SURF Security
71-75, Shelton Street, Covent Garden, London, WC2H 9JQ, UK
447 Broadway, 2nd Floor Suite #1365, New York, New York 10013, USA

SURF

FACT SHEET

SURF SECURITY DEEPWATER - DEEPFAKE DETECTION TOOL

Browser feature unique to SURF Security's Enterprise Zero Trust Browser® defends against scams and deepfakes

Introduction

In an era of rapidly evolving artificial intelligence (AI), deepfakes have emerged as a significant threat to individuals and organizations alike. Deepfakes are synthetic media, often in the form of videos or audio recordings, that convincingly replace a person's likeness or voice with someone else's. These manipulated media can be used for malicious purposes, such as spreading misinformation, manipulating public opinion, or perpetrating financial fraud.

SURF Security, a leading cybersecurity company, has developed a groundbreaking AI-powered deepfake detection feature to combat this growing threat.

What is SURF Security's Deepwater?

SURF Security's Deepwater deepfake detector tool is a browser-based tool that leverages advanced neural networks to identify and flag potential deepfakes in real-time. It is designed to work seamlessly with various audio sources within a browser, including online videos, communication software (e.g., Slack, Zoom, Microsoft Teams), and social media platforms.

Key Features and Benefits

- **High Accuracy:** The Deepfake Detector boasts an impressive accuracy rate of up to 98% in detecting AI-generated voices.
- **Real-time Detection:** The tool can analyse audio streams and identify potential deepfakes within seconds, enabling users to take immediate action.
- **Wide Compatibility:** The Deepfake Detector is compatible with any audio sources and communication platforms that run within the browser.
- **Ease of Use:** The tool is integrated into SURF Security's Enterprise Zero Trust Browser, providing a user-friendly experience.
- **Continuous Improvement:** SURF Security is committed to enhancing the Deepfake Detector's capabilities and expanding its language support to address the evolving nature of deepfake technology.

Recent Deepfake Breaches in the Press

The threat of deepfakes is not merely theoretical; it is a present and growing danger. Recent high-profile incidents highlight the potential consequences of deepfake attacks:

- **The $25 Million Deepfake Heist:** In a groundbreaking case reported by the South China Morning Post, an AI deepfake impersonation of a multinational corporation's CFO led to a $25 million theft. This incident underscores the financial risks associated with deepfakes.
- **Political Manipulation:** Deepfakes have been used to create fake phone calls and videos of political figures, aiming to sway public opinion and influence election outcomes. Notable examples include fabricated calls attributed to US President Joe Biden and a damaging deepfake video targeting UK politician Wes Streeting.
- **Personal Scams:** Deepfakes have also been employed in personal scams, where individuals are defrauded of thousands of dollars by AI-generated voices impersonating loved ones. These scams exploit the emotional vulnerability of victims, leading to significant financial losses.

The Importance of Deepfake Detection

The rise of deepfakes poses a multifaceted threat to society, undermining trust in information and eroding public discourse. Deepfake detection tools, such as SURF Security's Deepfake Detector, are essential for mitigating these risks and protecting individuals and organizations from the harmful consequences of deepfakes.

How SURF Security's Deepfake Detector Works

SURF Security's Deepfake Detector employs a sophisticated neural network trained on a vast dataset of deepfakes created by leading AI voice cloning platforms. This extensive training enables the tool to accurately distinguish between genuine human voices and AI-generated imitations.

The Deepfake Detector also incorporates a background noise reduction feature, ensuring clear audio processing for optimal detection accuracy. This feature is crucial for analysing audio recordings captured in noisy environments, where background noise could interfere with the detection process.

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 modelling 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.

Applications of SURF Security's Deepfake Detector

SURF Security's Deepfake Detector has a wide range of applications across various sectors:

- **Enterprises:** Protecting businesses from financial fraud, reputational damage, and other deepfake-related threats.
- **Media Organizations:** Ensuring the authenticity of audio and video content, combating misinformation, and maintaining public trust.
- **Law Enforcement:** Aiding in investigations, verifying evidence, and identifying perpetrators of deepfake-related crimes.

- **Government and Military:** Safeguarding national security, preventing espionage, and countering disinformation campaigns.
- **Individuals:** Protecting personal finances and reputations from deepfake scams and online impersonation.

SURF Security's Commitment to Combating Deepfakes

SURF Security is dedicated to staying ahead of the curve in the fight against deepfakes. The company is actively involved in industry collaborations to improve existing open-source databases of deepfake audio and videos. This collaborative approach fosters knowledge sharing and strengthens the collective defence against deepfakes.

SURF Security's Deepfake Detector is a pioneering solution that empowers individuals and organizations to defend against the growing threat of deepfakes. Its high accuracy, real-time detection capabilities, and wide compatibility make it an indispensable tool for navigating the complex landscape of AI-generated media.

As deepfake technology continues to evolve, SURF Security remains committed to refining its Deepfake Detector and collaborating with industry partners to ensure a safer and more trustworthy digital environment.

To learn more about SURF Security's Deepfake Detector and participate in the beta program, please visit: www.surf.security/deepfake

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

Founded in London, UK in 2022, SURF Security is an endpoint browser-SASE (secure access service edge) cybersecurity company that has created the world's first enterprise zero-trust browser and extension with security at its core. These two products capitalise on the rise of both the working-from-home phenomenon, and 'software as a service' or SaaS platforms that are used through a browser. SURF secures the browser itself, either replacing or augmenting consumer browsers such as Chrome, Edge, or Safari. This approach helps ensure compliance, defends organisations from breaches and protects users from social engineering attacks such as phishing—all on the user's device. www.surf.security

####