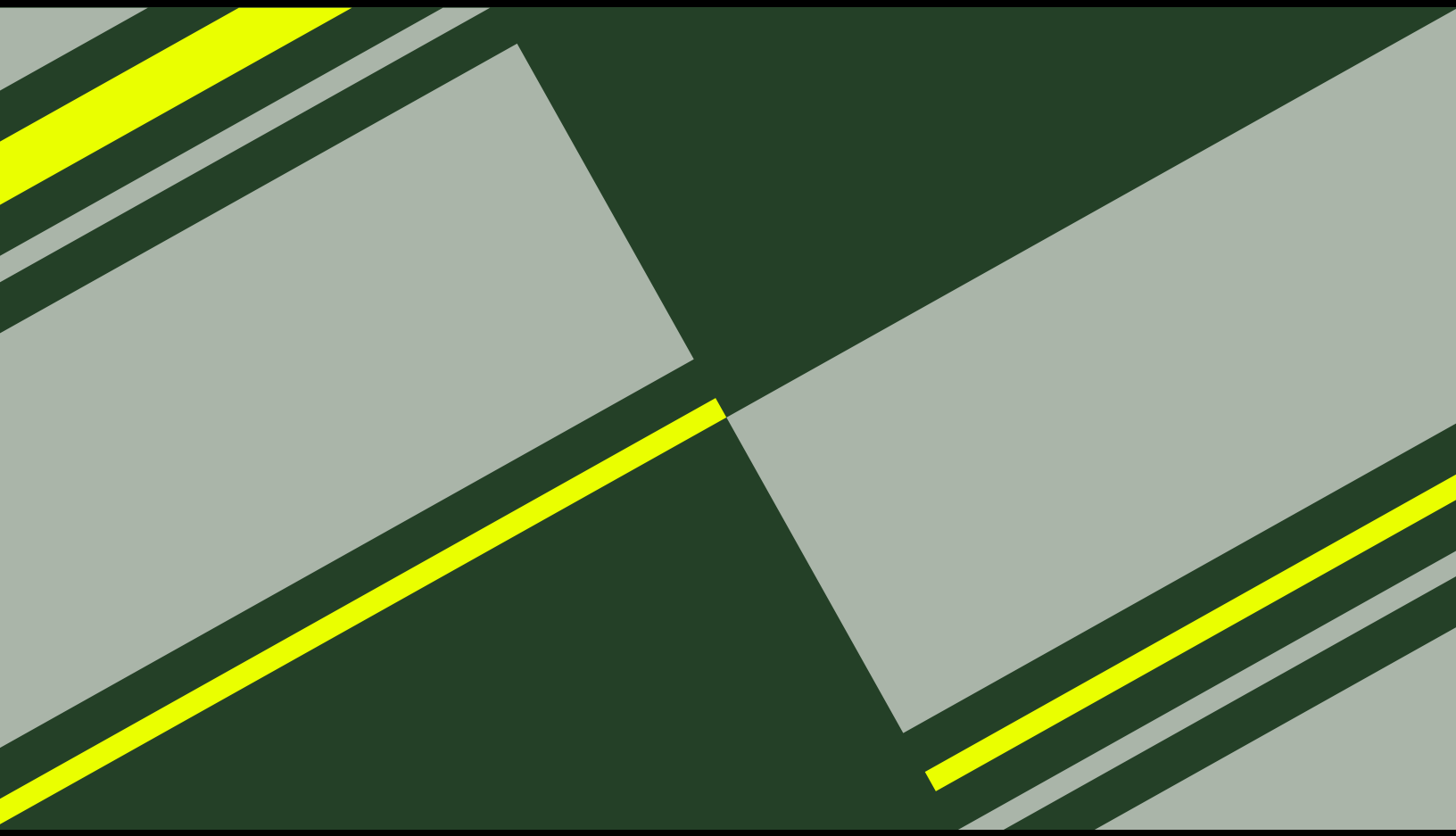
IMMUTA

2025 State of Data Security Report

Over 700 data leaders share their compliance, access, and AI priorities in 2025



SURVEY CONDUCTED BY UserEvidence

Table of Contents

Introduction & Executive Summary

Data practitioners face new AI-driven data demands, a growing selection of self-service data sharing solutions, and heightened security and privacy concerns. As the stakes of accessing and leveraging data get higher, the pressure on data leaders rises, too.

For better or for worse, most teams in this field face similar challenges. We surveyed 700+ IT and data security leaders to understand the most pressing issues they're facing, and the solutions they plan to implement next. **Nearly six out of 10 respondents say that their organization is failing to keep pace with data changes.** They're battling challenges like:

- Data privacy, security, and bias concerns.
- A lack of skilled data professionals to work on initiatives.
- Inability to access the right data at the right time.
- Limited data literacy across their organization.
- Difficulty integrating new data technologies and tools with existing systems.

These obstacles are far from the whole story, though. The majority report optimism about their data architecture, confidence in their data strategy, and understanding from their executive team. Two-thirds say that their data protection efforts have improved over the past year.

This report unpacks both the optimism and apprehension found in these results, to help data security, governance, and compliance leaders understand their industry's landscape and move forward with confidence in the year ahead. Let's dive in.

Terms Used in This Report

Data access governance: Data access governance refers to an organization's policies and procedures that facilitate data access. There are particular models for managing data access, such as role-based access control (RBAC) and attribute-based access control (ABAC). Data access governance refers to the implementation of those models and the management of the policies, including how they are stored, enforced, and monitored.

Data marketplace: A data marketplace is a mechanism for centrally publishing and requesting data products internally. From a single user experience, data consumers can search, find, request, and receive near-instant access to data to make decisions. The internal marketplace layer exists on top of the data storage platform with data access controls and a data catalog operating between. This allows teams to keep their existing data stacks while opening up previously siloed resources to others who will benefit from them.

Data mesh: Data mesh is a modern data architecture design that decentralizes data ownership, leaving data governance and quality in the hands of self-contained domains. Built to meet the needs of hybrid and multi-cloud data environments, data mesh reduces data silos and bottlenecks, and puts data in the hands of those who need it.

Data product: A data product is a curated, self-contained combination of data, metadata, semantics, and/or templates that is designed to deliver specific insights or functionalities that address business needs. Data products are intended to be shared and reused throughout an organization, taking the form of interactive dashboards, reports, machine learning (ML) models, APIs, and applications, to name a few examples.

Data domains: A data domain is a container that organizes data based on a categorical grouping or logical organizational structure. Domains allow data management responsibilities to be assigned to a specific business unit, subject matter expert, or team, which alleviates the burden on centralized IT teams to manage data enterprise-wide.

Key Insights

INSIGHT 01

Security and Access Are Top Concerns as Data Demands Grow

Two-thirds (64%) of data leaders say they face significant challenges providing timely and secure data access to authorized users. At the same time, the most common barriers to data access are privacy and compliance concerns.

