AI AT COMMVAULT

SECURE INNOVATION, INTELLIGENT RESILIENCE

Resilience for the AI era, responsibly deployed, and 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 is actively addressing these challenges head on. Our strategy helps customers adopt AI securely and responsibly – by protecting AI workloads, enabling clean recovery, enhancing customer outcomes through automation and governance built for the agentic era, and extending AI responsibly with governed data activation.

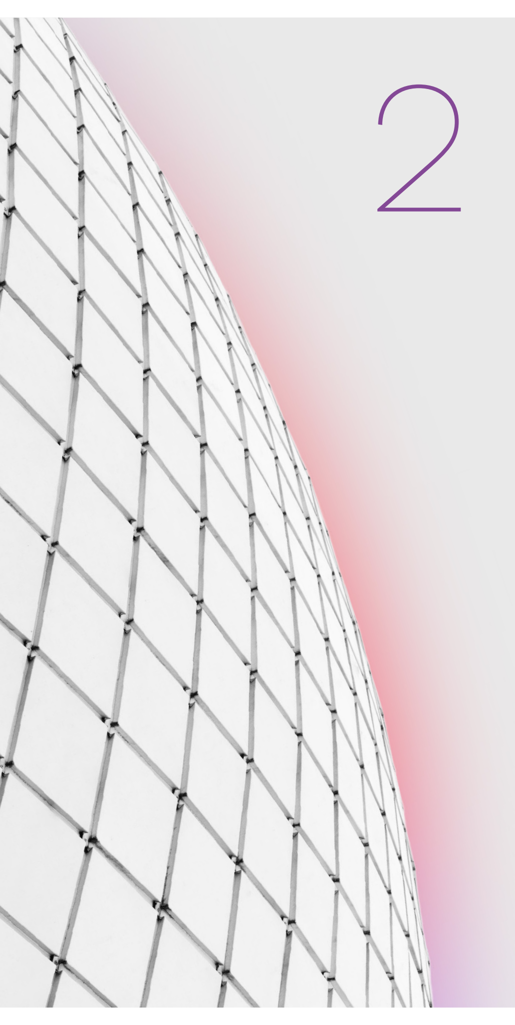
COMMVAULT'S STRATEGIC FOCUS AREAS

1 Protecting AI/ML Workloads

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

- Unified data and AI platforms (e.g., Amazon Redshift, Google BigQuery).
- Data lake storage and distributed file systems (e.g., Amazon S3, Apache Iceberg, 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 is designed to deliver 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.
- **Synthetic Recovery™:** AI analyzes multiple backup versions to help identify clean, uncompromised data and assemble it into a curated recovery point – helping teams restore faster while reducing the risk of reinfection.
- **Arlie Recover:** AI-assisted guidance helps users select clean recovery points, validate restoration paths, and take consistent recovery actions during a cyber incident.

Data Visbility, Classification, & Governance

- **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.
- **Data governance:** Real-time, agentless access controls provide visibility and protection for sensitive data across analytics and AI pipelines, including LLM and prompt protection.

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 help enable 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.

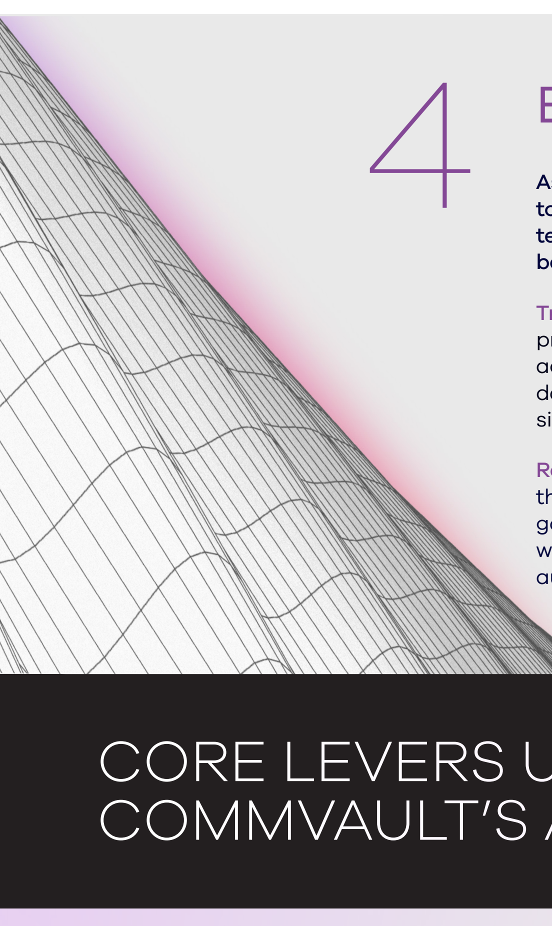
Generative AI–Enabled Assistance (Arlie AI)

