



**Cyral**

WHITEPAPER

# Cyral: Product Brief

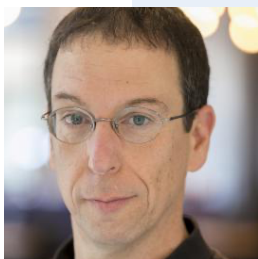
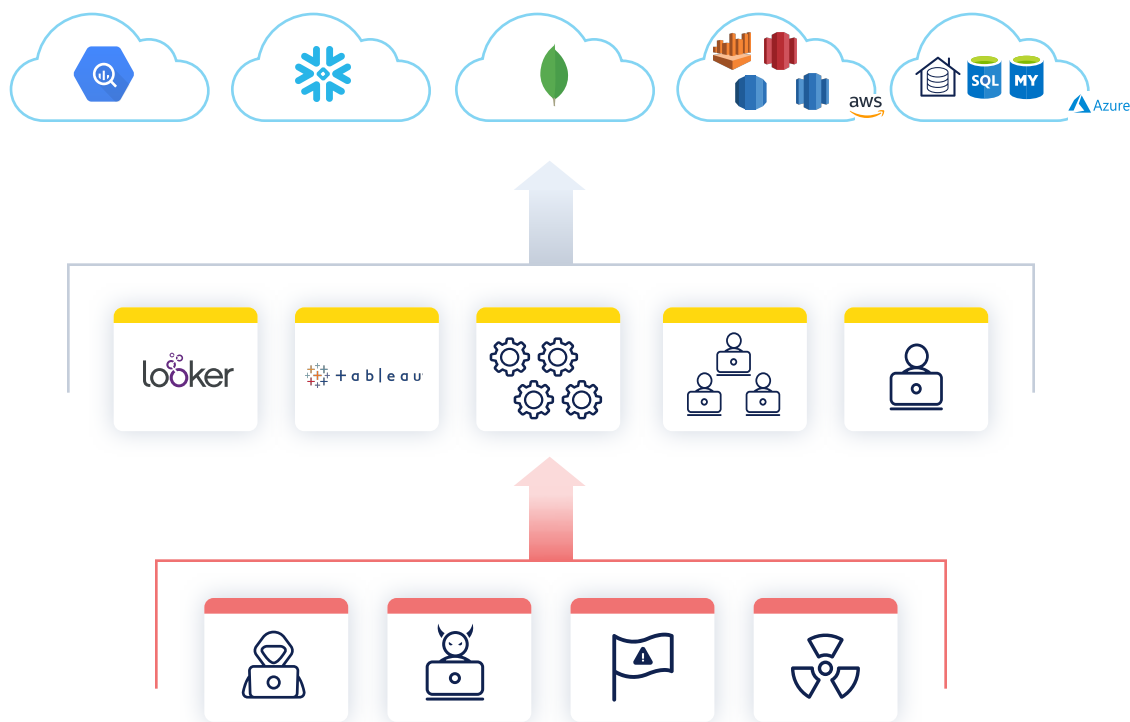
# Contents

Businesses use Cyral to Protect Their Data Using Security as Code	2
Cyral Zeroes in on the Crown Jewels that Hackers are After — the Data	3
Observability Benefits	5
Control Benefits	6
Security Benefits	7



# Businesses use Cyral to Protect Their Data Using Security as Code

Most breaches are targeted at data repositories where the crown jewels of an organization reside. To protect themselves against a breach, the best that security teams can do today is deploy solutions across all their apps, infrastructure, networks and devices, but that does not give them the required visibility and control over their data flows. This is exacerbated by modern data layer architectures deploying database-as-a-service instances, pipelines and cloud data warehouses that do not support traditional monitoring agents and host-based policy enforcements.

