Forcepoint Data Analyzer

Federated Search Across Cyber

Features and Benefits

- Retrieve information from multiple data sources located across jurisdictions with federated search
- Eliminate massive data duplication and facilitate interdepartmental information sharing via a virtual data warehouse
- Enable granularity of access through multi-tiered security
- Minimize the quantity of working data with faceted searching
- Enable analytic teams to focus on analyzing instead of researching and collating
- Visualize and expose patterns in large amounts of data
- Enhance the accuracy and timeliness of intelligence with integrated geospatial, link, and statistical visualizations
- Rapidly identify connections between perpetrators and organizations with automated data discovery
- Discover hot spots for crime and quickly plot and analyze geographic and chronological data
- Recognize a low total cost of ownership with easy deployment and minimal impact on IT infrastructure
- Seamlessly integrate with Forcepoint Cross Domain Solutions
- Alert and notify based on values or thresholds designated as important to an analyst
- Data generated is not proprietary and can be extracted in a number of usable formats to be used by other systems/technologies

The Challenge

The current global security landscape demands that organizations constantly adapt to new situations, make greater use of intelligence, stay current with technology, and expand cooperation between agencies. Today, organizations use tools that enable analysts to quickly access, understand, analyze, react to, and share massive amounts of data across jurisdictions quickly and easily. These information technology investments are enabling agencies to radically reduce cyber threats that impact national security. By providing advanced searching capabilities across vast amounts of information, agencies have access to critical information in seconds instead of what customarily takes days. Searches are returned as actionable results by displaying information as custom reports, link analysis, or geospatial visualizations to ensure comprehensive situational awareness.

Forcepoint Data Analyzer

Forcepoint Data Analyzer's search solution is an agile, adaptable, and scalable federated search and visualization platform that boosts the speed, collaboration and efficacy of investigative and analytical divisions. It provides access to hundreds of sources that an organization deems mission critical and applies automation, advanced data discovery, and visualization capabilities to rapidly deliver key insight to investigations. As individuals set and receive alerts to and from their mobile devices, they are empowered to immediately continue an investigation, regardless of their physical location. The customizable and easy-to-use interface makes complex queries easy to run or schedule, delivering reporting and visualizations to mobile devices and desktops alike. Unique to the industry, the search technology does not need to duplicate data for processing, ensuring low total cost of ownership and truly enabling information sharing, as the ownership of the data stays at the original source (Figure 1).

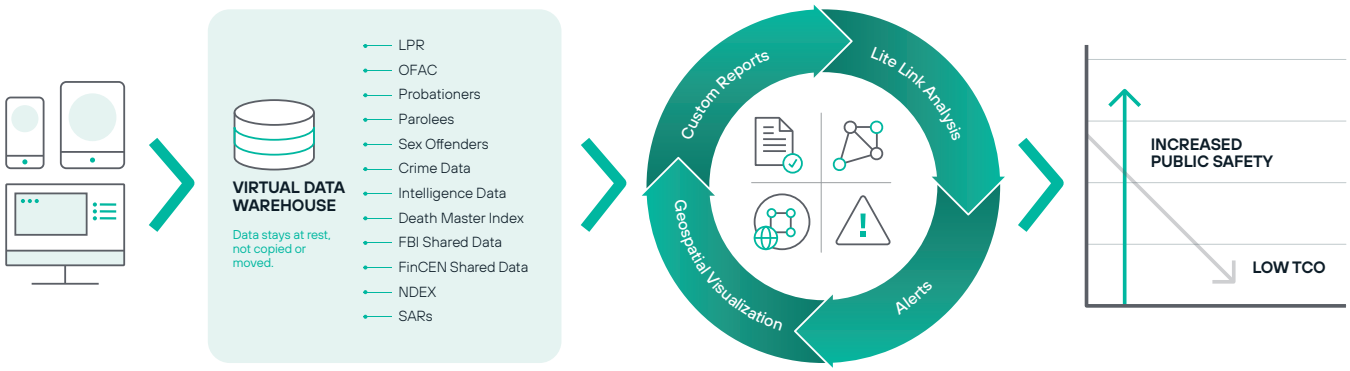
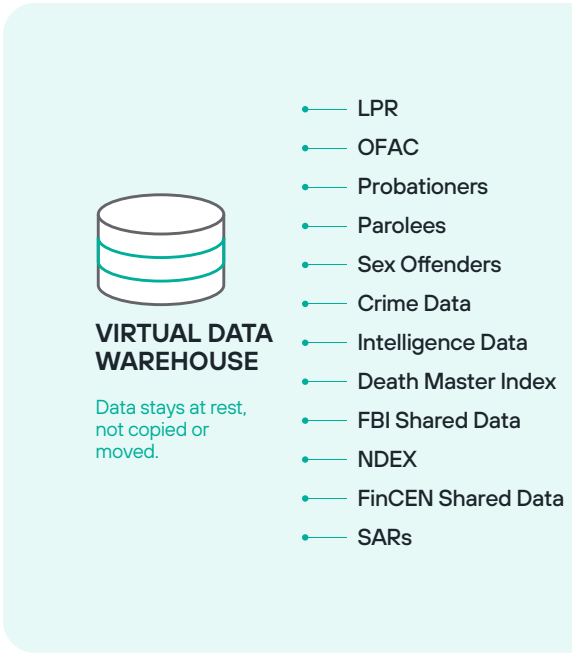


