Canopy

CASE STUDY

Review Provider Saves Client Over $300,000 on Data Breach Response

OVERVIEW

This Canopy partner is a Data Breach Response group that's focused on helping clients meet the numerous obligations for new and ever-changing privacy laws across all jurisdictions. Its global roster of vetted data breach analysts ensures they can quickly scale to any size project and conduct the necessary review and extraction of sensitive information.

A company in the Insurance sector experienced a data breach on a company file share, potentially compromising 440 GB of data (one million documents). They enlisted this partner's managed review services.

SOLUTION

Instead of leaning on traditional data mining methods like keyword searching, regular expressions (regex), and pattern matching, the team lead chose Canopy's Data Breach Response software. Canopy's purpose-built AI algorithms processed the data, detected PII with precision, and sped up the team's review workflows.

RESULTS

Within 24 hours of uploading the 440 GB data set, the team had an Impact Assessment Report summarizing Canopy's PII findings and recommending a prioritized review. They reviewed the data set nearly four times faster than with alternate methods, saving their client over $300,000.

Canopy

When a company in the Insurance sector experienced a data breach on a company file share, potentially compromising one million documents, they enlisted a Canopy Partner's managed review services.

Speed is a critical factor in data breach response, where deadlines are non-negotiable. Regulations like the California Consumer Privacy Act (CCPA) mandate breach notification to authorities and affected individuals within strict timeframes. Slow processes and tools not only increase regulatory risk exposure, but can also severely increase budgets, causing breached companies or their cyber insurers to bear exorbitant costs.

Yet, many breach response teams still rely on tools and techniques from parallel industries, resulting in slow and expensive services. Challenging convention, this managed review provider chose Canopy's Data Breach Response to deliver quality results as quickly as possible.

Set Up Success with AI-Powered Data Mining

When approaching a potential data compromise, the first step is to locate the personally identifiable information (PII) present in that data and flag those documents for further review.

In the past, the review provider's Data Breach Response group would have accomplished this via keyword searching, regular expressions (regex), and pattern matching — processes that can be more time-consuming and challenging for quickly zeroing in on PII.

Conversely, Canopy's advanced, AI-powered PII detection algorithms are purpose-built and continuously trained to find names, social security numbers, addresses, financial information, medical data, and dozens of other PII categories. Within 24 hours of uploading the 440 GB data set, the review provider had an Impact Assessment Report summarizing Canopy's PII findings and recommending a prioritized review. The project leads were able to filter the sensitive documents by PII type and density, allowing them to explore the scope of the compromise before beginning review.

Incident or Breach? Find Out Fast

440 GB
size of data set

1 million
documents

Day 1
automatic PII report

Canopy

"Canopy gave us the exact level of detail we needed to gauge the scope of this project," said a Senior Director. "We could immediately see what types of PII existed, how much there was, where the PII was located, and the exact context in which it occurred."

Canopy's Data Breach Response software didn't just significantly reduce manual data mining efforts; its upfront PII discovery also honed the team's focus, saving valuable review time.

Review the Right Files Faster

With Canopy, the team only needed to review about 70,000 documents — 15% of the data set after deduplication — in two different review groups:

