privacera

Governed Data Stewardship

Cut the bad—cost, complexity, confusion. Get the good—speed, security, simplicity.

WHITEPAPER

privacera

contents

EXECUTIVE SUMMARY

This white paper describes how organizations can eliminate the complexity and IT cost of managing data access while enabling the business to get the data they need faster. With this approach, organizations are able to eliminate a major IT bottleneck, reduce IT costs, increase business agility, and improve the enterprise's security posture. The business gets data faster, eliminates complexity and costs managing data access, industrializes data products and creates faster time to insights. Additionally, the corporate data security posture is improved by ensuring data is used for the right purpose, eliminating data proliferation, and establishing centralized auditing.

INTRODUCTION

Without question, data stewardship is at the heart of data governance, regardless of the type of data governance being implemented.

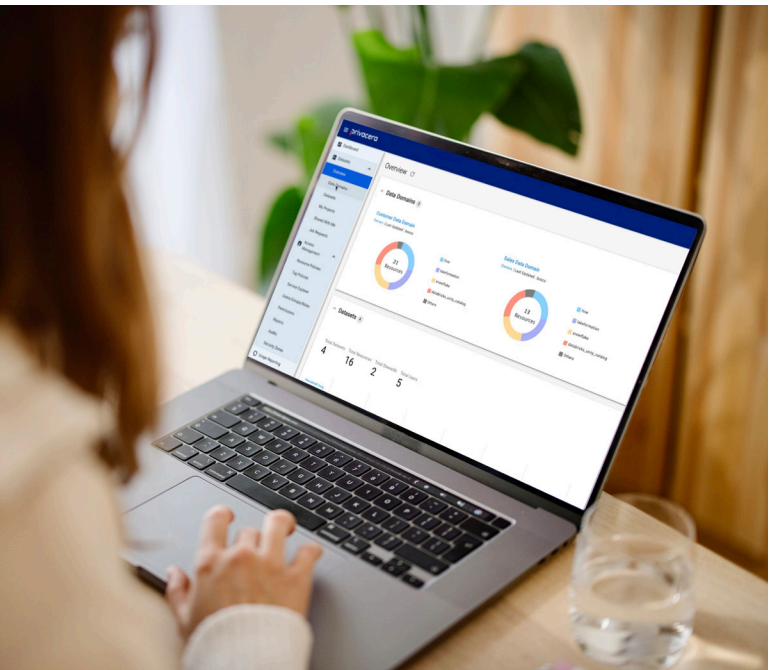
This is because data stewards provide the day-to-day data management for their organizations. And as a business function, it is the data stewards job to represent data owners. For this reason, data stewards sometimes act as data custodians. These are all good things.

In this role, data stewards define policies for data access, usage, provenance, retention, and archiving for their relevant business areas. To be clear, in some cases, this may be in conjunction with data governance personnel. Regardless of how policies are created, with appropriate data literacy

education, data stewards know the data and its associated risks.

Policies represent an important business function. They describe the organization's approach to managing data security and the conditions under which team members should or shouldn't be granted access to data. This includes approval and security requirements. A key part of this involves defining user-access rules and data-source-level security and access controls. Unfortunately, the granting of data access has remained a complicated function shared between identified representatives of data owners and IT security. This process actually slows self-service business intelligence (BI) in most organizations.

Even with all the above capabilities, data stewards or data custodians do not have the technical expertise to manage access to data within the data sources they are responsible for. Providing access to data—or turning the switch as one expert puts it—requires an in-depth understanding of each data system an organization possesses. So, how does it typically work today?



Business users create service management or Jira tickets when they want access to data. Because the ticketing system is not content aware, the receiver of the ticket needs to then manually find and route the ticket to the appropriate representative of the data owner. With their approval, an IT person or persons with the right skills for each data system access is requested to add the user to the access list. This all takes time that digital businesses do not have. This process is also very complex, with too many chances for requests to fall through the cracks.

This approach is also costly due to the volume of data-request tickets that need to be managed by the business and IT. And once there is business approval, access is manually provisioned on a system-by-system basis with all data systems being different. To be clear, it is highly inefficient to manage access to data on an account by account, workspace by workspace, or instance-by-instance basis often involving different IT experts. And this problem is compounding as data and datasets expand at a geometric rate.

