



CASE STUDY

Strengthening VoWiFi Security for Safer Mobile Communications

How Matrix Shell Helped a Telecom Operator Secure Its
VoWiFi Infrastructure Against Emerging Threats

Executive Overview

Voice over WiFi (VoWiFi) allows subscribers to make and receive calls over WiFi networks, improving coverage and user experience. Because these services operate over public and untrusted networks, strong security controls are essential to protect subscriber data and core telecom infrastructure.

A telecom operator engaged Matrix Shell to assess the security of its VoWiFi environment and identify weaknesses that could expose the network to unauthorized access or service abuse.

The assessment revealed gaps in traffic control, network segmentation, and data protection. By addressing these issues, the operator strengthened its VoWiFi security and improved the resilience of its IMS infrastructure.



Challenge

VoWiFi extends mobile voice services over WiFi networks, making secure communication more important than ever. If traffic is not properly controlled or encrypted, attackers may gain visibility into sensitive information or access parts of the internal network that should remain protected.

The operator wanted to validate whether its VoWiFi deployment could effectively defend against common security risks while maintaining a secure experience for subscribers.

Potential risks included:

- Uncontrolled signaling traffic
- Exposure of internal network services
- Leakage of sensitive subscriber information
- Unauthorized access attempts
- Increased operational and security risk



Objectives

The assessment was designed to:

- Evaluate the security of the VoWiFi environment
- Validate traffic control and signaling protection
- Assess network segmentation
- Identify information disclosure risks
- Strengthen security across WiFi-based voice services

Solution

Matrix Shell performed a comprehensive VoWiFi Security Assessment focused on the operator's ePDG and IMS infrastructure.

The assessment focused on three high-risk attack scenarios:

Uncontrolled Signaling Traffic

Validated whether signaling traffic was properly controlled to prevent excessive or unauthorized usage.

Internal Network Exposure

Tested whether internal IP addresses and services were accessible through VoWiFi connectivity.

Information Disclosure

Assessed whether subscriber information was adequately protected during communication.

The assessment combined controlled penetration testing with detailed analysis of network behavior to validate the effectiveness of existing security controls.

Testing Process

Phase 1

Information Gathering

- Reviewed VoWiFi architecture and network design
- Identified key connectivity paths
- Collected configuration details required for testing

Phase 2

Network Discovery

- Validated secure connectivity between devices and the network
- Observed traffic flow across VoWiFi services
- Evaluated routing and access behavior

Phase 3

Security Testing

- Tested signaling traffic controls
- Evaluated network segmentation
- Assessed information protection mechanisms
- Captured evidence to validate findings

Phase 4

Analysis & Reporting

- Analyzed identified security gaps
- Assessed operational and business impact
- Prioritized remediation actions
- Delivered practical security recommendations

Results & Impact

Weak Signaling Traffic Controls Identified

The assessment showed that signaling traffic could be generated without sufficient restrictions, increasing the potential for misuse of network resources.

Business Impact

- Uncontrolled signaling activity
- Increased opportunity for service abuse
- Reduced operational control
- Higher revenue risk

Internal Network Exposure

Testing identified internal network systems that were reachable through VoWiFi data paths due to insufficient segmentation.

Business Impact

- Increased attack surface
- Greater risk of unauthorized access
- Potential service disruption
- Improved need for network isolation

Sensitive Information Exposure

The assessment found that certain subscriber-related information was transmitted without adequate protection.

Business Impact

- Increased privacy risk
- Exposure of subscriber information
- Potential compliance concerns
- Reduced customer confidence



Overall Outcome

Following the assessment, the operator achieved:

- Improved visibility into VoWiFi security risks
- Stronger traffic control policies
- Better protection of subscriber information
- Enhanced network segmentation
- Reduced exposure to infrastructure attacks

Conclusion

As WiFi calling becomes a standard service, securing the VoWiFi environment is essential for protecting both subscribers and telecom infrastructure. Through a structured VoWiFi Security Assessment, Matrix Shell identified critical security gaps affecting traffic control, network exposure, and information protection.

By strengthening signaling controls, improving network segmentation, and enhancing encryption practices, the operator significantly improved the security and reliability of its VoWiFi services.

Matrix Shell continues to help telecom operators secure next-generation communication services with practical, standards-based security assessments.