

Exabeam vs. Splunk: Six Ways to Compare and Evaluate

SIEM platforms may appear similar, but important differences affect how your security team detects, investigates, and resolves threats. Splunk is widely used for log management, but many organizations encounter pricing complexity, modular add-ons, and operational friction. These issues slow progress when you're trying to improve threat detection, investigation, and response (TDIR).

Exabeam was created to solve these challenges. New-Scale Fusion uses machine-learned behavior models, Agent Behavior Analytics (ABA), dynamic risk scoring, and coordinated AI agents so you see risky behavior sooner and move investigations forward faster. This guide highlights six areas where Exabeam delivers stronger outcomes than Splunk.

1. Predictable Costs and Clear Value

Splunk's pricing hinges on ingestion volume, storage, compute, and multiple add-ons. As your data grows, you may see unpredictable charges, annual price uplifts, and rising spend when you enable advanced capabilities. Over time, these changes can raise your total cost of ownership.

Exabeam takes a modular approach. Analytics, automation, threat intelligence, user and entity behavior analytics (UEBA), and AI functionality are included. As your environment grows in volume and complexity, you gain more value from the same platform instead of constantly renegotiating how much you can afford to send to it. Exabeam reduces this overhead. You get broad prebuilt detection coverage, contextual correlation, and behavioral analytics without custom scripting. Move from detection to investigation in the same console instead of pivoting between tools and languages. Even if you don't have dedicated engineering resources, you can move faster because the platform carries more of the tuning work for you.

2. Less Tuning and Operational Overhead

Splunk requires continuous tuning. Your analysts must understand the Splunk Search Processing Language (SPL), configure correlations, maintain behavioral baselines, and make frequent adjustments to reduce irrelevant alerts.

Splunk also moved its updated UEBA into the Enterprise Security (ES) Premier tier. The older user behavior analytics (UBA) product reaches end-of-support on December 12, 2026. Customers must migrate to the new UEBA version, but there is no direct configuration or data migration path.

If you decide to adopt Splunk UEBA, you must also license ES Premier. That bundle includes security orchestration, automation, and response (SOAR); Threat Intelligence

Management; and the Splunk AI Assistant, even if you only want UEBA. You still face limited automation, heavy dashboard dependence, and little flexibility to adjust the underlying behavior detection logic. On top of that, behavioral modeling increases compute requirements, so you may need more Splunk Virtual Compute (SVC) units or additional hardware. Customers using ingest-based pricing typically see annual costs ranging from \$1,800 to \$18,000 for 1–10 GB per day depending on terms and support levels.

Exabeam reduces this overhead. You get broad prebuilt detection coverage, contextual correlation, and behavioral analytics without custom scripting. Move from detection to investigation in the same console instead of pivoting between tools and languages. Even if you don't have dedicated engineering resources, you can move faster because the platform carries more of the tuning work for you.

