SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Increasing Digital Confidence and Real-World Safety with Proactive Threat Management

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of viable options in the marketplace. Proven Solution Innovation Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study demonstrates Pine Risk Management's innovative capability to proactively identify and remove exposed personal information that adversaries use to locate, target, and harm executives, employees, and their families. This solution serves as a forward-looking early-warning system, including custom monitoring that flags threats to specific high-risk individuals in real time, closing the gap between digital exposure and physical risk.

Risk Issues and Mitigation Opportunities:

The client needed to get ahead of a threat environment expanding faster than any single tool could keep up with. Data exposure, scams, weird emails, online and physical threats, and reputation risks all came into play:

- **Extensive, exploitable exposure.** Home addresses, phone numbers, family relationships, and daily patterns for key personnel were available and accurate across hundreds of broker sites. These records are the starting point for doxxing, harassment, stalking, and fraud.
- **Confidence builders:** Based on their risk landscape, the client required white glove threat assessment and response that do not fit a standard call center or software-as-a-service offering. They need a solution strategically identifies and removes exposure.
- **Non-obvious targeting vectors.** Some key personnel had public-facing profiles and outside pursuits that created openings for pretext approaches, where a hostile party makes contact under a cover identity, posing as a peer or a documentary crew, to draw out compromising statements on camera. These are the vectors' automated tools sometimes miss.
- **A landscape shifting fast.** A volatile geopolitical climate meant the client's personnel could be targeted by anyone from ideological groups to government entities, and the picture was changing week to week.
- **Exposure that turns physical.** Personal details online became physical safety, fraud, and social-engineering threats, so digital exposure and physical risk had to be managed continuously as one problem.
- **More than data removal.** The client needed much more than data deletion. It faces scams, social engineering, impersonation, deepfakes and the occasional real, anomalous reach-out that simply feels wrong and needed a fast expert read.
- **Current solution left gaps.** Automated removal, the default most organizations rely on, misses re-exposure and non-obvious sources, cannot exercise judgment, and gives no one to call when something dangerous materializes.

©2026 Security Executive Council. All rights reserved. Learn more: www.SecurityExecutiveCouncil.com

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Increasing Digital Confidence and Real-World Safety with Proactive Threat Management

Solution Requirements:

The client required protection that reduced real risk without adding burden, alarm, or liability. Specifically:

- **Forward-looking early warning.** A system that watches the horizon and flags threats to specific high-risk people before they escalate, so protection stays ahead of the landscape.
- **Human expertise with a side of automation.** Automated scale for breadth, human experts for judgment, the hard removals machines cannot do, and rapid, coordinated response when something dangerous materializes.
- **Direct support for the people at risk.** When a sensitive finding surfaces, someone who will sit with the affected person and help them fix it instead of hanging in a leadership a report.
- **One integrated partner.** Privacy findings feeding threat intelligence and physical and executive protection decisions, and family members covered, all under one partner rather than a patchwork of disparate vendors.
- **Low burden, high discretion, and adaptability.** Fast onboarding, no added risk or attention, and protection that evolves as data-collection and attack methods change.

Delivered:

Pine Risk Management (PRM) has served as the primary security and risk management partner to this large non-profit organization with a high-profile executive team, supporting the client across threat intelligence, physical security, incident management and escalation, executive-safety monitoring, and security awareness and physical security training. The client is proactive by nature, but a rapidly shifting threat landscape in their sector, driven by a volatile political and geopolitical climate, raised the stakes for their leaders. This case study focuses on the program at the center of that partnership: Protective Privacy.

The partnership began with a digital exposure penetration test: PRM stepped into the shoes of malicious actors, searching for sensitive information that can be used against the organization, its leaders, and key employees. Once the exposure was understood, PRM inoculated the client against the tactics most likely to be used against them through training, monitoring, mitigation, and response.

PRM delivered Protective Privacy, an ongoing, human-led program backed by automated monitoring. Five capabilities carried the work:

- **The Exposure Watchdesk: custom, targeted early warning.** Standard social-media monitoring is a dashboard someone logs into to review threads after the fact. PRM's Exposure Watchdesk was

©2026 Security Executive Council. All rights reserved. Learn more: www.SecurityExecutiveCouncil.com

more effective. Working from the client's highest-risk individuals, analysts mapped the specific places those people would be discussed or targeted: hostile forums, certain government-linked outlets, and high-reach social accounts. A purpose-built system watches a large volume of those sources around the clock, at scale, for any sign that a protected person is being named, harassed, or targeted. When something triggers, a PRM analyst investigates within minutes to judge whether it is credible, and a persistent alert (email, text, and phone) repeats until both PRM and the client's designated security, HR, and/or executive stakeholders have acknowledged it. Unlike reputation monitoring, this hunts specific, high-risk threat cases and produces immediate, human-verified alerts. It is how PRM goes to bat for the people it protects.