Data access issues create far-reaching business impacts, from lost revenue and limited collaboration, to an inability to support customer needs and attract talent.

INSIGHT 02

Data Access Challenges Revolve Around People, Processes, and Technology

Enterprise data use is exploding, and the way employees expect to access and leverage data is rapidly changing as well. To resolve data access challenges, organizations must address issues that are people-, process-, and technology-related:

- 40% of respondents say that 6-10 people are involved in managing data governance and security, while a third say that 20 or more are involved.
- 53% say that data governance processes are done manually, and 62% say that data governance processes slow down the time it takes to access data.
- For 53% of respondents, data and technology management challenges have made managing their workloads more difficult than it was 12 months ago.

INSIGHT 03

Despite Its Potential, AI Presents Implementation Obstacles

54% of data leaders say that integrating AI/ML into business processes is a high priority over the next 12 months, yet 55% agree that their data security strategy isn't keeping pace with the evolution of AI.

The top AI implementation barriers they face range from difficulty integrating it into existing systems, to skills and budget shortages, to evolving regulations.

INSIGHT 04

Data Leaders Expect Results Across Multiple 2025 Initiatives and Investments

In 2025, strengthening data compliance and privacy programs to meet regulatory requirements is the highest priority initiative for data leaders, reiterating the importance of compliance to enable data access, rather than blocking it. Data access initiatives are pressing as well, with 44% focused on internal data products and 42% prioritizing self-service data access.

Across investments, data leaders are focused on business outcomes like faster access to data (32%) and improved compliance (26%).

INSIGHT 05

Data Challenges Are Primed To Become Opportunities

Three-quarters of data leaders feel confident in their organization's ability to address data threats, and two-thirds say that their ability to protect data has improved compared to a year ago.

While many organizations still contend with bottlenecks and data silos, these challenges pose an opportunity to embrace new self-serve solutions and federated models of data governance. Data leaders are likely to implement data marketplaces (68%), domain data ownership (70%), and data monitoring solutions (82%) in the coming year.

Methodology

Immuta commissioned independent market research agency UserEvidence to conduct the 2025 State of Data Security Survey.

Who are the survey respondents?

700+

data leaders and professionals surveyed.

48%

of respondents work in IT/Technology sectors.

Countries represented

United States, United Kingdom, Canada, Australia

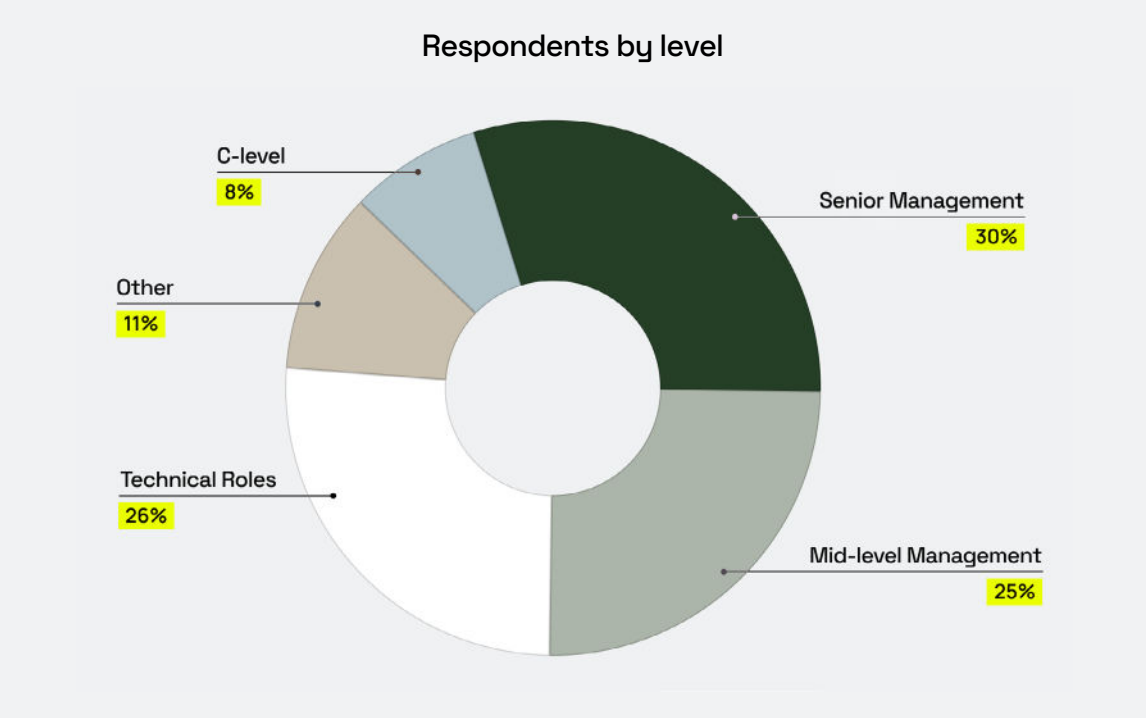
The study surveyed more than 700 data leaders and professionals from enterprise organizations across the US, UK, Canada, and Australia.

Nearly half of respondents come from organizations with 500-2,999 employees, while just over half come from organizations with 3,000 or more employees.

Respondents represent global, cloud-based enterprise companies across public and private sectors, with just under half (48%) from the IT and technology sectors.

Eight out of 10 respondents are employed within IT, while another 10% come from engineering, and 6% from data services and data management.

Nearly half of respondents hold leadership positions, ranging from C-level (8%) and senior management (30%) to mid-level management (25%) and technical roles (26%).



The most common job titles include IT or Engineering Director (21%), IT or Engineering Manager (14%), and Head of IT or Engineering (10%).

Respondents play a primary role in their organization's data management, with three-quarters (76%) saying that they regularly use data analytics, data governance, or data transformation tools in their role, and the remaining 24% reporting that they do so occasionally.

INSIGHT 01

Security and Access Are Top Concerns as Data Demands Grow

Respondents continue to wrestle with the age-old balance between accelerating data access and maintaining a secure environment.

"Compliance and access are highly correlated. I don't know if you could ever decouple them," says Joe Regensburger, Immuta's VP of Research. Data leaders feel the pressure to choose between agility and protecting their data. This false dichotomy pits the needs of the business against the security team's priorities — and pits both against the data team.

Nearly two-thirds (64%) of data leaders say that **their organization faces significant challenges in providing timely and secure access to data for authorized users.** And while a range of barriers stand in the way of access, half of survey respondents identify compliance and privacy as their primary data concerns in 2025.

64%

face significant challenges providing timely, secure data access to authorized users.

50%

say compliance and privacy are their top data concerns in 2025.

