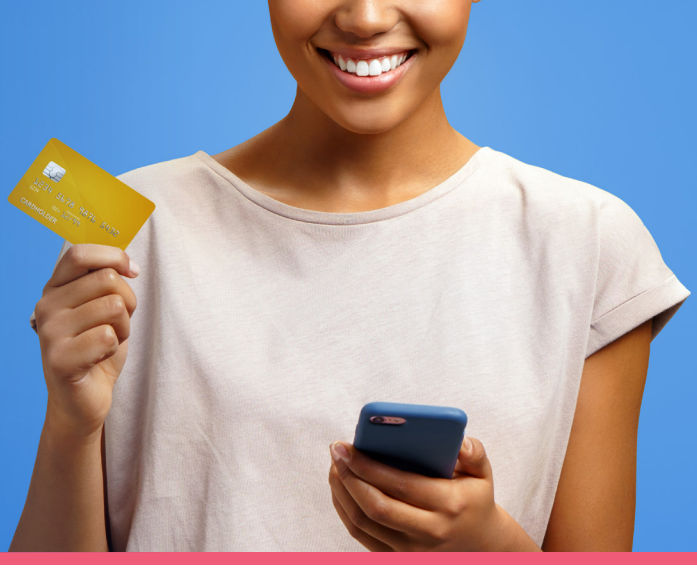
Cyral | CASE STUDY

How Cedar Secures Sensitive Data with Cyral



cedar

As Cedar rapidly grows and on-boards new healthcare providers, Cyral enables the company to maintain a consistent data security posture.

Cedar, who has raised over $350M in funding, is a fast-growing healthcare financial engagement platform whose mission is to empower individuals to easily and affordably pursue the care they need. Cedar partners with leading hospitals, health systems, and physician groups to personalize and simplify the billing and payment experience for patients, ultimately improving financial results for providers. Using intuitive product design and advanced data science, Cedar is the only platform to facilitate patient-centric financial engagement across the care journey.

In an industry where traditional players cut releases once every 18 months, Cedar powers innovation with two deploys per day, across multiple product teams working independently. This fast cadence requires automation at all levels, including automatic enforcement of internal data access policies so development teams stay secure and maintain an audit trail, and real-time data activity monitoring in production systems so the team can spot potential threats immediately

Industries: **FinTech, Healthcare**

Headquarters: **New York, NY**

Size: **400+ employees**

Customers: **2500+**

Market Cap: **$3B+**

Type: **Privately Held**

Founded: **2016**

THE RESULTS

- Implemented access controls to protect PII data
- Gained consistent data activity monitoring for all data and users
- Improved collaboration between security and DevOps

Their Challenge

Cedar is growing rapidly and quickly onboarding new providers. To deliver a personalized end-to-end billing experience for patients and an easy implementation for providers, Cedar fully integrates with the providers' EHR and billing systems. However, every provider has an individualized approach, complicating unified management of health records and databases. For Cedar's CISO Aaron Zollman, the security of their customers' data was of the utmost importance. Zollman had already implemented a robust security practice for all of Cedar's clients. But as their numbers grew, he wanted to be sure they could maintain the same levels of security without slowing down performance and quality of service.

Cedar sought to improve in the following areas:

Better management of database credentials and access as team continues to grow

Implement more robust alerting and blocking in case of potential data exfiltration of sensitive information

Simplify manual and complex workflows that slow down engineering

The Solution

> "Cyral was the missing piece for us in access governance. It helps us tell a clear story of why a piece of data is protected, who accessed it, how they authenticated and what queries they ran."
>
> **- Aaron Zollman, CISO, Cedar**

Granular and centralized controls for database credentials and access privileges

Managing database credentials and access for a growing number of users was becoming an increasing priority. Cedar uses various developer-friendly databases that don't support SAML authentication. Creating and regularly rotating database credentials for all users was inefficient but necessary.

To help them overcome this challenge, Cyral integrated with Cedar's Okta identity management instance to enable users to access data with their secure Okta credentials—not their database credentials. This allows for access governance at the granularity of Okta groups that map to the various database user personas (integration engineer, support engineer, data scientist), and the increased security associated with Okta's authentication policies.

The logs show which Okta user has accessed each piece of data and centralized controls, alerts, and data access logging helps Cedar easily review access certifications and demonstrate compliance. Every policy and permission change is tracked in version control, and every access to a particular set of data is tracked in centralized logs.

Enhanced security control and monitoring to protect PII against exfiltration

Cedar needed even more robust alerting and blocking capabilities to support the security team in case of potential attempts to exfiltrate sensitive information. Cedar already encrypts personally identifiable information (PII) at the application layer and in its data storage repositories, but monitoring all data interactions remained a top priority. With these initiatives in mind, Cedar needed to apply consistent security postures to data types at the same sensitivity level, regardless of how they're accessed, which engineering team is responsible for the data, or which client the data came from.

Cyral Enables Consistent Data Activity Monitoring

With Cyral, Cedar was able to gain consistency across all types of data endpoints: repositories, pipelines, and warehouses. Data access and monitoring policies span all data storage locations and are keyed to the actual data being protected, rather than its location. Data flowing into Cedar's environment goes through multiple stages and locations before being normalized and mapped against the production system. Cyral makes it easy to monitor sensitive data as it flows through the system. Cyral's universal access policies mean access rules for an email address or a SSN are the same, no matter where in the process the data is. Cedar now has consistent data activity monitoring for all data and users with high- confidence audit logs that provide rich context for every data access event.

About Cyral

Cyral simplifies security and governance for databases and data lakes. The cloud-native service is built on a stateless interception technology that enables consistent visibility, access control and authorization. Cyral enables DevOps and Security teams to automate their data security management workflows and prevent data theft.