TAG

SPECIAL ANALYST REPORT

TOP FIVE NARRATIVE THREAT INTELLIGENCE VENDORS

2025

BLACKBIRD.AI

SPECIAL ANALYST REPORT

TOP FIVE NARRATIVE THREAT INTELLIGENCE 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 Blackbird.AI in the area of Narrative Theat Intelligence Management for 2025 based on TAG's evaluation criteria..

Blackbird.AI leverages advanced artificial intelligence and natural language processing to provide digital risk protection by detecting and mitigating harmful narratives, disinformation campaigns, and coordinated influence threats targeting executives and organizations. Their platform helps monitor digital ecosystems for reputational risks, ensuring high-profile individuals are protected from manipulative information that could damage their public persona or brand integrity.

[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

Modern enterprises face the increasingly sophisticated threat of deepfakes and disinformation. Deepfakes, generated using AI and machine learning, create hyper-realistic but fabricated audio, video, or images. When combined with disinformation—deliberately false or misleading content—these tools can manipulate perceptions, spread false narratives, and cause reputational harm. Enterprises must now prioritize detecting and mitigating these threats to protect employees, customers, and stakeholders from misinformation and malicious attacks.

Deepfakes are increasingly used to advance social engineering attacks, such as impersonating executives in business email compromise (BEC) scams or manipulating voice calls for financial fraud. For instance, attackers can clone an executive's voice or likeness to authorize unauthorized wire transfers or gain access to sensitive information. Such incidents can result in direct financial losses, data breaches, and compliance violations. Enterprises need to adopt AI-based detection tools that analyze speech patterns, video artifacts, and other inconsistencies to identify fraudulent deepfake content.

Disinformation campaigns targeting enterprises can spread rapidly through social media, undermining public confidence in a company's brand, products, or leadership. Fake press releases, manipulated videos, or misleading images can be leveraged by competitors, activists, or cybercriminals to trigger stock price drops, customer distrust, or regulatory scrutiny. Enterprises must implement tools that monitor and detect disinformation in real time while establishing crisis response strategies to address and debunk false claims.

The rise of deepfakes and disinformation highlights the need for robust awareness training for employees and customers. Enterprise teams are often the first line of defense, and they must learn to recognize deepfake content and question suspicious communications. Organizations should integrate deepfake detection into cybersecurity awareness programs, emphasizing vigilance when receiving unexpected messages, video calls, or media files.

Combating deepfakes and disinformation requires advanced AI-driven solutions capable of detecting subtle inconsistencies in synthetic media. Tools that leverage machine learning algorithms, image forensics, and metadata analysis can help enterprises identify manipulated content with high accuracy. Additionally, monitoring platforms that detect disinformation campaigns in real time can prevent narratives from escalating.

