privacera

E-BOOK

GCP

Mastering Data Access

Why DIY Cloud Governance Falls Short

contents

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 GCP, 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 Google BigQuery-Only Environments

Google BigQuery

Google BigQuery is a fully managed, serverless, and highly scalable data warehouse designed for fast SQL-based analytics on large datasets. It allows organizations to process petabytes of data using standard SQL, making it ideal for big data analytics, machine learning, and real-time insights. Its pay-as-you-go pricing model and seamless integration with Google Cloud's ecosystem make it a cost-effective choice for businesses looking to democratize data access.

CHALLENGE #1

Manually granting access control hampers scalability and efficiency

As your data environment grows, it becomes significantly difficult for you to maintain consistent access control and governance policies for a large number of datasets, tables, and projects. The process is not only labor-intensive but also prone to errors, especially when done manually. This lack of automation creates significant challenges, such as ensuring compliance with privacy regulations like GDPR, HIPAA, and others. Manually enforcing access control policies and protecting sensitive data leads to inconsistencies and exposes organizations to risks of non-compliance, data breaches, and operational inefficiencies. The challenge extends further when it comes to managing encryption at scale.

UNWANTED SCENARIO EXAMPLE #1:

Retailer Struggles with Security Gaps in Google Cloud Ecosystem

A retail company, Tarmark, faces challenges in ensuring consistent access control and governance across its Google Cloud environment, which includes BigQuery, Cloud SQL, and Cloud Storage. Sensitive customer data, inventory metrics, and marketing assets are distributed across platforms. The IT team is burdened with working manual policy enforcement, which is both error-prone and labor-intensive. As data volumes are growing, the data team realized that this approach has become unscalable and is lagging behind on policy. The result of which is the company is exposed to compliance risks, inefficiencies, and potential security breaches.

SOLUTION #1

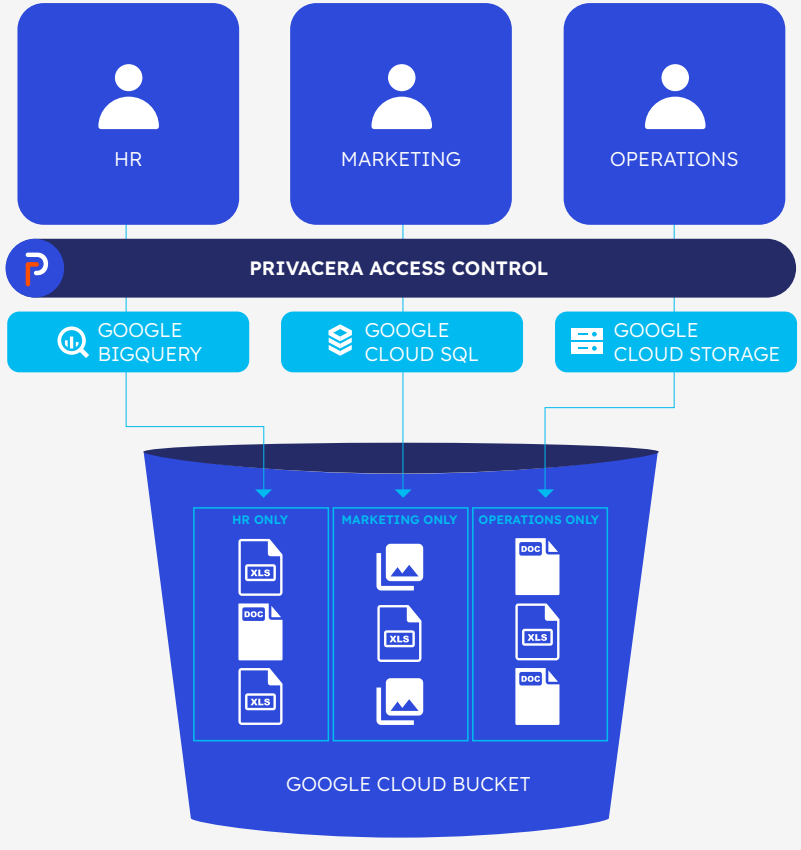
Privacera automates governance, applying access controls across Google projects and BigQuery, reducing risk

Privacera streamlines governance by automating access control across all BigQuery tables and Google projects, eliminating the manual, error-prone processes that often compromise security. 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. With Privacera, organizations can ensure consistent compliance and meet regulations like GDPR, HIPAA, and others. It also mitigates risks associated with data exposure, non-compliance, and security breaches. As an organization you are also able to securely manage sensitive data across teams and projects as they grow.