Figure 1: Federated searching across the enterprise coupled with automated discovery tools and lite-analytics supports intelligence-led investigations

Sophisticated & Simple

With decades of experience supporting organizations worldwide, the Forcepoint platform comes with customized templates housing complex algorithms derived specifically in support of strategic intelligence units. Powerful and extensive search algorithms hide behind the friendly facade of an easy-to-use interface, bringing the capability of an advanced analyst to the fingertips of an entry level workforce. In addition to improving the accuracy and speed of a division's output, automating complex human-led processes eases the burden from the loss of subject matter expertise suffered by organizations with high turnover rates.



Federated Searching

Federated searching ensures that analysts have instant access to all data necessary to develop an inclusive picture of a situation. It seamlessly connects any number of local and remote data sources to create the ultimate virtual data warehouse that eliminates data duplication and enables effective information sharing. The time-consuming process of cross jurisdictional and third-party approvals for access to information from multiple agencies is overcome.

Automated Data Discovery

Replace processes that require hours of human-driven big data collection, collation, and correlation of information with automation to reduce the amount of time dedicated to unnecessary investigations.

Scheduled Searches

Substitute time-consuming manual routine searches with scheduled searches and make the platform your near real-time information asset. Scheduling repetitive complex searches takes the burden off the human analyst and allows their focus to remain on efficient actionable intelligence production using the latest information. Custom algorithms derived from decades of experience ensure analysts have the information they need at their fingertips while freeing up the analyst to focus on developing accurate actionable intelligence.

Custom Reporting

Provide researchers with the flexibility and uniqueness that enables them to maximize their work efforts with customized reporting capabilities that can be modified, sorted, prioritized, and scheduled. Arriving to one's shift with reports, run and populated in the optimal fashion that each unique individual needs for maximum performance, allows individuals to hit the ground running upon starting their shift or running new searches while on the road.

Link Analysis

With link analysis visualizations of a search query on your mobile device, analysts can quickly deduce and act on next steps of a situation. Automated data discovery technology quickly unearths relationships between information stored across hundreds of data sources and returns information as actionable intelligence because it visualizes the associations between individuals, events, activities, locations, etc., enabling the analyst to naturally deduce progression of next steps of an investigation.

Geospatial

Geospatial representation of correlated data over time allows the tracking of asset movement or activities in a way that allows analysts to quickly see a change in pattern or behavior. Hot spots of activity or movement enable improved resource prioritization.

Alerting

Today's analysts demand near real-time alerting to their mobile devices in order to take action quickly and easily. In tandem, alerting can be set up for several individuals participating within an investigation for instantaneous collaboration and progression.

Customizable User Interface

Flexibility is provided to create custom dashboards for different roles and users, ensuring that the most relevant data is presented and available. This flexibility also allows the graphical user interface to be tailored to align with an organization's brand, such as color schemes and graphics.

Low Barrier to Entry

Have your platform up and running quickly. Given the system's search architecture, deployments are fast. Organizations with knowledgeable database administrators can receive database deployment training and add sources to the search platform and expand the search capability independent of third-party services.

Forcepoint Data Analyzer can analyze and pull data from data lakes easily and unlike other case management tools, ownership of data remains at the source.

Often moving data from its original source can compromise the validity of the data and in some cases is illegal. With federated search, analysts can query and view data from multi jurisdictions and multiple databases without moving it. The ability to view data at its source also eliminates the need for onsite storage.

