Insight AnalytiX 1.3
Privacy Risk Classifier

Know Your Data's Potential

Business Challenge

The explosion of data has been unprecedented in the last decade. According to Gartner, it's estimated that 80% of this data explosion can be attributed to the capturing of unstructured data. Experts project that the size of unstructured data will grow at a phenomenal rate of 62% a year. Most enterprises (an estimated 80%) have very little visibility into what's happening across their unstructured data, let alone how to manage it.

Unstructured data is challenging to manage, as it does not easily lend itself to the more traditional models of data storage and analysis. However, if you can find a better way to manage this kind of data and understand its content, that unstructured data can be an extremely rich source of relevant information that can add tremendous value to your business and you can effectively mitigate any data governance risks from regulations such as: PII, GDPR, HIPAA, CCPA.

Unlike this structured world, where information is stored in a pre-defined data model, unstructured data:
- Does not have a pre-defined data model or it is not organized in a pre-defined manner.
- Comes in many unrelated forms, such as documents, text files, spreadsheets, presentation files, video files, audio files, and pictures, to name some of the more common formats.
- Is typically stored in individual files without an organizational application organizing and managing the relationships between those files.

So how do you mitigate the data governance and security risk associated with massive amounts of unstructured data?

Analytics Driven Data Management

Data security has been paused due to a new change agent in today's IT world! It is no longer OKAY to be blind to what information is stored within your infrastructure. Information Technology must be able to identify, tag, manage, secure, audit, quarantine and move files that have PII, HIPAA, CCPA or GDPR data. Whether the goal is to quarantine, remove, secure, audit or analyze these sensitive data elements, IT industry must be able to protect the business from risks it did not know existed just a few years ago.

Insight AnalytiX's Privacy Risk Classifier delivers discovery, tagging, management, and movement of unstructured data based upon identifying the data that meets compliance handling requirements. Data privacy standards were created in the recent years to protect individuals and companies from misappropriation of key data such as:

- PII data - includes address, credit card, phone number data
- HIPAA data - includes diagnosis, prognosis and medication data.
- GDPR – applies to consumer facing organization that capture information such as username, password, and large amounts of personal information
- CCPA - gives consumers more control over personal information that businesses collect about them
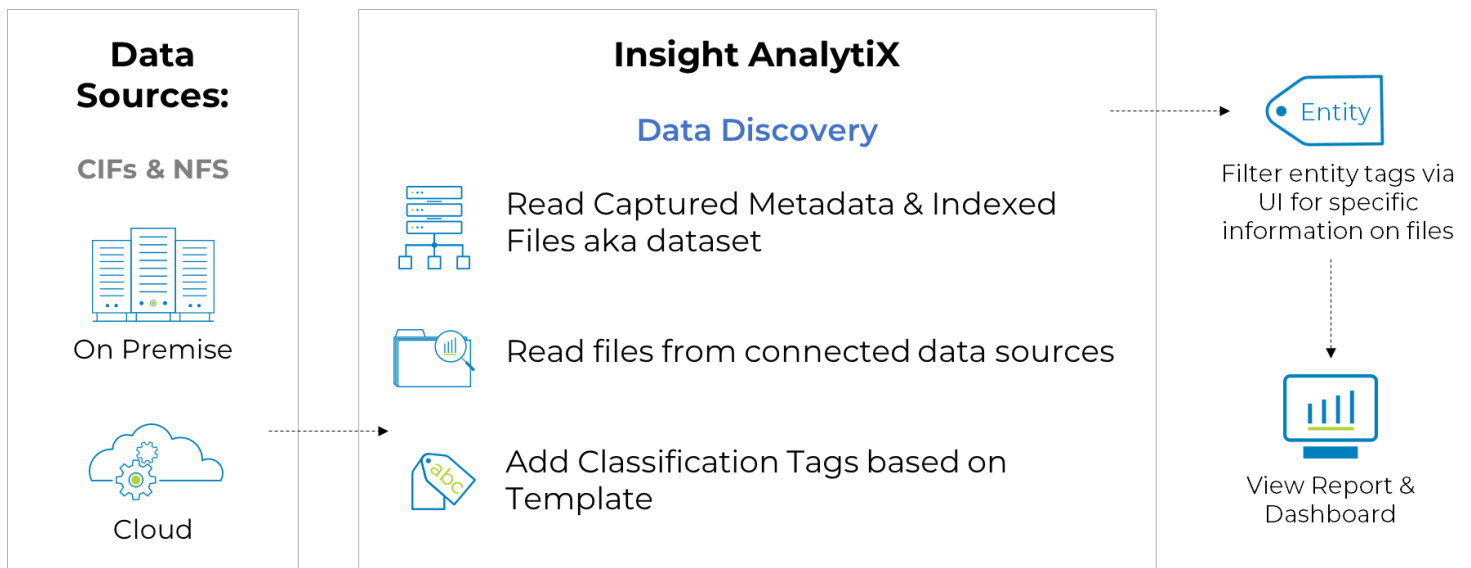
New default Report Templates

