TAG

SPECIAL ANALYST REPORT

TOP FIVE DATA DISCOVERY AND CLASSIFICATION VENDORS

2025

big·id next

SPECIAL ANALYST REPORT

TOP FIVE DATA DISCOVERY AND CLASSIFICATION VENDORS – 2025

PREPARED BY THE TAG ANALYST TEAM
www.tag-infosphere.com

LEAD ANALYST: DR. EDWARD AMOROSO
Chief Executive Officer, TAG Infosphere[1]
Research Professor, NYU[2]
eamoroso@tag-cyber.com

Version 1.0
2025

This TAG Analyst Report features the TAG Top Five vendor BigID in the area of Data Discovery and Classification for 2025 based on TAG's evaluation criteria..

BigID specializes in Data Discovery and Classification through its advanced, AI-driven platform, which automates the process of identifying sensitive and regulated data across structured and unstructured data sources. BigID's platform provides extensive metadata tagging, categorization, and data mapping capabilities, helping organizations understand what types of data they hold and where it is located. BigID's solution is particularly strong in supporting compliance requirements, offering granular data classification that aligns with regulations like GDPR, CCPA, and HIPAA, making it a powerful tool for organizations prioritizing data privacy and security.

[1] *TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science/sustainability for enterprise teams, government agencies, public policy lawmakers, academic researchers, and commercial vendors. See* ***https://www.tag-infosphere.com/****.*

[2] *NYU's Center for Cybersecurity (CCS) is an interdisciplinary academic center in which leading edge cybersecurity research, teaching, and scholarship are directed into meaningful real-world technology, platforms, and policies. See* ***https://www.cyber.nyu.edu/****.*

INTRODUCTION

Data discovery and classification are foundational processes in data security and governance, designed to help organizations identify, catalog, and categorize their data assets. With data residing across multiple environments—on-premises, cloud, and hybrid—having visibility into where sensitive data resides is crucial. Data discovery tools scan and map data assets across various storage systems, identifying data sources that may contain critical or sensitive information. This visibility allows organizations to know what data they hold, where it is stored, and whether it complies with internal and regulatory standards.

Once discovered, data classification comes into play by categorizing data based on sensitivity, risk, or business value. Classification typically involves assigning labels to data such as “confidential,” “public,” “restricted,” or “regulated,” making it easier to apply appropriate security controls. For example, financial data, personally identifiable information (PII), and intellectual property may be labeled as high sensitivity, requiring stronger protection measures. Classification is often automated using machine learning and pattern recognition, allowing large volumes of data to be categorized efficiently.

Data discovery and classification also enhance regulatory compliance by helping organizations identify and protect regulated data in line with standards like GDPR, HIPAA, and CCPA. These regulations require organizations to know where sensitive data is stored and who has access to it, and to implement adequate protection measures. By discovering and classifying data, organizations can identify compliance-related data, enforce access controls, and generate reports to demonstrate compliance.

Beyond security and compliance, data discovery and classification support better data management. When organizations know what data they have and how it is classified, they can make more informed decisions on data storage, retention, and usage. For example, data that is deemed low-sensitivity or redundant can be archived or deleted, freeing up storage space and reducing infrastructure costs. Classification also facilitates efficient data sharing within the organization by ensuring that employees can access only the data they need for their roles.

Finally, data discovery and classification play a critical role in reducing the risk of data breaches and insider threats. By knowing where sensitive data resides and who has access to it, organizations can implement more targeted access controls and monitor usage patterns for potential anomalies. In the event of an attack, having pre-classified data allows for a faster and more effective response, as security teams can focus on high-risk areas first.

EVALUATION CRITERIA

The process for calculating a TAG Navigator to determine the aggregate CVR for a cybersecurity vendor involves ten factors. How these factors are used has evolved and is now associated with a common, normalized interpretation and scoring that is being used in various sectors including cyber insurance as a basis for reviewing the effectiveness of a vendor in reducing the cyber risk of buyers. The ten factors are as follows:

1. **Company Stage:** This references where a given vendor currently resides in the corporate lifecycle. At one end of the scale are the start-ups driven by founding teams. Mature public companies with experienced management are at the other end of the scale.