- **Arlie chatbot:** Users can ask "how-to" questions and get detailed guidance on configuring and using Commvault® Cloud.
- **Job diagnostics:** Users can troubleshoot failed or stalled jobs by asking Arlie to analyze job details, surface likely causes, and recommend next steps.
- **API code assist:** Users receive step-by-step instructions on which APIs to use and how to use them.
- **Enhanced support:** Can help users to resolve issues faster by asking Arlie for troubleshooting help, recommended actions, and links to relevant documentation.

ML–Enabled Assistance

- **Smart job scheduling:** ML predicts optimal backup job timing and prioritization based on recovery point objectives.
- **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.



4 Extending AI Responsibly

As organizations adopt AI across analytics, operations, and business workflows, they need ways to activate data safely without creating new risks or unmanaged copies. Commvault helps teams extend AI responsibly by preparing trusted data for AI and enabling controlled interaction between AI systems and Commvault Cloud.

Trusted data activation for AI and analytics: Data Rooms provide a governed workspace for preparing and sharing data with analytics and AI platforms. By applying encryption, role-based access, immutability, and time-bound data sharing, Data Rooms help organizations use backup data for AI initiatives while helping to protect against exposure of sensitive information and simplify compliance requirements.

Responsible AI interaction with Commvault Cloud: Capabilities such as Conversational AI and the MCP Server allow AI assistants to interact with Commvault Cloud through a set of APIs governed by the customer's existing identity and RBAC permissions. This gives enterprises a way to explore agentic workflows and conversational operations while keeping authentication, authorization, and audit policies firmly in place.

CORE LEVERS UNDERPINNING COMMVAULT'S AI STRATEGY

1 Enabling Agentic Automation

Commvault is advancing toward a future where intelligent agents coordinate resilience operations across hybrid environments. This agentic foundation combines the Arlie Agent Library with capabilities such as Conversational AI and the MCP Server, helping enable AI-assisted workflows that complement user expertise and policy controls.

Agents work behind the scenes to:

- Analyze operational patterns and surface relevant insights.
- Recommend protection strategies based on coverage and risk.
- Assist with selecting clean recovery points and guiding restoration.
- Support policy-based actions orchestrated through approved APIs.

These capabilities reflect a shift toward a "headless" model of data protection – one built on automation, APIs, and coordination across systems – while preserving the governance, access controls, and auditability that enterprises require.

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

2 Developing and Deploying AI Responsibly

We are committed to the following principles, which embody our dedication to ethical AI development and deployment:

☑ **Reliability, safety, and control**

We have implemented rigorous testing, quality assurance protocols, and security measures.

☑ **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.

☑ **Data privacy and security**

Our AI systems are integrated with Commvault Cloud, limiting external access and enforcing role-based controls. With the addition of Satori Cyber, we extend this protection through real-time access governance for sensitive data, including enforcement and observability across AI workflows.

☑ **Transparency and explainability**

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

☑ **Human-centered approach**

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

☑ **Accountability and governance**

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

Learn more at: https://www.commvault.com/legal/responsible-ai

> **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:	Scalable protection for end-to-end AI infrastructure:	Engineered for automation:	Leading AI security and governance:
Capabilities like Arlie are designed to solve real problems – from automating recovery workflows to surfacing critical insights – not just demonstrate AI for AI's sake.	Commvault is designed to support the full AI stack, including unified data and AI platforms, data lakes, vector databases, and compute infrastructure – all from a single platform.	With native support for open standards like MCP, Commvault enables integration with intelligent agents, customer environments, and future AI ecosystems.	Commvault offers policy-based control over sensitive data access across AI, analytics, and SaaS environments – bridging security, compliance, and AI integrity.

We don't try to be the AI platform – we protect the AI platforms our customers rely on. Commvault is the single platform that combines data protection, cyber recovery, and data access governance – across structured and unstructured workloads. Where others offer isolated tools, we deliver unified resilience for modern AI. 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 →

Commvault®

commvault.com | 888.746.3849