IDEAL SCENARIO EXAMPLE #1:

Streamlining Data Governance: How Tarmark Achieved Scalable Security and Compliance with Privacera

By adopting Privacera, Tarmark automated governance processes. The data steward tagged the HR data as “HR only” data, Marketing data as “Marketing only” data, and Operations data as “Operations only”, and created a policy to provide access to people within the department. Then through attribute-based access control (ABAC) model, Privacera controls access based on users’ department and streamlined operations, reduced management time by 70%, eliminated human error, and ensured consistent compliance with GDPR and CCPA. Privacera’s scalability also allowed Tarmark to confidently expand into new markets while maintaining robust data security.



- GOVERNANCE
- COMPLIANCE
- GDPR, CCPA
- SIMPLICITY
- DATA SECURITY
- LESS ERROR PRONE

CHALLENGE #2

Manually integrating new projects, datasets, and tables into the governance framework is inefficient and error-prone

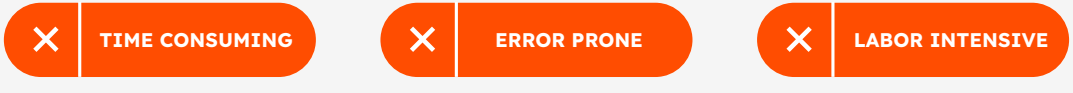
Adding new datasets and tables to large-scale data environments creates challenges. You have to resort to manually integrating these resources into the governance framework. Each dataset requires defining roles, permissions, and policies, involving coordination between IT administrators, compliance officers, and data stewards. Reliance on ticketing systems exacerbates delays, as requests undergo lengthy reviews and approvals, often taking hours to several days. These inefficiencies slow access to critical data and reduce productivity across teams.In some cases this could take 2 hours to 2-5 days and slow down the entire data management process and increase the risk of security breaches or non-compliance with regulations.

UNWANTED SCENARIO EXAMPLE #2:

Manually Addition of Dataset at a Large Retail Compromises Security & Compliance and Creates Inefficiencies

A large retail company, Tarmart, faced challenges with manual data governance as its data environment expanded across platforms like BigQuery and Cloud SQL. Furthermore, adding a new dataset to its system involves multiple stakeholders, including compliance officers, IT administrators, and data stewards, each playing a critical role. The process begins with the data owner submitting a request, detailing sensitive information like PII or email data within the dataset. The IT administrator reviews the request and forwards it to the compliance officer, who determines the appropriate access policies based on the type of data and the user groups needing access. Once the compliance officer establishes the policy, they pass it to the data steward, who ensures the dataset is managed according to organizational standards. Finally, IT administrators upload the dataset and grant access based on the defined policies, acting as facilitators. Though this collaborative workflow ensures security and compliance, it can also introduce inefficiencies, especially when managing multiple stakeholders and manual approvals.

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



SOLUTION #2

Privacera automates data access, governance, and compliance at scale

Privacera simplifies the integration of new datasets into BigQuery projects, datasets, and tables by automating permissions and policy management. Unlike manual ticketing systems and policy creation, Privacera dynamically assigns permissions based on attributes such as User, Object, Action, and Environmental factors. This ensures efficient, secure access without manual intervention. New datasets, objects, and tables are automatically governed upon creation, seamlessly inheriting existing rules. This eliminates delays typically associated with adding new assets while maintaining consistent governance, security, and compliance standards.

By automating dataset governance, Privacera enables organizations to manage data growth without the administrative burden. Teams can allocate more time to strategic initiatives rather than repetitive tasks. Automation also enables your organizations to scale more quickly while maintaining consistent governance policies across your entire data environment.

