telesign | bics | routemobile

Proximus Global

Whitepaper

# Proximus Global: Security and fraud prevention for modern telecom ecosystems

# Content

# Glossary

| Abbreviation | Full term | Description |
|---|---|---|
| **A2P** | **Application-to-person** | Messaging traffic sent from applications or enterprises to end users, typically for notifications, authentication, or marketing. |
| **AIT** | **Artificially inflated traffic** | Fraudulent generation of voice or messaging traffic to artificially increase volumes and revenue, often involving premium routes or interconnection abuse. |
| **API** | **Application programming interface** | A technical interface allowing systems or applications to exchange data. |
| **CLI** | **Calling line identification** | The phone number presented to the called party, commonly referred to as caller ID. |
| **CDR** | **Call detail record** | A record containing details of a voice call or message, used for billing, analysis, and fraud detection. |
| **GTP-C** | **GPRS tunnelling protocol – Control plane** | A mobile network signaling protocol used to manage sessions and mobility in packet-switched networks. |
| **GT** | **Global title** | A routing identifier used in SS7 signaling to direct messages to the correct network element. |
| **IRSF** | **International revenue share fraud** | A fraud technique generating high volumes of calls to premium-rate numbers to share in the revenue. |
| **NIS2** | **Network and information security directive 2** | EU directive strengthening cybersecurity and resilience requirements for critical infrastructure and service providers. |
| **NVA** | **Network vulnerability assessment** | A non-intrusive assessment identifying weaknesses and misconfigurations in signaling and interconnection environments. |
| **OTT** | **Over-the-top** | Communication services delivered over the internet, outside traditional telecom networks. |
| **P2P** | **Person-to-Person** | Messaging traffic exchanged directly between individual end users. |
| **PBX** | **Private branch exchange** | A private telephone system used within an organization, often targeted in fraud attacks. |
| **RCS** | **Rich communication services** | An enhanced messaging protocol providing rich media, read receipts, and branding capabilities. |
| **SIM box** | | Device for connecting multiple SIMs to a single connection |
| **SIM farm** | | Device using large volume of SIM cards to send messages, often to send fraud. |
| **SS7** | **Signaling system no. 7** | A legacy signaling protocol used for call setup, routing, roaming, and billing. |
| **STI** | **Signaling threat intelligence** | Intelligence and risk scoring derived from global signaling data to identify and mitigate signaling-based threats. |
| **STIR/SHAKEN** | — | Standards for authenticating and verifying caller identity to combat spoofed and fraudulent voice calls. |
| **TCG** | **Transaction control group** | Aggregated transaction data used for traffic analysis, billing, and fraud detection. |
| **TIDS** | **Telecom intrusion detection system** | A system monitoring signaling traffic to detect abnormal behavior, threats, and emerging vulnerabilities. |
| **VoLTE** | **Voice over LTE** | Technology enabling voice calls over LTE packet-switched networks. |
| **Wangiri** | — | A fraud technique involving missed calls designed to prompt victims to call back premium-rate numbers. |

# A new era of network trust and threat complexity

# A new era of network trust and threat complexity

International telecom networks have evolved into highly interconnected, software-driven ecosystems. As a result, security and fraud prevention are no longer back-office risk functions, but core indicators of network quality, operational excellence, and competitiveness.

Fraud has evolved from isolated incidents into coordinated, technology-driven campaigns. Malicious actors now use automation and artificial intelligence to scale attacks, adapt quickly, and personalize fraud. In parallel, telecom infrastructures must support multiple generations of technology and communication channels, which increases complexity and expands the attack surface across roaming, interconnection, and messaging.

Effective security and fraud prevention now directly influence competitiveness. Proactive monitoring, real-time threat intelligence, and automated enforcement are designed to help reduce unnecessary traffic, limit revenue leakage, and protect network resources. Insufficient protection, by contrast, may lead to financial loss, service degradation, regulatory exposure, and reputational damage.

The impact extends beyond network operations. Fraud increasingly causes direct financial harm to consumers and enterprises, erodes brand trust, and triggers stricter regulatory requirements around user protection and accountability.

Operators need a layered security approach across the entire communication chain. Proximus Global provides solutions designed to support network, communication, and end-user protection to shift operators from reactive defense to a proactive 2026-ready posture.

