IBM Security
White Paper

Intelligence Industry Solutions

IBM i2 Enterprise Insight Analysis

Contents

Executive summary

IBM® i2® Enterprise Insight Analysis enables organizations to analyze large volumes of data to generate actionable insights in near real time. A powerful combination of visual tools and automated analytics helps analysts to quickly uncover patterns, trends and connections that are hidden within large and disparate data sets.

The solution provides the following key business outcomes:

- **Expands operational flexibility**—provides rapid results for both highly detailed queries and multiple concurrent searches
- **Improves cooperation and information exchange**—collaborative environment supports secure storage and intelligence sharing between analysts, teams and agencies
- **Increases efficiency**—integrated custom analytics help analysts filter large volumes of data to find items of interest
- **Enhances productivity**—identity and relationship an identity and relationship recommendation engine add-on automatically processes duplicates and highlights hidden connections in the data
- **Reduces training requirements**—easy-to-use visual queries let analysts draw detailed searches rather than generating complex SQL statements
- **Enriches intelligence products**—market-leading visualization tools with integrated geospatial capabilities let analysts aggregate and analyze data sets in depth

i2 Enterprise Insight Analysis augments and extends the capabilities of analysts, helping them to extract more value from the data and enabling them to perform rapid analysis in support of timely decisions.

Introduction

Is your organization looking to detect and disrupt activities such as cyber attacks, terrorist threats, corporate espionage, illegal trading or fraud? Or perhaps you want to optimize your business processes and decisions by harnessing the power of big data. Whatever scenario describes your business need, i2 Enterprise Insight Analysis can help bring clarity to your data challenges.

i2 Enterprise Insight Analysis combines a rich client for multidimensional visual analysis with a data warehouse to provide advanced analytics at speed and scale. Analysts can rapidly query and filter high volumes of transactional data, such as communications intelligence, network events and financial transactions. Using the client, analysts can combine and analyze the data, layering their results with additional detail to create a richer, more complete intelligence product.

Visual queries allow analysts to quickly create and run complex searches across the data warehouse without needing to learn complicated query languages. Instead, analysts construct queries by drawing visual representations of the relationships and conditions they are seeking. i2 Enterprise Insight Analysis then translates the visual representation into a query statement that is optimized to minimize the execution time. This capability significantly improves analyst efficiency and helps lower the minimum training needed to conduct entry-level analysis.

The automated identity and relationship Recommendation Engine Add-On constantly scans the data and proactively alerts analysts when new information is available, and when data points are altered, strengthened or resolved. This means analysts do not need to evaluate all the incoming data and can focus on the new information that affects a specific analysis.

Concept

The requirements for an optimum analytics tool include:

- **A human-centric approach to data.** Analysts don’t want to think in terms of data structures. The tool must allow them to describe their queries in everyday terms. These include searching for financial transactions that follow a certain pattern of activity, or looking for a hacker with a list of aliases.
- **A visual canvas for examining the data.** Analysts need a tool that supports visual operations for finding data of interest, allowing them to adjust the focus to the scope that is required for an investigation.

- **Data exploration support.** Analysts need to be able to follow multiple threads of investigation with ease. The tool must keep track of their work while they explore.
- **Ability to handle large amounts of disparate data.** Analysts need to be able to sift through large volumes of data, filtering their results to focus on items of interest. The tool must be very responsive, even with large data volumes that support both time-sensitive queries and forensic analysis. For example, one analyst might want to identify a current associate who crossed the border at the same time as the subject of interest five years ago. At the same time, another analyst might be tasked with matching people on a watch list against the passenger manifest of an inbound flight that arrives in two hours.
- **Automatic resolution of duplicates and connections in the data.** Analysts need a tool that continually scans incoming data, merging items without manual intervention while also highlighting non-obvious connections for further analysis. In a globally connected world, the tool must be able to identify patterns that cross linguistic and cultural boundaries.
- **Secure collaboration.** Analysts need to be able to work together, creating and sharing intelligence products. The tool must preserve a historical record of their work while, at the same time, controlling access to restricted data.

Functions

As shown in Figure 1, i2 Enterprise Insight Analysis is comprised of architectural elements that combine to deliver the capabilities that distinguish the solution from all others.

