Emerging Tech: AI Vendor Race: Eroding Digital Trust Threatens the Global Economy, Forcing Adoption of Digital Trust and Authenticity Platforms

5 March 2026 - ID G00840381 - 12 min read

By: Alfredo Ramirez IV, Apeksha Kaushik

Initiatives: Technologies and Markets; Strategy, Risks and Opportunities

> Disinformation is reaching crisis levels globally, and by 2027, the majority of digital media will be synthetic rather than human-created. Digital trust and authenticity platforms will rebuild trust in digital content, disrupting the industrialized disinformation supply chain that threatens businesses, governments and society.

Overview

Opportunities

- C-level leaders have the opportunity to make their products business-essential by enabling organizations to adopt a media zero trust (MZT) approach, where media is assumed to be fake unless authenticated to be real. Digital trust and authenticity platforms (DTAPs) will be at the center of making decisions or taking actions based on the content, narratives or identities represented in digital media.
- Product leaders must urgently transition from offering point solutions to developing consolidated DTAPs by deciding whether to build or partner for capabilities in content authenticity, impersonation prevention, and narrative intelligence.
- To secure near-term market adoption, product leaders must align their strategy with the emerging business imperative for “trust operations” (**TrustOps**) by positioning their DTAPs as central systems of record.
- Product leaders must proactively architect their platforms with robust digital provenance and disclosure features to ensure long-term compliance with impending global transparency legislation.

Recommendations

- Achieve business-essential status for your products by enabling organizations to adopt a media zero trust (MZT) approach, leveraging DTAPs to authenticate digital media before making decisions or taking action based on its content, narratives, or identities.
- Assert market leadership by transitioning from point solutions to consolidated DTAPs, either by building or partnering for capabilities in content authenticity, impersonation prevention, and narrative intelligence.
- Increase near-term market adoption by aligning product strategy with the emerging imperative for TrustOps, positioning DTAPs as the central systems of record for digital trust and authenticity.
- Position for long-term compliance with emerging global transparency legislation by proactively architecting platforms with robust digital provenance and disclosure features.

Strategic Planning Assumptions

Trust in digital content is so important that, in 2030, enterprises will spend more than $25 billion authenticating it.By 2027, more than 70% of all digital content will be synthetic, making it as important to prove what is true as to detect what is false.

Analysis

Technology Definition

Digital trust and authenticity platforms (DTAPs) bring together the primary features of **disinformation security**, which include content authenticity, impersonation prevention, and narrative intelligence, for the dual purposes of alerting on what is fake and authenticating what is real. Previously, these features have been separate point solutions. DTAPs bring these together to disrupt what has become an industrialized disinformation supply chain that threatens businesses, governments and society.

While a true DTAP remains a future state, the following sample represents a nonexhaustive list of vendors that have gone to market with capabilities from more than one of the below-described disinformation security feature areas.

Sample Vendors

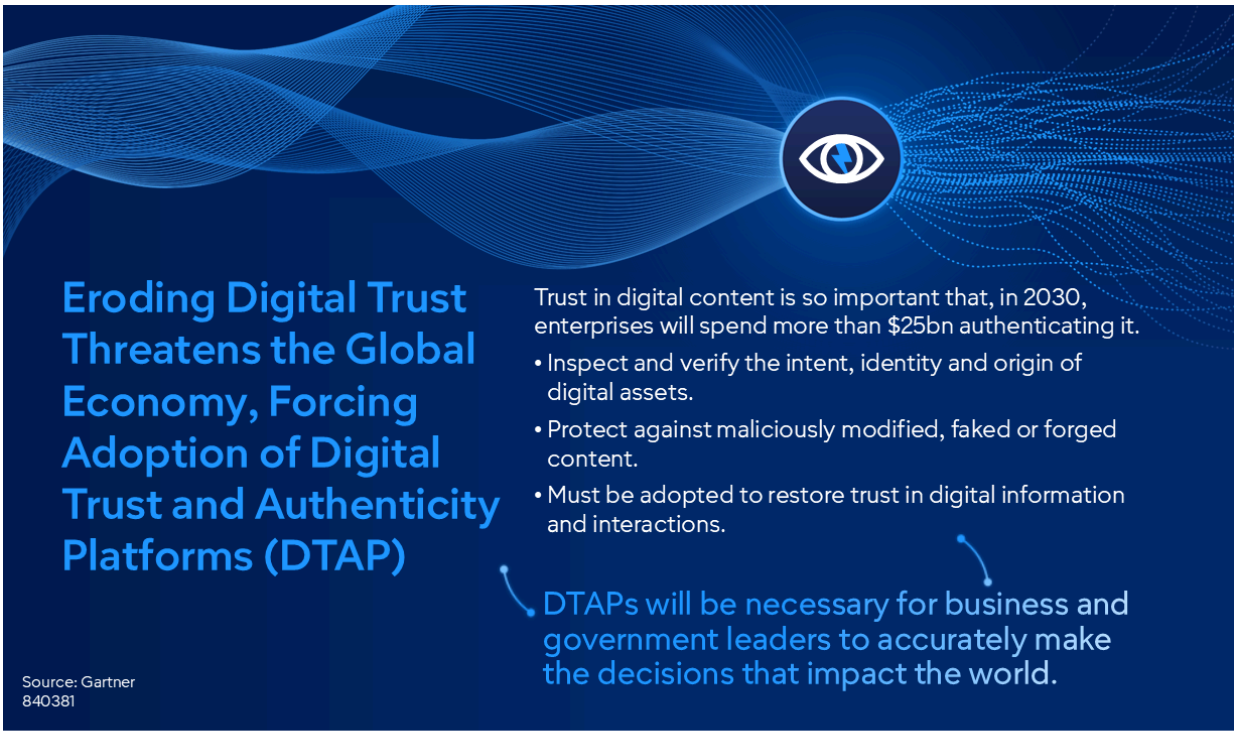
Alto Intelligence, Blackbird.AI, Brinker, Cyabra, DeepTrust, Doppel, GetReal Security, IdentifAI, Pindrop

