Recorded Future®

2024 State of Threat Intelligence

RESEARCH CONTENT 2024

550+ cybersecurity executives, managers, and practitioners share how they're using threat intelligence, what they want from vendors, and how they plan to strengthen their efforts.

Research conducted and verified by

UserEvidence

Table of Contents

Every year, enterprise organizations invest tens to hundreds of thousands of dollars in threat intelligence to identify and mitigate major risks to the business. Their data, reputation, and revenue are worth millions or even billions of dollars, making the right solution worth every penny.

Demand for threat intelligence is growing:

9/10

cybersecurity leaders say their organization plans to invest more in 2025.

But spending more doesn't always mean spending more strategically—so security teams are considering how best to spend their increased threat intelligence budget. They need to keep pace with evolving threats, address threats before they have an impact, and communicate threat intelligence wins more broadly to justify continued investments.

How are companies using, sourcing, and improving threat intelligence? In 2024, we surveyed over 550 cybersecurity executives, managers, and practitioners to understand how they're using threat intelligence, what they want from vendors, and how they plan to strengthen their efforts.

> We've got to shift the whole focus to stopping the event before it happens and that is the shift that most security teams really have to undergo.

Jason Steer
CISO, Recorded Future

Survey demographics

Recorded Future partnered with third-party researcher UserEvidence to survey 554 cybersecurity executives, managers, and practitioners:

- All respondents come from organizations with over 1,000 employees.
- Over half (53%) are cybersecurity managers or directors.
- 80% of respondent organizations have a dedicated threat intelligence team.
- Respondents are all either very familiar (73%) or moderately familiar (27%) with their company's threat intelligence tools and policies.

Key Insights

01 Organizations are embracing proactive threat intelligence

The top two reasons that enterprise organizations use threat intelligence are to assess risk from a range of threats (76%) and to prioritize vulnerabilities and weaknesses most likely to be targeted (72%).

Cybersecurity teams are turning their attention to how they can move into the offensive position. Instead of reacting to threats once they've become attacks, they use threat intelligence to increase visibility and mitigate risks so they can stay several steps ahead of threat actors.

02 Teams measure success based on detection, response, and remediation outcomes

Respondents say they base the success of threat intelligence on these top three measures:

- 66% cite enhanced threat detection rates
- 59% cite improved response times
- 57% cite a reduction in the number of incidents

Threat intelligence also delivers related benefits like improved threat detection accuracy and improved prioritization of security efforts.

03 Internal research and threat intelligence vendors come out on top

Cybersecurity teams look to a range of sources for threat intelligence, but internal threat research is the most common, with 83% continuously or frequently obtaining intel. Threat intelligence vendors come in second, with 75% relying heavily on these solutions.

Other key threat intelligence sources include industry consortiums, open-source data feeds, and security tool vendors.

04 Support, efficiency, and actionable insights are top vendor traits

When working with threat intelligence vendors, respondents say that specialized support and customized insights are most important. 58% rank access to experts with specialized skills and the ability to request analysis and reports addressing their specific problems as extremely important.

Other top factors are integration with existing security tools and workflows, automated data collection and insights, and actionable information about threat actors, tactics, and techniques.

05 Threat intelligence programs continue to mature

Most cybersecurity teams are confident about the maturity of their threat intelligence program. 85% report that their efforts are intermediate or advanced, and 80% say that their organization has a dedicated threat intelligence team.

While the cyber threat intelligence team understandably uses threat intelligence most often, multiple other teams also rely on its insights.