# The strategic shift: From cost center to competitive advantage

# The strategic shift: From cost center to competitive advantage

Security is no longer a defensive cost center, but a core enabler of sustainable growth.

### Revenue protection

Combat industrialized fraud to prevent revenue leakage and inflated interconnection costs.

### Operational efficiency & scalability

Reduce unnecessary traffic and protect network resources through automation.

### Regulatory compliance

Meet global security mandates (STIR/SHAKEN, NIS2, CLI authentication).

### Customer trust & differentiation

Protect end-users, strengthen trust, and differentiate through secure communications.

### Ecosystem readiness

Ensure eligibility for roaming, messaging, and API-driven partnerships.

# The 2026 threat landscape: What operators must prepare for

# The 2026 threat landscape: What operators must prepare for

## From single-channel to omni-channel fraud

The expansion of OTT messaging and RCS is accelerating a shift toward **omni-channel fraud**. Attacks increasingly start on regulated telecom channels (SMS or voice) and then migrate to **encrypted OTT platforms**, where operators have no visibility or enforcement capabilities. A growing pattern is "Hello" fraud: low-volume seemingly harmless greeting messages used to trigger engagement before switching victims to encrypted channels for social engineering and scam activity.

This trend exposes a structural trade-off. While encryption and richer messaging improve privacy, they simultaneously reduce operators' ability to detect and block abuse. Yet end-users still expect operators to protect them, widening the gap between responsibility and technical control.

## AI-Driven industrialization of fraud

Generative AI is fundamentally changing fraud economics. Attackers can iterate faster, personalize content at scale and continuously optimize scams based on success and failure analysis. AI also enables **low-and-slow attacks**, deliberately engineered to stay below traditional detection thresholds. As a result, real-time detection, behavioral analysis and automation are becoming prerequisites rather than differentiators.

## Clear shifts in traffic patterns

Based on live Proximus Global network traffic:

### Inbound fraud dominance

Outbound Voice fraud (IRSF) is controlled, while inbound spam calls and robocalls continue to grow across regions.

### Compromised legitimate assets

Over 60% of voice fraud uses valid, non-advertised numbers. Many SMS attacks originate from real subscriber SIMs, making static blacklists less effective.

### Geographic redistribution

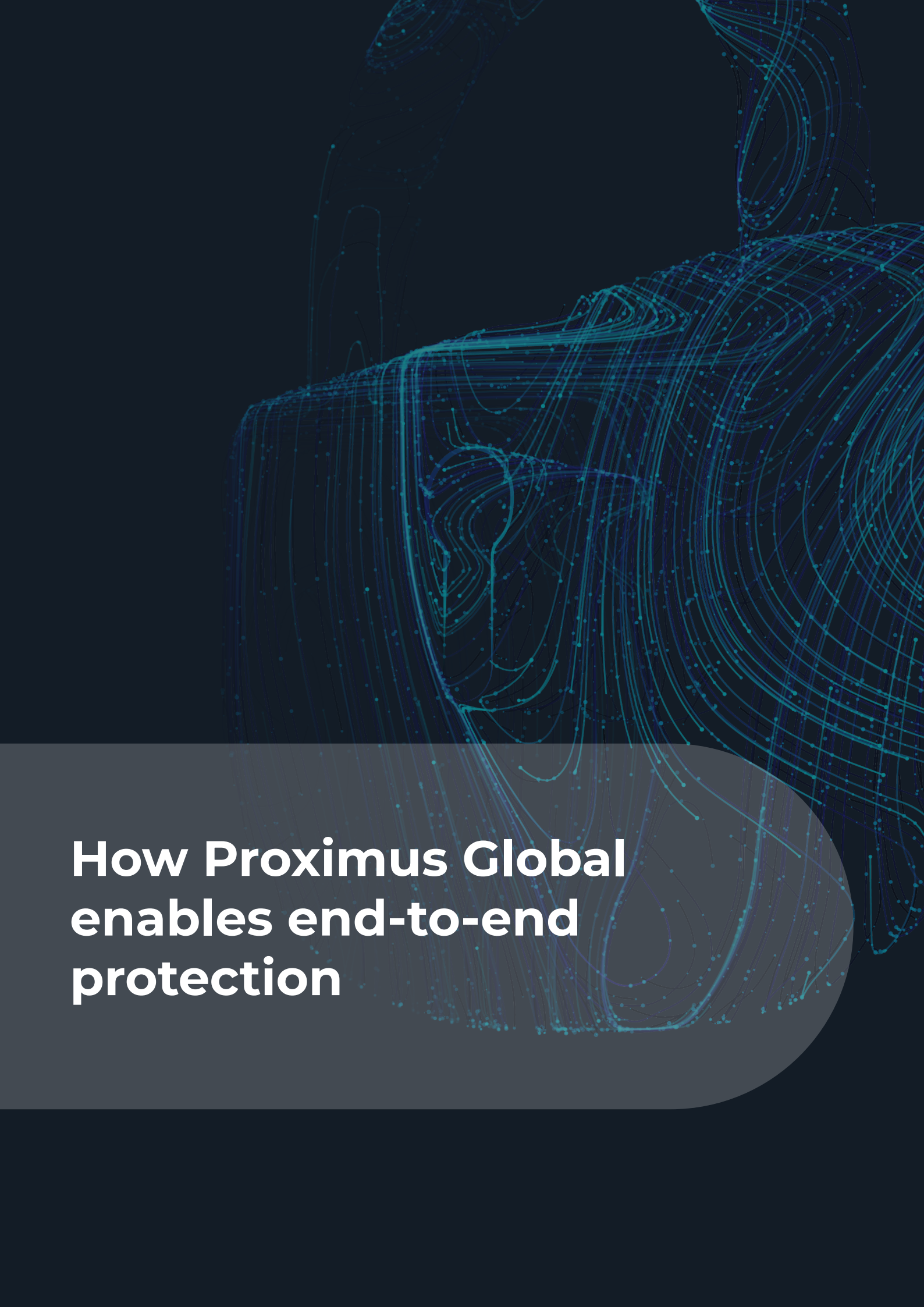
Traditional high-risk routes (satellite, Caribbean) have declined. Fraud increasingly originates from within the same regions it targets.

