privacera

E-BOOK

AZURE

Mastering Data Access

Why DIY Cloud Governance Falls Short

contents

Introduction 3

Part 1: Native Access Controls: Implications within a Single Cloud 4

Challenges for Azure-Only Environments 4

Azure Challenge & Solution #1 5

Azure Challenge & Solution #2 9

Azure Challenge & Solution #3 13

Azure Challenge & Solution #4 17

Azure Challenge & Solution #5 21

Part 2: Disadvantages of Database or Cloud Specific DIY Controls 26

Part 3: How Privacera Can Help 29

Unified Data Security Platform Advantage 30

Conclusion 31

INTRODUCTION

It's time for CIOs and CISOs to confront the data security and governance complexities of their cloud environments.

Organizations traditionally managed singular, relatively straightforward systems. Today, with hybrid and multi-cloud infrastructures, they face a tangled web of diverse storage, compute, and consumption technologies. The challenge of securing and governing data across this landscape is immense.

Unfortunately, organizations have resorted to solving the security and governance complexity leveraging the native options provided by AWS, who often claim to solve data governance problems pertaining to not only the single cloud, but also hybrid, multi-cloud environments. However, organizations quickly realize that this Do-It-Yourself (DIY) solution creates new data security and access management challenges within the single cloud. Then for the hybrid, multi-cloud environment, DIY solutions only work within the specific cloud vendor ecosystem, and they have the burden of integrating different data sources and managing security and governance across their diverse environment. As organizations dig deeper, the stark reality emerges: governing data across hybrid, multi-cloud is far more complicated. Furthermore, these solutions are not as scalable and flexible as one would expect.

Most organizations who had resorted to DIY solutions with a single cloud vendor discovered that their governance and compliance needs are unmet. For this reason, CIOs and CISOs must take action to streamline the security and governance challenges posed by any (single, hybrid and/ or multi) cloud environment and bolster protection before it's too late. They need a unified data security platform.

PART 1

Challenges for Azure-Only Environments

Azure Synapse Analytics is a comprehensive data integration platform that brings together big data and data warehousing capabilities. It allows organizations to query data on their terms using serverless or provisioned resources and integrates seamlessly with other Azure services for a unified analytics solution.

Azure Blob Storage is Microsoft's object storage solution optimized for unstructured data such as text or binary data. It provides scalable, cost-effective storage with high availability and supports secure data access through granular permissions, making it ideal for various enterprise workloads.

CHALLENGE #1

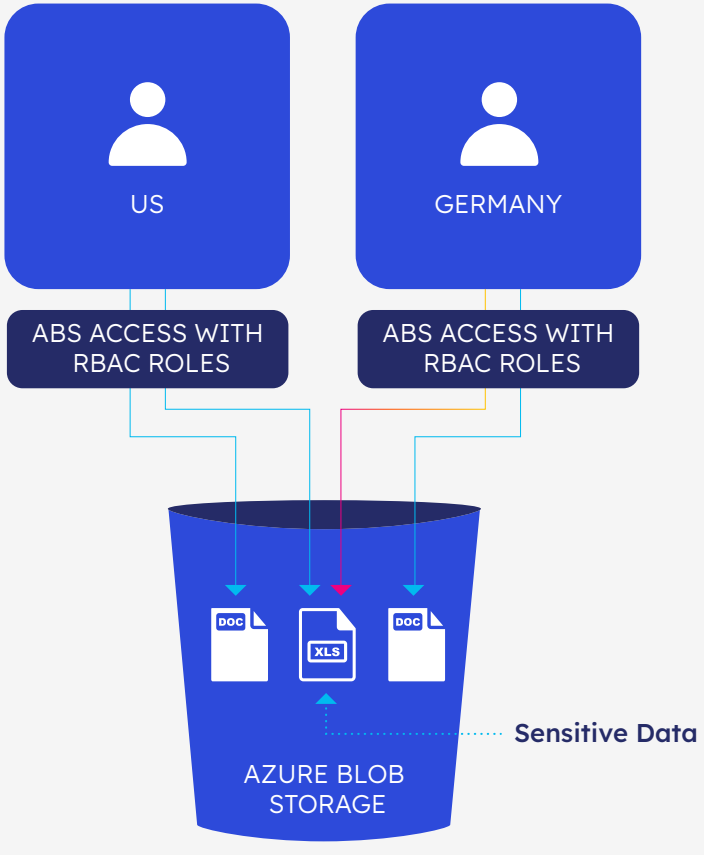
Over-Permissioning with RBAC-based access imposes a security risk

Azure Blob Storage uses RBAC roles and access keys for managing permissions, often applied at the bucket level. Granting a user access to a bucket inadvertently provides visibility into all blobs within it. This over-permissioning can lead to data exposure, particularly when sensitive and non-sensitive data coexist within the same storage bucket.

UNWANTED SCENARIO EXAMPLE #1:

Over-Permissioning in Azure Blob Storage: A Pharma Company's Data Governance Dilemma

A pharma company managing PBs of data, which included sensitive social security records, faced critical governance issues with Azure Blob Storage. Permissions were managed at the bucket level using RBAC roles and access keys. However, this granted all users access to all blobs within a bucket - resulting in over-premissioning. Employees, who were not supposed to have access to sensitive records, also had access to it. The data exposure increased the risk of compliance violations, highlighting the urgent need for a more secure and scalable governance solution.



Per Compliance mandate, the German team shouldn't have visibility into US data. The German team HAS visibility into sensitive US data

- ✕ GOVERNANCE
- ✕ COMPLIANCE
- ✕ GDPR, CCPA

SOLUTION #1

Privacera centralizes access to Azure Blob Storage with ABAC and object-level controls to provide fine-grained access

With Privacera, you can centralize access management for Azure Blob Storage. This helps you eliminate the need for thousands of RBAC roles. You can classify or tag data at blob, folder or object level and policies can be created to provide access based on those classification. After which, attribute-based access control (ABAC) model can allow you to dynamically set permissions based on user attribute, data attribute, group affiliations, and roles - giving you fine-grained access control. This fine-grained access control ensures only authorized users can access specific objects, reducing over-permissioning risks.