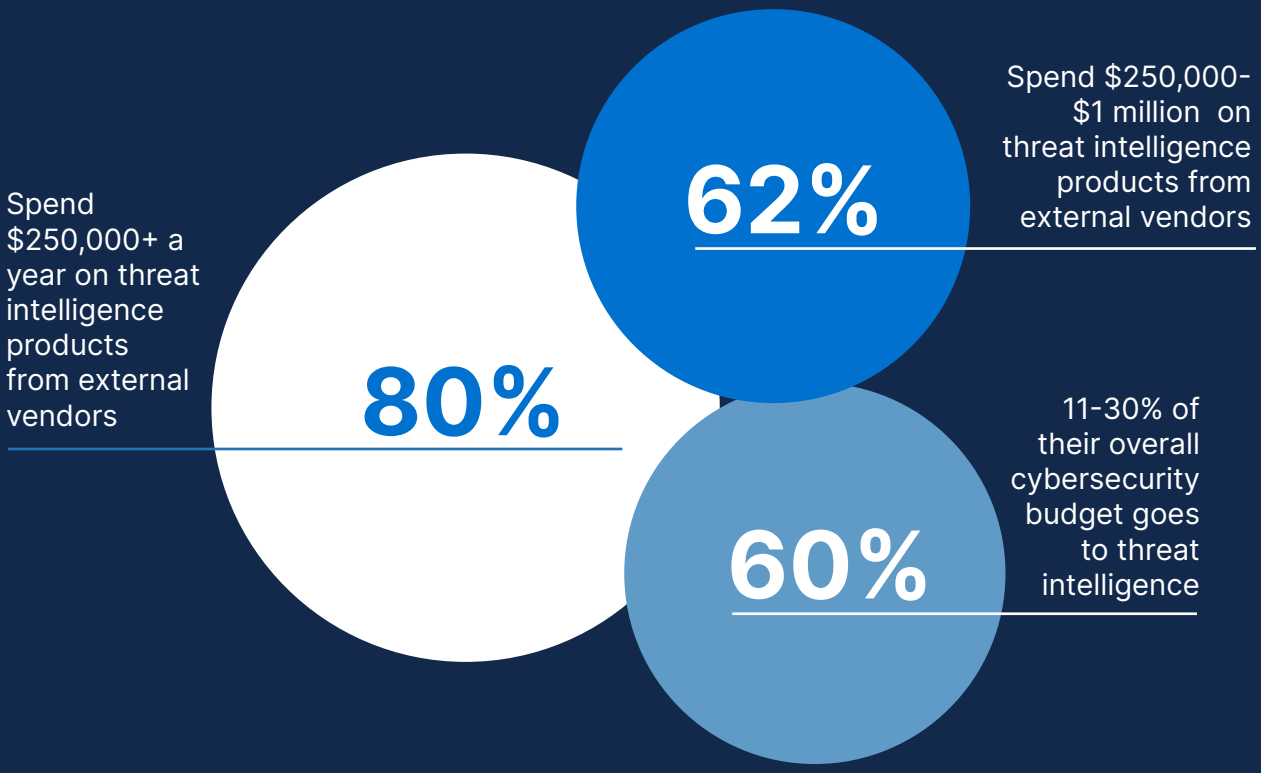
06 Security teams are spending more strategically on threat intelligence

Enterprises want to make their threat intelligence budgets go further. While nine out of 10 respondents say that their organization plans to spend more on threat intelligence in 2025, eight out of 10 plan to consolidate duplicative threat intelligence vendors during the same time.

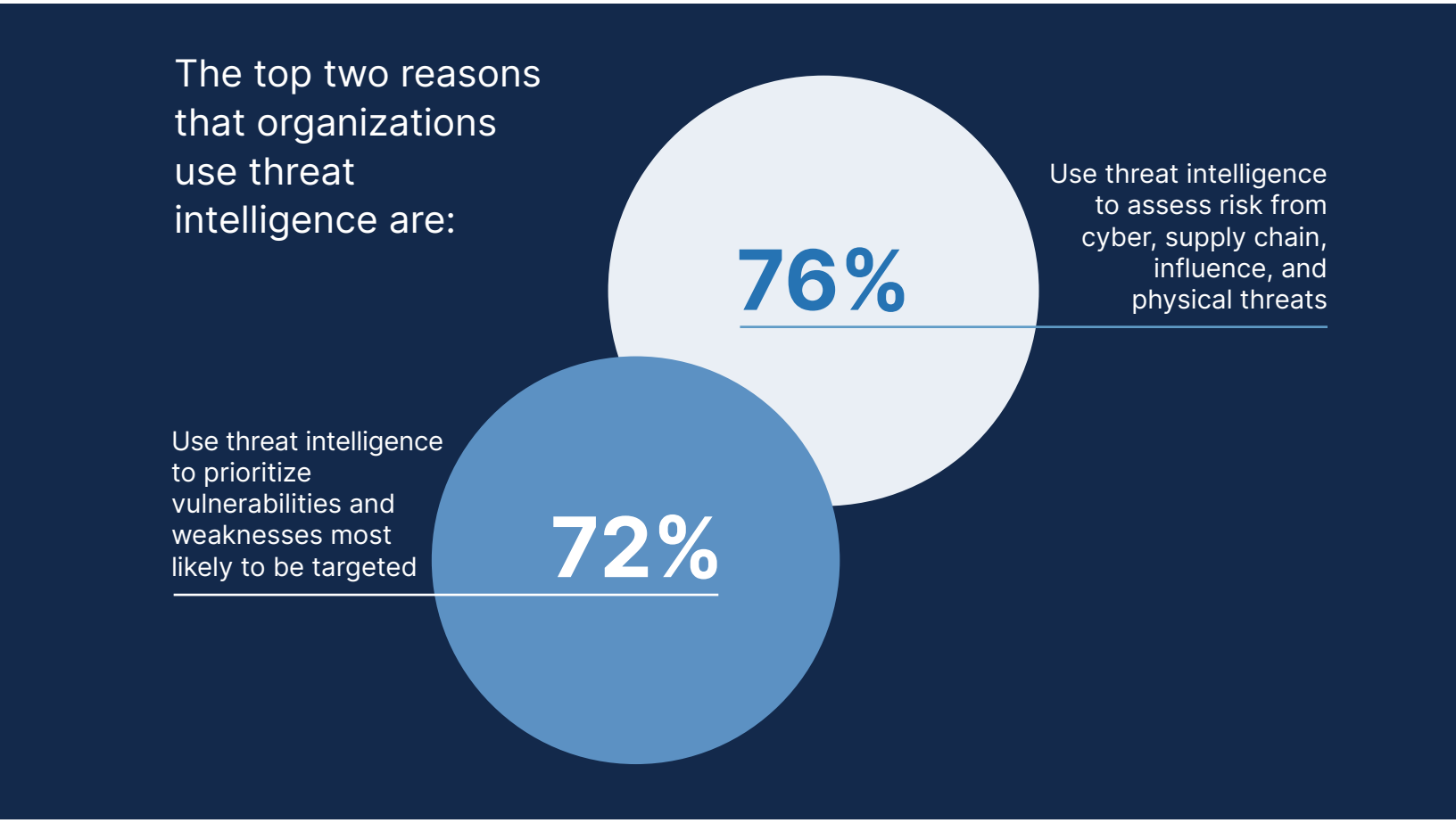
Threat intelligence has taken its place as a strategic pillar. 88% of cybersecurity leaders say their organization always or frequently uses threat intelligence for strategic planning, and 96% say that threat intelligence is important for justifying business investments to leadership.

