SPONSORED CONTENT | WHITE PAPER

The future-ready foundation: What CIOs need to support innovation and compliance efforts

Improve governance, resilience, and data management with a unified data fabric.

CIO

SPONSORED BY CLOUDERA

As systems, data, and decisions become more distributed, CIOs need clear visibility and accountability across their data landscape. But in many cases, that visibility hasn't kept pace with how businesses operate today.

Most organizations didn't intentionally design the complex data environments they now manage. Some decisions were deliberate, made to support growth, resilience, or new ways of working. Others accumulated gradually, as teams added platforms and tools to meet immediate needs.

At the same time, data has taken on a more active role in daily operations, supporting decisions that happen faster and at greater scale. As a result, data, security, and governance teams are being asked to support new AI use cases while regulatory expectations — including the General Data Protection Regulation (GDPR), the Digital Operational Resilience Act (DORA), and state privacy laws — continue to evolve.

With so many changes happening at once, enterprise IT leaders are seeing artificial intelligence (AI) security and compliance risks rise: 46% say data leakage and unauthorized access are top obstacles to AI adoption, according to Cloudera analysis. These risks increase when organizations don't have a unified view of where their data lives, how it's used, and who controls it.

Only 9%

of organizations say all their data is fully accessible and controlled for AI use.

Source: Cloudera, "The Evolution of AI: The State of Enterprise AI and Data Architecture"

Without consistent visibility and governance across IT environments, organizations struggle to enforce policies, demonstrate compliance, or move AI beyond isolated pilots. That's why CIOs need a data foundation that provides agility and resilience, better positioning them to adapt to what lies ahead.

New pressures increase risks

Most organizations now run data across public cloud, private cloud, on-premises, and sovereign environments. In many cases, this is a deliberate choice driven by cost, performance, resilience, and/or regional and regulatory requirements. When planned well, hybrid environments enable teams to place data and workloads where they make the most sense.

Problems emerge when hybrid environments grow by accident rather than design, without a unifying data and governance strategy. Over time, systems that were added for valid reasons often become fragmented data silos that weren't built to operate in a unified way. In addition, data no longer lives only in dashboards and reports. It flows through pipelines, feeds AI models, and drives automated processes that continuously act on it. When data is used by AI systems, access control and audit requirements become stricter.

As organizations expand across hybrid and multicloud environments and push AI into production, they begin to see governance and compliance problems emerge with greater speed and variety. These issues often surface at critical moments — during an audit; when a model is questioned; or when teams are asked to explain where data came from, who accessed it, and how it was used.

Across industries, the same challenges continue to arise:

- **Policies don't carry across environments:** Data and access controls are applied differently across clouds and on-prem systems, creating gaps that are easy to miss.
- **End-to-end data lineage is hard to prove:** As data moves and is transformed for analytics and AI, maintaining a clear, auditable trail across systems and infrastructures becomes difficult.
- **AI adds scrutiny to existing data practices:** Teams are expected to explain how models behave and what data trained them, without knowing how AI regulations might change.
- **Training data is difficult to validate at scale:** Ensuring that models rely on approved, consented, and unbiased data becomes an ongoing governance effort.
- **Teams and skills don't line up with the work:** Data, cloud, security, compliance, and AI teams operate in silos, and few organizations have people who can bridge data platforms as well as regulatory requirements.

Nearly half of IT leaders say regulations delay cloud plans, and more than one-third have moved or plan to move workloads back on-prem due to compliance concerns.

Source: Foundry, "2025 Cloud Computing Study"

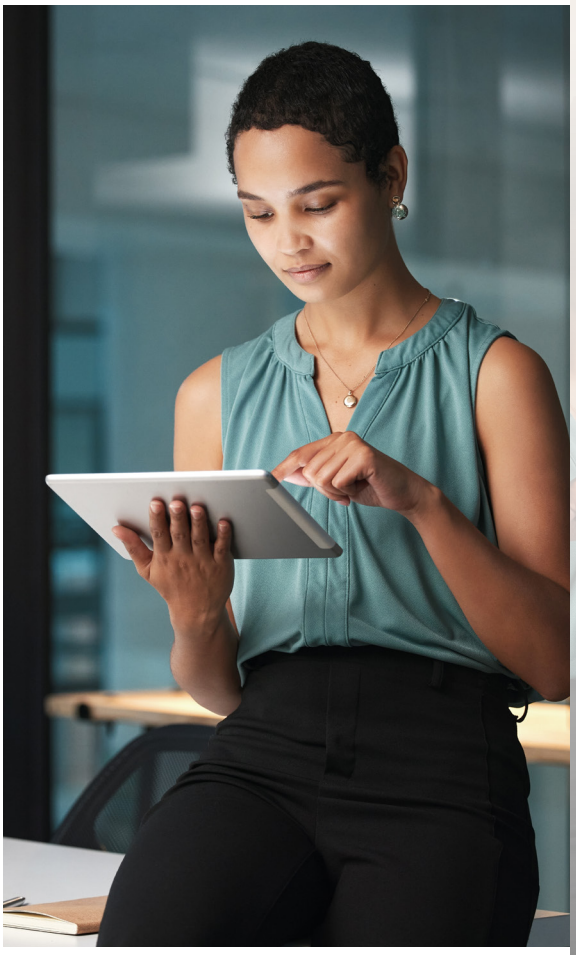
Newer regulations now require continuous proof of proper data handling across all environments, which makes fragmented approaches even harder to sustain. When governance differs from one system to the next, organizations must re-create security policies, audit processes, and review controls each time they add or change an environment. These efforts drive up

costs and increase the risk of human error. Over time, policies may be applied inconsistently or dropped altogether, exposing sensitive data and pulling teams away from innovation.