The above process means data access takes too long to grant. Eliminating time-consuming data access management is a top requirement for large enterprises today. Organizations report data-access processes taking weeks and even months due to manual processes—time they simply can't afford. Isn't there a better approach? Without question, data stewards are the best people to ensure data access is authorized, fair, legitimate, cost-effective, and timely.

Changing the Paradigm

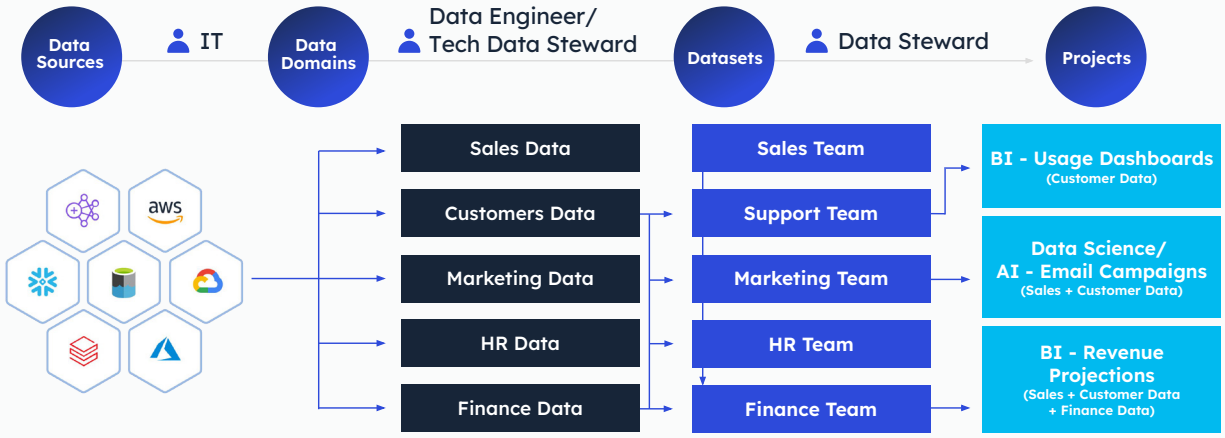
So what is the better way forward? A more effective model for data access, usage, and governance starts with organizations discovering the sensitive data across their organization and then protecting that data against unauthorized release. When this is accomplished, organizations can establish a better approach to data access, especially where organizations have created data marketplaces and want those marketplaces to operate efficiently, effectively, and safely.

Harvard Business School Professors Marco Iansiti and Karim Lakhani say, “a well designed data platform improves the organization’s ability to focus on crucial challenges of data governance and security...defining appropriate checks and balances on access and usage, inventorying the assets carefully and providing all stakeholders with necessary protection.” Put another way, organizations must securely accelerate data access for those with a legitimate business need.

How Does “Better” Work

A better process starts with data engineers, emerging technical data stewards, or data custodians. Technical data stewards or data custodians are a technical role. They ensure the protection, safe transport, and appropriate storage of business data, connecting data sources to business-defined data domains. Where there is a predefined data marketplace, ideally, this can be acquired and display the marketplace’s domains and datasets, which then governs access from this point forward.