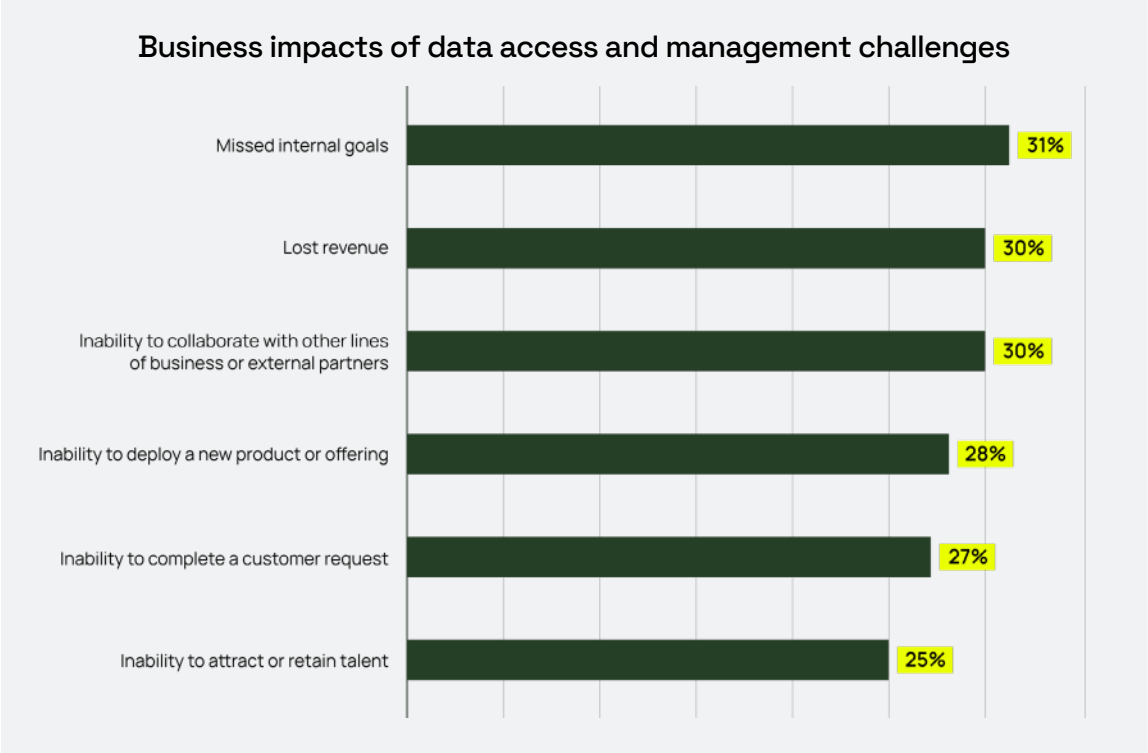
The other top barriers data leaders face trace back to one of these two core challenges:

- **Security concerns:** Along with compliance and privacy, 39% of respondents report complex and unscalable data access policies and processes.
- **Siloed, fragmented, or inaccessible data:** 45% face data silos and fragmentation across teams, and 36% cite a lack of centralized data access management system. 34% don't have the resources to handle data access requests, and the same percentage point to their legacy tools and processes lacking agility.

Enterprises have a responsibility to protect their customer and proprietary data. Yet for the sake of the business, they also need to put their data to work. Until they can reconcile those two goals, they'll see widespread consequences.

The Ripple Effects of Data Access

Data access issues create tangible downstream effects on business performance. Respondents attribute these business impacts to data access and management challenges:



To sum up that list in one data point, over half of respondents rate the impact of data access barriers on their organization's ability to achieve its business objectives at a 4 or higher on a scale from 1 to 5.

More importantly, two-thirds (64%) agree that **data access challenges have impacted the ROI of their company's data platforms.** Organizations are investing heavily in these tools for storing and leveraging their data — but a data platform can only make a business impact if its data is accessible to business users.

> **"From a business value point of view, getting data into the hands of people that can extract value from it, is the number one priority."**
>
> **Joe Regensburger, VP of Research, Immuta**

Data access challenges are nothing new, but the urgency to solve these problems is higher than it has ever been. Next, we'll unpack the specifics of this challenge and how they impact enterprises.

INSIGHT 02

Data Access Challenges Revolve Around People, Processes, and Technology

The challenge of managing enterprise data isn't just that the volume and complexity are exploding. The way data consumers expect to access data is also changing. They demand speed more than they value controls, and they're telling IT what they want, rather than asking what data is available.

> **"From a business value point of view, getting data into the hands of people that can extract value from it, is the number one priority."**
>
> **Steve Touw, Co-Founder and CTO, Immuta**

When asked about their biggest roadblocks to efficient data access and management, respondents validated that the challenge is three-pronged, rather than singular:

PEOPLE

44% cite too many people or teams involved in data management and decision-making — the top response — while 36% note difficulty communicating with other stakeholders.

PROCESSES

42% point to not having the right processes in place.

TECHNOLOGY

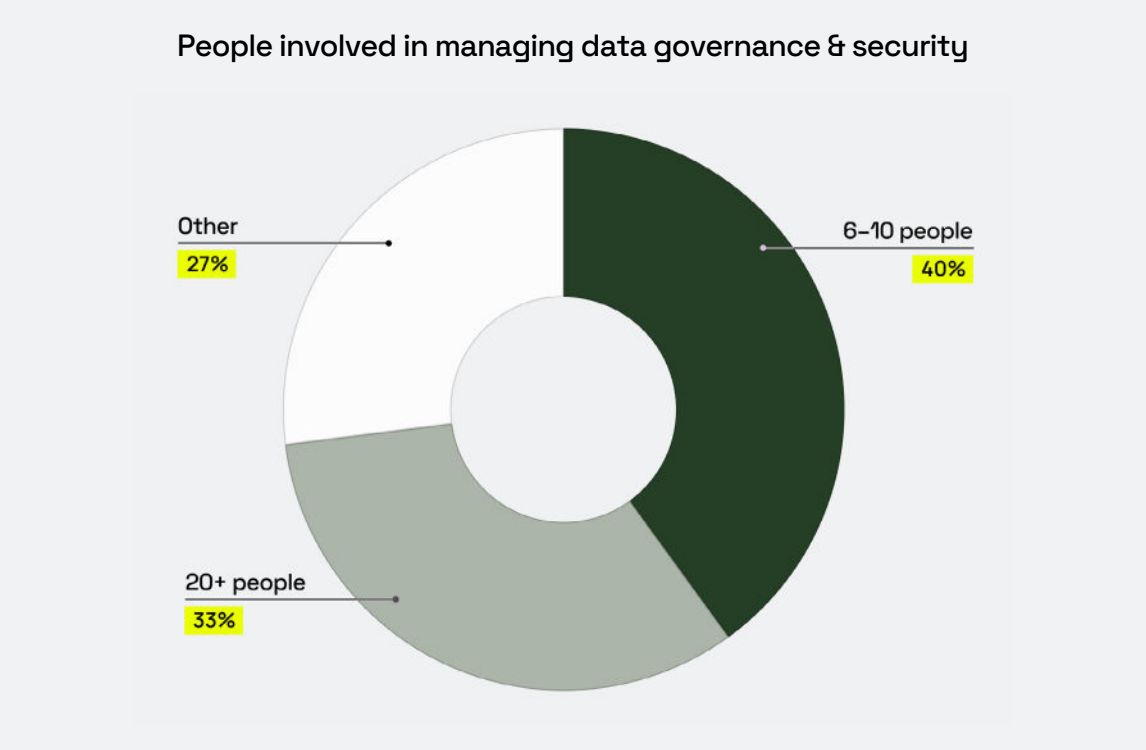
41% say not having the right tools blocks efficient data access and management.

