COHESITY

ActualTech MEDIA

AI-Driven Data Insights

Lawrence Miller

- Common AI Adoption Challenges
- Key AI Data Analytics Use Cases
- Core AI Data Analytics Capabilities

IN THIS PAPER

Organizations are rapidly turning to AI technologies to help unlock the value of their data to fuel growth and stay competitive, improve decision-making speed and accuracy, and streamline compliance and risk management with AI-driven insights. Learn how AI-driven data insights can help your organization make smarter business decisions.

Highlights include:

- Common AI adoption challenges
- Key AI data analytics use cases
- Core AI data analytics capabilities

CONTENTS

2 Recognizing AI Adoption Challenges

3 Exploring AI Use Cases

4 Identifying Must-Have AI Data Analytics Capabilities

5 Customer Story

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 also 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.

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 multi-cloud 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.

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 security and 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.

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

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 multi-cloud 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.

With the rise of AI, backup data is no longer just for recovery.

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

Visit https://www.cohesity.com/solutions/ai-conversational-search/ to learn more about AI-powered data insights with Cohesity Gaia, and download Protect, recover, and get more from your data: A guide to selecting an AI-powered data security and management platform.

COHESITY