KASEWARE

Protecting the Executive

A Strategic Guide to Designing a Modern Executive Protection Program

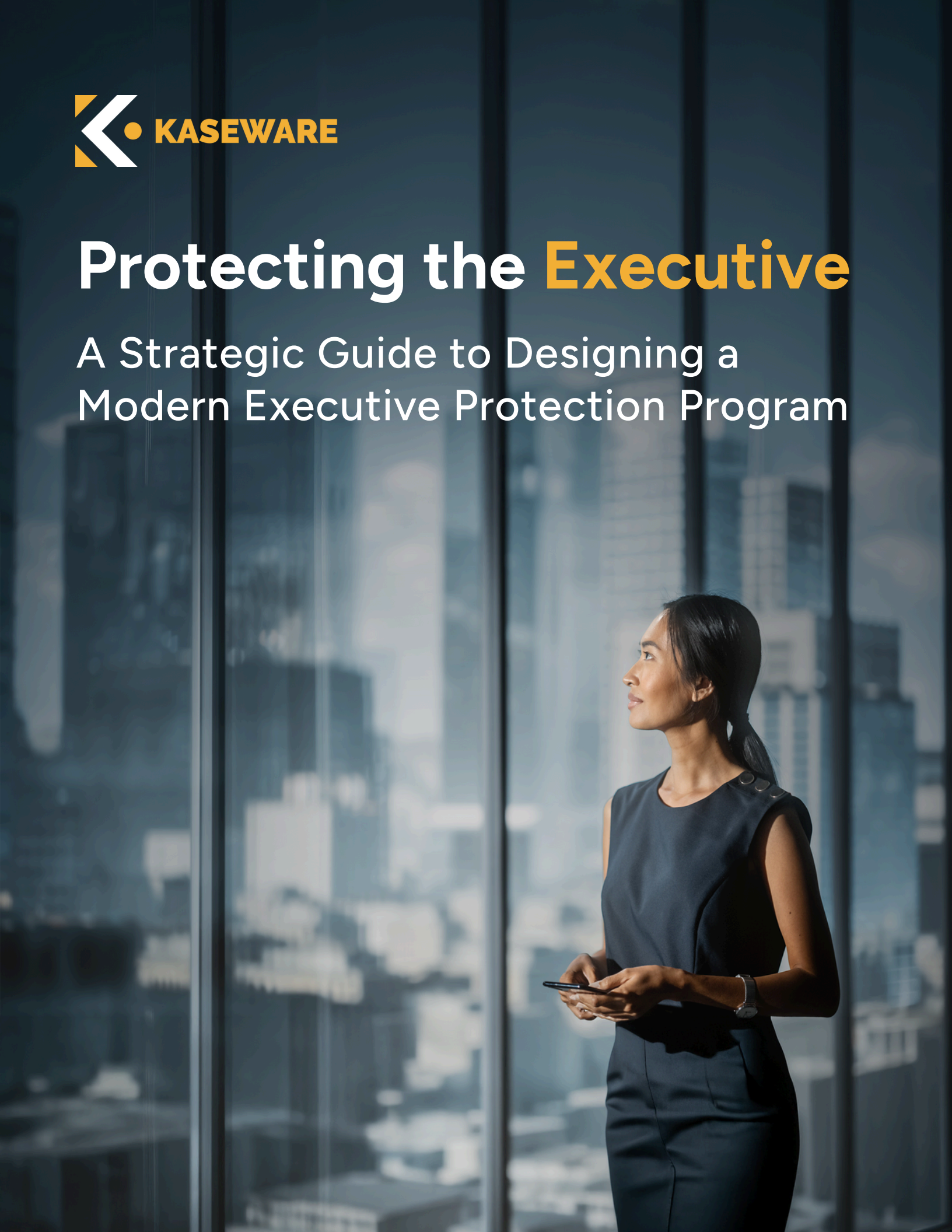


Table of Contents

Executive Protection Is in the Spotlight

Today's executives operate under constant visibility and exposure. They make public decisions, represent global brands, and lead organizations during times of increased polarization, volatility, and rising digital exposure. With that visibility comes risk, including personal, reputational, and organizational threats.