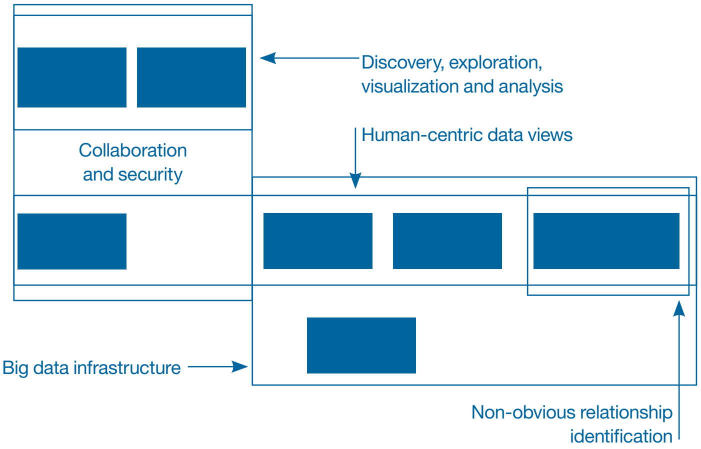
Discovery, exploration, visualization and analysis
Human-centric data views
Collaboration and security
Big data infrastructure
Non-obvious relationship identification

Figure 1: The architectural elements of i2 Enterprise Insight Analysis that support analysts' requirements.

A human-centric approach

When analysts must work with data using technical query languages, they end up wasting a lot of time and effort having to translate their questions into the language of computers. Instead, an efficient analytics tool must allow analysts to work directly with real-world constructs, even though the underlying data may express these concepts very differently. For example, communications intelligence data sets often describe, in very technical formats, phone handset types, provider identifiers, call timings and cell tower data. However, analysts are interested in phone calls, people, geographic locations and time. The strength of a solution depends on how well it performs this translation.

i2 Enterprise Insight Analysis uses a schema that represents data in terms of entities, links and properties as the key definition of the human-centric data model. The schema is easily constructed and maintained using visual tools. All of the elements of the human-centric data view layer represent data in terms of this analyst world view, relying on the data loading infrastructure to perform translations from technical data formats.

This data model enables analysts to ask questions in human terms using the unique visual query functionality. Rather than forcing analysts to construct SQL statements, a visual query lets analysts draw their searches in terms of the entities, links and properties defined in the data model.

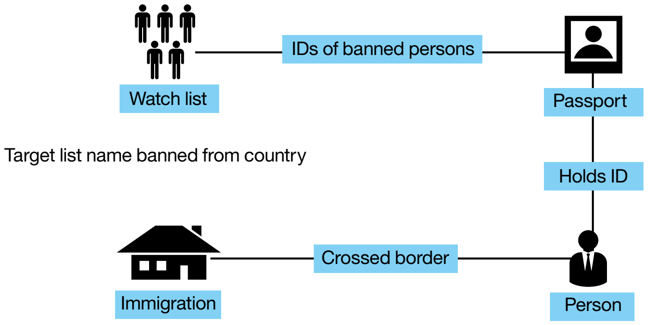

Figure 2: Visual query that searches for people on a watch list who have crossed the border.

In addition to well-established data sets that are processed on a daily basis, analysts often need to work with special data sets that do not have a predictable format or delivery schedule. For example, an analyst might want to investigate a list of names found in a notepad or files seized from a computer at a customs checkpoint. The rich client supports special data sources by enabling the analyst to describe how the data set maps to the entities or relationships of interest to them.

Working with data visually

Pictures can communicate information much more concisely than words. But the types of graphical elements that are required depend on the context. For example, visualizations that are commonly used in business reports, such as pie charts and bar graphs, are less appropriate for intelligence work, where associations, events and time lines are of interest. More importantly, graphics must be interactive. Analysts must be able to take a data set, represent it visually, redraw it, change the layout, view details and add related data. The i2 Enterprise Insight Analysis rich client performs all of these frequently used analytical operations and much more.

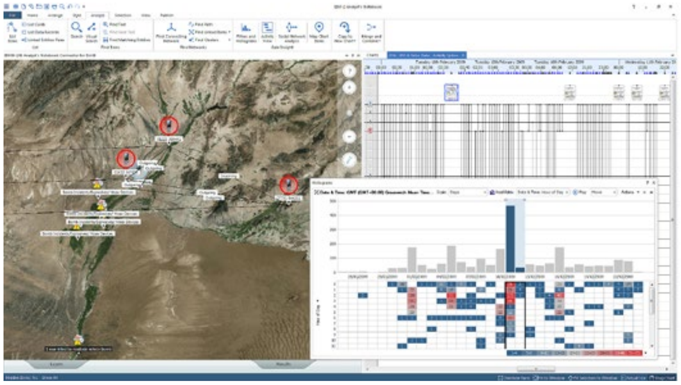

Figure 3: Streamlined access to common analytical operations in the rich client.

