Overcoming the Challenges of Data Security Governance

What is Data Security Governance?

According to Gartner, Data Security Governance (DSG) enables the assessment, prioritization and mitigation of business risks caused by security, privacy, and other compliance issues, as data proliferates across on-premises and multi-cloud architectures. It establishes a balance between business priorities and risk mitigation through data security policies that can be applied across the whole IT architecture.

Benefits of Data Security Governance

- **Risk Mitigation:** By adopting DSG, risk organizations can identify potential security, privacy, and compliance risks associated with their data assets, and mitigate them.
- **Business Continuity:** Effective DSG ensures data remains available and accessible to authorized users, avoiding downtime caused by system or platform failures.
- **Regulatory Compliance:** DSG helps organizations adhere to relevant data protection and compliance regulations, and comply with data sovereignty requirements, thereby avoiding fines and reputational damage.
- **Data Privacy Protection:** The framework established by DSG includes privacy policies and controls that safeguard sensitive data, ensuring it is used appropriately and individual privacy rights are respected.
- **Safeguarding Mission-Critical Assets:** With data proliferation, protecting crown jewel datasets is paramount. DSG helps prevent unauthorized access and theft of critical business information.

Organizations have both structured and unstructured data, both of which need DSG. Cyral, and this document, is focused on structured data which typically lives in databases, data warehouses and data lakes.

For a deeper discussion on this topic, refer to our white paper **"Understanding and Navigating the Data Security Landscape".**

Components of a Data Security Governance Program

An effective DSG program typically includes the following components:

- **Discovery & Classification:** Scan and classify sensitive data to maintain a definitive catalog.
- **Fine-grained Authorization:** Leverage attribute-based policies for
  - **Confidentiality:** Restrict user data access to authorized users for approved purposes.
  - **Data Protection:** Guarantee data integrity and prevent tampering.
  - **Secure Data Copy:** Make data available for testing and modeling without spillage.
- **Assurance:** Provide immutable records for
  - **Monitoring:** Understand who accessed what data.
  - **Reporting:** Provide an audit trail of configuration and access changes.

Obstacles

Building a successful and efficient DSG program faces the following obstacles:

Fragmentation of Controls

Most enterprises end up using different tools for each aforementioned component of their DSG program. This fragmentation of controls creates the following challenges:

Increased cost

Maintaining multiple licenses and support agreements with different vendors often leads to unnecessarily higher costs.

Maintenance overhead

Managing multiple discrete solutions significantly increases the complexity of an IT environment and incurs avoidable maintenance overhead.

Integration difficulties

Solutions from different vendors may be difficult or even infeasible to integrate in a cohesive way. This leads to operational redundancies and information silos among other issues.

Inconsistent protection

Different vendors adhere to different standards, making it difficult to guarantee a consistent level of security and functionality across all systems.

IAM Products Don't Govern Data Access

Identity and Access Management (IAM) is often the bedrock of most security programs. IAM products allow users and their permissions to be managed in one central identity provider, such as Active Directory, Okta or SailPoint. This has multiple benefits:

- It allows users to access services using their already-known identity and permissions.
- It prevents drift between the users and their known permissions across services.
- It helps avoid or minimize dormant accounts and permissions.

However, access to databases and data warehouses is usually managed using roles which cannot be managed using IAM products. This severely impairs the security administration of these data repositories. Permissions management, access reviews, reporting and any related remediation must be done manually.

The “Shadow Users” Problem

Additionally, unlike most other enterprise services, databases and data warehouses are often accessed indirectly using applications, BI tools, notebooks, etc. These applications use a single service account for their access, completely hiding the identity of the actual users. These “Shadow Users” can easily bypass all authorization and monitoring controls and often have privileged access to data.

Example

We encountered an interesting example of this problem in a FinTech company that wanted to prevent engineers from using ETL job credentials to authenticate into the database to access tables that they were not authorized to in their role as an engineer.

The intent was far from malicious, it was to quickly debug business logic issues in their production applications, but was nonetheless an area of high risk. In case any of those engineers got compromised, it would give an attacker a beeline path to the company’s most sensitive customer data.

Gaps in Controls

As a result of IAM limitations and the “Shadow Users” problem, DSG programs suffer from the following typical gaps even when all best-in-breed niche controls are applied in a cohesive manner.