Table 1: Disinformation Security Features and Capabilities

Features	Content authenticity	Impersonation prevention	Narrative intelligence
Capabilities	■ Content credential analysis ■ Multimodal deepfake detection ■ Manipulated media analysis ■ Pixel analysis and heat mapping	■ Biometric analysis ■ Behavioral analysis ■ Name, image and likeness monitoring ■ Identity graphing	■ Attacker and target attribution ■ Platform contagion and spread ■ Bot-based amplification attribution ■ Intent analysis

Source: Gartner (March 2026)

Figure 1: Top Disruptor: Digital Trust and Authenticity Platforms (DTAPs)



- *We have effectively entered a world without truth, in which it will be increasingly impossible to operate a government, company, or organization without an effective DTAP in place.*
- *It is currently cheaper and easier for bad actors to create and deploy deepfakes and disinformation than it is for the average person, or even a leader, to access reliable digital trust and authenticity tools. DTAP access must become as ubiquitous as issuing an organizational email address for every individual.*
- *The internet itself will segment into untrusted areas and organizational TrustNets, which are collaborative and technologically advanced trust networks among organizations with capabilities designed to publish and consume reliable information (see Emerging Tech Impact Radar: Disinformation Security).*
- *Organizations will need to stand up trust operations, or TrustOps, as an additional capability, not an extension of existing cybersecurity or GRC. TrustOps should be governed in each enterprise by a trust council that uses TrustNets to guarantee the provenance, accuracy, chain of custody and audit trail of inbound and outbound content.*

The Industrialized Disinformation Supply Chain

Disinformation has evolved into a global, industrialized threat, amplified by generative AI that enables large-scale, low-cost influence operations and impersonation attacks. Media platforms lack incentives and capability to regulate synthetic content, while policy and enforcement for digital authenticity remain underdeveloped worldwide. As a result, organizations must independently safeguard their operations. DTAPs offer a technological solution to counter the industrialized disinformation supply chain.

News and Media Outlets

Legitimate news outlets must adopt DTAPs to authenticate their content and debunk false claims, ensuring audiences receive accurate information. Meanwhile, fake news sites mimic credible sources to legitimize and spread disinformation, influencing public opinion and market behavior. As attackers increasingly use synthetic media, integrating DTAPs into journalistic practices is essential for both validating authentic reporting and detecting falsified sources.

Entertainment & Celebrity

Fake celebrity endorsements, scandals, or statements can be rapidly created and disseminated, while intellectual property theft involving unauthorized use of name, image, likeness (NIL), and voice is increasingly common. To address these risks, DTAPs are essential for monitoring narratives and verifying media to detect and prevent NIL violations.

Cybersecurity

Security operations centers (SOCs) traditionally focus on protecting organizational systems such as networks, endpoints, and data. With the rise of deepfake-enabled social engineering attacks, DTAP signals must be integrated into cybersecurity tools and understood by practitioners, representing a significant shift in cybersecurity products, services, and practices.

Government

Governments face growing challenges in maintaining election integrity and preventing the malicious misrepresentation of leaders and policy issues, as generative AI makes it easier for individuals and organized groups to rapidly spread disinformation on a global scale. The threat is heightened by adversarial state actors who can now effortlessly translate and localize disinformation across languages and regions, making cross-border influence operations a persistent and credible risk to public safety.