Executive protection has become a strategic imperative. Once viewed as a luxury for unique situations and Fortune 50 companies, it is now a priority for companies facing increased pressure to safeguard their leadership. Threats no longer begin at the edge of a physical property. They emerge online, through public sentiment, or within the organization, and they often escalate quickly. **According to recent findings** from ASIS International, **42% of organizations say executive protection now receives significantly more attention than it did just ~18 months ago**, highlighting the growing importance of executive protection as part of modern security strategy.

This guide offers a clear framework to help build or strengthen an executive protection program. From risk assessment to cross-functional coordination, each step is designed to help you **lead with clarity, scale with consistency, and demonstrate long-term value.**

Why Executive Protection Has Become a Strategic Imperative

Executive protection used to focus on proximity, travel, and events. That approach no longer fits the threat landscape due to the increasingly sophisticated risk environment. Today's executives face heightened visibility, greater digital exposure, and increasingly complex risks across both public and private domains.

The nature of threats has changed:

- Public sentiment turns quickly
- Personal information is widely accessible
- Harassment moves from digital to physical
- Reputational attacks spark from a single headline
- Family and associates can become indirect targets
- Ai tools provide a new pathway for threats

Traditional executive protection strategies cannot stand alone. Chief Security Officers (CSOs) must now lead programs that integrate intelligence, monitor sentiment and behavior, and coordinate response across internal and external teams.

A DEFINING MOMENT FOR COPORATE SECURITY

In late 2024, UnitedHealth CEO Brian Thompson was assassinated in a public incident that stunned the corporate world. While such events remain rare, they reflect a growing reality: high-profile executives are increasingly vulnerable to targeted violence, whether motivated by ideology, personal grievance, or broader unrest.

Many executives are unaware of just how exposed their personal data has become. According to research by **Nisos**, **98% of corporate executives have a property publicly linked to their name, and 58% had Social Security numbers appear in breach data**. These exposures make it easier for bad actors to exploit or cause harm.

Executives live in the spotlight. That spotlight attracts scrutiny, anger, and sometimes danger, especially for executives in **more scrutinized industries such as healthcare, finance, and energy**. When leadership decisions impact large audiences or attract controversy, the risk intensifies.

The shift is clear: protection programs must evolve and adapt to evolving risk. Executive risk now moves through social media, data breaches, online narratives, and reputational volatility. Protection strategies must be comprehensive and inter-connected, spanning physical, digital, and behavioral domains.

What a Mature Executive Protection Program Looks Like

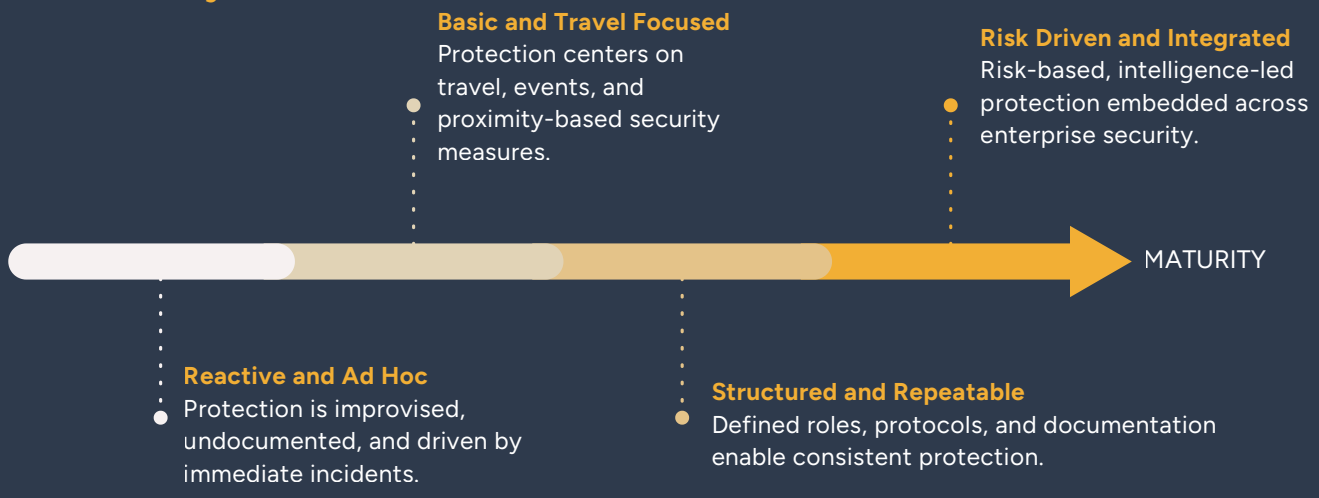
Executive protection programs can vary widely in structure and effectiveness. Some are ad hoc and reactive, while others are more strategic, structured, and capable of adapting to evolving risk. What separates them is maturity —the degree to which protection is planned, documented, and aligned with broader security priorities.