2. **Message Efficacy:** This involves the vendor’s marketing and value proposition message. At one end of the spectrum is an unclear description focused mostly on features. At the other end is a strong message of what solution is being addressed and why.

3. **Pace of Innovation:** This involves how rapidly the vendor is innovating. At one end of the scale are the vendors innovating at an impressive pace. At the other end of the scale are companies who slow innovation in favor of scale.

4. **Vision and Strategy:** This addresses whether the vendor articulates their role and purpose. At one end of the scale are vendors developing a future vision. At the other end of the scale are vendors who describe a clear vision and strategy for their company.

5. **Strength of Management:** This references whether a strong management team exists. At one end of the spectrum are companies with new managers in their first leadership roles. At the other end are companies with a mature, experienced leadership team.

6. **Strength of References:** This involves the references who can vouch for a vendor. At one end of the scale are new vendors with virtually zero customers and at the other end, we find vendors with massive global customer bases.

7. **Financial Strength:** This addresses the company's funding, revenue, and profitability. At one end of the spectrum are companies with weak near-term financial prospects. At the other end are well-funded or public companies with growing revenue and profits.

8. **Ability to Scale:** This addresses whether the solution can be provided to a large base. At one end of the spectrum are companies that struggle to support new customers. At the other end are companies with a platform that can handle rapid growth.

9. **Product Functionality:** This references whether the solution addresses the needs of its customers. At one end of the spectrum are companies with a prototype. At the other end are companies with a working solution that is thoroughly used and supported.

10. **Infrastructure Maturity:** This references whether the company is sufficiently protecting user data and ensuring proper support for customer security. New vendors are usually challenged in this area and often do not have security teams in place.

More information on these ten factors that comprise the set of criteria used in rating cybersecurity vendors is available on-demand from TAG. Research as a Service (RaaS) customers can review the justifications for ratings through their TAG RaaS portal account. They can also obtain more detailed guidance on roughly 4700 commercial cybersecurity vendors. Information on TAG RaaS subscriptions can be obtained at https://www.tag-infosphere.com/.

