ONTIC

The Complete Guide to Buying Protective Intelligence Software

WHAT TO LOOK FOR WHEN CONSIDERING A PROACTIVE THREAT MANAGEMENT PLATFORM

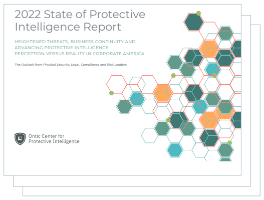
TURN THE PAGE TO DIVE DEEPER INTO THE FOLLOWING

Executive Summary

Threats infiltrate nearly every aspect of business, from hybrid work, supply chains and domestic extremism, to cyber-physical insider threats, global security and extreme weather events. Companies and their corporate security teams are being flooded with physical threat indicators. However, it's often difficult to see the signal through the noise.

The lack of a comprehensive view of potential threats to executives, employees, customers and assets and an inability to effectively collaborate at scale could be the difference between a missed threat signal and a mitigated risk. These missed signals can lead to significant financial damage, business continuity and resilience disruption, reputational damage and even loss of life for many organizations.

Take for example the fact that the average cost of an out-of-court settlement for employer negligence in workplace violence incidents is half a million dollars. The average cost of an insider attack and its consequences in North America is $13.7M. The average revenue loss to US organizations that experience supply chain disruptions is $228M. And, three of four CEOs will be personally liable for cyber-physical security incidents by 2024.



2022 State of Protective Intelligence Report

HEIGHTENED THREATS, BUSINESS CONTINUITY AND ADVANCING PROTECTIVE INTELLIGENCE: PERCEPTION VERSUS REALITY IN CORPORATE AMERICA

The Outlook from Physical Security, Legal, Compliance and Risk Leaders

Ontic Center for Protective Intelligence

Ontic's 2022 State of Protective Intelligence Report

The impact of a missed threat is clear and as corporate security professionals know best, the days of waiting for something to happen are long gone. Once an incident occurs, it's often too late. No security team wants to be left cleaning up, trying to connect the dots post-incident, struggling to explain why signals were missed while the business leaders are attempting to keep operations moving, address employee concerns and salvage the company's reputation.

All of this is why there is a widespread movement underway to transform physical security. Almost universally, 95% of respondents in Ontic's 2022 State of Protective Intelligence Report say U.S. companies in 2022 are actively consolidating their multiple threat intelligence, monitoring and alerting solutions into a single software platform that enables holistic data analysis and reporting across physical security, cybersecurity, HR, legal and compliance.

To be successful in this time of consolidation and transformation, it's essential you select a protective intelligence software platform that solves your unique problems. To do so, you'll need to clearly define your own needs, as well as have a good understanding of how different vendors' capabilities meet those needs.

Leverage this guide to inform your decision on selecting a software solution that enables a proactive approach to help protect your employees, customers and assets while improving security and operational efficiency, minimizing organizational risk and reducing complexity across the organization.

Why Protective Intelligence Software?

Protective intelligence means many things to many people. To the security intelligence analyst working in a 24-hour GSOC, protective intelligence is one thing. To the security consultant with an MA or MS in psychology, protective intelligence means something else. To the U.S. Department of Justice or the U.S. Secret Service, it takes on another meaning.

pro•tect•ive in•tel•li•gence

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

It may also be called something different depending on who you talk to – threat intelligence, digital intelligence, security and risk management, threat management, physical security information management. The list goes on.

At its core, the most defining element of protective intelligence is its proactive rather than reactive approach to threat management.

In simple terms, protective intelligence is the process used to identify and assess threats. A well-designed protective intelligence program will have a number of distinct and crucial components or functions, but the most important of these are:

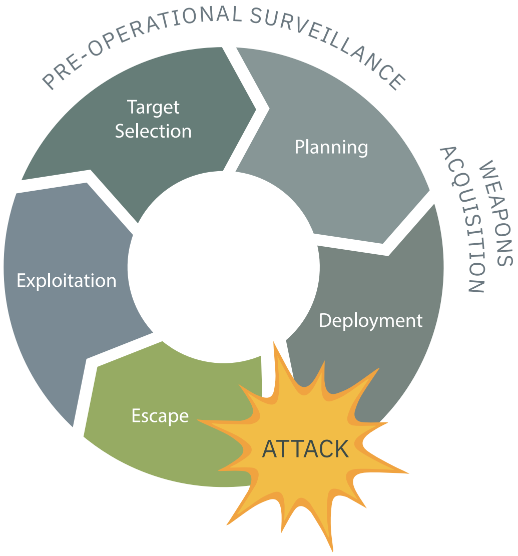
- **Countersurveillance**
- **Investigations**
- **Analysis**

However, to implement an effective security program it's essential to first understand the threat. Knowing the threats you're facing should be the "center of gravity" for your security program.

THE ATTACK CYCLE

The concept of the attack cycle arises from counterterrorism cycles. Bad actors follow familiar patterns before, during and after an attack no matter their motive. While this framework was developed for counterterrorism purposes, its concepts can be applied to protective intelligence.

Together, target selection, planning, deployment, attack, escape and exploitation are the parts of the attack cycle. For corporate security teams, the planning and target selection phases of attacks are the best opportunity to disrupt and interrupt.



THE RISK OF ‘BUSINESS AS USUAL’

Unfortunately, many corporate security teams know the attack cycle exists but because of limited staff, budgets and lack of internal buy-in from key decision-makers they are stuck in a place of operating the same way they always have been.

Business as usual can mean many different things depending on the structure of the program. **Here is one example.**

CURRENT STATE OF PROGRAM

- Team members spend time between multiple, disconnected tools trying to connect data points
- There’s a low level of confidence in the awareness of all potential threats
- It’s unclear what tasks have been completed and what to do next
- It’s impossible to monitor all the activity and identify the signals that need attention
- There are too many sources of potential threats and it’s hard to keep up

CONSEQUENCES OF CURRENT STATE

- Time is wasted jumping between tools attempting to piece together a holistic picture
- The threat landscape is growing and important signals are being missed
- Your data is stored in multiple places and there is limited visibility across the organization (HR, legal, cyber)
- There is no confidence in being prepared to act quickly to mitigate risk and avert incidents

So, let’s say one of these consequences results in a severe workplace violence incident at the company’s headquarters. Now the reputation of the corporate security team will take a major hit within the company. There will be internal audits (Risk, Compliance, Legal) questioning everything the team does in an effort to understand what went wrong. Risk controls will need to be updated to help prevent this from happening again. Policies and procedures will be implemented to support those risk controls in an attempt to ensure this never happens again.

And all of those things only do one thing – make the job of corporate security that much harder.

This is why protective intelligence software is a force multiplier for an enterprise. It gives one central destination for corporate security programs, a place to store data, collect research and investigate threats, provide cross functional collaboration and communication for the security team and across the organization and offers a full picture of the threat landscape tied to actionable workflows for a coordinated response — ensuring business continuity to protect company value.

Navigating the Buying Process

Whether this is your first time purchasing software or you're a seasoned buyer, being familiar with the documents and steps listed below will be important. Best practices for each step of the buying process include:

1. UNDERSTANDING YOUR INTERNAL STAKEHOLDER MOTIVATIONS AND HOW TO COMMUNICATE VALUE
2. PURCHASING AND PROCUREMENT
3. INFOSEC / IT APPROVAL
4. MASTER SERVICE AGREEMENT APPROVAL AND SIGNATURE