How cybersecurity teams use threat intelligence

As we've noted, threat intelligence budgets are set to grow in the near future: 90% of respondents say that their organization plans to invest more in 2025. But where do budgets stand now? Eight out of 10 security managers and practitioners say they spend more than $250,000 per year on threat intelligence products from external vendors, with 62% spending between $250,000 and $1 million. This amounts to a noticeable portion of their security spend — 60% of respondents say that 11-30% of their overall cybersecurity budget goes to threat intelligence.

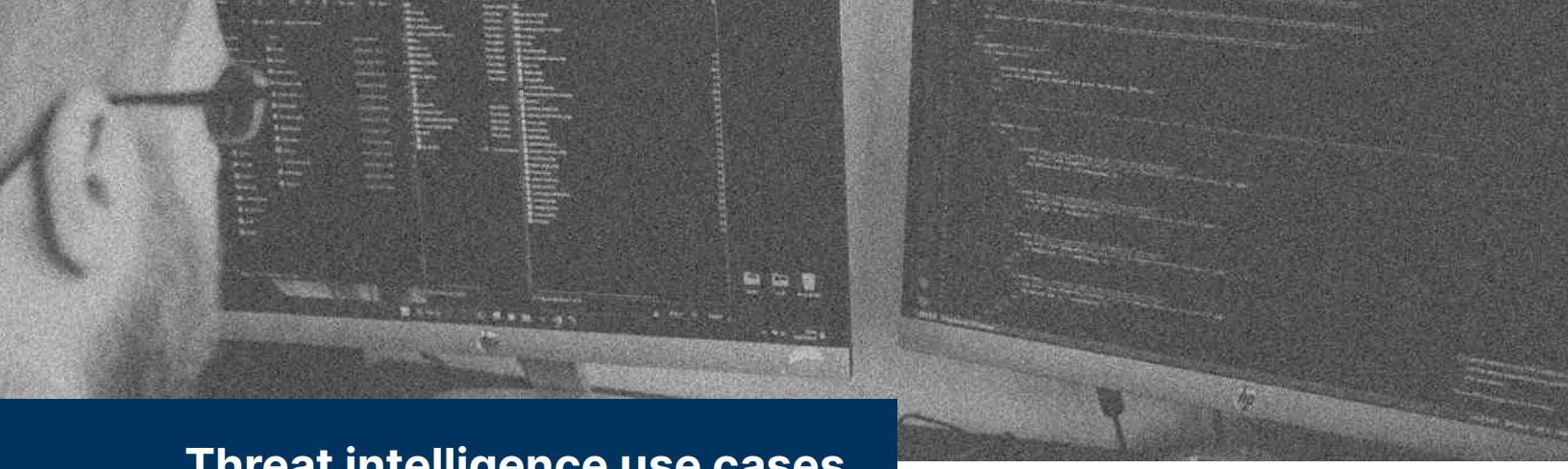


Threat intelligence is no longer just a defensive tool — instead, it's a powerful business enabler with far-reaching benefits and use cases across the organization. Companies use threat intelligence to strengthen their all-around security posture as they work to understand the threat landscape and protect their environment.



Both of these "whys" show security teams moving into an offensive position. Instead of reacting to current attacks, they proactively assess risk from across threat vectors and work to understand the gaps that most need protection.

At least half are also using threat intelligence as a way to strategically influence their organization — guiding investments, reducing the security skills gap, and communicating risk to business leaders. With such business-critical goals in mind, let's explore how they use threat intelligence.



Threat intelligence use cases

Cybersecurity managers and practitioners typically use threat intelligence across nine core use cases which correspond to three primary categories.