Legal

Legal systems now face the "liar's dividend," where individuals may dismiss authentic video or audio as deepfakes to evade accountability, impacting any legal proceeding involving digital evidence. There is an increasing need to distinguish real victims from synthetic content and to identify which portions of partially synthetic media are authentic. In this context, DTAPs are essential for analyzing large volumes of digital evidence and supporting investigations and prosecutions.

Now (0 to 1 years): DisinfoSec Feature Consolidation

The DisinfoSec market is undergoing rapid consolidation, as point solutions for content authenticity, deepfake detection, impersonation prevention, and narrative intelligence are increasingly being integrated into consolidated DisinfoSec and digital trust and authenticity platforms. This trend is driven by the urgent need for comprehensive solutions that address multiple facets of digital threat and authenticity. Vendors lacking the resources or strategic intent to internally develop or acquire these capabilities are instead seeking partnerships, often leveraging managed service providers to deliver DTAP capabilities. As a product leader, it is crucial to decide whether to invest in expanding in-house capabilities or to pursue strategic alliances to remain competitive in this evolving landscape.

The Near-Term Horizon (1 to 3 years): DTAP Becomes Business Essential

To remain competitive in the evolving DTAP market over the next one to three years, you should proactively align your product strategy with the emerging business imperative for trust operations. Begin by anticipating the rise of TrustOps teams, trust councils, and chief trust officer (CTrO) roles, ensuring your platform supports board-level reporting needs. Position your DTAP as the central system of record to combat disinformation, monitor narratives, and preempt incidents. Finally, invest in market education highlighting the dangers of trusting unauthenticated content, which must be viewed as unreliable by default — making comprehensive DTAP integration a critical requirement for your customers.

The Medium-Term Transition (3 to 8 years): DTAP Becomes Society Essential

In three to eight years, the DTAP market will be shaped by new legislative requirements, such as the California AI Transparency Act, mandating the disclosure of digital provenance data by online platforms, device manufacturers, and generative AI providers. As similar regulations are adopted across other states and countries, compliance will become a baseline expectation for market participation. Product leaders must prepare for an internet landscape that bifurcates between open platforms, where synthetic content is permitted, and emerging TrustNets, which prioritize authenticated and reliable content. To stay ahead, you prioritize building robust provenance and disclosure features, ensure your DTAP can adapt to diverse regulatory environments, and position your platform as a trusted backbone for compliance and the creation of new, trusted digital ecosystems.

The Long-Term Future (8+ Years): DTAP as a Utility

Beyond eight years, DTAP capabilities will become foundational societal infrastructure, as essential to delivering trusted information as water treatment plants are to delivering potable water. Telecommunications providers will routinely screen all forms of content, including audio, text, and video, before transmission, establishing this as a standard practice for commercial channels. Product leaders must prepare to deliver platforms that offer scalability and transparency required of critical utilities, ensuring your solutions can serve as the backbone for trusted digital engagement across all sectors of society.

Certified Media and Content — Internet bifurcates Into the Internet of TrustNets Versus Everything Else

- *DTAP functionality will enable trusted networks, TrustNets, to exist that only allow verifiable authenticated content. This should be the only content relied on to make consequential decisions.*
- *Other parts of the internet will continue to be available where content authentication is not required.*
- *New parts of the internet will be created entirely for the sharing of generated content.*
- *Efforts like the Coalition for Content Provenance and Authenticity (C2PA) and Google SynthID are continuing to gain momentum out of the necessity to prove the provenance of digital content.*
- *Digital capture devices will begin to more broadly adopt digital source type provenance indicators, for example: Google Pixel 10 Phone supporting C2PA joins Leica Camera AG, Sony Alpha, Canon EOS, and Nikon Z6III.*

Legal and Regulatory — Legal Necessity for Products and Services to Authenticate Evidence

- *Questioning the authenticity of any digital media submitted as legal evidence becomes the first line of every defense attorney requiring legally sanctioned DTAP for evidence admission in courts of law around the world.*
- *Regulatory uncertainty increases as some governments race ahead, and others wait and see, to define and enforce new standards. This will increase the need for legal and regulatory advisory in cases of digital authenticity.*
- *Name, image and likeness (NIL) concerns around misuse are escalating as celebrities are being deepfaked in endorsing products, services and political positions that they have not agreed to.*
- *Opportunities for legal specialty over defamation, impersonation, related to synthetic content.*

Healthcare — DTAP for Departments of Health, Prescription and Medication Vendors and Telemedicine

- *Disinformation about treatments, vaccines, or medical professionals will require DTAP for departments of health around the world.*
- *DTAP will be required for systems that issue prescription lenses and medications over digital channels based on uploaded documentation.*
- *Impersonation of doctors or health officials in telemedicine or via mass media channels is a concern.*

Organizations — Rise of the Chief Trust Officer (CTrO) and Trust Councils

- *CTrO is a role that exists at some organizations but is still relatively underutilized. This role should grow to own the budget and solutions that all organizations face because of the rise in disinformation and related dangers.*
- *Trust councils will be necessary to have representation from various stakeholders across an organization.*

Cybersecurity — Presignals and AI to Combat AI

- *Cybersecurity tools will need to ingest signals from DTAPs to meet the increasing threats.*
- *Most security operations center (SOC) teams are already inundated with data and alerts.*

- *AI SOC tools will need to be adopted by SOC teams to meet these combined challenges.*

Evidence

[1] Top 10 Examples of Deepfake Across The Internet, Hyperverge.

