CUSTOMER CASE STUDY

Scaling fast without sacrificing security: SkyTel's MDR journey

SkyTel has always operated at the intersection of trust and pressure. As a growing business process outsourcing (BPO) delivering sensitive customer operations across several countries in North and South America, their business runs on the simple promise that data stays safe, and service stays uninterrupted.

SOPHOS

SKYTEL

Industry
Telecommunications and business outsourcing

Sophos Solutions
Sophos Managed Detection and Response (MDR)

Sophos Central

Sophos Firewall

Number of Users
1,500

Website
skytel.tech

Growth brings new opportunities — and with them, a more dynamic security environment.

Every new market added a new network. Every client added another compliance layer. And every day, adversaries evolved.

"We have operations distributed across different countries, with infrastructures that demand flexibility but also a unified regional vision of security," Carlos Adonaylo, the head of cybersecurity for SkyTel, said.

He wasn't talking about theoretical risk — this was the reality of operating in a fast-scaling environment. SkyTel recognized that sustaining growth required a security model designed for agility and resilience.

SkyTel's rapid regional expansion presented an opportunity to rethink its security operating model. Rather than scaling internal resources alone, the company made a strategic decision to complement its team with external specialists — a mature, efficient approach that ensures security evolves in lockstep with business growth.

SkyTel's vision is to become the leading AI-first BPO, pairing "hyper-realistic and empathetic virtual agents" with human intelligence to resolve complex cases.

But there's a hidden truth in every AI-first strategy: Your security posture must evolve just as fast as your technology. For BPOs, every new market introduces unique compliance requirements and increases the attack surface. This potentially introduces new risks that can impact client trust and business continuity.

SkyTel had already invested in advanced tools like Sophos Endpoint and Extended Detection and Response (XDR), but the threat landscape was changing faster than any single team could manage. Today's attacks are automated, aggressive, and accelerated by AI — requiring defenses that operate at the same speed.

This reality drove SkyTel to evolve toward a hybrid security model, combining AI-driven detection with human expertise for advanced analysis and response.

"In 2025, we decided to expand our response capability since our internal IT team did not have enough specialists to react with the required speed to complex incidents," Adonaylo said.

This turned out to be an inflection point. SkyTel didn't need more tools, they needed more human capacity, faster detection, and continuous coverage across every country, client, and connection point.

Impact

- 360-degree regional visibility.
- Real-time threat detection.
- Faster, cleaner compliance.
- Improved synergy between AI tools and the company's IT and security teams.

SOPHOS

Choosing MDR as a force multiplier

SkyTel chose Sophos MDR as a strategic force multiplier. MDR delivers a 24/7 managed SOC powered by AI and backed by global cybersecurity specialists. This hybrid approach ensures threats are detected and blocked at machine speed, while human experts provide deep investigation and rapid response — a level of resilience that positions security as a growth enabler, not a constraint.

From day one, MDR became the always-on extension of their team with a 24/7 managed security operations center (SOC), AI-driven detection, and a team of global cybersecurity experts at their back. Sophos MDR combines human expertise with advanced AI to deliver around-the-clock threat detection, investigation, and response — a level of protection SkyTel couldn't replicate internally.

"The MDR service provided exactly what we needed: A 24/7 managed SOC with advanced monitoring, analysis, and incident response capabilities," Adonaylo said.

SkyTel gained what every global BPO needs: A single, unified view of security across all countries and clients, eliminating blind spots and strengthening trust.

This wasn't just an uplift in tooling. It was a strategic shift from reactive protection to proactive, intelligence-led protection, a strategic shift that positioned security as a growth enabler, not a constraint.

The transformation: Visibility, confidence, and control

Even before the onboarding project was fully completed, SkyTel saw a tangible impact.

"We have already seen greater visibility into our infrastructure, earlier detection of events, and smooth collaboration with the HO team," Adonaylo said. "The main goal — strengthening our security posture and protecting critical assets — has been fully achieved."

With MDR in place, SkyTel gained:

- 360-degree regional visibility: Unified visibility across four countries, reducing blind spots and improving decision-making.
- Real-time threat detection: Early detection across on-prem and cloud infrastructure.

"We have already seen greater visibility into our infrastructure, earlier detection of events, and smooth collaboration with the HO team. The main goal — strengthening our security posture and protecting critical assets — has been fully achieved."

Carlos Adonaylo - CISO

- Faster, cleaner compliance: Simplified compliance reporting, saving time, and reducing audit stress.
- A lift in security maturity: Security wasn't a bottleneck anymore — it was a business enabler.
- Human + AI constructive collaboration: Perfectly aligned with their company vision of hybrid intelligence.

To learn more visit Sophos.com

SOPHOS