Prepare your data for whatever comes next

Although IT leaders can't plan for every specific rule, they can put foundations in place that enable their data environments to adapt. What matters most is the ability to introduce new AI use cases, shift workloads or data when regulations or business needs change, and meet new requirements without redesigning their platform each time. Leaders also need to reduce the cost and complexity of managing their data. For example, rather than having to learn and operate multiple platforms, users can manage one platform from a single data control plane.

Two capabilities make this level of flexibility and control possible. First, teams should have the freedom to run and, when necessary, move each workload where it makes the most sense, without rearchitecting or rewriting for each environment. Second, they need unified control over data access and governance so the same rules apply no matter where data or workloads run.



IT leaders can satisfy both conditions with:

- **One set of data policies across environments,** defined once and enforced consistently, even as data or workloads move between clouds, on-prem systems, and AI pipelines.
- **Automatic tracking of data access and use,** enabling teams to quickly explain who accessed data, where it moved, and how it was used, including in AI models.
- **Governance built into data and AI workflows** to ensure that controls are applied before systems go live instead of being added later to fix gaps.
- **Clear, consistent metadata** that helps teams immediately identify sensitive, regulated, or restricted data regardless of where it runs.

With these capabilities in place, IT can adjust accordingly, supporting new priorities while keeping risk under control.

Putting flexibility and control into practice

A shared foundation built on consistent rules, visibility, and guardrails helps IT teams better manage governance as workloads move across environments. Cloudera's unified data fabric ensures that security, access controls, and audit requirements remain consistent wherever workloads run, enabling organizations to adapt without rebuilding governance each time. This enables IT leaders to:

- **Run workloads where they make the most sense, without redesigning the platform:** The same data and AI services run across public cloud, private cloud, on-premises, and sovereign environments, so infrastructure choices reflect business or regulatory needs rather than platform limits.
- **Move workloads as needs change while maintaining controls and visibility:** Access controls, identity, and protections stay in place as workloads move, avoiding blind spots when systems shift.

- **Define governance once and apply it everywhere:** Policies are enforced through shared metadata and identity controls, so the same rules follow data across environments.
- **Prove compliance continuously:** Built-in monitoring and reporting provide a clear view of data access, use, and movement, supporting GDPR, DORA, emerging AI regulations, and data sovereignty requirements.
- **Scale AI without introducing new exposure:** Governance extends to AI pipelines and models before they go live.
- **Replace accidental hybrid complexity with intentional flexibility:** CIOs gain a governed foundation that adapts as technologies, regulations, and priorities change.

Get ahead of regulatory changes

"If you want to do serious work with AI, get your data house in order," says Wim Stoop, Senior Director of Product Marketing at Cloudera. "Governance and security have to come first."

The regulatory landscape continues to evolve, even as AI accelerates how data is used across the enterprise. That's why CIOs need a data foundation that holds steady as requirements, technologies, and environments change.

Cloudera provides that foundation, enabling enterprises to improve compliance, resilience, and readiness for whatever comes next.

Better manage and govern data anywhere it goes. Learn more about Cloudera's Unified Data Fabric.

Lessons learned: How organizations are adapting to regulations

Responding to new data residency requirements

A global financial institution runs fraud detection models across regions. When new regulations require financial data and AI processing to remain within a specific country, the team redeploys the same models and pipelines into a sovereign environment without rewriting applications, meeting the requirement immediately while keeping fraud detection operational.

Enforcing regional data boundaries without limiting analysis

A public sector agency analyzes sensitive citizen data across regions with different privacy laws. By applying consistent governance controls, the agency keeps data confined to its jurisdiction while still enabling approved analysis, ensuring that data from one region is never accessed outside its legal limits.

Maintaining sovereignty without vendor lock-in

A telecommunications provider launches services in a sovereign cloud but wants the option to change infrastructure providers if needed. By separating compute from storage and keeping data in open formats, the company retains control of its data and can move workloads without costly migrations or long-term dependency on a single vendor.

> "Cloudera provides us with the flexibility to adopt a hybrid cloud approach, depending on different regulatory or technical requirements. **This gives us the freedom to always stay a step ahead and mitigate the risk of vendor lock-in."**
>
> – **Ciro Milite**, Director of Data and Digital Services Management, Eutelsat Group

CIO

SPONSORED BY CLOUDERA