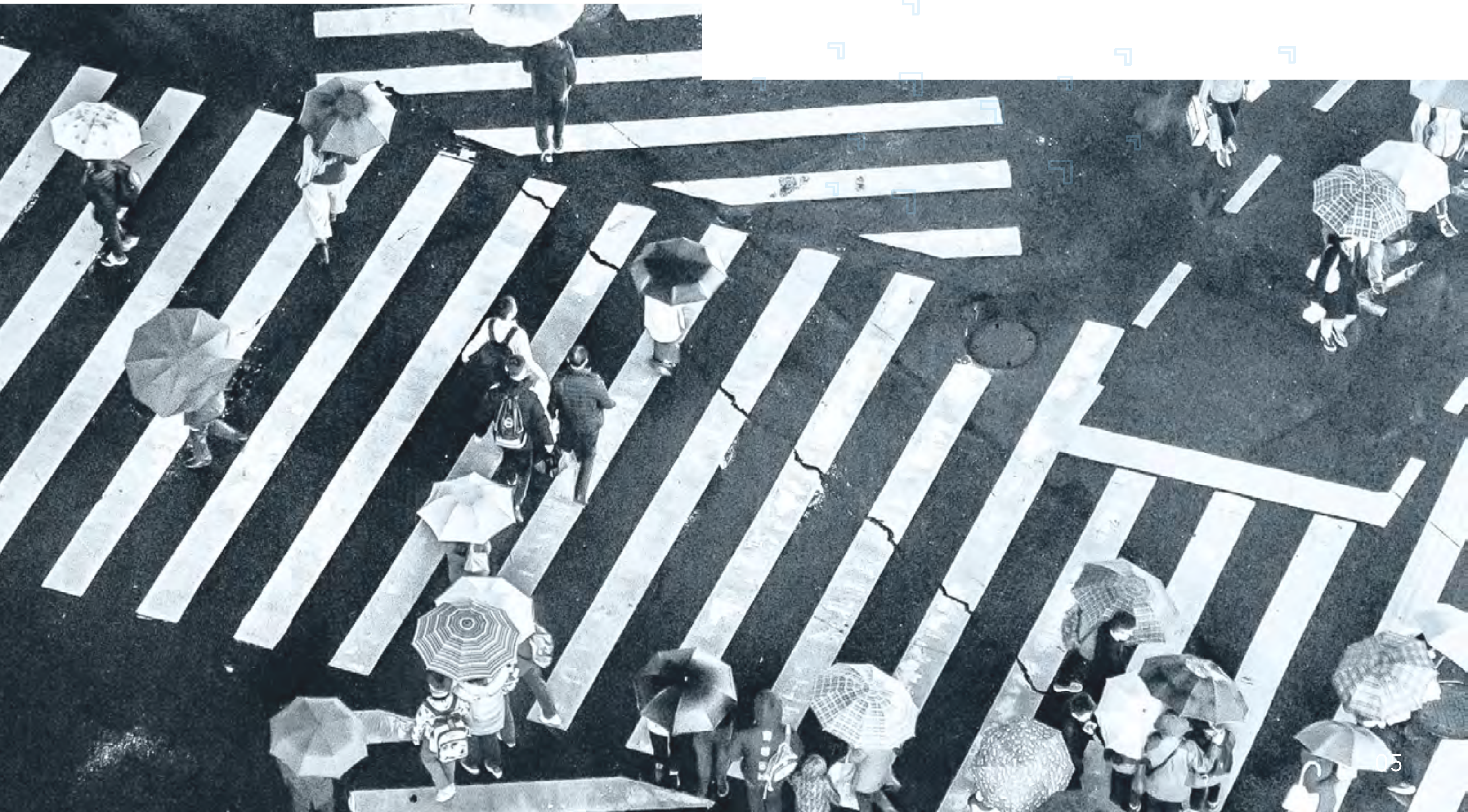
1 UNDERSTANDING YOUR INTERNAL STAKEHOLDERS AND HOW TO COMMUNICATE VALUE

Most of the time corporate security teams align with a department that is not involved day-to-day in security. They may have limited direct access to senior leadership and find themselves fighting for budget dollars alongside more visible counterparts like cybersecurity. This makes the process of gaining buy-in for a protective intelligence platform that much harder.

No matter what group you report into, or who it is you need to secure buy-in from, whether it be the legal, risk and compliance team or the business resilience team, or even the finance/procurement team, it's important to involve key stakeholders from the beginning. Ensure that you're not only involving them but that you're demonstrating the value along the way.

It all starts with knowing the priorities and motivations of internal peers and stakeholders across the organization so that you can earn their attention and foster a sense of trust. Better understanding their needs and motivators mean you'll have an easier time tailoring your approach and solutions to keep them engaged.

