ThreatConnect.
now a part of Dataminr

Unified Cyber Risk Intelligence (UCRI) in Action

Results of Our 2025 Customer Survey

Contents

ThreatConnect.
now a part of Dataminr

Executive Overview

Great Intelligence Doesn't Live in Dashboards. It Changes Outcomes.

Security teams aren't short on data. They're short on **intelligence that actually changes outcomes.**

What teams need instead is decision-grade intelligence: intelligence that arrives with enough context, relevance, and confidence to support real decisions — not just analysis.

Across industries, defenders are inundated with alerts, indicators, and risk signals. But signal volume doesn't translate into advantage, and, in fact, often leads to alert fatigue, analyst burnout,false positives, and missed attacks. In practice, most teams still struggle to answer three basic questions fast enough to matter:

- Does this emerging threat matter to us?
- If so, how much does it matter to the business?
- What action is actually warranted right now?

For many teams, these questions surface in the worst possible moments — during a zero-day headline, an executive escalation, or a late-night incident bridge. Alerts are firing. Slack channels are exploding. Someone is pasting CVEs into chat while another person scrolls through dashboards trying to reconstruct context that should already be there. Decisions still have to be made — even when the intelligence isn't ready.

Industry analysts have put a spotlight on this gap and begun to name ways to close it. Gartner, for example, describes it through the concept of **Unified Cyber Risk Intelligence (UCRI)** — a model that emphasizes fusing internal and external signals, aligning intelligence to business risk, and delivering it to the teams that must act.

What Is Unified Cyber Risk Intelligence (UCRI)?

Unified Cyber Risk Intelligence (UCRI) is a framework developed by Gartner to describe how modern security teams should operate: by fusing internal and external signals, aligning intelligence to business risk, and delivering that intelligence directly to the teams that must act on it.

In other words, UCRI is about turning intelligence into decisions — and decisions into action.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

Gartner and other analysts are seeing what ThreatConnect customers have long recognized – intelligence is only helpful if it provides foresight into what may happen, focuses resources on the most significant threats, and enables rapid and decisive action. This report is not an analysis of the UCRI or other analyst frameworks. Instead, it shows the real-world results that can be achieved when these frameworks turn into action.

The 2025 ThreatConnect Customer Survey captures how organizations use ThreatConnect to turn intelligence into an operational system—one that delivers early awareness, sharper focus, and decisive action across detection, response, vulnerability management, and leadership.

The takeaway is simple:

When intelligence is unified, contextualized, and operationalized, cyber defense teams stop reacting — and start leading with confidence.

Why Intelligence Fails to Enable

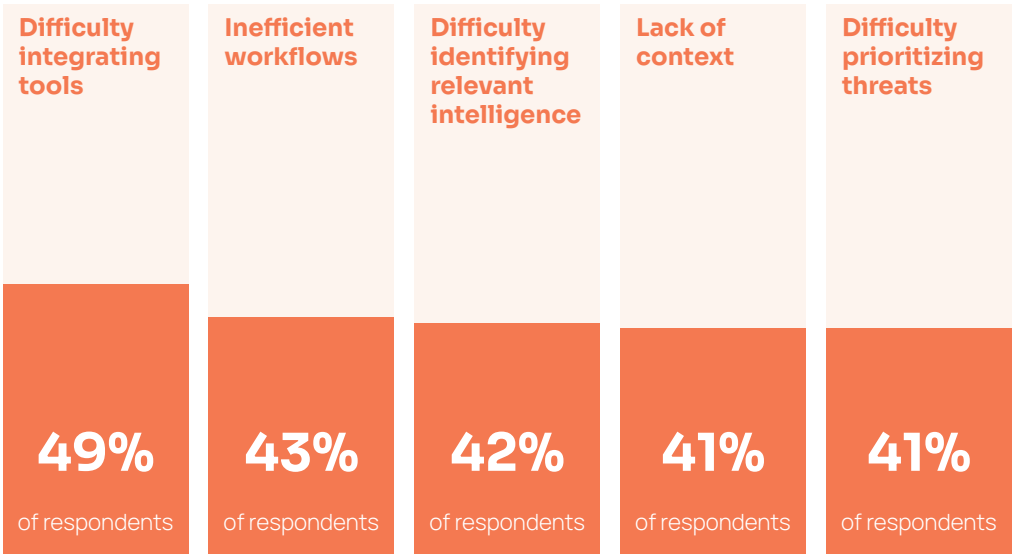
The Case for ThreatConnect (and for UCRI) Cyber Defense