Whether you are building a new program or strengthening an existing one, it is important to understand the **four common stages of maturity** that can help you evaluate your current position and plan what comes next.

The more structured your program becomes, the more proactive and effective your team can be. You shift from reactively putting out fires to proactively identifying patterns and mitigating risks. You protect against reputational threats before they gain traction. You align protection with executive needs and business priorities.

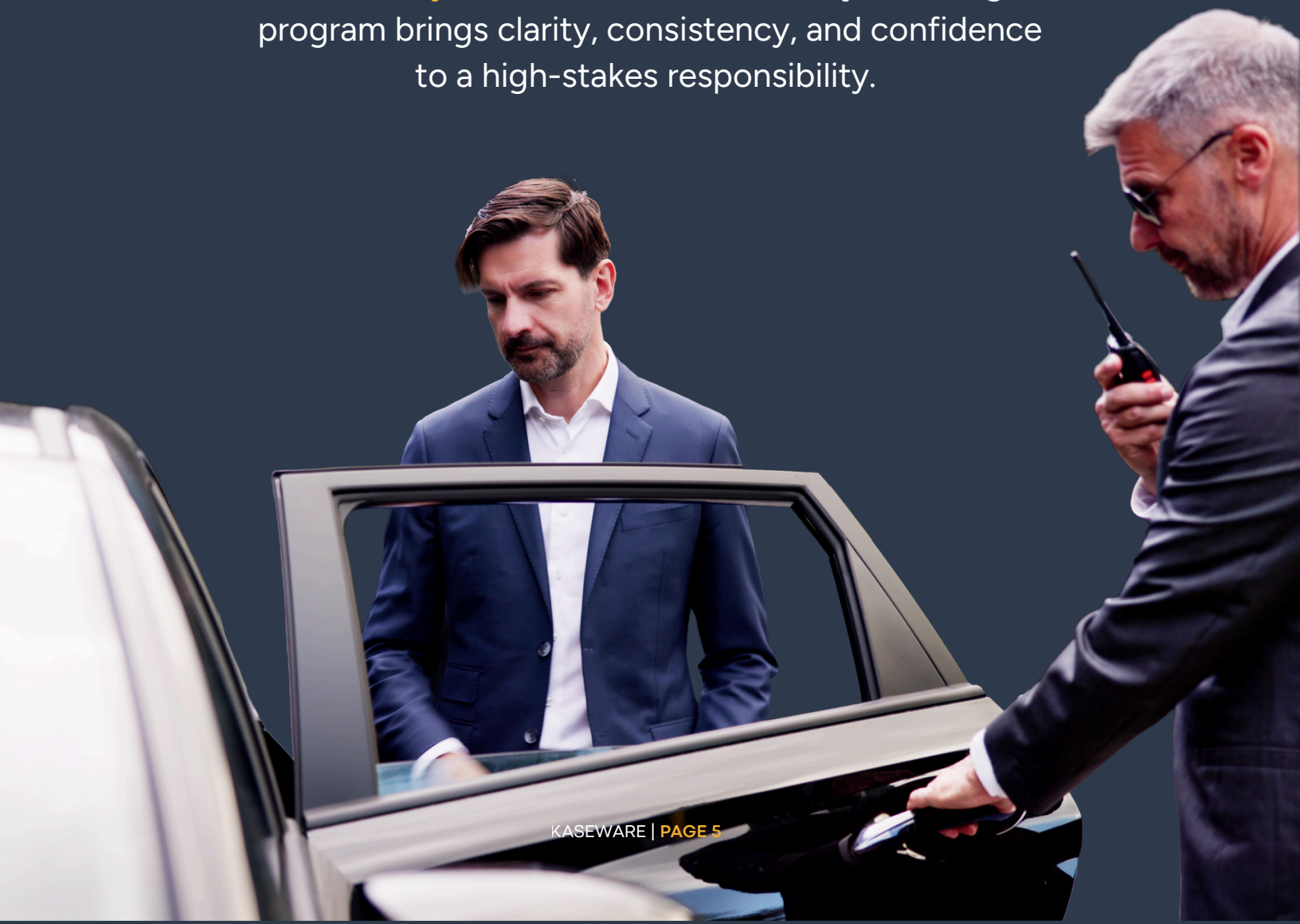
> "A mature executive protection program is measured not just by the speed of the ability to respond, but even moreso by the consistency in the ability to prevent. The strongest programs align intelligence, processes, and people so protection becomes proactive, repeatable, and integrated into the broader security strategy, not treated as a standalone function."
>
> - John Gill, Former CSO of the White House

