JETTEE

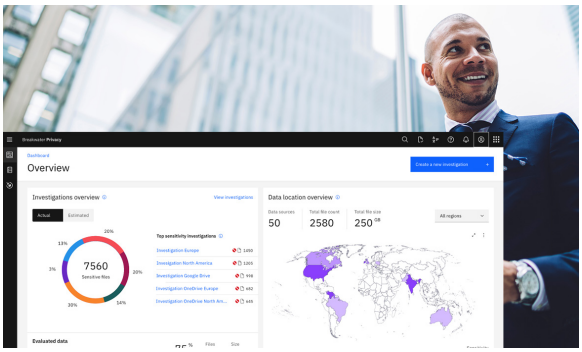
Jettee Governance

Cybersecurity and Data Privacy for Unstructured Data

Jettee Governance enables customers to identify and remediate sensitive content in a fraction of the time by connecting to multiple unstructured data sources and leveraging artificial intelligence (AI) to sample and segment data targeting hot spots. Problematic data can be grouped, and policy-driven actions like Quarantine, Delete, and Append Name can be applied. These capabilities are beneficial to proactive cyber security processes by protecting or removing files that hackers typically access during a cyber breach.

Foundational Privacy Capabilities

Jettee Governance is designed to simplify the implementation and ongoing operation of the Privacy function within companies. Jettee Governance supports these foundational cybersecurity & privacy requirements:



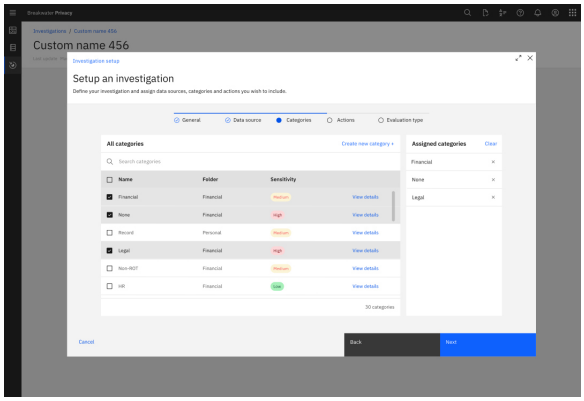
- Risk Assessment
- Data Breach Response
- Data Profiling and Classification
- Risk Mitigation and Data Minimization
- Data Migration and Localization

Create Investigations

- Natively connect to data sources including MS365 and on-premise file shares
- Select scan preferences and built-in categorization types
- Rapidly identify the areas of highest risk without the need to index every document

Out of the Box Categorization

- Jettee provides a set of **out of the box categorizations** that prioritize the combinations of personal information that should be considered the riskiest.
- The categories cover **Personal, Financial, Health, Employment & Biometric Data** and can be utilized to help comply with multiple regulations, including **CCPA/CPRA, GDPR, LGPD, HIPPA, and PCI.**



Statistical Sampling & AI Segmentation

- A practical methodology for identifying and prioritizing data stores with high volumes of sensitive data/PII.
- **Sampling** is the process of **evaluating a select number of files** out of an entire corpus and extrapolating the analysis to the larger data set with a level of confidence.
- **AI segmentation** creates the equivalent of a fingerprint of files that contain sensitive data/PII.
- The **Jettee AI** then predicts which documents most likely contain sensitive data/PII.
- Combined with sampling, these techniques provide the fastest method to profile and reduce risk in large volumes of data.

Analyze Results and Take Action

- Powerful visualizations show your actual and estimated risk over time.
- Problematic data can be grouped, and **policy-driven actions** like **Move/Quarantine**, **Delete**, and **Append Name** can be applied.

Jettee Governance Cloud

Jettee Governance runs on the Jettee Governance Cloud which can be deployed in a hybrid fashion, full SaaS or deploying analytics nodes behind the firewall or in private cloud environments. The platform scales to large enterprises through the deployment of decentralized processing nodes. Additionally, organizations can deploy instances within a region in compliance with data localization regulations.

About Jettee

Jettee helps mitigate risk and gain insight from sprawling information by combining technology automation and human expertise. Our expert consulting, software, and managed services address the challenges within information governance, disputes and investigations, regulatory compliance, privacy, and cybersecurity. Our solutions allow governance, legal, and risk professionals to locate, access, analyze, and manage information by making data transparent and actionable. Jettee helps clients in public and private sectors mitigate risk, improve productivity, and increase profitability by transforming how they use data.

Learn more at www.jettee.ai.