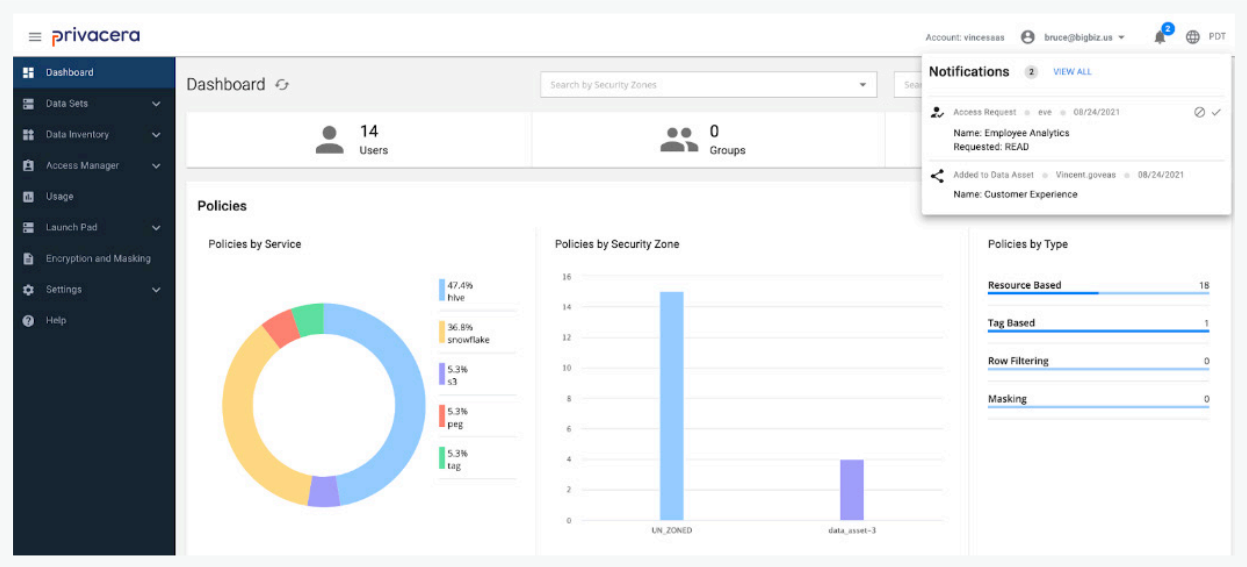
In the better approach, data stewards act on behalf of data owners and manage the last mile of data stewardship by provisioning data access to business users. This moves data control to the place it should have always been in the business. In doing this function, business stewards provision virtual datasets to users. Instead of creating a service management ticket and waiting for data custodians and IT to respond, data consumers can go to data stewards who can quickly, and in many cases, automatically provision data for sanctioned uses.



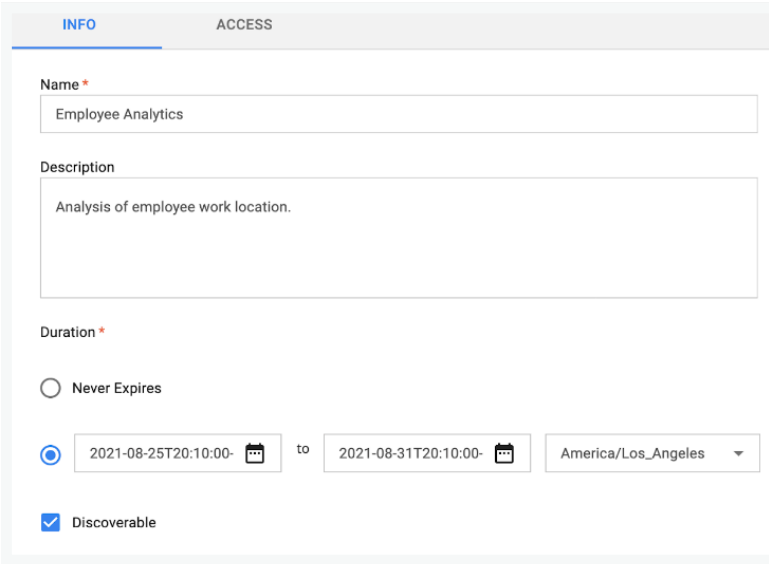
This can include providing time-bound or project-based access to data, ensuring data is used for the right purpose. Additionally, with experience, data stewards can learn from how data is accessed and add business-domain-based rules for data access and security.

Managing Within Privacera

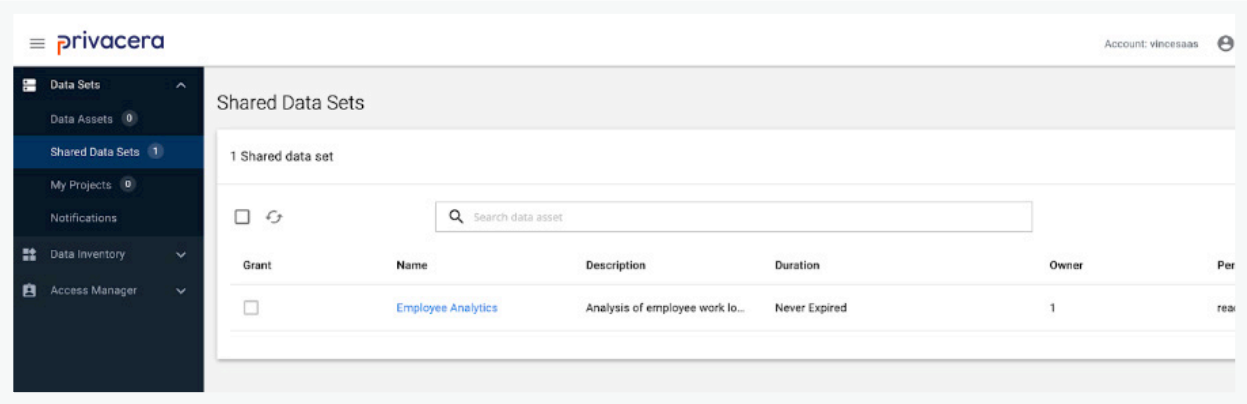
Let's run through how this process works in Privacera, including top benefits. As we said, a data engineer connects data sources to a business data domain, which is aligned to how the business uses and understands data. The data engineer then assigns that business data domain to a relevant data steward. Once this is done, the steward then receives notification the business domain has been linked to data, and they have been granted access to manage this data on behalf of the business.



