comviva
A TECH MAHINDRA COMPANY

↑ **175%**
1st month

↑ **367%**
2nd month

In white route traffic within.
100% in revenue with in the 1st year

ARRESTING REVENUE LEAKAGE FOR A **LEADING OPERATOR** IN **AFRICA**

The customer is one of the largest telecom company in Africa, with 13 million subscribers, accounting for more than 50 percent of the market share. It is a subsidiary of the leading service provider and one of the most admired brands in Africa.

Challenge:

→ Regain Revenue by Blocking Fraudulent A2P Messages
→ Continuous decline in A2P traffic on its network
→ Monitize A2P messaging

The operator with a subscriber base of 13 million observed a significant continuous decline in A2P traffic on its network, leading to revenue loss. Key challenge for mobile network operators is to monitor adequately, control, guard and therefore monetize their SMS traffic effectively.

Solution:

The fact that we have deep industry expertise, with two decades of rich experience; **20+ Tier**

A deployments of our firewall solution and having managed messages to the tune of **11,000 TPS** in a single deployment made us the technology provider of the choice.
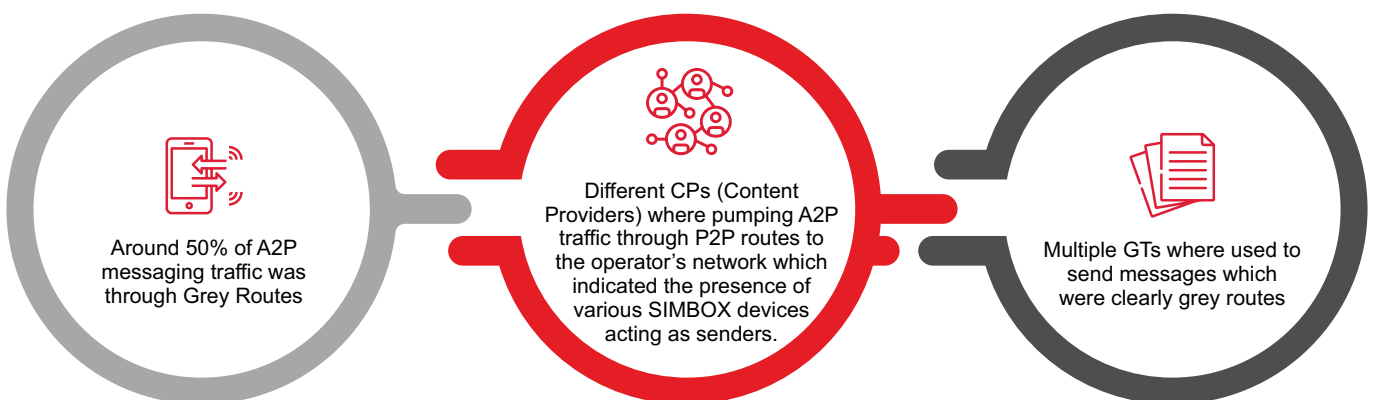
Comviva's messaging firewall platform is one of the most comprehensive network-based and content-based security solutions, enabling operators to effectively monetize A2P traffic. It leverages machine learning concepts based on neural network algorithms to auto-classify the incoming message traffic.

Once the model learns the correlation between labels and data, it starts predicting the message categories to which real-time policy decision engines apply the actions defined for each policy.

Comviva also offered business consulting and operations capability designed to ensure that the platform is operated, configured, and updated with the latest security rules on an ongoing basis.

As a first step we did deep analysis, leveraging our neural network model, to identify types of fraud and fraudsters across the operator's network and came up with following insights:

Around 50% of A2P messaging traffic was through Grey Routes

Different CPs (Content Providers) where pumping A2P traffic through P2P routes to the operator's network which indicated the presence of various SIMBOX devices acting as senders.

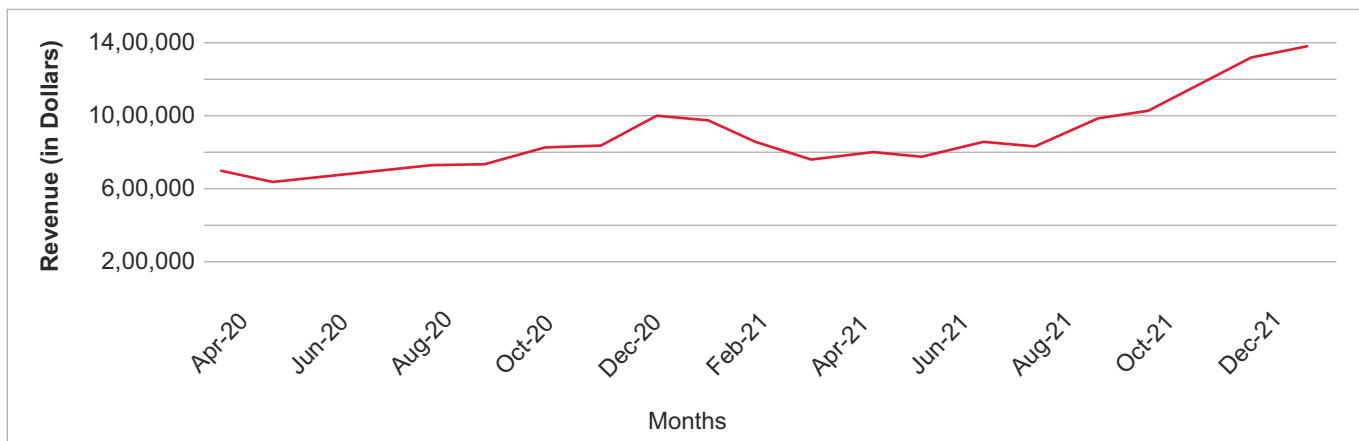Multiple GTs where used to send messages which were clearly grey routes

The real-time policy decision engine of the platform blocked the messages from the SIMBOX devices and blacklisted all those senders that appeared to be SIMBOX devices.

The neural network model was trained with newer grey route message patterns to keep the platform one step ahead of the fraudsters in terms of capturing the grey content.

Benefit:

→ An increase by **175%** in white route traffic within 1st month and **367%** in 2nd month of messaging firewall deployment.

→ An increase of **100%** in revenue within the year of messaging firewall deployment.