USE CASE

Healthcare System Avoids $1.4M in Potential Toll Fraud Losses

Toll Fraud Eliminated Preventing Further Financial Losses for Top-Ranking Academic Medical Center

After a significant financial loss following a breach of its voice network, a major academic medical center was in desperate need of a solution that would protect its voice channel from further attacks and identify and block any future call-threats in real time. The need for up-to-date information on telephony security threats and how to protect its patients and operations was paramount.

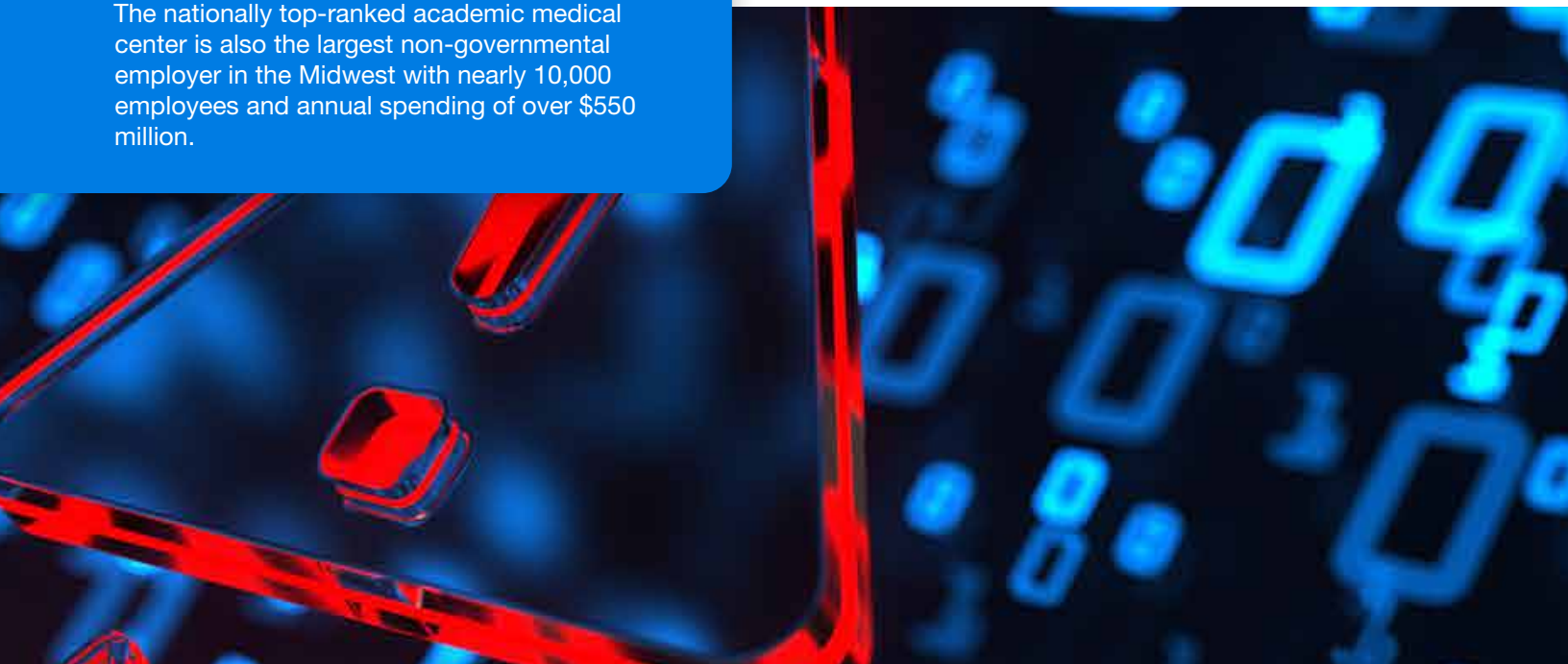
Call pumping is the practice of scammers increasing call volumes to certain telephone numbers to generate fraudulent revenue. In this case, the hackers made overseas toll calls, resulting in significant financial loss. In such a high-touch industry, medical centers must ensure that fraud risk is mitigated and that phone lines are open for legitimate business call traffic.

Business Challenge

A major medical center was losing significant revenue from toll fraud. Hackers had breached its voice system and were making overseas toll calls at $30 per minute. Over the course of six months, the client was hit with $700,000 in fraudulent toll charges. International revenue sharing fraud, also known as toll fraud, is a scheme to artificially generate a high volume of international calls on expensive routes. Fraudsters make calls to what are known as premium rate numbers and take a cut of the revenue generated from these calls.

Toll Fraud & Call Pumping

The nationally top-ranked academic medical center is also the largest non-governmental employer in the Midwest with nearly 10,000 employees and annual spending of over $550 million.



Solution

A voice network security platform, including a voice firewall and voice intrusion prevention (IPS) was deployed, along with detailed call analytics and reporting. An additional layer of protection was added to manage the identification and blocking of call threats in real-time. As a result the high-volume spoofed calls attacking the firm's voice system were stopped.

Outcome

The client avoided a potential annual loss of $1.4 million in fraudulent toll calls. The solution eliminated the toll fraud and protected the medical center's voice system from other types of fraudulent calls to patient rooms while optimizing capacity for expected business call traffic. Real-time reporting keeps the medical center staff up-to-date on telephony security threats and the measures taken to protect their patients and operations.

TNS Enterprise Voice Security can help:

- Detect and filter suspicious voice traffic
- Deliver passive caller authentication through IVR integration
- Support dynamic threat mitigation and policy enforcement
- Improve inbound call answer rates and reduced wait times for customers.
- Use metadata and behavioral analytics to evaluate caller legitimacy without disrupting legitimate interactions
- Provide real-time insights and forensic call reporting

About TNS

Established more than 30 years ago, TNS has facilitated billions of branded calls, supporting thousands of organizations across more than 60 countries. TNS has over 10 years of call identification experience and handles over 1.5 billion daily call events from over 500 operators.

To learn how TNS Enterprise Voice Security can help your business, please contact our team.

solutions@tnsi.com
tnsi.com/solutions/communications/restoring-trust-to-voice/