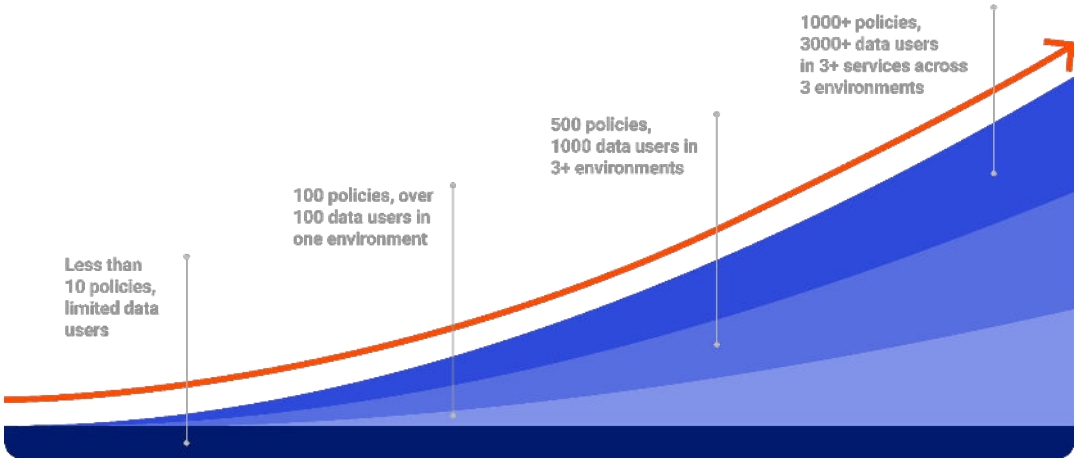
privacera

Keys to the Kingdom: The Costs and Missed Opportunities of Failing to Implement a Data Security Platform

Organizations face the daily challenge of balancing critical data requirements—straddling the need to open certain gates to enable self-service data access while closing other access points to maintain various internal and external compliance. Your teams must have access to your walled data to actuate value. But multiple, significant risks inevitably follow. Ignoring this reality opens an organization to severe losses and potentially crippling costs. Privacera addresses all this by ensuring data is regulated and monitored in a unified manner, making data access privileges and governance an attainable and maintainable effort for IT without compromising the keys to the kingdom.

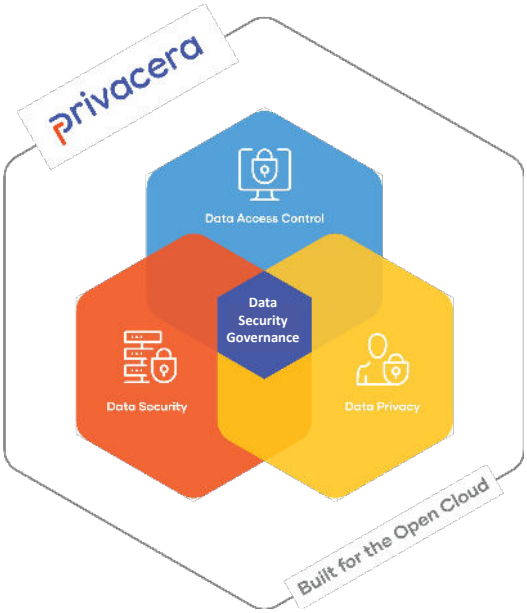


Without the right platform and support, a myriad of internal processes, systems, and compliance cases lead to a logistical nightmare for anyone who needs to enable data democratization or comply with local regulators. While business intelligence and data science tooling provide access, this opens the gates to potential risks and losses. And do-it-yourself / native setups only provide a bandaid, leaving you with endless data and system connections to enable. As the number of users and data policies increase over multiple services and environments, time and financial investments only grow exponentially.

Transform Risk to Reward with an Enterprise Data Security and Governance Platform

Only enterprise data governance provides a comprehensive system of checks and balances across systems, silos, and the cloud. It scales with the enterprise, allowing business stakeholders to own policies and system compliance. Ultimately this provides the entire organization with regulatory stopgaps, with accountability taking place at the business level, taking the pressure off IT and enabling analytic and data science workflows.

In the following breakdown, let's take a systematic look at data governance opportunities and production costs organizations will face when designing and funding their architecture, and how Privacera addresses each of these.



Cost of Doing Nothing / DIY	Opportunity with Privacera

Risk from Data Breach

Security is a shared responsibility. The average cost per breach is around $4.24m per breach according to Digital Guardian. And if you are in Finserv it is upwards of $5.7m. Healthcare breaches can reach up to $9.2m.[1] GDPR, CCPA, and related regulations result in real fines, with 2021 having the highest average cost in 17 years.[2]

Regulatory fines	Consistent auth policy control and auditing
Loss of proprietary information	Start at zero trust / enable access
Reputational risk to IT and the organization	Accountability at the business level

Productivity in Governance

The fully loaded costs in the US for a data engineer are around $130 - 200k per year. Typical staff costs per reporting cycle are often as high as $25k and could be repeated on a quarterly basis. In general with automation, you will see a 50-75% reduction in policy administrators.

Manual effort (incomplete inventory)	Automation / data discovery
Increased staffing costs	Reduced admin / eng. costs
Difficult to share private data	Ease of encryption

Empowering Self-Service

Greater access to data equals more informed analytics, reduced time to insights, and faster decisions. For a typical Fortune 1000 company, a very attainable 10% increase in data accessibility has the potential to produce an increase of over $65m net income.[3]

Opportunity loss/lack of innovation	Rapid access to critical data / increased ROI
Slow turnaround time / stale insights	Streamlined/simplified data governance
Draining IT resources/bandwidth	Empowering with access-request approval

Working Across Data Architectures

Even on a single cloud provider, there are diverse standards and approaches to "data governance," with a variety of implications for IT and the organization as a whole. Add to that multiple data and cloud providers and you get a compounded issue.

Scattered auth/governance	Consistent compliance/sharing
Decreased trust in infrastructure	Increased use of data services
Vendor lock-in	Built on open-source
Multiple standards	Centralized governance across the ecosystem

(1) Digital Guardian: How much does a data breach cost in 2021?, (2) IBM's Cost of A Data Breach, research by Ponemon Institute, (3) Forbes: The Four Key Pillars to Fostering A Data-Driven Culture, (4) Tessian: 30 Biggest GDPR Fines So Far (2020, 2021, 2022)