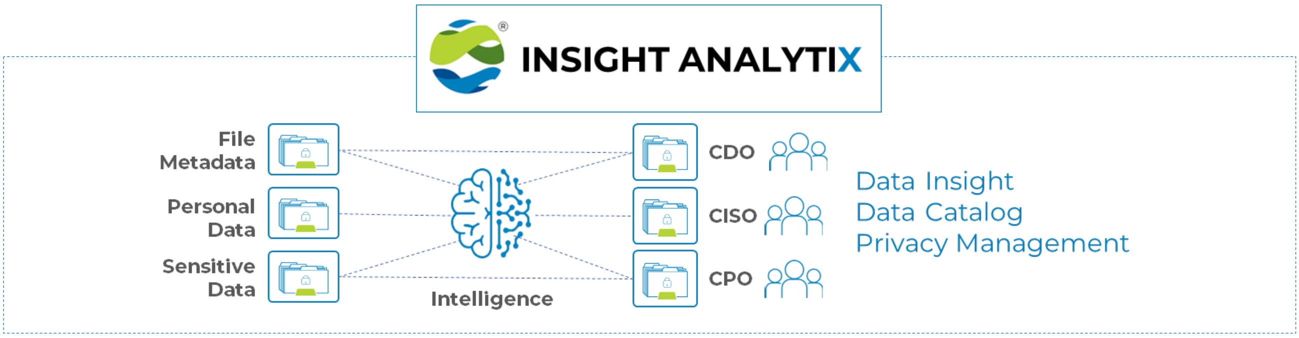
Analytics Suite

Mobility | **Analytics** | Security | Compliance

Data is the lifeblood of every organization, and there are endless references to data being “the new oil”. The challenge in most enterprises is that their data is oil in crude form -- without refinement, it has limited to no value. Enterprises are generating data at an exponential pace, typically growing their unstructured data by over 30-40% year over year. That growth is creating a data deluge with limited to no visibility into the context (metadata) or content of the data. In addition to that, most data management practices continue to be siloed based on department and area of operations. An infrastructure team views data purely from a storage perspective, a CDO looks at ensuring compliance to Data Management standards, a CISO looks to ensure that data is protected, and lines of business looks to extract value. Each stakeholder does so with an independent lens and without much interaction with the other stakeholders.

With the **Data Dynamics Analytics Suite**, enterprises can leverage a single Platform to address the value that each of the constituents mentioned above are seeking. The Analytics Suite provides critical insights into the metadata for storage visibility and infrastructure optimization. Content analytics in the Analytics Suite provides risk analysis for personal and business sensitive data to help ensure compliance and security. Line of business owners can analyze data to extract patterns or insights that allow them to make informed decisions. The Analytics Suite uses artificial intelligence and machine learning technologies to transition data from simply existing since creation in a stored state into aligned and refined data for business value.



Data About the Data

The Data Dynamics Analytics Suite provides metadata analysis that lays the foundation for enterprises to understand the data itself. Characteristics such as file ownership, when files were created, when files were last accessed, and what type and size files they are just some of the data points captured and provided for reporting and decision making. This insight is valuable to identify security vulnerabilities, such as files or folders that have broad or universal access, but it also provides insight into trends based on users or business units. In most enterprises, when employees leave, their “orphaned data” continues to reside in the same storage as when they were an active employee. The orphaned data in most organizations eventually becomes a compliance challenge, as there is no owner for these files and, depending on the content, those files can present a potential exposure risk. Most environments have a large percentage of files that have not been touched since 30 days after creation. This leads to a massive primary and expensive storage sprawl without any real value. As such, understanding the age and last access times of your files provides a means to clean up and tier enterprise data to lower-cost storage, be it local or in the cloud.

Personal Data

Personal data is defined as any information that relates to or is identifiable to an individual. Personally identifiable information about an individual could include a driving license, a national ID such as a Social Security number, a name and date of birth, and many other such parameters. A single piece of personal information alone, such as an IP address or “blood type”, may not be considered personally identifiable, but when put together with additional data points, may be used to identify a given individual or device. Storing personal information creates a custodial relationship for an enterprise, and a growing number of local and federal laws are being implemented to ensure the proper storage, access, and usage of such data.

With the Data Dynamics Analytics Suite, personal data can be identified via built-in templates or customized as required. The Suite provides risk analysis functionality that ranks files based on the type and amounts of personal data that are found. This provides enterprises with a method of understanding files that need to be reviewed and acted upon, including integrating the permissions currently granted as a factor in the security remediation. Customized templates can be created that look for particular fields that may be required based on jurisdiction and or other business needs.

Business Sensitive Data

As a result of daily operational activity, business-sensitive information is stored in files on a daily basis. This can include aggregate or individual customer information; for example, a document that contains the strategy based on which a financial institution trades equities. Access to this type of information by competitors can create a significant business loss. The Analytics Suite provides integration with business glossaries, including Collibra, so existing repositories may be integrated to identify sensitive information as classified. Industry vertical-based glossaries are provided as templates, including templates for Oil & Gas, Healthcare, and other major industries. The goal is to have as much of the terminology available within the Platform itself, and the customer can simply customize as required. This ease of integration expedites the deployment and use of the Analytics Suite and helps to identify business-sensitive information for operational use, as well as to ensure that information is stored and managed in a secure manner.