IntelligenceReveal™ for Multi-Source Exploitation

Digital Intelligence

BAE SYSTEMS

IntelligenceReveal™ for Multi-Source Exploitation

IntelligenceReveal for Multi-Source Exploitation is a comprehensive solution which collects data of all types from multiple sources and enables analysts to perform complex yet intuitive analysis on the data which helps build a single, unified intelligence picture. The solution speeds up the intelligence analysis process. It facilitates the production of intelligence insights which would never otherwise have been reached, enabling your analysts to answer their investigative questions faster, more efficiently and more effectively.

The Challenge

In today's digital world, everything we do leaves a digital footprint and produces information about what we have done, what we are planning to do, what we are interested in, who we are and who we know. For analysts who are tasked with the defence of our nations, or the protection of our citizens from criminals, this data contains valuable intelligence which can help answer their investigative questions and provide insights into the activities, motives and intentions of Subjects of Interest.

However, this information is hidden amongst different types of data which is generated in many different formats, from many different applications, and stored in many diverse systems in multiple locations. And the amount of data being produced by our digital lives is enormous, and growing every day.

Analysts seeking solutions have historically faced complex challenges:

- How to exploit the data available in multiple, different locations, while respecting restrictions on the data stipulated by its owners
- How to make that data easily searchable and retrievable and quickly available for analysis
- How to process different types of data in different formats such that the information within can be extracted
- How to respect the sensitivity of data, and ensure that access to data is only available to those with the appropriate security clearance, and recognising that some security policies prevent the fusing of different types of data or data from specific sources
- How to scale any solution so that it caters for the burgeoning volumes of data being produced from many sources
- Shortage of analytic skills: agencies need analysts with new data analytic skills, but they are in short supply
- An increasing amount of communications data is being encrypted, which puts pressure on ensuring that the maximum amount of intelligence is derived from data from other sources.

Until recently, analysts in many agencies would be focussed on collecting and analysing selected data from one or two particular sources. In some cases, this would be done manually, often also working from paper-records. Security and policy concerns may additionally prevent sharing of valuable data with other departments and organisations. For some, this approach has resulted in an inefficient, costly, time-consuming process which cannot scale to the challenges of the growing data burden being produced by the digital world. Furthermore, in some cases this siloed, outdated approach has also proved to be dangerous, with analysts missing valuable intelligence insights which could otherwise have proved invaluable in helping to mitigate threats.

The Solution: IntelligenceReveal for Multi-Source Exploitation

IntelligenceReveal for Multi-Source Exploitation is a new solution, designed to address the multiple challenges analysts face in the digital world. Whereas other solutions may focus on the gathering and analysis of specific data types from particular data sources, IntelligenceReveal for Multi-Source Exploitation is a comprehensive solution that enables analysts to federate the search of data in their different locations or to gather and store all types of data (e.g. communications metadata, communications content, flight information, ANPR data, open-source data etc., as shown in Figure 1 below) from multiple sources, and then exploit the wealth of intelligence contained within it through powerful analysis.