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

NARRATIVE THREAT INTELLIGENCE

TOP-TIER VENDOR PROFILE

BLACKBIRD.AI

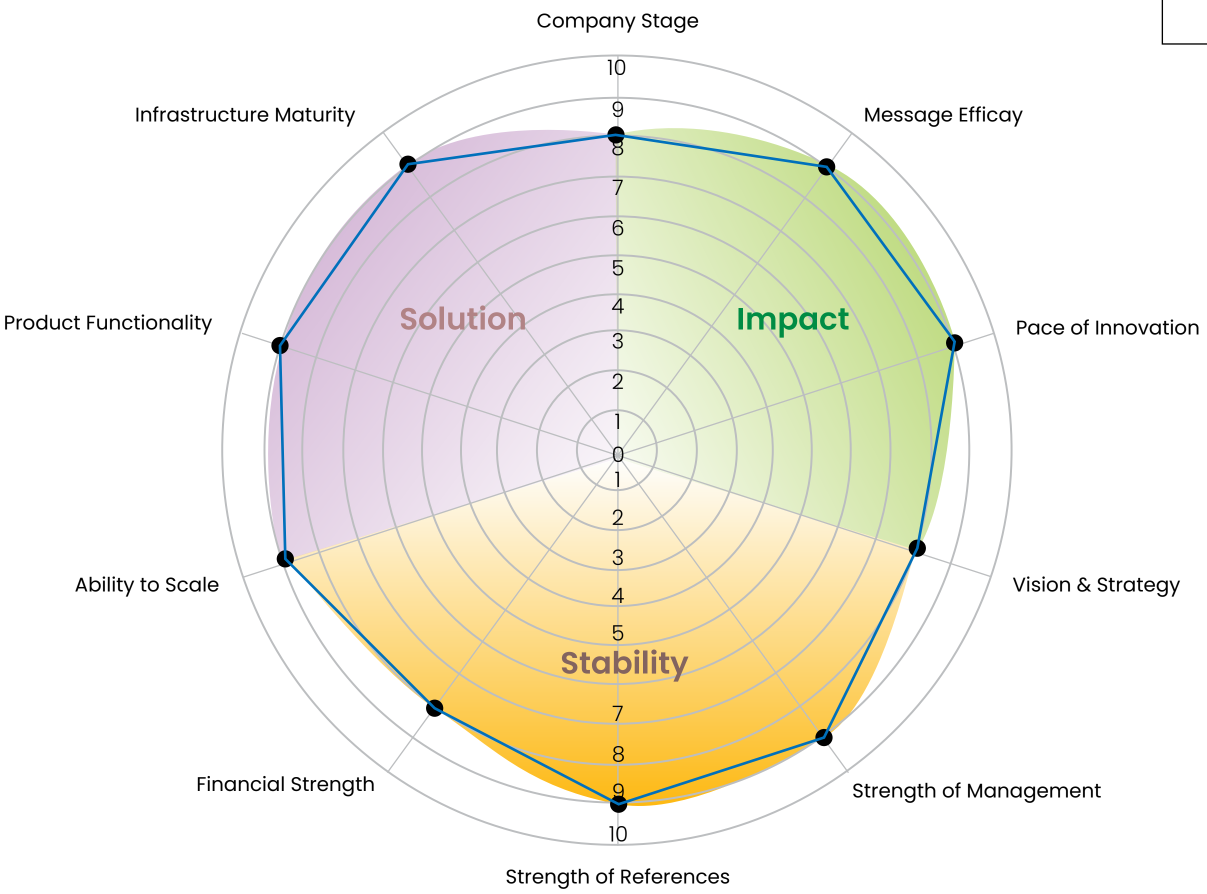
10

CVR

RATING

8.7

0



Blackbird.AI delivers a powerful platform for detecting disinformation and deepfakes through the use of artificial intelligence, natural language processing, and advanced network analysis. The platform scans vast amounts of online data, including social media platforms, news outlets, and communication channels, to identify signs of manipulated content and coordinated disinformation campaigns.

A unique feature of Blackbird.AI's platform is its ability to analyze the behavioral patterns and digital footprints of actors involved in spreading disinformation. By mapping networks of fake accounts, bots, or organized campaigns, Blackbird.AI provides actionable intelligence that allows enterprises to neutralize threats before they escalate.

The platform generates comprehensive reports with detailed insights that enterprise teams can use to address reputational risks, respond to media threats, and protect key stakeholders from manipulation.

Blackbird.AI's solution is designed to scale across industries, enabling companies to monitor for risks specific to their business domains. For example, in finance, healthcare, and public relations, the platform helps organizations detect and counter false narratives that could disrupt operations or damage trust. Through AI-powered monitoring and reporting, Blackbird AI equips enterprise teams with the tools needed to combat sophisticated disinformation threats and reduce cyber risks effectively.

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, artificial intelligence, and climate science.

tag-infosphere.com

BLACKBIRD.AI

ABOUT BLACKBIRD.AI

Blackbird.AIprotects organizations and executives from narrative attacks that cause financial and reputational harm. Our AI-driven Narrative Intelligence Platform identifies key narratives that impact your organization/industry, the influence behind them, the networks they touch, the bot behavior that scales them, and the cohorts and communities that connect them. This information enables organizations to make better strategic decisions to reduce risk, especially during times of crisis.

blackbird.ai