The differentiator of i2 Enterprise Insight Analysis rich client's user interface from other tools is the application of modern, user-centric design principles to help drive efficiencies in the analysis workflow. Common analytical techniques, such as finding related entities, identifying the most connected entities, or constructing a heat map based on properties of interest, are built into the user interface. These makes them easily accessible with the minimum number of clicks.

Drawing insights from big data

Online transaction processing (OLTP), such as those found in applications that support online purchases, typically work with a few records at a time. Analytics and reporting workloads read large chunks of data—sometimes entire database tables. Traditional business intelligence tools that support analytics workloads rely on batched operations to process large quantities of data. However, this approach is not suitable for intelligence analysis, where the questions that need answering cannot be predicted in advance. Intelligence and investigative work require an iterative method where, over many interactions with the data, the analyst focuses on the results. The system must respond rapidly to each interaction, which requires a solution that can search hundreds of terabytes of data very quickly.

In addition to being responsive, operational analytics systems need to continuously ingest new data, sometimes sourced from OLTP systems. The concurrency needs of such systems can be addressed by making the analytic or reporting queries run as fast as possible, thereby avoiding conflicts with the data ingestion. There is only one way to scale such requirements to high data volumes—massively parallel hardware. If the processing for a single complex query can be parallelized and executed on multiple database engines, the challenge of increasing data volumes can be met by increasing the degree of parallelism. This is a key design aspect of the optional i2 Enterprise Insight Analysis data warehouse appliance. It uses a partitioned database with specialized hardware, providing fast interconnects to support high degrees of parallelism.

Modern web search engines use commodity hardware with massively parallel processing in large server farms. But to achieve the required retrieval speeds, indexes of search results are created for every possible simple search criterion, for every possible search term. The searches that analysts need to run cannot be addressed in the same way, as the search criteria are complex and address domain-specific needs. Users are unlikely to notice if their web search results are a few hours out-of-date, but analysts need to be certain that they are searching the latest available data, which puts further demands on data ingestion. For example, if your analytics system fails to ingest the passenger manifest for inbound flights in a timely manner, border controls are compromised and national security is put at risk. Simply deploying large numbers of commodity servers cannot address the competing needs of rapid searches with continuous data ingestion. The specialized hardware of the optional i2 Enterprise Insight Analysis data warehouse appliance is specifically designed for this purpose.

Very large volumes of data demand a different approach to data ingestion. The traditional extract, transform and load (ETL) process wastes a lot of time transferring the data between the ETL solution and the data warehouse, particularly during the transform phase. In an analytic system, the workload from analyst queries tends to ebb and flow over the day, so any idle system capacity can be used for data ingestion. Moving the processing of complex data transformations to the optional i2 Enterprise Insight Analysis data warehouse appliance allows for faster overall ingestion. Similarly, if the complex queries that are needed for reporting are delegated to the appliance, reporting is accelerated as well.

Connecting the fuzzy dots

With big data, the volumes can be so large that it is not possible for human analysts to be part of the processing flows to recognize patterns in the data. Therefore, the solution must not only be capable of processing large volumes of data quickly, it must also make connections between related data records just as quickly. To truly mimic human analysts, the system must identify potential duplicates even when the data does not directly match.

i2 Enterprise Insight Analysis features a Recommendation Engine Add-On that axiomatically performs rapid identity resolution that would otherwise require large numbers of trained personnel. The Recommendation Engine Add-On accumulates contextual information for every single identity in the data. Determining an identity involves making assertions based on context and using those assertions for downstream analysis. When new information invalidates a previous assertion, the recommendation engine add-on automatically corrects the assertion. A positive match results in the resolution of two duplicate records into a single identity, whereas disambiguation of a previous false positive results in the creation of two disconnected records.

Collaboration and security

Individual desktop-based analytical applications are compromised by a lack of institutional memory. Clientandserver solutions, such as i2 Enterprise Insight Analysis, preserve knowledge by letting analysts save and organize their work so that it is accessible to others. The collaborative nature of the i2 Enterprise Insight Analysis solution enables workflows. For example, a cross-functional team of analysts can use their individual areas of expertise to create a single intelligence product. Or a workflow can be used to implement reviewing and sign-off procedures.