Before adopting ThreatConnect, survey respondents described a familiar reality: intelligence existed — but it didn't move fast enough, didn't carry enough context, and rarely landed where real decisions were made.

What Gartner labels as the *"absence of unified intelligence"* showed up for customers in very practical ways: disconnected tools, missing context, and an inability to prioritize what actually mattered.

Instead of a shared, operational view of risk, teams were forced to manually stitch together context — pulling indicators from one tool, asset details from another, and business impact from spreadsheets or tribal knowledge — often while an incident was already unfolding.

Top Challenges Before Implementation



These challenges are the predictable outcome of intelligence that isn't unified — regardless of what framework, vendor, or reporting model sits on top of it.

The Cost of Fragmentation (By Product Area)

49%
of respondents reported difficulty integrating SIEM, SOAR, and EDR tools

83%
struggled to find relevant information quickly during investigations

80%
struggled to prioritize threats by business impact

These customer-reported breakdowns are exactly what UCRI aims to prevent.

Customer Voice: What "Fragmented" Felt Like

> "ThreatConnect provides a single source of threat intelligence truth that is operationalized in one platform..."
>
> — Threat Hunter, Fortune 500 Insurance Company

This is the moment where unified intelligence stops being an abstract concept and starts being operationally real. The moment where intelligence either becomes operational — or becomes noise.

Before ThreatConnect, early warning often looked like this: a vague alert about "active exploitation in the wild," no clear indication of whether the organization was exposed, and no easy way to tell which systems — if any — were actually at risk. Teams either overreacted and burned cycles, or waited and hoped the issue wouldn't become their problem.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

ThreatConnect.
now a part of Dataminr

Foresight:

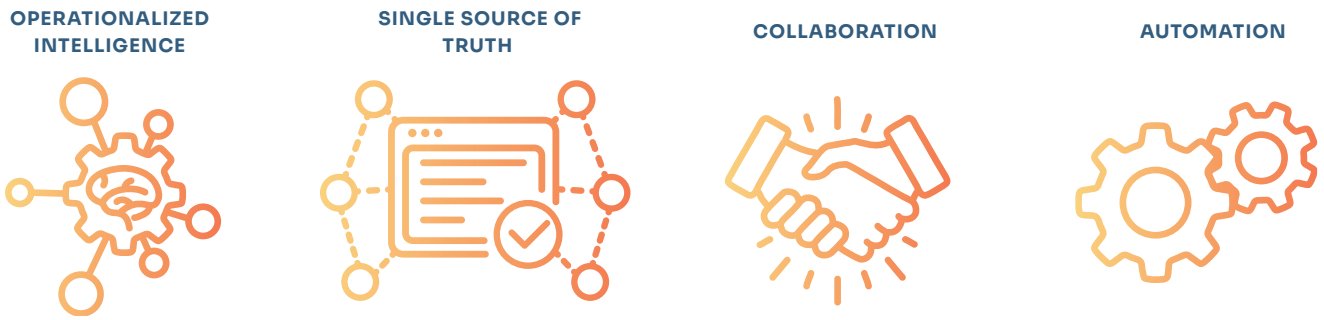
Seeing What Matters Earlier — and Knowing It's Relevant

The first breakthrough customers experience with ThreatConnect is **Foresight**: the ability to see emerging threats early, with enough context to know whether they matter. In Gartner's UCRI framework, this is the point at which internal and external signals are fused into a shared intelligence fabric.

