Five Threat Coverage Capabilities You'll Unlock With Outcomes Navigator

Know What You're Covering—and What You're Not

Most SIEM platforms stop at ingestion. But real security outcomes require more than collecting logs. They require visibility into what your data is actually doing: what threats it helps you detect, what gaps it leaves open, and how well you're aligned to strategic use cases and the MITRE ATT&CK® framework.

That's what Outcomes Navigator delivers. Built into the Exabeam New-Scale Security Operations Platform, it transforms passive data collection into active, actionable insight—no spreadsheets, bolt-on tools, or manual mapping required.

Five Capabilities That Turn Detection Into Outcomes

1. Real-Time Use Case Coverage Assessment

With Outcomes Navigator, you gain always-on insight into how well your environment supports the threats that matter most. It continuously maps ingested log sources with detection logic for high-priority use cases like lateral movement, phishing, or account compromise. Exabeam Nova tells your team exactly what's covered, what's not, and suggests next steps to improve your security posture.

Whether you're a CISO looking for high-level assurance or an analyst responsible for detection engineering, Outcomes Navigator gives you a single source of truth for evaluating your current posture.

Without this visibility, analysts are often forced to stitch together dashboards and spreadsheets to understand their coverage. Rule tracking becomes manual, use case alignment becomes inconsistent, and leadership is left making assumptions instead of confident, data-driven decisions. It becomes difficult to know whether you're better prepared for a ransomware attack or if insider threats will go undetected. Outcomes Navigator eliminates that guesswork by providing a real-time, prioritized view of your detection coverage so you can act decisively and improve continuously.

What this looks like without Outcomes Navigator:

- Analysts relying on tribal knowledge or spreadsheets to track detection rules
- Security leaders unsure whether key threats like ransomware or insider misuse are properly covered
- Gaps in use case coverage only discovered during an incident or audit

2. Native MITRE ATT&CK Alignment

Outcomes Navigator delivers built-in, continuously updated alignment to the ATT&CK framework without third-party tools or manual mapping required. It visually maps your current coverage across tactics, techniques, and procedures (TTPs), so you can quickly identify what is covered, partially supported, or what is missing entirely.

This gives security teams the ability to prioritize detection engineering and justify log collection based on threat coverage, not disconnected data points. And it helps prevent wasted effort by flagging when existing data already meets coverage goals. Additionally, Exabeam Nova reviews your coverage model, suggests improvements, and can engage in conversation to help you decide what do next.

What this looks like without Outcomes Navigator:

- Manual spreadsheets or disconnected tools to manually track ATT&CK framework alignment
- Uncertainty about which techniques your SIEM really detects
- Budget spent on new data sources without knowing if they improve ATT&CK coverage

3. Log Source Value Analysis

Most organizations ingest more logs than they need, but don't know which ones are contributing to meaningful outcomes. Outcomes Navigator gives you a clear, ranked view of log source value: Which data supports active detections mapped to ATT&CK, use cases, or compliance—and which logs are underused or irrelevant.

With this insight, teams can optimize log ingestion to reduce costs while improving effectiveness. You can confidently reduce or refine log collection without compromising visibility.

What this looks like without Outcomes Navigator:

- No visibility into which logs support real detections
- Overspending on low-value or redundant data that inflates storage, ingest, and licensing costs
- Difficulty justifying log collection and retention policies

4. Outcome-Driven Prioritization

Treating every log source or rule the same leads to wasted effort and missed outcomes. Outcomes Navigator helps you focus your program on high-impact priorities like insider risk, lateral movement, or compliance. It guides you toward the rules, fields, and data that matter, so your team can drive better results without overingesting or overbuilding.

By linking detection coverage to your specific goals, Outcomes Navigator makes it easier to tune existing content, identify where parsing improvements are needed, and avoid collecting data that doesn't move the needle.

Exabeam Nova, the security-specific AI assistant built into Outcomes Navigator, delivers prescriptive guidance based on your current posture and strategic goals. Its six specialized agents continuously evaluate your data, rules, and use case coverage to suggest improvements and highlight where your detection logic is already sufficient so you can reduce waste and focus effort on your organization's priorities.

These agents include:

- **Advisor Agent:** Surfaces ATT&CK and use case coverage gaps
- **Search Agent**: Enables natural language queries across your data
- **Visualization Agent:** Converts queries into dashboards and charts
- **Threat Scoring Agent:** Prioritizes detections based on dynamic scoring
- **Investigation Agent:** Summarizes threat context and recommended actions
- **Analyst Assistant Agent:** Provides real-time, context-aware support

These agents help make Outcome Navigator's guidance precise, dynamic, and aligned with how your team works.

What this looks like without Outcomes Navigator:

- Generic detection tuning with no link to business risk
- Ingesting more data just in case, instead of improving what you already have
- Limited ability to demonstrate program maturity or strategic coverage improvements

5. One Platform, No Extra Tools

Understanding your detection posture shouldn't require additional tools. Outcomes Navigator is built natively into the New-Scale Platform, with no separate UI, no agents to deploy, and no content packs to chase down. It's always on, continuously updated, and accessible to both analysts and security leaders, making posture insight a built-in part of your operations, not a separate project.

What this looks like without Outcomes Navigator:

- Reliance on external spreadsheets, custom dashboards, or third-party tools
- More time spent reporting on coverage than improving it
- Fragmented visibility across detection, data, and outcomes

Why It Matters Now

Security teams are under increasing pressure to modernize detection, cut unnecessary ingest costs, and prove value to the business. But without visibility into how your SIEM is performing—what it's detecting, what it's missing, and what to do about it—it's difficult to operate with confidence or improve over time.

Outcomes Navigator changes that. It continuously evaluates your detection coverage across use cases and frameworks like ATT&CK, shows which data sources are driving real outcomes, and highlights where additional logs, improved parsing, or rule adjustments could unlock better coverage. When no additional data is needed, it flags that, too—helping you reduce ingestion without introducing risk.

Security teams using Exabeam have already seen the benefits:

- 90% increase in detections for identity-based threats
- 70% of log sources onboarded in less than 30 days
- Over 50% reduction in time to detect and respond
- 35% lower total cost of ownership

These results aren't just operational wins. They're strategic differentiators. With trending insights and prioritized recommendations built in, security leaders can move beyond static reports and speak confidently about both current posture and future readiness. And with Exabeam Nova continuously analyzing detection logic, rule performance, and data contribution, your team gains guidance that's timely, actionable, and grounded in the actual state of your environment.

See Where You Stand

Want to understand your current posture and see what's possible with Outcomes Navigator?

- Watch the demo
- Read the Outcomes Navigator feature brief
- Request a personalized walkthrough

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

Learn more at www.exabeam.com →