AI at Commvault

Secure Innovation, Intelligent Resilience

Resilience for the AI era.
Responsibly deployed. Broadly supported. **Ready when it matters.**

Enabling a Secure AI Future

AI is advancing rapidly – driven by exponential gains in model scale, GPU performance, and orchestration frameworks. Standards like the Model Context Protocol (MCP) are emerging, and agentic software is reshaping enterprise UX by introducing autonomous systems that reason, adapt, and act across environments.

But this momentum introduces risk. Runtime attacks, adversarial prompts, hallucinations, and data poisoning now threaten the reliability of AI systems and their supply chains. Agentic architectures demand a new level of security, control, and operational resilience.

Commvault addresses these challenges head on. Our strategy helps customers adopt AI securely and responsibly – by protecting AI workloads, enabling clean recovery, and enhancing customer outcomes through automation and governance built for the agentic era.

Commvault's Strategic Focus Areas

1 Protecting AI/ML Workloads

AI models, datasets, pipelines, and vector indexes are now part of the AI application stack. Commvault provides broad support across this stack, enabling end-to-end data protection and recovery at scale for:

- Unified data and AI platforms (e.g., Amazon Redshift).
- Data lake storage and distributed file systems (e.g., Amazon S3, FSx, Azure Data Lake, Lustre).
- Search and vector retrieval systems (e.g., Apache Solr, Elasticsearch, Amazon DocumentDB, Azure Cosmos DB, Google Cloud SQL).
- Compute and DevOps infrastructure (e.g., Amazon EC2 Trn2 UltraServers, Azure DevOps).

From models and datasets to configurations and metadata, Commvault delivers scalable, fast recovery, enabling sustained AI innovation.

2 Enabling Cyber Resilience and Clean Recovery

Modern cyber threats increasingly target backup systems, exfiltrate data, and poison training datasets. Commvault's AI-enhanced cyber resilience capabilities are designed to detect, contain, and recover from such attacks:

Cyber Threat Detection & Resilience

- **Backup malware detection:** AI uses signatures and file comparisons to identify malware and altered files in backups.
- **Threat scanning:** Leverages global threat intelligence and ML to detect advanced malware in backup data.

Data Classification & Risk Analysis

- **Sensitive data discovery:** AI identifies and classifies sensitive files to support compliance and data protection.
- **Anomaly detection:** ML monitors file behavior to detect deviations from normal activity and alert admins to potential threats.

This approach helps organizations respond to threats with minimal downtime and maximum confidence in restored data and model integrity.

3 Enhancing the Customer Experience

Commvault embeds AI and ML across the user experience to deliver faster, more intuitive interactions, from assistance to automation.

Generative AI–enabled features are user-invoked, allowing teams to interact with Commvault using natural language prompts and guided workflows, while ML-enabled features operate behind the scenes, learning from system behavior to optimize performance and reduce manual intervention.

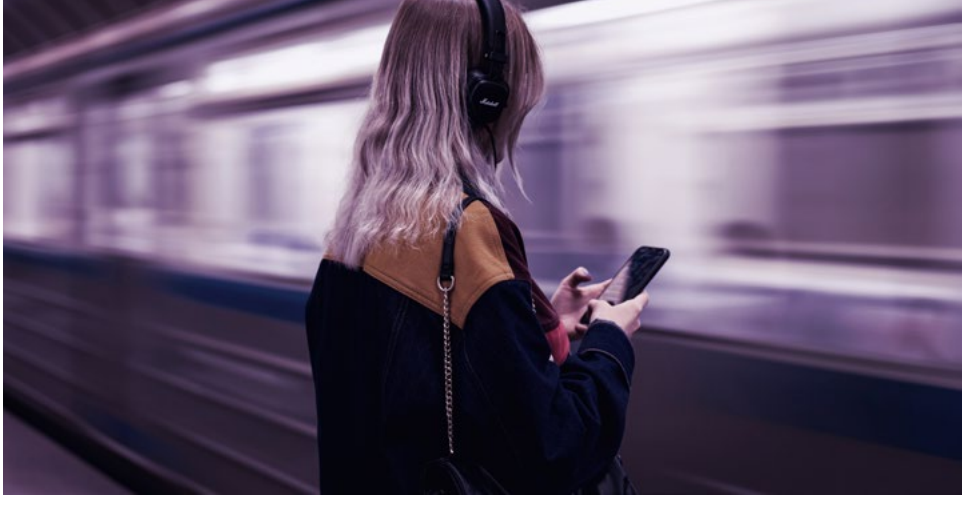
Generative AI–Enabled Assistance (Arlie AI)

- **Arlie chatbot:** Users can ask "how-to" questions and get detailed guidance on configuring and using Commvault® Cloud to maximize cyber resilience.
- **Active insights:** Users can trigger AI to detect and summarize operational issues. Arlie Sense analyzes audit trails and job history to highlight key patterns, risks, and recommended actions.
- **API code assist:** Users receive step-by-step instructions on which APIs to use and how to use them.