IDEAL SCENARIO EXAMPLE #1:

Enhancing Data Security in Pharma Company with Privacera's Fine-Grained Access Control

Privacera empowered the pharmacy company to maintain robust data security by implementing fine-grained access control through an attribute-based access control (ABAC) model. With Privacera, the data steward tagged the US data as "US only" and Germany data as "Germany only", and created a policy to provide access to people within the locations. Then through attribute-based access control (ABAC) model, Privacera controls access based on users location and, hence, the sensitive data is only visible to the US team and not the German team. Furthermore, Privacera also enabled the marketing team to share some datasets that have sensitive data with the finance team by masking (e.g. xxx-xx-xxxx) it. Now, they are able to ensure that access is restricted to specific blobs rather than entire buckets. By eliminating over-permissioning, they also simplified access management and ensured compliance with stringent government regulations.

Sensitive Data is Masked; e.g SS # is shown as xxx-xx-xxxx and xxx-xx-1234

Data has been tagged by the region: US team Only and Germany only.

The German team DOESNT have visibility in US data and vice versa

- GOVERNANCE
- COMPLIANCE
- GDPR, CCPA

CHALLENGE #2

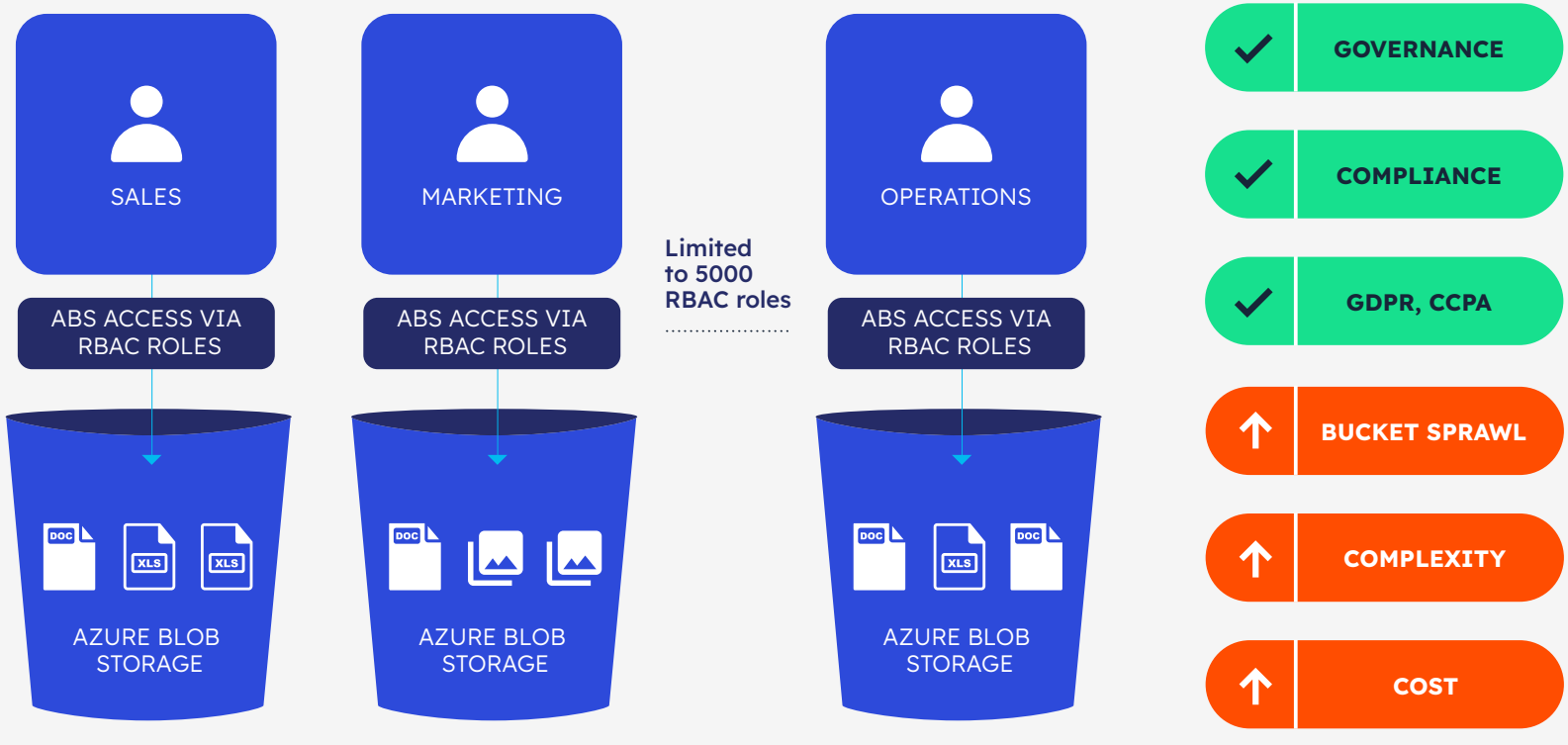
Creating separate buckets for sensitive data results in role sprawl and complexity

To separate sensitive data, organizations often create additional buckets and apply unique RBAC policies to each one. This approach results in bucket sprawl, which makes management more cumbersome and highly prone to errors. Over time, the growing number of buckets becomes harder to track and control. These manual steps add complexity and increase the risk of mistakes. In addition, there is a hard limit to number characters (2000) you can have in a policy and number of RBAC roles (5000) in a domain.This practice also leads to higher operational inefficiencies, slowing down workflows and consuming more resources.

UNWANTED SCENARIO EXAMPLE #2:

The Hidden Costs of Bucket Sprawl: A Technology Company's Struggle with Data Governance

A technology company, Lubar, responsible for public health data faced significant challenges managing sensitive information within its Azure Blob Storage environment. To ensure data security, the IT team created separate buckets for sensitive and non-sensitive data - while applying unique RBAC policies to each. However, this led to severe bucket sprawl. The IT team started facing the difficulty of managing permissions and monitoring access consistently. These inefficiencies not only slowed down operations but also increased the likelihood of errors, exposing the agency to compliance risks and potential data breaches.