- **Adversarial exposure research and removal.** Automated removal across 590+ data brokers became the first line of defense, not the only one, run continuously with before-and-after verification. On top of it, analysts ran manual adversarial searches, thinking like an attacker across property records, voter-registration location (widely accessible even after other data is deleted), mobile-carrier data, social media, and facial recognition of the open web, the non-obvious sources most competitors skip. When a sensitive finding surfaces, PRM meets one-on-one with the affected person to counsel them through addressing it.
- **Breach, impersonation, and deepfake monitoring.** Dark-web and breach searches for exposed credentials, with optional 1:1 sessions so high-risk individuals can see exactly what an attacker sees and gets support as they address the risks during the call. Facial-recognition and deepfake monitoring, plus fake-profile, fake-job, domain-spoofing, and DMCA work to shut down impersonation of the people and brands.
- **Rapid response and a human helpdesk.** When doxxing or a credible threat appears, PRM drove coordinated takedown and suppression across hosts, providers, domain owners, and search. Between incidents, a human helpdesk answers the "Is this real?" questions and triages the anomalous reach-outs, enabling the business and building confidence that proportionate help is one call away.
- **Awareness, inoculation, and integration.** Training tied to each person's real exposures and current tactics, from deepfake demonstrations to live account lockdowns. Everything integrated with the client's threat-intelligence and physical and executive-protection program, with home-security reviews, TSCM sweeps, standby executive protection, and an IRS Section 132 assessment available as needed. PRM's team is unusual in being both practitioners who ran these programs inside companies and consultants who frequently see the same threats across industries.

Outcome and Benefits of Service:

The program delivered a set of benefits leadership could act on and report:

- **Early warning that buys time.** Anecdotally, insurance costs remained flat and were reduced in some areas. The client’s confidence level of effectively assessing and responding to threats was 5 out of 10 before PRM and then moved to 9.5 out of 10 once PRM’s solution was implemented. HQ

©2026 Security Executive Council. All rights reserved. Learn more: www.SecurityExecutiveCouncil.com

re-location cost and efforts were optimized, with a more effective, holistic risk assessment being completed by PRM.

- **Exposure that automation misses.** Manual adversarial research surfaced non-obvious vectors, from property and registration records to pretext-approach openings, that a data-removal subscription most likely will never catch. PRM worked directly with the affected people to close them.
- **One coordinated program instead of many vendors.** Privacy, threat intelligence, and physical security under one partner removed the cost and the gaps of stitching together point vendors. Program costs fell roughly 10% after the first year as onboarding efforts drop, a savings passed to the client.
- **The family attack vector.** Protecting household members removed the easiest path an adversary had to reach a principal.
- **Eliminate Distractions.** Leadership was able to show what information may have been exposed and what is being done about it, supporting Board, insurer, and IRS Section 132 discussions. Dedicated third-party security leadership gave executives and employees confidence that an experienced team of security experts who know their business are monitoring and addressing physical and digital threats. With PRM, the client received a human-verified response and recommendation to each threat, finding the exposure missed by automation.

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations.

Note: *The Security Executive Council's Solution Innovation case study represents a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

A General Comparison of Competition

Three things set this solution apart: a custom early-warning system that flags threats to specific high-risk people in real time, with a human read within minutes; manual adversarial research and facial recognition that dig into sources most services skip; and one partner covering digital privacy, intelligence, and on-the-ground physical protection, with a dedicated team working alongside your organization and impacted personnel.

©2026 Security Executive Council. All rights reserved. Learn more: www.SecurityExecutiveCouncil.com

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Increasing Digital Confidence and Real-World Safety with Proactive Threat Management

Marks reflect publicly available information and PRM's assessment of the market as of the case-study date; competitors are welcome to confirm or correct.

Attributes / Capabilities	PRM	Company A	Company B
Continuous monitoring and removal across 650+ data brokers	YES	YES	YES
Coverage extends to executives' family members	YES	YES	YES
Dark Web / breach exposure monitoring	YES	YES	NO
Facial-recognition monitoring of the open web	YES	NO	NO
Manual adversarial research (property, voter-registration, telecom, social)	YES	NO	NO
Custom targeted-threat early warning with human triage in minutes	YES	NO	NO
Rapid doxxing response: takedown and suppression	YES	UNSURE	NO
One-on-one counseling of the affected person, not only a report	YES	UNSURE	NO
Awareness training tied to each person's real exposures	YES	NO	NO
Integrated threat intelligence (geopolitical, strategic, opposition)	YES	NO	NO
Integrated on-the-ground physical and executive protection	YES	NO	NO
One partner across digital privacy, intelligence, and physical security	YES	NO	NO

Legend: **YES** capability present **NO** not offered **UNSURE** varies / not publicly confirmed

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/solutions/vendor-innovations

©2026 Security Executive Council. All rights reserved. Learn more: www.SecurityExecutiveCouncil.com