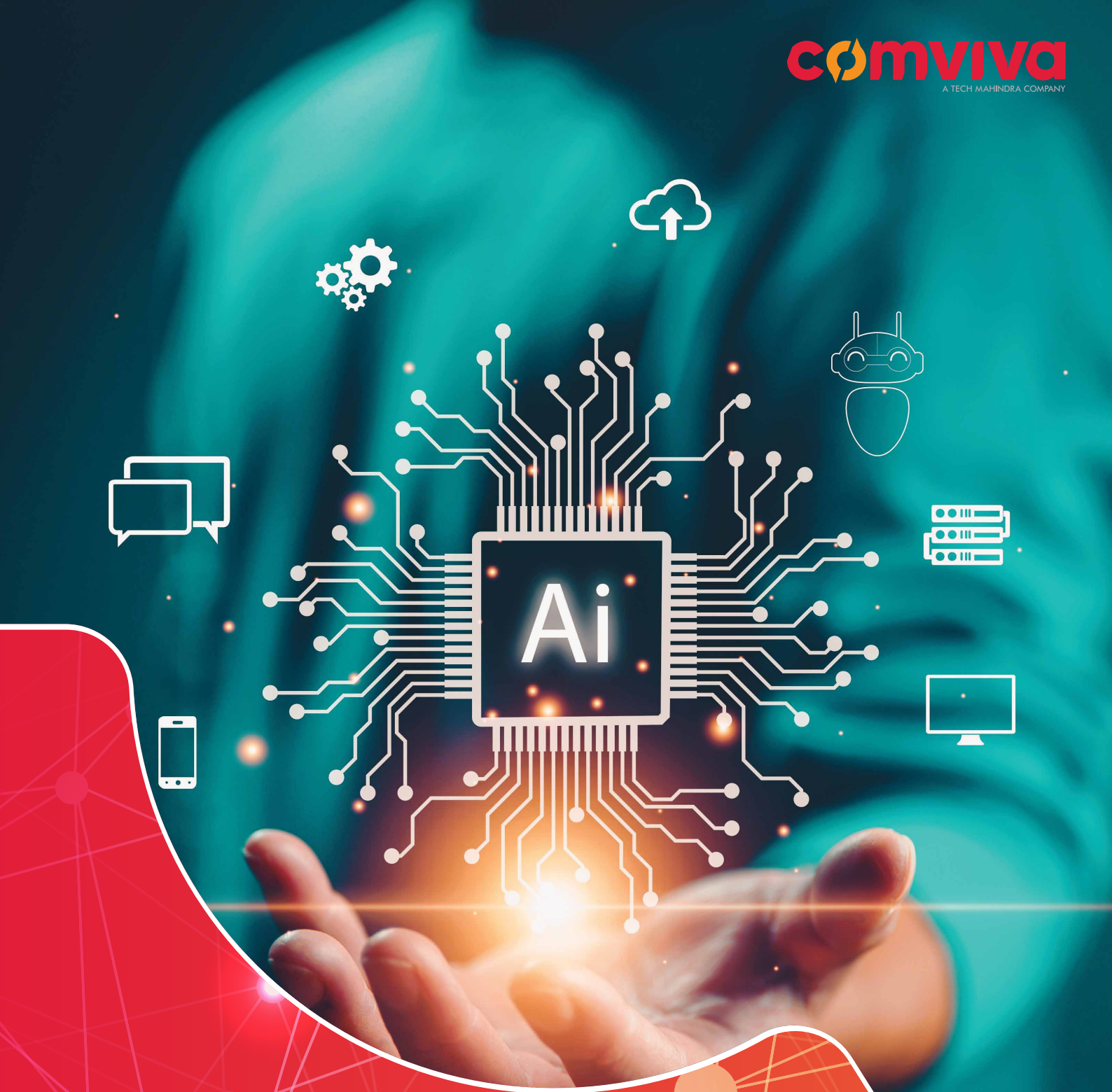
comviva
A TECH MAHINDRA COMPANY



AI Powered Messaging Firewall

Protecting Telecom Networks from SMS Frauds and Grey Routes

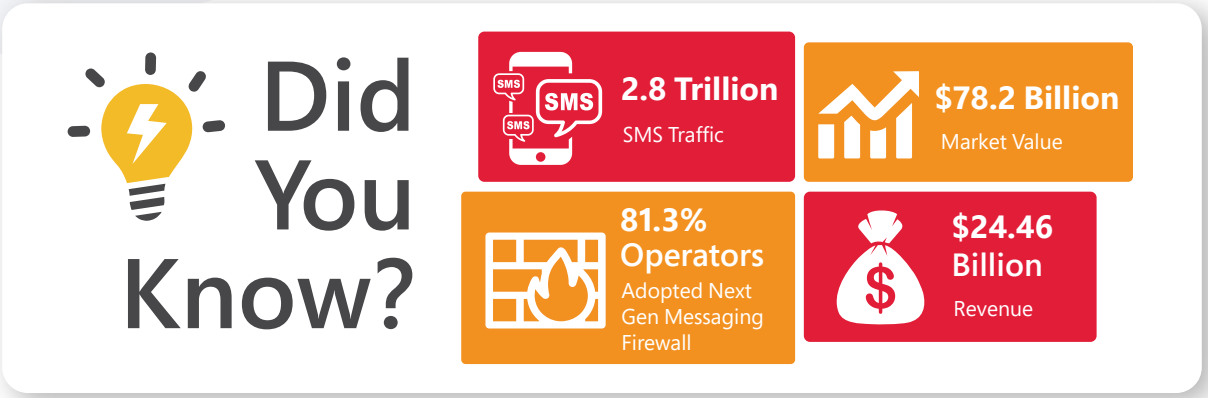
SMS FRAUD ON THE RISE

In today's digital landscape, where communication is a cornerstone of business operations, protecting operators and enterprise messaging channels is critical. SMS spam and fraud are growing threats, stealing data, infecting devices, and tricking users. Traditional firewalls struggle as attackers adapt. AI-Powered Messaging Firewall solutions offer a smarter defense, blocking evolving fraud patterns and anticipating future threats, safeguarding enterprises from financial losses, reputational damage, and operational disruptions.