Here's how each of those facets plays out.

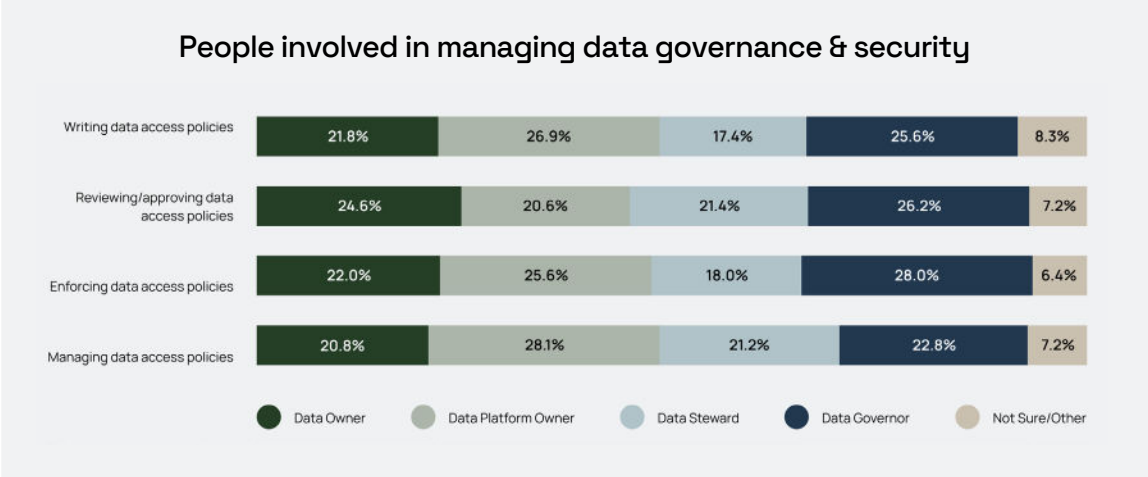
People: How the Data Consumer Has Changed

In 2025, a data consumer can come from anywhere in the organization — not just data engineering or IT — thanks to generative AI putting more data in more employees' hands. To grant wider access faster, enterprises need solutions like internal data marketplaces that offer proactive security, data monitoring, and self-service access.

Alongside growing data consumer numbers, many organizations still have too many layers of review and approvals. 40% of respondents say that six to 10 people are involved in managing data governance and security at their organization, while a third report that 20 or more people are involved — the more dependencies, the more risk of miscommunication and inconsistency.



Across all respondents, responsibilities for most data workflows are spread somewhat evenly across data owners, platform owners, stewards, and governors. While platform owners are most often responsible for writing (27%) or managing data access policies (28%), data governors most often enforce these policies (28%) and audit for compliance (25%).



For sustainable data access at scale, enterprises need visibility first and foremost. They need an understanding across all teams of what data products departments are using, what constraints apply, and what steps are involved in approval.

> **"Greater visibility means data consumers aren't fishing for access — they know what's permissible and what's not. Data governors know the job requirements of the internal customers who are asking for access. A marketplace helps scale because it looks across an organization and provides insights on every employee's wants and needs to get everyone on the same page."**
>
> **Joe Regensburger, VP of Research, Immuta**

Process: Enterprises Overwhelmed by Policies

Three-quarters of respondents agree that their organization has a clearly defined and well-documented data governance strategy. But while speed and security aren't mutually exclusive, implementation currently creates bottlenecks. Over half (53%) say that **most data governance processes are done manually,** and 62% say that **data governance processes slow down the time it takes for users to access data.**

53%

say that most data governance processes are done manually.

62%

say that data governance processes slow down the time it takes for users to access data.

51%

feel overwhelmed by the number of data access control policies they use to manage data.

What's more, 51% of respondents feel overwhelmed by the number of data access control policies they use to manage data. This pressure stems from a wide swath of both internal and external regulations — seven out of 10 data leaders are subject to 10 or more, including 33% that are subject to 25 or more. When the governance processes to comply with these regulations are manual, everything slows down.

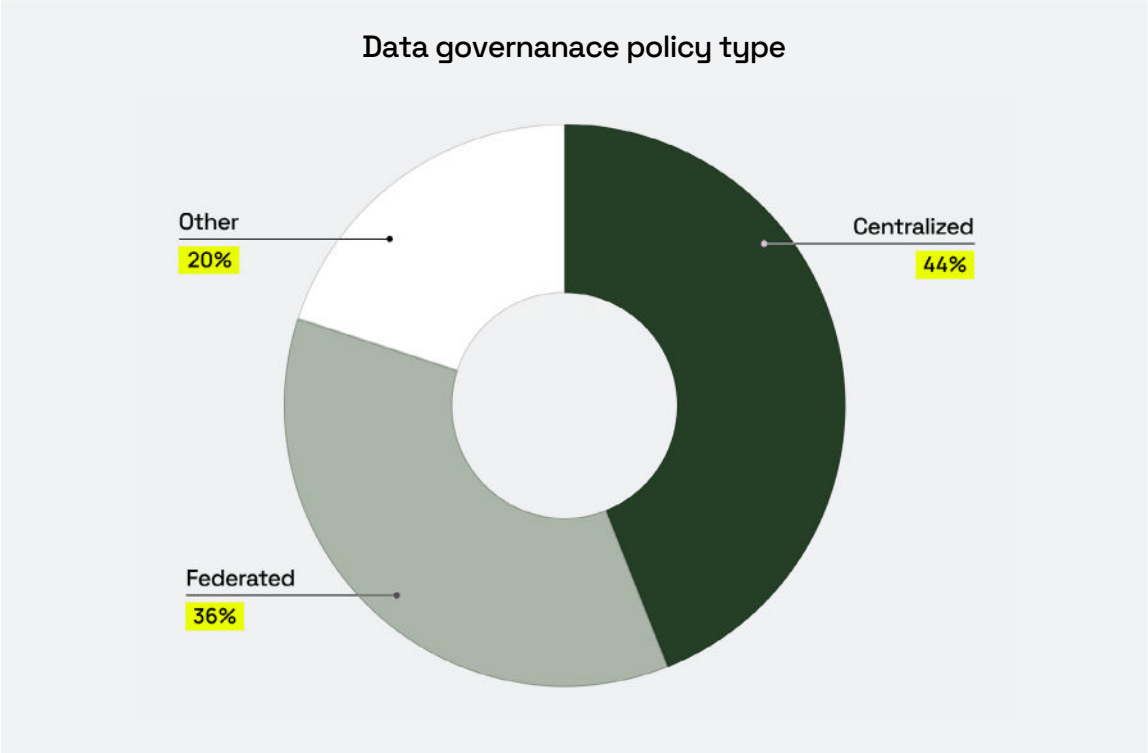
> **"If you have the right privacy controls in place, you can actually give more data to more users instead of having to lock it down and keep it within certain domains or teams."**
>
> **Bart Koek, Field CTO, Immuta**

Respondents most commonly said that their approach to data governance is centralized, with strict control and oversight (44%). This is the status quo due to legacy approaches to data platforms and consolidation, but it can result in massive silos and access challenges, including cumbersome policies.