Executive Protection Maturity Model



Key Aspects of a Modern Executive Protection Program

Executive protection is about more than safeguarding individuals. It reflects how an organization prepares for risk, protects its leadership, and sustains business continuity in moments of uncertainty. A strong program brings clarity, consistency, and confidence to a high-stakes responsibility.



The Importance of Assessing Risk for EP Programs

Modern executive protection is no longer defined by proximity, staffing levels, or static protection plans. In today's threat environment—marked by targeted violence, online hostility, insider risk, and geopolitical volatility—effective EP programs are built on continuous, intelligence-led risk assessment.

The goal is simple: align protective resources and operational tempo to real risk, in real time.

Assessing Risk Across the Executive Protection Landscape

Executive Risk
Each executive carries a unique risk profile shaped by their role, visibility, decision-making authority, public exposure, travel patterns, and personal and professional footprint. Risk assessments must account for evolving grievances, fixation behaviors, and changes in exposure, not just historical threats.

Location & Travel Risk
Risk varies significantly by geography, venue, and itinerary. Assessments should incorporate regional threat conditions, crime trends, venue security posture, transportation routes, and emergency response capabilities updated continuously as conditions change.

Online & Digital Risk
Digital exposure increasingly drives physical risk. Social media activity, doxxing attempts, impersonation, deepfakes, and hostile online rhetoric often serve as early indicators of escalation. Monitoring online risk is now essential to proactive executive protection.

Converged Risk
Threats rarely exist in isolation. The most effective programs correlate online indicators, physical security intelligence, insider risk signals, and travel data to identify patterns and pre-incident warning signs.

The Importance of a Consistent Risk Metric

Executive protection programs are strongest when they are anchored to a consistent, defensible risk metric. Without a common risk framework, protection decisions can become subjective, inconsistent, or difficult to justify to leadership.

A standardized risk metric allows organizations to:

- ✓ Measure and compare risk across executives, locations, and events
- ✓ Adjust protection posture based on risk indicators
- ✓ Prioritize resources and operational approach where risk is highest
- ✓ Communicate risk clearly to executives and stakeholders
- ✓ Demonstrate accountability and program value by anchoring decisions to empirical data

Detecting Exposure Early with OSINT

Many issues that later turn into executive protection concerns start online. Information about executives, their families, travel, or routines can be disclosed in public forums, social media, news coverage, or breached data long before a physical incident occurs.

Open-source intelligence (OSINT) helps security teams find this information early, allowing them to understand risk exposure and threat intent. Used well, OSINT gives teams better visibility into what is being said or shared online so they can anticipate risk rather than react to incidents once protective conditions have already deteriorated.