Insight AnalytiX 1.3 includes a set of default, system-created report templates that group entities and fields based on specific useful sets of information relevant to customer environments.

The default report templates in Insight AnalytiX 1.3 are as follows:
- Human Resource Data
- Highly Sensitive Identity Data
- Highly Sensitive Health Data
- Special Category Data
- Sensitive Health Data
- Highly Sensitive Financial Data

In addition, you can create your own custom report template.

Data Sources:

CIFs & NFS

On Premise

Cloud

Insight AnalytiX

Data Discovery

Read Captured Metadata & Indexed Files aka dataset

Read files from connected data sources

Add Classification Tags based on Template

Entity

Filter entity tags via UI for specific information on files

View Report & Dashboard

Insight AnalytiX - Privacy Risk Classification

Companies that do not address proper compliance with handling their unstructured data face enormous financial risk, so how can they address this risk while doing more with less?

The Insight AnalytiX platform merges the discovery of file and object metadata with the ability to scan file/objects for specific data types, PII, HIPAA, GDPR or CCPA. Insight AnalytiX not only discovers sensitive data based upon its templated search technology, it allows companies to identify where the data should be stored and how it should be managed to reduce their risk. Some common questions that companies are asking are:

- How much of PII data exists in existing open shares in our company?
- Have we experienced a security breach and were we able to identify what data might have been accessed?
- Are we supporting HIPAA requirements to manage and protect patient data with 10-year retention?
- Are we able to meet GDPR requirements to manage and protect personal data for 2-year retention?
- Are we prepared to face the complexities of CCPA compliance?
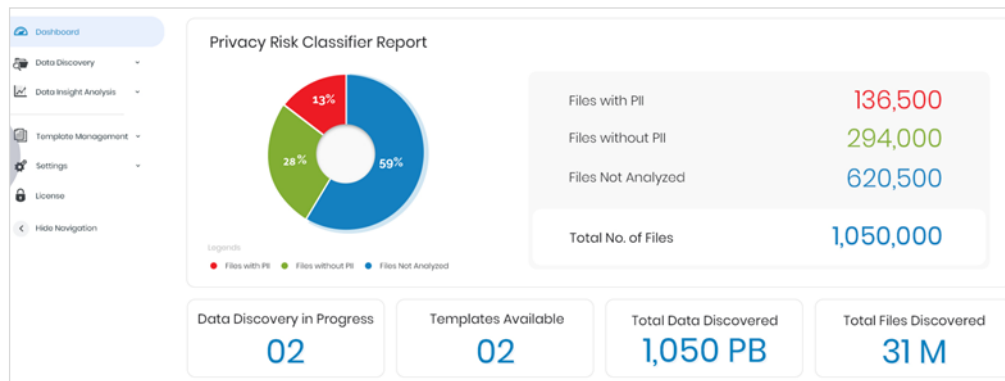
Figure 2: Privacy Risk Classifier Dashboard

Data Dynamics Privacy Risk Classifier is the industry's first search based application to identify PII data risk across storage, application and cloud environments.