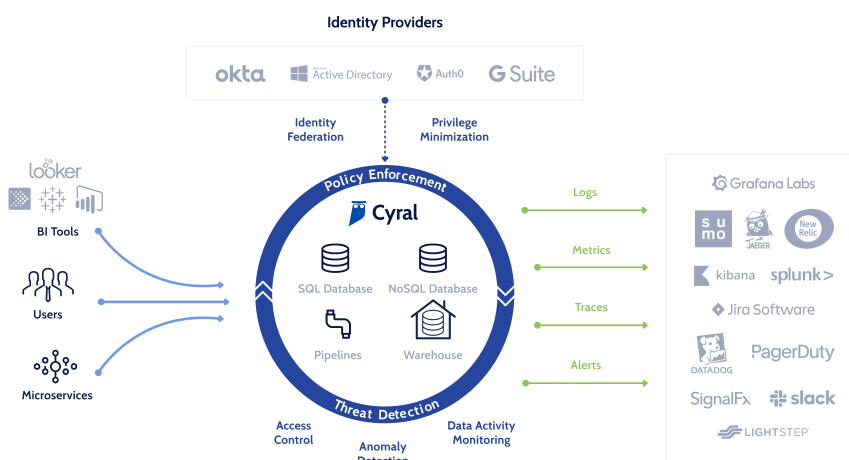


“The industry has long needed a new cloud security service — one that operates directly at the data layer where the crown jewels of business reside.”

— DR. DAN BONEH

# Cyral Zeroes in on the Crown Jewels that Hackers are After — the Data

Cyral is the first cloud-native Security as Code solution to protect the modern data layer. Our platform makes it easy for engineering teams to observe, protect, and control data endpoints in a cloud and DevOps-first world.



## In-line and Scalable

Modern databases, pipelines and data warehouses are provisioned dynamically, modified frequently and scale elastically. For it to be effective, monitoring and policy enforcement must be in-line and real-time. Cyral has invented a stateless data interception technology that is high performance (sub millisecond impact) and scales dynamically with the workload.

## Easy to Adopt

Collaboration is a key part of effective security strategies. Cyral was designed to be plugged seamlessly into existing DevOps and SecOps workflows. Deploy using Terraform, Cloudformation, Chef, Ansible, Puppet. Logs, metrics, traces and alerts can be sent to popular DevOps tools like Splunk, DataDog, ELK, Grafana, PagerDuty and the service can integrate popular security tools used for identity management (Okta, Gsuite, Microsoft AD), incident response (Jira, Hive), forensics and compliance management.



"As a leader in the experience economy, Turo is focused on delivering cutting edge digital experiences to all of our consumers. To enable this, our engineering team relentlessly pursues automation while emphasizing the security of our customers' data.

To earn and keep our customers' trust while delivering an experience they'll love, we need security solutions that are API-first, agile, and fit into all our existing DevOps workflows. That's why we turned to Cyral for enhanced protection of our data that doesn't slow our teams down."

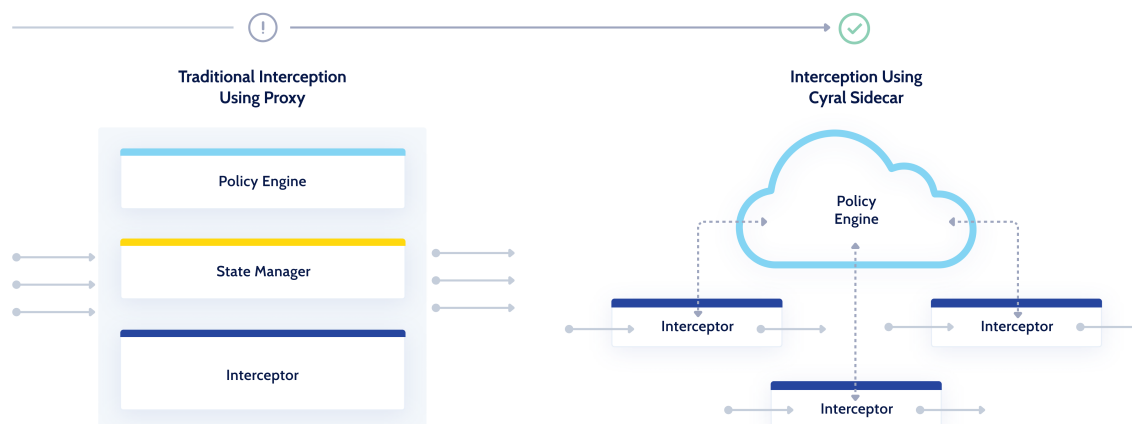
— ADAM BOVILL, DIRECTOR OF ENGINEERING AT TURO