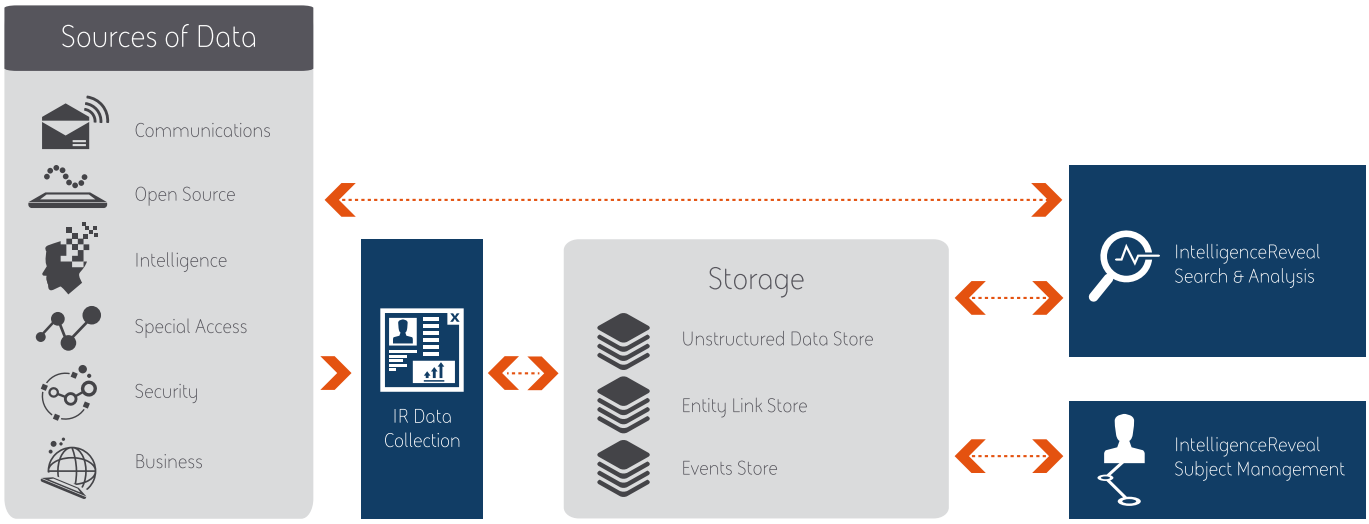


Figure 1: Diagram outlining solution for IntelligenceReveal for Multi-Source Exploitation

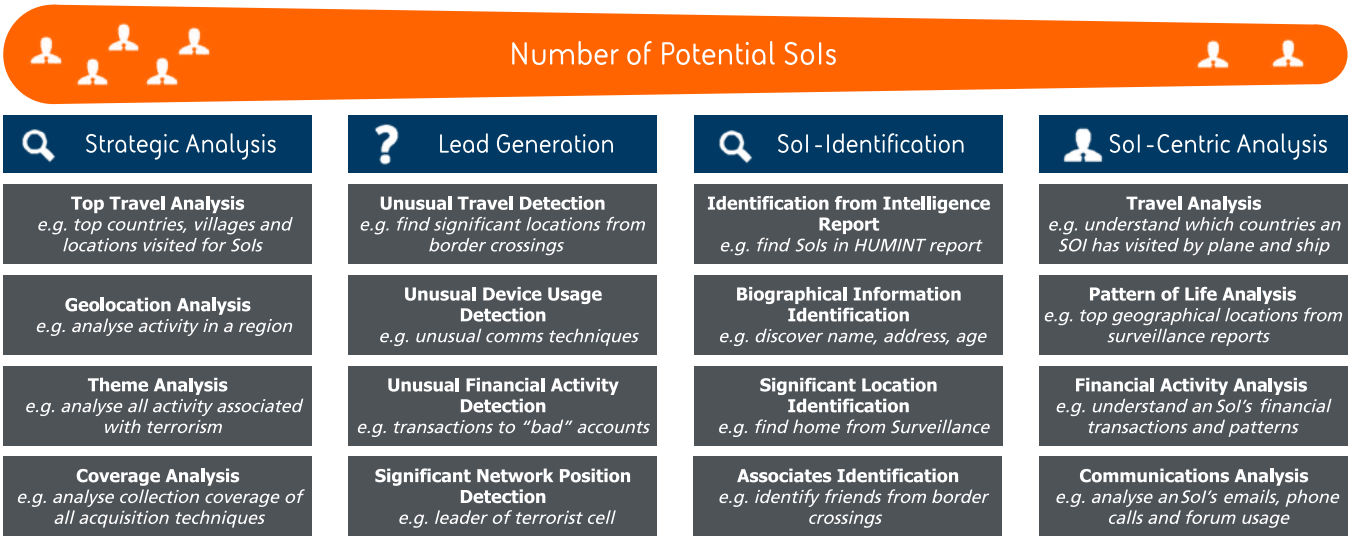


Figure 2: Diagram outlining the investigative process for Multi-Source Exploitation with examples of questions which can be answered