But being collaborative does not mean that all data should be accessible to everyone. With i2 Enterprise Insight Analysis, an organization can define a security model that classifies the data and matches the classification to the clearance level of the analyst attempting to access the data. The security aspect of i2 Enterprise Insight Analysis is compatible with a wide variety of enterprise directory solutions, as well as being extensible in order to support custom solutions. i2 Enterprise Insight Analysis includes robust audit logging designed to meet the needs of intelligence and investigative agencies worldwide. This solution also supports automatic purging of data to meet the legal requirements for data retention.

Use cases

i2 Enterprise Insight Analysis is a cross-industry solution that is relevant to any organization challenged with turning overwhelming data into actionable intelligence and insight. It has uses cases in defense, intelligence, security and commercial spaces.

i2 Enterprise Insight Analysis can address needs across the spectrum of intelligence, security and investigations:

Intelligence

- Military intelligence
- Counter terrorism
- Counter fraud
- Data trend analysis
- Reputation analysis
- Cyber analysis
- Epidemiology

Security

- Indications and warning
- Incident correlation and prediction
- Disaster response
- Vetting
- Security incident investigation
- Insider threat
- Cyber analysis
- Epidemiology

Investigations

- Computer incident response
- Fraud investigation
- Law enforcement investigation
- Vetting
- Security incident investigation
- Insider threat

Expanding into the cyber and commercial space, i2 Enterprise Insight Analysis can address:

General use cases

- Advanced persistent threat discovery
- Insider threat identification and investigation
- Disgruntled employee identification
- Employee sensitive data caching
- Asset vulnerability vs. criticality comparison
- Threat campaign tracking
- Strategic report production for leadership
- HIPS and IDS correlation
- External scanning pattern analysis
- Spear-phishing identification and impact analysis
- Pirated software use identification
- Threat intelligence integration into incidents
- Big data analysis search across large data sets

Financial sector use cases

- Fraud detection and investigation
- Retrace trades for compliance
- Insider trading identification and investigation
- Executive information security protection
- Reputation and brand awareness
- Integration of state-level threat reporting
- Vendor risk management compliance tracking
- Identify employees with competitive “side jobs”
- Identify individuals leaking info to media
- Discover customer data leaked online
- Discover leaked sensitive documents online
- Darkweb data aggregation and discovery
- Social media monitoring and investigation

Conclusions

i2 Enterprise Insight Analysis provides a sophisticated, yet easy-to-use environment that enables analysts to search large, complex and dynamic data sets. Analysts can quickly uncover information buried in large volumes of data with the help of automated and assisted analytics. Freed from the requirement to use complicated query languages and the need to constantly monitor incoming data, analysts can concentrate on collaboratively creating and sharing valuable intelligence products.

i2 Enterprise Insight Analysis enables your analysts to provide rapid, in-depth analyses of large data volumes, while enabling your organization to make smarter and timelier decisions. The powerful and intuitive visual query and analysis tools open up low-level analysis tasks to a wider range of users, while also providing the sophisticated features required by professional analysts.

The scalability, modularity and interoperability of i2 Enterprise Insight Analysis enable you to support and augment your existing infrastructure rather than replacing it. You can deploy features and functionality to meet the needs of multiple operating environments, missions and users.

For more information

To learn more about the IBM i2 Enterprise Insight Analysis offering, please contact your IBM representative or IBM Business Partner, or visit ibm.biz/IBMi2EIA

About IBM Analytics

IBM Analytics software delivers data-driven insights that help organizations work smarter and outperform their peers. This comprehensive portfolio includes solutions for business intelligence, predictive analytics and decision management, performance management, and risk management.

IBM Analytics solutions enable companies to identify and visualize trends and patterns in areas, such as customer analytics, that can have a profound effect on business performance. They can compare scenarios, anticipate potential threats and opportunities, better plan, budget and forecast resources, balance risks against expected returns and work to meet regulatory requirements. By making analytics widely available, organizations can align tactical and strategic decision-making to achieve business goals. For further information please visit **ibm.com**/analytics.

Request a call

To request a call or to ask a question, go to **ibm.com**/analytics/contactus. An IBM representative will respond to your inquiry within two business days.

References

- IBM i2 Enterprise Insight Analysis for Defense Intelligence solution brief
- Insight Analysis for Cyber Analysis Solution brief
- IBM i2 Enterprise Insight Analysis Release Notes
- IBM i2 Enterprise Insight Analysis V2.1 announcement letter

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle