# RedShift Networks Advances Zero-Trust Voice Security Platform

*Enterprise platform extends voice security to combat AI-generated fraud*

RedShift Networks Advances Platform

MINNEAPOLIS, MN, UNITED STATES, August 6, 2026 /EINPresswire.com/ -- RedShift Networks, the leader in communications detection and response for internet protocol (IP) and unified communications (UC) voice security, today announced advancements in its voice security platform, designed to bring real-time threat enforcement and centralized management to the fight against the accelerating AI-driven deepfake crisis.

Employees at more than 40% of organizations have faced a deepfake, combined with social engineering, on an audio call. Deepfake identity fraud attempts have surged dramatically, by at least 2,100% globally.

> In just seconds, enterprises can lose six or seven figures. Here at RedShift Networks, we're providing the infrastructure to stop threats before they penetrate the infrastructure."
>
> *Mike Wagner, CEO*

"Despite this unprecedented growth in global threats, voice continues to be the only channel where identity is inferred rather than verified," said Mike Wagner, CEO, RedShift Networks. "Email has SPF, DKIM, and DMARC. Web traffic has TLS. Voice still trusts caller ID – an antiquated protocol that doesn't stand up against widespread spoofing."

The infrastructure that powers IP voice deepfake attacks requires automated botnet delivery, spoofed caller IDs, and compromised trunks. RedShift Networks blocks those malicious delivery vectors in real time with its industry-leading platform, featuring three integrated layers of IP and UC voice security:

- Global Threat Intelligence leverages 15+ years of proprietary data to identify bad actors and emerging threats before they reach the network.

• Call Threat Manager neutralizes six categories of voice threats before the call connects.

• Centralized Management System works as a single console to push policies, monitor health, and enforce consistent protection across every site simultaneously.

“Bad actors are exploiting voice at wire speed,” said Wagner. “In just seconds, enterprises can lose six or seven figures. Here at RedShift Networks, we’re providing the infrastructure to stop threats before they penetrate the network.”

The addition of advanced features builds on RedShift Networks’ announcement of expanding Global Threat Intelligence to global enterprises, providing every organization with access to the world’s most comprehensive voice threat identification engine.

For over 15 years, RedShift Networks has powered IP voice security for the world's largest telecommunications carriers. To learn more about RedShift Networks, visit https://www.redshiftnetworks.com.

About RedShift Networks

RedShift Networks applies security to the IP voice layer with zero trust functionality embedded in its leading communications detection and response platform – solving the AI-driven identity crisis for high-velocity communications. With a global footprint, RedShift services customers focused on high-velocity communications to stop threats before they penetrate the voice network. For more information, visit https://www.redshiftnetworks.com.

Lora Osborn
ACF Redshift
email us here
Visit us on social media:
LinkedIn