Juniper Research predicts that the global SMS firewall market is predicted to reach **USD 2.98 billion in 2024 and USD 4.63 billion by 2029, growing at a CAGR of 9.2%** during the forecast period. This signifies the increasing importance of securing messaging channels.

EVOLUTION OF A2P SMS

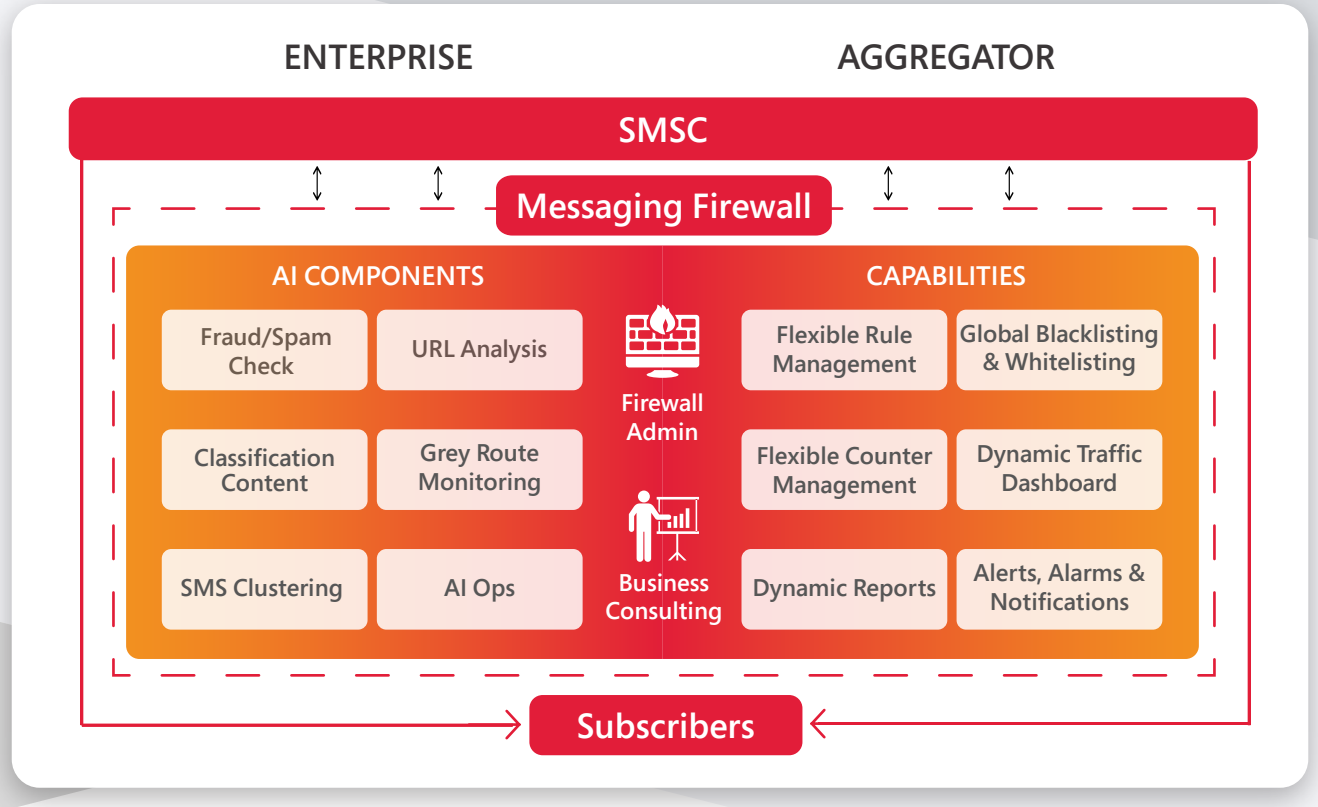
Juniper Research estimates that the A2P messaging market's value will grow from **$48 billion** in 2022 to $78.2 billion by 2027. The heavy adoption of A2P messaging by businesses is attributed to real time, automated and targeted communication between applications and individuals.