[2] Digital clones made by AI tech could make Hollywood extras obsolete, The Washington Post.

[3] Deepfakes and Their Impact on Society, Openfox.

[4] New Hampshire investigating fake Biden robocall meant to discourage voters ahead of primary, AP News.

[5] British engineering giant Arup revealed as $25 million deepfake scam victim, CNN Business.

[6] The TAKE IT DOWN Act: A Federal Law Prohibiting the Nonconsensual Publication of Intimate Images, Congress.gov.

[7] Why detecting dangerous AI is key to keeping trust alive in the deepfake era, World Economic Forum.

[8] Google's New AI Tool Generates Convincing Deepfakes of Riots, Conflict, and Election Fraud, TIME; Scholarly Commons, Boston University School of Law.

Notes

Historical Context

2022

- OpenAI releases ChatGPT and DALL·E 2.
- Stable Diffusion is released.
- Midjourney released.

- U.S. “Deepfake Task Force Act” introduced with aims to address national security risks from synthetic media but not passed into law.2022 — A deepfake video of Ukrainian President Volodymyr Zelenskyy was broadcast on a hacked Ukrainian TV station. The video showed him appearing to call on his soldiers to surrender to Russian forces, quickly debunked by an official video message. This was a significant early example of deepfakes being used for political warfare and disinformation during an active conflict. [1]

2023

- OpenAI releases GPT-4; Google launches Bard; Meta releases Llama.
- Midjourney continues to improve its AI image generation models.
- EU Digital Services Act (DSA), which mandates transparency and accountability for online platforms regarding disinformation and synthetic content2023 — Deepfakes became a major issue in the U.S. actors’ guild, SAG-AFTRA, strike due to concerns about the use of AI to create and store digital likenesses of actors. [2] The number of deepfakes shared online reportedly grew to over 500,000 video and voice deepfakes. [3]

2024

- **Multimodal AI** models (text, image, audio) become publicly available
- Enhanced AI tools for video generation and editing are released such as OpenAI’s Sora and Google’s Veo
- Open-source **generative AI** models see rapid advancement
- Content Authenticity Initiative (CAI) provides a push for digital watermarking and provenance tracking
- U.S. and EU propose stricter laws on AI-generated content and election interference2024 — China enacts rules requiring clear labeling of AI-generated media. A deepfake robocall using a convincing AI-cloned voice of President Joe Biden was sent to voters in New Hampshire. [4] London-based engineering and design firm, Arup, was targeted via a Hong Kong-based employee in a deepfake video call scam that resulted in a loss of over $25 million. [5]

2025

- Google's Veo 3 is released
- Google's Gemini 2.5 Flash Image (Nano Banana) is released
- TAKE IT DOWN act becomes law [6]2025 — Veo 3 publicly enables hyperrealistic text to video generation coupled with native synchronized audio, dialogue and sound effects. Gemini 2.5 Flash Image (Nano Banana) publicly enables the creation and manipulation of images with very little technical effort. It can maintain character consistency between edits making things like face swapping and background changes simple text to image or drag and drop operations.According to reports, financial losses from deepfake fraud in North America exceeded $200 million in Q1 2025. [7] TIME magazine demonstrates use of Veo 3 to create convincing deepfake videos of regional conflict, disease conspiracy and election fraud. [8] 2025 marks the year that technology has enabled anyone to create convincing media of anything or anyone else, at low or no cost, with low or no technical ability.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Data View: What Is the Impact of GenAI on the Attack Landscape?

Emerging Tech Impact Radar: Disinformation Security

Emerging Tech: AI Vendor Race: Disinformation Security Products Must Be Part of Cybersecurity

Table 1: Disinformation Security Features and Capabilities

Features	Content authenticity	Impersonation prevention	Narrative intelligence
Capabilities	■ Content credential analysis ■ Multimodal deepfake detection ■ Manipulated media analysis ■ Pixel analysis and heat mapping	■ Biometric analysis ■ Behavioral analysis ■ Name, image and likeness monitoring ■ Identity graphing	■ Attacker and target attribution ■ Platform contagion and spread ■ Bot-based amplification attribution ■ Intent analysis

Source: Gartner (March 2026)