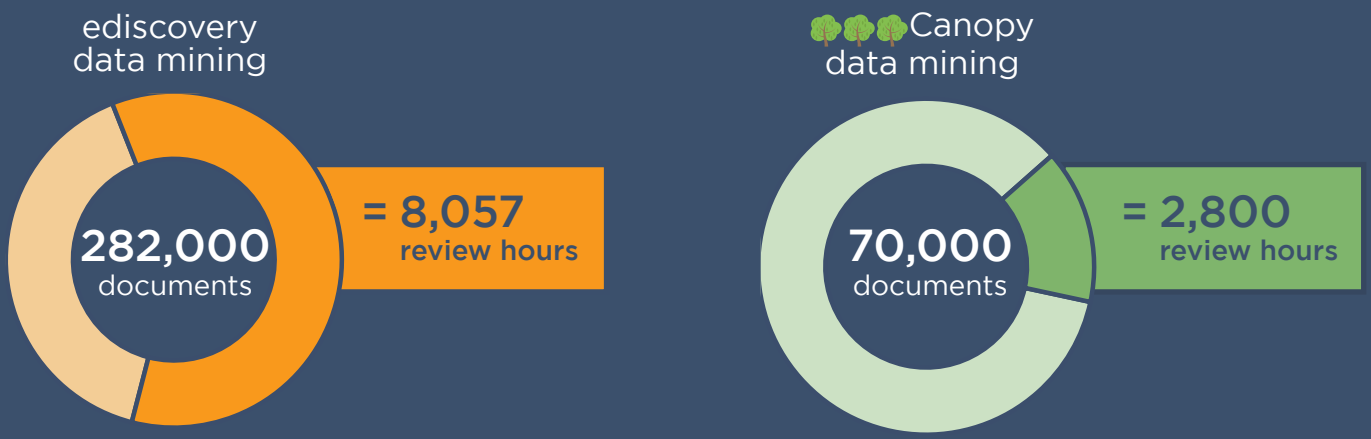
- **Flagged for PII Review:** Layering Canopy's PII detection with client-business & data insight, they prioritized a review of 69,000 documents by file type (e.g., Excel spreadsheets) or potential PII type.
- **Representative Sample:** They performed statistically significant sampling or an accelerated PII review of roughly 1,000 documents to validate Canopy's accuracy and confirm the defensibility of the approach.

> "If we were handling this project using traditional methods, we would have needlessly reviewed 4x as many documents to find the same amount of PII."
>
> **Senior Director, Co-Lead**
> of Canopy Partner's Data Breach Response Group

Other managed review providers not using the latest purpose-built technology would need to review significantly more documents due to overinclusive data mining via search terms, regex, and/or pattern matching.

In fact, team leads estimated that with alternative data mining methods, they would have reviewed closer to 60% of the original data set. At an

More Documents = Longer PII Review



Canopy

average review rate of 35 documents per person per hour, this would waste critical time and resources, increasing the project budget significantly and making it more challenging for the breached company to meet mandated notification deadlines.

"We were very impressed by the accuracy of Canopy's PII detection. The software did a lot of the work for us upfront," said the Senior Director, Co-Lead. "If we were handling this project using traditional methods, we would have needlessly reviewed four times as many documents to find the same amount of PII."

> "Canopy's PII detection alone saved us thousands of review hours. Not only were we looking at less stuff, but we were looking at the right stuff."
>
> **Managing Director, Co-Lead**
> of Canopy Partner's Data Breach Response Group

Further, upon evaluating the documents that Canopy had flagged for review, the team found that approximately 80% of them did in fact contain reportable PII. Comparatively, their prior experience was the opposite — with alternative breached document review tools, typically only about 20-30% of reviewed documents actually contained PII.

"Canopy's PII detection alone saved us thousands of review hours. Not only were we looking at less stuff, but we were looking at the right stuff," said the Managing Director, Co-Lead.

Efficiencies that Lead to Faster, Less Costly Results

In addition to narrowing their focus to the sensitive documents upfront, the team leads used Canopy's time-saving features to further speed up their review and entity resolution. They were able to:

- Complete an accelerated review of 84,767 thumbnails in just two days.
- Review Excel spreadsheets in minutes rather than days, including front-loading spreadsheets of entities to speed up the subsequent review & entity resolution.
- Complete entity resolution in 1 week with Canopy, compared to an estimated one month using alternative methods like SQL and Excel.

By choosing Canopy's purpose-built Data Breach Response software over traditional tools and processes used to address data security incidents, this review provider is blazing a new trail among breached document review teams.

"Thanks to Canopy's Data Breach Response software, we saved our client over $300,000 on this review," said the Managing Director, Co-Lead. "Its PII detection, PII review efficiencies, and streamlined entity deduplication cut weeks off our traditional timeline, enabling us to deliver high-quality services faster and in a more cost-effective way."