### SMS fraud acceleration

AIT, smishing, and P2P-to-A2P abuse are increasing rapidly. Millions of attacks are identified and mitigated daily across networks using our solutions, yet volumes continue to grow.

### Regulatory escalation

Do-Not-Originate lists, traceback obligations, CLI authentication and financial penalties are expanding globally.



# How Proximus Global enables end-to-end protection

# How Proximus Global enables end-to-end protection

Proximus Global applies a unified security strategy built around three essential layers: network, communications, and end-user. Each layer addresses distinct threat vectors, yet works together to create an end-to-end protection model built for modern telecom environments.

### Network layer

Safeguards the core network and interconnection fabric by detecting and blocking signaling threats, protocol abuse, and vulnerabilities that compromise confidentiality, integrity, and availability.

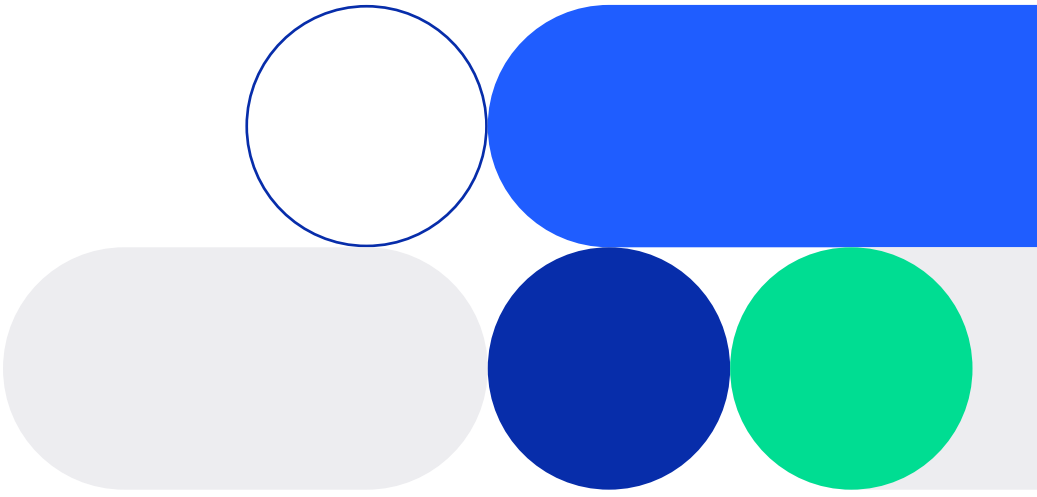
### Communications layer

Protects voice, messaging, and roaming traffic from fraud, routing abuse, inflated traffic, spoofing, and monetization-driven threats that directly impact both operators and enterprise customers.

