

FACT SHEET

Protect Analytics AI™ for Relativity

An AI-Enabled Sensitive Data Detection, Identification,
and Visualization Toolset from HaystackID®

HAYSTACK®



AI-Enabled Sensitive Data Management: A Deep Dive into HaystackID's Protect Analytics AI for Relativity

Protect Analytics AI for Relativity, developed by HaystackID, offers an innovative solution to the complex problem of managing vast, unstructured datasets, particularly those containing sensitive information like PII, PHI, technical data, and entities. The AI-enabled platform can precisely identify and classify a wide array of internationally sensitive data types and entities. Integration with Microsoft® Power BI® enables users to benefit from interactive visualizations that facilitate efficient data sorting, querying, and analysis. It also provides customizable risk categories, assisting users in managing potential data breaches and overall risk. Further enhancing its utility, the Protect Analytics AI for Relativity presents a sensitive data density score to immediately focus on the most sensitive documents within a dataset. Thanks to its extensibility and scalability, the solution is optimized for use within Relativity, suitable for on-premise or cloud-based environments, and capable of evolving alongside your organization's needs.

Offering Benefits

- Advanced Data Detection and Classification
- Interactive Visualizations
- Customizable Risk Categories
- Sensitive Data Density Scoring
- Extensibility and Scalability

Protect Analytics AI for Relativity is a sophisticated toolset offered by HaystackID that includes AI-enabled tools for the precise detection, swift identification, and interactive report visualization of sensitive information directly into Relativity.

Microsoft, Azure, and Power BI are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product and company names mentioned herein may be trademarks of their respective owners.

From Challenge to Solution: Considering Sensitive Data

Managing vast, unstructured datasets, particularly those encompassing sensitive information like PII, PHI, technical data, and entities, is a formidable challenge in the digital age. HaystackID responded to the growing need for efficient, comprehensive mechanisms for sensitive data management, leading to the inception of Protect Analytics AI for Relativity.

Protect Analytics AI for Relativity deploys advanced artificial intelligence capabilities to confront this challenge effectively. It is carefully constructed to identify diverse internationally sensitive data types. These encompass globally pertinent PII/PHI, such as age, gender, religion, employment, ethnic group, and more than 140 sensitive data types specific to different regions.*

**Regional Sensitive Data Support: The United States, United Kingdom, Argentina, Australia, Belgium, Brazil, Canada, Chile, China, Columbia, Croatia, Denmark, France, Finland, Germany, Hong Kong, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Mexico, The Netherlands, New Zealand, Norway, Paraguay, Peru, Poland, Portugal, Singapore, South Africa, Spain, Sweden, Thailand, Turkey, and Venezuela*

Moreover, Protect Analytics AI for Relativity can precisely detect credentials and secrets** and distinguish entities, such as people, places, and organizations. This facilitates the swift identification of sensitive data populations, accelerating notifications to an individual or organization in compliance with most jurisdictions.

***Detection of Credentials and Secrets: Authentication Tokens, AWS Account Access Keys, Microsoft Azure® Certificate Credentials for Application Authentication, HTTP Authentication Headers, Encryption Keys within configuration files, code, or log text, Google Cloud API Keys, Google Cloud Service Account Credentials, JSON Web Tokens, HTTP Cookies, OAuth client secrets in configuration files, JSON, URLs, or other text, Clear Text Passwords in Configuration Files, Weakly Hashed Passwords, XSRF Tokens, SSL Certificates IMEI Hardware IDs, IMSI IDs MAC Addresses, URLs and Storage Signed URLs, and IP Addresses.*

Protect Analytics AI for Relativity integrates robust, interactive visualizations via Power BI directly into Relativity, allowing users to effortlessly sort, query, and analyze fielded data for quick interrogation, classification, and remediation. It assigns each sensitive data classifier a customizable risk category, enabling users to filter data types according to medical, high, and low-risk categories. It also provides a sensitive data **DENSITY SCORE** to focus immediately on the most sensitive documents within a given data set.

Additionally, this solution uses various internal and external processing techniques and machine learning models to classify*** documents comprehensively and individual entries in those documents. It is intended for classifying large, unknown corpora of documents.

