Lightbeam

Invisible

DSPM on Google Cloud

Hypergrowth AI Company Ensures Data Security at Scale

Case Study | Customer Story

Overview

Invisible Technologies is a fast growing AI software company, recently recognized as the second fastest growing AI startup in the United States.

By combining automation with a global human workforce, Invisible helps enterprises scale complex workflows. As its data footprint expanded rapidly across cloud systems, the company prioritized precise, responsible data security to safeguard sensitive information and support safe AI driven operations.

Customer Story Summary

Challenges

- Needed accurate real-time visibility into sensitive data across Google Workspace, Slack, and structured data stores
- Wanted a DSPM platform that operated entirely in their own Google Cloud environment
- Required insight into sensitive data access that affects AI usage and IP protection
- Sought a partner who could support current needs and long term governance vision

Approach

- Deployed Lightbeam in Google Cloud in under two hours
- Connected Google Workspace, Slack and structured data systems for continuous DSPM
- Applied Lightbeam's identity driven discovery to improve accuracy across unstructured content
- Used the platform as a critical tool for access governance, retention policies, and AI data controls

Results

- High accuracy in scanning and classification across collaboration platforms
- Immediate insight into potentially targeted and sensitive data sets
- Strengthened controls for AI model training and internal data handling
- Significant gains in privacy operations efficiency to reduce manual effort

Challenge

The Invisible security team wanted a single tool to easily catalogue sensitive data stored across their environment and how it was accessed between employees, workflows, and AI tools.

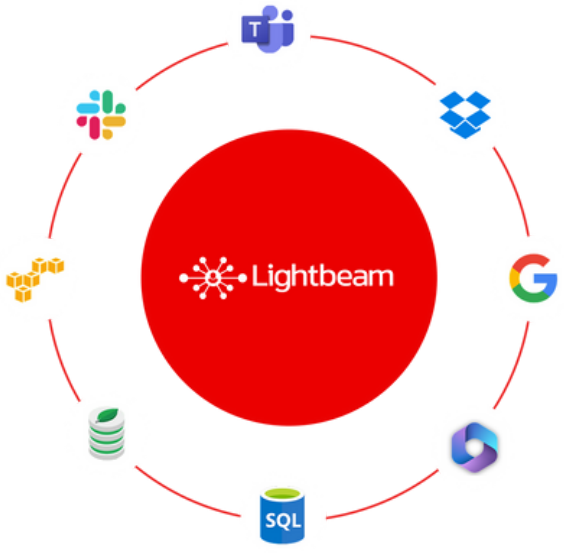
Traditional approaches struggled with the volume and variety of unstructured content in Google Workspace and Slack. The company wanted simplicity, accuracy they could trust, the ability to keep all scanning inside their own Google Cloud environment, and a foundation aligned with their desired governance practices.

> *"It was very important for us to easily see in real-time where our sensitive data was and make sure it stayed in the right places, especially as we expanded our use of AI."*
> *-**Patrick McKinney, Vice President Security, Invisible***

How Invisible Evaluated DSPM Vendors

Invisible conducted a structured RFP with a weighted scorecard to evaluate four DSPM platforms.

The goal was to measure each solution's accuracy, deployment model, partnership approach, and alignment with the company's operational and AI governance needs. They wanted a tool that was easy to use, respected their cloud architecture, and demonstrated high precision in both structured and unstructured environments.



DSPM Evaluation Criteria

Invisible aligned its selection criteria with modern DSPM evaluation frameworks focused on accuracy, identity context, deployment flexibility, and the potential for real remediation.

Criteria Table included some of the below:

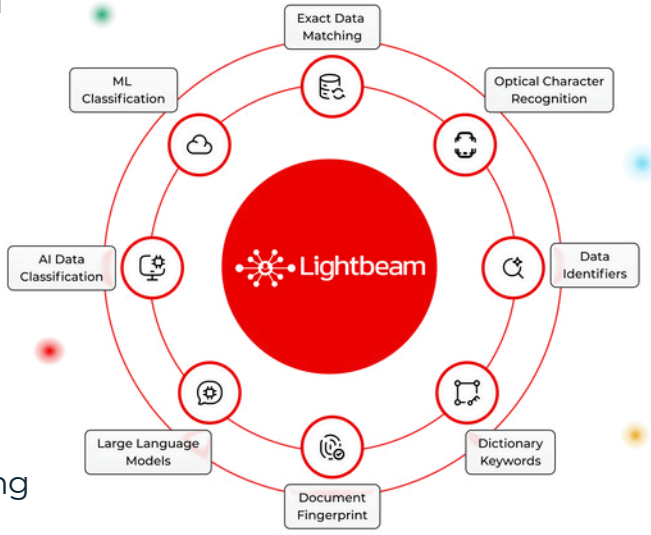
- **Deployment Flexibility and Data Residency:** Scanning needed to stay inside GCP.
- **Classification Accuracy for Unstructured Data:** Required for IP protection and AI governance.
- **Full Content Inspection:** Necessary for dependable results.
- **Identity and Access Context:** Enabled better governance decisions.
- **Integration Fit with Google Workspace and Slack:** Essential for collaboration workflows.
- **Ease of Use and Operational Overhead:** Needed to simplify daily work.
- **Automated or Assisted Remediation:** Important for future enforcement.
- **Vendor Partnership and Responsiveness:** Critical for long term alignment.
- **Cost to Value Ratio and Clear ROI:** Needed measurable benefits quickly.