### End-user layer

Secures subscribers and their digital identities by mitigating social engineering, identity abuse, account takeover attempts, and AI-enabled scams through intelligence-driven risk scoring and verification.

Together, these three layers deliver a comprehensive, 360-degree protection framework that enables operators to evolve from reactive controls to a proactive, intelligence-driven security posture.



# Securing the core: Signaling & interconnect defense

Signaling-based attacks targeting confidentiality, integrity, and availability across roaming and interconnection, with legacy protocols remaining the primary exposure.

## Main threat types:

- Signaling protocol abuse (SS7, Diameter, GTP-C)
- Global Title (GT) spoofing and misuse
- Exploitation of misconfigurations

## How protection is applied

### Network Vulnerability Assessment (NVA)

- Non-intrusive penetration tests
- Covers all major threat types including denial of service, SMS interception and location tracking
- Applies to SS7, Diameter, GTP-C, SIP and HTTP2

### Hosted Signaling Firewall (HSF)

- Real-time blocking of vulnerabilities at transit layer
- Covers all major threat types, following GSMA recommendations, including Category 1, 2 and low layer format filtering
- Applies to SS7 and Diameter

### Telecom Intrusion Detection System (TIDS)

- 24/7 monitoring of raw signaling data to identify attempted and successfully exploited attacks based on defined detection parameters
- Covers all major threat types, going beyond GSMA recommendations
- Applies to SS7, Diameter, GTP-C, SIP and HTTP2

### Signaling Threat Intelligence (STI)

- Behavioral insights and AI-based risk scoring of Global Titles
- Built on 100,000+ profiled SS7 nodes daily
- Integrate with any existing monitoring system

# Voice, Messaging and Roaming: Securing high-risk traffic channels

This layer is where fraud directly translates into revenue leakage, regulatory exposure and customer harm.

## Main threat types:

- Routing and bypass
- Artificially Inflated Traffic (AIT)
- Fraudulent traffic
- Origin abuse
- Premium rate fraud
- Roaming fraud

## How protection is applied

### FraudGuard voice

- Near real-time hosted detecting and blocking at the transit layer
- For local subscribers and inbound roamers across telco and enterprises
- Outbound premium rate: IRSF, arbitrage, PBX hacking, call stretching, FAS and roaming fraud
- Inbound fraudulent traffic: Wangiri, robocalls, spam, flash calls
- Origin abuse: CLI spoofing, number hijacking

### FraudGuard SMS

- Near real-time hosted detecting and blocking at the transit layer
- For local subscribers and inbound roamers across telco and enterprises
- Outbound premium rate: AIT (A2P & P2P), Malware-generated fraud and IRSF
- Inbound fraudulent traffic: Smishing (A2P & P2P), Spam, "Hello" fraud
- Origin abuse: Originator Spoofing

### Voice Roaming Firewall

- Real-time protection against voice fraud from outbound roamers
- Near real-time hosted detecting and blocking at the transit layer
- Outbound premium rate: IRSF, roaming-specific fraud, arbitrage

### Monetization services

- CDR- or TCG-based hosted detection of illegitimate routing
- Routing and bypass: SIM-box, SIM-farm, grey routes, OTT fraud, interconnect misuse
- Fully managed E2E monetization service for A2P business

## Local deployments

**Local Protection (by 365squared – part of Proximus Global)**

**365voice: local voice firewall** | **365secure: local SMS firewall** | **365detect (+): local monetization**

# Protecting digital identity in an AI driven fraud era

## What is at risk?

Fraud at the end-user layer leads to **financial loss, account takeover, erosion of trust, and brand damage.** Consumers expect operators to safeguard their digital identity even as threats grow more sophisticated. Our solutions are designed to support operators in addressing these risks.