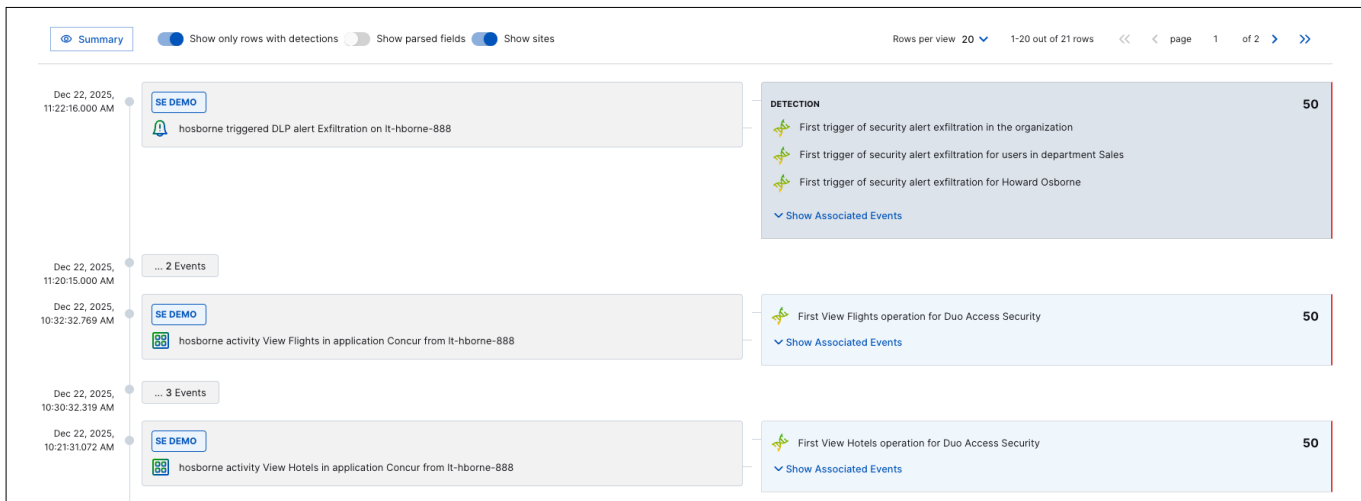


Figure 1.

Threat Timelines assemble related activity into a clear sequence so you can see how suspicious behavior unfolds from start to finish.

3. Manual Workflows Slow Investigations

QRadar forces analysts to pivot between tools, reconstruct timelines, and repeat enrichment steps. These gaps slow investigations and increase operational strain.

Why Exabeam

Threat Center centralizes alerts, evidence, and timelines. Threat Timelines reveal user and entity activity in order, giving you a clearer understanding of how an incident unfolds. Exabeam Nova agents streamline key steps. The Investigation Agent creates summaries and proposes next actions. The Analyst Assistant Agent brings forward relevant evidence as you work. With Automation Management and no-code playbooks, teams eliminate repetitive steps and focus on resolution.

4. Built for the Cloud, Not Adapted for It

Splunk Cloud is a managed version of an on-premises architecture. Scaling often feels like hardware planning. At higher event volumes, you can run into performance bottlenecks. Updates may require downtime and partial outages are common. Because the architecture relies on search-time processing rather than parsing at ingestion, performance can slow as your data grows.

New-Scale Fusion is cloud native. It processes more than two million events per second (EPS) and manages ingestion, parsing, and detection from one console. See system health, consumption, and performance at a glance and know where to act if something degrades. OpenAPI Standard (OAS) support makes it easier for you to connect the platform to your broader security and IT ecosystem.

