COHESITY PRESENTS

Innovations

LEARNING SERIES

Protect, Recover, and Get More from Your Data

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

Lawrence Miller

COHESITY

POWERED BY ActualTech MEDIA

Innovations

LEARNING SERIES

Protect, Recover, and Get More from Your 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

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 Data" explores common data management and security challenges organizations face and how they can solve them to remain resilient as threats evolve.

CHAPTER 1

Multicloud 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, multicloud 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 multicloud infrastructures.

In a multicloud architecture, an organization uses two or more cloud computing services from different cloud providers in order to improve their disaster recovery capabilities, leverage best-of-breed technologies, optimize application workloads, and reduce risk. However, it is not without its drawbacks—87% of organizations adopting a multicloud strategy, say managing multicloud has become one of the top three cloud challenges for enterprises.

Why? Sometimes, multicloud 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 in Microsoft Azure. Other times, they are deliberate, but by nature, multicloud 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 workloads across on-premises and hybrid multicloud 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.

Multicloud Data Protection and Recovery Use Cases

Multicloud 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 Multicloud Data Protection and Recovery Solution

As data becomes more valuable to organizations, a modern data protection and recovery solution for multicloud 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

Ausenco Strengthens Security and Cuts Management Time with Cohesity DataProtect Delivered as a Service

A multinational engineering and consulting services provider, Ausenco backs up 100 TB of critical Microsoft 365 (M365) data for its more than 3,000 employees. The previous backup solution—Veeam software on self-managed cloud infrastructure—no longer met the company's security needs and took 20 hours/week to manage. By switching to Cohesity DataProtect delivered as a service, Ausenco reclaimed 20 hours/week previously spent managing backup infrastructure, introduced 4-hour service-level agreements (SLAs) for file recovery, and obtained the immutable backups required for cyber insurance and peace of mind. All without additional costs.

CHALLENGE

Ausenco's engineering and consulting services business is growing—especially among mining companies experiencing soaring demand for battery metals. The company backs up 100 TB of critical M365 data for its more than 3,000 employees. "Microsoft provides some data protection built-in, but not enough

for our business," says Kalpesh Bhathella, Ausenco's Director of Operational Services. "We retain some SharePoint and OneDrive files indefinitely, and can't afford to lose them to cyberattacks."

Until 2022, Ausenco's IT team backed up M365 data with Veeam software, using infrastructure as a service (IaaS) from Amazon Web Services (AWS). But managing the infrastructure and software was brutal, consuming 50% of one IT administrator's time. Another shortcoming: taking immutable backup copies, a must-have to recover from cyberattacks, would require more infrastructure and more management time. "Security is top of mind for us," Bhathella says. "Prospective customers always ask about it, and lately they also want to know if we have cyber insurance. We needed immutable copies, but without more management burden."

SOLUTION

After evaluating Cohesity and Rubrik, Ausenco selected Cohesity DataProtect delivered as a service, which provides backup and recovery capabilities for software as a service (SaaS) like M365 as well as other cloud or on-premises data Ausenco might add later. "We liked the idea of a fully-managed cloud service because self-managing infrastructure makes no sense in this day and age if IT is not your core business," Bhathella says. "And only Cohesity creates immutable backups by default."

The Cohesity cloud service was up and running quickly in approximately 2 weeks. The IT team rarely has to think about it anymore. "After initial configuration, Cohesity just worked," Bhathella says. "On the rare occasions when we've needed support, Cohesity figured it out right away. We've never had to escalate."

OUTCOME

For Ausenco, the top benefit of the Cohesity solution is a stronger security posture. “We do everything we can to prevent cyberattacks, but having the ability to restore clean M365 data from Cohesity’s immutable backup copies means we have a solid fallback. Storing immutable backups offsite also helped us qualify for cyber insurance, which prospective customers ask about.”

Stronger security costs less, not more. “The savings from not having to pay monthly fees for cloud infrastructure fully paid for Cohesity DataProtect delivered as a service,” says Bhathella. “On top of that, we’re saving the 20 hours a week we used to spend tuning and managing our backup software and cloud infrastructure.” The team member who used to devote 50% of their time managing backups can now spend that time on higher-value digital transformational work. And together with Ausenco’s other cybersecurity measures, immutable backups helped the company qualify for favorable rates on its cyber insurance policy.