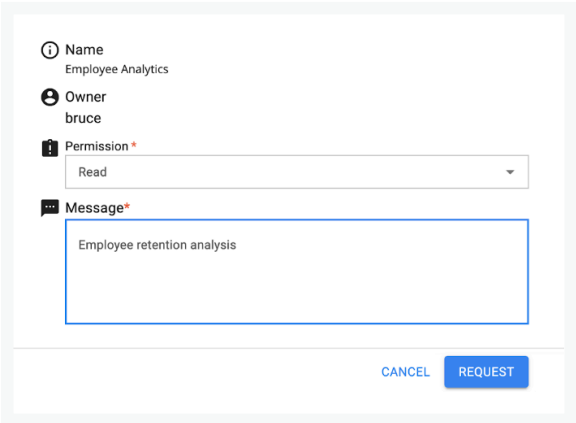
Once business data domain access is provided, the data steward or technical data steward creates a set of virtual business datasets from the data domain they have been provided access to. The ability for data stewards to create virtual datasets and then manage access requests is transformative for business users. It means they can directly look for and discover datasets and then request access without the complexities of a service management ticketing system. In this process, they discover data and relevant data custodians. With this, they can then ask for permission. They no longer need to wait for an IT technician to provision the data.



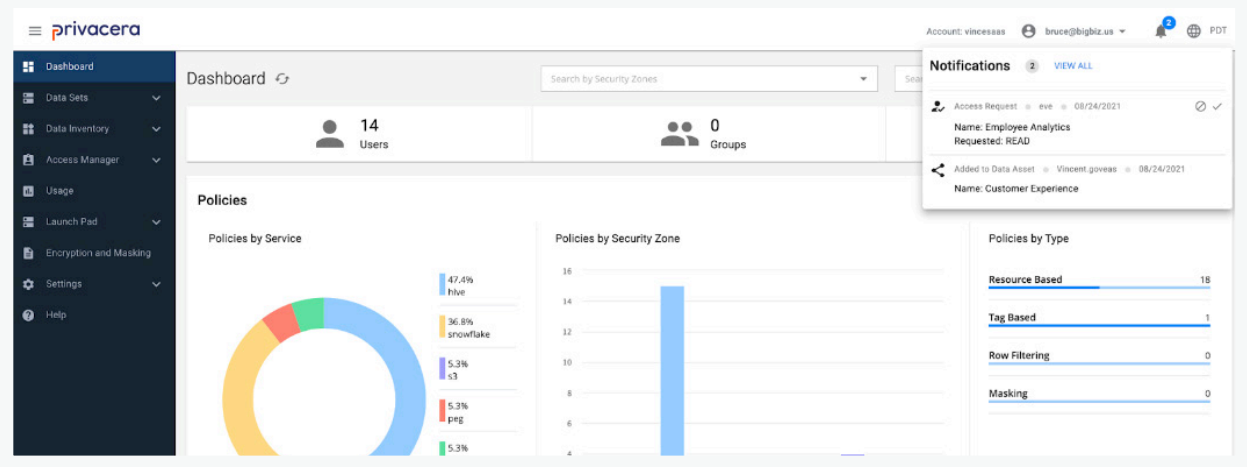
Here, the business user discovers datasets established by the data steward and determines whether they relate to a project they are working on.



