Commvault

SOLUTION BRIEF

PROTECT & LEVERAGE AI

Empower Innovation with Protected, Resilient AI

AI is transforming how businesses innovate — but it's also transforming the threat landscape.

New risks like data poisoning, adversarial prompts, and model corruption can quietly erode trust in AI systems and expose sensitive data.

The challenge and our solution
Hybrid and cloud-native environments amplify these challenges, spreading data and models across multiple platforms, vector databases, and GPU infrastructure — expanding the attack surface and complicating recovery.

Organizations face challenges such as:

- Compromised models or tainted training data disrupting AI accuracy
- Difficulty identifying and isolating AI-related threats across hybrid clouds
- Slow or incomplete recovery after AI system compromise
- Limited visibility and governance across connected AI data pipelines

- **3 in 4 organizations** have suffered an AI-related security incident.
- **Over one-quarter** of enterprises report AI data-poisoning intrusions.
- **Emerging AI threats—** adversarial prompts, poisoned data, runtime attacks—are already impacting real-world operations.

The consequences: corrupted models, business disruption, and IP exposure.[1]

AI Resilience Powered by Unified Data Protection

Help protect AI data, models, and pipelines — end-to-end
Commvault Cloud can safeguard AI data stacks — from data lakes and pipelines to vector databases, models, and compute environments. It helps organizations maintain data integrity, deliver clean recoveries, and extend AI securely across hybrid and multi-cloud ecosystems.

Through policy-based controls, AI-assisted anomaly detection, and verified recovery points, Commvault can deliver AI-enhanced cyber resilience — helping to confirm the data fueling your AI remains trusted, policy compliant, and uncompromised.

Recover confidently with intelligent automation
When attacks or corruption occur, Commvault can automate clean recovery using **AI-enhanced composite cleanpoints**, helping systems return to verified, uncompromised states. This can dramatically reduce downtime, accelerate recovery, and support continuous business operations — so innovation never stops.

Connect securely, innovate freely
With **Data Rooms** for secure data extensibility and **MCP Server** for agentic automation, Commvault Cloud Unity enables organizations to protect, connect, and leverage data across AI ecosystems — without creating new silos or losing control.

This integration-first design supports leading AI and cloud platforms such as **Azure and Snowflake**, allowing enterprises to expand their AI capabilities with full resilience and policy governance built in.

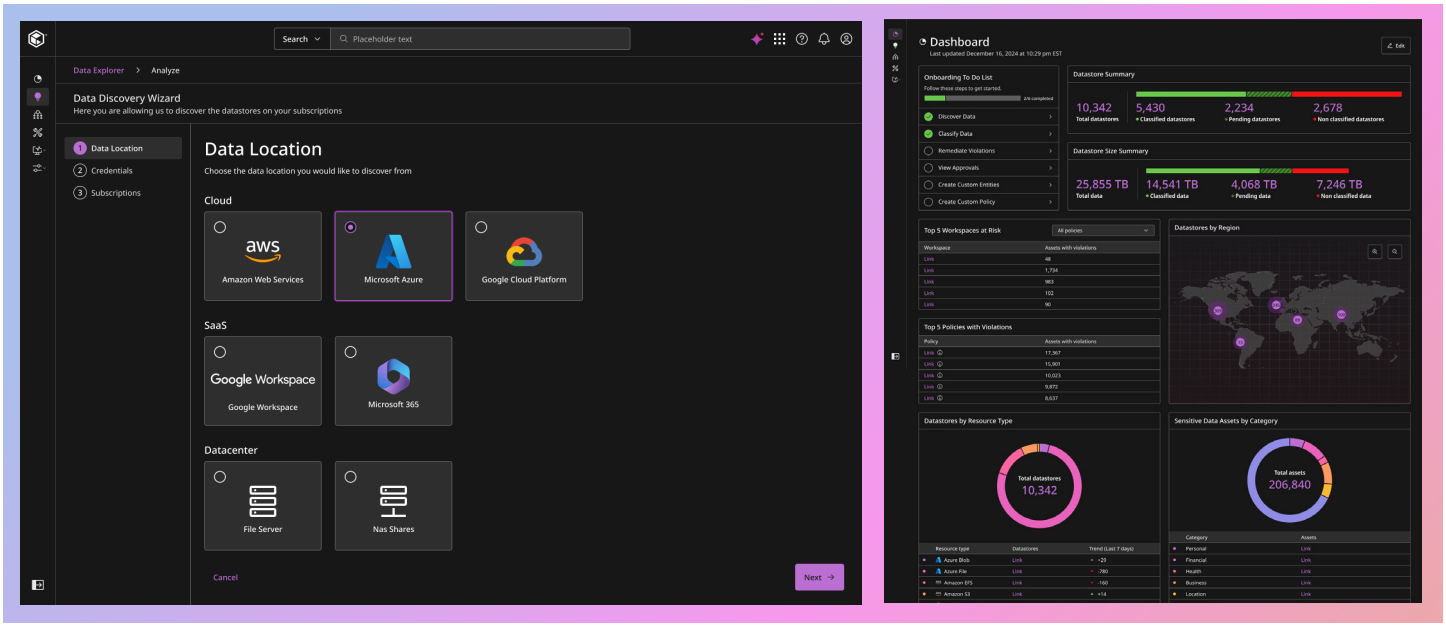
1 The impact is already being felt across industries: more than 75% of organizations report experiencing AI-related security breaches, and 26% of enterprises in the U.S. and UK have faced AI data-poisoning intrusions.

BENEFITS

1 **End-to-End AI Stack Protection**
Help protect AI data, vector stores, and models across on-prem, cloud, and edge with policy-based controls and continuous validation.
→ Empower data integrity across every AI workflow.

2 **AI-Enhanced Detection & Clean Recovery**
Uses AI-assisted analytics to help identify anomalies and rebuild clean recovery points automatically.
→ Minimize impact and restore trust rapidly.

3 **Secure AI Extension & Integration**
Connects safely to enterprise data lakes and AI ecosystems for agentic workflows.
→ Drive innovation with built-in policy governance and resilience.



Learn how Commvault Cloud Unity helps you protect, recover, and extend AI securely — without compromise.
Visit **commvault.com/solutions/protect-and-leverage-ai**