In practice, customers describe it much more simply: They stop guessing — and having the same argument in three different tools about whether a threat is real for them.

What Customers Value Most (Foresight Signals)

Top Value Drivers Identified by Customers:



Operationalized Intelligence at Scale

Customers consistently describe this as the moment intelligence leaves the dashboard and enters the environment This is what UCRI-enabled Foresight looks like when it's real: intelligence that moves fast, carries context, and reaches every environment that needs it.

> "ThreatConnect has allowed us to operationalize hundreds of thousands of threat indicators across several disconnected enterprises."
>
> — Director of Cybersecurity Operations

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

Centralization Enables Context — Not Just Visibility

Centralization creates the conditions UCRI calls for — customers experience it as speed, confidence, and fewer blind spots.

> "ThreatConnect allows us to identify, contextualize, and enrich potential threats quickly..."
>
> — Senior Intelligence Analyst

Foresight Travels Downstream

79% of respondents reported that ThreatConnect improved the effectiveness of their SIEM, EDR, XDR, and SOAR tools. This is the clearest signal that Foresight isn't trapped upstream. It's reaching the cyber defense teams that act.

What Changes When Foresight Works

When Foresight is operating correctly — whether you call it UCRI or not — teams gain:

- Earlier awareness without noise
- Shared context across functions
- Confidence that what they're seeing actually matters

That confidence is what enables Focus.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

ThreatConnect.
now a part of Dataminr

Focus:

Seeing More Isn't Enough. Knowing What Matters Is the Breakthrough.

From Severity-Driven Reaction to Business-Aligned Decision-Making

Foresight answers the question *"Does this threat matter to us?"* **Focus** answers the harder one: *"How much does it matter — compared to everything else?"*

For many security teams, this is where intelligence programs stall. Even with better visibility, teams are still forced to make tradeoffs under pressure. Vulnerabilities stack up. Alerts compete for attention. Priority debates become subjective, inconsistent, or driven by whoever shouts the loudest.

This is the gap that Gartner's Unified Cyber Risk Intelligence (UCRI) model explicitly calls out: intelligence must be aligned with business risk—not just technical severity—if it's going to guide real decisions. ThreatConnect customers describe Focus not as a new process, but as a new level of clarity — one they can defend to leadership.

The Focus Problem Before ThreatConnect

In practice, prioritization often meant weighing multiple issues that all appeared "critical" on paper. One affected a development system with multiple compensating controls. The other touched a customer-facing application tied to revenue. Without business context, both landed in the same queue — and teams lost time debating instead of fixing the one that actually mattered.

Before implementing ThreatConnect, most customers struggled to translate intelligence into priorities that leadership could stand behind. They knew *what* was happening — but not *what mattered most to them* or w*hat to do first*.

Where Prioritization Broke Down

80%

of respondents struggled to prioritize threats by business impact before implementing cyber risk quantification with Risk Quantifier

44%

cited difficulty prioritizing threats as a top pre-implementation challenge

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

This wasn't a tooling gap. It was a decision gap — decisions were being made without enough context to drive the right focus. Without a way to connect threats to assets, controls, and business impact, prioritization defaulted to:

- CVSS scores
- Generic "critical" labels
- Volume-driven escalation

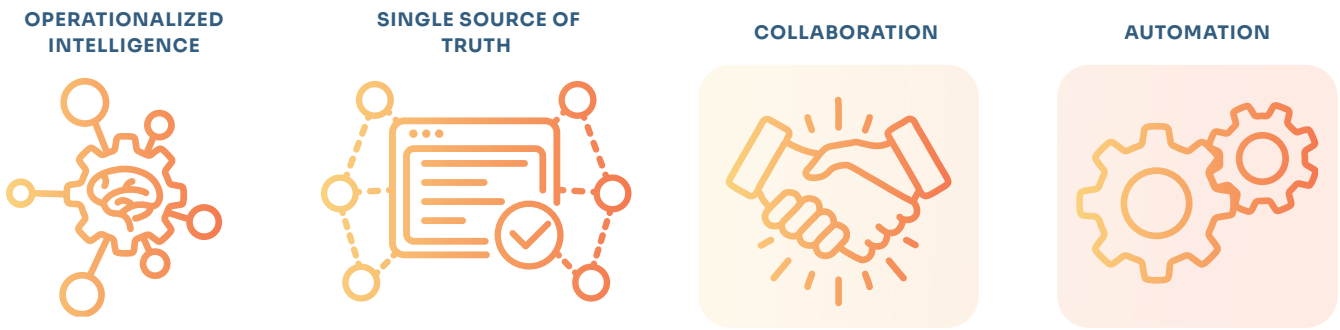
Which meant teams stayed busy — but not consistently effective.

What Focus Looks Like When It Works

Focus emerges when intelligence stops being descriptive and becomes **decision-grade.** Instead of asking, *"Is this bad?"* teams can ask, *"Is this bad for us — and how bad?"* In UCRI terms, this is where fused intelligence is contextualized against business objectives. In customer terms, it's where noise drops, and confidence rises.

What Customers Value Most (Focus Signals)

Top Value Drivers Identified by Customers:



In the context of Focus, automation and collaboration matter most — because prioritization only works if everyone sees the same picture.

Automation That Enables Focus — Not Just Speed

Automation is often framed as a way to move faster. Customers describe something more important: **the ability to concentrate effort where it matters most.**

80% of respondents identified the ability to bring together threat, asset, and business data as a key ThreatConnect differentiator

By unifying those data sets, teams aren't just automating tasks — they're automating *judgment*. This is where Focus becomes sustainable. Analysts don't have to manually reconstruct context for every alert. Priority is derived consistently, using the same inputs, across teams.

False Positives Drop When Priority Is Clear

74% of respondents reported false-positive reductions of

25% or greater

42% of respondents reported false-positive reductions of

50% or greater

One of the strongest indicators that Focus is working is what doesn't happen: unnecessary escalation.

Just as importantly, teams reported less second-guessing, fewer emergency escalations, and greater confidence in saying "this can wait"—without fear of being wrong in hindsight.

These reductions aren't the result of applying stricter filtering. They're the result of **prioritizing smarter** — understanding when a threat meaningfully changes risk posture, and when it simply adds noise.

This aligns closely with the spirit of UCRI: intelligence that enables teams to act and to confidently stand down when action isn't warranted.

Focus Creates Shared Confidence — Not Just Individual Insight

Customers repeatedly described ThreatConnect as a "**command center**" — a place where intelligence, operations, and leadership converge around the same set of facts. Where shared clarity matters. When priority is grounded in a business context:

- IR teams know what to tackle first
- Vulnerability teams know what can wait
- Leaders have confidence in why decisions were made

Debate shifts from *"Is this serious?"* to *"How do we address it?"*

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

ThreatConnect.
now a part of Dataminr

Action:

Turning Priority Into Decisive, Coordinated Response

From Focus to Action

By the time Focus is working, something subtle but important has changed.

Teams no longer feel trapped between:

- Overreacting to every headline, or
- Taking on risk they can't justify.

They know where to apply effort — and they can defend those decisions to the business. That clarity is what makes **Action** possible at scale.

Knowing What Matters Is Only Valuable If You Can Act on It

During an active incident, even small delays compound. Context gets lost as tickets move between teams. Analysts re-explain the same threat to responders, who then re-explain it to leadership — often with slightly different interpretations. By the time action is taken, the original intelligence has gone stale.