According to The Security Executive Council (SEC) **there are several things you can do to understand internal customers better and earn their buy-in. Learn more on the next few pages:**



Personas

Personas are research-based prototypes developed to represent individuals within a demographic — including their challenges, needs and motivations. These highly realistic yet fictional characters can help you understand how a person might feel about a product or service offering.

Let’s highlight the legal, risk and compliance function as an example. Below will help you better think about the role of this stakeholder as it relates to the use of a proactive threat management platform, as well as the risks they care about most.

By better understanding each persona’s responsibilities, goals, challenges and what resonates, you can better tailor your position as to why a protective intelligence platform is needed.

There are two strategies you can use to understan your personas:

1. Observations from day-to-day interactions such as meetings and conversations.
2. Surveys or interviews where you ask questions about goals and objectives to gauge how people feel about the existing security program.

Legal, Risk and Compliance

Primary Job Responsibilities

- Oversee litigation matters related to M&A, significant cases, incidents and investigations
- Review key cases with the CEO and manage legal spending and global legal considerations
- Lead the legal function, provide the leadership team with legally sound advice on organization issues, limit risk, ensure legal compliance
- Partner with finance, HR, Security and others to develop policies and procedures that support a safe work environment and consistent application

Goals

- Protect the company assets and bottom line with appropriate policies and procedures
- Improve cross-functional communication and collaboration to ensure consistent compliance and minimize risk
- Ensure proper documentation and consistent procedures in legal matters while reducing the cost of investigations and outside counsel

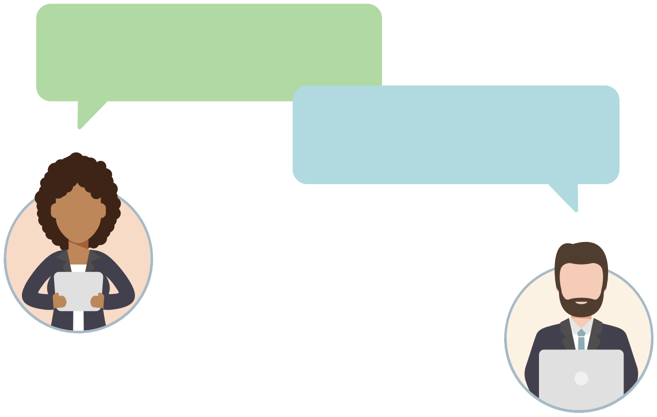
Their Challenges

- Having proper visibility of incidents and investigations to understand the risks to the organization and provide appropriate guidance
- Collecting all information and documentation related to risk, the mitigation decisions and mitigation actions to support a defensible program
- Ensuring that all security operations are practiced within the laws and data privacy and compliance rules are consistently met

Messages That Will Resonate

- Proactive identification and forecasting of isks to minimize disruptions and damage
- Increased visibility of threats and vulnerabilities across the organization and for executives
- Consistent, standardized data collection and analysis and investigation procedures

Interviews



Candid conversations can be helpful, but having more formal interviews with a standardized set of questions is better — especially when speaking with senior stakeholders. This will help you explore their understanding of your program, existing security-related concerns and perceived ownership of security processes.

When compiling your survey, consider the following:

- Select simple but specific questions:
  "Please rate your confidence in the visitor badging system on a scale of 1 to 10."
- Make questions relevant to each audience:
  "As an HR leader, how satisfied are you with the visitor check-in process for candidates visiting the building?"
- Include a few open-ended questions to allow comments:
  "If you could change anything about the organization's on-site security, what would it be?"
- Don't provide too many answer options

Here are a few things you can do to ensure your interviews are a success:

- Create a base set of questions and tailor them to each audience or role
- Follow your line of questioning and leave room for outside comments and follow-up questions
- Consider having someone outside the security team conduct the interview (to ensure interviewees are forthcoming)
- Retain a professional security research and advisory group that can help you

Surveys

A satisfaction survey can help you better understand the effectiveness and value of your program by determining how people perceive security within your organization, as well as what's working and what's not. This will help you glean insight into how you can better engage end-users.

For example, you might discover that onsite employees are frustrated by an unreliable keycard entry system, so they think nothing of holding the door open for others and potentially allowing unbadged people to enter the building.