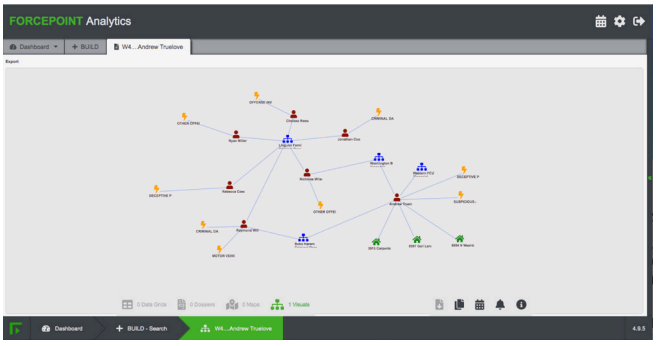


Figure 3: Quickly visualize previously unknown criminal associations on your mobile device.

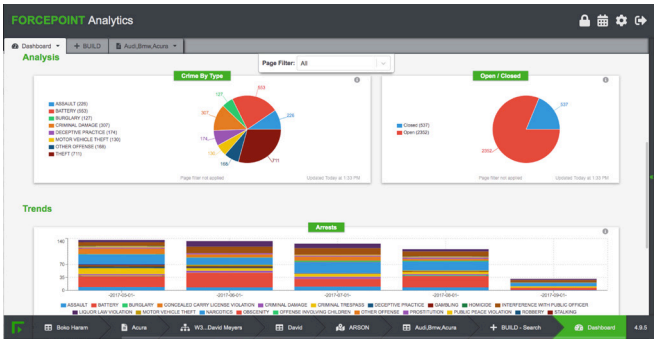


Figure 4: Speed multiple investigations with customized reporting capabilities that can be modified, sorted, prioritized and scheduled.

Figure 5: Delivers the capability of an advanced analyst to the fingertips of an entry level workforce through simple to use icons

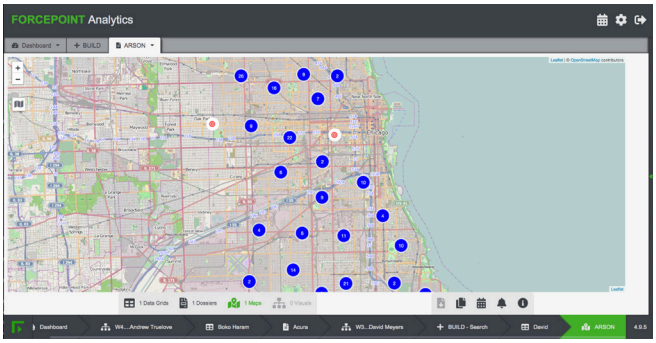


Figure 6: Track of movement of assets or activities to quickly see a change in pattern or behavior.

Search Technology with a Low Total Cost of Ownership

The system resides on top of your existing sources, so there is no need to reformat or restructure your data. This saves you valuable time and money while improving the quality and accuracy of your results.

- → **Circumvent costs associated with housing big data** by implementing a virtual data warehouse approach (Figure 2). The technology mimics the outcome of a traditional warehouse while preserving the custody, security and physical ownership of the data on the original source (never copied or moved). Other options will copy or move data as a batch import process overnight, leaving the analyst working with old data versus near real-time live data.

- → **An infrastructure built to handle the typical big data** problems of incomplete, erroneous, and inconsistent types of data, but unlike most, we are still able to derive results and patterns out of the information. We can take imperfect and inconsistent information and still develop actionable intelligence.

- → **Ownership of the data stays with original source.** Unlike other technology options, the data is not ingested into a proprietary database therefore ownership of the data stays with the data owner, reducing the need to share ownership of the data with a third-party source which can create problems in the long run.

- → **Comply with Freedom of Information Act (FOIA)** requirements by leaving ownership of the data at the original source. Unlike other technologies that ingest data, Forcepoint Data Analyzer relieves organizations from legal responsibility of reporting on the data due to ingestion.

- → **Instantaneously search live data** across internal or external databases, websites, emails or office documents. Latency impacts are greatly reduced because unlike other case management tools that download and store data, Forcepoint Data Analyzer accesses live data. If data is unavailable, analysts receive notice but are able to work with the previous data set until the new data is available.

- → **Comply with data privacy and security restrictions** via the integrated security manager and identify options with unique permissions by individual user or group which is critical for records and information management divisions.

- → **Customize the types of results returned from multiple systems** with full text indexing designed with powerful search capabilities like phonetics and synonyms. Data stays at the original data source and analysts always get the most current data.

forcepoint.com/contact

Forcepoint