ONTIC SUMMIT 2026

Stage Zero on the Pathway to Violence and the Expanding Role of EP

This session examined how executive protection is expanding beyond traditional external threats into a blended environment shaped by insider risk, online radicalization, workplace violence, and reputational exposure. Cynthia Marble introduced “stage zero” on the Pathway to Violence as the behavioral space before ideation, while Mo Baloch described how American Airlines built an executive protection program by linking risk to business impact, benchmarking peers, and scaling resources carefully through technology, partnerships, and measurable outcomes.

Speakers

Mo Baloch
Director of Protective Services
American Airlines

Cynthia Marble
Sr. Director, Executive Protection Practice
Ontic

Key Themes and Topics

Executive Protection Now Requires a Blended Threat Model

Executive protection can no longer focus only on stalkers, letter writers, and known external actors. Security leaders must address a blended threat picture that includes disgruntled employees, cyber-enabled threats, and online radicalization directed at executives and brands.

Stage Zero Matters More Than Waiting for a Clear Threat

The discussion emphasized that concerning behavior often begins before a person reaches ideation on the pathway to violence. Fixation, desperation, despondency, and problem-solving through violence are more useful early warning signals than waiting for a clearly defined grievance.

Behavioral Threat Assessment Should Trigger Early Management

Organizations often wait too long to complete a full threat assessment before acting. Cynthia stressed that once pre-incident behaviors appear, security teams should begin protective and intervention measures immediately to reduce escalation and protect both people and operations.

Continued on next page

Key Themes and Topics

Online Amplification Is Reshaping Executive Risk

Online sentiment, admiration of violence, and digitally driven fixation are changing how threats emerge and spread. Security teams must monitor when language becomes more specific, more intense, and more normalized, because those shifts can indicate accelerating risk toward executives.

Boards Respond to Business Impact, Not Security Language Alone

Board support becomes stronger when executive protection is framed in terms of resilience, continuity, reputational damage, stock impact, and executive productivity. Programs gain traction when leaders can clearly explain operational gaps, benchmark peers, and show measurable organizational value.

Actionable Takeaways

Build a Stage Zero Detection Framework

Create a structured internal model for identifying fixation, desperation, despondency, behavior changes, and other pre-incident indicators. Train security, HR, and key business partners to recognize these signals early so protective and intervention measures begin before ideation hardens.

Implement a Unified Security Technology Platform

Adopt a centralized system of record that connects incidents, investigations, and risk data across teams. This enables better visibility, reduces silos, and allows security leaders to identify patterns, improve decision making, and proactively manage risk at scale.

Shift From Reactive Investigation to Proactive Risk Management

Do not wait for perfect intelligence or a completed threat assessment before taking action. Establish decision rules that allow teams to implement proportionate protections, support interventions, and investigative follow-up as soon as concerning pre-incident behavior is identified.

Frame Security Requests in Business Terms

Present executive protection needs in terms of resilience, time saved, continuity, and reputational preservation. This approach improves board and executive buy-in because it shows how security investments protect enterprise performance, not just individuals.

Continued on next page

Actionable Takeaways

Benchmark Peers, but Design for Your Risk Profile

Study mature executive protection programs across comparable organizations, then build a fit-for-purpose model tailored to your company's leadership exposure, travel patterns, public profile, and threat environment. Avoid copying another program wholesale without matching it to your realities.

Measure Both Activity and Impact

Track operational metrics such as trips, POIs, and case volume, but also quantify higher-value outcomes like executive time saved, risk mitigated, and resilience improved. Impact metrics help security leaders justify resources and sustain long-term program credibility.

Notable Quote

"We want to leverage tech. We want to leverage our existing vendors and we want to put everything together in one common operating picture. So one single pane of glass is what I was after"

- Mo Baloch

Director of Protective Services, American Airlines

Final Message

Executive protection programs are strongest when they identify risk before it becomes intent, translate threat into business impact, and act before intelligence feels complete. The opportunity is not just to protect executives, but to strengthen resilience, decision-making, and trust across the enterprise.