Yet, when done properly — through dynamic policy enforcement and a unified strategy — governance is an enabler, not a blocker.

The policy overwhelm that data leaders feel is driving a shift in enterprises' approaches to data governance. Federated data governance, with shared responsibility and accountability, makes a strong showing (36%) – and this number is likely to grow.

"A lot of organizations have the goal to get to the federated model," explains Bart Koek. "It strikes a balance and allows the departments to settle their specific rules because they know how to control their data best while still complying with the global regulation."



In recent years, many businesses have adopted a data mesh architecture to allow data domains to create their own data products and control how they are put to use. While this approach decentralizes control of the data, it creates challenges of its own, from new silos to monitoring issues to policy management. Organizations need modern platforms that allow self-service access along with dynamic policy enforcement and unified governance.

Technology: Time To Rethink the Legacy Tech Stack

When enterprises first recognized that more data equaled better decisions, they went all in on data consolidation within platforms. Today, we're seeing the ramifications of having a data repository that's built for data collection but not visibility.

Data silos create delays in data access — over a third (37%) of respondents say it takes them at least a week to access data after requesting it. In some good news, this number has decreased since our 2024 research, when 44% said accessing a new dataset took a week or more. Yet there's still room for improvement, especially when a third of data leaders say that data users can't easily find, request, and access data without IT support.

53% of respondents say that data and technology management challenges have made their workload more difficult than it was a year ago.

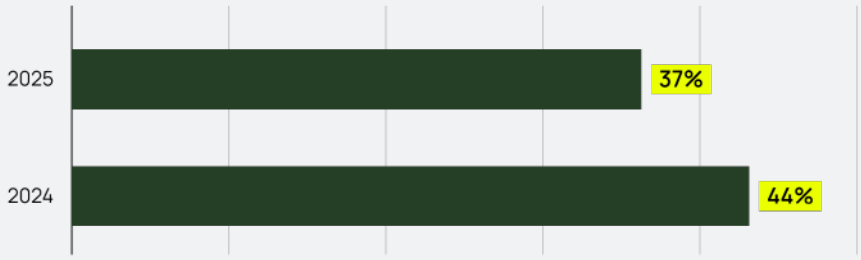
33%

of data leaders and professionals surveyed say that data users can't easily find, request, and access data without IT support.

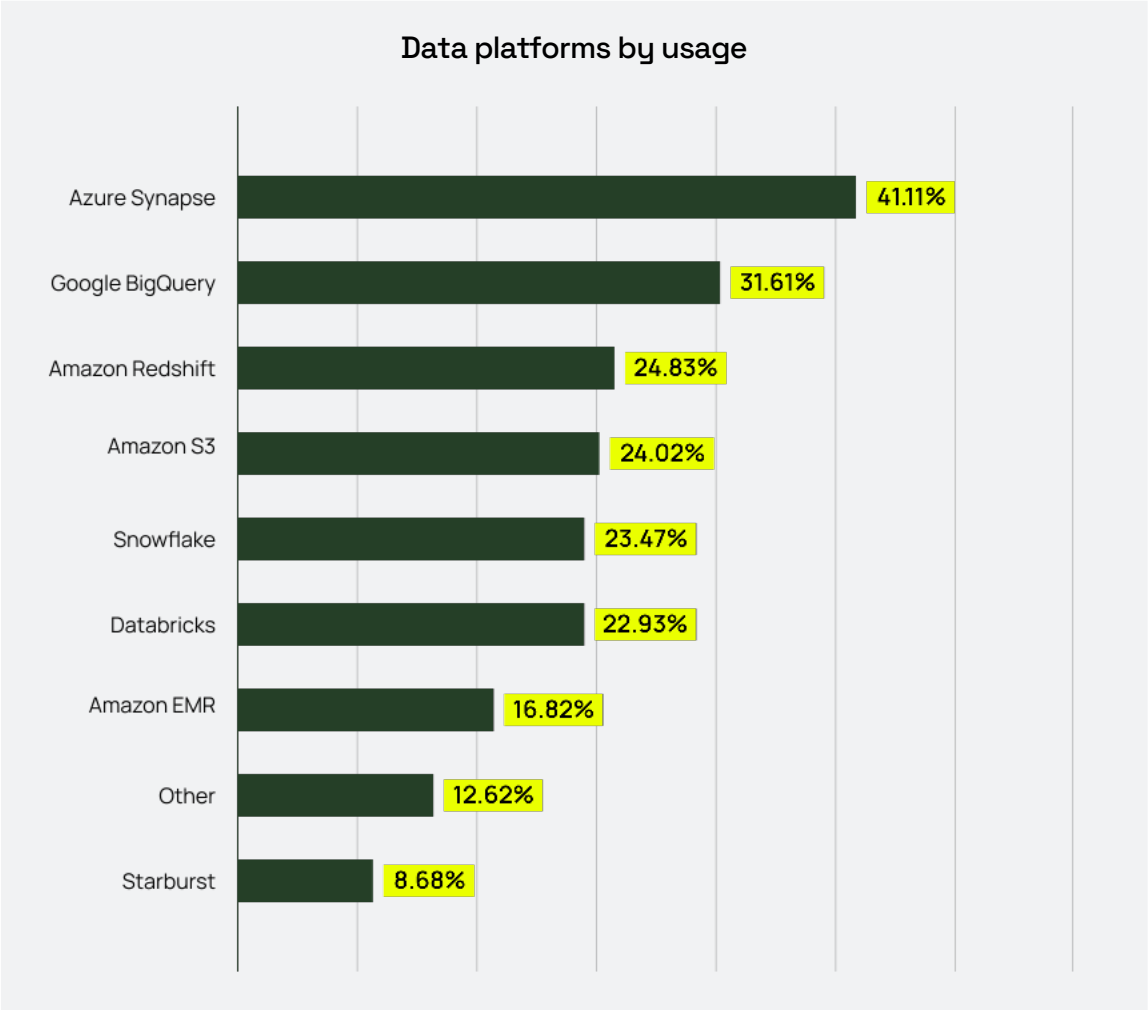
53%

data and technology management challenges have made their workload more difficult than it was a year ago.