A Common Challenge for Executive Protection Teams

Industry research and practitioner experience show that OSINT is often underused in executive protection. Many teams only turn to online monitoring when a situation already feels risky, or they use it inconsistently due to capability gaps.

At the same time, teams increasingly recognize that signs such as grievance, fixation, or targeting behavior often appear online first. The challenge is not awareness; it is having the ability to consistently find relevant information, understand it, and act on it as part of everyday protection planning.

Quick self-check

- [ ] Do you review online exposure and activity as part of routine protection planning, or only when concerns arise?
- [ ] Can you spot online language or behavior that may signal fixation, grievance, or targeting against an executive, organization, location, or event?
- [ ] Do you have confidence in deciding when online activity should change how you plan or protect?
- [ ] Do you monitor reputational or narrative issues online that could increase attention or targeting risk?
- [ ] Do you track digital references to executives, family members, or travel that could elevate exposure?
- [ ] Can you assess whether threat language or grievance behavior online may lead to real-world escalation?
- [ ] Is OSINT consistently integrated into how your team gathers intelligence, prioritizes concerns, or informs protection plans?

Build a Flexible, Repeatable EP Program Structure

Assessing where your executives are exposed is crucial, but it only matters if it drives structured action. Another aspect in building an executive protection program is creating a framework that turns insight into predictable, repeatable results.

Three Pillars to support a successful EP Program Structure

Clearly Defined Roles

Every protection plan must have assigned responsibilities. Who leads the program? Who reviews risk assessments? Who travels with the executive? Defined roles reduce confusion and allow teams to coordinate across functions and locations without hesitation.

Documented Decision Pathways

Risk exposure events require timely decisions. You need to know when to escalate, who approves specific actions, and how information flows during high-stakes scenarios. Documented pathways reduce bottlenecks and prevent costly delays when response time matters most.

Repeatable Processes

Protection efforts should not be reinvented for every itinerary or incident. Repeatable processes, such as travel risk checklists, incident documentation protocols, and escalation playbooks, enable consistency without sacrificing flexibility. They also enable teams to improve and become more cohesive over time.

Whether you manage protection internally, outsource to vendors, or use a hybrid model, these three pillars are foundational to a program that scales according to risk. By building around structure rather than individuals, you strengthen the reliability of your protection strategy and set the stage for operational growth.

Operationalize the Program Across Teams

Executive protection cannot succeed through the efforts of a single person or team. It is the product of coordination between CSOs, intelligence analysts, field agents, program leads, and support roles that handle logistics, travel, and response. The strength of your protection strategy depends on how well these moving parts work together.