SOLUTION #2

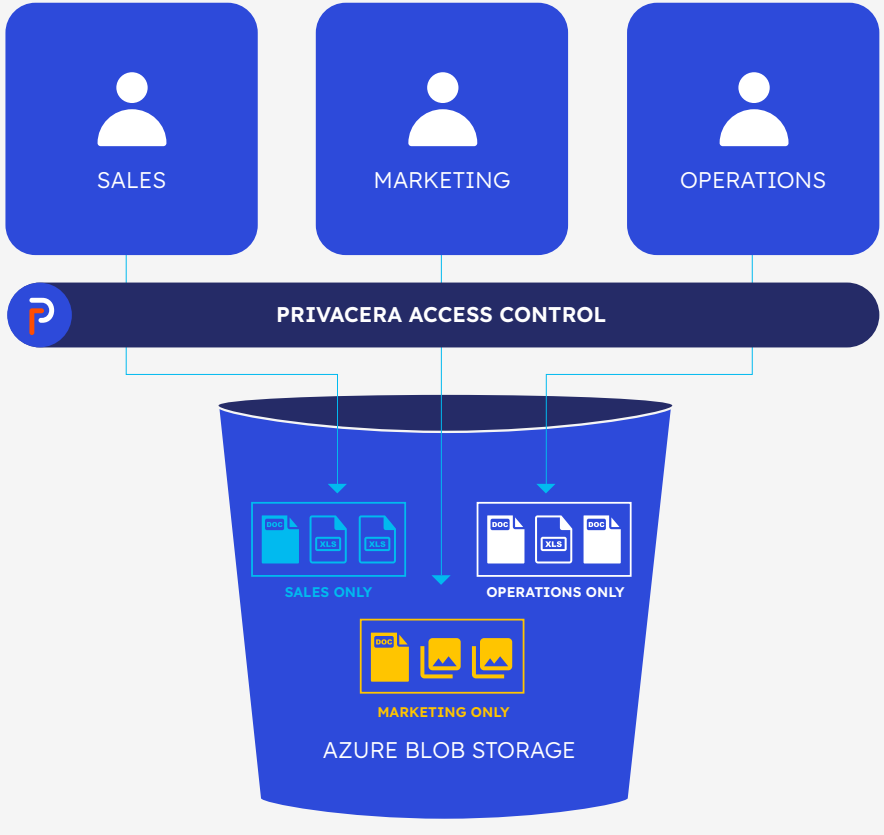
Privacera eliminates bucket sprawl with object-level access control and automated permissions

Privacera automates access provisioning. It allows organizations to dynamically enforce policies across new buckets and blobs with precision. All done through built-in automation, which also reduces bucket sprawl and eliminates much of the manual overhead. This is because Privacera provides you a platform where you can get centralized dynamically controlled access at object-level. Instead of creating new RBAC roles and buckets for each use case. Data stewards can classify or tag data at bucket, folder or object level and policies can be created to provide access based on those classification. After which, attribute-based access control (ABAC) model can allow you to dynamically set permissions based on user attribute, data attribute, group affiliations, and roles. Privacera then helps you manage permissions through its automated access model - streamlining access control and governance to specific groups or users. This approach helps you to significantly reduce bucket and role sprawl.

IDEAL SCENARIO EXAMPLE #2:

Streamlining Data Governance: How Privacera Transformed Access Management for a Lubar

Lubar leveraged Privacera to automate access provisioning. Right away this helped them eliminate the need for creating multiple buckets for sensitive and non-sensitive data. Privacera helped them manage data access by individuals (user attribute). Data stewards tagged the Sales data as “Sales only” data, Marketing data as “Marketing only” data, and Credit card data as “Operations only” data, and created a policy that users within respective departments can only access data assigned to them. Then through attribute-based access control (ABAC) model, Privacera controls access based on the user’s attributes.



- GOVERNANCE
- COMPLIANCE
- GDPR, CCPA
- SIMPLICITY
- LESS ERROR PRONE
- COST EFFICIENCY

CHALLENGE #3

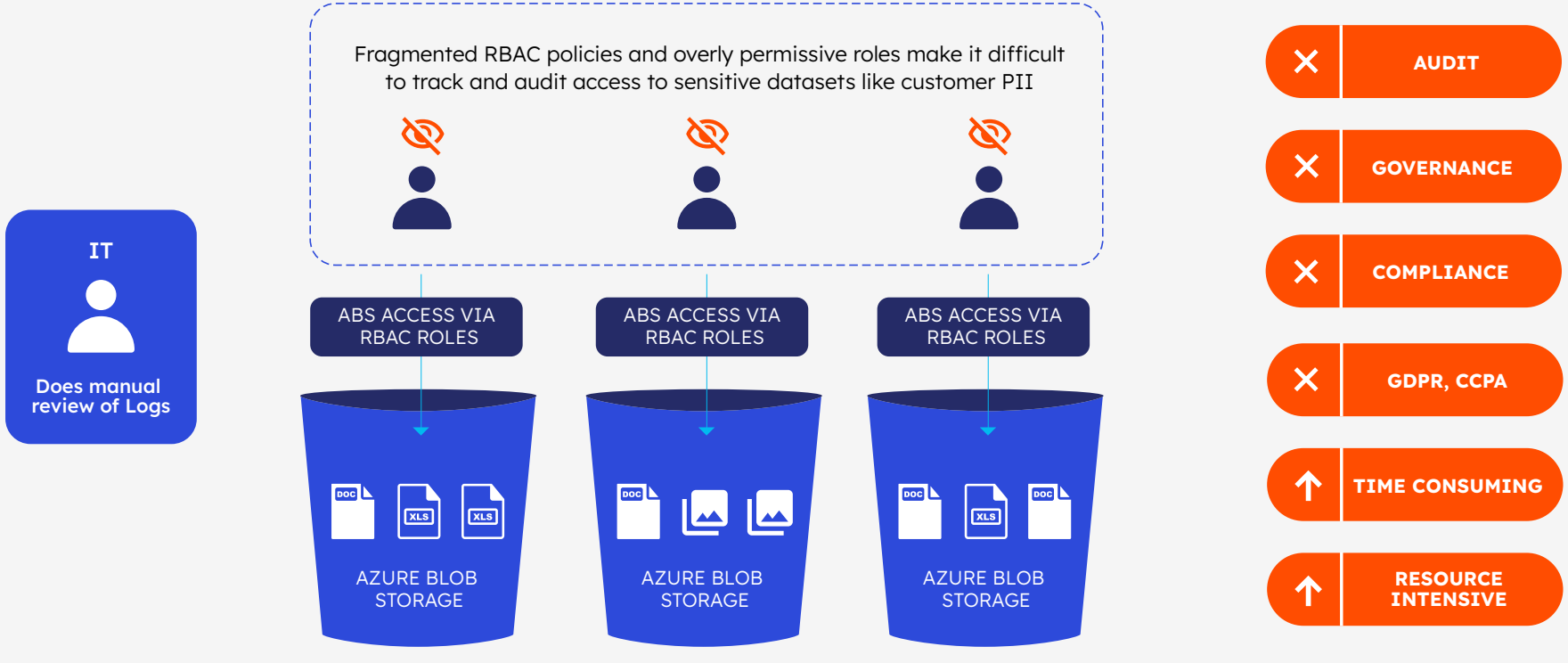
Lack of visibility and auditability of access and permissions

The decentralized governance of access control in Azure Blob Storage often creates operational blind spots to the IT administrators. Due to over-permissioning the compliance team has limited visibility into users' access. This lack of clarity poses serious challenges during audits and policy enforcement. Without centralized control, organizations struggle to maintain consistent oversight. They face growing compliance risks and inefficiencies in managing access. These issues slow down processes and increase administrative burdens. The result is a fragmented system that hampers security and productivity.

