Arctera Insight Classification

AI-powered classification and risk detection.

Avoid an Information Crisis

The Arctera Insight Classification engine provides an unmatched level of automation and intelligence. It delivers consistent data classification built to identify risk as well as dark data standing in the way of successful data security and compliance teams. Classification is designed to automatically classify data to better enable and automate data management across your entire organization by offering scalability and performance for large amounts of data. Arctera sets the standard for classification, with hundreds of built-in policies, thousands of patterns, and full support for custom configurations.

Reduce Data Risks and Limit Sensitive Data Exposure

Classification gives you the ability to define patterns and policies using a single console no matter where the data exists within your organization's data landscape. It delivers actionable intelligence about your organization's data, so you can make more informed decisions regarding storage optimization, regulatory compliance, and data security.

Arctera delivers classification via the following features:

- Over 1,400 pre-trained patterns to detect sensitive data types and behaviors, such as bribery, financial distress, outside business activities, auto-generated email, subscriptions/newsletters, social security numbers, credit card numbers and medical records

- Supports Natural Language Processing AI to include built-in features such as Sentiment Analysis and language detection featuring 35 language detection policies

- More than 330 preconfigured policies that align directly to GDPR, CCRA, HIPAA, PCI corporate and public governance initiatives, and other regulations relevant to different countries around the world

- Proprietary confidence scoring to minimize false positives and a built-in test tool to ensure classification accuracy

- Extensibility, so you can configure it to recognize custom data patterns such based upon keywords with nested condition logic, document matching, regular expressions, exact data match and much more

- New patterns and policies released and updated quarterly to help you stay up to date with the current regulatory environment

- All patterns and policies are created and vetted by subject matter experts in their respective fields including compliance, privacy, security and others

Automate Your Compliance and eDiscovery Needs

Classification helps to identify and eliminate the challenges posed by dark data, which often hinder data security and compliance efforts. It allows for a more efficient response to data discovery for compliance and legal purposes by simplifying the search for relevant data through the use of classification tags. Classification policies and patterns facilitate the identification of sensitive data and encompass specific policies customized to industry and government regulations to automate classification for enhanced compliance readiness.

Recognizing the importance of classification, we've integrated it deeply into our Data Compliance suite. Classification is not just an optional add-on but a central feature, essential for robust data governance and compliance. We focus on the core components that shape our platform's capabilities.

Now, let's explore how you can enhance your compliance strategies by leveraging this essential capability.

Strengthen Risk Awareness and Optimize Data Discovery

Unlocking the power of classification at the core of your data strategy enhances both risk visibility and governance efficiency. By analyzing metadata, user behavior, and content classification, organizations gain insight into potential threats and uncover hidden personally identifiable information (PII) within dark data.

With AI-driven classification, sensitive content is identified and categorized across your data landscape, supporting proactive compliance, improved preparedness, and faster response times. Integration with information governance workflows aligns classification tags with retention policies, ensuring consistent, policy-based data management. This alignment optimizes storage resources, enforces defensible data retention and expiry, and strengthens overall compliance posture.

To learn more about Arctera Insight Information Governance, visit: arctera.com/information-governance

Streamline Data Discovery and Review

Using advanced data classification, investigators can access a complete set of forensic analytics tools. This helps them quickly find and review important data for legal cases while removing unnecessary information. Through classification, we can prioritize identifying and examining essential data for your case while efficiently filtering out irrelevant information.

Classification also plays a vital role in protecting sensitive and privileged documents, reducing the risk of accidentally revealing confidential information. With our eDiscovery service, you can navigate through data sets with accuracy, ensuring compliance and confidentiality at every stage.

To learn more about Arctera Insight eDiscovery, visit: arctera.com/compliance/ediscovery

Enhance Supervision and Communication Oversight

Integrating classification with surveillance enables proactive monitoring and management of communications across email, chat, voice, and collaboration platforms. By applying AI-driven sentiment analysis, pattern recognition, and language detection, compliance teams can quickly identify risky behavior, policy violations, or potential misconduct. Classification ensures relevant content is captured for review while filtering out noise, improving accuracy, and strengthening overall compliance readiness.

To learn more about Arctera Insight Surveillance, visit: arctera.com/surveillance