

Corporate Security Software Buyer's Guide

How to evaluate the right platform for your security program



Table of Contents

PAGE

04

Core capabilities to evaluate

[Read Now →](#)

PAGE

07

Consider your real use cases

[Read Now →](#)

PAGE

11

Assess integrations and technical fit

[Read Now →](#)

PAGE

12

Evaluate the vendor, not just the software

[Read Now →](#)

PAGE

14

Build the internal case

[Read Now →](#)

PAGE

17

Make the decision based on how you want to operate

[Read Now →](#)

PAGE

18

See how Ontic fits your requirements

[Read Now →](#)

The tools and technology your security team relies on shape how quickly you can understand risk and coordinate a response, helping you keep your people safe and your business resilient.

For many security teams, that technology has accumulated over time: specialized tools for specific needs, spreadsheets for others, and manual processes that connect the pieces. That approach may work, but it can also leave data and workflows disconnected and put more responsibility on your team to build the full picture. The question when evaluating a new platform is whether it can improve on what you already have enough to make a change worthwhile.

This guide will help you evaluate where a platform can make a meaningful difference, what to look for as you compare your options, and which questions to ask along the way. It will also help you define the outcomes you expect from the investment and build a stronger case for change internally.

Use it to:

- Compare platforms against the same criteria
 - Prepare for demos and RFP conversations
 - Align security, IT, procurement, and other stakeholders
 - Look beyond features to implementation and long-term fit
-

Core capabilities to evaluate

Physical security platforms can look similar on a feature list, but differ significantly in how they connect data, support workflows, and carry context across different security functions. Evaluating those capabilities together can help you understand how well a platform will actually support your team day to day.

As you compare platforms, look for one that can help your team:

Unify intelligence across people, places, assets, and threats

You rely on data from within and outside of your business. A strong platform should connect with the systems and sources you already use and bring that data together, helping your team see relationships and context that can be missed when information lives in separate systems.

ASK VENDORS:

Can you show us how data from different sources, including external sources like OSINT and internal systems like HRIS, connects around a person, location, asset, or developing threat? What other systems can we integrate as our needs evolve?

Turn fragmented data into actionable insight

More data does not necessarily mean better decisions. Your platform should help your team make sense of what it is seeing, identify meaningful patterns, and focus attention where it matters.

ASK VENDORS:

How does the platform help us distinguish meaningful risk from noise and determine what requires attention? And how are you using AI to help with this?

Core capabilities to evaluate

CONTINUED

Connect intelligence with operations

Intelligence is most useful when it informs what happens next. Connecting it directly to cases, tasks, procedures, and decisions reduces manual handoffs and keeps important context with the work.

ASK VENDORS:

When intelligence requires action, how does it move into the workflows and procedures our team uses to respond? Can this be automated or is it manual?

Use AI built on the right foundation

Not all AI is created equal. The quality of what an AI model can surface, summarize, or recommend depends heavily on the data and context it can access. Look for AI built on a strong foundation of connected security data, with access to the people, places, events, threats, operational history, and procedures that give meaning to individual signals.

Just as importantly, consider how AI is incorporated into the work itself. It should help your team make sense of information, recognize patterns, and move work forward within existing security workflows while keeping people in control of consequential decisions.

ASK VENDORS:

What data and organizational context does your AI have access to? How does it use that context within our security workflows, and what controls keep people involved in the decisions and actions that matter?

Adapt to how your team operates

Every security program has different processes, escalation paths, reporting requirements, and stakeholders. Your platform should be configurable enough to reflect those differences without requiring extensive development.

ASK VENDORS:

What can our administrators configure themselves, and what changes require vendor support or custom development?

Core capabilities to evaluate

CONTINUED

Support collaboration across teams

Security work frequently involves partners outside the security function. The right platform should make it easier to share the necessary context while maintaining appropriate controls over sensitive information.

ASK VENDORS:

How can security collaborate with teams like HR, legal, or facilities while controlling what information each stakeholder can access?

Help your team identify risk earlier

The value of connected data grows when it helps your team recognize that something is changing before a situation escalates. Look for a platform that can surface relevant signals, relationships, and trends across your environment.

ASK VENDORS:

How does the platform alert us to emerging concerns or meaningful changes that we might otherwise miss?

