EBOOK

How to Drive Data Value and Innovation with Unified Data Security Governance

Grow at Speed without Risking Data Access, Privacy, and Security

privacera

Data is at the heart of everything your organization does.

It has the potential to inspire innovation, enhance customer experience, and optimize business operations; the opportunities are endless. But your company can't create this value if your business users don't have the secure data access they need to gain insights that drive innovation and growth.

This challenge is huge for organizations that take a resource-intensive DIY or native approach to data access and governance, where:

A **DIY approach** centers on manually coding data access policies and separate database policies to create the idea of a centralized approach.

A **native approach** relies on the sophisticated access control mechanisms of each database but is limited to a single service or cloud offering.

These methods "do nothing" to establish consistent data access, privacy, and security, putting organizations at significant risk for a potential and costly data breach.

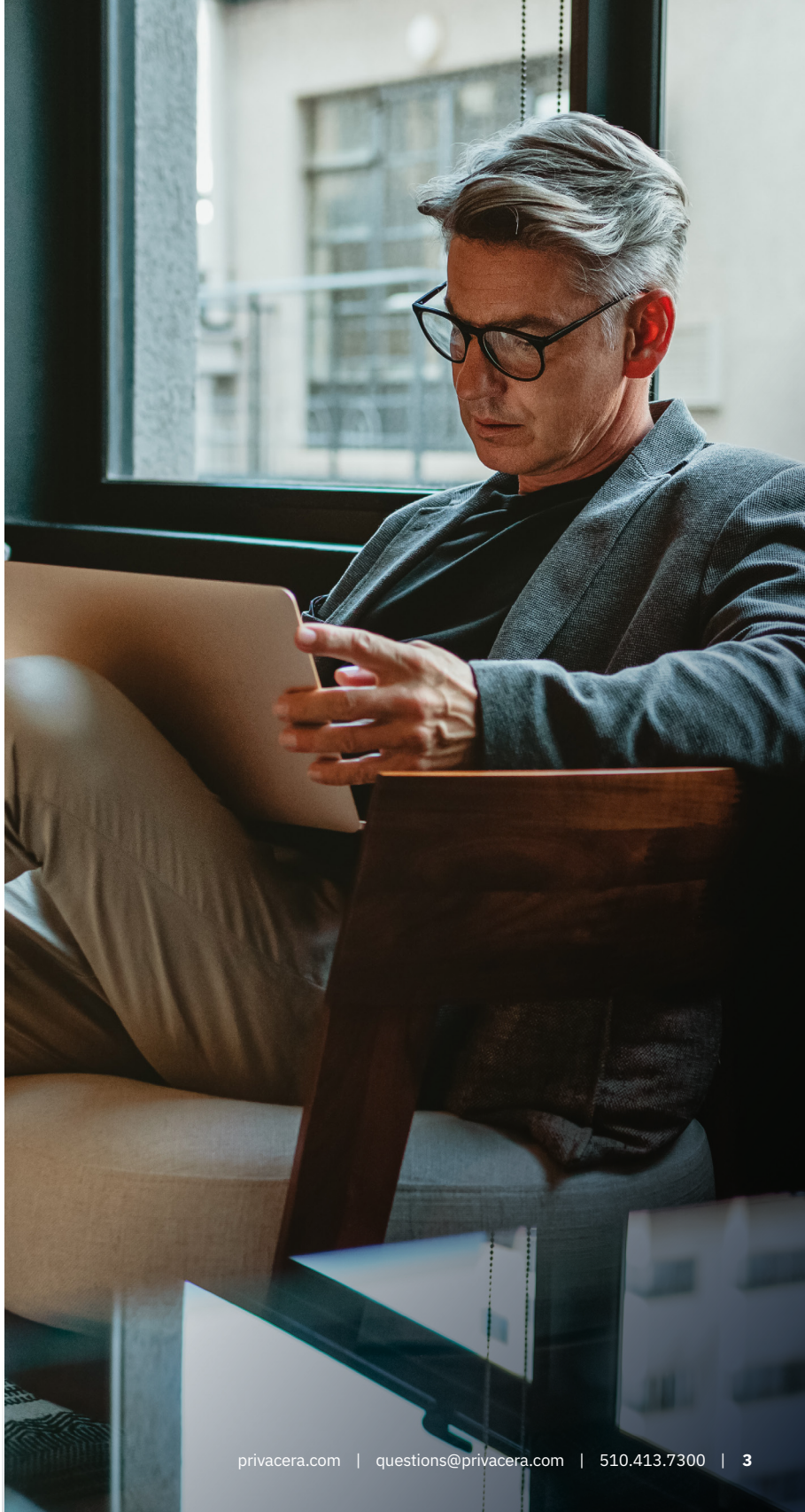
Whether you use one of these approaches to data security governance or are considering it, this guide is for you.