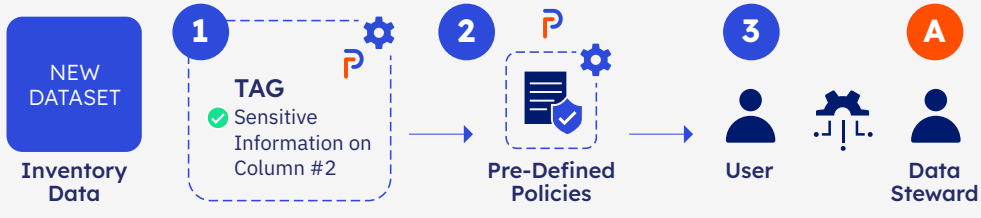
IDEAL SCENARIO EXAMPLE #2:

Privacera Ensures Access, Security, and Compliance at Scale by Automating Access to New Datasets at Tarmart

At Tarmart when the data owner added a new dataset, e.g to Inventory Data, privacera automatically detected that a new dataset was added to BigQuery. Next, it identified sensitive information based on data and metadata (e.g. schema, format). Based on this information, Privacera then applies the necessary tags, and makes it available to the system by making it public. Existing policies are leveraged to apply permissions to the data. In this case, Privacera ensured that the newly created "dataset" in inventory Data in S3 was instantly governed with existing policies.

As a result, the following policy was enforced: "Mask sensitive information for non-HR and non-US members". Instead of relying on ticketing systems and manual approvals, Privacera dynamically applies predefined access controls based on user roles, group memberships, and compliance requirements. This guarantees that authorized users can securely access new Inventory Data without disrupting workflows.

This automation reduces administrative overhead at Tarmart and enhances operational efficiency - which enables teams to make immediate use of new Inventory Data for business insights and decision-making.



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 #3

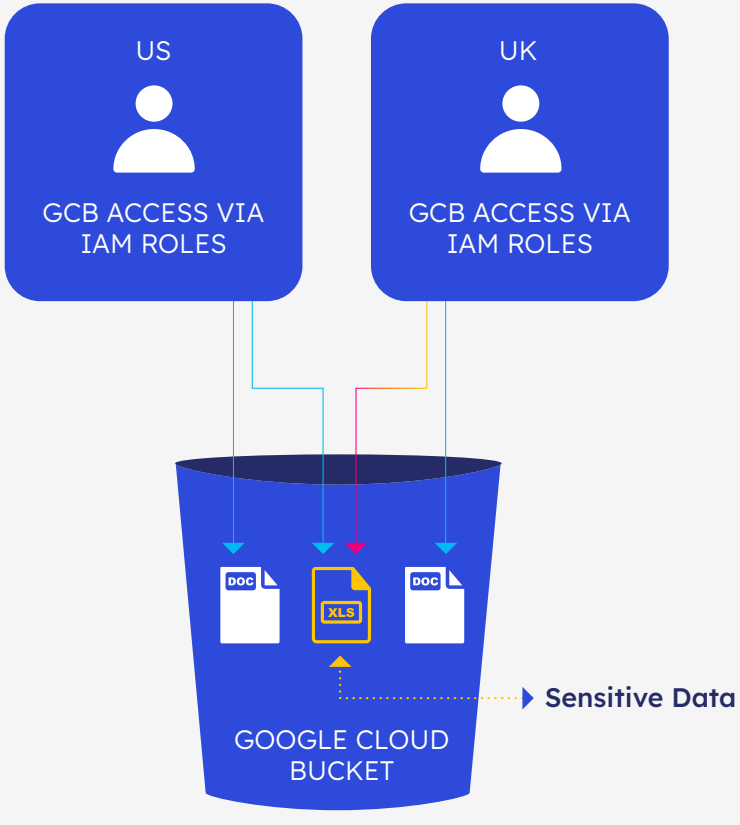
Over-Permissioning with IAM-based access imposes a security risk

Some organizations rely on IAM for access control. However, IAM-based access control in GCS applies permissions at the bucket level. This means that all objects within the bucket are accessible to users with permissions for that bucket. In short, every user has access to everything within the bucket. This leads to over-permissioning and exposes sensitive data to unauthorized users, posing a significant security risk.