Maintain a defensible record

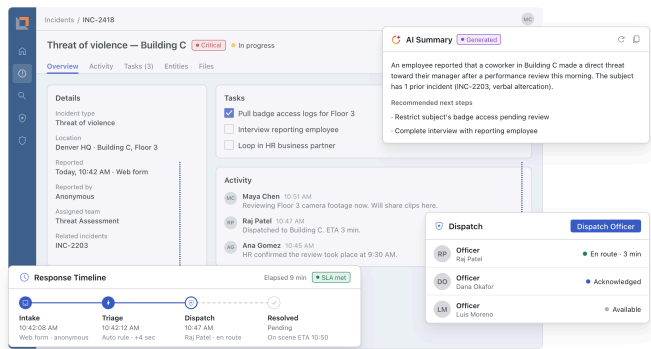
When an incident or investigation is reviewed later, your team needs to reconstruct what happened, what information was available, what decisions were made, and what actions followed.

ASK VENDORS:

Can you show us how the platform preserves evidence, decisions, ownership, actions, and timelines throughout a case or incident?

Consider your real use cases

A platform may have the capabilities you need on paper, but the real test is how they come together during the work your team performs every day. Ask vendors to demonstrate your actual use cases from beginning to end so you can see how information moves, where context is preserved, what requires manual work, and how the platform supports decisions and response along the way.



Incident Management

WHAT TO LOOK FOR

Flexible intake from forms, alerts, email, and integrated systems

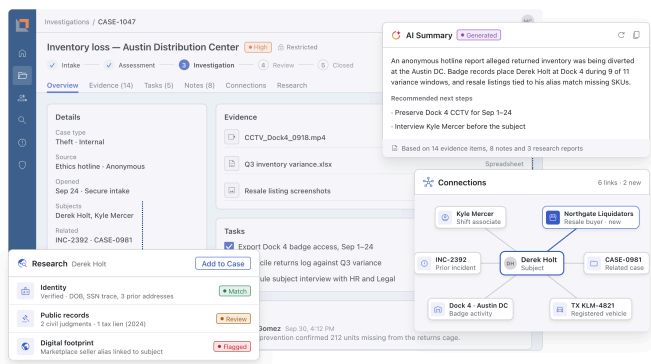
Automated triage, routing, and escalation

Integrated dispatch and response coordination

In-workflow communication, tasks, and followup

AI-generated incident summaries with relevant history and emerging connections

Auditable timelines linking incidents to people, places, intelligence, and investigations



Corporate Investigations

WHAT TO LOOK FOR

Secure, configurable intake and case workflows

Integrated identity, public-records, and digital research

Connections across related people, places, incidents, and cases

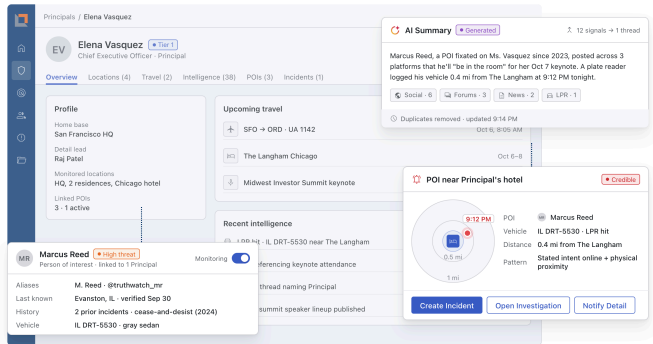
Centralized evidence, tasks, notes, and collaboration

AI-generated case summaries that highlight key developments and reduce manual review

Complete audit trails and leadership-ready reporting

Consider your real use cases

CONTINUED



Executive Protection

WHAT TO LOOK FOR

Principal profiles connected to locations, travel, intelligence, and incidents

Living POI profiles with identity data, history, and monitoring

Continuous digital and physical threat monitoring

Actionable alerts tied to POIs, locations, and threat patterns

AI that deduplicates and summarizes signals around principals and POIs

A direct path from a credible signal to an incident, investigation, or response

GSOC Operations

WHAT TO LOOK FOR

A common operating picture across risk signals, sites, people, and prior activity

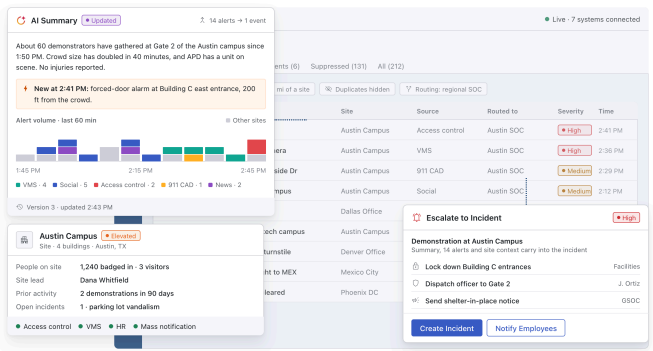
Configurable alert filtering, triage, and routing