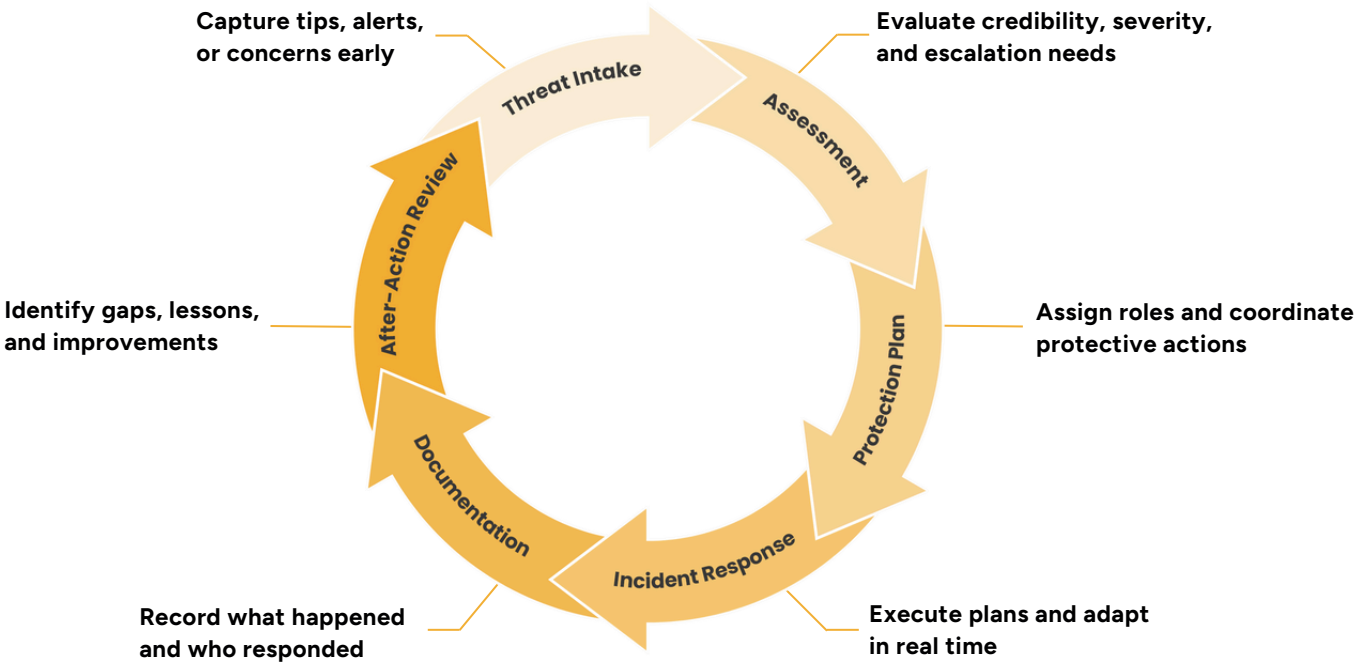
This aspect turns planning into action. It connects risk assessment to execution, and builds the workflows that allow your team to respond consistently across events, time zones, and threat levels. When operations are coordinated, protection becomes faster, clearer, and easier to improve over time.

One System for Coordinated Executive Protection Management

Kaseware gives protection teams a shared space to manage threat cases, assign roles, and document response in real time. Instead of switching between tools or chasing updates across systems, teams can see what is happening, what is next, and who is responsible.

Access controls ensure the right people see the right information. **Shared dashboards** and **task tracking** keep everyone aligned. When protection teams work from a single source of truth, they move faster and make fewer mistakes, especially in high-pressure moments.

Operational Workflow Cycle



Monitoring Behavioral Threats and Insider Risk in Executive Protection

Effective executive protection extends beyond external threats and travel security. Risk to executives can also emerge from within the organization, either through concerning behaviors directed at leadership or through insider misuse of trusted access. While related, these risks are distinct and must be assessed separately to support sound protection decisions.

Behavioral Threats: Early Indicators of Executive Risk

Behavioral threat monitoring focuses on observable conduct that may signal intent to harm an executive or influence executive decision-making. These behaviors—such as grievance, fixation, intimidation, or boundary testing—may originate from employees, contractors, or external actors and often appear in communications, workplace interactions, or online activity. Identifying these indicators early allows executive protection teams to adjust posture, increase awareness, and intervene before threats escalate.

Insider Risk: When Access Creates Opportunity

Insider risk involves individuals with legitimate access to executives, facilities, or sensitive systems who misuse that access intentionally or negligently. While many insider incidents are non-violent, the combination of access and proximity makes them highly relevant to executive protection.

Where Executive Protection Risk Converges

The highest-impact EP risks arise when concerning behavior intersects with access, authority, or proximity to executives. Effective EP programs continuously assess both behavioral indicators and opportunity, recognizing that executive risk is dynamic, not static.

Supporting Behavioral and Insider Risk with Kaseware Partners

WAVR-21

A structured behavioral threat assessment framework that helps organizations evaluate violence risk and coordinate response across security, HR, legal, and leadership.

LEARN MORE

Posthire

Continuous criminal monitoring that extends visibility beyond periodic background checks through real-time alerts.

LEARN MORE

Strengthen Internal Reporting and Coordination

Why Cross-Functional Alignment Matters

Sensitive issues like privacy, employee behavior, public exposure, and crisis response often sit at the intersection of multiple departments, such as HR, IT, and Legal teams. When these groups operate in silos, early warning signs easily get lost, responses slow down, and risks escalate. Strong executive protection programs define how departments coordinate, share intelligence, and act together before a threat becomes a crisis.

