TechArena®

Recovery Is an AI Imperative

What I learned at SHIFT, and why the C-suite should pay attention

By Allyson Klein

November 2026

To say I was excited to go to Commvault SHIFT is an understatement. First, Nashville has a particular pull given its storied history in delivering music to the world. But really, Dolly Parton aside, the opportunity to talk to a room full of CISOs about how they sleep at night was a unique opportunity for learning. I got a terrific education and walked out with one clear conviction. With ramp of AI across enterprise functions and sophistication of attack surfaces mounting, recovery has become an enterprise AI imperative. Not models. Not GPUs. IT has spent the last couple of years grappling there. Recovery.

That may sound like a strange claim from someone who spends most of her time talking about AI infrastructure. But listen to what Commvault CEO Sanjay Mirchandani put on the table in his opening keynote. AI vulnerability now comes from two directions at once: attackers armed with AI, and our own AI agents making errors at machine speed. His call to action to the collective audience was blunt: "AI makes attacks faster, it makes mistakes faster, and it does it with fewer people watching."

> "AI makes attacks faster, it makes mistakes faster, and it does it with fewer people watching."
>
> **Sanjay Mirchandani**
> CEO, Commvault

He backed his perspective up with a story that should be read aloud in every boardroom. An AI coding agent deleted a company's production environment and its backups in nine seconds. Gulp. When customers showed up, the company no longer had the records to serve them. That story has stuck with me since Sanjay shared it, not because it's alarming (it is) but because it's plausible.

Commvault's answer? A confetti cannon of product launches built around a central idea: if vulnerability is continuous, recovery has to be continuous too. Recovery Studio orchestrates the rebuild of entire business services, not just data. AgentRecover audits and rolls back what AI agents did on Microsoft Foundry and Amazon Bedrock AgentCore. New work with NVIDIA, Databricks and Zscaler pushes recovery and governance into the AI data pipeline itself. Fantastic partnerships for a host of companies who enterprise IT relies on are on board, integrating their observability and management into Commvault's suite to ensure IT can recover as an interconnected team. Sweet.

Of course, after a couple of decades in tech, I'm aware that great technology does not always find its way above the line in a budget. Why should the C-suite move recovery to the front of the AI agenda, and why is that so hard for CISOs to make happen? To explore this further, I've given my best thoughts on five reasons executives should prioritize recovery alongside AI proliferation, and two obstacles that keep CISOs from turning that imperative into a funded plan.

AT A GLANCE

5 reasons for C-suite prioritization

01 AI agents are a new kind of unpredictable insider

02 The business runs on services

03 Identity failures are the new blast radius

04 AI is only as trustworthy as its data

05 Recovery lets you scale ROI from AI

2 struggles for every CISO

01 The C-suite views recovery as insurance

02 AI is moving faster than governance can follow

Top Five Reasons for C-Suite Prioritization

01 Your AI agents are a new kind of unpredictable insider

For decades, we treated people as the unpredictable part of the enterprise and systems as the predictable part. BNSF CISO Alex Levy captured the shift on stage this week: AI adds chaos on both sides of that equation pointing out issues with human interaction with AI (human errors) and agents gone rogue as two equally concerning challenges to address with urgency.

That unpredictability and mix of human and agent should get C-Suite attention. An agent with broad permissions can change records, move data and reconfigure systems faster than any human can notice. Prevention alone will not catch every bad action, because many of those actions will be authorized. Commvault's response, AgentRecover, discovers agents, maps their dependencies, audits what they did and restores the agent and the resources it touched. While this, in my mind, doesn't address every eventual outcome of a catastrophic event, it gets an IT organization along the path of agentic meltdown recovery.

02 The business runs on services

Sanjay clearly articulated why data recovery alone was not enough in this age, stating "restoring files was never the hard part." The hard part is bringing back a working business service, with its applications, identities, configurations, network rules and infrastructure, in the right order. This is a complexity that brings most point tools to their knees with Commvault estimating 28 days to recovery based on these traditional approaches.

No executive team would accept a 28-day outage in its AI roadmap, yet many have one built into their recovery plan without knowing it. Recovery Studio is Commvault's attempt to close that gap, and CTO and AI Officer Pranay Ahlawat called it "the DevOps moment for recovery." That got my attention as it speaks to an agility that I haven't seen in historic approaches. While details were light in the conference elements I saw on this subject, the value proposition was quite clear if Commvault can deliver the goods.