1. Proactive threat detection and response

In the top three use cases, over half of respondents rely on threat intelligence to support a proactive approach to identifying and addressing threats to the business. They use threat intelligence to:

- Enhance their existing security tools and accelerate alert triage
- Prioritize vulnerabilities and exposures in order to reduce their attack surface
- Increase visibility into threats to the business

Security teams often struggle to identify which threats are most critical to their business because they have to gather information from many different internal and external sources. Centralized threat intelligence solutions, such as Recorded Future's Collective Insights, help by consolidating this information. They highlight the most important findings and provide essential context, making it easier for teams to prioritize and address the most urgent areas of concern.

2. Improved understanding of the threat landscape and risks to the business

Many of the other top use cases rely on a greater understanding of different types of risk. Threat intelligence lets them:

- Identify risks to the supply chain and third parties (52%)
- Analyze and model cyber risks (52%)
- Identify risks to specific physical locations and facilities (48%)
- Report on threat actors and understand their tactics, techniques, and procedures (46%)

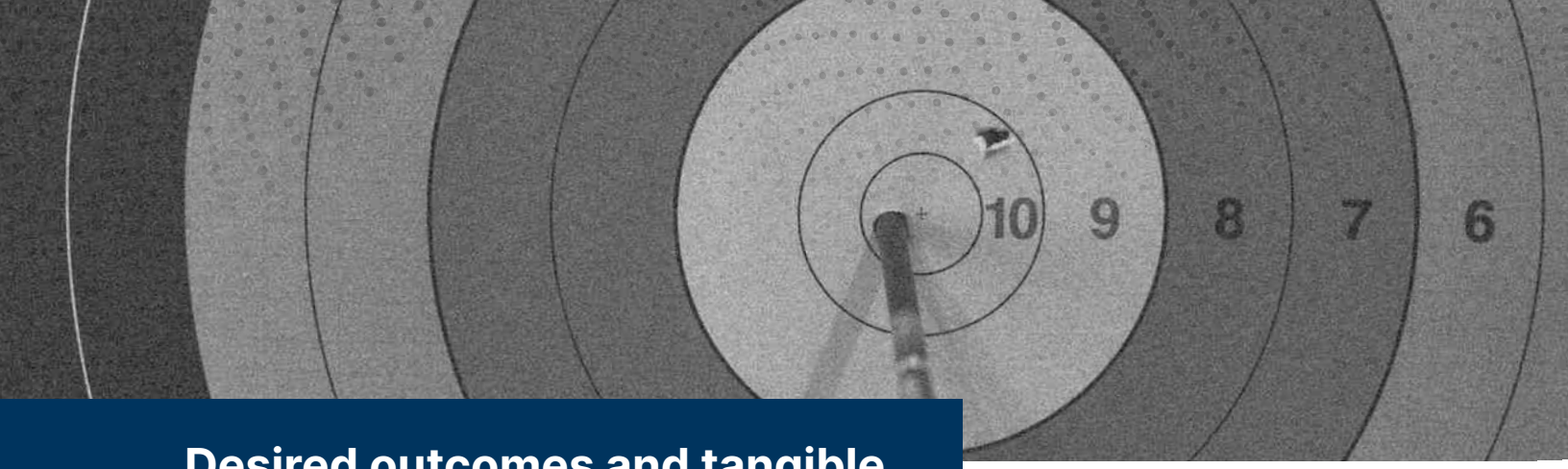
By assessing a wide range of risk factors, high-performing cybersecurity teams help their organization achieve stronger footing when it comes to the threats they might face from anywhere. Risk identification also reveals weaknesses that security needs to shore up to protect the business.

3. Online risk mitigation for continued digital transformation

Finally, nearly half of respondents use threat intelligence to mitigate online risk:

- 49% use it to protect their brand and reputation on the web and in social media
- 47% use it to reduce online fraud.

Protecting for misuse of their brand and online fraud helps teams continue pushing innovation online.



Desired outcomes and tangible benefits from threat intelligence

An organization's measures of success for a program or initiative say a lot about their desired outcomes. So what outcomes are security teams looking for from threat intelligence? These are the top three ways respondents measure the effectiveness of their threat intelligence program:

- **66% say enhanced threat detection rates.** Threat intelligence helps security teams identify more threats from any attack vector or actor.
- **59% say improved response times.** The sooner organizations act to address threats, the better they are at limiting fallout and impact from a potential attack.
- **57% say reduction in the number of incidents.** In an ideal world, organizations would proactively identify and respond to all threats before they become attacks. Threat intelligence helps them get closer to achieving that goal.

In turn, these measures of success translate directly to the benefits security teams glean from threat intelligence. For instance, the top two reported operational benefits are **improved threat analysis and faster incident response**, and the top tactical benefit is **improved threat detection accuracy**.