### Main threat types:


Identity abuse


Social engineering


Fraudulent traffic

### How protection is applied

**365guard (by 365squared – Part of Proximus Global)**

- Local protection against malicious end-user traffic
- Social Engineering: smishing (P2P, A2P), "Hello" fraud
- Fraudulent traffic: bulk messages, genAI-enabled scams

**Intelligence API (by Telesign – Part of Proximus Global)**

- Real-time risk score for individual phone numbers intended to support fraud risk assessment and decision-making
- Identity abuse: Inconsistent phone attributes and usage patterns
- Fraudulent Traffic: association with fraud, spam or promo abuse

**PhoneID API (by Telesign – Part of Proximus Global)**

- Verified phone number and subscriber data, designed to assist in identity verification workflows as configured by the customer
- Identity abuse: Inconsistent signals across contact data, subscriber status, porting history, call forwarding, SIM swap, age verification and more

# Why Proximus Global

# Why Proximus Global

### Proven at global scale

We support the protection of international telecom traffic daily and identify and address millions of fraud attempts in real time, backed by decades of telecom security expertise.

### Expertise built into operations

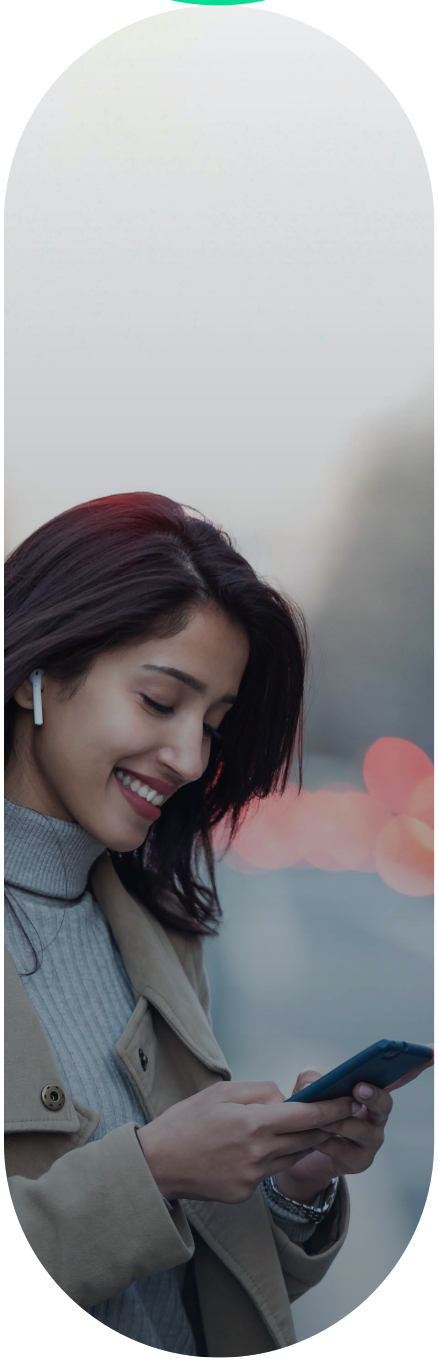
Security solutions designed to be operationally integrated, continuously refined through live networks, real incidents and global threat intelligence.

### Easy and flexible to consume

Managed and hosted solutions shift complexity away from operators, helping reduce operational burden while accelerating time to protection.

### End-to-end protection

A single partner providing solutions designed to support the security of networks, communications and end-users



## What operators must do now?

The fraud landscape evolves faster than traditional security approaches can adapt. Operators delaying comprehensive protection face increasing exposure across revenue, regulatory compliance, and customer trust.

**In 2026, security is no longer optional, but a key differentiator for telecom operators.**

Contact your Proximus Global account team to assess your security posture and discuss protection strategies tailored to your network.


Proximus Global

Proximus Global, combining the strengths of Telesign, BICS, and Route Mobile, is transforming the future of communications and digital identity. Together, our solutions fuel innovation across the world's largest companies and emerging brands. Our unrivaled global reach empowers businesses to create engaging experiences with built-in fraud protection across the entire customer lifecycle. Our comprehensive suite of solutions – from our super network for voice, messaging, and data, to 5G and IoT; and from verification and intelligence to CPaaS for personalized omnichannel engagement – enables businesses and communities to thrive. Reaching over 5 billion subscribers, securing more than 180 billion transactions annually, and connecting 1,000+ destinations, we honor our commitment to connect, protect and engage everyone, everywhere.

Learn more at **proximusglobal.com**

proximus Global