cyera

Case Study

How a Global Technology Company Gained Accuracy, Confidence, and Control Over Sensitive Data

"What made the difference with Cyera comes down to one word: accuracy. I knew beyond any reasonable doubt that what the tool was telling me was accurate." - Security leader at a global technology company

The Innovation Tension

A global technology company operates at the intersection of high-speed development and strict regulation. As a builder of low-code, fast-to-market solutions for customers in regulated industries, the organization faces a unique tension: the need to innovate quickly while helping clients navigate a complex web of global data privacy and security laws.

While the organization knew they had sensitive data, they lacked the clarity needed to manage it effectively. The team generally knew where some data lived, but could not determine the specific sensitivity of each dataset, the risks involved, or how to prioritize security actions without slowing innovation. Manual classification was impossible at their scale. As one security leader at the company put it: "I was lucky I even knew where my sensitive data was. What I needed was help identifying the level of sensitivity... and mapping it to a risk taxonomy."

The Barriers to Progress

Before Cyera, the company relied on legacy Data Loss Prevention (DLP) tools that didn't fit modern demands. These tools lacked deep content visibility, forcing the security team to use restrictive policies and limited innovation that became a bottleneck for the business.

Lack of confidence in their data affected their security maturity. Without certainty, they could not safely implement high-impact controls like data retention, destruction, or modern DLP. They were caught in a reactive cycle, managing a global customer base across regions with different compliance rules, without a clear way to trust what they were seeing.

A Mindset Shift in Data Discovery

The decision to partner with Cyera was more than a tool swap; it was a fundamental mindset change. The onboarding process required minimal effort and energy from the team, allowing them to move quickly from evaluation to active operations.

The impact was felt almost instantly. Cyera's AI-driven scanning began validating months of the team's internal, manual mapping work across all business lines. It acted as a powerful verification layer that checked their assumptions and highlighted hidden risks. Reflecting on this phase, the security leader noted: "It actually confirmed all of the many months of research and collaboration... and validated that immediately."

Turning Accuracy into Action

The true differentiator was accuracy. In a field where false positives can lead to dangerous errors, the team finally found a source of truth they could rely on. “What made the difference was accuracy," the security leader explained. "I could know beyond any reasonable doubt that what the tool was telling me was correct.”

This accuracy reshaped their workflow. With the confidence provided by Cyera, the team moved away from rigid, location-based DLP rules to context-aware policies based on the data. This clarity allowed them to execute high-impact strategies like data retention and destruction safely. These policies are easy to get wrong, but with Cyera, the team could make decisions knowing they were not mishandling sensitive information or deleting critical assets.

The Results: A Mature, Proactive Program

By the end of the implementation, the organization had transformed its security posture. They moved from a manual, reactive state to a proactive governance model that serves as a force multiplier for their lean team.

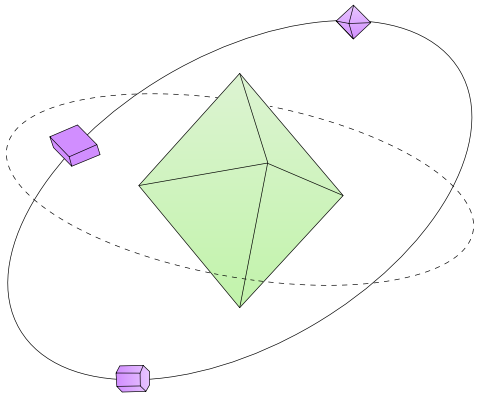
The achievements were measurable:

- **Operational Velocity:** Innovation accelerated as DLP became a facilitator rather than a bottleneck.
- **Risk Reduction:** The team implemented safe data destruction, which also resulted in storage cost savings.
- **Proactive Auditing:** They launched external-access security audits to identify and secure high-risk identities.
- **Continuous Growth:** The partnership evolved alongside the business, with the security leader stating: “I’ve never had another SaaS provider that listened to every piece of feedback and delivered every feature... I have grown measurably and the platform has grown measurably in this partnership.”

Ultimately, Cyera gave the organization the “absolute confidence and knowledge” about the state of their sensitive data, proving that in data security, accuracy is what turns answers into action.

“With accuracy, I can focus exclusively in automation and remediation.”

- Security leader at a global technology company



Explore What's Possible Data security leaders do not need more alerts. They need better answers. And accuracy is what turns answers into action. See how teams gain clarity, confidence, and control.

Book a demo →