ONTIC

Guide

Seeing Around Corners

Defining a Proactive Approach to Security and Five Reasons Why It Can't Wait

Technology has given more industries than we can list a reason to reinvent their business model. Security and protection teams are no exception. The concept of protection as it relates to people and assets has evolved dramatically, and it's hard to believe we once relied solely on guesswork, binoculars, and 3x5 index cards to assess a case.

The way companies collect and connect information can turn fragmented data into actionable intelligence. This allows teams to quickly detect and disrupt possible threats. This technology-supported approach, referred to as protective intelligence, allows teams to act thoughtfully and proactively. They can see through the noise to know what to act on and when.

Protective intelligence is not the most common term among security professionals, but the concept has been around longer than we realize. What is it exactly?

pro•tect•tive in•tel•li•gence

Protective intelligence is an investigative and analytical process used by protectors to proactively **identify, assess,** and **mitigate** threats to protectees.

In this guide, we'll break down the components that make up the tradecraft of protective intelligence. We'll also share five reasons why a proactive approach to security will define the success of companies and organizations in the coming years.

> *"The ability to see around corners has never been more important."*
>
> *Fred Burton*
> *Executive Director of the Center for Protective Intelligence, Ontic*
>
> – Security Magazine

SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

Breaking “Protective Intelligence” into Digestible Components

01 IDENTIFY

How do protective intelligence teams recognize threats?
The most fundamental step in identifying threats is conducting a thorough assessment of the risks and vulnerabilities relating to the assets you're charged with protecting. This allows the organization’s entire security apparatus to implement proactive measures at various levels and quickly share information — before a threat materializes.

However, protective intelligence is only as valuable as it is available and accurate. Security teams need the ability to retrieve data quickly on past incidents to identify behaviors and patterns. All of the information that the security team comes in contact with — from security officer reports, to person of interest (POI) descriptions, to field observations (including vehicle descriptions) – is valuable data and should be stored and assessed thoroughly.

02 ASSESS

Are they a threat, or not?
Security practitioners begin the assessment process by outlining their research, which consists of assessing the problem, collecting and analyzing data, and preparing a report of the findings. To bring color to the threat(s) in need of attention, the investigation may include (but is not limited to) any of the following:

- Security officer reports/chronologies
- Human resources reports
- Open source intelligence (OSINT) research
- Proprietary database research
- Consultation with psychology professionals

CIVIL RECORD
CRIMINAL RECORD
HUMAN OBSERVATIONS
VISITOR MANAGEMENT
BREAKING NEWS
LOCATION DETECTION
DARK WEB SCAN
OPENS SOURCE / SOCIAL MEDIA
VEHICLE LOCATION
INTERNAL / CUSTOM SYSTEMS

03 MITIGATE

What strategy will create the safest outcome for the protectee?
At this point, the security team has sufficient support for why or why not the person of interest (POI) is a threat, and to what degree. They can now decide on the preferred course of action — one that will produce the safest outcome for the protectee.

With upwards of 10 or 20 active threat cases to monitor at any given time, the ability to allocate resources to track and reassess becomes increasingly difficult. Finding a platform that surfaces alerts, according to level of priority, is one way to help. It’s an example of how technology has freed up space for security teams to be the eyes and ears of the company, versus being buried in data.

For protective intelligence teams, monitoring and reassessing are ongoing processes. Many times, there’s no clear-cut indicator for when a particular threat case can be put to rest. It will depend on the judgement of those who know best: security intelligence analysts and leaders.

Five Reasons to Implement Proactive, Always-on Security—Now

We can all agree that a proactive approach to security — or what we call protective intelligence — sounds like a smart idea. No protection officer prefers reacting to a situation as it unfolds. But why is this important to your organization? Here are five imperatives for shifting to a proactive, always-on security mindset today.

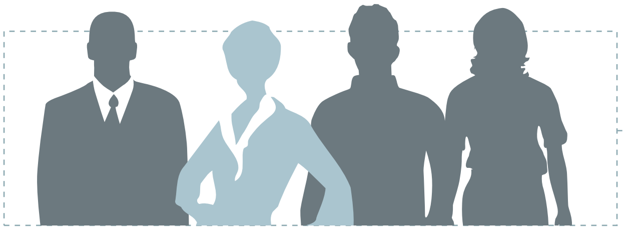
01 YOU HAVE A DUTY OF CARE

Companies have an obligation to ensure the workplace is safe and secure. From workplace violence to active shooters and insider threats, the duty of care for employees is ever-increasingly a company challenge. Physical security threats are on the rise with an increase in both internal and external threats.

1 in 7 Americans say they do not feel safe at work

In the coming years, physical security will be the most important issue corporations need to address. Being safe at work cannot be assumed, and in order to attract top talent, your company must uphold a higher standard of protection.