- **Tedious Permissions Management:** Continuous pruning and minimizing permissions GRANTed across different database objects and roles, among other manual processes.
- **Exposure to Unidentified Actors:** Actions executed by users associated with service accounts used by applications and tools go unnoticed by policies and logs.
- **Unregulated Data Flows:** Increased risk of data spillage and abuse due to the proliferation of privileged access through ETL and streaming pipelines.
- **Incomplete Visibility:** Incoherency caused by a mix of short-use accounts and service accounts using varied syntaxes hinders troubleshooting and reporting.

Organizational Sprawl

Lack of concerted ownership

The responsibility of securing data spans multiple teams (e.g., security, enterprise architecture, IT, and data teams), often resulting in conflicting priorities and decisions.

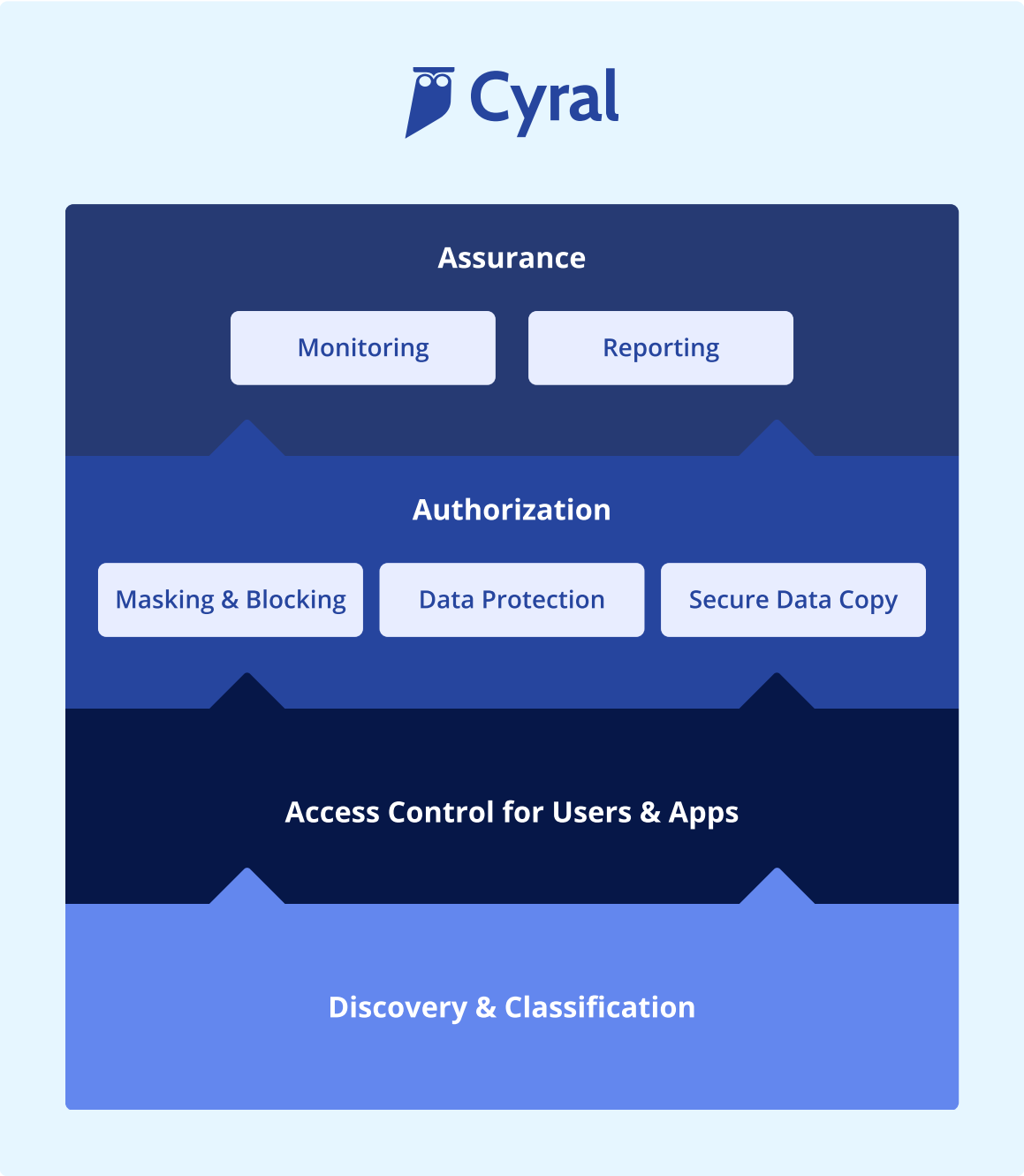
Heterogeneous processes

Different teams often use disparate systems and processes for managing and consuming data, often requiring a different approach to policy administration.