Threat intelligence also benefits organizations by helping them set the right priorities:

- **39% of respondents say that improved vulnerability prioritization is a top tactical benefit.**
- **58% cite better prioritization of security efforts as a top operational benefit.**

- **46% report an improved ability to prioritize and justify investments in cybersecurity technologies and personnel, the top strategic benefit.**

Across all security managers and practitioners, threat intelligence offers critical input to more efficiently and effectively address threats. It also provides a path to more strategic threat detection and response by equipping teams to prioritize high risks and filter out the noise. In this way, threat intelligence contributes to a more resilient business.

Here's an example: Imagine that several hundred employee credentials from within your organization were found in infostealer logs. Now, it's the security team's responsibility to follow up on each of those identities manually and reset compromised credentials. Manual password resets take time — during which threat actors could perform an account takeover or sell the credentials to the highest bidder.

Recorded Future automated this process. Security teams can now automatically populate the details of the stolen information into a workflow with Okta. Through partnerships with trusted third-party vendors, the identity protection process happens in the background without manual work from the team.

The product also executes fully automated account resets for any accounts that need to be triaged.

With the help of threat intelligence, automation protects security practitioners' time and resources for greater efficiency and capacity while, above all, protecting the interests of the organization.

Where cybersecurity teams get threat intelligence

Threat intelligence is a central element of a strong cybersecurity program: 96% of respondents say that comprehensive threat intelligence is important to their cybersecurity program, including over half that call it essential. Threat intelligence is only as good as the sources pulling information for security teams, though. Which ones do they rely on most often?

Across security managers and practitioners, **the most common source is internal threat research**. Nearly half (45%) of teams rely on internal research continuously, while 38% rely on it frequently. For most organizations surveyed, someone on the cybersecurity team conducts ongoing manual investigation around their risk surface and the broader landscape, as well as looking to internal telemetry data to assess and triage risks.

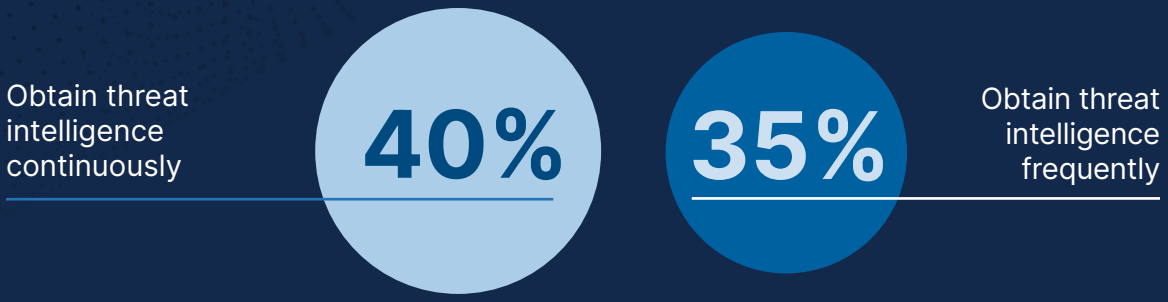
Rely on internal research continuously

45%

38%

Rely on internal research frequently

The second source organizations look to most often is threat intelligence vendors — 40% obtain threat intelligence continuously, and 35% frequently. These vendors provide a comprehensive understanding of the threat landscape with data from many sources, analysis, and automated alerts or reporting.



When organizations implement threat intelligence without using a vendor, they typically turn to one or more of three alternatives:

1. **Open-source feeds or industry consortiums.** These sources for threat intelligence may be free or charge a small fee.
2. **Point solutions.** Security teams might rely on a provider that supports one or a handful of use cases around threat intelligence but doesn't offer a comprehensive solution.
3. **The platform approach.** Some of the bigger cybersecurity players (e.g., CrowdStrike and Microsoft) have offerings that cover some threat intelligence use cases alongside their more recognized products.

The data reveals that security managers and practitioners do look to these kinds of sources within their workflows:

- 70% look to industry consortiums and standards bodies continuously or frequently.
- 60% rely on free or low-cost threat data feeds continuously or frequently.
- 77% get threat intelligence from security tool vendors, but it's an intermittent process for most, rather than a continuous one.

The problem with these solutions is that none of them offers the full scope of information needed, which places manual effort on the team and adds noise to the process of collecting threat intelligence.

The answer? A single solution — such as a threat intelligence provider — that allows security teams to rely on a central platform instead of many different products.

What buyers look for in a threat intelligence solution

Security teams searching for a threat intelligence vendor now have plenty of options to choose from — so they can afford to be selective about the features that are most important to them. Why do security managers and practitioners work with threat intelligence vendors? Here are three of the top themes.

1. Specialized support and customized insights

Security teams want a comprehensive platform to help them identify and address threats — but that's not all they're looking for. They want **the support and expertise of professionals** who can help them with their organization's individual needs. For instance, 58% of respondents ranked access to experts with specialized skills as extremely important when working with threat intelligence vendors. Teams want access to smart and experienced people who can help make their company more secure, whether they're evaluating a third-party solution or facing a complex risk to the business.

The same percentage of security leaders ranked **the ability to request analysis and reports addressing their specific problems** as extremely important. They want customized guidance through the security challenges they face.