It's for data platforms and data security professionals in upper management who need a cost-effective data governance solution. And it's for data-forward leaders who want to enable data democratization and self-service to drive company innovation and growth.

This e-book explains how to:

- Avoid the cost and risks of doing it yourself—that is, doing nothing—to unify data security governance.
- Adopt a unified approach to data access, privacy, and security on a single platform that creates value and achieves ROI.
- Choose a data security governance solution that drives data value and innovation.

By reading this e-book, you'll understand why a unified data governance solution outweighs the DIY and native approaches. You'll also discover how it enables data access, privacy, and security for data democratization across your organization. Let's get started.



1 Unify Your Data Security Governance

Enforcement of data security governance often falls on IT teams to create solutions on-premises that exist in silos for each database or service.

PROBLEM

Divided Approach

Ownership can vary between these teams:

- Data platform
- Information security
- Data analytics

This divide can lead to the following challenges:

- Security teams often prioritize perimeter security with less focus on data security. However, both are critical as organizations move from a coarse-grained, external threat focus to fine-grained controls centered on insider threats and data leakage.
- For organizations that use a modern cloud data stack, data spans multiple services in the cloud, making it difficult to enforce security holistically, with scarce resources to manage it.

With these approaches, your organization risks data security, inaccurate insights, and delayed growth.

SOLUTION

Unified Approach

Information security and data analytics teams must agree on a solution that serves both sides and gives business users what they need. A unified approach to data security and access governance unites the needs of your data platform, information security, and data analytics teams on a single platform.

By unifying your data security governance, you promote data access, privacy, and security governance across your entire organization. You enable your teams to create policies by using a common UI and enforce and execute them across your entire data estate. The underlying data service enforces native policies, including advanced tag-based, attribute-based access control (ABAC) and role-based access control (RBAC) policy creation.

You also democratize your data for business users at all levels to create opportunities to drive growth.

2 Deploy Zero Trust

In a general sense, DIY projects might seem cheaper. But a DIY or native approach to data governance is far from cheap and presents a greater risk of a data breach. In fact, in 2022, the average cost of a data breach worldwide reached $4.35 million, averaging $6 million for financial services and $10.10 million for healthcare.[1] Each year, the cost grows more and more.

PROBLEM

High Potential for a Data Breach

That risk is too great when you break down the financial impact of a data breach:

- **Fees and recovery:** Most of the cost goes to:
  - Fines charged by regulatory and government agencies
  - Remediation efforts to identify, evaluate, and correct vulnerabilities
  - Legal fees
- **Data loss:** You lose proprietary information to cybercriminals who may demand a ransom to return it to you.
- **Reputational risk:** Beyond these amounts is damage to your brand, reputation, relationship with your clients and prospects, and the potential loss of business.

Massive reputational risk isn't solely on IT, but on the entire organization. The goal for the CISO and CDAO is to avoid this risk.

SOLUTION

Consistent Authorization Policy Control and Auditing

Organizations that deploy zero trust reduce the costs of a data breach by 20.5% compared to those that don't use zero trust.[2]

With zero trust at the foundation of your data security governance solution, your security teams can authorize access to data on a need-to-access basis across the enterprise. This solution gives them a strong point of reference when the auditing team asks about security or presents them with challenges. The accountability now rests at the business level, not the IT and security levels.

59%

of organizations that don't deploy zero trust incur an average of USD 1 million in greater breach costs compared to those that do.[3]

1. IBM. Cost of a Data Breach 2022: https://www.ibm.com/reports/data-breach.
2. Ibid.
3. Ibid.

3

Automate and Encrypt Data Access

DIY and native approaches to data governance lack encryption, limit access, and impede productivity.