Establishing Reporting and Escalation Pathways

Employees are often the first to notice concerning behavior or reputational risks. When reporting systems are secure and structured, these early signals can reach the right team in time.

With **Kaseware Public Portals**, organizations provide secure reporting channels accessible to the entire workforce. Reports can be submitted anonymously, giving employees a safe way to raise concerns without fear of retaliation. By triaging submissions, HR and security teams can escalate reports that indicate potential executive threats, enabling faster and more informed responses.

Coordination Gaps to Watch For

Even the best tools and protocols fail when coordination breaks down. These are three of the most common failure points to monitor and resolve:

- **Threat intelligence that never leaves a department**
  Signals trapped within one team prevent early intervention. Cross-functional sharing ensures risks are seen and addressed.
- **Delayed action because no one owns escalation**
  Unclear roles can stall response. Teams need defined authority and clear escalation paths.
- **Lack of documentation for legal, HR, or communications follow-up**
  After an incident, centralized records are critical for investigations, reviews, and accountability.

Prove the Program Works and Saves Money

Executive protection can be a difficult line item to defend. And often the executives you're trying to protect are your greatest barrier to a more effective executive protection program. When programs work, incidents are avoided, and when incidents are avoided, leadership may question whether protection was ever needed in the first place.

But the value of executive protection is not theoretical. Market volatility, legal fallout, and reputational damage can result from a single high-profile event. According to SHRM, **the average cost of a single workplace violence incident is estimated at $250,000**. When an executive is involved, those costs often rise dramatically due to shareholder response, media scrutiny, legal proceedings, and long-term brand impact.

Among the biggest challenges to proving the value of an executive protection program is calculating ROI and ensuring executive compliance to the program.

Proving Impact Through Data

To justify investment, you must continually prove performance results. That means building reporting systems that show how the program reduces risk and improves readiness over time. Track and report on:

- Risk trends and exposure across executives, regions, or time
- Response timelines and escalation speed
- Threats detected, mitigated, or prevented
- Incident patterns and areas for program improvement

According to a recent report, in 2024, about **31 percent of S&P 500 companies reported providing executive security perks**, with a median cost of roughly $94,276, more than double the median from 2022. That increase reflects a broader shift. Companies are no longer asking if executive protection is worth it. They are asking how to measure and sustain it.

Getting Buy-In Without Fear Mongering

Executives typically don't respond well to scare tactics, and they shouldn't have to. The key to buy-in is positioning security as a business asset, not just a response plan.

Proving Impact Through Data

Lead with Value, Not Fear
Rather than providing the latest sensational headlines,instead, focus on how protection enables business continuity, protects shareholder value, and ensures operational stability, especially in high-risk regions or roles.

Offer Options, Not Ultimatums
Executive buy-in improves when leaders feel in control. Offer structured choices that meet risk standards, like travel protocols or communication safeguards, without forcing a one-size-fits-all mandate.

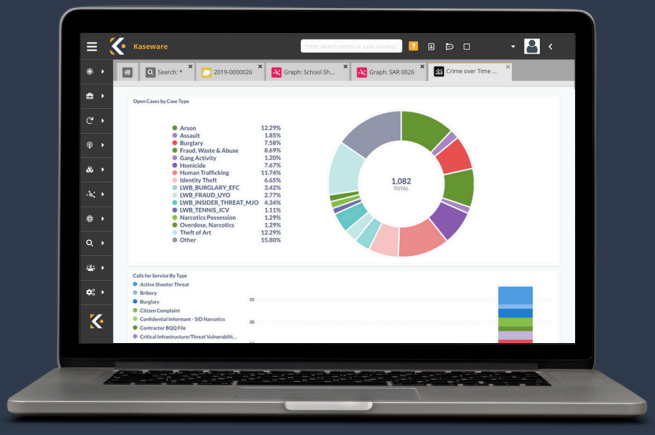
Make Security a Business Enabler
The best protection programs don't slow down the business—they support it. When security becomes seamless and data-backed, executives are more likely to see it as a smart investment, not a sunk cost.