Respondents who report waiting a week or more for data access



The existing legacy data stack holds today's data consumers back from the very insights and decision-making that led to big data in the first place. It's not enough to have the data. Enterprises need to either build new access controls on top of their data platforms or replace the legacy infrastructure altogether.



A federated model of data access and management will allow organizations to democratize data consumption and data products, and centralize data governance and security. The result? Better data access for individual lines of business, and ultimately better productivity across the business.

To navigate data silos and get the most out of the data without building a custom large language model (LLM) from scratch, enterprises turned to retrieval-augmented generation (RAG). But organizations are looking for other approaches to build on RAG, which will address fragmented data and leverage it for one of their most pressing workflows: AI initiatives and tools.

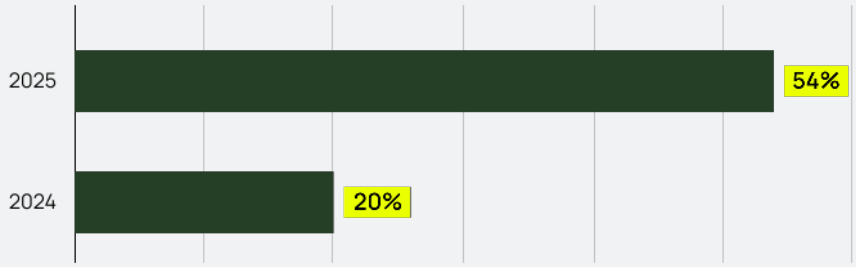
INSIGHT 03

Despite Its Potential, AI Presents Implementation Obstacles

AI continues to hold strong as a top enterprise priority. 47% believe that AI/ML integration will have a high impact on business outcomes, and they're planning accordingly for the coming year:

- Three-quarters of respondents say their organization is likely to implement AI/ML applications in the coming year.
- 54% of data leaders say that integrating AI/ML models into business processes to improve decision-making or automation is a high priority over the next 12 months, placing AI second only to security initiatives. This is a significant jump from last year's research, when just 20% of respondents said the same.

Integrating AI/ML models into business processes as a high priority



Many organizations remain in a speculative, aspirational stage of AI implementation. As Bart Koek explains, "People want to use AI, and they're trying to get the first use cases live. They have security and other concerns, but they're not at the stage yet where those problems actually occur." Early on, security and scalability are valid concerns. But it's the right time to practice AI with a few initial key use cases, and address those issues as you build.

Mark Guntrip, Immuta VP of Portfolio Marketing, recommends considering your position on the AI maturity curve.

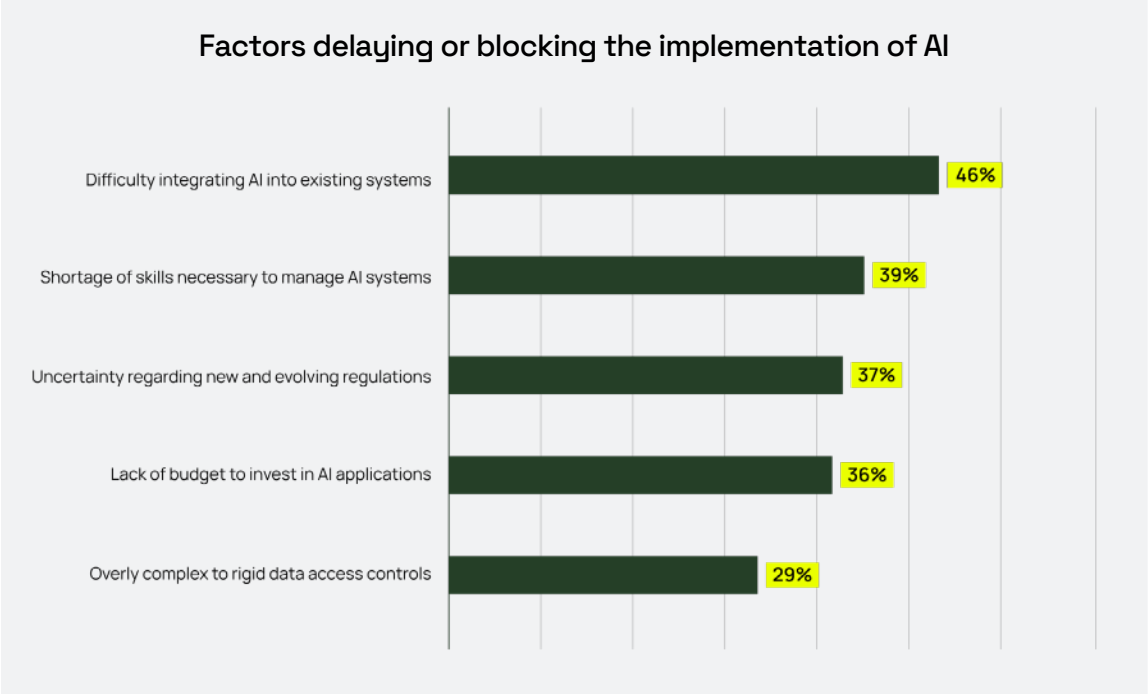
Are you still "experimenting," or are you investing in specific use cases or pilot projects? If the latter, do you know who your data consumer is? Once you're clear on who your data consumer is, your top priority is to make those use cases available and to scale them across your organization.

Most data leaders are facing implementation barriers as they progress through these stages — here's what they're up against.

The AI Obstacles Data Leaders Face

Despite high hopes for AI outcomes, many feel that their organization is falling behind. Over half (55%) agree that their data security strategy is failing to keep pace with the evolution of AI. This number is even higher than the 50% who said they weren't keeping pace in 2024.

What is limiting their progress? Respondents cite a range of factors delaying or blocking the implementation of AI applications within their organization, with the top responses including:



Most of these barriers represent the growing pains of AI, especially integrating AI into existing systems. Integration is primarily an upfront investment in making sure whichever models you use can access data in secure and compliant ways that *also* drive business value.

While data access controls are further down the list, they're still a blocker for nearly a third of data leaders — which likely stems from the regulatory uncertainty and compliance challenges AI brings. The more data that enterprises send to external providers (LLMs), the more they move outside their zone of control — and the greater the security risks they face. Data leaders can address these issues in two ways:

1. Clarify end-user agreements with external providers. Know what's being shared and what's being used to train the next generation of models, and your data obligations to your customers.
2. Implement access control solutions at the data layer – not just the prompt layer – as part of your tech stack, with controls for what data can be sent, where, and why.

AI can drive massive business value if organizations solve the problem of access and agility versus governance and security. The modern data marketplace fills those gaps by defining the roles, rules, and capabilities that lead to success with AI and other initiatives.