UNWANTED SCENARIO EXAMPLE #3:

The Consequences of Over-Permissioning: How GCS Exposed Technotech to Data Breach

Technotech, a growing tech company, faced security risks with Google Cloud Storage (GCS). As the company expanded, this led to over-permissioning, granting employees from different divisions access to sensitive US data. This exposed critical personal information, such as employ's PII records to unauthorized users, increasing the risk of breaches.



Per Compliance mandate, the UK shouldn't have visibility into US data.

UK team HAS visibility into sensitive US data.

SOLUTION #3

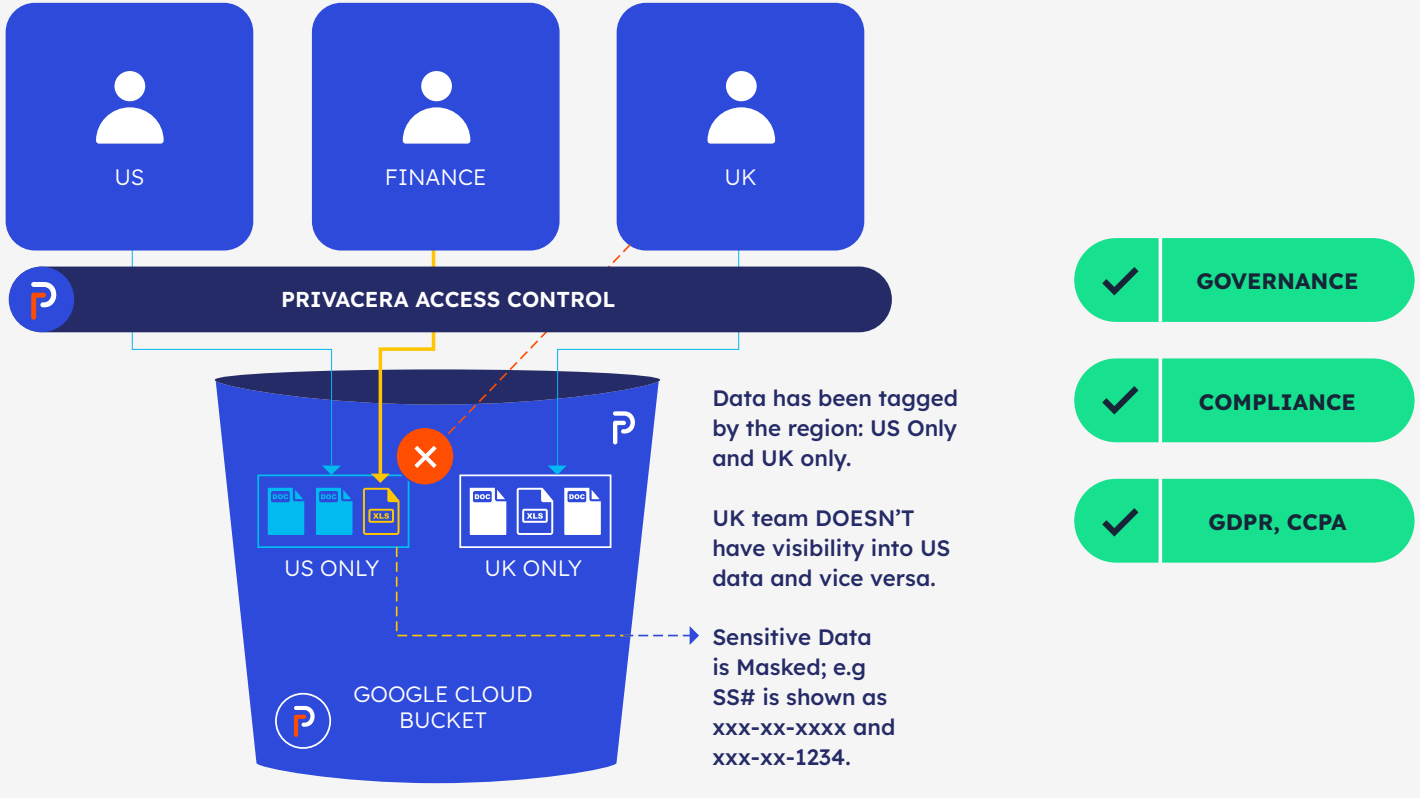
Privacera centralizes access to Google bucket with ABAC and object-level controls to provide fine-grained access