PROBLEM

Lack of Productivity

A lack of productivity from DIY and native approaches occurs for several reasons:

- **Cost:** They require additional IT staff and resources to build and manage the solution. They also need a full-time experienced data engineer, which alone can mean an extra $120k–$200k per year.
- **Limited data sharing:** Your users can't access the data they need. Instead, they must ask the IT team to handle their one-off custom requests to get the private data they need.
- **Sustainability:** These solutions don't scale easily as your organization grows, making the increase in requests difficult for the IT staff to manage and complete efficiently.

As organizations grow over time, the number of users and policies increase. To keep up, data scientists need greater access to more data from a system that lacks the capacity to scale. This situation creates organizational data friction, preventing critical access to and effective use of the data.

SOLUTION

Automated Data Discovery and Encryption

Choosing a unified data governance platform means greater productivity, which is enabled by:

- **Reduced cost:** The automation alone reduces policy administrator resources by 50%–70%. It also decreases the IT, data engineering, and administration costs a DIY or native solution requires.
- **Data security automation:** Automation for sensitive data discovery, classification, and tagging used to create tag-based policies and rules enables fine-grained data access enforcement.
- **Scalability:** As your organization grows and the number of new policies increases, the platform scales to keep up with the additional users and policies. Self-service capabilities enable end users to get near real-time data access.

Through the platform's built-in encryption, your end users can access critical data sets, but can't view any sensitive data they don't have privileges to, allowing analysis without exposure to sensitive data.

4 Enable Self-Service

One of the biggest challenges of DIY and native approaches is they don't give your users the data or accuracy of data they need to make effective decisions.

PROBLEM

Outdated Data

In-house approaches are limited by the budgets and resources to support and maintain them. A solution without the capabilities and features your business users demand prevents them from getting access to the data they need. As a result, in-house approaches slow innovation and growth opportunities for your data analyst and business teams.

Because your critical teams become consumed with filling requests, they are slow to deliver timely data, resulting in outdated analytics and stale business insights. Eventually, IT resources become so tied up in handling data requests, they don't have time to handle their core business responsibilities.

$65 million

The **increase in net income** by Fortune 1000 companies that increase data access by 10%.[4]

4. "The Four Key Pillars To Fostering A Data-Driven Culture." Forbes, March 2019, accessed March 1, 2023: https://www.forbes.com/sites/brentdykes/2019/03/28/the-four-key-pillars-to-fostering-a-data-driven-culture/

SOLUTION

Self-Service with Rapid Access to Critical Data and ROI

To successfully enforce data security policies across the business, data governance ownership transfers from centralized teams and processes to business teams who know the data and context. This simplified approach streamlines data security governance and empowers teams with approved, designated data access without bombarding IT with endless access requests.

From a single platform, they gain the ability to:

- Own the data quality.
- Manage the data stewardship tasks.
- Get quick access to critical data through automation and self-service.

This concept, referred to as *federated governance*, makes it easier to trust data across the data mesh. The greater access your business users have to your critical data, the more informed analytics they'll have. This approach to self-service also prevents the widespread problem of data-security extremes. It ensures your data security is neither so stringent where too few get the data they need to do their jobs, hampering insight analysis, nor so open it leaves your data vulnerable to unauthorized access.

5

Enable Consistent Compliance and Data Sharing

Working with analytical tools using a siloed, source-by-source approach creates inefficiencies and inconsistencies in your data security governance strategy and implementation.

PROBLEM

Scattered, Inconsistent Data Governance

Working across data architectures presents challenges for IT teams. Each cloud provider has five or more different data governance standards, placing extra demands on IT teams for the additional skills and resources to manage them. These demands compound as your organization adds more cloud services, such as Databricks, Snowflake, and Starburst.

As a result, you get scattered authorization and governance from working with various vendors and being locked into their agreements. Plus, because you have to deal with multiple data standards, depending on each vendor solution, your infrastructure concedes to a lower level of trust.