Comprehensive Product Capabilities

To provide its comprehensive capability, the solution includes the following products, enabling analysts to execute their investigative processes quickly and effectively (see Figure 2):

IntelligenceReveal Data Collection

Processes data from the following sources: structured biographical data (e.g. passports), unstructured data (e.g. intelligence documents) and structured event data (e.g. telephone calls or IP data) and includes the following features:

- Data loading, supporting historical and incremental loading
- Entity security level labelling
- Entity extraction classification: classifies Entities from unstructured text into pre-defined structured categories, such as people, locations, organisations and expressions of times.

IntelligenceReveal Search & Analysis

Aimed at both data and non-data specialists alike, IntelligenceReveal for Multi-Source provides a scalable suite of sophisticated tools for searching and then analysing the multi-source data through a number of advanced and yet intuitive visualisations, providing:

- Simple and Advanced Search functionality – a range of comprehensive search capabilities including multiple keywords search, geo-search, exact search and character insensitive search, Boolean and wildcard searches
- Federated Search, where the user can search data directly in its original location, covering both external and internal data sources. This is often required where the data to be searched is owned by someone else or the data cannot be copied and then moved from its original source
- Comprehensive inbuilt analytics to help speed up search and analysis, e.g.
  - Common Travel – analytics looking for people who have travelled together on multiple flights
  - Significant meetings – analytics looking for people who have been geographically located close to each other at similar times
  - Significant SIM Swapping – analytics looking for an unusual number of SIM swaps
- Entity analysis using a network visualisation
- Unstructured analysis including visualisations for displaying key words, sentiment and the unstructured content itself
- Event analysis using map, timeline, and grid visualisation
- Export and publish – data can be published/exported as MS Word, CSV and snapshots of visualisations
- Attribute-level security – ensuring users can only view records they are authorised to see
- Data Provenance - the solution keeps a record of the source of information and the date of its acquisition
- Auditability – maintains a full log of user actions for auditing purposes.

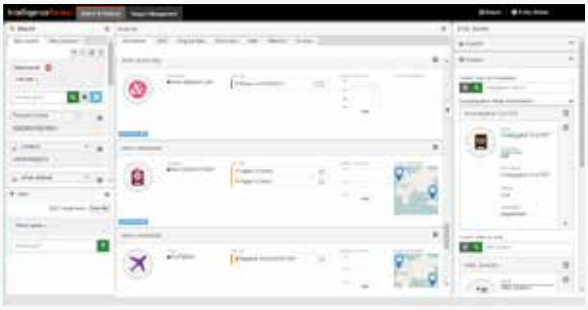


Figure 3: The Search and Analysis capability offered by the BAE Systems IntelligenceReveal for Multi-Source Exploitation solution.

IntelligenceReveal Data Stores

Highly efficient, available and expandable data store which enables flexible and high performance searching of large volumes of metadata and unstructured text. Constructed with the latest technology for managing big data, the data store can scale up to storing petabytes of data.

IntelligenceReveal Subject Management

A suite of tools and applications for managing, storing and sharing key data on Subjects of Interest (SoIs), cyber threat actors and investigations including:

- Biographical data (name, data of birth, hair colour), devices, online identifiers and locations
- Which SoIs or cyber threat actors belong to which investigations
- Entity Builder: During data analysis using the Search & Analysis tool, analysts can pre-load shopping baskets of valuable data relating to individual SoIs or investigations: shopping baskets can then be uploaded to the Subject Management database.