2. Efficiency in threat detection and response

A single threat intelligence solution enables security teams to get off the hamster wheel of manual threat investigation. It pulls information and insights from many sources — including an organization's existing security tools — into a central platform. This enables automation and streamlined operations: maximum information with minimal burden on the cybersecurity team.

Efficiency comprises another top priority for cybersecurity teams: 54% cite that it's extremely important for vendors to **integrate with existing security tools and workflows to reduce analyst workload and investigation time**. Similarly, 53% say that vendors' **ability to automate data collection and surface relevant insights in real time was critical, not only saving the security team time** but allowing them to identify and address threats sooner.

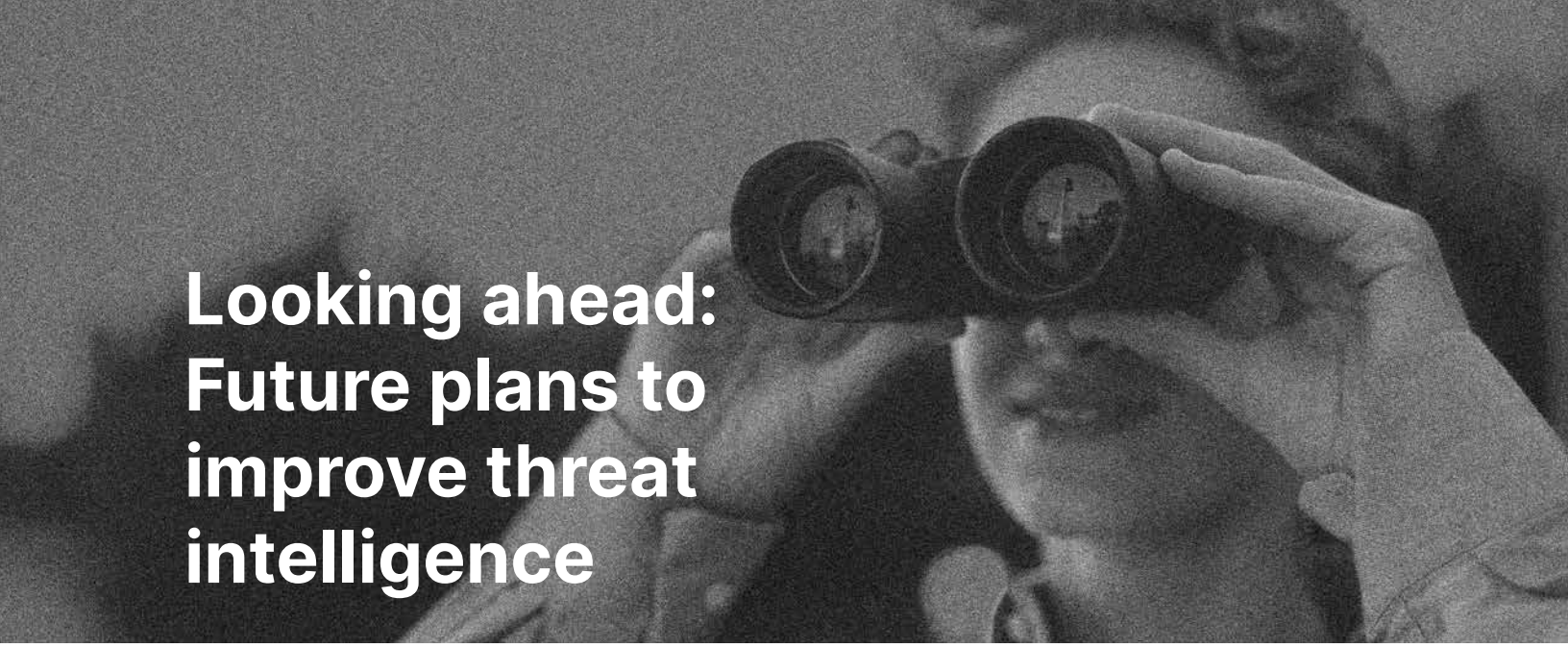
3. Visibility and actionable insights

In cybersecurity, missing a single threat can be devastatingly costly. While teams contend with countless potential points of vulnerability, threat actors only need to succeed once to cause major fallout.

That's why one of the benefits of a threat intelligence solution is the increased visibility and insights it can offer. Security practitioners rank these reasons for working with a vendor as extremely important:

- Vendors provide actionable information about threat actors, indicators of compromise, attacker tactics, techniques, and procedures (TTPs), and other topics (56%)
- Teams can find information focusing on threats targeting our industry, applications, and systems (55%)
- Vendors are better able to monitor discussions and activities on the dark web (49%)

With increased visibility and advanced insights, cybersecurity teams can understand more about their threat landscape and take the necessary steps sooner.