INSIGHT 04

Data Leaders Expect Results Across Multiple 2025 Initiatives and Investments

Last year, data leaders contended with more challenging workloads, manual processes, and slow time to data. But data investments continue to grow in 2025: Seven out of 10 data leaders say that their data security budget has increased over the past 12 months, similar to last year. Where are those investments going this year?

Security as a Top 2025 Priority

Respondents revealed that the highest priority data initiative over the next 12 months is strengthening data compliance and privacy programs to meet regulatory requirements (58%). We also found that:

- 78% of data leaders say that their data governance or security tools need to be improved.
- 41% cite increasing data security and governance training as a high-priority initiative this year.

58%

of data leaders say that strengthening data compliance and privacy programs to meet regulatory requirements is their highest priority data initiative.

78%

of data leaders say that their data governance or security tools need to be improved.

41%

of data leaders cite increasing data security and governance training as a high-priority initiative this year.

Doubling Down on Data Products

With 44% of respondents focused on developing and sharing internal data products in 2025, the effort being put into data access initiatives will extend to data product publication and management.

The expected impact of these efforts is rising, too. 43% of respondents say that accelerated internal data product publishing would have a high impact on the business, a massive jump from 13% of last year's respondents.

Enterprises are also looking outward at data products. Another 26% say monetizing their data through external data products is a priority, pointing to specific use cases for their data beyond compliance and access.

44%

of respondents are focused on developing and sharing internal data products.

43%

say accelerating internal data product publishing will have a high impact on the business.

26%

are prioritizing monetization of external data products.

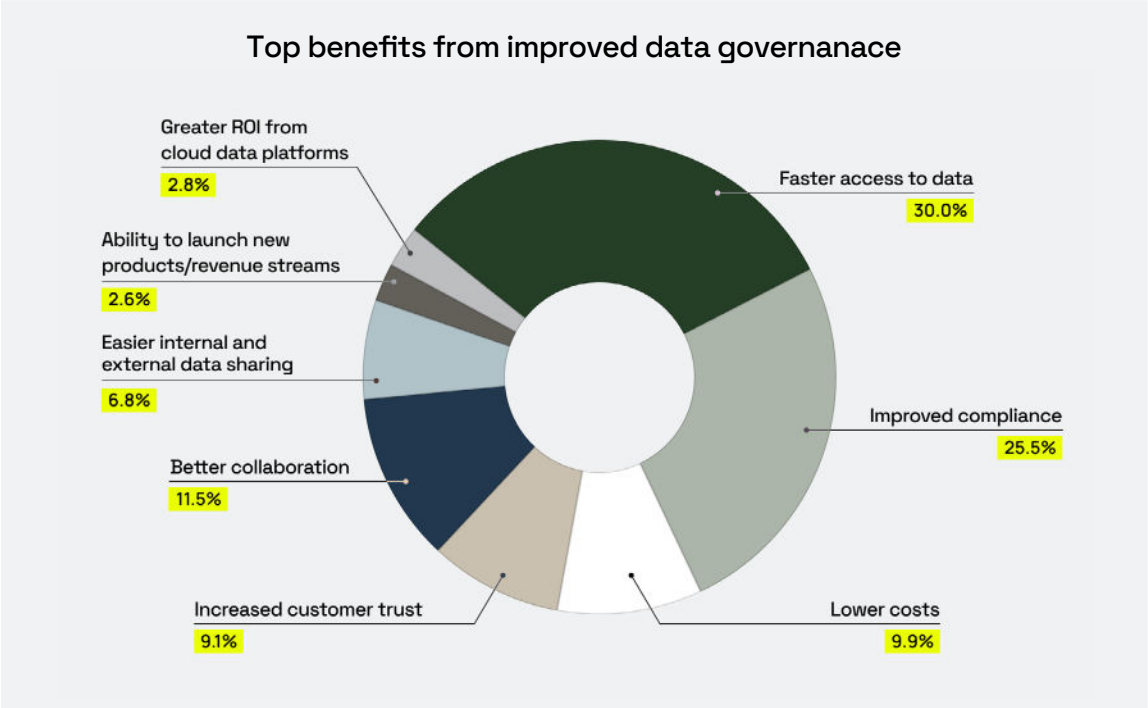
The Push for Self-Service

With access and visibility as business-critical goals, it's no wonder that 42% cite enabling self-service data access for users across the organization as a high priority.

What's more, they anticipate results from these data efforts. 48% believe that self-serve data access will have a high impact on business outcomes, and 41% say the same about data marketplace implementation – which is a primary medium for publishing and sharing data products.

The Expected Outcomes of These Investments

In the next year, respondents expect their organization to benefit from improving data governance processes in two key ways: faster access to data (32%) and improved compliance (26%). Respondents could only pick one response to this question, so these benefits lead by a wide margin over other potential benefits like better collaboration (12%), lower costs (10%), and increased customer trust (9%).



As we've seen, access and compliance are interrelated outcomes — and enterprises will see the strongest business results when they treat governance as an enabler rather than a blocker.

When you have the right compliance measures in place, you can access more data and put it to work more effectively.

INSIGHT 05

Data Challenges Are Primed To Become Opportunities

Despite the changes and challenges data leaders face, it bears repeating that two-thirds feel that their ability to protect data has improved compared to a year ago. Even while roughly three-quarters of respondents feel confident in their organization's ability to address data threats, they acknowledge room for improvement.

66%

say their ability to protect data has improved compared to a year ago.

75%

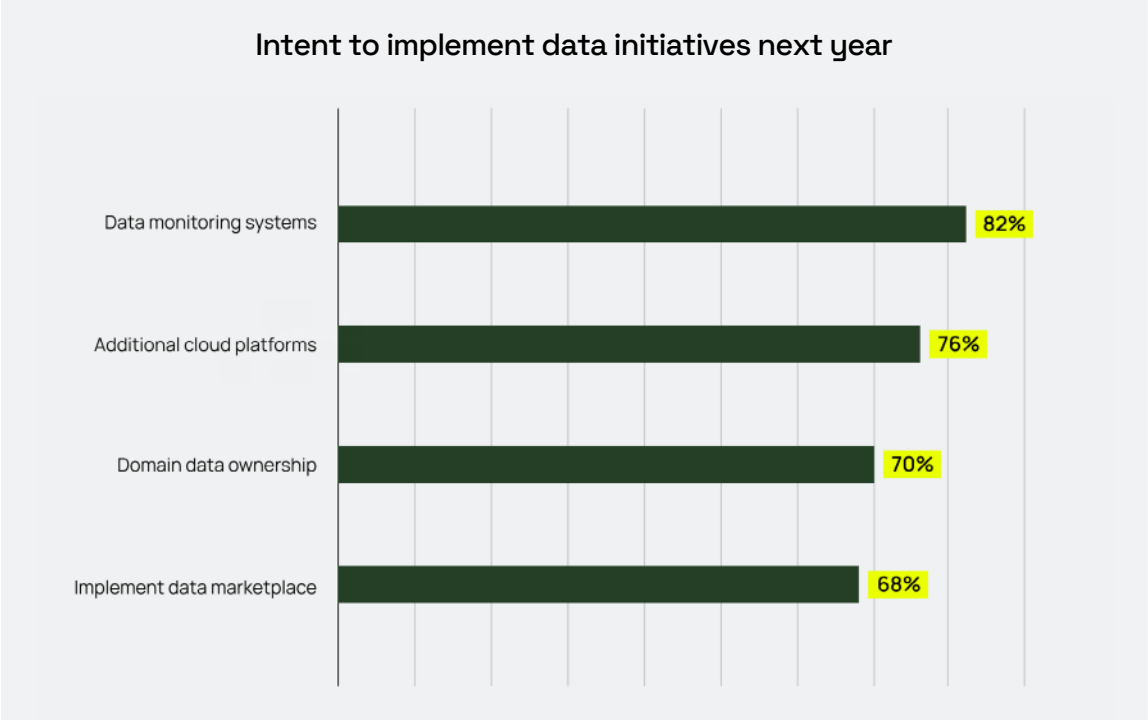
feel confident in their organization's ability to address data threats.