> *"Unstructured data is one of those things in the DSPM space which isn't easy to get right all the time. With structured data in a database it's very easy... Unstructured data, images, PDFs and all that sort of stuff... being able to scan the plethora of data we have in there, it was actually smooth"*
>
> ***-Patrick McKinney, Vice President Security, Invisible***

Solution

After completing the evaluation, Invisible selected Lightbeam for its identity-centric architecture, accuracy in unstructured data classification, and support for full deployment inside their own cloud infrastructure.

The platform was installed and operational within an hour, and full scanning began shortly after. Once connected to Google Workspace, Slack, and other systems, Lightbeam provided immediate clarity into where sensitive data lived, how it was being accessed, and which areas represented the highest levels of risk.



Deployment in Google Cloud Platform

Because Invisible operates primarily in Google Cloud Platform, the team wanted a DSPM platform that deployed natively in their own cloud tenant without moving data externally.

Lightbeam provided a fully in tenant deployment model that kept all scanning and analysis inside Invisible's environment. The team could scale compute resources dynamically. Large classification jobs could use additional computing resources to scan terabytes quickly, while ongoing maintenance scans used minimal resources. This elasticity matched Invisible's cloud operating model. Purchasing Lightbeam through Google Cloud Marketplace also allowed Invisible to use existing GCP committed spend, simplifying procurement and budgeting.

> *"Deploying Lightbeam in Google Cloud was simple. The data stayed in our environment, and the ability to scale compute and buy through Google Cloud Marketplace made it easy to fit into our budgeting model."*
>
> ***-Patrick McKinney, Vice President Security, Invisible***

Results

Lightbeam formed an important part of Invisible's strong and reliable foundation for data security. The platform immediately provided real time data on where sensitive data lived across Google Workspace, Slack, and other core systems.

This clarity helped the security organization pinpoint patterns, locate exposure points, and highlight high-risk data concentrations that were previously hard to detect efficiently. The platform delivered high accuracy in full-content classification, which gave the team confidence to use the results for broader governance work. With a dependable baseline, the team began improving access controls, shaping retention policies, and reinforcing safeguards that keep sensitive information out of AI model workflows.

The shift from manual discovery to automated DSPM created major efficiency gains. The team cut the effort required for privacy requests by an estimated 80 to 90 percent, which allowed them to redirect time toward higher-value improvements. The platform also gave the team a unified view of data and access, which supported least privilege evaluations and helped tighten access controls across the environment.

The system delivered value immediately by surfacing data concentrations that required attention. With strong vendor support and a deployment model that fit naturally into Google Cloud, the security team strengthened its data security program while continuing to scale a rapidly growing business.

> *"The accuracy was dead on. Lightbeam showed us where our sensitive data was right away, and the ROI came very quickly."*
>
> *-**Patrick McKinney, Vice President Security, Invisible***

Future Plans

Invisible plans to expand Lightbeam into additional data systems such as Postgres and Databricks, build out access governance workflows, and enforce retention and minimization policies. They also plan to push Lightbeam labels back into Google Drive to support downstream controls and reinforce their responsible AI program.

> *"We see Lightbeam becoming the first lens we use to understand all of our data as we continue to grow."*
>
> *-**Patrick McKinney, Vice President Security, Invisible***

Lightbeam

About Lightbeam

Lightbeam is an identity-centric data security platform that reduces breach risks, ransomware costs, and regulatory penalties by unifying DSPM, privacy, and governance. Using patented Data Identity Graph technology, it discovers and maps sensitive data—including shadow data—across structured, unstructured, and semi-structured sources, enabling precise governance, automated privacy workflows, and enhanced data security. For any questions or suggestions, please contact us at: sales@lightbeam.ai or visit us at https://lightbeam.ai

GET A DEMO