## How It Works

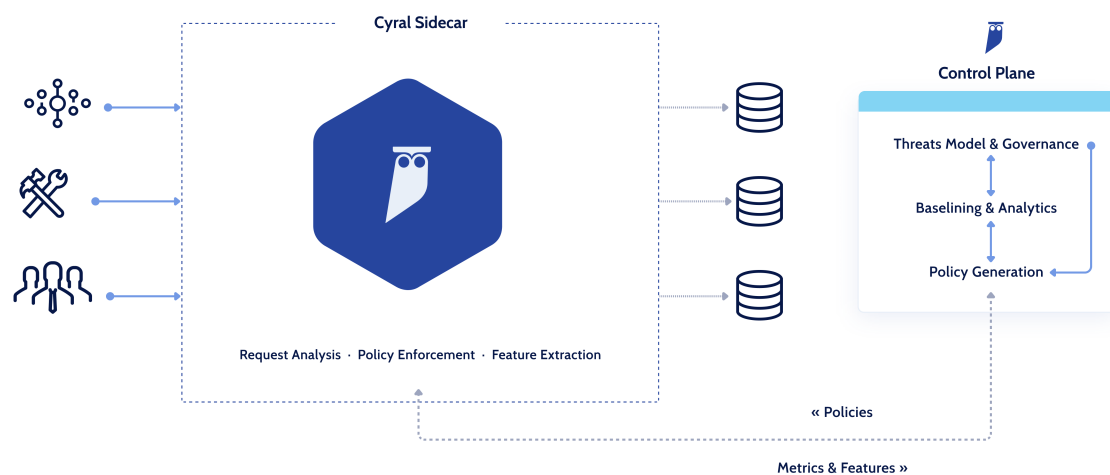
Cyral has invented the first data layer sidecar - a stateless interception service for data endpoints. Cyral sidecar can be deployed in customer's cloud or on-prem environment as a Kubernetes service, autoscaling group, cloud function or host-based install. All the data flows and sensitive information stays inside the customer's environment where the sidecar is deployed, creating no risk of spillage. Our customers can deploy multiple sidecars and easily administer them using a SaaS based control plane. All integrations and provisioning can be managed centrally from here. It offers intuitive workflows to implement security policies and react to threats.



Unlike traditional application proxies, our sidecar defers all session state management to the data layer connections themselves. This elegant design allows multiple sidecars to be deployed in a high-availability configuration and enables a true fail-open design. It has been designed for performance and imposes no measurable impact on latency.



Sidecar intercepts requests to data endpoints with no impact to latency or throughput. It continuously examines, normalizes, and analyzes all requests for policy violations. It alerts on suspicious activity and can block known threats and disallowed accesses. Logs, metrics, traces and alerts get sent to tools of your choice.



# Observability Benefits

Cyral generates unified logs, traces, metrics and alerts that can be consumed through various standard tools for request tracing, monitoring, auditing, forensics and incident response. Example benefits include the following:

## Examples

### Logs

- Who added a new column to the table yesterday?
- Did an Admin execute this DML statement?
- Who granted read privileges to the scientist role on this database?

### Metrics

- Trending # queries per database compared to average
- Trending # of primary / secondary auth failures across all databases
- Aggregate execution time by user / query type for cloud data warehouse

### Traces

- Which service upgrade caused data spillage in canary?
- Which app initiated the service calls that violated tenant policy?
- Which user triggered data leak across multiple microservices?

### Alerts

- Full table scan comprising of sensitive information
- Employee accessing a production database
- Access from a disreputable IP address



