cyera

Case Study

Out of the Dark: How Patelco Credit Union Turned Data Governance From Theory Into Action

Patelco Credit Union had already built strong data governance, with clear policies and controls in place. The piece the team wanted next was visibility: a true view of where its sensitive data lived and how concentrated the risk was. The controls were still manual and inconsistent, leaving that picture incomplete.

Before Cyera, says Bhavani Palukuri, Vice President Enterprise Architecture & AI Innovation at Patelco, "it was all dark data." That was especially true of unstructured data such as documents, since structured data in systems like Snowflake already had stronger controls. The governance was solid, but the team needed to see what lay beneath it, particularly across those unstructured sources. "We don't know where our sensitive data is, how concentrated they are."

For a team responsible for identifying, classifying, protecting, and enforcing controls on sensitive data across the enterprise, that blind spot was the whole problem. As Palukuri puts it, the “biggest gap is the data visibility.”

Patelco is an Azure shop, with on-premise tools and applications alongside the cloud. For Palukuri, any data protection capability had to live inside that architecture rather than run as a parallel system. “Integrating natively within our existing architecture is very important for us,” he says.

The Gap Between Policy and Practice

Patelco had data governance policies and controls in place, but they were manual and inconsistent, with no automated visibility into where sensitive data resided or how concentrated the risk was. The framework existed in theory, but the unstructured data underneath was dark.

An Enabling Layer, Built Into the Architecture

Rather than add another standalone tool, Patelco made Cyera the foundational layer for finding and classifying sensitive data inside its existing stack. “Foundationally, Cyera is an enabling tool,” Palukuri describes, and the team uses it to identify sensitive data across its Azure and on-premises environments.

From there, enforcement runs through the systems Patelco already operates. The team applies data protection controls through Microsoft Purview and drives incident response through Jira playbooks. Cyera surfaces the sensitive data and the risk. Patelco’s existing tools act on it.

Governance You Can Execute

The shift Palukuri describes is not about owning one more product. It is about turning governance from a document into something the team can act on:

"Data protection maturity is not just about adding one more tool, it's about enabling execution of the governance... Otherwise, this just becomes a theoretical work."

The Results: From Dark, Unstructured Data to Action

Since deploying Cyera, the change at Patelco is evident in how the team handles and reports risk.

Risk reduced with focus	"We are a lot more confident and more focused on how we reduce our risk," now that the team can see where high-risk sensitive data is concentrated.
Audit readiness	The team is "ready for many regulated audits," with a more focused compliance posture than before.
Leadership visibility	Palukuri can now report "where our concentrated risks are, what are we doing and how the maturity is progressing."
Executable governance	Visibility into sensitive data lets the team enforce its governance, not just define it.

For Palukuri, that is the real measure of maturity. Strong policies were never the issue. Acting on them was. With sensitive data finally visible, Patelco can govern in practice, not just on paper. He also sees the next frontier taking shape, pointing to agent security as the area data protection leaders will need to watch.

"Especially with Cyera, we can get a visibility into the data and we can make actionable outcomes out of it," he says. That, more than any single tool, is what brought Patelco's unstructured data out of the dark.