INTRODUCING MESSAGING FIREWALL SOLUTION

Comviva's Messaging Firewall offers robust network and content-based security, empowering operators to monetize A2P traffic and safeguard subscribers from network abuse. It uses real-time AI and advanced machine learning to classify SMS traffic, preventing spam and fraud, minimizing revenue loss, and reducing operational efforts.

Additionally, Comviva offers Revenue Protection and Services for optimal platform operation, providing a comprehensive solution for enhanced security and subscriber retention.



CAPABILITIES OF MESSAGING FIREWALL

Machine Learning Techniques
ML algorithms for fingerprinting commercial messages with fast changing patterns

Greater Control over Traffic
Flexible rule and counter management with content and threshold control

Reporting & Analytics
Comprehensive suite with dynamic dashboards and report builder

Content Fingerprinting
Fingerprinting with custom configuration, keyword transformation and vernacular language analysis

Domain Filtering
Inline domain/ URL analysis integrating with world renowned malicious domain list provider

Global Threat Intelligence
Access to repository of global signatures with periodic updates for proactive action

Risk and Reputation Assessment
Ascertain behavioural reputation of A2P sender to detect bad sources and arrest suspected threats

Regulatory Compliance
Adherence to GDPR regulatory compliance; Fully compliant to global industry accepted Firewall security standards such as GSMA SG.22

MESSAGING FIREWALL'S REVENUE PROTECTION & SERVICES

Messaging Firewall's Revenue Protection and Service team consists of skilled consultants with thorough knowledge of market, product and operations and assists operators in maximizing revenue.

01 ANALYTICAL SUPPORT FOR TRAFFIC MANAGEMENT

By analyzing the network traffic, Messaging Firewall's Revenue Protection and Service team helps the operator in providing platform management support. These services include penetration testing to detect any anomalies in the network and prevent revenue loss. Penetration testing tool simulates the path of SMS and detects grey routes efficiently. It also offers high brand coverage, accurate grey route detection, and automated reporting and analysis.

02 THREAT INTELLIGENCE AND CONSULTATION

The Revenue Protection and Support team helps the operator drive A2P revenues by carrying out a market assessment of the local Enterprise Messaging business opportunity and assists with the potential business value and risk.