Be prepared

While you might be fully convinced of the platform's capabilities and value, others may not be. Don't get caught off guard with typical questions those who are not as convinced may ask in water cooler (or these days, Zoom) conversations. Below are questions you may be asked as well as some potential responses. Be sure to customize these responses to be specific to your business and work with the vendor to help provide specific proof points to back you up.

QUESTIONS	ANSWERS
How does the platform address challenges our team faces when it comes to efficiency and gathering information?	The platform has built-in continuous monitoring and storage of all of our data. It provides real-time activity to everyone on the team within one platform so that we don't have to keep jumping back and forth between multiple tools.
There are only so many hours in a day. How effective is the platform in helping our team actively manage threats?	A lot of the tools we currently use are not providing data in real-time nor are they helping us to surface what really matters through all the noise. This platform has automated data collection, storage and reporting on threat actors and risks and provides automatic updates to activities on POIs or open cases.
There are inevitably many threats that we aren't even aware of yet. How can the platform help us identify the unknown threats that have the potential to cause harm to the company?	The great thing about this platform is that it has direct integrations with public data research tools and data providers to help us ensure we're not missing any threats that may result in larger risks to the company.
How does the platform ensure long-term business resilience, continuity and reputation?	The key to this platform is proactivity. Because it has built-in continuous monitoring of data, activity and records to surface new and updated information, we can ensure we're being less reactive ultimately making us more resilient as an entire organization.

2 PURCHASING AND PROCUREMENT

If your company has a Purchasing and Procurement department, it is common for this team to be involved throughout the process. (If you'll be the purchasing contact, skip to the next step of the buying process)

There are a few important elements you'll want to ask about upfront:

Procure-to-pay (P2P) system
Does your company have a procure-to-pay (P2P) system in place such as COUPA, SAP ARIBA, or Ivalua? If so, there is typically a standardized process associated with moving a contract through the system.

Purchasing contact
Will someone be assigned from the Purchasing and Procurement department? What is this individual's role (Contracts Administrator, Procurement Officer/Specialist, etc.) and how do they perform their duties as a liaison between your company and the vendor?

Vendor validation team
Is there a separate Vendor Validation team? It is customary for all new vendors to be verified, which typically requires a unique form to be completed that can include standard items, such as Ontic's W-9 and banking details.

Do note that the Purchasing and Procurement individual is typically juggling multiple administrative duties for incoming vendors in various stages. Ask the vendor to do everything in their power to make things easy with all of the documentation bundled up and ready to go for your team. Also, check to see if they are already an established vendor in the most common P2P platforms.

3 INFOSEC / IT ASSESSMENT AND APPROVAL

On occasion, you may have an internal team who wants a more comprehensive understanding of the technical deployment of the platform you are considering. It's important to ensure the vendor you're working with has an InfoSec / IT Assessment Manual that outlines the security policies and processes they have implemented.

Keep in mind that IT departments are often concerned with the storage of personally identifiable information (PII). Select a vendor that makes it clear they do not store any customer or financial information and that identified threats with activity that needs to be continually monitored are the only data points being stored.