03 Identity and attestation failures are the new blast radius

Every agent runs on an identity, and identity systems are where attackers now aim first. Sanjay described attacks on compromised cloud identities designed to destroy infrastructure as a common occurrence for customers. If Active Directory, Entra ID or Okta goes down, nothing else matters, because no one and nothing can log in to fix it.

Signal the confetti! Commvault extended its identity work this week with Identity Attack Intelligence across Active Directory, Entra ID and Okta, plus AD Pre-Recover, a standby replica that can stand up identity services quickly. As non-human identities multiply with every agent deployment, identity recovery belongs on the executive risk register next to ransomware.

04 AI is only as trustworthy as the data behind it

Of course, we were going to get to my favorite subject…data…and how AI is nothing without it. With enterprises ramping inference and agentic tapping live enterprise data, every CEO should ask if the data feeding the company's AI current is authorized and clean. Commvault's collaboration with NVIDIA pairs NIM (NVIDIA inference microservices) and Nemotron Retriever with Commvault Data Activate, so protected data, even cold and tape data, can be tapped by AI with authorization and traceability.

05 Recovery lets you scale driving ROI from AI investment

This was Sanjay's walkoff message, and I think it is the most important business argument of the week: "Recovery is what lets you say yes to AI in the enterprise." He described the shift as moving from insurance to assurance, and you can see a mental model shift within C-suite executives when you tip from a cost to benefit perspective. This is the language CISOs must deliver in strategic planning discussions to get to a yes.

> "Recovery is what lets you say yes to AI in the enterprise."
>
> **Sanjay Mirchandani**
> CEO, Commvault

The two struggles for every CISO

If the case is this clear, why isn't every CISO walking out of the boardroom with a funded recovery plan? From the hallway conversations in Nashville and what I hear from security leaders across our community, two obstacles keep thwarting progress.

01 Cute quips aside, the C-Suite views recovery as insurance

Buried as an IT ops cost, recovery is arguably in the wrong budget, under the wrong owner, with the wrong metrics. Security owns the threat, infrastructure owns the backups, application teams own the services and nobody owns the full rebuild of the business. Who would want to own that pressure?

There is also an accountability trap. When a recovery fails, the CISO often takes the blame even though the budget, the tooling and the runbooks all sit with other teams. That makes some security leaders cautious about raising the issue at all, because naming the gap without the authority to close it feels like owning a failure before it happens.

02 AI is moving faster than governance can follow

Business units are deploying agents on Microsoft Foundry, Amazon Bedrock AgentCore, Databricks and dozens of SaaS tools, often run without a central inventory. When I was leading corporate teams, I saw this all of the time. Move with agility or bring IT in and do something the proper way. In today's pressure cooker environments, guess what happens? It is very hard to protect, let alone recover, what you don't know about.

That leaves CISOs arguing for controls on systems they did not approve and may not know exist. Non-human identities pile up faster than access reviews can keep pace. Commvault's agent discovery and its Zscaler partnership, which pairs AI policy enforcement with rollback of harmful agentic activity, point in the right direction. But the organizational work of getting AI teams to register, scope and protect their agents still falls on the CISO, usually without the authority to require it.

The TechArena Take

Commvault came to Nashville with a tight story and the product news to back it, and I left convinced that the industry has been debating the wrong question. We have spent two years asking what enterprises need to build in order to run AI. The better question is what they need in place to survive it when something goes wrong, because something will. A nine second deletion event is not a hypothetical anymore, and neither is an agent with credentials doing exactly what it was told to do at a scale no one reviewed.

THE STAKES, IN TWO NUMBERS

9 sec

Time it took an AI coding agent to delete a company's production environment and its backups

COMMVAULT SHIFT KEYNOTE

28 days

Commvault's estimate of time to recovery using traditional point-tool approaches

COMMVAULT

What Commvault is selling is less a backup portfolio than a governance posture, and that is where the hard part lives. Recovery Studio and AgentRecover only matter if someone in the organization owns the rebuild of the business, not just the restore of the files. Until that ownership question gets settled at the executive level, CISOs will keep making a technically sound case to a budget process that still reads recovery as insurance.

My advice to the C-suite is simple. Ask your team how long it would take to bring a core business service fully back, and ask who owns the answer. If the room goes quiet, you have found your next AI investment.



TechArena 2026

© TechArena 2026. Other names and brands are property of their respective owners.