Reduce Cost with Fewer Systems

Many programs struggle with overlapping tools, fragmented workflows, a lack of integration and inconsistent documentation. Streamlining your technology stack improves efficiency and reduces cost over time.

- Consolidated case management and reporting reduce tool overlap
- Streamlined workflows lower administrative burden
- Standardized documentation supports regional consistency and executive visibility

Kaseware helps protection teams centralize documentation, analyze results, and communicate program value with clear, defensible data.



LEARN MORE

Technology That Powers Executive Protection

Strong executive protection depends on good coordination and good information. Technology helps teams plan, communicate, and respond more effectively, while staying aware of issues that may affect the safety of executives and their families.

KASEWARE

SCHEDULE A DEMO

KASEWARE: INVESTIGATIVE CASE MANAGEMENT AND INTELLIGENCE IN ONE PLATFORM

Kaseware provides investigative case management and intelligence solutions in support of executive protection within one secure system. Built by former FBI Special Agents and used globally, Kaseware enables consistent workflows, structured documentation, and faster response. Built by former FBI Special Agents and used globally, Kaseware enables consistent workflows, structured documentation, and faster response.

OSINT COMBINE

SCHEDULE A DEMO

OSINT COMBINE: ADVANCED OPEN-SOURCE INTELLIGENCE SOFTWARE AND TRAINING

OSINT Combine, now merged with Kaseware, is a veteran-operated leader in open-source intelligence software and training. Their platform, NexusXplore, expands situational awareness beyond the physical protective environment. With NexusXplore, analysts can efficiently identify executive digital exposure, monitor threat-relevant online activity, and surface early warning indicators. When integrated into executive protection workflows, OSINT helps teams anticipate emerging concerns earlier and make more informed protective decisions.

Together, these technologies turn executive protection strategy into **real-world capability**—from **early detection** to **coordinated**, **defensible action**.

Build Your Executive Protection Program with Confidence

The Executive Protection discipline is continuing to evolve and adapt. Once viewed as a specialized service only for high-profile individuals, it is now becoming a strategic priority among organizations navigating a more complex and volatile threat landscape.

Today's threats evolve quickly and come from more directions, spanning physical, digital, reputational, and internal domains. Protecting executives effectively now demands intelligence capabilities, cross-functional coordination, and the ability to respond to risk signals before they escalate. Programs that do not adapt will fall behind as the expectations and risks continue to grow.

A Final Note: Emerging Risks to Watch

Synthetic Media and AI Impersonation
Deepfakes and generative AI are making it easier to impersonate executives, spread false narratives, and launch reputational attacks at scale.

Digital Threats Turning Physical
Online harassment, doxxing, and ideological targeting are increasingly moving from screen to real-world action often with little warning.

Evolving Insider Threats
Insider threats are becoming harder to detect as personal grievances, social influence, and access to data create more complex risk profiles.

Geopolitical Volatility and Unpredictable Travel
As global instability increases, executive travel is becoming harder to secure, especially in regions facing political unrest or economic stress.

Breach-Driven Executive Exposure
With more executive data available from breaches, targeting is becoming more personalized, calculated, and difficult to anticipate.

As threats become more dynamic and personalized, executive protection must evolve in step. Programs should continuously reassess exposure, test protocols, and prepare teams to respond to risks that look different than they did a year ago.

KASEWARE

Mission Focused. Outcome Driven.

One system to connect investigative teams and tools to identify, uncover, and protect

Backed by Expertise

Founded by former FBI Special Agents our platform is continuously guided by former law enforcement and security professionals.

Consolidate to One System

Collect, analyze, and connect information and people working an investigation in a single place, for a single pane of glass view.

Highly Configurable

Modify the platform to your unique workflows and processes to maintain compliance, avoid mistakes, and make connections.

Schedule a Demo

www.kaseware.com
salesteam@kaseware.com
+1 (844) 527-3927

Respond • Investigate • Resolve