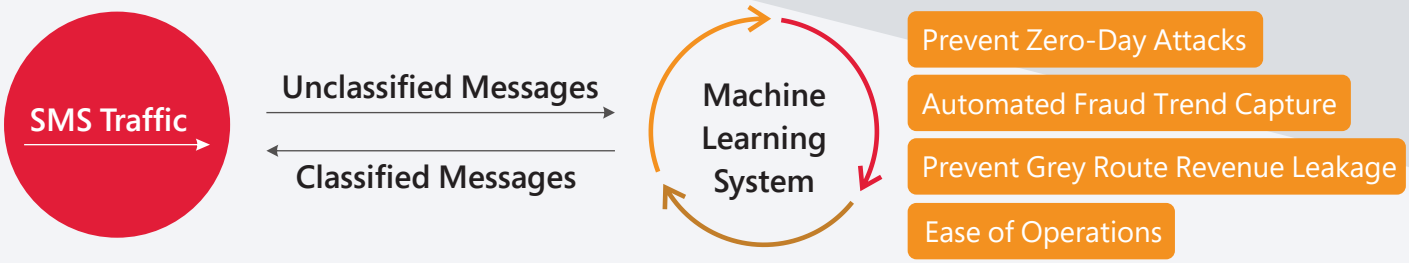
03 NETWORK AUDIT WITH GREY ROUTE PROBE

Grey Route Probe is designed to detail out potential weaknesses in an operator network with respect to cases of network fraud and grey route traffic. With a testing penetration scheme, it carries out a thorough inspection of the operator network. The analysis on results of Grey Route Probe is used by the Revenue Protection and Service team to build an action plan to curb security threats of fraud and grey route.

TRADITIONAL VS AI FIREWALL

Parameters	Static Rule-based Firewall	AI/ML based Firewall
SMS Fraud Coverage	Limited to regional SMS threats pre-configured manually as rules	Utilizes Global Threat Intelligence data providing high fraud coverage
Evolution	Limited ability to adapt to new threats. Manual effort required to update for new threats	Adapts to new threats and techniques automatically achieved with a one-time solution deployment
Response Rate	Detection of frauds conducted only after observing the fraud historically	Captures Zero-Day SMS fraud attacks
Accuracy	Limited accuracy due to static rule set	High accuracy due to machine learning algorithms
False Positives/ Negatives	More false positives/negatives due to static rule set	Fewer false positives/negatives due to advanced ML and NLP based algorithms
Performance Analysis	Performance analysis provides limited business insights	Performance is monitored in real-time that provides rich business insights of the network
Overall Support Cost	Potentially impacted due to increased fraud and spam messages	Improved due to reduced fraud and spam messages

MESSAGING FIREWALL MACHINE LEARNING FRAMEWORK



BENEFITS OF MESSAGING FIREWALL

01 | LEVERAGING AI TO ENHANCE FIREWALL CAPABILITIES

Employing Machine Learning to detect ever-evolving fraud & spam SMS patterns, capture malicious URLs and reduce manual intervention for identifying grey route.

02 | INCREASED A2P MONETIZATION

Messaging Firewall arrests grey route revenue leakages and ensures increase in A2P revenues that bypass authentic SMS routes to prevent A2P charges.

03 | HIGHER CUSTOMER SATISFACTION AND REDUCED SUBSCRIBER CHURN

AI Firewall safeguards A2P channel for brand enterprises and creates a secure space for communication resulting in reduced subscriber churn.

04 | ADHERES TO REGULATORY COMPLIANCES

Empower your Telco with our cutting-edge Firewall solution, ensuring seamless compliance with government regulations.

WHY COMVIVA?

- **25Bn** messages processed yearly
- Reduced spam by **95%** for an operator
- Up to **5X** revenue boost for operators
- **4000** international brands monetized
- UNO Firewall featured in **5** of Rocco's reports

About Comviva Technologies Ltd.

Comviva simplifies business complexity. Our innovative portfolio of digital solutions and platforms brings greater choice, faster time to market and flexibility, to better meet the evolving needs of our customers as they drive growth, transform, and bring efficiency. From maximizing customer lifetime value to enabling large-scale digital transformation, we partner globally with organizations in the communications and financial industry to solve problems fast and transform for tomorrow.

Comviva solutions have been deployed by over 130 Communication Services Providers and Financial Institutions in more than 90 countries and have delivered the benefits of digital and mobility to billions of people around the world. Comviva is a completely owned subsidiary of Tech Mahindra and a part of the Mahindra Group. For more information, visit us at **www.comviva.com**