UNWANTED SCENARIO EXAMPLE #3:

A Global Retail Tackles Azure Blob Storage Access Control Challenges to Strengthen Compliance and Efficiency

A global retail chain, Tarmark, encountered significant challenges with decentralized governance in Azure Blob Storage. As their e-commerce platform expanded, over-permissioning became a persistent issue, granting unnecessary access to sensitive sales data and customer records. This lack of centralized visibility made it difficult to track who accessed what data, creating blind spots during audits. Policy enforcement became a manual, time-consuming process, increasing the risk of non-compliance with data protection regulations like GDPR and CCPA. These inefficiencies left Tarmark vulnerable to potential breaches and operational disruptions, exposing the urgent need for a streamlined access control solution.



SOLUTION #3

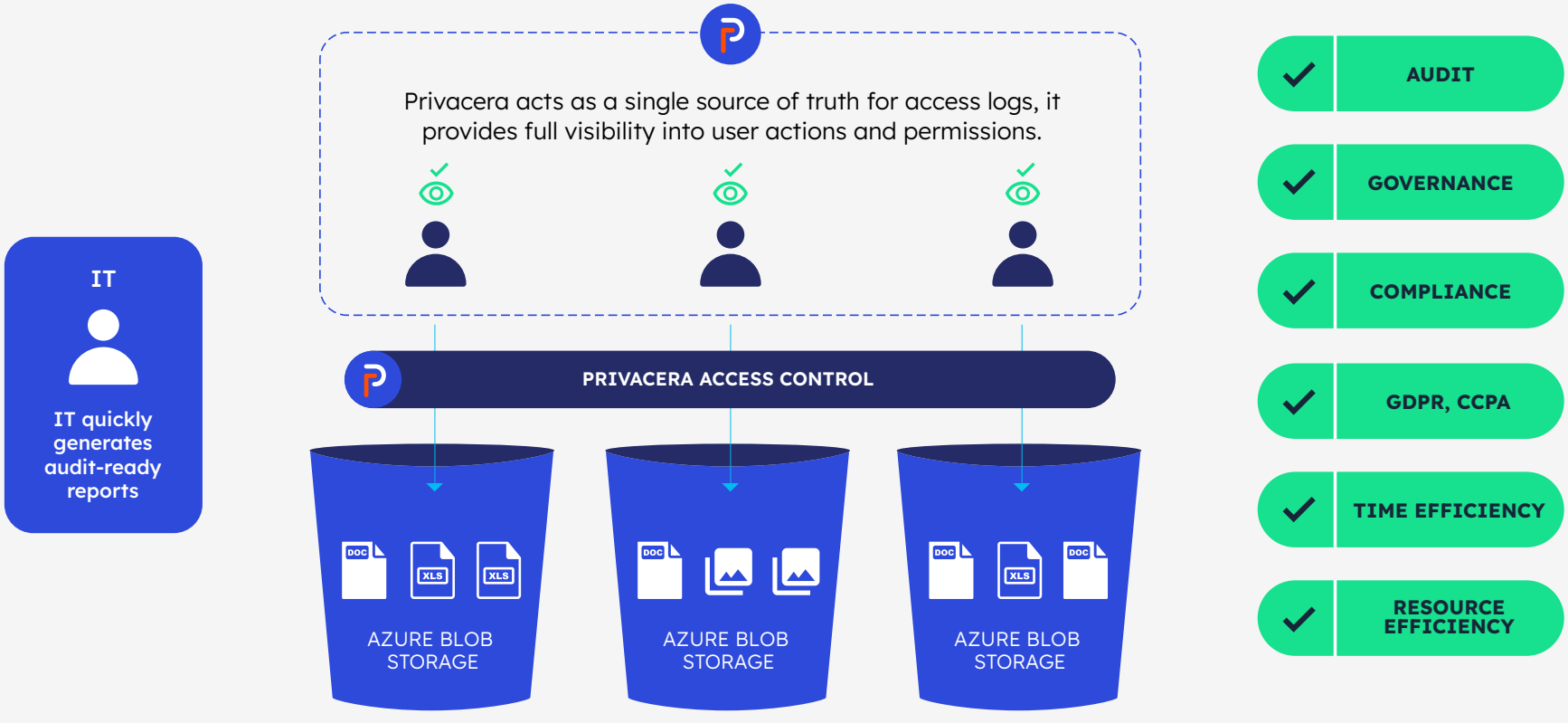
Privacera provides comprehensive visibility of access and governance

Privacera provides a centralized platform for unified access management across Azure Blob Storage. Its audit and reporting capabilities offer comprehensive visibility into user permissions and access history. This centralized governance simplifies compliance by standardizing access controls, ensuring consistent policy enforcement, and demonstrating robust data privacy measures during audits.

IDEAL SCENARIO EXAMPLE #3:

How Tarmark Strengthened Data Governance and Compliance with Privacera

Tarmark transformed its data governance and compliance processes by implementing Privacera to address challenges with decentralized access control in Azure Blob Storage. Privacera's centralized platform unified access management helped the IT team to deliver a comprehensive audit and reporting with detailed information into user permissions and their access history. By standardizing access controls and ensuring consistent policy enforcement, Privacera simplified compliance, reduced risks, and streamlined operations.



CHALLENGE #4

Inefficiencies in Manual Access Control for Adding New Datasets

Granular access control often necessitates manual interventions, especially when additional datasets are introduced and the right access needs to be granted. These processes are time-intensive and prone to human error. They added complexity and increased operational risks for organizations. Manual methods to add specific policies also slow down workflows and create inefficiencies. Without automation, the risk of misconfigurations rises significantly. This can lead to security breaches and compliance failures. Streamlined solutions are essential to reduce these challenges. Organizations need better tools to ensure accuracy and efficiency.

UNWANTED SCENARIO EXAMPLE #4:

Scaling Challenges: Managing Sensitive Data with New Datasets at AutoParts Inc

A manufacturing company, AutoParts Inc., faced challenges with managing sensitive parts and inventory data. As they added more datasets, they manually applied different RBAC policies. This process was not only slow, but also became more difficult to manage with the increase in the number of policies. This often led to misconfigurations and exposed them to security breaches and compliance issues. The manual approach slowed workflows and made it hard for them to scale securely.