Insight AnalytiX 1.3: New and Differentiating Features

Insight AnalytiX provides risk identification and assessment based on the amount and combination of personal information found within a data set. In addition to risk identification, data can be classified to provide context via intelligent tagging, even allowing for auditing against pre-defined corporate standards, mitigating the need for user-dependent controls. Insight AnalytiX is the first step to identifying the potential exposure that exists within a hybrid cloud file storage environment.

▪ **Enables remediation of potentially-sensitive data**

Remediation is a new feature added to Insight AnalytiX 1.3. Now, Insight AnalytiX 1.3 does more than simply scan and analyze your environment for data that could potentially expose your employees and customers to risk, it allows you to resolve those issues.
With this version of the product, your organization can mitigate the risk of sensitive data access and misuse through a robust, multi-approver remediation workflow. In this workflow, all necessary stakeholders are assigned tasks to request, approve, and execute different types of Remediation assignments, and all users are able to easily see the status of each Remediation project as it progresses.

▪ **Quarantine your sensitive data to a secured and accessible locations**

The new Remediation workflow in Insight AnalytiX 1.3 uses StorageX migration and replication functionality to allow users to quickly and securely migrate sensitive data from their current storage location to a more secure location, such as a share on a file storage resource or an object storage bucket. Sensitive files may be moved from one file-share to another file-share and a file-share to an object-store location which includes NFS, and SMB based storage technologies. Object storage includes any S3 compliant object store and support for Azure-Blob.

▪ **Enables blockchain-based file audit trails**

In Insight AnalytiX 1.3, Auditing creates an immutable record of changes performed to sensitive attributes of a file. Blockchain technology built in to ControlX is implemented to provide a scalable and immutable audit trail. A combination of off-chain and Blockchain technologies are used in a way that the references to any personally identifiable data may be erased when required. Whenever an audited file is modified, the change is added to the blockchain, and you can then view a report of all audited changes for the dataset as a whole or for a specific file, as needed.

- **Allows users to secure sensitive files**

In Insight AnalytiX 1.3, the Remediation Analyst may choose to secure files from unnecessary access. This is achieved by excluding public access from the reported sensitive files. This IX 1.3 release supports SMB based storage on a single Microsoft Windows AD domain.

- **Adds new silent installer option**

Insight AnalytiX 1.3 includes a new silent installer, which allows you to rapidly deploy an Insight AnalytiX environment without needing to run the RPM-based installer or go through multiple configuration windows. The silent installer takes a customizable pair of configuration files and automatically populates your installation, including all Content Processing Engines, Data Science Engines, Orchestration Engines, and Insight AnalytiX servers.

- **Improves the installation process**

By using an RPM-based installer, Insight Analytix 1.3 improves performance of the installation process, cuts installation time by 100 percent, and simplifies user requirements.

- **Expands Linux installation support**

This version of Insight AnalytiX allows users to install multi-node instances of the product on servers running Red Hat Enterprise Linux 7.9, 8.1 and 8.2.
In addition, Insight AnalytiX now supports installation on both Minimal and GUI-based versions of Linux, including both CentOS and Red Hat Enterprise Linux.

Privacy Risk Classifier Use Cases

- Identify Sensitive Information or PII Data
- Reduce Sensitive Data Exposure
- Assess Industry Compliance (GDPR, HIPPA, CCPA)
- Assist in the protection of GDPR governance
- Assess data for PII before moving to the cloud

It is likely that these questions are now front and center within your 2020 'must haves'.

Book a Demo to See Insight AnalytiX in Action

Find answers to your questions by contacting Sales@datdyn.com