**Faster Time  
to Resolution**



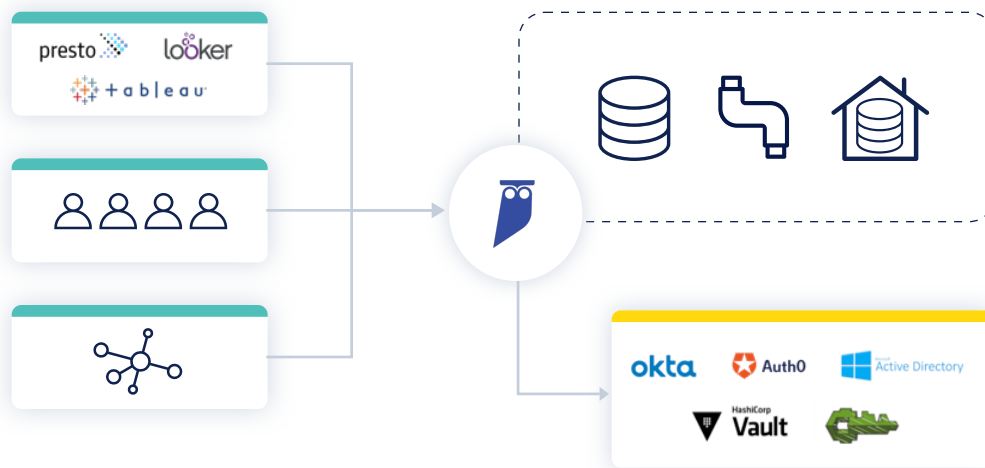
**Simplify  
Audits**



**Data Activity  
Monitoring**

# Control Benefits

Cyral can block requests to the data layer based on rich, granular policies and integrates with standard SAML and OIDC based identity providers. This enables companies to use Cyral to control access to various databases, data warehouses, and pipelines for all users, tools and applications.



Example benefits include

- Federate authentication to the data layer with your SSO provider
- Enable field-level policies based on identity and rich context-based constraints
- Easily monitor and minimize all privileges
- Enable ephemeral access with just-enough privileges
- Both alert and block on disallowed access



“By storing data in SaaS repositories like S3, Snowflake, BigQuery, and RDS, enterprises gain agility but make governance harder and increase the risk of breach. Cyral provides a unique solution for companies to protect their data while also improving visibility for their backend teams.”

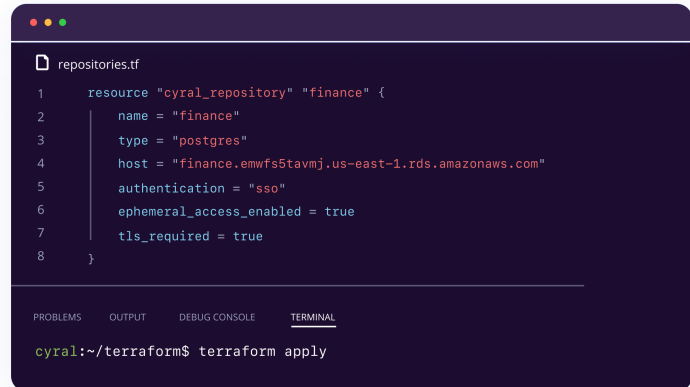
— KEVIN PAIGE, CISO



# Security Benefits

Cyral enables a security as code methodology for development and security teams to collaborate with each other. It can be integrated into the CI/CD pipeline, tightly coupling application development with security management, while simultaneously allowing your developers to focus on core features and functionality, and simplifying configuration and authorization management for security teams.

Cyral has the ability to detect and block threats, and helps protect from the various threats and vulnerabilities.



```
repositories.tf
1 resource "cyral_repository" "finance" {
2   name = "finance"
3   type = "postgres"
4   host = "finance.emwfs5tavmj.us-east-1.rds.amazonaws.com"
5   authentication = "sso"
6   ephemeral_access_enabled = true
7   tls_required = true
8 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
cyral:~/terraform$ terraform apply
```



"At Uplift, data is a key asset and its security is paramount. For us, a security solution must strike the right balance between agility and effectiveness. We needed efficient access controls that allow us to do more with our data while simultaneously eliminating risk and enabling teams to move forward with the greatest speed. With Cyral, we found a solution that does just that."

— STU KELLY, CTO AT UPLIFT

For organizations adopting cloud-native architectures and DevOps practices, security often ends up being a challenge, forcing them to choose between agility and increased risk. Cyral's Security as Code-centric approach to protecting data enables the development and security teams at these organizations to better collaborate to observe, control and protect their data endpoints. It tightly couples application development with security management, providing unique insights for developers and access control mechanisms for security teams. This allows your developers to focus on core features and functionality, and simplifies configuration and authorization management for security teams. This improves collaboration between Development and Security teams and helps nurture a culture of security across the organization.



Cyral is the first cloud-native Security as Code solution to protect the modern Data Layer. For the first time, get a unified view of all your data layer activity. Easily observe, protect, and control your data endpoints in a cloud and DevOps-first world.

Cyral's unique data layer sidecar intercepts all requests to every database, data warehouse and data pipeline from any user, application or tool, without impacting performance or scalability. Our sidecar deploys within your existing infrastructure, Cyral enables visibility and control without changing your applications or workflows.

---

Want to learn more about using Cyral in your environment?  
Sign up for a tech talk with one of our engineers!

[cyral.com/tech-talk](https://cyral.com/tech-talk)