ML-Enabled Assistance

- **Smart job scheduling:** ML predicts optimal backup job timing and prioritization based on recovery point objectives – no manual tuning required.
- **Predictive forecasting:** ML anticipates storage needs based on usage trends, enabling proactive capacity planning.
- **Semantic search:** ML interprets and corrects search inputs for more relevant results and smoother navigation in the Commvault Cloud console.

Free up resources spent on troubleshooting to focus on innovation.



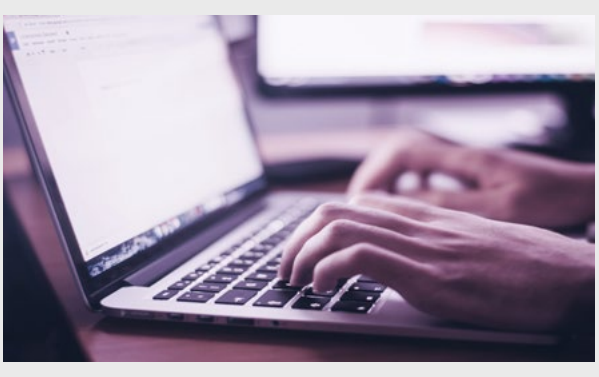
Core Levers Underpinning Commvault's AI Strategy

1 Enabling Agentic Automation

Commvault is advancing toward a future where intelligent agents coordinate security, operations, and recovery across hybrid environments. We envision a distributed fabric of AI agents, orchestrated by Arlie, working across the Commvault ecosystem to:

- Detect anomalies and threats.
- Take corrective actions (e.g., trigger snapshot isolation and validation).
- Collaborate across systems.
- Launch policy-based runbooks to restore services.

These capabilities align with a headless backup model, driven by APIs and designed for coordination with frameworks like MCP.



Learn more at:
commvault.com/blogs/the-agentic-revolution

2 Developing and Deploying AI Responsibly

AI can unlock massive value – but it must be built and used with intention. We are committed to the following principles, which embody our dedication to ethical AI development and deployment:

☑ *Reliability, safety, and control*

We prioritize our AI systems' reliability and safety by implementing rigorous testing, quality assurance protocols, and security measures.

☑ *Transparency and explainability*

We provide clear explanations for AI decisions whenever appropriate, enhancing understanding of data usage, decision rationale, and outcomes.

☑ *Fairness and bias mitigation*

Our AI systems are designed to operate fairly and impartially. We continuously evaluate our algorithms to identify and mitigate unintended biases.

☑ *Human-centered approach*

We make sure AI-enabled insights are delivered to humans to aid decision-making and are not used to initiate actions autonomously.

☑ *Data privacy and security*

Our AI systems are tightly integrated with Commvault Cloud, restricting access to its functionalities from outside the platform. Role-based access control is in place.

☑ *Accountability and governance*

Our governance framework includes comprehensive risk and impact assessments to proactively identify and address potential ethical concerns.

LEARN MORE

> I love Commvault's AI vision because it hits all the key elements of AI that are important to us. It offers GenAI to make my cyber response engineers more effective. It bakes AI into the platform to improve our overall resilience. And it helps protect AI workloads to make sure those workloads have the same resilience as the rest of our critical data.
>
> **Michele Buschman**
> Chief Information Officer, American Pacific Mortgage

Why Commvault: Trusted AI Enablement

Commvault enables organizations to move forward with AI while protecting what matters most. We stand apart through a combination of deep platform integration, security-first engineering, and practical automation designed for the real-world demands of enterprise AI.

Our key differentiators:

AI that delivers value, not just checks a box:

Capabilities like Arlie are designed to solve real customer problems – from automating recovery workflows to surfacing critical insights – not just demonstrate AI for AI's sake.

Scalable protection for end-to-end AI infrastructure:

Commvault supports the full AI stack, including unified data and AI platforms, data lakes, vector databases, and compute infrastructure – all from a single platform.

Engineered for automation:

With native support for open standards like MCP, Commvault aims to enable integration with intelligent agents, customer environments, and future AI ecosystems.

We don't try to be the AI platform – we protect the AI platforms our customers rely on. By focusing on resilience, control, and automation, Commvault empowers organizations to adopt AI securely and sustainably – and stay ready for what's next.

LEARN MORE

To learn more, visit **commvault.com**

Commvault® | commvault.com | 888.746.3849