TrendAI™

SOLUTION BRIEF

TRENDAI VISION ONE™

Deepfake Detector

Detect and block synthetic media threats in real time to protect identities, data, and trust.



Confronting AI-driven deception head-on

Deepfakes, AI-generated media that replicate real voices, faces, and behaviors, pose an escalating threat to individuals and organizations. Our latest report on the AI criminal toolkit reveals how these forgeries enable executive impersonation, targeted extortion, and large-scale misinformation campaigns. As this technology becomes more realistic and widely accessible, traditional security measures struggle to keep pace with it. This leaves organizations like yours vulnerable to sophisticated synthetic threats that demand adaptive defenses.

TrendAI Vision One™ Deepfake Detector

TrendAI Vision One™ enhances your organization with advanced deepfake detection for live, interactive environments, such as conference calls, virtual meetings, and one-on-one video sessions on platforms like Microsoft Teams, Google Meet, and Zoom. Currently supported on Microsoft Windows OS, you have the ability to analyze audio and video streams in real-time. Ensure every participant is authentic and block manipulated content before it can disrupt communication or compromise trust. Leverage targeted protection to protect critical conversations and preserve the integrity of your organization's virtual engagements.

Part of the TrendAI Vision One™ industry-leading AI security platform

Enable your organization to enforce deepfake detection seamlessly across endpoints by harnessing the power of TrendAI Vision One™ Endpoint Security. By unifying this policy with threat response and visibility in a single console, you're enabled to streamline protection for critical assets. Seamlessly integrate with existing security layers and third-party tools to extend this unified approach across IT and OT environments. Deliver actionable insights to help your organization anticipate and counter emerging threats.

Beyond detection, TrendAI Vision One™ Cyber Risk Exposure Management (CREM) allows you to strengthen every layer of defense natively with TrendAI Vision One™ XDR for Endpoints and TrendAI Vision One™ Zero Trust Secure Access (ZTSA). Proactively neutralize deepfake-driven attacks and reinforce trust in every interaction.

KEY BENEFITS:

- Stop deepfakes before they cause harm
- Strengthen trust in every digital interaction
- Detect scams and impersonations with AI precision
- Protect identities with real-time audio and video analysis
- Stay ahead of evolving threats with continuously updated detection models

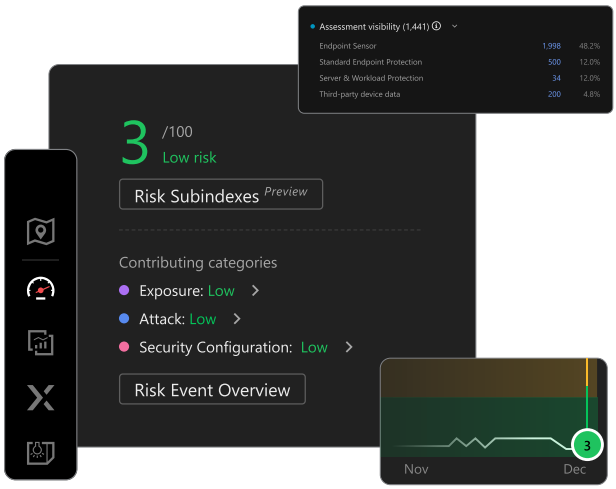
TrendAI™ Vision One

Industry-Leading AI Security Platform



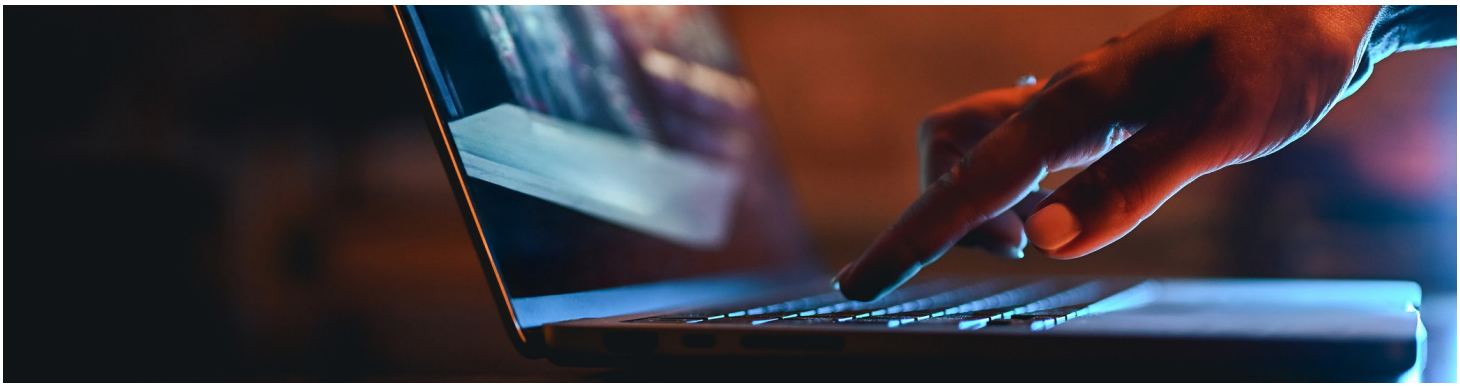
AI Fearlessly

TrendAI Vision One™ is the only enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection to help you predict and prevent threats, accelerating proactive security outcomes.



Ready to see Deepfake Detection in action?

Request a demo to see how our tools work in real time.
Contact us to schedule a consultation with a security expert.
Get started at TrendMicro.com/VisionOne.



How it works

TrendAI Vision One™ gives you access to its deepfake detection policy when a participant's camera is turned on, ensuring protection during live video interactions. Leverage advanced AI and machine learning techniques to identify subtle signs of media manipulation across both video and audio streams, including:

Face-swapping and face-reenactment detection

Utilize advanced deep learning algorithms and convolutional neural networks (CNNs) trained on extensive datasets of real and synthetic media to detect:

- **Spatial-based patterns**, including artifacts such as inserted objects, inconsistencies in skin tone, hair, lighting, and distortions in facial structure
- **Frequency-based patterns**, including high-frequency components generated during image manipulation, which are often missed by pixel-level analysis

Synthesized audio identification

Detect fake audio, such as voice deepfakes commonly used in scam calls, through deep learning models trained to identify:

- **Time-domain patterns**, which analyzes unnatural tone, cadence, and volume compared to authentic voices
- **Frequency-domain patterns** based on generated noise that is imperceptible to the human ear

INDUSTRY LEADERSHIP

- Disclosed 73% of vulnerabilities in the market, Omdia Research
- Leader in 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms 20 times
- Leader in IDC MarketScape: Cloud-Native Application Protection Platform 2025 Vendor Assessment
- 100% analytic coverage across all major attack steps in the 2025 MITRE ATT&CK® Evaluations

About TrendAI™

TrendAI™, a business unit of Trend Micro™ and global AI security leader, makes the world safer for digital information exchange across enterprises, governments, and organizations. Powered by security expertise and innovation, TrendAI™ leverages artificial intelligence to protect over 500,000 enterprises and millions of individuals across AI, cloud, networks, endpoints, and devices. AI Fearlessly. TrendMicro.com

Copyright ©2026 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo, the t-ball logo, TrendAI Vision One are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. Trend Micro, the Trend Micro logo, and the t-ball logo Reg. U.S. Pat. & Tm. Off. TrendMicro.com
[SB00_Deepfake_Detection_Solution_Brief_260120US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy

Start free trial of TrendAI Vision One™

Learn more at trendmicro.com