PINPOINT LABS

ELLWOOD EVIDENCE SAVES MORE THAN $200K WHILE ELEVATING COMPLIANCE CAPABILITIES WITH PINPOINT LABS' HARVESTER

Overview

Ellwood Evidence is a Canadian forensics and eDiscovery firm focusing on civil and criminal litigation. William Ellwood, their Forensic Lead and CISO, has an extensive background with forensics software training that led him to build a highly technical, hands-on team. They take a different approach to eDiscovery – when something looks amiss, they're willing and able to dive in, uncover any errors, and implement technical solutions. So when a new client came with an active risk, Ellwood knew their typical tools wouldn't provide the necessary answers. With Harvester, they discovered a highly flexible yet polished product that could be configured to a custom solution.

Their client was involved in an open-ended incident response, investigating a case of intentional data manipulation and possible data loss. While most compliance tools will monitor and flag malicious activity, none were capable of monitoring a database of this size – between 300 and 400 terabytes spanning 40 machines, each containing anywhere from 500 gigabytes to more than 70 terabytes of data. Due to the client's highly regulated industry and the ongoing compliance risk, it was crucial for Ellwood to isolate and contain the problem as quickly as possible.

To begin the assessment phase, agents were deployed in three days and fully online within the following week. Despite the performance limitations of the client machines, Harvester was able to process roughly 40 gigs per hour and quickly determine the extent of the damage. Only 8.7 terabytes were affected, giving Ellwood and their client a much more manageable amount of data.

> **Many of the previous tools that we evaluated or previously knew about didn't have the configurability or granularity that we needed to do either a search in place or a data assessment and triage. We found it very useful that we could specify with Harvester that we were only interested in very particular pathways… Because we were able to pause in the data assessment phase, we could deploy the agent, do an initial data assessment, and then query those assessment databases to figure out what the story was, without actually having to copy it back to destination storage.**

The client didn't know the specific search terms to look for, so they didn't want to do any data collection. Instead, they wanted to assess the data that was potentially at risk and then have the ability to search it in the future. Traditional e-discovery systems typically have their own processing and digestion tools and then will conduct the text extraction manually, but Ellwood was able to configure Harvester to only pull from the affected data locations and generate a dtSearch index automatically.

AT A GLANCE

PROBLEMS LEAD US TO OUR SOLUTIONS

- *Ellwood Evidence's client had an ongoing security risk scattered across 300-400 TB of data*
- *No other platforms could assess and triage a database of that size*
- *Harvester was able to identify the affected areas without requiring a full data extraction, saving significant costs*
- *The client can now query everything from their affected database and use it to track and eliminate additional security risks*

ELLWOOD EVIDENCE SAVES MORE THAN $200K WHILE ELEVATING COMPLIANCE CAPABILITIES WITH PINPOINT LABS' HARVESTER

"What we like about Harvester is that it really lets the dtSearch index shine. It was pulling apart email archives and sending those emails one by one to dtSearch for text extraction, giving us a significantly better index quality. We could also actually query the results and see exactly what Harvester found. It's a particularly powerful value add that allowed us to review hits at the individual rows of data instead of just at the file level."

As far as cost, Ellwood says there wasn't any competitor with the same capabilities, especially at the scale this client needed. They estimate that any alternative approach would have cost around $200K more than by using Harvester Enterprise, in terms of inappropriate software licensing from alternatives and/or additional hourly effort. Harvester does not require the entire dataset to be ingested, and licensing is based on agent concurrencies that allow clients to avoid overbuying or inflating project costs.

Ellwood was able to run hundreds of thousands of search terms against the generated indices in a cost effective manner. With a data assessment and index structure from Harvester, the database could then be queried by any means, eliminating the "black box" workflows that typically result from an e-discovery process. Encrypted files were embedded into the database, allowing affected files to be zipped and sent out without having to go back to the target servers.

While the incident response is still ongoing, the client can now run ad hoc searches from the Harvester database as needed, quickly generating results from across terabytes of data. But for Ellwood, they say it's really the support from Pinpoint Labs that has added the most value to their business.

"We can use this tool all over the place. It's not just oriented to enterprise or centralized environments – we can leverage our licenses across both Harvester Enterprise and Portable. So we can prepare something and send it off to a custodian, it'll run on their laptop, they can ship it back to us, and then we can confirm with the logs that everything ran correctly. It allows us to have hands-off, non-invasive but still defensible collections, even at a small scale." They've also started using Harvester's deduping and de-NISTing capabilities, cutting their capture sizes in half.

"Pinpoint Labs is a joy to work with and really, Harvester does what no other e-discovery tool can do. It's approachable for a junior, but also has a high skill ceiling that allows more technical users to make it a truly custom solution."

HARVESTER

- PROCESS OST'S AND PST'S WITH 64-BIT OUTLOOK
- SEARCH AND COLLECT FROM MICROSOFT EXCHANGE, GMAIL, YAHOO, OUTLOOK.COM, AND WEBMAIL VIA IMAP
- REMOTE DISCONNECTION WITH AUTO RESUME
- MULTITHREADED
- EARLY DATA ASSESSMENT REPORTS
- KEYWORD FILTER LOOSE FILES, ATTACHMENTS, ARCHIVES, AND EMAIL
- SEARCH MULTIPLE TIMESTAMPS
- HARVESTER 'ESI' EASY VAULT (CUSTODIAL DRAG AND DROP WINDOW)
- DENIST AND DEDUPE AT POINT OF COLLECTION
- PORTABLE AND SERVER VERSIONS