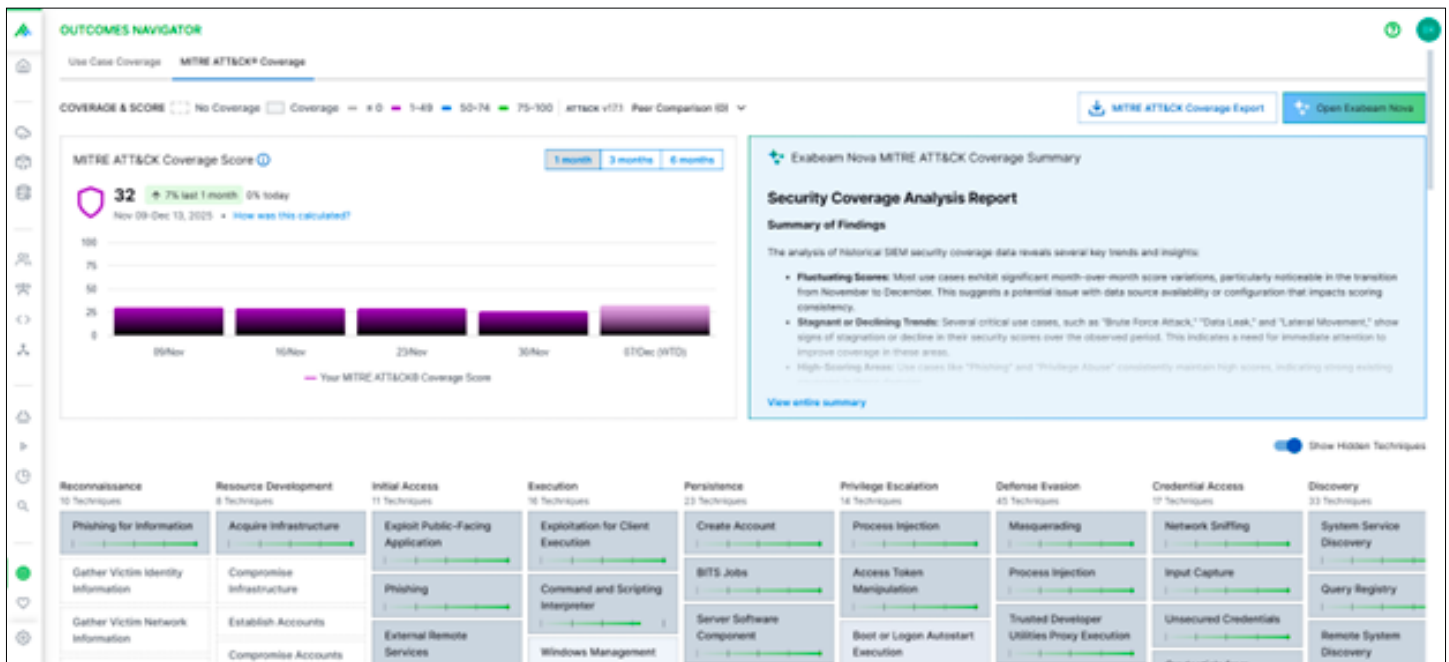


Figure 2. Outcomes Navigator shows detection coverage mapped to ATT&CK and highlights where to focus improvements.

5. Stronger Detection Coverage From Day One

Exabeam provides extensive prebuilt detection coverage aligned to the MITRE ATT&CK® framework. With the Outcomes Navigator app, you see which detections are fully covered, which are partial, and where you have gaps mapped to real use cases. You also receive prioritized recommendations so you know which improvements to make first.

Splunk offers Security Essentials with mapped detections, but program-level visibility is limited.

Teams often have to build custom dashboards or bring in third parties to understand how detection coverage is trending. Splunk ES includes roughly 200 prebuilt detections. That means you still need to build correlations for lateral movement, privilege escalation, and insider threats, and you may not reach mature detection coverage for six to twelve months.

Exabeam shortens this timeline by combining behavioral analytics for users, entities, and agents; dynamic risk scoring, and clear posture guidance so you can see exactly where to strengthen your program next.