1. Data Owners submits a ticket to assign policy for the new dataset – incl. information of sensitive data (PII, Email) in the dataset
2. IT administrator takes the request and submits it to the compliance officer
3. Compliance officer understands the class of people who can access the data
4. Creates a new policy
5. Sends the update to the Data Steward
6. Data Steward enforces policies and manages (data integrity, governance, monitor) the data
7. Admins, finally, uploads the data and grants assess to data (facilitator)

✕ TIME CONSUMING ✕ ERROR PRONE ✕ LABOR INTENSIVE

SOLUTION #4

Privacera automates data access, governance, and compliance at scale

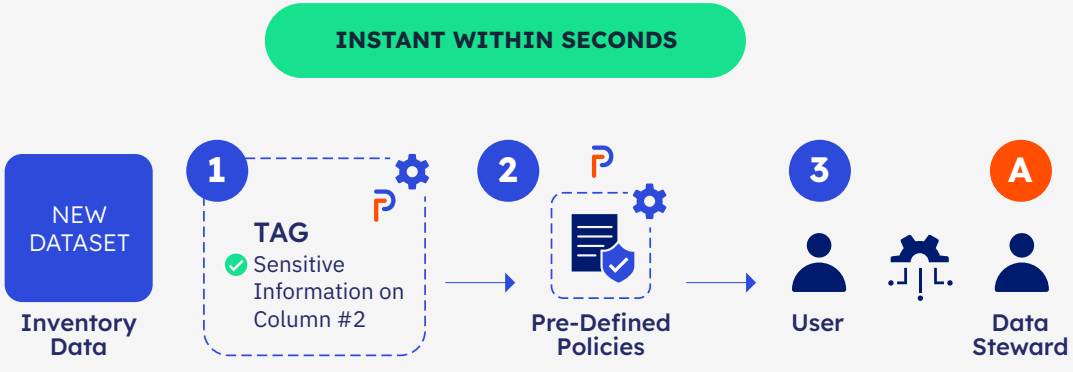
Privacera centralizes access control and policy creation based on tag and resource, offering streamlined and efficient data organization. Through Privacera, administrators can add new datasets without the burden of understanding and creating new policies. All they (data users) have to do is to tag or classify the data with its attributes based on location, department, group, project, and sensitivity information. Once the data is tagged correctly, Privacera's Attribute-Based Access Control (ABAC) leverages existing pre-defined policies to apply permissions to the right set of users based on their attributes and access rights. This ensures "birth right access" to the new data as soon as it is created and tagged appropriately, without the need to update policies for new data or resource information. This reduces the complexity and makes management more straightforward. The ABAC model ensures consistent governance and simplifies scalability as data grows. It enables organizations to handle large datasets efficiently while maintaining strong security and compliance controls.

IDEAL SCENARIO EXAMPLE #4:

How a Leading Saas Company Simplified Data Management and Security with Privacera and ABAC

Management and Security with Privacera and ABAC

AutoParts Inc. implemented Privacera to centralize access control for Azure Blob Storage. As new datasets were introduced, data owners tagged it based on location, department and sensitivity information. Once the data is tagged correctly, Privacera's Attribute-Based Access Control (ABAC) leverages existing pre-defined policies to apply permissions to the right set of users based on their attributes and access rights - giving users "birth right access" to the new data right away. Hence, the need for manual intervention or unnecessary policy creation is eliminated, this reduces the complexity of managing security across buckets, and improves scalability. As a result, AutoParts Inc. could efficiently manage its growing datasets while maintaining robust security and compliance.



1. Privacera detects a new dataset, identifies sensitive information based on data and metadata (e.g schema, format), assigns tag and makes data available to system
2. Privacera leverages pre-defined polices to apply permission: Mask sensitive information for non-HR and non-US members
3. Users are granted "birth right access" to the dataset
A. Data Steward manages (data integrity, governance, monitor) the data

✓ TIMELY ✓ LESS ERROR PRONE ✓ EFFICIENT

CHALLENGE #5

Manual access control hampers scalability and efficiency

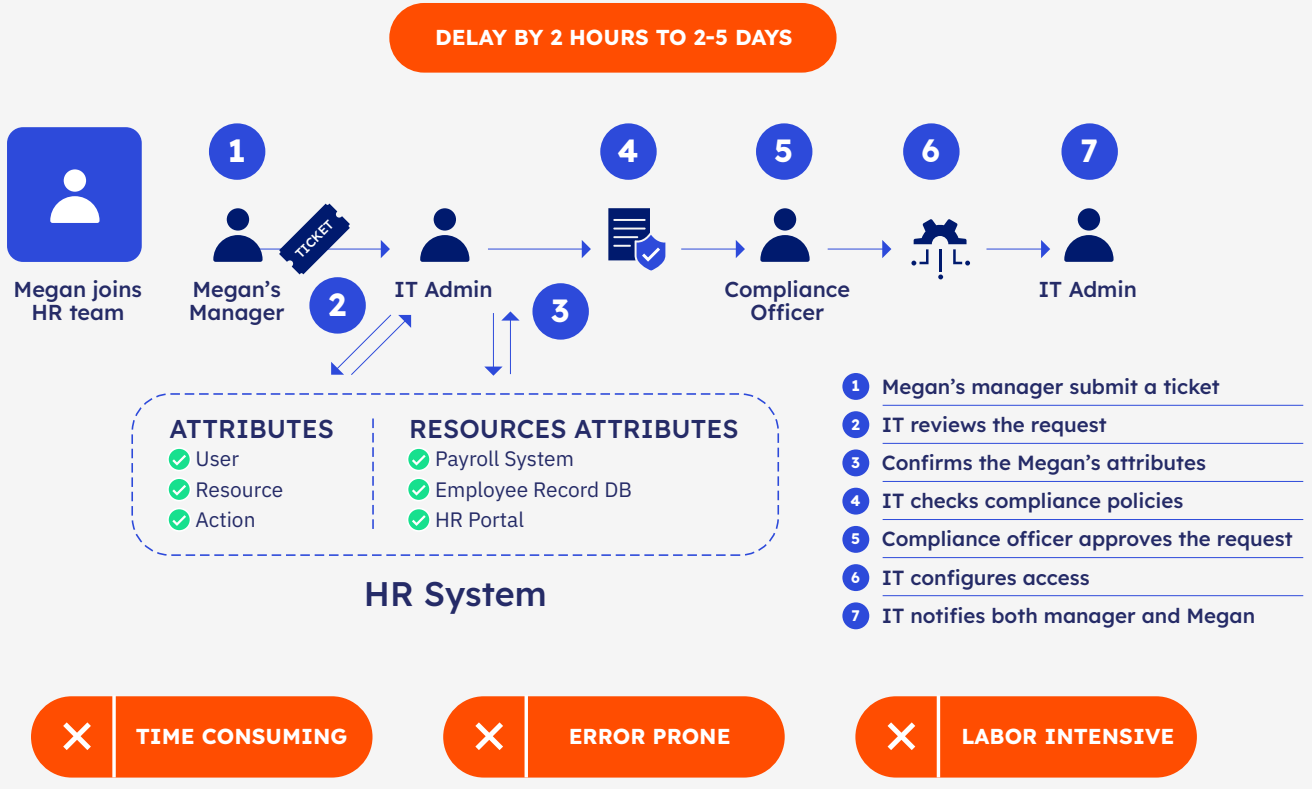
Organizations managing large-scale data environments face significant challenges with manual processes for access control and governance. The reliance on ticketing systems for access requests in platforms like Azure Blob Storage creates bottlenecks, delays, and a heavy administrative burden. Each new request requires manual review and approval, leading to slower data access, reduced productivity, and a higher likelihood of errors. In some cases companies could take 2 hours to 2-5 days.