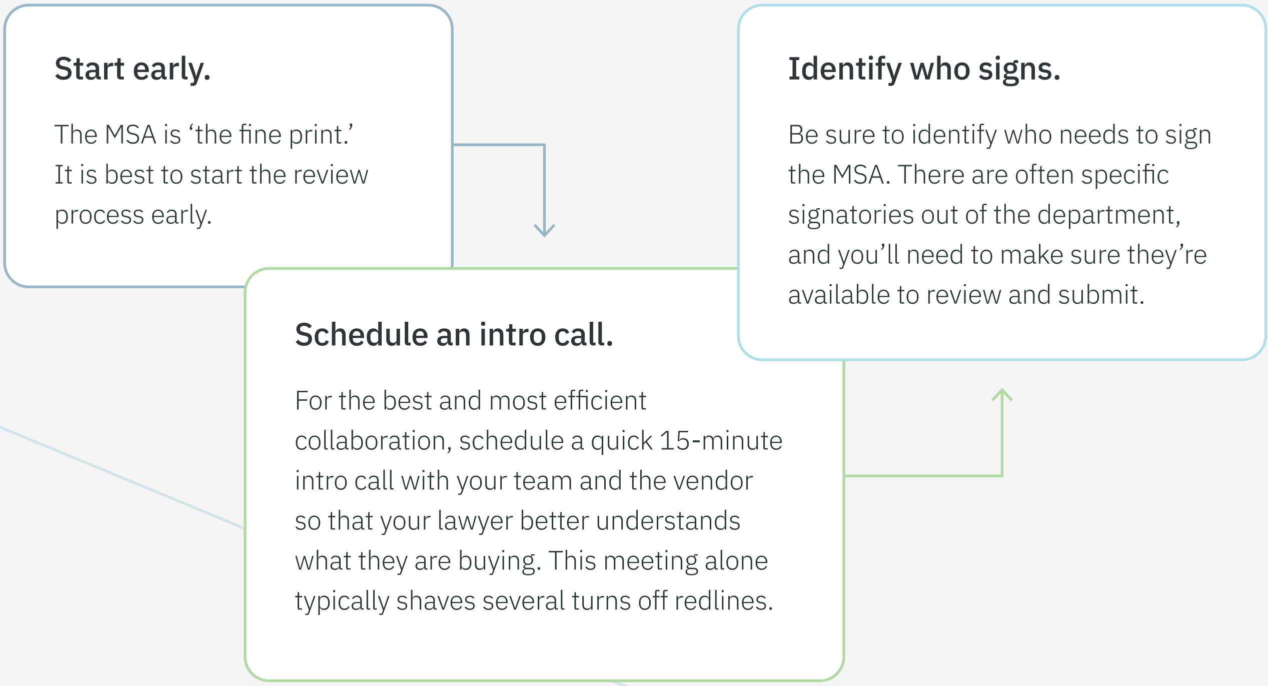
4 MASTER SERVICE AGREEMENT APPROVAL AND SIGNATURE

The Master Service Agreement (MSA) is a legal document that details how you and the vendor agree to do business. There are no financial obligations in this document. Your legal department will likely need to review.

If your company contracts legal counsel for software purchases, it's important to know early on so you can communicate project timeline goals and company-specific information.

If your legal team recommends using their MSA template, let them know that this can cause added time for both sides as the document typically needs to be heavily edited to address the specific nature of that vendor offering and data provider partners.

HAVING ALL TEAMS INVOLVED FEEL GOOD ABOUT WHAT THEY ARE SIGNING IS ESSENTIAL. HERE ARE SOME MSA BEST PRACTICES:



Start early.

The MSA is 'the fine print.' It is best to start the review process early.

Schedule an intro call.

For the best and most efficient collaboration, schedule a quick 15-minute intro call with your team and the vendor so that your lawyer better understands what they are buying. This meeting alone typically shaves several turns off redlines.

Identify who signs.

Be sure to identify who needs to sign the MSA. There are often specific signatories out of the department, and you'll need to make sure they're available to review and submit.

Ensuring Quality Data Sources

It's essential for the vendor you select to have an open platform that supports direct integrations with your existing data sources, systems and devices. That way you can leverage secure connections with industry-leading data providers within one platform, removing the need for multiple tools and services while also ensuring you have always-on and real-time data streams.

As you evaluate threat intelligence vendors, ensure that they have access to many (or all) of the following sources needed to identify potential risks to the business. And, while they might have access to all of these, make sure the data is also actionable, continuous and not noisy. Listening without being able to take action is meaningless.

OSINT	Social media	Real-time events	The deep and dark web
Adverse media	Interactive maps and weather alerts	RSS feeds	Public records*

It's also important to look for platforms that support integration with your own systems and devices, including:

License plate reader (LPR) cameras	Visitor management systems (VMS)	Access control systems	Customer relationship management (CRM)
Collaboration tools	Authentication services	HR systems	IoT devices

Most of the time, these platforms have a flexible, open API that supports secure integrations with any data provider or tool, whether it be hardware or software. This helps ensure the security organization is connected across the organization.