Cyral: An Integrated and Comprehensive Platform

Cyral can replace these niche tools with a unified and comprehensive DSG platform. Additionally, Cyral's patented stateless interception technology allows it to incorporate access controls directly into the stack, which helps address the gaps outlined above.

Cyral's Data Security Governance platform

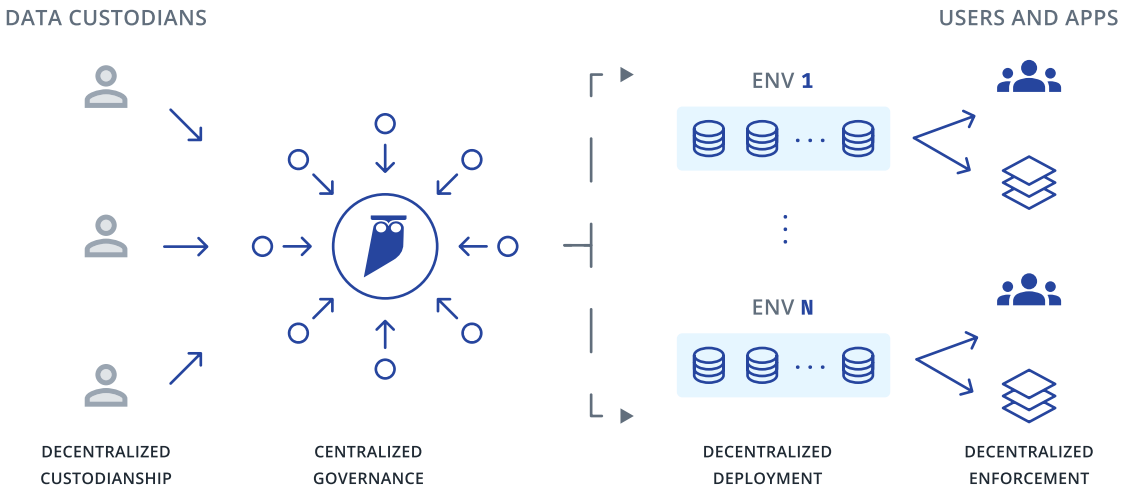


Key benefits of Cyral's platform include:

Data minimization	Tech stack simplification
Improved visibility & control	Increased agility

Built for a Decentralized Architecture and Organization

Centralized controls for a decentralized architecture



Cyral manages policies outside of the databases themselves, stores them in a distributed manner, and allows them to be specified using attributes and identities managed in standard systems like AD, SailPoint, Okta, etc. This provides the following unique advantages:

- **Seamless Policy Enforcement:** Policies can be enforced across all users and apps, without requiring any workflow or tooling changes.
- **Flexible Deployment Options:** Cyral can be deployed across multiple environments (on-prem, AWS, OCI, etc.) and using standard orchestration tooling, such as K8s, ECS, VMs, rpm, etc.
- **Collaborative yet Centralized:** Policies can be specified by multiple teams in their preferred formats, accommodating both ClickOps and GitOps workflows, all without compromising enforcement consistency ensured by centralized policy management.

About

Cyral provides controls for privacy, compliance, governance and protection thereby reducing risk, complexity, and cost for managing structured data. The Cyral platform discovers data, unifies access controls for users and applications, enables fine-grained authorization policies and provides complete monitoring and reporting. This comprehensive coverage enables risk-based governance, limits the blast radius of data-related incidents and reduces overhead and costs. Cyral's technology allows customers to implement data security controls using their existing, centralized entitlements, thereby simplifying administration and automating remediation. Customers use Cyral to accomplish least privilege, data minimization, spillage prevention and Zero Trust.

For more information, visit **www.cyral.com** or follow **@CyralInc** on Twitter.