Additionally, integrating new objects, datasets, and tables into governance frameworks compounds the problem. Every new asset requires manually creating roles, permissions, and policies, which increases operational complexity. This labor-intensive approach results in delays, misconfigurations, and potential security vulnerabilities, making it difficult to scale efficiently while maintaining compliance and security standards.

UNWANTED SCENARIO EXAMPLE #5:

The Hassle of Granting Data Access: A New Employee's Onboarding Challenge

Megan, a new member of the HR team, joins the organization, and her manager submits a ticket via the IT department's ticketing system requesting access to HR-related data and tools. The IT team reviews the request, confirms Megan's role, and seeks additional clarification on specific data and systems she requires access to. The manager responds, detailing that Megan needs access to the payroll system, employee records database, and the HR portal for managing benefits. The IT team checks compliance policies and ensures the requested access aligns with her role. They may reach out to the HR compliance officer for approval if sensitive data is involved. After final approval, the IT team configures access and notifies both the manager and Megan. Megan then tests her access, and if any discrepancies arise, she or her manager may need to follow up for adjustments, closing the ticket once all issues are resolved.



SOLUTION #5

Privacera increases efficiency by automating data access, governance, and compliance

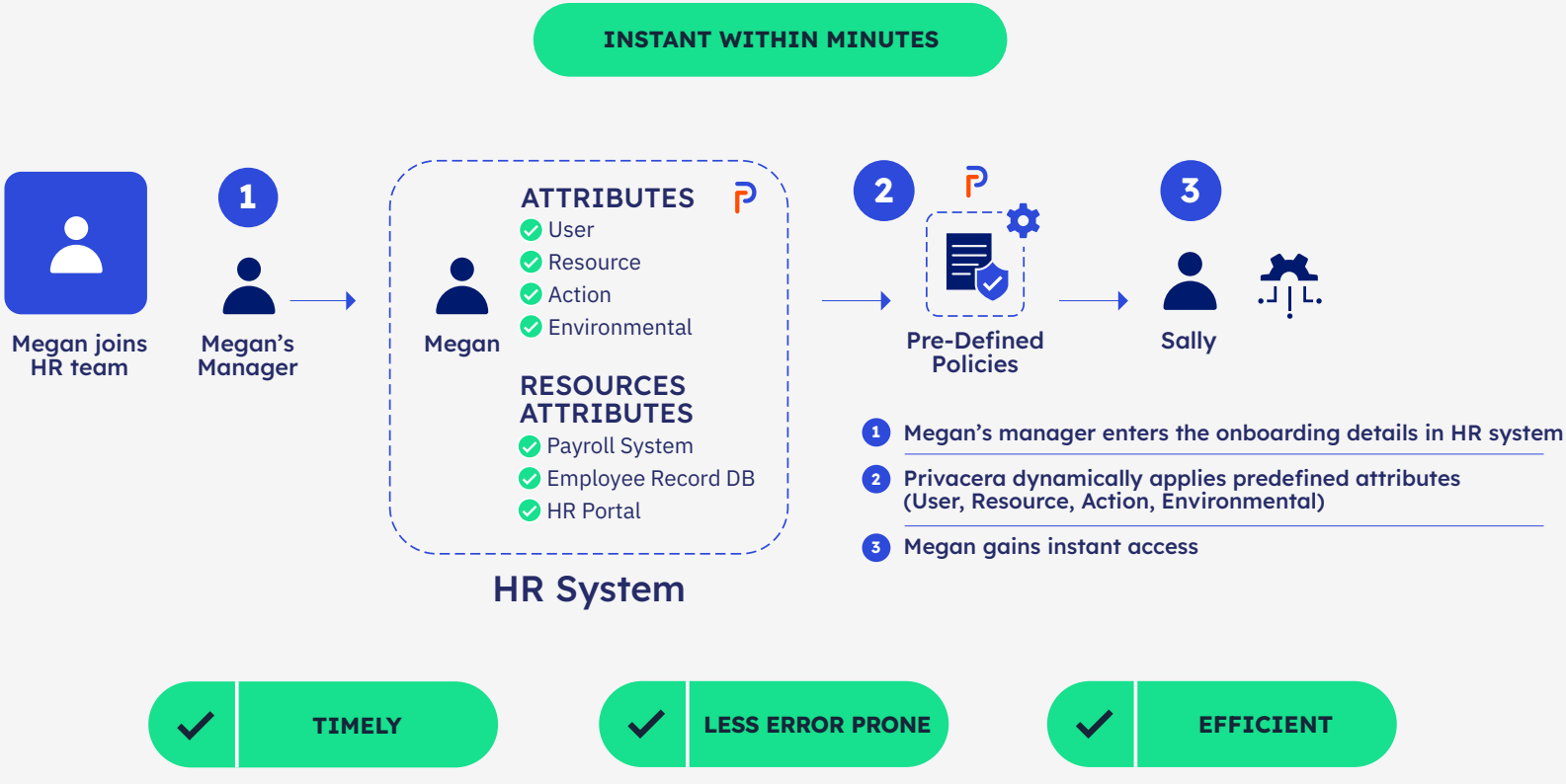
Privacera streamlines access control and governance by automating the management of permissions and policies for datasets in Azure Blob Storage. Its integrated approach eliminates the need for manual ticketing systems and manual policy creation, reducing overhead and accelerating data access. By dynamically assigning permissions based on attributes (User, Object, Action, Environmental), Privacera ensures that access is granted efficiently and securely. Furthermore, new objects, datasets, and tables are automatically governed as soon as they are created, with existing rules applied seamlessly. This automation eliminates delays in onboarding new people or adding new assets, and ensures consistent governance without sacrificing security or compliance.