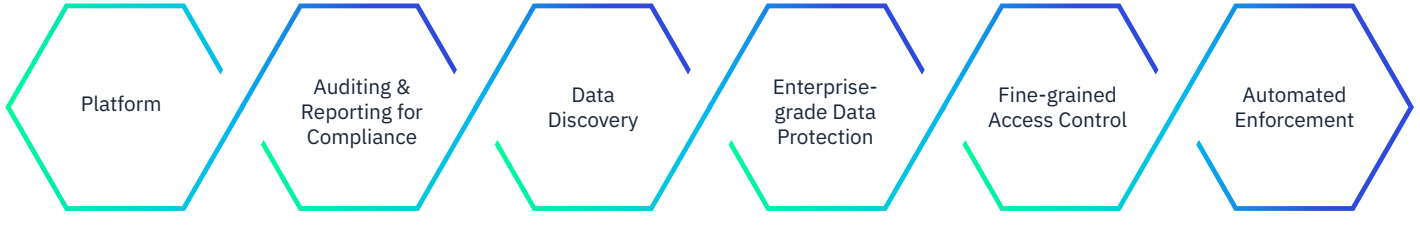
SOLUTION

Centralized governance across the ecosystem

By providing data access, privacy, and security on a single platform, you enable consistent compliance. You can easily apply policies, such as GDPR, CCPA, LGPD, and HIPAA, for data distributed across multiple cloud databases, analytics platforms, reporting systems, and regions.

A single integrated system makes it easier and faster for you to transform your sensitive data across cloud databases and analytical platforms. When built on open standards—specifically Apache Ranger—a single system centralizes data and security governance across individual services natively and the data ecosystem, whether resources are on-premises or in the cloud. As a result, you enable data sharing and data democratization throughout your organization in a trusted, secure environment.

Components of Unified Data Security Governance



6 Choose a Data Security Governance Solution

To achieve the full advantages of a unified data governance solution—and realize the greatest impact on your ROI—ensure your platform has these key features:

- **Rapid access.** Empower your analytics teams to access new data sources securely, unencumbered by a confusing array of different access controls.
- **Democratized access.** Protect sensitive data with masking and encryption techniques, enabling analysts and data scientists to use regulated data to extract insights.
- **PII discovery.** Discover sensitive data automatically by using data dictionaries, pattern matching, and models to detect personal attributes like Social Security numbers and birth dates.
- **Fine-grained control.** Look for RBAC to grant access according to employees' roles, and ABAC to govern access based on employee attributes.
- **Flexibility.** Define access policies at the database, table, column, object, or file level. Give data administrators the ability to manage fine-grained access controls for on-premises data lakes, public cloud services, and third-party cloud-native services from a single console.
- **Automated enforcement.** Automatically enforce policies regardless of data location. Use tag-based policies to apply on-premises access and encryption rules equally to cloud-based data.
- **Compliance.** Protect data according to privacy laws, such as GDPR, CCPA, and LGPD (Brazil), and HIPAA compliance for personal healthcare data.
- **Consolidation.** Define and enforce data access policies through a single platform, reducing the number of policies—even by the thousands—across your organization.
- **Coverage.** Give enterprise users the ability to manage access policies from a single interface. Native connectors provide coverage across cloud platforms such as:
  - AWS
  - Databricks
  - Google Cloud Platform
  - Microsoft Azure Databricks
  - Snowflake
  - Starburst
- **Reports and alerts.** Generate reports by monitoring and auditing data access behavior. Get alerts when users access sensitive data.
- **Scalability.** Take comfort in knowing, as your organization grows and data quantities increase, your data security governance platform scales to handle the higher volumes of data and number of users.
- **Ease of maintenance.** Make it easy for your managers to change and add access policies, speeding up user access and lowering TCO for your organization.

Start Your Journey to Unified Data Security Governance

The path to becoming a data-driven organization starts with unified data security governance. This approach pivots your organization from “doing nothing” to enabling data democracy for everyone.

To increase the value of your data for faster time to insights and innovation, look for a unified data security governance platform that:

Empowers you to holistically secure and protect your data with consistent and native enforcement across your hybrid cloud data estate by using connectors.

Automatically synchronizes policies for native integration and enforcement on the data source with no impact on query performance and no changes to end-user queries.

Automates policy creation based on roles, resources, attributes, and tags, including built-in approval workflows for federating governance tasks to business owners.

Is based on Apache Ranger and open standards to support a variety of data assets, native integrations with access and identity management tools, and optimized interoperability with your top applications to future-proof the open cloud.

Provides built-in algorithms for data classification, masking, or encrypting to support regulations, such as GDPR, SOC, CCPA, PCI, FISMA, GLBA, HIPAA, and LGPD.

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 data access to data consumers, the company provides data privacy, security, and governance on its SaaS-based data security and access 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, 2022. Learn more about Privacera at privacera.com.

privacera