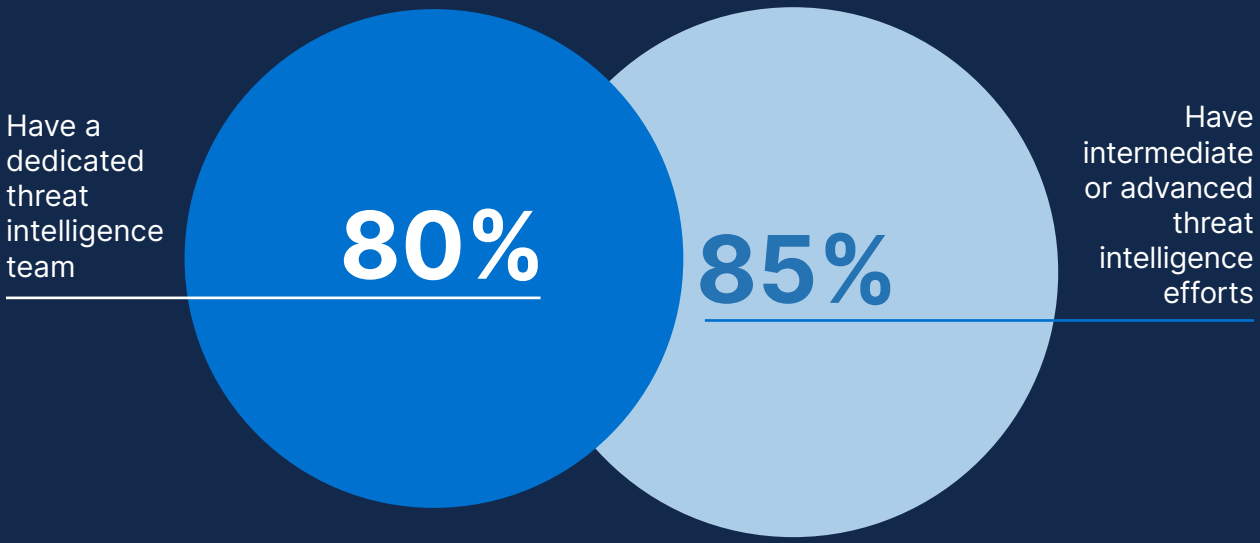


Looking ahead: Future plans to improve threat intelligence

As the threat landscape continues to grow more complex, businesses recognize the need to be even more strategic with their threat intelligence efforts going forward. Here is what we uncovered about their plans.

Multiple teams benefit as threat intelligence matures

Of those surveyed, 80% say that their organization has a dedicated threat intelligence team — which aligns well with the 85% of respondents who said that their threat intelligence efforts are intermediate or advanced.



Security teams are dedicating talent resources to this function, further supporting that it's a growing priority. It's not just those employees that use threat intelligence, though. Of the teams that primarily use threat intelligence, cyber threat intelligence (CTI) naturally came out on top, with cybersecurity engineering and architecture in close second. But numerous other teams also rely on threat intelligence including risk management, Security Operations, Risk and Compliance, Vulnerability Management, and Fraud Prevention. Threat intelligence furthers the needs of the whole security team — and the entire organization.

In fact, the primary way organizations plan to improve their use of threat intelligence over the next two years is through integrating threat intelligence with additional cybersecurity workflows and teams; two-thirds of respondents plan to do so. Threat intelligence has a growing presence not just in enterprise organizations' budgets but in their tech stacks, team priorities, and even business strategies.

More strategic spending and wider applications for threat intelligence

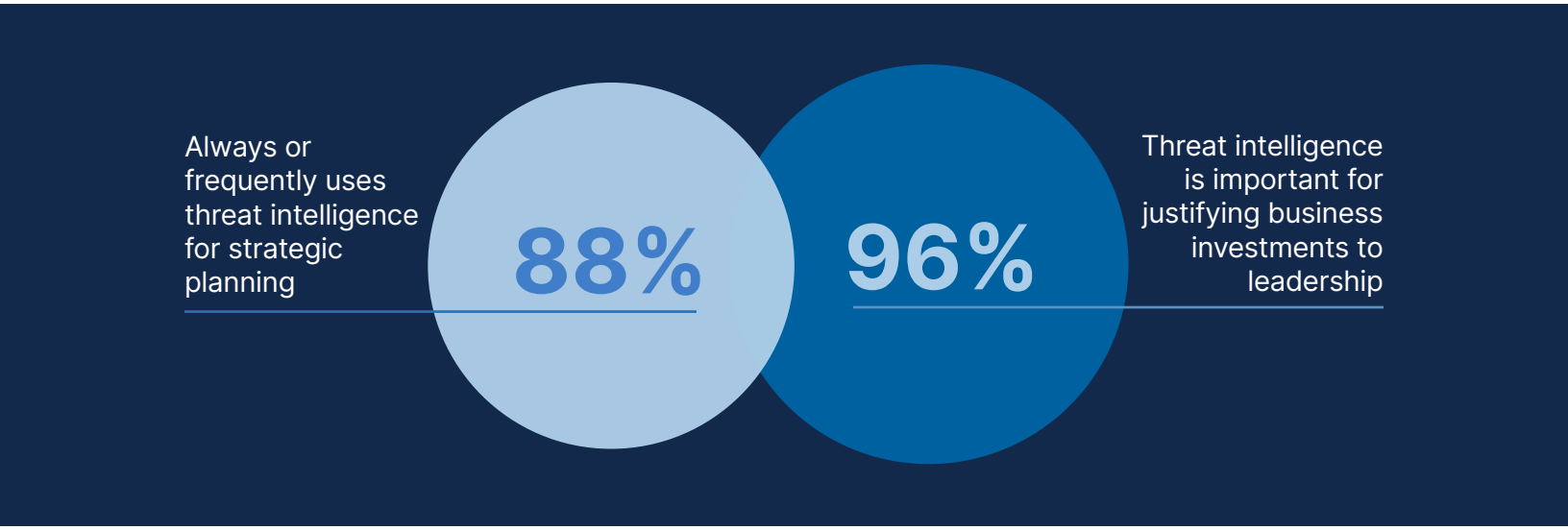
Enterprise organizations aim to be more strategic with where they spend their threat intelligence budget and how they apply its insights.