With Privacera, organizations can manage the exponential growth of data while maintaining operational efficiency. Teams can focus on innovation and strategic tasks rather than administrative work, enabling scalable and secure data environments that adapt effortlessly to evolving business needs.

IDEAL SCENARIO EXAMPLE #5:

Streamlined Onboarding: How Privacera Simplifies Secure Data Access for New Employees

When Megan joins the HR team, the ideal scenario using Privacera streamlines and automates her access to necessary datasets and systems without relying on manual ticketing processes. Once Megan's onboarding details, such as her role, group memberships, and attributes, are entered into the HR system, Privacera dynamically applies predefined access policies aligned with the HR role. These policies grant her secure access to specific datasets in Azure Blob Storage, such as payroll and employee records, while ensuring compliance with governance rules. As Privacera automatically governs new datasets and applies existing rules to them, Megan gains instant, secure access to any new HR datasets created after her onboarding. This approach eliminates delays, reduces administrative overhead, and ensures consistent governance, enabling Megan to start contributing to her team immediately while maintaining robust security and compliance standards.



Azure RBAC	Privacera
Over-permissioning with RBAC roles imposes a security risk	**Centralized ABAC with object-level controls provides fine-grained access control**
Creating separate buckets for sensitive data results in RBAC role sprawl & complexity (limited to 5000 roles)	**Eliminate role sprawl with object-level control and automated permissions**
Lack of visibility and auditability of access and permissions (complex, hard to decipher etc)	**Privacera provides comprehensive visibility of access and governance** (centralize platform w/easy to manage policies)
Manually adding new dataset is time-consuming and error-prone	**Predefined policies instantly gives "birth-right access" to user of the data**
Manually granting access control hampers scalability and efficiency (character limit of 2000 to create policies)	**Automated data access, goverance, and compliance increases efficiency** (classification and tagging, and policy)

PART 2

Disadvantages of Azure Specific DIY Controls

Organizations often adopt an Azure-specific approach to access and security management, assuming it provides tighter control and cost efficiency. Azure itself promotes its native tools as comprehensive solutions for data governance and security. However, as data volumes grow and extend across various Azure services, this strategy quickly shows its limits. Maintaining custom integrations, managing fragmented access controls, and ensuring consistent compliance across siloed systems becomes increasingly complex and resource-intensive. Without a unified approach, businesses face mounting inefficiencies, security risks, and scalability roadblocks that hinder innovation and strain resources.

DIY Security and Governance Challenges in Hybrid and Multi-Cloud Environments

DIY data governance in hybrid or multi-cloud environments presents two problematic options: managing each data silo separately or stitching together fragmented vendor controls. Both are inefficient and create security gaps. Managing data silos individually leads to inconsistent policies, compliance issues, and higher IT costs. Without standardized frameworks, auditing becomes fragmented, increasing risks and inefficiencies. On the other hand, using cloud vendor solutions may seem cost-effective but results in tech debt and integration challenges, slowing down authorized users and stifling business agility. A unified approach is essential to navigate these complexities and improve operational efficiency.

Operational Impact of Making and Managing DIY on Your Own

Managing cloud complexity on your own is daunting. From classifying metadata to syncing policies and building custom integrations, the cost of a DIY approach is not only in time and resources but in long-term sustainability. Many organizations struggle with the complexity of data integrations and scripts. Some organizations have tried using Google Sheets and custom scripts to manage policies, but they quickly realize that it becomes an unsustainable burden. DIY solutions lack transparency, slow operations, and make compliance harder. Employees face delays in data access and onboarding, and identifying data owners becomes time-consuming, further hindering progress.

Limitation of Integrating DIY with Different Cloud Environments

Cloud vendor solutions may seem cost-effective, but lack scalability, flexibility and integration for hybrid and multi-cloud environments. Each of these vendors operate as a walled garden, forcing enterprises to stitch together controls, creating tech debt that drains resources and hinders agility. This disjointed approach complicates legitimate data access, slowing down authorized users with manual processes, ultimately hindering productivity and operational efficiency. Furthermore, organizations depend on legacy governance methods, which end up becoming roadblocks and delay access to critical data.

Cost in-efficiency with DIY

DIY cloud management comes with tangible costs that many organizations underestimate until they are deep into their cloud journey. Managing the complexity of varied data sources, each with different standards, drives up integration challenges and total cost of ownership.

Cloud is not inherently simple, and without a cohesive strategy, the costs - both financial and operational - quickly escalate. The issues faced by our customers with DIY security, particularly in data management and governance, can be summarized as follows:

Scalability Challenges with DIY

As data volumes grow, manual governance processes become impractical for customers. For example, a financial services institution (FSI) faced a scalability wall with their 31 petabytes of data spread across multiple systems (Redshift, Spark, EMR, Flink, etc.) created complexity and management sprawl. Managing large amounts of data across thousands of tables and datasets proved overwhelming in the end, making it hard to govern, control, and secure access.

Access Control Issues in DIY

Coarse-grained access controls lead to overly permissive and difficult-to-manage access. The inability to efficiently track and manage who had access to what data created significant security risks. The complexity of managing sensitive data in highly regulated industries required dynamic access management solutions to better handle user attributes and group memberships.

Operation Inefficiencies with DIY

For many customers, manually processing access requests (via ticketing systems) and manual onboarding into governance frameworks created operational bottlenecks and error-prone processes. Manual encryption for data masking was inefficient at scale, slowing down data access and adding costs.

Data Visibility and Redundancy in DIY

Some customers lacked central visibility into their data lakes, which hindered the ability to track datasets, distinguish environments, and monitor access. Multiple copies of datasets led to increased storage costs and difficulties in identifying production vs. test datasets.

Redundant and untracked datasets exacerbated costs, while reliance on tribal knowledge for periodic cleanups was unsustainable.

Technology Sprawl and Integration Complexities with DIY

The integration of various technologies like Databricks, EMR, Redshift, and others introduced maintenance and administrative burdens. Ensuring seamless data access across these platforms was difficult. Organizations struggled to manage data governance across multi-cloud environments, further complicating compliance and security efforts.