Many, if not most, enterprise organizations remain entrenched in the status quo assumption that governance slows down access. They accept manual data policies because they've been operating within them for years. For the 37% whose data consumers wait a week or more to access data and the third who still need IT support for data requests, these bottlenecks are business as usual — even if they're holding the business back.

> **"Quite often, we see people use manual security processes for years. It might seem okay, but they don't think about how it could be a lot better by having the right policies in place that scale or having a marketplace that automatically provisions the data."**
>
> **Bart Koek, Field CTO, Immuta**

Rather than accepting these norms as inevitable, it's time for data leaders to turn these challenges into opportunities. In the next year, respondents share that they're likely to implement data initiatives like:

- Data monitoring systems (82%). This investment signals that enterprises are doubling down on data protection by understanding the data they have and how it's being used.
- Additional cloud platforms (76%). Data volumes only continue to grow, so organizations need flexible, accessible platforms that give the right teams access to the right data.
- Domain data ownership (70%). Along with the 68% who are likely to implement a data marketplace, this finding reveals the need for distributed data ownership and self-service data access that meet changing data consumer needs.



Taken together, these initiatives point to platform owners' desire to drive adoption and ensure that people use the data — while also incorporating controls to prove data isn't being overshared. Data marketplaces offer a clear solution.

An internal data marketplace gives near-instant data access to the consumers who need it. After being published, internal data products are available for employees to easily and securely find and use. This enables more seamless internal data sharing across teams, so multiple departments can access and benefit from datasets. But it also enhances data monitoring capabilities and unified auditing to ensure security without sacrificing speed.

> **"You want to give them the freedom to build these data products, but you have to put some guardrails in place so that your vision will actually work — you can share data products across lines of business and ensure that governance and compliance are being followed appropriately. Without those guardrails in place, you're going to fail."**
>
> **Steve Touw, Co-Founder and CTO, Immuta**

A data marketplace makes it possible to put such guardrails in place while freeing up the lines of business to build and publish the data products they need. It's the solution enterprises need to put data in the right hands – and keep it out of the wrong ones.

Find Your Partner in Data Access and Security in 2025

Scaling your data stack to overcome existing fragmentation and handle the ongoing influx of data (plus consumer needs and requests) is the order of the day. The right approach to governance ensures that your customer and proprietary data stays protected. And instead of holding back business initiatives, it enables your data to go where it needs to serve the business.

As you look to the year ahead, envision a new approach to data for your organization: one where consumers can efficiently discover data products, where you can seamlessly enforce policies that don't hinder progress, and where data accelerates business innovation.

> **"What's not uncertain is that data continues to grow, and there is a lot of value in it. As the potential footprint of your data expands, access becomes more of a business value question than a regulatory question—how broadly data is shared and how tightly it's controlled"**
>
> **Joe Regensburger, VP of Research, Immuta**

Unlock the full potential of your data – without compromising security or compliance. The Immuta Platform empowers you to safely scale data access, automate governance, and enable self-service access for faster, smarter insights.

Take the first step to putting your data to work – safely and confidently.

Glossary

Data access governance / **Data access management:** Data access governance and data access management are often used interchangeably. Both terms refer to an organization's policies and procedures that facilitate data access. There are particular models for data access, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). This term refers to the implementation of those models and the management of the policies, including how they are stored, executed, and monitored.

Data domains: A data domain is a container that organizes data based on a categorical grouping or logical organizational structure. Domains allow data management responsibilities to be assigned to a specific business unit, subject matter expert, or team, which alleviates the burden on centralized IT teams to manage data enterprise-wide.

Data marketplace: A data marketplace is a centralized location for data consumers to search, find, request and receive access to data from a single user experience. The internal marketplace layer exists on top of the data storage platform with data access controls and a data catalog operating between. This allows teams to keep their existing data stacks while opening up previously siloed resources to others who will benefit from them.

Data mesh: Data mesh is a modern data architecture design that decentralizes data ownership, leaving data governance and quality in the hands of self-contained domains. Built to meet the needs of hybrid and multi-cloud data environments, data mesh reduces data silos and bottlenecks, and puts data in the hands of those who need it.

Data product: A data product is a curated, self-contained combination of data, metadata, semantics, and/or templates that is designed to deliver specific insights or functionalities that address business needs. Data products are intended to be shared and reused throughout an organization, taking the form of interactive dashboards, reports, machine learning models, APIs, and applications, to name a few examples.

Generative AI: Generative AI is a form of artificial intelligence that uses generative models to create and output various content types, including text, images, graphics, audio, and video.

Large Language Model: A Large Language Model (LLM) is a type of machine learning model known for its natural language processing (NLP) capabilities. LLMs are trained using massive data sets, and can both understand humans and generate conversational responses to questions or prompts.

Machine Learning: Machine learning (ML) is a subset of artificial intelligence (AI) that uses data and algorithms to train machines to learn as humans do. ML plays an emerging role in the data science field, as algorithms learn to review large data sets then identify patterns, predict outcomes, and make classifications.

Unified audit: Unified audit capabilities provide a single, transparent view across all data access, enabling visibility to accelerate audits and ensure compliance.

About Immuta

Immuta enables organizations to unlock value from their cloud data by protecting it and providing secure access. The Immuta Data Security Platform provides sensitive data discovery, security and access control, data activity monitoring, and has deep integrations with the leading cloud data platforms. Immuta is now trusted by Fortune 500 companies and government agencies around the world to secure their data. Founded in 2015, Immuta is headquartered in Boston, MA.

IMMUTA®

25 Thomson Place, 4th Floor, Boston, MA 02210 immuta.com (800) 655-0982