*Arrests, incarcerations, release, civil records, federal court records, sex offender registries, terrorist watch list, etc.

Vetting the People Behind the Platform

In almost all cases, once you purchase a platform you'll be connected with a representative from the Client Success team to support you. But oftentimes this person isn't fully dedicated to your business and has limited time and resources to actually support you. In the world of security, it's essential that you have a team who is always on just like the platform is and that understands the ins and outs of not only the platform but of your business and the industry at large to best support you.

With how much limited time security teams have to manage the increase in threats, it can be hard to get it all done in a timely manner – even with the help of technology. So, be sure you're also asking vendors if they have a services arm of their business. In some cases, vendors will employ a team of experts who can serve as an extension of your team. Think of them as dedicated analysts that provide ongoing or on-demand services to support your unique needs. Anything from investigations to threat assessment and management training to establishing best practices and efficiencies within the platform.

Below is a checklist of items to consider when vetting the team behind the technology:

- ☐ Has past experience in corporate security or adjacent industries like the military or private sector (this should be for both your assigned Client Success contact, as well as those who built the platform and founded the company)
- ☐ Responds in a timely manner and on a 24/7 basis for any urgent needs
- ☐ Is educated on the platform and understands the ins and outs
- ☐ Has experience implementing and supporting sophisticated software solutions beyond the initial onboarding timeframe
- ☐ Provides dedicated resources focused on helping you achieve your outcomes as your program priorities shift
- ☐ Is willing to continually train and educate new members of the team/users of the platform to ensure the most robust understanding of the platform capabilities

Red Flags When Measuring a Protective Intelligence Solution’s Value

Demonstrating the value of new technology that is deemed costly can be a great challenge. But before you can make the case for change, do some due diligence to vet solutions for potential gaps or limitations in the offering.

ASK ABOUT THE FOLLOWING

❗ Over saturation of data that can frequently produce false positives or is not relevant

Ask your vendor how they help surface signals that will matter to you and your team rather than surface any and all signals with limited context.

❗ The ability to detect and follow a threat from identification to action and assessment

It’s essential that the platform allows you to follow a threat through the entire lifecycle. Many platforms specialize in only one area i.e. investigations or identification and lack actionability.

❗ Support for team collaboration across the organization

Security is the responsibility of everyone. It’s important to involve other departments like cyber, HR, legal, risk and compliance, business continuity and resilience, and even marketing/communications in some instances. A platform should make collaboration simple and easy.

❗ Heavy reliance on machine learning and artificial intelligence

Human verification is critical in security intelligence. Ensure that a vendor who uses technology to collect and connect threat data has a complementary human vetting process and doesn’t rely solely on AI.

❗ Data is not being provided in real-time

To make timely, relevant risk decisions it’s key for your team to have access to real-time information.

10 Questions To Ask Yourself Before Selecting a Vendor

Now that you have all you need to ensure you're selecting the right protective intelligence solution, here is a list of the most critical questions to ask any prospective vendor before making your final selection:

01 How can your intelligence and product support the different teams in my organization, both the departments (HR, legal, compliance, IT, business resilience/continuity, etc.) as well as the security group?

02 Do you have a services portion of your business that can support my team with things like investigations, threat assessment and management and best practices for the platform?

03 Is your platform secure and resilient?

04 Does your platform have reporting functionality?

05 How does your product support/apply to the entire intelligence cycle and how does that inform the way your product is developed?

06 What data and tools do you integrate with out of the box and can I bring my own systems?

07 Does your platform provide a simple, intuitive user experience?

08 Is your platform scalable?

09 How long does it take to generate the information and how quickly can it be shared?

10 What's your definition of protective intelligence, how does your company think about it?

86%

of clients reported that Ontic has helped their team focus on higher level problems and priorities

92%

of clients and their leadership reported that they are more confident in the safety of their organization upon implementation of the Ontic Platform

Receive a demo from the industry's most trusted protective intelligence provider and watch leaders just like you discuss how they are utilizing protective intelligence in their corporate security programs.

Request a demo

For more information please visit ontic.co

ONTIC