With Privacera, you can centralize access management for Google Bucket. This helps you eliminate the need for thousands of IAM roles. You 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 - 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 #3:

How Privacera Helped a Technology Company Prevent Data Exposure with Granular Access Control

Technotech adopted Privacera, and it allowed their data team to restrict access to data based on user roles and locations. The US team has sales and marketing data - including sensitive data in the same bucket as the Sales team. Though the bucket is shared between the two members from the two countries, the UK team only has access to the data that is granted to them. The data steward tagged the US data as “US only” data and UK data as “UK only” data, 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 UK 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.



CHALLENGE #4

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

To implement more granular access control, organizations often create separate cloud storage buckets and IAM roles for sensitive data. This results in bucket sprawl, excessive IAM role management, and increased complexity, which can lead to operational inefficiencies and higher chances of human error. In addition, there is a hard limit to number characters (2000) you can have in a policy and number of IAMs roles (5000) in a domain.

UNWANTED SCENARIO EXAMPLE #4:

A Leading SaaS company's Governance Struggles: The Hidden Costs of Bucket Sprawl and IAM Overload

Technotech, a leading SaaS company, struggled with managing data governance as its engineering and marketing departments expanded their use of Google Cloud. To implement more granular access controls, the company created separate cloud storage buckets and IAM roles for sensitive data. However, this led to severe bucket sprawl and an overwhelming number of IAM roles to manage, creating operational inefficiencies and increasing the likelihood of human error. The IAM roles increased to 5300 due to different projects and as a result they ended hitting the limit of 5000 within the domain.The lack of a streamlined approach made it difficult to enforce consistent governance policies, exposing Technotech to potential data breaches and compliance risks while overburdening its IT team with excessive administrative overhead.

SOLUTION #4

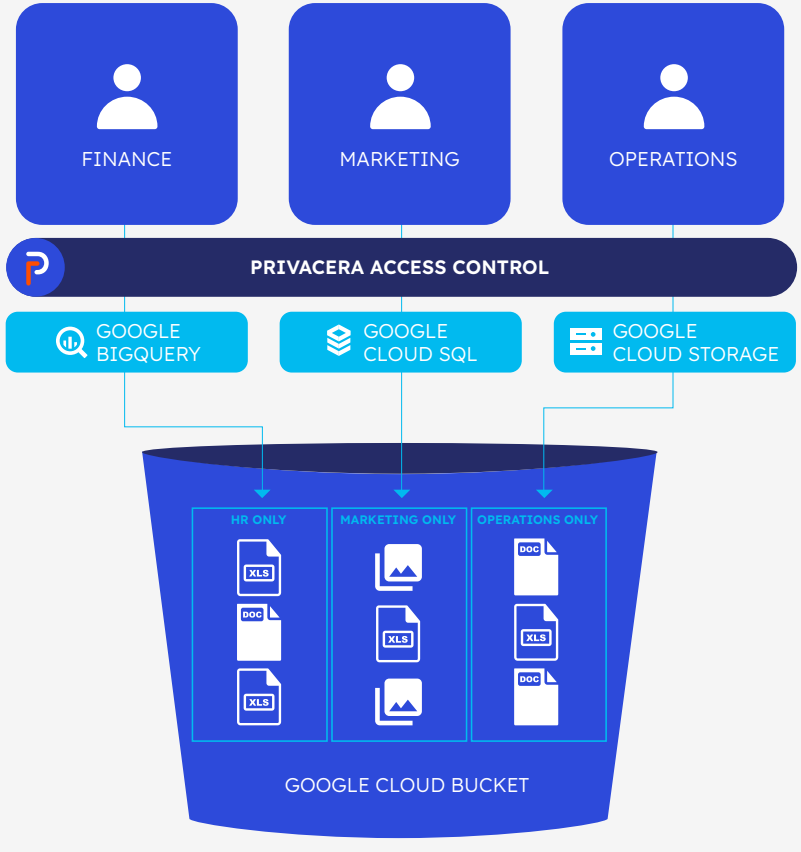
Privacera eliminates bucket sprawl with object-level access control and automated permissions

