SURF SECURITY LAUNCHES WORLD'S FIRST AI DEEPFAKE DETECTING BROWSER

LONDON, UNITED KINGDOM, November 20, 2024 /EINPresswire.com/ -- SURF Security, has today launched the beta of its neural net powered deepfake detection tool for customer testing. The SURF Deepwater deepfake detector tool is built into the SURF Security Enterprise Zero-Trust Browser® and defends enterprises, media organisations, police, and militaries around the world from AI deepfake threats. It can detect with up to 98% accuracy whether the person you're interacting with is a real human or an AI imitation, alerting users to potential deepfake threats within seconds.

> SURF's Deepwater deepfake detector is the first truly useable, real-time defence against deepfakes."
> *Ziv Yankowitz, SURF Security's CTO*

AI deepfakes are being used by threat actors to cause huge financial losses. For example the South China Morning Post reported on a 'first-of-its-kind' $25 million theft involving an AI deepfake impersonation of the CFO of a multinational corporation. Forty nine percent of the world's population lives in a country holding a national election this year, and AI deepfakes are being used to spread misinformation and sway political outcomes. Recent examples include fake phone calls purporting to be from US President Joe Biden, and a damaging fake recent election-timed video of UK politician Wes Streeting.

As generative AI tools get more powerful and easier to use, the risk from deepfakes is accelerating at an alarming rate. According to recent research, deepfake scams have grown by 303% in the USA year-on-year, and even faster in countries such as Portugal (1700%), China (2800%), Singapore (1100%), and myriad others. Individuals have also been defrauded with thefts of thousands of dollars caused by terrifying AI scams using a loved one's voice.

SURF Security's deepfake detector can protect against such threats and will work with any audio source within the browser, including online videos or communication software such as Slack, Zoom, Google Chat, Microsoft Teams, and WhatsApp etc. Users will simply need to press a button to verify if audio – recorded, or live – is genuine or AI generated.

"SURF's Deepwater deepfake detector is the first truly useable, real-time defence against deepfakes," said Ziv Yankowitz, SURF Security's CTO. "To maximise its effectiveness, we focused on accuracy and speed. The tool's neural network is trained using deepfakes created by the top AI voice cloning platforms, has an integrated background noise reduction feature to clear up audio prior to processing, and can make a determination in less than 2 seconds. Of course, AI

voice cloning software becomes more capable by the day, so like all of cybersecurity, we are committing to winning an ever-evolving arms race."

“The rise of AI-based deepfakes presents significant security challenges for organisations, which can lead to reputation damage, data loss, regulatory non-compliance, and financial losses. SURF Security’s AI Voice Detector addresses the challenge right at the user interaction layer - the Browser, which could substantially reduce incident rates without having to invest in yet another deepfake detection tool,” said Swetha Krishnamoorthi, Industry Principal, Cybersecurity, Frost & Sullivan. "This capability is crucial for entities such as governments, politicians, customer service centres, and C-suite executives, providing robust protection against deepfake-driven cyber threats and safeguarding brand integrity."

“Deep fakes are in use today by criminal gangs that leverage the technology as part of their confidence scams that attempt to defraud individuals and companies. That’s why deep fake detection built into Surf’s secure enterprise browser is an exciting and vital feature for enterprise end-users,” said Jarad Carleton, Global Research Director, Cybersecurity, Frost & Sullivan.

SURF Security uses military-grade AI deepfake detection technology that runs on emerging technologies such as State Space Models that can detect deepfakes across languages and accents by modeling probabilistic relationships between audio frames to show inconsistencies. This allows for high speed and high accuracy, even with audio clips as short as a single second. SURF Security will also add AI image detection to the browser’s toolkit in the future.

SURF intends to work with industry to improve existing open-source databases of deepfake audio and videos. Any media, law-enforcement, companies or organisations interested in protecting themselves from deepfakes can sign up for the beta programme here: https://www.surf.security/deepfake

The full product is expected to launch in Q1 of 2025.

Melanie Johnson-Holliday / Tara Antoni
Eskenzi PR
email us here
Visit us on social media:
LinkedIn