Staying ahead of the curve helps your team identify early warning signs to manage and mitigate risks, fulfilling your duty of care.



02 YOU FACE DISRUPTIONS TO BUSINESS CONTINUITY AND INCREASED FINANCIAL RISK

Unmanaged physical threats elevate business continuity risk, leading to a substantial increase in financial liability. Security leaders want to go to bed at night more confident that their team will not miss something that could result in a disruption in business continuity, have an unfortunate financial impact to the business, or even lead to loss of life.

The result of just one missed signal has the ability to compound into an all consuming event. The impact is clear:

- The average cost of an insider threat incident is $11.45M. [A]
- The annual cost of workplace violence for employers is $121B, and just one incident could cost your company over $11M. [B]
- In the next four years, three out of every four CEOs will bear personal liability for cyber-physical security incidents, pushing beyond the traditional corporate liability perimeter. Gartner predicts these incidents will increase dramatically in the next few years if the lack of spending in cyber-physical security continues.
- The financial impact of cyber-physical attacks resulting in fatalities will reach over $50B by 2023. [C]

A. Ponemon Institute
B. Department of Justice and the National Institute for Occupational Safety and Health
C. Gartner

03 YOU MUST KNOW THE UNKNOWNS

How many risks are you overlooking? Through active threat hunting, shift from reactive threat defense to a well-deserved sense of control. The threat landscape has fundamentally changed and expanded, creating an enormous increase in data and pre-incident indicators that have become unmanageable. All too often, security teams are relying on reactive threat defense — such as investigating a suspicious vehicle or an internal employee conflict — instead of proactive threat hunting — such as assessing executive travel and running regular, continuous background checks.

By aggregating historical and real-time intelligence in one place, your team can better connect the dots. These dots become intelligence and are integral in better identifying pre-incident indicators, assessing risk, and mitigating potential threats — before it's too late.

04 YOU NEED BETTER VISIBILITY ACROSS THE THREAT LANDSCAPE

Security insights need to be easily accessible and clearly presented to connect the dots and take action. Today's typical security professional accesses at least a dozen different sources of data on a daily basis. What's more, all too often, time-sensitive and sometimes life-saving insights may be hampered by paper records, manual processes, and the potential for associated threats to be catalogued as independent events by siloed teams.

Without a comprehensive view of potential threats to executives, employees, and customers, the gap between a missed signal and a mitigated threat, or even life or death, becomes more and more narrow.

Modern and proactive security organizations take a team approach, and companies need a process to encourage this collaborative framework. Consolidating data across teams for investigations with audit trails, timelines, and link analysis allows for more holistic input and observation, and ensures that everyone can work from the same source, or "same sheet of music." There is only so much information an analyst can gather, evaluate, and understand in a day. The value of trusting one source allows companies to see ahead and catch any pre-incident indicators before a threat materializes.

05 PROTECTION NEVER RESTS

Real time access to data and insights are critical given that threats can live anywhere, at any time. It's hard to be proactive when it takes several hours to assemble a POI report or there's a 24-hour delay in sharing this information between teams that need to know what's going on as incidents transpire. Security teams need the ability to retrieve data quickly on incidents in order to act timely, thoughtfully, and with enough space to think through multiple scenarios.

Investments in data-driven risk management have proven helpful in 2020 as information rapidly evolved during the COVID-19 crisis. In fact, 86% of PwC Digital Trust Insights Pulse Survey respondents identified "real-time threat intelligence" as one of the most impactful investments they've made in the past 2-3 years. Leveraging a database of information that's on 24/7 lowers the likelihood that changes in information will slip through the cracks and helps teams stay ahead when activity veers off center.

Quantifying the Impact of Making Nothing Happen

Security teams work tirelessly to detect threats and maintain control so employees can do their best work and the company can continue to grow. But being proactive isn't the easiest thing to quantify. A security framework that embeds timely and accurate reporting to summarize threats addressed, reports assembled, and persons interviewed demonstrates the safety barrier security teams work so hard to maintain.

The Need for Change Today

Trying to manage a rapidly evolving threat landscape reactively with old school methods is no longer acceptable. Outgunned, security teams must fight fire with fire, and being reactionary will not lead to sustainable outcomes. In order to proactively address these modern threats, security teams need more than data. They need intelligence — in real time. With this mentality and framework, seeing around corners will be the new normal.

Ontic's Protective Intelligence Platform enables enterprise security teams to see around corners and keep their businesses safe.

Learn More

Let's make nothing happen together TM

Ontic is the first protective intelligence software company to digitally transform how Fortune 500 and emerging enterprises proactively 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 also provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals at major corporations via its Center for Protective Intelligence.

To learn more about Ontic's Protective Intelligence Platform, contact us at info@ontic.co

ONTIC