

## OVERVIEW

Early case assessment (ECA) is the process by which legal teams gather and review electronically stored information at the onset of litigation to determine litigation risks and the estimated costs.

## CHALLENGES

Up to 90% of an organizations data is unstructured

Few tools exist to quickly and easily search unstructured data

Most ECA tools require data to be moved to proprietary systems for analysis

Lack of data insight or technology forces over-collection

Remote workforces, BYOD and satellite offices further complicate efforts

The ECA process has become time consuming and cost prohibitive

## BENEFITS

Search and analyze unstructured data in place, before collection

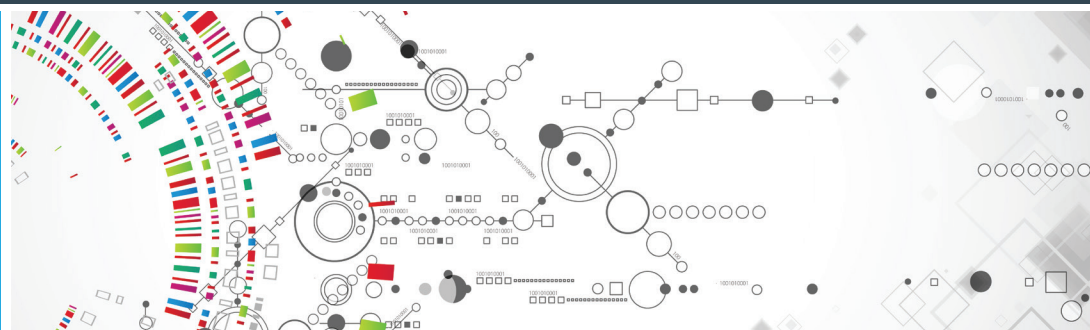
Advanced search quickly finds relevant and important information

Understand risks to make smarter litigation decisions

Filter non-responsive and privileged data at the source for reduced cost

Perform file-level actions such as collect, quarantine or delete

Export search criteria for use in visual analytics programs such as Tableau



## HEUREKA SOLUTION

The Heureka Platform provides real-time access to unstructured data across your enterprise from a single interface, regardless of location. We provide the ability to search and analyze data at the source of creation, without moving a single file to a centralized location.



### ENDPOINT SERVICE

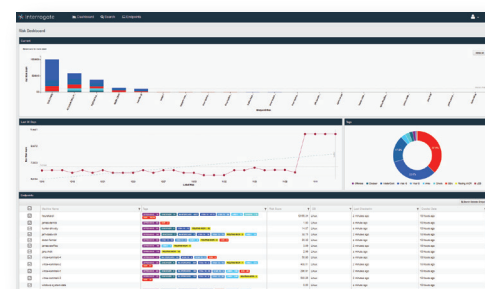
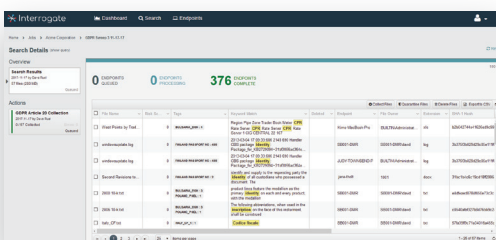
Heureka's intelligent endpoint service creates a full text and metadata index, which is stored locally on each endpoint. The index is updated daily with new or modified data, and happens silently in the background, with minimal impact to end-user productivity.

### CENTRALIZED SEARCH WITH rapID

Heureka's rapID is the heart of the system. It gives you the ability to initiate searches across any number of selected index groups. Search results are returned to rapID for further analysis allowing you to surgically target only responsive data and perform actions such as collect, quarantine, or delete.

## KEY FEATURES

Heureka's risk dashboard displays high-risk endpoints along with the risk types including PII information. Current and 30-day views are instantly available along with user selectable drill-down for information. Endpoints can be selected for file-level detailed searching including keywords, complex queries or regular expressions for specific pattern matches. File-level actions such as collect, quarantine or delete round out the workflow along with export reporting.

File Name	Size	Date	Other Metadata
Report for...	100KB	2017-01-01	...
...	...	...	...

- Single user interface manages all endpoints
- Define and locate sensitive data
- Search and analyze in place, before collecting
- Find documents by keywords, queries, tags or regular expressions
- Collect, quarantine, delete and report
- Auto-classification and/schedule searching
- Extract and collect individual messages from containers (avoid overcollection/overprocessing)