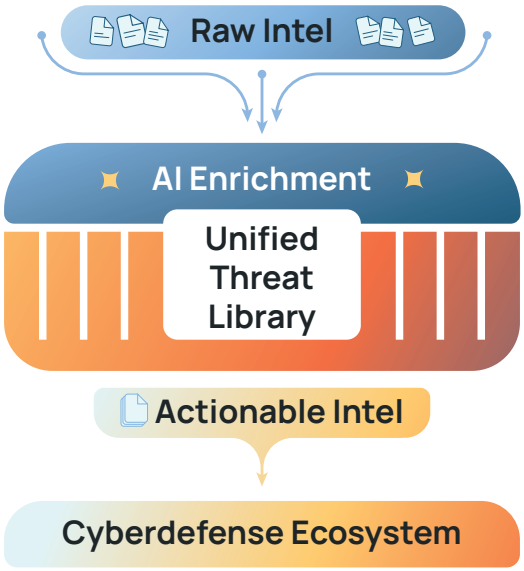
Foresight lets teams see what's coming. Focus lets them decide what matters most.

Action is where intelligence finally proves its worth.

This is the moment when decisions turn into containment, mitigation, and response — across IR, detection, vulnerability management, and leadership. And it's where many intelligence programs fail. Why? Because even when priorities are clear, execution is often fragmented:

- Context is lost as work moves between tools
- Manual handoffs slow response
- Teams operate in parallel, not in sync

In Gartner's UCRI framing, this is the final — and most critical — requirement: intelligence must be delivered to the right functions *in a form they can act on immediately.*



ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

ThreatConnect customers describe the shift in much simpler terms:

> "We stopped talking about what we should do — and started doing it."Action at Scale: What Changes After ThreatConnect

When intelligence is unified, and priorities are clear, response becomes faster — and more consistent.

Customers See Measurable Gains in Speed and Precision

70%
of respondents confirmed reduced Mean Time to Respond (MTTR) for standard incidents

70%
of respondents reported false-positive reductions of **25% or greater**

41%
of respondents reported false-positive reductions of **50% or greater**

70%
of respondents said ThreatConnect improved the effectiveness of their SIEM, EDR, XDR, & SOAR tools

These results point to a single theme:

Better intelligence at the start of the workflow produces better outcomes at the end. Action isn't happening faster because teams are rushing. It's happening faster because they're **starting from better intelligence.**

Automation That Executes — Not Just Accelerates

Automation plays a central role in Action — and customers are clear about how it helps. It's not about removing humans from the loop. It's about removing friction from execution.

That level of automation doesn't just save time. It ensures that when action is taken, it's:

- Consistent
- Context-aware
- Aligned with earlier prioritization decisions

> "ThreatConnect has made it easier to streamline how we act on an alert, automating up to 70–80% of the workflow."
>
> — Automation Engineer

Alert → Context → Action

Action Travels Across the Security Stack

One of the strongest signals that Action is working is how far intelligence travels *after* a decision is made. ThreatConnect customers report that intelligence doesn't stall at the point of analysis — it flows into the systems responsible for execution.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

81% of respondents reported improved effectiveness of SIEM, EDR, XDR, and SOAR tools

This matters because it shows Action isn't isolated to one team or workflow. It's coordinated.

In UCRI terms, this is downstream dissemination. In practice, it means responders start with answers — not questions.

When Action Works, Confidence Follows

Speed is important. Confidence is essential. When teams know:

- Why they're acting
- What outcome they're trying to achieve
- And how that action aligns to business priorities

Response becomes something they can **defend** — not just execute. And leaders are confident that their teams are taking the optimal action to eliminate exposure and improve their security posture.

That confidence is evident in how customers rate ThreatConnect's role in their operations.

ThreatConnect Becomes Mission-Critical

79% of respondents rated ThreatConnect as "critical" or "very important" to operations.

That rating reflects more than satisfaction.

It reflects reliance — on intelligence teams' trust during high-pressure moments, when the cost of being wrong is high and the tolerance for delay is low. ThreatConnect isn't just supporting response — it's shaping how response happens.