With Privacera, you totally eliminate the need for separate buckets to isolate sensitive data. This is because Privacera provides you a platform where you can get dynamically controlled access at object-level at a centralized level. Instead of creating new IAM roles and buckets for each use case, Privacera helps you eliminate the need for thousands of IAM roles. You 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 - giving you fine-grained access control. This fine-grained access control ensures only authorized users can access specific objects, reducing over-permissioning risks. This approach also helps you to significantly reduce bucket and role sprawl and never hit the character and/or bucket limit.

IDEAL SCENARIO EXAMPLE #4:

A Unified Framework: How TechEdge Overcame Bucket Sprawl Challenges

Technotech transformed its data governance by leveraging Privacera's unified framework to tackle bucket sprawl in its growing BigQuery environment. With Privacera', data stewards tagged data and created policy, where each team member accesses only their authorized datasets, ensuring finance sees financial records, marketing views campaign analytics, and operations handles logistical data. Privacera's attribute-based access control (ABAC) prevents unauthorized access, safeguarding sensitive information and ensuring compliance with regulations like GDPR and HIPAA. Finally, the reduction of the number of buckets and roles helped them overcome the hard limits of maximum buckets and roles they could possess.



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

CHALLENGE #5

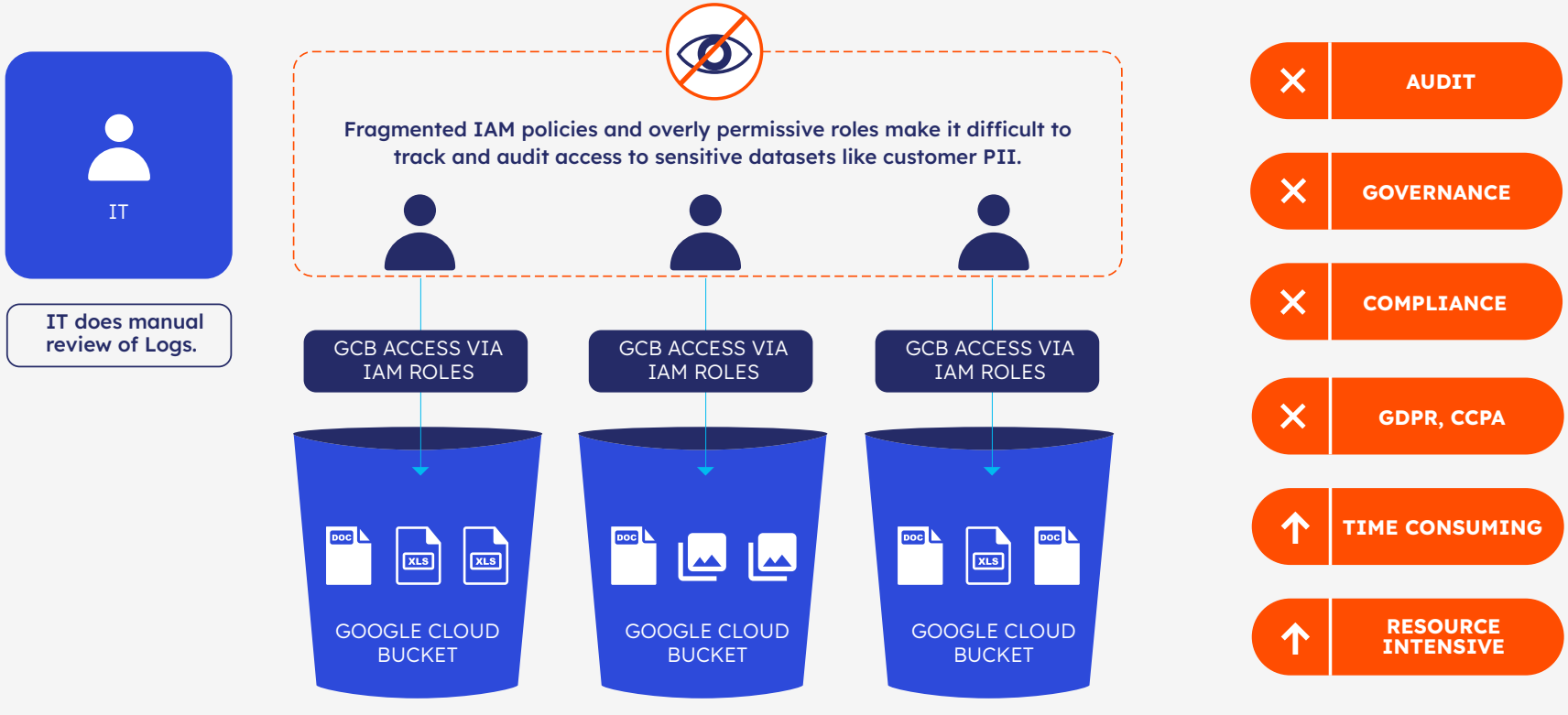
Lack of visibility and auditability of access and permissions. Privacera provides comprehensive visibility of access and governance

