ONTIC®

Whitepaper

Family Office and High-Profile Security

Three Ways to Elevate a New Standard of Protection

There's a complex web of activity that surrounds high-profile individuals and their families. When you move past the surface of philanthropic events, appearances at exclusive venues, and global travel, there is a great deal of risk to mitigate on a day-to-day basis. So rarely does protection end with the principal — it extends far beyond to family, personal assistants, and even their personal trainers.

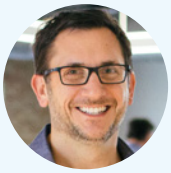
With principals living and operating online and on the ground, the ability to capture more sensitive information is getting easier, as activity and locations can be easily discovered by an adversary.

We must work harder to protect.

As family offices work tirelessly to anticipate risk and protect the activity that orbits around their principal, it's critical to consider ways in which teams can work smarter to identify potential threats before they amount to something greater.

In this whitepaper we share three core considerations to elevate the standard of protection for family office security:

"It's important to reverse engineer things, and put ourselves in the place of the threat actor to figure out, 'What, what steps would I take if I were the bad guy in order to get into the world of this protectee?'"



Thomas Kopecky

Co-Founder and Chief Strategy Officer, Ontic

1

Work Smarter

Adopt a Process That Can Be a Force Multiplier

2

Work in Real Time

Move from Manual to Automated

3

Know What Matters

Maintain Privacy and Discretion

1. Adopt a Process That Can Be a Force Multiplier

The intricacies of protecting a family office take on several roles, reaching beyond the typical duties of a corporate executive protection agent and into projects and assignments that one might never expect.

Oftentimes, “teams” are comprised of one individual in charge of supporting not only the main principal, but their family as well.

Keeping high-profile individuals and their families safe has never been harder. With an unmanageable amount of data coming in from multiple angles, chances are high that a threat will be missed.

With the right technology and systems in place, offices can see threats with more clarity and context and deliver a high-level summary to their principal or family office CEO with confidence. Additionally, knowing that your process can easily scale and adapt to changes in team structure and new threats (i.e., health and safety) is critical, because we know that a family office is a business and it must adapt to economic changes.

A PERSPECTIVE FROM A FORMER PROTECTIVE INTELLIGENCE ANALYST
(Professional Sports Team Family Office)

In essence, I was supporting four agendas:

1. The principal as the leader of a multinational corporation;
2. Their family office that included varied business meetings domestically and internationally;
3. The sports team that included more meetings, special events, and of course — the sporting events themselves;
4. The needs of the principal’s family.

Travis Lishok

Associate Director of the Center for Protective Intelligence, Ontic

2. Move from Manual to Automated

Believe it or not, there are more offices than we realize that rely on hard copy reports. This leaves teams scrambling to connect the dots when an issue arises — unsure if it relates back to a known threat actor, or is something entirely new.

Managing a principal's online presence is imperative in this day and age, as even the smallest piece of information sets an adversary down a path to find out more intimate details about a principal.

Specifically, here are a few ways to manage online presence and ensure intelligence is always on:

SOCIAL MEDIA TRAINING

Informing high-profile protectees (principals, families and their teams) on the power of social media and the risks associated with sharing your location, travel, etc. It requires discipline to remain discrete and it often takes a difficult conversation about the principal's children to mitigate possible risks down the road.

NEWS AND MEDIA

Depending on the principal's role (professional athlete or high-profile CEO), media is never far behind. "From my own interactions with diverse intelligence teams, there appears to be a correlation between the volume of inappropriate contacts and the number of times the principal is mentioned in the news. Similar to marketing a brand, if your name is mentioned enough then it creates awareness — but this awareness can also trickle down to those that you'd prefer keep a distance from your protectee," says Travis Lishok who formerly supported a high-profile family office.

ALWAYS-ON MONITORING

Automation allows for information to be surfaced as soon as a threat arises. Being alerted in real time to something as small as a speeding ticket can inform a team that a POI is in the vicinity. Manually monitoring for new activity leaves room for error - especially as the list of threat actors expands.

"We use a white glove service to continuously monitor doxxing and threats surrounding our executives. If an executive prefers to be hands-off, our security team is allowed to continually monitor new threats, new personal data that is showing up online, and see what data is getting removed from the internet by our service."

Senior Manager, Corporate Security — Media and Technology Company

3. Maintain Privacy and Discretion

It's no surprise that family offices require the utmost level of privacy and discretion in their day-to-day operations. Even the smallest oversight can result in harm to people or assets.

Whether it be negative news mentions or something as large as mitigating a stalker's actions, there is no detail too small.

A threat that often drives many personal security decisions is the concept of kidnapping — specifically targeting significant others or children. However, as Fred Burton, Executive Director of the Ontic Center for Protective Intelligence, shares, "Threat of kidnappings is very low for high-net worth families and CEO's within the United States. I've come to believe that these kidnapping fears are not based on facts, but driven by perceptions and the media interest surrounding historical cases."

PRE-OPERATIONAL SURVEILLANCE

One of the most well-known kidnapping cases is that of Sidney Reso, the former President of Exxon International. The details of what unfolded on a seemingly routine morning opens our eyes to the negative implications of having a predictable routine and one that is easily surveilled. Author Philip Jett shares that it took five months of surveillance going out to this subdivision at different times of the day to observe Reso's actions from a construction site across the street from his residence.

Stalking is also a common threat when it comes to high-profile individuals. It carries the same urgency of being diligent about pre-operational surveillance that other threats do, as they precede potentially more violent events or actions. According to Reid Meloy, forensic psychologist, author, and co-founder of WAVR-21, "The other thing we know about stalkers, in general, is they tend to be at least average IQ, if not brighter. So a lot of times they have the cognitive ability to be able to plan and prepare sometimes elaborate ruses or certain disguises, things of that nature as a way to pursue their target."

IDENTIFYING WARNING SIGNS

Having technology that spots and surfaces warnings of potential stalkers, social media threats, etc. is a key component in avoiding small issues and worst-case scenarios. It's critical to identify and act on warning signs. But with limited resources and only so many hours in the day, how do you know what actions to take next?

Family offices benefit from streamlined tools that guide the identification of threats, gathering of information, assessment, creation and implementation of plans for addressing threats. Knowing a threat is out there is one thing, but effectively taking action on it creates a safe environment, trust with your principal, and ingrains a repeatable process that teams can depend on. Because we know all too well that a quiet day is rare in today's threat landscape.

Final Thoughts

Know your threats. Every family office has them, but each one is unique to the principal(s) you are protecting. As Fred Burton shares, “Security programs and systems should be threat-driven, taking into consideration a holistic and comprehensive view of the risk.”

In order to fully understand the risk to your family office, the first step is to hire a reputable firm to do a baseline threat assessment to understand what you are protecting against. This includes assessing the online presence of the principal and their family, and hunting for adverse intelligence, negative sentiment or targeted threats.

Let’s make nothing happen together™

Named the top industry innovator in the Frost Radar™: Digital Intelligence Solutions, 2021, Ontic is the first protective intelligence software company to transform how Fortune 500 and emerging enterprises address physical threat management to protect employees, customers and assets. Ontic’s SaaS-based platform collects and connects threat indicators to provide a comprehensive view of potential threats while surfacing critical knowledge so companies can assess and action more to maintain business continuity and reduce financial impact. Ontic provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals through its Center for Protective Intelligence and Center of Excellence, the latter of which also offers program development and training services in behavioral threat assessment, threat management, and violence prevention for major corporations, educational institutions and government agencies.

For more information please visit ontic.co or follow us on Twitter @ontic_ai

ONTIC®