****Enterprise Specific Categories: Source Code, Finance Documents, Resumes, Blank Legal Form Templates, Legal Briefs, Legal Court Orders, Law Documents Containing the Text of a Law or Regulation, Legal Pleadings, Patent or Patent Application Documents, System or Application Log File, and Database Backup Files.*

Protect Analytics AI for Relativity Benefits Snapshot

- **Advanced-Data Detection and Classification:** Utilizing state-of-the-art AI capabilities, Protect Analytics for Relativity can identify and classify a broad array of sensitive data types, including but not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), technical data, and specific entities such as people, places, and organizations. *This feature not only enhances data management and security but also aids in regulatory compliance.*
- **Interactive Visualizations:** The integration with Power BI provides robust, interactive visualizations right inside Relativity. *This enables end-users to easily sort, query, and analyze fielded data for rapid interrogation, classification, and remediation.*
- **Customizable Risk Categories:** Each sensitive data classifier is assigned a customizable risk category, allowing users to filter medical, high, and low-risk data types. *This granularity facilitates more targeted, efficient data breach notification and overall risk management.*
- **Sensitive Data Density Score:** The system calculates a sensitive data density score, which guides end users to immediately focus on the most sensitive documents within a given data set. *This feature helps prioritize the data review process, saving time and resources.*
- **Extensibility and Scalability:** Protect Analytics for Relativity uses a CLR-based architecture, permitting integration of any process using a wrapper, connector, or direct implementation of the algorithm. Furthermore, it can be deployed in either on-premise or cloud-based environments thanks to the ASP.NET core running in a containerized setting. *This extensibility and scalability make it a solution that can grow and evolve alongside an organization's needs.*

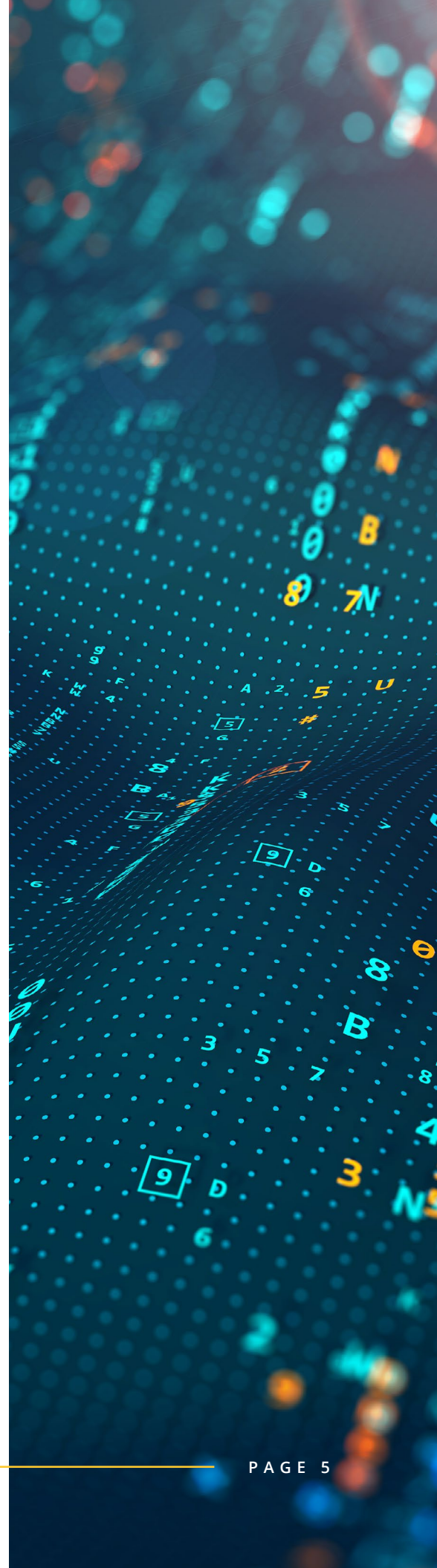
Real-World Success: Protect Analytics AI in Action

Protect Analytics AI for Relativity has empowered numerous clients across multiple sectors and geographies to classify and handle their sensitive data more effectively in hundreds of engagements.