Governance and Compliance Risks with DIY

Relying on federated permission management (with lower-level controls) without centralized oversight made it hard to ensure proper governance and compliance with regulations.

There were risks of non-compliance due to potential delays in processing data access requests and manual governance approaches. In summary, organizations face difficulties with scalability, access control, operational inefficiencies, data visibility, and governance across complex cloud ecosystems, leading to rising costs, security risks, and challenges with regulatory compliance.

PART 3

How Privacera Can Help

Privacera empowers organizations with comprehensive visibility into all sensitive data across various source systems. With its built-in automation and a robust suite of over 50 connectors developed through extensive engineering efforts, Privacera significantly reduces the need for staff such as data platform administrators and data engineers. Each data platform follows different standards for access policies, creating a heavy burden on IT and security teams to maintain consistent organizational policies.

Privacera automatically detects sensitive data across multiple cloud databases and analytics platforms, allowing rules to be written once and applied across all sources. By leveraging pattern recognition and machine learning, Privacera enhances the discovery and tagging of unprotected data and personally identifiable information (PII). This enables data stewards to make informed decisions regarding what data needs protection and who should have access across various systems.

Moreover, Privacera automates the scanning, identification, and tagging of sensitive data both on-premises and in the cloud, covering the entire data estate. It provides a unified view of access policies, reducing inconsistencies, redundancies, and manual errors associated with policy administration. With fine-grained policies in place, organizations can mitigate the risks of data breaches and leaks, resulting in a 50-75% reduction in the resources required for policy administration through automation.

Greater access to data leads to more informed analytics, reduced time to insights, and faster decision-making, empowering organizations to act swiftly in a data-driven world. By streamlining data governance, Privacera ensures that organizations can navigate the complexities of data security with ease and confidence.

Unified Data Security Platform Advantage

A unified data security platform offers significant advantages akin to the efficiencies gained from standardization in enterprise architecture, as highlighted in “Enterprise Architecture as Strategy.” By adopting a centralized approach to data security, organizations can reduce complexity and minimize the number of platforms they operate, leading to lower costs and IT budgets that are 15% leaner.

This unified governance model delivers immense value by significantly lowering the administrative burden associated with managing data security and access control. Organizations can reduce the number of dedicated resources focused solely on policy administration and data access management, allowing teams to redirect their efforts toward more strategic initiatives. This streamlined approach alleviates the workload on policy administrators while accelerating user onboarding and data access, ensuring that critical business information is readily available.

By consolidating data governance policies under one system, organizations enhance transparency, consistency, and auditability, which improves compliance standards and bolsters security postures. The reduction of manual processes and duplicative controls makes it easier to audit and enforce compliance, enabling employees to gain expedited access to data. This facilitates better decision-making while ensuring regulatory requirements are met.

Moreover, enhanced efficiency in managing data governance not only improves internal processes but also elevates employee satisfaction and customer experiences. With quicker provisioning of data access and reduced labor in managing security, organizations become more agile, better equipped to handle growth and ensure data democratization. This unified approach ensures faster access to data, stronger compliance, and reduced operational complexity, resulting in a more agile and secure environment.

Finally, a unified platform future-proofs your data estate. As new data technologies emerge - often without the input of data teams - the ability to seamlessly integrate new data sources into an existing central platform offers substantial benefits. For instance, one manufacturer/retailer we work with was able to reduce the introduction of new data by up to 95%, demonstrating the transformative power of a centralized data security approach.

Conclusion

In today's complex hybrid and multi-cloud landscapes, CIOs and CISOs must confront the intricate challenges of data governance that traditional enterprise data warehouses (EDWs) no longer address. While cloud vendors like AWS, Databricks, and Snowflake promise solutions, their offerings often fail to integrate effectively across different platforms, leaving organizations struggling with fragmented controls and inefficiencies.

The DIY approach to data governance presents a false sense of control, forcing teams to either manage each data silo independently or piece together disjointed vendor tools, both of which lead to increased operational costs and compliance risks. Without a cohesive strategy and centralized governance framework, organizations face spiraling costs and diminished agility, hampering their ability to respond swiftly to data needs. A unified data security platform emerges as the key to overcoming these challenges, streamlining processes, enhancing compliance, and significantly reducing the administrative burden associated with managing diverse data sources. By leveraging Privacera, organizations can automate governance, gain comprehensive visibility into sensitive data, and ensure that data access is both efficient and secure, ultimately transforming their approach to data security in an increasingly complex environment.

AUTHORS:

Balaji Ganeshan, CEO & Co-Founder, Privacera
Balaji Ganesan is CEO and co-founder of Privacera. Before Privacera, Balaji and Privacera co-founder Don Bosco Durai, also founded XA Secure. XA Secure's was acquired by Hortonworks, who contributed the product to the Apache Software Foundation and rebranded as Apache Ranger.

Don Bosco Durai, CTO & Co-Founder, Privacera
Don Bosco Durai (Bosco) is CTO and co-founder of Privacera, an entrepreneur and a thought leader in enterprise security. He is the co-creator of Apache Ranger, which is the de facto centralized authorization tool for most open source big data tools. Prior to founding Privacera, Bosco was also the co-founder of XA Secure, which redefined access security at scale.

Ibrahim "Ibby" Rahmani
Sr. Director of Marketing & Product Marketing
Ibby Rahmani is the marketing lead at Privacera, with a proven track record of launching successful programs at Alation, Hitachi, HP, and VMware. He specializes in AI, data technologies, and go-to-market strategies, translating complex innovations into clear, impactful messaging. Passionate about driving industry awareness, he creates compelling content that highlights emerging trends and real-world applications.

Jason Payne, Head of Solutions Engineering, Privacera
Jason Payne is the Head of Solutions Engineering and Technical Services at Privacera, specializing in data security and governance. He leads technical strategies for data access and privacy and shares insights through Privacera's technical video series.

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. Delivering trusted and timely access to data consumers, Privacera provides data privacy, security, and governance through its SaaS-based unified data security platform. Privacera's latest innovation, Privacera AI Governance (PAIG), is the industry's first AI data security governance solution. Privacera serves Fortune 500 clients across finance, insurance, life sciences, retail, media, consumer, and government entities. The company achieved AWS Data and Analytics Competency Status, and partners with and supports leading data sources, including AWS, Snowflake, Databricks, Azure and Google. Privacera is recognized as a leader in the 2025 GigaOm Radar for Data Access Governance. Learn more at privacera.com.

privacera