AI-assisted event grouping and evolving event summaries

Incident intake, escalation, and task coordination

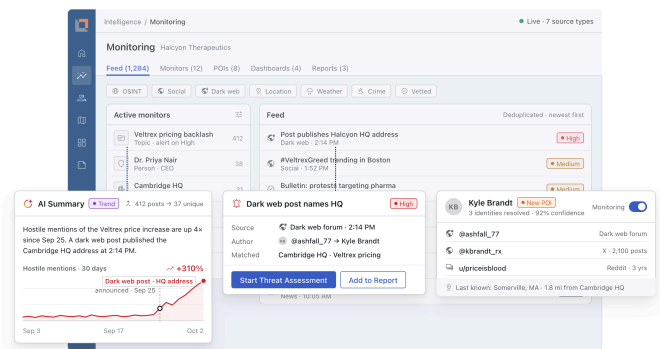
Integrations with relevant security and business systems

Context that carries from detection through response and reporting



Consider your real use cases

CONTINUED



Threat Intelligence

WHAT TO LOOK FOR

Broad OSINT, social, dark web, location, weather, crime, and vetted sources

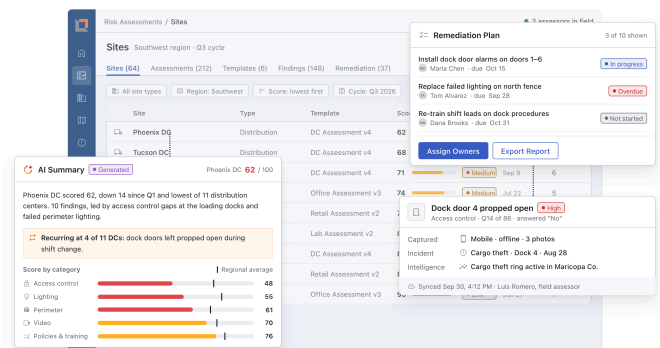
Targeted monitoring of relevant people, places, assets, and topics

POI management, identity resolution, mapping, and analysis

Configurable alerts, dashboards, and reports

AI-powered deduplication, summarization, and trend detection

Workflows that turn intelligence into assessment or action



Site Risk Assessments

WHAT TO LOOK FOR

Standardized, configurable assessments that scale across site types

Mobile and offline field data collection

Consistent scoring to compare and prioritize sites

AI-assisted assessment summaries and identification of recurring vulnerabilities

Clear remediation ownership, deadlines, and tracking

Connections to incidents, intelligence, and changing threats

Tip: Give every vendor the same scenario and ask them to show the workflow from beginning to end. That makes it much easier to see where a platform genuinely connects the work and where your team will still be responsible for filling the gaps.

Choose a platform that can scale with your program

You may be solving an immediate need, but the platform should also support a growing security program as you add teams, regions, locations, and use cases. Ask questions to evaluate scalability, like:

- Can we add teams, regions, and locations without rebuilding the environment?
- Can different teams work from the same platform while maintaining appropriate permissions?
- Can administrators make routine changes without relying heavily on the vendor or developers?
- Can we add new security use cases over time?
- Can the platform replace unnecessary point solutions while still integrating with specialized systems we want to keep?
- Will the data and operational history we build today become more useful over time?

Assess integrations and technical fit

The value of an integration goes beyond moving data from one system to another. Your platform should be able to connect information from the systems your organization already relies on and make that data useful alongside the people, places, threats, incidents, and workflows it relates to. Evaluate both what a platform can connect to and what your team can actually do with that information once it is connected.

Map your ecosystem

Identify the systems that may need to connect with the platform, including:

- Access control and badge systems
- HRIS and employee data
- Existing incident or case systems
- Threat intelligence and OSINT sources
- Communications tools
- SSO and identity management
- Travel, facilities, event, and executive protection data

A better integration question

INSTEAD OF ASKING:

“Do you integrate with our access control system?”

Then evaluate data, access, and security requirements:

Data flow: What information can come in? What can go out? How frequently?

APIs: Are APIs available and well documented?

Permissions: Can access reflect the sensitivity of different cases, teams, and data?