One example involved a large Europe-centric telecommunications company that experienced a security incident involving both unstructured and complex structured data. The organization engaged HaystackID's global cyber discovery and incident response practice to analyze terabytes of data that was known to have been exfiltrated by the threat actor, in addition to other data that had potentially been compromised to determine the scope of the incident, the extent of compromised file repositories, and what (if any) access to PII/PHI, trade secrets, and other sensitive data the threat actors were able to obtain.

Although the client's infrastructure was incapacitated, many of its human resources were offline, and limited guidance was available from the client's SMEs as to the function and content of each database, HaystackID analyzed hundreds of individually structured data repositories, each comprised of millions of rows of data.

HaystackID deployed its Protect Analytics AI offering, which allowed the investigation to occur in a secure, scalable, and high-speed environment. In turn, the HaystackID team was able to quickly identify the most sensitive data affected by the incident. HaystackID's combination of leading-edge technology and human expertise resulted in a complete analysis of hundreds of millions of rows of data in less than 72 hours. The HaystackID team further identified and segregated specific record sets containing sensitive PII for further analysis and privacy review.



HaystackID's cyber, privacy, and incident response teams devised and documented a defensible method-based approach to significantly reduce the potential time and cost associated with reviewing all of the potentially affected data. Using HaystackID's Protect Analytics AI platform, the approach provided regulators with an acceptable alternative to line-by-line analysis while also providing the client with a faster and more cost-effective solution overall. Additionally, advanced visualizations delivered via Protect Analytics' Power BI integration allowed key client stakeholders to visualize exceptionally dense tranches of sensitive data for triage early on in the engagement. Early visualizations also allowed the legal team to gain insight into the potential location of data subjects impacted by the breach. This ultimately allowed them to understand early their global regulatory obligations across almost 80 jurisdictions where data subjects were impacted.

HaystackID worked closely with in-house and outside counsel as well as the company's own cyber incident-response team to learn from the incident by using the HaystackID team's output to assess ongoing and future privacy risks on a global scale. With that review, HaystackID was able to help the company reassess, revise, and restructure policies and practices to mitigate the risk of future incidents.

The project was successful in many ways. HaystackID's use of its Protect Analytics AI and deployment of its cross-functional team of forensics, cyber discovery, incident response, privacy, and data science professionals saved the client a great deal of money (millions of pounds) while also allowing them to respond effectively in establishing breach reporting timeframes to various regulators. In addition, HaystackID's efforts provided an opportunity for the company to build on lessons learned from the incident, setting it up for future success.

Protect Analytics AI for Relativity is a testament to HaystackID's commitment to providing robust, efficient, and comprehensive data protection solutions. Leveraging AI's power, Protect Analytics AI for Relativity aids in effectively classifying and safeguarding sensitive data, enabling end users to make risk-based judgments with confidence and precision, thus keeping organizations secure and compliant. As we continue to evolve with the ever-changing digital landscape, we remain dedicated to advancing and refining our tools to provide industry-leading solutions for document classification and data protection that are interoperable and integrated with Relativity.

Learn More. Today.

[Contact us today](#) to learn how HaystackID's cyber, privacy, and incident response teams can help empower your organization to effectively classify and manage sensitive data with Protect Analytics AI for Relativity.

About HaystackID®

HaystackID is a specialized eDiscovery services firm that supports law firms and corporate legal departments and has increased its offerings and expanded with five acquisitions since 2018. Its core offerings now include Global Advisory, Discovery Intelligence, HaystackID Core™, and artificial intelligence-enhanced Global Managed Review services powered by ReviewRight®. The company has achieved ISO 27001 compliance and completed a SOC 2 Type 2 audit for all five trust principles for the second year in a row. Repeatedly recognized as a trusted service provider by prestigious publishers such as Chambers, Gartner, IDC, and The National Law Journal, HaystackID implements innovative cyber discovery services, enterprise solutions, and legal discovery offerings to leading companies across North America and Europe, all while providing best-in-class customer service and prioritizing security, privacy, and integrity. For more information about its suite of services, including programs and solutions for unique legal enterprise needs, please visit HaystackID.com.