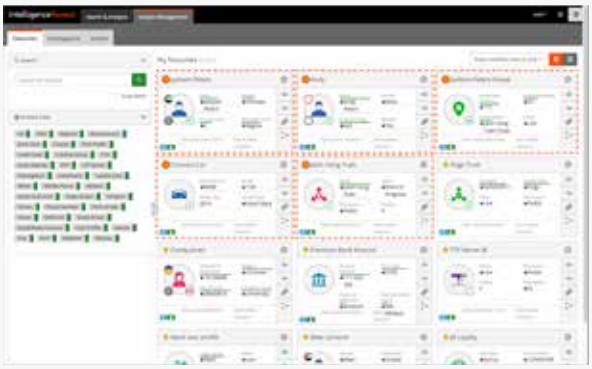


Figure 4: The Subject Management capability offered by the BAE Systems IntelligenceReveal for Multi-Source Exploitation solution.

IntelligenceReveal Technical Tools Training

Upon request, BAE Systems can provide extensive training to enable analysts to use the solution and its component products to best effect.

IntelligenceReveal Processes and Operating Model

BAE Systems can share our experience derived over many years, providing proven working processes, operating models, organisational structures and guidance on required skillsets, all of which are designed to help different organisations maximise the effectiveness of users approaching individual missions utilising this state-of-the-art technology.

Other Related BAE Systems Solutions

As shown in the diagram on page three, IntelligenceReveal for Multi-Source Exploitation exploits data from multiple sources. In some cases, this data could be provided to the IntelligenceReveal for Multi-Source solution from other related BAE Systems solutions, such as:

- Communications data supplied by the BAE Systems CI Metadata and Content Exploitation solutions, including data acquired from BAE Systems probes within national networks, and then stored and analysed with the BAE Systems IntelligenceReveal and X-Stream product suites
- BAE Systems Open Source Exploitation
- BAE Systems cyber solutions, which includes cyber defence data supplied from the BAE Systems National Network Cyber Centre (NNCC) solution which collects and analyses data from CSPs.
- BAE Systems Unstructured Data Exploitation.

Using these other solutions and products, it is possible for customers to deploy an extended comprehensive single architecture which spans from the probes on an IP or voice network (non IP) through to the multi-source analysis applications, yielding significant operating efficiencies and enhancing agencies ability to fulfil their missions.

Flexible Architecture

From years of working with Intelligence Agencies and Law Enforcement Agencies, BAE Systems knows that each customer is different. The architecture of IntelligenceReveal for Multi-Source Exploitation allows each implementation to be tailored to an individual customer's needs, such as the available data sources, different security and policy rules governing data acquisition, retention and sharing, etc. The framework also enables third party products and/or customers' existing products to be easily integrated into the solutions, so that legacy investments can be protected and the functionality and benefits from other best-of-breed technologies can be harnessed. Training and operating models can be customised to individual customer requirements, as needed, to ensure maximum effectiveness of the solution once deployed. Furthermore, it is possible to integrate our features within other frameworks and add bespoke features needed by customers.