At the same time as the vast majority of organizations plan to spend more on threat intelligence in the year ahead, eight out of 10 respondents say their organization plans to consolidate duplicative threat intelligence vendors in 2025. While they're spending more on threat intelligence, security teams want to get more value from that money, which likely means shifting to a premium offering.

A comprehensive threat intelligence solution drives operational efficiency for cybersecurity and cost efficiency for the business, but its insights also equip leaders to use threat intelligence to influence wider business initiatives and strategies.

Already, 88% of survey respondents say their organization always or frequently uses threat intelligence for strategic planning. Cybersecurity teams advise company leadership on the potential threats of new initiatives and risk mitigation, and they look to threat intelligence to do so.

What's more, a full 96% of security executives, managers, and practitioners say that threat intelligence is important or very important for justifying business investments to leadership. The role of threat intelligence has advanced from a primarily preventive position to a more holistic influence on business decisions — and this is no small feat.



Historically, many organizations have viewed security with primarily begrudging acceptance. They know it's essential to protect their most valuable assets. But because the security team sometimes has to deny expenses or processes because of risk or control access to protect data, other departments view security as a blocker. In many cases, an inflexible security policy that keeps employees from doing their job doesn't lead to a more secure environment. Instead, the rigidness of the policy forces people to find ways around it and not be transparent.

The fine line that security teams walk is to **uphold robust security measures without limiting business agility and innovation.**

> At the end of the day, people need to do their job. My job is not to stop them from doing their job — it's to make sure they do it safely and securely.

Jason Steer
CISO, Recorded Future

Threat intelligence helps organizations balance security with agility. When the cybersecurity team can compare the overall threat landscape to their own company's specific needs and vulnerabilities, employees can innovate and work safely. Security leaders need to be aware of how policy inflexibility negatively impacts employees' workflows. When they instead partner with other teams and equip them with safe and secure best practices, security becomes a strategic enabler of the entire company.

This is the future of threat intelligence, and it's why so many companies are increasing their investment.

They need a central source of information on the threats they face, actionable insights, and robust support to guide them through their unique security needs and challenges.

Time to take stock: How does your strategy compare?

In light of this overview of the 2024 outlook on threat intelligence, you might be considering how the program at your organization stacks up. **How mature is your threat intelligence strategy?**

The vast majority of security practitioners and leaders are doubling down on threat intelligence — spending more, expanding and enhancing their uses for its insights, and

folding it into a more strategic role. Increased threat intelligence spending across the board — along with the ever-growing sophistication of threat actors and vectors — should signal that now is the time to revisit your own investment.

Just as strong threat intelligence entails finding weaknesses and vulnerabilities in your infrastructure, strong security entails looking for the gaps in your threat intelligence strategy. As Jason Steer asks, "How confident are you in your EDR tool and other security controls actually giving you the early signs of a ransomware attack? That's why you need to rethink your security tools."

Whether your team faces operational inefficiencies or reacts to attacks instead of proactively addressing risks, a comprehensive threat intelligence solution is worth the investment.

> Threat intelligence will always improve your visibility. The important part is to do so without overburdening your team.

Jason Steer
CISO, Recorded Future

To see more threats, identify them faster, and take action to remediate attacks, look to the most comprehensive and independent threat intelligence platform. Invest in Recorded Future —

Explore today >

UserEvidence Research Methodology

About UserEvidence

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according totheir research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

UserEvidence Research Principles

These principles guide all research efforts at UserEvidence -whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

Principle 1 - Identity verification.

In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (ie so a vendor can't just create 17 gmail addresses that all give positive reviews).

Principle 2 - Significance and Representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas - to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

Principle 3 - Quality and Independence

UserEvidence is committed to producing quality and independent research at all times. This starts at beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

Principle 4 - Transparency

We believe research should not be done in a black box. Fortransparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.