Governance: How are retention, auditability, and data handling managed?

Security review: Can the vendor provide the documentation your IT and security teams will require?

ASK:

“Show us what our team can actually do differently once that access control data is connected.”

Evaluate the vendor, not just the software

The platform is only one part of what you are buying. The expertise behind it, the direction of the product, and the support you receive from implementation onward can all determine how successfully the technology becomes part of your operation. Evaluate whether the vendor can support both where your program is today and where you want to take it.

Domain expertise

Look for a vendor that understands corporate security because its team has worked in it, not just built technology for it. Former practitioners can bring firsthand experience to the partnership, helping you think through how to build or mature your programs in addition to how to configure the technology.

ASK VENDORS:

Who on your team has direct corporate security experience? Will we have access to them in an advisor capacity? Do they help inform the product?

Product direction

The platform should continue to evolve alongside the way security teams operate. Understand where the vendor is investing and whether its roadmap supports greater connectivity across your program, including how it is approaching AI, automation, and emerging security needs.

ASK VENDORS:

Where are you investing in the platform over the next few years, and how will those investments help us get more value from the data and workflows we build today?

Implementation and time to value

A strong platform still has to go through the process of becoming part of your team's day-to-day operation. Look for a structured implementation process that starts with your priority use cases and workflows, clearly defines what your team needs to provide, and gives you a realistic path from configuration to meaningful use.

Look for:

- Clear implementation phases, responsibilities, and milestones
- Configuration based on your actual security workflows
- A focused initial scope tied to priority use cases
- Training and enablement for users and administrators
- A path to expand into additional teams or use cases over time

ASK VENDORS:

What will it take to get our priority use cases live and actively used, what will you need from our team, and how will you measure whether we're getting value?

Partnership and ongoing support

The relationship should not end once implementation is complete. Consider who will support your team afterward, how they will help you solve new operational challenges, and whether they can connect you with additional technology, services, and expertise as your needs evolve.

ASK VENDORS:

Who will work with us after launch, and how will you help us continue to improve and expand how we're using the platform?
What services and partner ecosystem can we access when we need capabilities or expertise beyond your platform?



The goal is to choose more than software. Look for a vendor with the technology, security expertise, and long-term partnership to help your team successfully operationalize it.

Build the internal case

Security investments can be difficult to make a business case for. The value of preventing an incident or identifying a threat earlier is real, but it is not always easy to quantify, and security is still often viewed primarily as a cost center. Building support for a new platform means making both the need for changing the status quo and the value of the investment clear to stakeholders beyond security.

Start with the current state

Document where your team is losing time, context, or visibility today. Be specific about the operational problems you are trying to solve and the risk they create.

Examples:

- Information spread across multiple systems
- Manual handoffs between teams
- Duplicate or overlapping tools
- Difficult or inconsistent reporting
- Processes dependent on individual knowledge
- Limited visibility across security functions

Establish a problem that stakeholders agree is worth solving. Consider what happens if nothing changes, too. Where could the current approach leave the organization exposed, slow your ability to respond, or make it harder to support broader business priorities?

Identify the outcomes you expect

Define what should improve if you solve those problems. Lead with the security and risk outcomes the investment should support, then quantify those outcomes where you reasonably can.

Potential outcomes include:

- **Earlier risk identification:** Greater ability to surface relevant signals, relationships, or changes before a concern escalates.
- **Reduced exposure:** Fewer gaps in visibility, missed handoffs, or delays that can allow a developing risk to go unaddressed.
- **Time saved:** Fewer hours spent gathering information, conducting repetitive research, preparing reports, or moving data between systems
- **Lower costs:** Fewer overlapping tools, reduced outside services, or less custom development and maintenance
- **Faster response:** Less time between identifying a potential issue and assessing, escalating, or responding to it
- **Greater capacity:** More incidents, investigations, assessments, or requests handled without increasing headcount
- **Stronger defensibility:** A clearer record of the information available, decisions made, and actions taken

Where possible, establish a baseline and target for what you want to improve. For example:

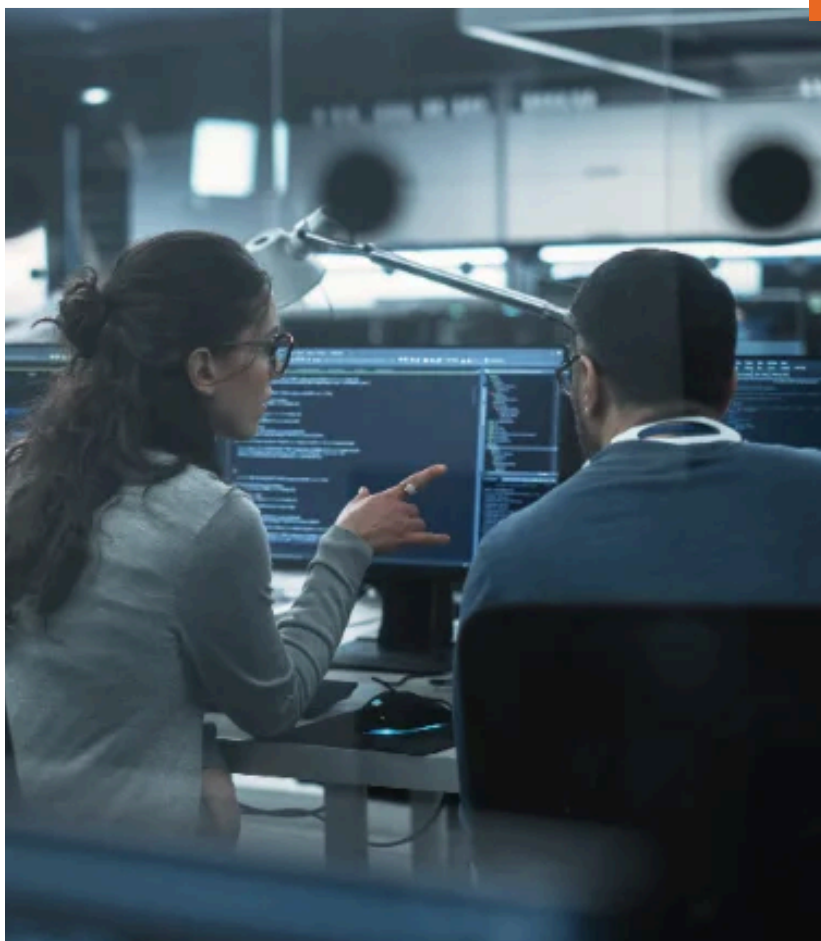
“Our current process for identifying and assessing potential threats relies on too many manual steps, delaying our ability to understand and act on risk. We need to reduce assessment time by 30% so our team can identify credible threats and intervene sooner.”



Ready to take the next step internally? Our [Guide to Gaining Approval and Budget](#) shares advice from other corporate security leaders on navigating stakeholders, securing executive buy-in, and building the business case.

Tailor the case to your stakeholders

Connect the case for change to the priorities of the people involved in the decision. Finance may care about cost and capacity, IT about integration and complexity, legal about consistency and defensibility, and executive leadership about risk to the business. Bringing those perspectives into the evaluation early also helps demonstrate that the eventual recommendation reflects broader organizational requirements, not only the needs of the security team.



Build a Defensible Case for Change

1. ESTABLISH THE NEED

- ☐ We can clearly articulate the problem we need to solve
- ☐ We understand the risk of continuing with our current approach
- ☐ The problem connects to broader business priorities

2. BUILD A FAIR EVALUATION

- ☐ Requirements reflect the needs of key stakeholders
- ☐ Vendors are evaluated against consistent criteria
- ☐ Real workflows and use cases are part of the evaluation
- ☐ Findings and tradeoffs are documented

3. JUSTIFY THE DECISION

- ☐ The selected platform meets our priority requirements
- ☐ Expected security and business outcomes are clear
- ☐ Implementation and ongoing support have been vetted
- ☐ We can explain why this approach is stronger than the alternatives, including maintaining the current state

Make the decision based on how you want to operate

The best platform for you is the one that fits the way your team needs to operate: connecting relevant data, preserving context, supporting your procedures, and helping people move from information to action without rebuilding the picture every time something happens.

YOUR EVALUATION SHOULD LEAVE YOU CONFIDENT ABOUT THREE THINGS

- 01 Will it meaningfully improve how we operate today?
- 02 Can our team realistically implement and adopt it?
- 03 Will it become more valuable as our security program grows?

- If the answer to all three is yes, you've found a platform that can serve as the foundation for how your security program operates and evolves as you mature.



See how Ontic fits your requirements

See how Ontic connects intelligence, incidents, investigations, assessments, and security operations in one platform, and evaluate it against the requirements that matter most to your team.

[Schedule a demo](#)