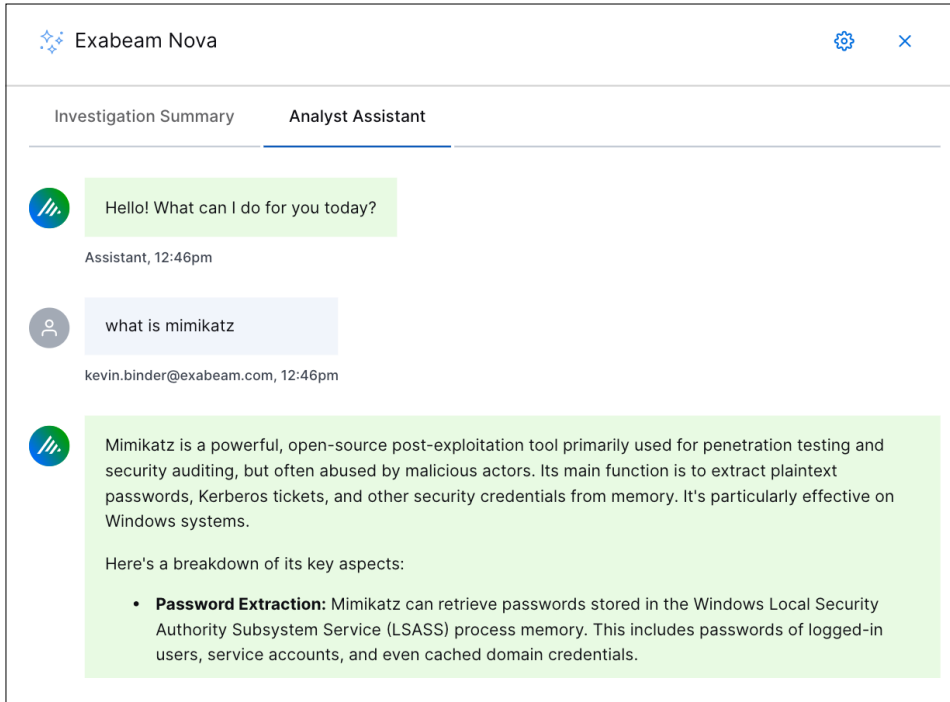


Figure 3.

The Exabeam Nova Analyst Assistant Agent answers questions in real time and provides clear context to help you move investigations forward.

6. AI Agents That Drive Real Outcomes

The Splunk AI Assistant converts natural language into SPL and offers basic triage help. These features depend on specific cloud versions and must be enabled by account teams. More advanced agents are still pending general availability.

- **Exabeam Nova** is a system of six coordinated AI agents within New-Scale Fusion that helps at each stage of detection, investigation, and response:
- **Advisor Agent:** Delivers daily security posture insights, shows ATT&CK mappings, and provides prioritized recommendations through Outcomes Navigator
- **Search Agent:** Converts natural language into Exabeam Query Language (EQL) for deep search in multiple languages, aligned to the Common Information Model (CIM)

- **Visualization Agent:** Builds dashboards and charts from search results, helping identify patterns and anomalies
- **Threat Scoring Agent:** Assigns contextual risk scores using adaptive learning to prioritize events and cases
- **Investigation Agent:** Generates summaries, classifies activity, and recommends next steps to help close cases faster
- **Analyst Assistant Agent:** Provides real-time investigation support by surfacing relevant evidence and answering analyst questions

These agents automate repetitive work, reduce manual context gathering, and help show you measurable improvements in your security program without extra modules, usage limits, or version restrictions.

Augmenting Splunk With New-Scale Analytics

If you're not ready to replace Splunk, you can augment it with [New-Scale Analytics](#) to add advanced behavioral detection, risk scoring, and automation.

How It Works:

- Splunk continues to be your log collection and storage platform.
- Exabeam connects through the Splunk Cloud Collector or APIs to ingest both live and historical data.
- Data is normalized using the Exabeam Common Information Model for consistent parsing and correlation.
- More than 500 machine-learned behavioral models baseline user and entity activity.
- Deviations receive risk scores and related activity is assembled into Threat Timelines.
- Outcomes Navigator maps your data to use cases and ATT&CK, helping you find detection gaps and set priorities for improvement.

Why Teams Use This Approach

By layering New-Scale Analytics on top of Splunk, you gain high-fidelity detection of credential misuse, insider threats, and lateral movement while reducing false positives and analyst workload. It gives you a low-disruption, cost-effective path to modernize security

Conclusion

Log search alone can't meet the needs of a modern security operations team. Exabeam delivers behavior-based detection, automated timelines, AI agents, and posture insights that strengthen investigation and response. You see activity in context, resolve more threats, and advance program maturity forward without overhauling your entire stack.

If you want to explore what this looks like in your own environment, [request a demo](#) of New-Scale Fusion and see how to modernize detection, investigation, and response without a disruptive migration.

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 →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.
© 2026 Exabeam, LLC. All rights reserved.