

Red Points launches Deepfake Protection to detect and take down AI-generated videos impersonating public figures

The new solution combines honeypot agents, facial and voice recognition, behavioural analysis, and NLP to find and remove impersonation infringements.

NEW YORK, NY, UNITED STATES, July 21, 2026 /EINPresswire.com/ -- [Red Points](#), the AI-against-AI

“

A year ago, this was a problem for politicians and celebrities. Today, we're seeing cases from executives and public figures who never thought they'd be a target.”

Laura Urquizu, CEO and President of Red Points

company protecting over 1,300 brands worldwide, today announced the launch of Deepfake Protection, a service that detects and eliminates AI-generated videos that impersonate a public figure's likeness for fraudulent purposes.

Coverage spans TikTok, Instagram, X, Facebook, and YouTube, and applies to videos distributed both as advertisement and organic content.

The shift in who gets targeted is notable. [Deepfake impersonation](#) was, until recently, associated almost

exclusively with political figures and global celebrities. Red Points' own client base points to a broader pattern: actors, athletes, artists, influencers, and executives at large and mid-sized companies, known to international or regional audiences, increasingly find themselves managing their first case, having never previously considered themselves a plausible target. Cases have surfaced across sectors including financial services, sports, and entertainment, among others.

"A deepfake doesn't have to be perfect to be dangerous, it just has to be convincing enough for the moment it's shared – but they are getting close to perfect," said Laura Urquizu, CEO and President of Red Points. "A year ago, this was a problem for politicians and celebrities. Today, we're seeing cases from executives and public figures who never thought they'd be a target."

"Confirming who's in a video and understanding what they're being made to say are two different problems, and you need both to know whether something's actually dangerous. We've spent years building and refining computer vision and language models side by side for exactly these kinds of cases, so neither piece is bolted on, they're built to work together from the start," said David Torrejon, Chief Product Officer at Red Points.

Solving Deepfake Detection and Enforcement

Deepfake Protection combines two functions. The first is detection: infringers operate in a deliberately volatile environment engineered to evade it —rotating creatives, disposable ad accounts, short-lived campaigns— and in video-native formats (reels, shorts) where titles, captions, and hashtags carry little or no exploitable text signal. Flagging an incident the moment it surfaces is therefore an adversarial problem: the metadata traditional monitoring relies on is thinning out.

Deepfake Protection overcomes this with layered detection. On top of keyword and reverse-image search, it deploys honeypot discovery agents that match the exact victim profile each fraud campaign targets by geography, age, and interest signals. By feeding those signals into each platform's recommendation and ad-delivery systems, the agents cause the fraudulent organic posts and paid ads to be served to them directly.

The second function is enforcement, where the challenge is scalability and accuracy at once: automation is what makes takedowns viable at volume, but volume is also what makes false positives expensive — wrongly flagging legitimate or parody content erodes trust and invites counter-notices. Red Points resolves this tension through its broader brand-protection stack. It draws on computer vision technology refined over years of identifying minor visual nuances and manipulated content —trained on more than 2.7 billion data points processed every month— plus an orchestration of voice analysis, NLP, and risk models. This layer contextualizes each video, validates fraudulent intent —separating a genuine scam from protected or incidental use— and triggers cease-and-desist actions automatically.

About Red Points

Red Points is the AI digital risk company delivering fully managed protection against counterfeits, impersonation, and piracy at scale.

Trusted by more than 1,300 organizations, Red Points combines AI trained on 2.7 billion data points each month with over a decade of enforcement expertise. Its Brand Knowledge Layer tailors decisions to each brand, threat, and platform, while safe AI automates high-volume work and IP experts continuously adapt the system as threats evolve.

With 250+ professionals across New York, Barcelona, Beijing, and Salt Lake City, Red Points combines global expertise and scalable technology to protect brands and executives from digital threats.

Sergi Garcia

Red Points

comms@redpoints.com

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.