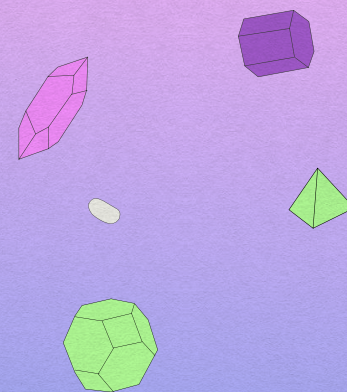


From Invisible Data Risks to Automated Action: How A Canadian Financial Institution Built Unified Visibility and Remediation



“Data governance is one of the anchor points of our data and AI strategy. Protecting data and ensuring the right people have the right access at the right time is key to maintaining trust.” - a Principal Product Owner at Financial Institution

As a financial institution in a complex regulatory environment, the organization treats data governance as foundational. It is essential not just for security but also for enabling data and AI initiatives across the organization.

But even with strong controls, invisible risks remained. Legacy data shared years ago, outdated access permissions, and orphaned content from departed teams quietly expanded the organization’s attack surface without clear ownership or visibility.

The Challenge: Unknown unknowns and unmanaged data risk

The company’s data loss prevention program relied on native tools that used regex, custom scripts, and manual processes. This made it hard to scale data protection across the business.

Several challenges stood out:

<p>Invisible risks had become normalized.</p>	<p>Sensitive data remained accessible to former contractors and in files owned by teams that no longer existed, without anyone’s awareness.</p>
<p>Limited visibility into unstructured data.</p>	<p>While structured data was manageable, unstructured data scattered across Box, Google Workspace, and cloud platforms introduced risks that remained hidden from the team.</p>
<p>DLP coverage was narrow.</p>	<p>Out of hundreds of sensitive data points, only a handful could be effectively monitored.</p>
<p>Remediation was manual and fragmented.</p>	<p>Even when issues surfaced, tracking and resolving them across teams and tools took a long time.</p>

“One of the most common issues we experience is the unknown unknowns and invisible risks - risks that have just become part of the ecosystem.”

- a Principal Product Owner at Financial Institution

As a Data-Driven Financial Institution, the team needed a way to bring hidden risks to light, understand them in context, and respond quickly without increasing operational burden.

The Solution: Automated discovery, unified visibility, and integrated remediation

This Canadian financial institution needed a way to see and organize its data across platforms. They chose Cyera to help bring structure to their security and governance work.

Broad, low-friction visibility

Cyera connected to the company's main platforms, including Box, Google Workspace, Google Cloud, and, later, NetApp. This made it possible to see both structured and unstructured data together, without switching tools.

“The fact that it tied in so well meant that not just structured data, but unstructured data became visible to us in ways we didn't know existed.” - Principal Product Owner, at the Canadian Financial Institution

This approach surfaced risks that were previously hard to spot, like files created by business users or teams working outside standard governance processes.

Seeing value almost immediately

The team saw results quickly after onboarding. The first scans revealed uncontrolled sharing that put PII at risk. Issues were discovered and resolved almost immediately. Within a week of scanning Google Workspace, the team could show clear results to leadership.

“We discovered uncontrolled sharing that put PII at risk, and we managed it instantly.” - Principal Product Owner, at the Canadian financial institution

Turning insight into action

Cyera is more than a discovery tool; it integrates with the company's workflows, enabling the team to act on their findings.

By linking with Jira, the team could automatically track remediation work as issues were found. Adding identity context clarified who had access and why, so decisions about permissions were based on real data. The team also included these findings in their regular reporting and assurance routines, keeping the process familiar and efficient.

“This allows us to automate our remediation workflows and track everything in one place.” - Principal Product Owner, at the Canadian financial institution



The Results: Clear security improvements and greater governance confidence

The team was able to identify and address previously invisible data risks more quickly and efficiently.

1. Better classification:

By classifying data at scale, Cyera surfaced hundreds of previously unknown data types.

“I have never seen data classification at scale like Cyera’s.” - Principal Product Owner, at the Canadian financial institution

2. Smarter retention and disposition

By gaining a clearer view of their data landscape, the team moved from reactive management to proactive strategy. Implementing custom data classes lets the team pinpoint transitory content that had been hidden in the noise. With this visibility, teams no longer had to guess what to keep. They could confidently purge outdated files, shrinking the bank’s digital footprint while lowering storage costs and security risks.

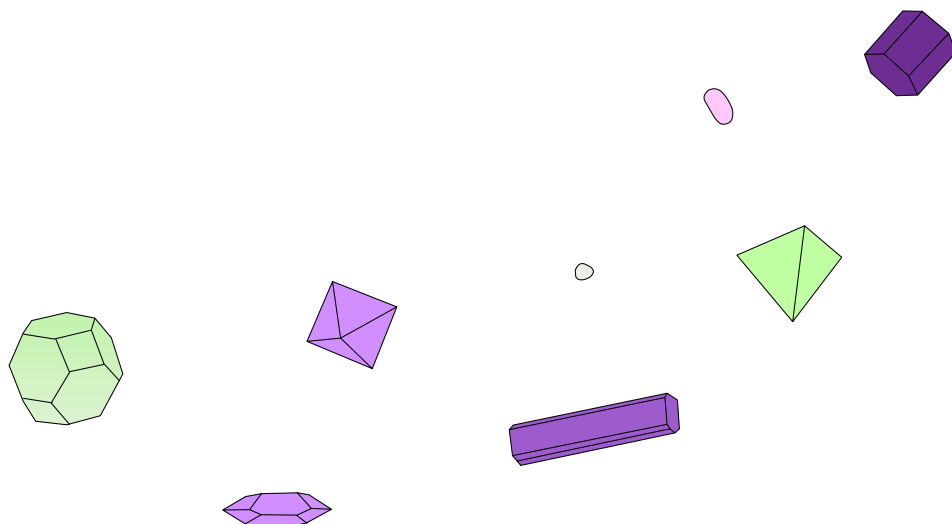
“Every time you remove a file from the network, it reduces risk and reduces cost.” - Principal Product Owner, at the Canadian financial institution

3. Faster progress toward regulatory compliance

“That gets us much further along the pathway for regulatory compliance.” - Principal Product Owner, at the Canadian Financial Institution

The implementation of Cyera accelerated this Canadian financial Institution’s regulatory roadmap. By transforming dark data into discoverable, classified assets, the team gained the visibility needed to quickly meet stringent compliance standards. This clarity enabled a shift from reactive monitoring to proactive defense, especially through targeted external access reviews of high-risk identities.

“Every team we’ve demonstrated it to is excited to see what they can do with the tool.” - a Principal Product Owner at Financial Institution



Why The Canadian Financial Institution Chose Cyera

This company chose Cyera not just for its technology but also for its approach:

Uncovering hidden risks that once flew under the radar

Reliable, precise classification they could count on every time

Seamless automation that blended effortlessly with their daily operations

A product team that listened and delivered requested capabilities

A platform designed to grow and evolve alongside their organization

“Cyera is the tool that allows you to say: it doesn’t have to be this way.”

- Principal Product Owner, at the Canadian financial institution

Explore What's Possible with Cyera

Unseen risks do not fade away; they quietly multiply until addressed.

Book a demo and discover how organizations like this transform hidden data threats into clarity and confident action.

Book a demo 

