

How **Cyera** is Powering Carmoola's Next Phase of Data Security Innovation



Carmoola is redefining the car-buying experience, providing instant budget approval and flexible car loan management—all through an easy-to-use mobile application that has best-in-class customer satisfaction with a sector-leading net promoter score of +92. As a result, Carmoola handles vast amounts of sensitive information, from financial records to personal data, which is why the company is committed to leading the way in data security.

Carmoola partnered with Cyera to advance its existing security program with enhanced data visibility, AI-powered classification, and greater controls across its data ecosystem.

Balancing Security Innovation with Scalability

Carmoola's Head of Infrastructure, Dmytro Shamenko, faced a challenge familiar to data security practitioners: ensuring security processes could scale with the company's expanding client base and increasing data volume.

“We wanted to answer critical questions like: What data do we have? How is it classified? Where is it stored? And who has access to it?” Dmytro explains.

The primary goal was to automate Carmoola's data registry, providing a comprehensive view of sensitive assets across the organization. This registry would encompass employee data, analytics, application data, and user uploads—critical assets that, if left unidentified or unprotected, could pose significant business risks.

Carmoola also sought to implement a robust data classification system, one that would empower the compliance team to act independently and efficiently. This capability was critical not only for meeting regulatory requirements but also for proactively mitigating risks across platforms like Google Workspace, AWS, and Snowflake.



Why Cyera Was the Right Choice

Cyera emerged as the solution that aligned best with Carmoola's vision. Its ability to automate data discovery and classification across multiple environments—including AWS, Snowflake, and Google Workspace—immediately set it apart.

“Cyera immediately [met] our requirements, like all of them in one,” says Shamenko.

“It addressed our need for data registry, classification, and identifying issues with improper data placement.”

Moreover, the “smooth” integration with AWS services made Cyera an ideal fit. Carmoola leverages a variety of AWS services, including Aurora for database management, EC2 for tasks involving data handling, and S3 for object storage. Cyera connects to AWS via native APIs to scan and discover data at scale. Through the use of AI, the platform quickly classifies data housed within AWS services with 95%+ precision—whether it's structured, semi-structured, or unstructured. Additionally, Cyera provides critical context about data within AWS and other data sources, including what it entails, its sensitivity, where it resides, how it's protected, who has access to it, and if it violates known compliance frameworks. The implementation process to begin discovering and classifying data can take as little as five minutes.



Rapid Deployment, Immediate Insights, Empowered Teams

Cyera provided immediate visibility into Carmoola's data estate, identifying key areas of risk and enabling the team to address and monitor for misconfigurations and overexposed data. This complemented AWS's native security features, offering a new layer of protection.

"We configured everything in one day, then it took about two days for scanning. By the end of the scanning, we already analyzed and classified all data."

Another significant impact of Cyera's platform was the newfound independence of Carmoola's compliance team. Gathering evidence for compliance was burdensome and resource intensive.

"Now, they can independently find answers, eliminating bottlenecks for the entire team," Dmytro notes. This shift not only improved operational efficiency but also allowed the infrastructure team to focus on other strategic priorities.

Reducing Data Security Risk at Scale

Additionally, Cyera's visibility into data enhanced Carmoola's ability to maintain strict control over platforms like Google Workspace, where the sheer volume of data-sharing activities requires constant oversight. As part of Carmoola's proactive approach to data security, the company sought to identify and manage sensitive files more efficiently, ensuring they were properly stored, classified, and accessed only by authorized personnel.

Cyera's platform enabled Carmoola to identify overexposed files, classify them according to sensitivity, and flag instances of excessive access or improper sharing. This newfound visibility allowed the team to proactively address potential risks by either restricting access, deleting unnecessary files, or educating employees on secure data-sharing practices.

By uncovering these issues, Cyera reduced Carmoola's data attack surface, helping to maintain customer trust and meeting strict regulatory requirements.



Leading the Way in Data Security



Carmoola's partnership with Cyera has positioned it as a leader in data security innovation. The company has not only improved its data protection but also strengthened trust with its customers by demonstrating a proactive approach to compliance and risk management.

Looking ahead, Carmoola plans to expand its use of Cyera's AI-powered data loss prevention capabilities, ensuring they remain ahead of the curve.

“We wanted a platform that could automate the hard stuff, provide the visibility we needed, and let us focus on delivering value to our customers. Cyera has done that and more.”

By adopting Cyera, Carmoola enhanced its ability to manage and secure sensitive data across a complex environment, empowering teams to operate more efficiently and ensuring that trust and security remain at the core of its mission.

