

Managing HEIGHTENED *external* threats

Luis Ortega – VP of International Enterprise Accounts, Allied Universal Enhanced Protection Services – and Ruben Mora – Regional Sales Director for LATAM, G4S – discuss security in a polarised world

In an increasingly polarised world, the nature of corporate risk is changing. The gap between traditionally “stable” and “volatile” regions is narrowing and threats to organisations are no longer isolated by geography or limited to criminal activities. Increasingly, they are ideological, driven by digital narratives that can escalate into real-world danger within hours.

To operate safely in this environment, multinational organisations must move from static to proactive security models with intelligence-led protection strategies. To learn more about how organisations are adapting, Luis Ortega, VP of International

Enterprise Accounts, Allied Universal Enhanced Protection Services and Ruben Mora, Regional Sales Director for LATAM, G4S shared insights with ISJ.

From tangible to symbolic targets: The new threat landscape

“Today, companies are being targeted more for what they represent, rather than what they own,” explained Ortega. Ten years ago, security leaders worried primarily about conventional threats such as theft, fraud and localised instability. Today, companies and their executives are increasingly targeted for what they symbolise: Proxies for wealth, power or political positioning.

As a result, organisations can become lightning rods for attacks not because of any specific actions, but because of narratives assigned to them online by third parties. Social media accelerates the spread of these narratives. According to the 2025 World Security Report, which surveyed 2,352 chief security officers across 31 countries, 73% reported their companies were targeted by misinformation or disinformation campaigns last year.

These narratives can directly motivate threat actors, creating risks that were rarely part of the corporate threat equation a decade ago. Organisations must stay ahead of these emerging risks with proactive threat intelligence

“In an increasingly polarised world, business continuity depends on keeping leaders safe, informed and operational.”

in order to maintain an effective security posture on the ground. Ortega describes the moment we are living in as “the bits and the atoms coming together... against us.” The dividing line between online sentiment and real-world threats is rapidly disappearing.

On-the-ground realities in LATAM

Latin America illustrates these global shifts clearly. “Latin America is a collection of countries with different backgrounds and histories, and unfortunately there is a convergence of threats,” Mora explains. Across the region, factors such as political activism, civil unrest and emerging criminal networks are shaping a complex

risk landscape that requires tailored responses.

The 2025 World Security Report identified economic instability as the top security-impacting hazard in Latin America, cited by 41% of CSOs, up significantly from 26% reported in 2024. Companies operating in higher-risk environments are increasingly moving beyond traditional guarding models toward enhanced strategies that integrate technology with human intelligence.

In the same 2025 report, 46% of CSOs said they expect to invest in AI-powered video surveillance, analytics and threat detection. Facing tighter budgets and evolving



Luis Ortega
VP of International Enterprise Accounts, Allied Universal Enhanced Protection Services



Ruben Mora
Regional Sales Director for LATAM, G4S



risks, simply adding more security professionals or front-desk personnel is no longer sufficient for many organisations. They are seeking protection models that actively mitigate risk rather than merely providing a visible deterrent.

Redefining threat assessment: Managing information overload

As online signals increasingly translate into real-world actions, threat assessments must begin earlier.

“The first warning signs are often found online,” says Ortega, “not necessarily at the front gates or the front door. We can’t treat them as separate threats coming from different directions. They’re all converging.”

Organisations must pay attention not only to who is physically nearby, but also to who is talking

about their brand online, how quickly sentiment is spreading and what actions it may be calling for. Digital signals have become a key source of actionable intelligence. However, access to data alone is not enough. “The information flow is overwhelming,” Mora explains. “You need a program that can take that input and make something out of it, identifying the next potential threat.”

“In an increasingly polarised world, the nature of corporate risk is changing.”

“When is an alarm truly an alarm? When is it a false signal? And when is it an early indicator of something to come?” Security teams require training, specialised expertise and analytical tools to filter the noise and convert massive data

streams into prioritised intelligence they can act upon.

Why static security is no longer sufficient

“Traditional security models often fail because they assume stability,” Ortega states. That assumption is increasingly unrealistic. Protests can form within hours, borders can close overnight and digital narratives can spread globally before security teams even become aware of them. When digital threats and physical protection are managed separately, organisations risk missing critical warning signals. Real-world incidents rarely respect boundaries between digital and physical environments.

“More and more, the things we need to protect are not physical,” Mora explains. “And even if they are physical, they are not fixed. We have to think about protecting the brand, wherever it operates.”

Today’s security programs must protect traveling executives, mobile operations, supply chains and intangible assets such as reputation. Anticipation and real-time adaptation have become essential capabilities.

The four pillars of modern protection

As risks become faster, more narrative-driven and less geographically predictable, organisations must rethink how their security programs are structured. Four capabilities are increasingly essential for operating safely in today’s polarised environment:

Decision-grade intelligence – security teams must move beyond passively logging alerts and instead track emerging digital narratives and geopolitical signals. “And once they detect them,” Ortega notes, “they have to translate that information into clear guidance that leaders can act upon.” Organisations today receive vast amounts of data from cameras, sensors and monitoring platforms. Without the expertise to interpret it, however, that data becomes noise rather than intelligence. Effective programmes transform raw information into decision-grade risk insight.

Integrated executive protection – with digital and physical threats converging, modern protection programs must address both domains together rather than treating them as separate challenges. Early warning signals that begin as online narratives frequently escalate into real-world risks. The urgency for this integrated approach is reflected in the data: The 2025 World Security Report found that 42% of CSOs reported an increased threat of violence toward executives.

Real mobility and response – when conditions change rapidly, whether due to civil unrest, border restrictions or escalating digital sentiment, organisations must be able to respond immediately. Ortega emphasises that companies must have the ability to “re-route, relocate or pause operations without creating confusion.” Protecting executives in these situations requires highly trained

professionals skilled in counter-surveillance, defensive driving and dynamic risk response.

“Organisations must stay ahead of these emerging risks with proactive threat intelligence in order to maintain an effective security posture on the ground.”

Enterprise-wide consistency – security can no longer operate as a siloed departmental function. It must be embedded as an organisational culture. According to the 2025 World Security Report, companies with strong, widely adopted security cultures are significantly more confident in their ability to manage both internal and external threats. Achieving this consistency often requires moving beyond fragmented local security contracts. The report reveals that

organisations using a single third-party provider for the majority of their physical security needs experience fewer incidents and report far greater confidence in their ability to respond to threats.

Evolving security threats require a new approach

In an increasingly polarised world, business continuity depends on keeping leaders safe, informed and operational. The days of relying solely on a guard at the door are over.

Digital threats are no longer just a communications challenge – it is increasingly recognised as a precursor to real-world incidents. Organisations looking to strengthen their security posture need partners capable of combining human expertise with advanced technology.

Approaches that integrate risk and vulnerability consulting, intelligence services and executive protection are becoming increasingly important. Programmes such as the Enhanced Protection Services (EPS) framework illustrate how these capabilities can be combined to help organisations stay ahead of persistent, evolving risks without disrupting core operations (Allied Universal).

