TAG

SPECIAL ANALYST REPORT

TOP FIVE DEEPFAKE/ DISINFORMATION DETECTION VENDORS

2026

GetReal

SPECIAL ANALYST REPORT

TOP FIVE DEEPFAKE/DISINFORMATION DETECTION VENDORS – 2026

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

2026

This TAG Analyst Report features the TAG Top Five vendor GetReal Security in the area of Deepfake/Disinformation Detection for 2025-2026 based on TAG's evaluation criteria..

GetReal Security focuses on real-time, multimodal identity defense to identify deepfakes and AI-generated deception and verify authenticity. Combining AI and machine learning, content analysis, continuous authentication, and adaptive enforcement, GetReal protects trust in digital interactions. Their technology analyzes forensic artifacts within visual and audio data – including inconsistencies in pixels, facial movements, and speech cadence – to detect synthetic content. This helps enterprises stop GenAI-powered identity threats, identify disinformation campaigns, and protect brands, customers, and employees.

[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/.

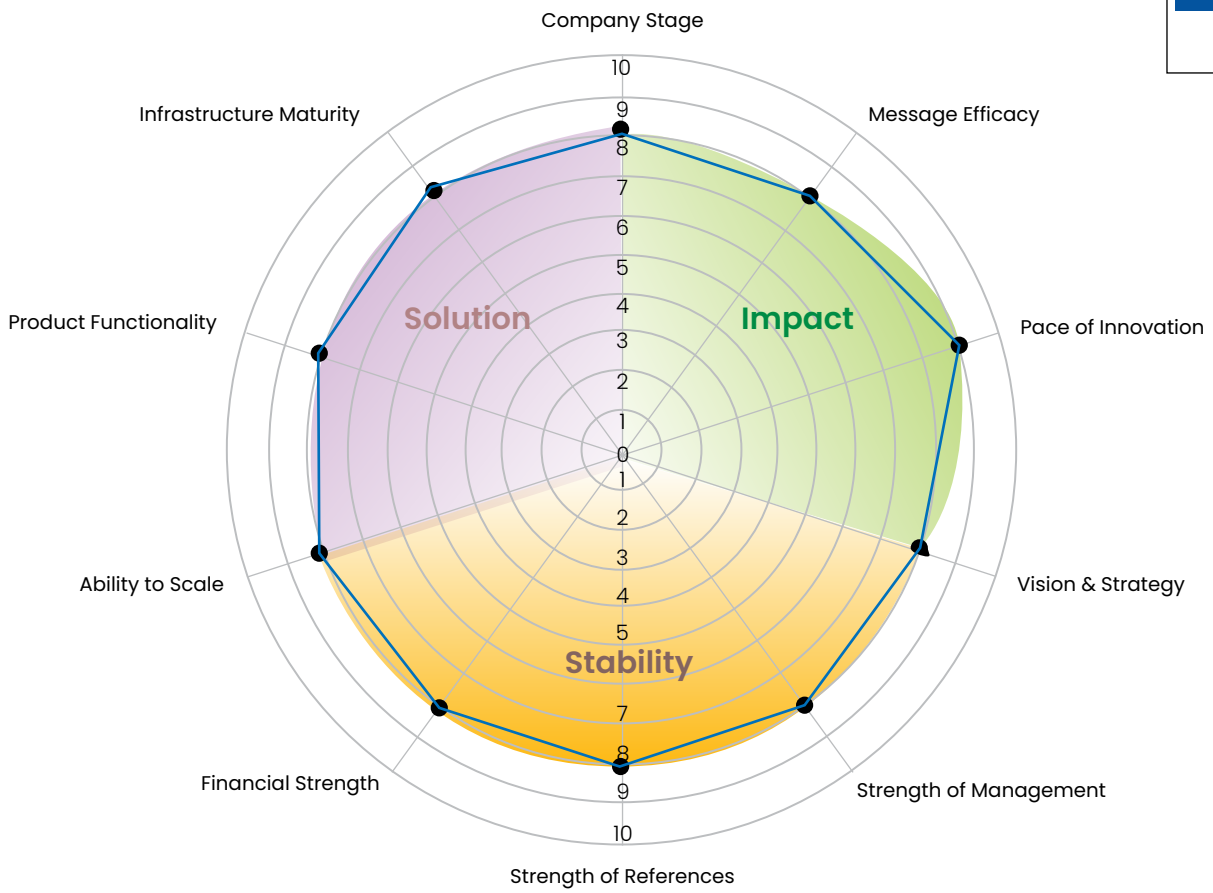
TAG TOP FIVE NAVIGATOR

DEEPFAKE/DISINFORMATION DETECTION PLATFORM

TOP-TIER VENDOR PROFILE

GETREAL SECURITY

CVR RATING 8.1 (10 / 0)



GetReal Security employs advanced artificial intelligence and machine learning techniques to detect deepfakes, imposters, digital identity attacks, and manipulated content. Their solution focuses on analyzing subtle anomalies in digital media, such as visual inconsistencies in lighting, texture, and facial symmetry, as well as irregularities in audio cadence. By leveraging these forensic methods, GetReal Labs can accurately identify synthetic media that may not be obvious to the human eye with explainable, defensible evidence.

In addition to its multimodal deepfake detection capabilities, the GetReal platform integrates with existing enterprise workflows to deliver actionable insights, identity assurance, and threat reporting. Beyond flagging manipulated content, the platform ensures the identity on the other side of video and voice interactions are who they claim to be through biometric checks. GetReal also enables real-time security policy enforcement to respond to anomalies, block suspicious interactions, and mitigate active threats. Threat intelligence and an identity threat graph further strengthen these capabilities by mapping identity relationships, flagging repeat attackers, and giving security teams visibility into identity-driven attacks—ensuring customers, employees, and stakeholders are not misled by harmful or fraudulent content.

GetReal Security also supports education and awareness initiatives for enterprise teams by providing training tools that demonstrate the growing sophistication of deepfake technologies. By improving organizational understanding of how manipulated media can undermine operations, GetReal helps businesses develop comprehensive strategies to counter emerging 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.

©2025 TAG Inphosphere, Inc.

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

ABOUT GETREAL SECURITY

GetReal Security protects enterprises against AI-powered digital identity threats. Our platform combines advanced AI with world-class digital forensics to verify images, audio, and video to detect and mitigate deepfakes, impersonation, and synthetic identity fraud in real time. We defend user identities while strengthening trust across digital communications and workflows.

getrealsecurity.com

Copyright © 2025 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere's written permission. The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.