Customer Voice: Action Without Friction

> "ThreatConnect tools are user friendly, offering robust API capabilities that offer a seamless integration within one's network — enabling users to quickly respond to cyber threats."
>
> — Global Director of Threat Intelligence

This quote captures the final outcome of Action done right: Execution that feels natural — not forced.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

From Action to Operating System

When Foresight, Focus, and Action work together, something fundamental changes. Threat intelligence stops being a supporting function and becomes an **operational backbone** — informing decisions, guiding execution, and improving outcomes across the organization.

This is where ThreatConnect customers find themselves today:

- Seeing threats earlier
- Prioritizing based on real business impact
- Acting faster, with confidence, across the stack

Analysts may describe this progression using frameworks such as Unified Cyber Risk Intelligence. Customers describe it through results.

Either way, the outcome is the same: **Intelligence that actually changes outcomes.**

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

ThreatConnect.
now a part of Dataminr

Intelligence Is Only Valuable When It Changes What Happens Next

Across this report, one pattern is unmistakable.

ThreatConnect customers aren't winning because they collect more intelligence. They're winning because intelligence has become **operational.**

It shows up earlier.

It arrives with context.

And it drives decisions that teams can execute — and defend.

Seen through an industry lens, these outcomes closely resemble what Gartner describes as Unified Cyber Risk Intelligence: intelligence that is unified, contextualized, and delivered to the teams that must act. But customers didn't adopt a framework.

They adopted a system that works.

What the Survey Proves

The 2025 ThreatConnect Customer Survey doesn't just reflect satisfaction. It reflects **operational dependence.** Across industries and use cases, customers report that ThreatConnect enables them to:

- See emerging threats earlier — with relevance
- Prioritize risk based on real business impact
- Act faster, with fewer false positives and less friction
- Improve the effectiveness of the tools they already rely on
- Reduce response time while increasing confidence

These are not abstract benefits. They are measurable outcomes — backed by real data, real workflows, and real teams operating under real pressure.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

When Intelligence Becomes an Operating System

When Foresight, Focus, and Action work together, intelligence stops behaving like a feed, a report, or a function. It becomes infrastructure.

ThreatConnect customers describe this shift clearly:

- Intelligence informs detection before alerts fire
- Risk context shapes priority before tickets are created.
- Action is coordinated across teams before incidents escalate.

This is what it means for intelligence to operate continuously — not episodically — across the security organization.

Why This Matters Now

Threat environments are accelerating. Teams are under pressure to do more with less. And the cost of acting on the wrong signal — or acting too late — continues to rise. In that environment, intelligence programs don't need more dashboards. They need **decision-grade clarity.**

The results in this report show what's possible when intelligence is designed to support decisions — not just describe threats.

Final Takeaway

None of this is easy work. Security teams are asked to move faster, justify decisions more clearly, and reduce risk with fewer resources — often while being judged after the fact. The results in this report matter because they reflect what happens when intelligence finally supports teams rather than slows them down.

Frameworks like UCRI help articulate where the industry is headed. ThreatConnect customers are already there. They've moved beyond fragmented intelligence and reactive response and built a system that delivers:

- Earlier awareness.
- Clearer priorities.
- Decisive action.

That's not the future of threat intelligence.

It's what's working today — in production, under pressure, at scale.

Related Products

- **TI Ops** – Enrich vulnerabilities with live intel, ATT&CK mapping, and context models.
- **Polarity** – Surface vuln-to-threat context right in analyst workflows.
- **Risk Quantifier** – Translate exposures into financial risk and prove the ROI of patching.

Learn More:

sales@threatconnect.com

www.threatconnect.com

ABOUT THREATCONNECT:

ThreatConnect powers smarter, faster, and more resilient cyber defense by uniting threat intelligence, security operations, and cyber risk management. Our Intel Hub platform brings threat and risk data together to help organizations prioritize what matters most, operationalize defenses more efficiently, and communicate cyber risk in business terms. Trusted by over 250 global enterprises, ThreatConnect enables security teams to adapt to evolving threats, make better decisions, and prove their impact - from the SOC to the C-suite.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240