The lack of centralized governance in GCS can make it difficult to track access and ensure that policies are consistently enforced. This creates challenges during audits and increases the risk of non-compliance with data privacy regulations.

UNWANTED SCENARIO EXAMPLE #5:

The Risks of Fragmented Governance: How Lack of Control in GCS Led to Compliance and Security Challenges

Streamline Manufacturing, a global industrial supplier, struggled with a lack of centralized governance across its Google Cloud Storage (GCS) environment, which stored sensitive production data like design files, supplier contracts, and IoT sensor logs. The absence of consistent access controls made it difficult to track which user had access to which data. This not only increased the risk of unauthorized exposure and errors, but this fragmented approach also complicated audit processes. The access policies were not uniformly enforced, and it delayed necessary audits.



SOLUTION #5

Privacera provides comprehensive visibility of access and governance

Privacera offers centralized visibility into data access and policy enforcement across GCS. Its comprehensive audit and reporting capabilities enable organizations to track user access and data usage in real-time, simplifying audit preparation and ensuring compliance. By standardizing access control and enforcing policies, Privacera helps organizations meet regulatory requirements and demonstrate commitment to data privacy and security.

IDEAL SCENARIO EXAMPLE #5:

How Privacera Transformed Streamline Manufacturing's Data Governance and Compliance Efficiency

Streamline Manufacturing adopted Privacera and eliminated fragment access control in the Google Cloud Storage (GCS) environment. Its data and governance team gained centralized visibility into data access and governance. Privacera's solution provided real-time insights into data usage, helping track compliance more effectively. Privacera's audit and reporting features simplified audits, reduced preparation time, and ensured compliance with GDPR and ISO 27001.

GCP IAM	Privacera
Manually granting access control hampers scalability and efficiency (character limit of 2000 to create policies)	**Privacera automates governance, applying access controls across Google projects and BigQuery, reducing risk**
Manually integrating new projects, datasets, and tables into the governance framework is inefficient and error-prone	**Predefined policies instantly gives “birth-right access” to user of the data**
Over-permissioning with IAM roles imposes a security risk	**Centralized ABAC with object-level controls provides fine-grained access control**
Creating separate buckets for sensitive data results in IAM 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)

PART 2

Disadvantages of GCP Specific DIY Controls

Organizations often adopt an GCP-specific approach to access and security management, assuming it provides tighter control and cost efficiency. GCP itself promotes its native tools as comprehensive solutions for data governance and security. However, as data volumes grow and extend across various GCP 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