AI can do for your organization.** Many organizations are latching onto AI as the flashy new thing, but they don't necessarily have a firm understanding of what AI is, what it can deliver, and how to align it to their business objectives. It is important to have a goal in mind when designing your AI solution, whether it's custom built or a complete solution. Defining the problem you want to solve, whether it's deeper analysis, improvements for productivity, doing analysis, or resolving security issues faster is important in order to be successful.

Responsible AI is an approach to developing and deploying AI from both an ethical and legal point of view. The goal of responsible AI is to employ AI in a safe, trustworthy, and ethical fashion. Key responsible AI principles include:

Transparency. Protect access to data with role-based access controls (RBAC). Promote transparency and accountability around access and policies.

Governance. Help ensure the security and privacy of data used by AI models and the workforce—so the right data is exposed only to the right people with the right privileges.

Exploring AI Use Cases

AI-driven data insights help organizations maximize the value of their data through many common enterprise use cases, including:

Threat detection. Ransomware and other cyberattacks use increasingly stealthy and deceptive tactics. An AI-powered modern data management solution allows you to integrate data anomaly detection within your security operations center (SOC) to amplify and support existing threat hunting, incident response, and recovery processes.

Data classification. AI can help organizations discover and classify their sensitive and regulated data to accelerate incident response in a data breach or ransomware attack. An AI-powered modern data management solution uses advanced pattern matching to automatically discover and accurately classify data across silos.

Compliance and risk management. AI can reduce the amount of time compliance teams spend producing audit logs and performing data forensics. It enables users to ask questions about their data, such as historical records, cited documents, or emails to support compliance, risk management, and legal use cases, and receive human-like, actionable responses. Users can then ask follow-up questions in a conversational manner, and dig deeper into answers as if they were speaking directly with a subject matter expert, helping them get information more quickly.

Identifying Must-Have AI Data Analytics Capabilities

With the rise of AI, backup data is no longer just for recovery. For example, backup data can be used with large language models (LLMs) to create relevant and accurate answers based on corporate data. In addition to enabling multicloud data protection and recovery and mitigating ransomware risk, backup data (and its metadata) can now be indexed and mined to fuel AI models. When coupled with a modern data platform, the following AI technologies transform data into knowledge with near-real-time insights to enable smarter business decisions and enhance cybersecurity capabilities:

- **Generative AI (GenAI).** GenAI uses algorithms to generate new content (such as written content, image, video, audio, computer code, and so on) based on user input. Unlike earlier versions of AI, GenAI can create new content, like cyberthreat analyses presented in a conversational user interface. GenAI can be a force multiplier for understaffed security teams by providing real-time threat detection, enhanced threat intelligence, automated security patching, improved incident response, and more.

- **Large language models (LLMs).** LLMs are learning models that are trained on vast amounts of data and apply language to GenAI capabilities. LLMs provide accurate responses to user or machine queries that are human readable and actionable. In this way, LLMs allow security teams to spend less time scripting or writing Boolean queries, and focus more on quickly resolving security incidents.

- **Retrieval augmented generation (RAG).** Retrieval augmented generation (RAG) is a natural language processing (NLP) technique that combines the strengths of both retrieval- and generative-based artificial intelligence (AI) models. RAG AI can deliver accurate results that make the most of pre-existing knowledge but can also process and consolidate that knowledge to create unique, context-aware answers, instructions, or explanations in human-like language rather than just summarizing the retrieved data. For example, these capabilities can help security analysts use their data to gain insights that improve the speed and accuracy of their response to an incident.

- **AI-powered conversational search.** AI-powered conversational search uses natural language queries that allow your users to "have a conversation with your data." Using common language, users can ask questions about your data, dig deeper into datasets, and obtain context-rich answers. AI-powered conversational search allows information security risk teams to have a more contextual dialog, for example, to streamline compliance, risk management, and discovery operations with the ability to responsibly and securely search enterprise data.

CUSTOMER STORY

JSR Corporation Turns to Cohesity for Cyber Resilience

JSR Corporation, a manufacturer of synthetic polymer materials, is a $4 billion parent company of JSR Micro, Crown Biosciences, KBI Biopharma, and other subsidiaries, with 47 sites across the globe and over 7,500 employees.

CHALLENGE

JSR Corporation needed a robust data recovery and backup solution for its on-premises and AWS environments to protect against ransomware and other cyber threats. Additionally, they wanted an AI-powered solution that would help break down data silos and unlock data across the organization.

SOLUTION

JSR Corporation turned to Cohesity and AWS to modernize how it protects its IT estate from threat actors, empower their data scientists, and meet compliance requirements.

Ryan Reed, Head of IT Products and Services at JSR Corporation, says “Cohesity Gaia has performed as well or better than many of the models that we tested. Some of the large language models we eliminated pretty early on because they just weren’t performing as we expected. We’ve seen Cohesity Gaia be able to really perform [and] it’s really easy to get the data into Cohesity Gaia.”

OUTCOME

Cohesity allows JSR to seamlessly backup its entire data estate on AWS, thereby reducing ransomware risk and ensuring a robust business continuity and disaster recovery capability. With Cohesity Gaia, JSR can flag certain data—such as research on behalf of clients which might have to be saved for up to 12 years—to be retrieved or stored for a long period of time.

LEARN MORE

Throughout this Innovations Learning Series guide, you've learned how a modern data management platform can simplify multicloud data management, enable rapid ransomware recovery, and deliver intelligent insights with AI-powered analytics for better decision making.

To explore more, visit https://www.cohesity.com/solutions/cloud/aws/ for insights on modern data management, ransomware recovery, and AI-driven analytics.

Ready to experience it firsthand? Start your journey with a free trial or explore the Demo Center to see Cohesity in action.

ABOUT AWS PARTNER COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easy to secure, protect, manage, and get value from data—across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions can be delivered as a service, self-managed, or provided by a Cohesity-powered partner. Learn more at https://www.cohesity.com/aws.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit actualtechmedia.com/content/