For the first time, Ausenco is offering a 4-hour SLAs for M365 email or file recovery—a big hit with the company’s busy engineering, consulting, and operations teams. “With our old backup solution, restoring a lost Exchange, SharePoint, or OneDrive file could take weeks because our IT admin had to comb through hundreds of backups just to find it,” Bhathella says. “Cohesity’s search engine is like the Google of backups. We just enter a filename or phrase, and a list pops up. The file we’re looking for is often right on top.”

Now Ausenco is preparing to use Cohesity DataProtect delivered as a service to protect other workloads besides M365, including on-prem and AWS virtual machines. For extra resilience Bhathella plans to back up certain workloads on Microsoft Azure—a hybrid

cloud setup. The IT team will be able to view and manage backups and restores in any cloud from the same Cohesity interface, enjoying a unified management experience.

As Bhathella sums it up, "With Cohesity DataProtect delivered as a service we have everything we need to protect any kind of data as our business grows: immutable backups, fast restores, and great support—all without having to worry about infrastructure management."

While a multicloud 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

Emerge IT Solutions Helps Client Recover from Ransomware Attack in Just 3 Days with Cohesity DataProtect

Founded in 2004, Emerge is committed to being the most trusted technology adviser in the Ohio Valley. The company accomplishes this with best-in-class technical knowledge and competency, leading technology, superior customer service, and a commitment to long-term relationships.

CHALLENGE

Emerge IT Solutions has been helping customers in the Midwest with their IT needs since the early 2000s. For several years Emerge has seen surging interest in its managed cybersecurity services. Some companies that Emerge works with face pressure from supply chain partners to meet more stringent cybersecurity policies, making compliance important for revenue attainment and retention.

Emerge offers managed data protection as part of its OmniWATCH suite of security offerings, which also include penetration testing, security auditing, and threat detection. Until 2022, Emerge used several popular backup technologies. But backing up several petabytes took 24 hours, and restoring large data sets sometimes took days.

SOLUTION

Emerge found its answer in Cohesity DataProtect, which it offers as a managed service. Running on Emerges private cloud, DataProtect reduces risk with immutable copies, multifactor authentication (MFA), and role-based access controls (RBAC). And it's fast. Today, Emerge uses Cohesity DataProtect to back up several petabytes of customer files, including virtual machines (VMs), virtual desktops, applications, and data. For extra protection, Emerge uses Cohesity's DataLock feature to create a backup snapshot that nobody can alter—not even an administrator—until the lock expires.

For a large manufacturer with multiple locations, Emerge's Cohesity-powered backup and recovery service paid for itself many times over in the first month. Weeks after Emerge implemented Cohesity DataProtect for backup and recovery, the manufacturer was hit by a targeted ransomware attack that encrypted nearly all of its 65 VMs and 500 virtual desktops.

Emerge quickly confirmed that certain production servers were encrypted, and that the problem was spreading. The manufacturer's security partner soon determined that the event was a large-scale attack by a nation-state threat actor.

Emerge sprang into action to restore clean files from the Cohesity backups, forming a team that worked around the clock for three days. The first step in recovery was identifying the

most current backup copy that wasn't infected. The Emerge team used a third-party tool to identify the most recent backup without the attack signature.

Working from the clean copy, Emerge began restoring VMs and virtual desktops in the order the customer requested—most critical first. The recovery process was so straightforward that Emerge needed no help from Cohesity support despite having deployed DataProtect only one month earlier.

OUTCOME

Fast recovery had a significant impact on the bottom line. Recovering in three days instead of the 14 to 21 days typical of this type of attack saved approximately $12 million in downtime costs. No ransom was paid.

Now Emerge is putting Cohesity DataProtect to work for disaster recovery, using it as part of a hybrid cloud. If a customer's production environment goes down, Emerge can spin up their VMs right on its private cloud or in Azure.

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/ 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 COHESITY

COHESITY

Cohesity is a leader in AI-powered data security. Aided by an extensive ecosystem of partners, Cohesity makes it easier to 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 are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including 47 of the Fortune 100.

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/