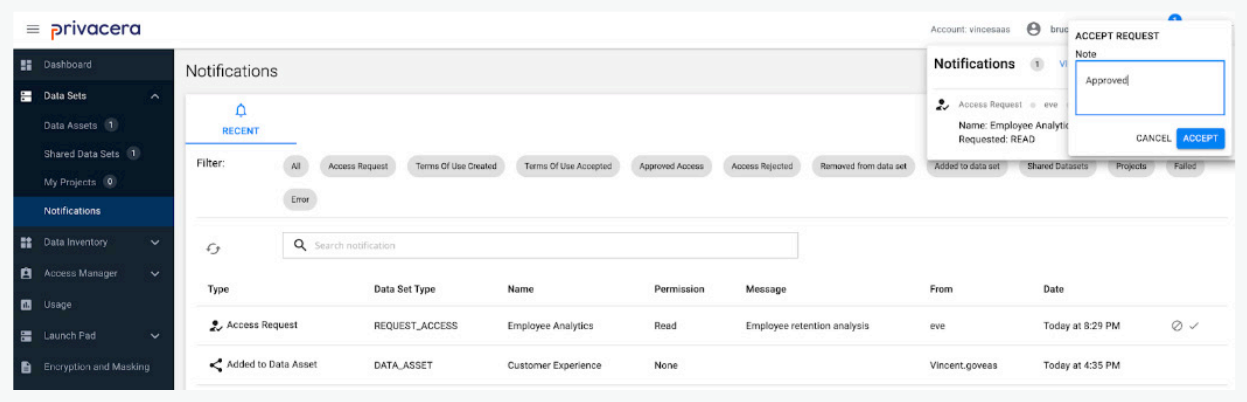
At this point, the business user can request access to the data from the data steward instead of creating a service management ticket and waiting. This eliminates the complexity, time-consumption, and cost of managing data access.



Once the data consumer has put a request into the system, the data steward is alerted that access to one of the datasets they created has been requested.



At this point, the data steward can approve or deny the business user's request, request more information from the user, or provide information to the requesting user on the sensitivity of the data that the business user is requesting. This can include informing the user about appropriate use as well as compliance, security, and privacy guardrails for a dataset. This ensures data is used for the right purpose.

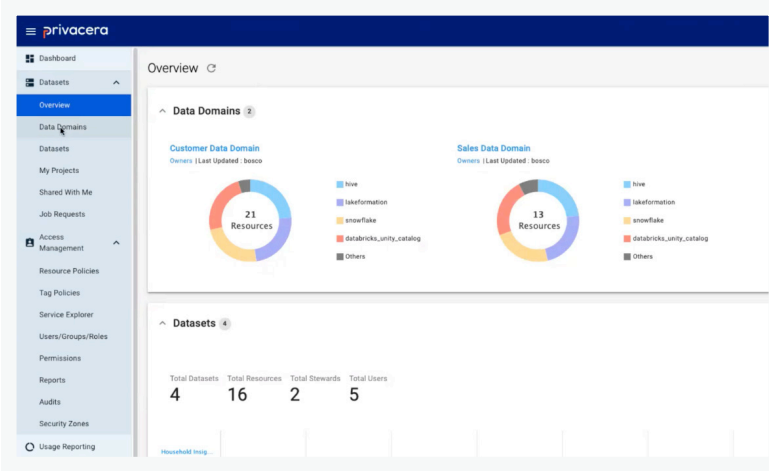


With an appropriate reason for access, the data steward approves access and the dataset appears in the business user's list of approved datasets. To be clear, depending upon the application for data, certain fields that are highly sensitive but not needed may be masked or otherwise obscured.

There is no additional work to do. No longer does IT need to find the relevant data steward and then go through a manual data provisioning process. The approval process immediately provides access to the data the data consumer needs and IT and data stewards get a business view of all the data they are responsible for.

As we described, a much simpler process is created where data consumers request access to data with the request going to the data owner or data steward. Upon approval, Privacera automatically provides access. Data access can be created for a specific purpose and for a specific time to further ensure proper use of data.

The solution can also be integrated with data catalogs, such as Collibra or Alation, and integrated into their workflow, significantly streamlining the



data access process. So, if access is granted, using Collibra Data Marketplace for example, Privacera can automatically create the access control and provision access to the data consumer. This results in a more powerful and relevant data governance process, with the ability to address the entire data estate.