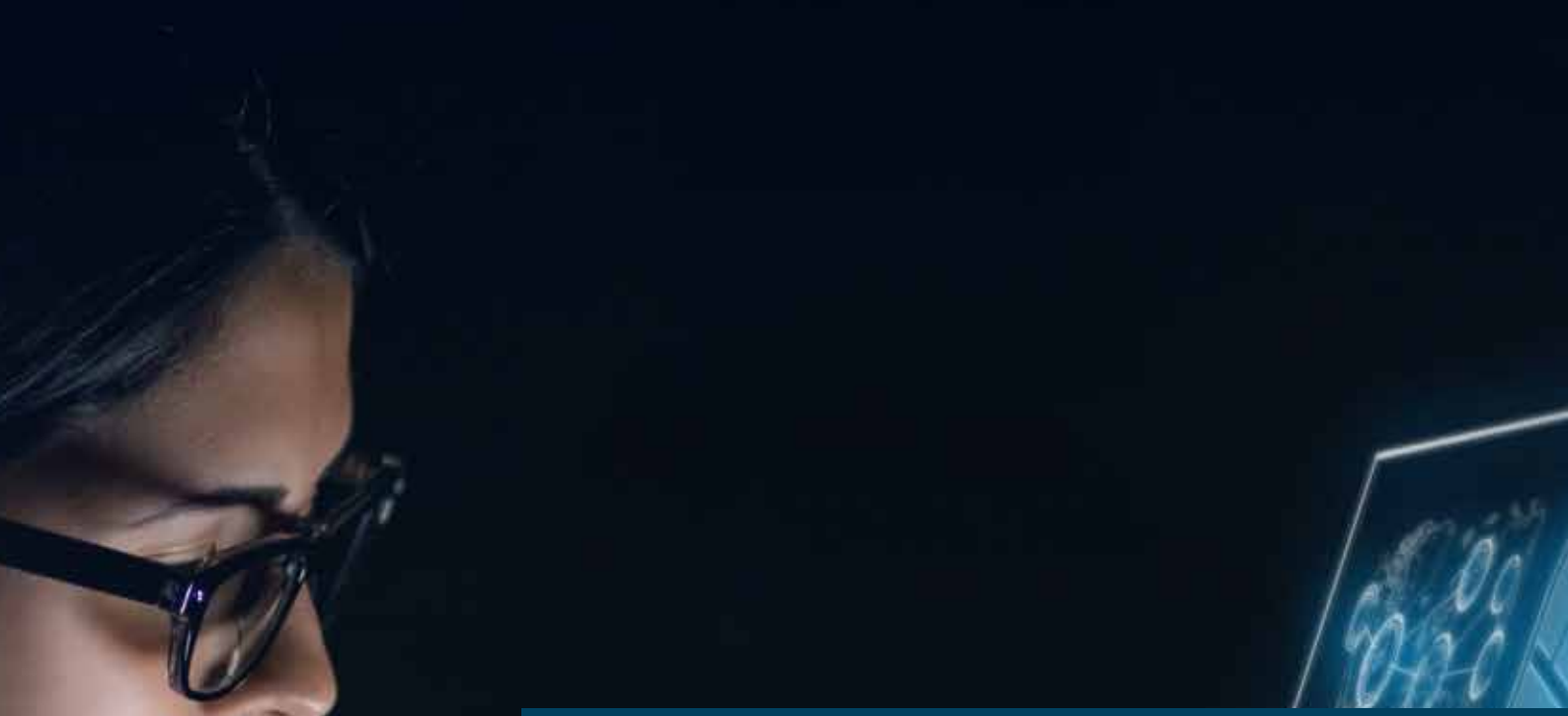
IntelligenceReveal for Multi-Source Exploitation allows each implementation to be tailored to an individual customer's needs

Summary

BAE Systems has a rich heritage in data analytics, Communications Intelligence, and working with Intelligence Agencies, Law Enforcement Agencies and Communications Service Providers. Drawing upon the experience gained from working with our partners to solve their problems and improve their mission capabilities, and coupled with our extensive technology expertise in Big Data analysis, BAE Systems has developed the IntelligenceReveal suite of solutions and products. A member of the IntelligenceReveal family, IntelligenceReveal for Multi-Source Exploitation provides agencies and analysts with a comprehensive and scalable data collection, analysis and management solution for the digital age.

The technology provided by IntelligenceReveal for Multi-Source Exploitation provides analysts with a step-change in their mission capabilities, enabling them to accomplish in seconds that which previously would have taken hours. Its powerful visualisation and analysis capabilities enable users to see correlations between data which yield investigative insights which analysts using alternative approaches would never have seen or thought of. Using IntelligenceReveal for Multi-Source Exploitation, analysts can exploit the intelligence hidden within the data, and agencies can operate more efficiently and effectively, transforming the capability of their existing analyst resources and empowering swifter, greater mission success.

To learn more about IntelligenceReveal for Multi-Source Exploitation please contact us.



We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
1676 International Drive
Suite 1000
McLean, VA 22102
United States
T: +1 (703)848 7000

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
1 Raffles Place #42-01
Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

CREST CESG Certified Service Cyber Incident Response CPNI Centre for the Protection of National Infrastructure

BAE SYSTEMS