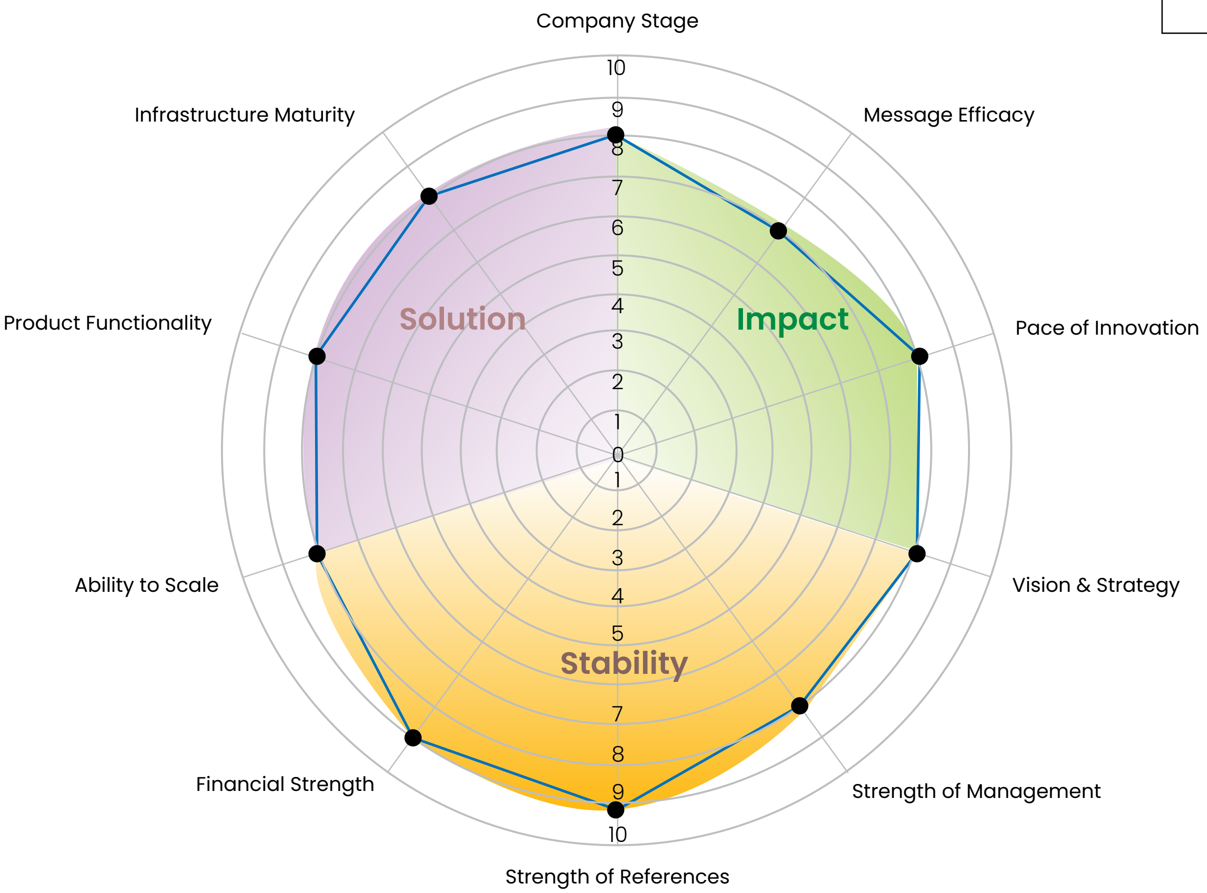
TAG TOP FIVE NAVIGATOR

DATA DISCOVERY AND CLASSIFICATION PLATFORM

TOP-TIER VENDOR PROFILE

BIGID

10
CVR
RATING
8.1
0



BBigID supports enterprise cybersecurity by providing robust data discovery and classification tools that allow organizations to locate, understand, and protect sensitive data across complex data environments. Its platform uses advanced machine learning to automatically scan and discover data from structured, semi-structured, and unstructured sources, enabling companies to gain visibility into all data assets across cloud and on-premises locations. By identifying where sensitive information resides, BigID empowers organizations to make informed security decisions and reduce data-related risks.

With its data classification capabilities, BigID helps organizations categorize data based on type, sensitivity, and regulatory requirements, including standards like GDPR, CCPA, and HIPAA. The platform offers customizable classification policies that can detect and label personal, financial, and health information, ensuring that data is properly identified and managed. This enables companies to establish robust data access controls, apply relevant security policies, and align data handling with compliance mandates.

BigID further enhances enterprise cybersecurity by integrating discovery and classification with data governance and risk management tools, allowing for a more comprehensive approach to data protection. Through continuous monitoring, BigID alerts security teams to unusual access or data movement, which could indicate security threats.

Methodology: The TAG Navigator uses 10 factors to assess vendor's solutions. Each factor represents a key aspect of the solution's value and has been deemed by TAG as a reasonable predictor of its success in the discipline. TAG's Cyber Vendor Ratings (CVR) factors are rated on a scale of 1-10. The solution analyzed above has been selected by TAG as a top-tier solution within the discipline.

TAG

SPECIAL ANALYST REPORT

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, and artificial intelligence.

tag-infosphere.com

big·id next

ABOUT BIGID

BigID empowers organizations to connect the dots across data & AI: to know their enterprise data and take action for data-centric security, privacy, compliance, AI innovation, and governance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

bigid.com