Here, there is no need to create a service management or Jira ticket and burden IT with the time and effort required to manually create access controls, which could easily span multiple data systems and physical or business data domains. Streamlined data access, complete with robust data security and compliance, must be a cornerstone for all data-driven organizations.

But for organizations that need more complex workflows with Privacera's API, it is possible to use the power of service management ticketing system workflows with Governed Data Stewardship. Here is how this would work. The user discovers data within Privacera. When they request access to data, an API is invoked that shares with the service management system the data being requested and the relevant data steward. This way, the ticket can be automatically routed to the appropriate data steward(s) with any additional predefined approvals. When the final approval is given, the ticketing system then connects with Privacera, and approval is automatically managed as described above.

How Governed Data Stewardship Helped a Global Retailer

This Fortune 100 retail customer had a complex environment. It needed a better way to manage data. The retailer had more than 40 workspaces and over 60,000 tables. There were over 20 data analytics teams all attempting to use the data. This customer wanted to:

- Reduce complexity
- Mitigate cost
- Increase data security
- Reduce data risk (PII/PHI exposure)

With Privacera's Governed Data Stewardship, the customer organized data for the business. They created approximately 60 business data domains and datasets. With this, data consumers were able to shop and request access to data domains and datasets. And best of all, one data steward managed requests from this point forward.

> With Privacera's Governed Data Stewardship we accelerated the time for data scientists and analysts to access data to under an hour.
>
> HIGH TECH COMPANY CDO

Business Impacts

What are the business impacts Governed Data Stewardship provides? What are the concrete business returns for investing in today's economic environment? Clearly, while cost-saving matters, there needs to be a concrete business impact to invest. Governed Data Stewardship provides four tangible benefits.

1

Eliminates IT Data Bottlenecks

Implementing Governed Data Stewardship means the business gets data faster. This is accomplished by reducing data-provisioning time. At the same time, it eliminates time-consuming work managing data access.

2

Reduces IT Costs

The automation provided with Governed Data Stewardship eliminates the complexity and cost of manually managing data access. This reduces costs through automation, process improvement, reduced operational costs, and reduced compute and storage costs. This also reduces IT workload and eliminates manual IT processes.

3

Empowers Business Agility

The need to industrialize data products and create faster time to insights will only continue to grow. Govern Data Stewardship enables data stewards who know the data and the context to manage access at the speed of business. This reduces time to insights by onboarding data and users faster. At the same time, it makes data more accessible and easier to manage.

This supports the move to self-service BI. It is important to remember that how organizations distribute data enables them to better manage through tough economic times. Given that self-service is about enabling business users to directly discover data they need for their jobs, access acceleration means business users get access to the right data faster, with direct consequences for a company's top and bottom lines.

4

Improves Security Posture

Governed Data Stewardship ensures data is used for the right purpose. At the same time, it eliminates data proliferation and centralizes auditing. This moves the management of data to data stewards who understand the data risks for their function and business area. This act simultaneously provides greater data access and security.

In closing, leading enterprises intimately understand the need to eliminate the complexity and IT cost of managing data access and security. Businesses who can get the data they need faster, while maintaining security and compliance, hold the superior competitive advantage. Explore more on Privacera's Governed Data Stewardship.

Fortune 500 enterprises trust Privacera for their universal data security, access control, and governance. Discover how to streamline data security governance with Privacera.

Take a unified approach to data access, privacy, and security with Privacera.

REQUEST A DEMO CONTACT US

Privacera, based in Fremont, CA, was founded in 2016 by the creators of Apache Ranger™ and Apache Atlas. Built on the principle of delivering trusted and timely access to data consumers, the company provides data privacy, security, and governance on its SaaS-based data and AI security governance platform. It serves numerous Fortune 500 clients in the finance, insurance, life sciences, retail, media, consumer industries, and government agencies and entities. Privacera has been recognized as a leader in the 2023 GigaOM Radar for Data Governance and has achieved AWS Data and Analytics Competency Status. The company was also named a 2022 CISO Choice Awards Finalist and received the 2022 Digital Innovator Award. Recently, it was named a "Sample Vendor" for data security platforms in the Gartner Hype Cycle for Data Security, 2023. Learn more about Privacera at privacera.com.

privacera