New-Scale Analytics

Accelerate Threat Detection With Advanced Behavioral Analytics for Human and Digital Entities

Security teams face a constant stream of alerts while advanced threats hide abnormal activity inside legitimate behavior. New-Scale Analytics detects these threats earlier by applying behavioral analytics to users, service accounts, and AI agents and automating investigation steps. Your team can focus on credible, high-risk activity instead of alert volume.

Threat Detection Built for Today's Challenges

New-Scale Analytics strengthens existing SIEM investments by identifying activity that traditional rule sets can miss. It analyzes broad telemetry, including network data from NetMon, the network traffic analysis add-on, and emerging AI usage signals. This exposes low-and-slow attacks that blend into routine operations.

Integrated Exabeam Nova agents extend detection and investigation by:

- Assisting with rule creation and conversion
- Automating triage workflows and background context collection
- Summarizing threat activity
- Grouping related detections and historical cases
- Guiding investigation steps

This reduces manual analysis and helps analysts prioritize high-risk activity sooner.

Establish Behavioral Baselines and Identify Risk Faster

New-Scale Analytics continuously builds and adapts behavioral baselines for every user, account, and agent. It combines user and entity behavior analytics (UEBA) with Agent Behavior Analytics (ABA) in a unified model, creating an evolving view of behavior for human and AI agents. Direct Claude Enterprise ingestion adds activity logs and chat API telemetry to this behavioral context.

When activity deviates from individual or peer baselines, New-Scale Analytics applies multi-layered risk scoring that combines behavioral variance with contextual signals. This prioritizes activity that indicates credible risk rather than simply elevating frequent events.

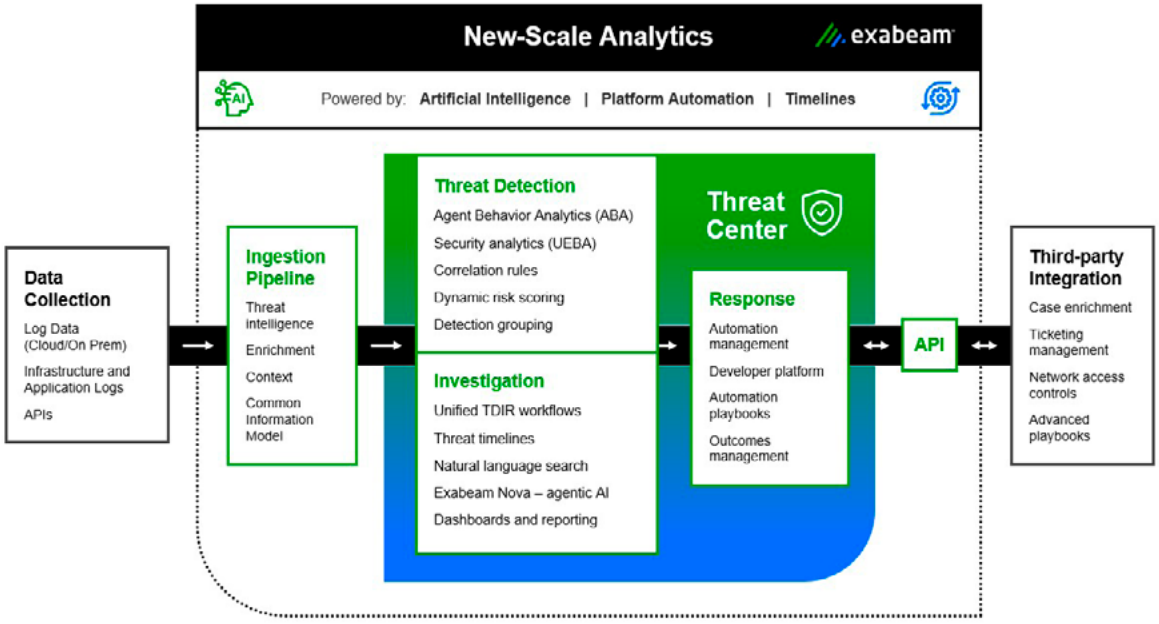

Figure 1.

New-Scale Analytics turns raw log data into prioritized behavioral detections, dynamic timelines, and automated response.

Prioritize Risk With Business Context

Attack Surface Insights enriches detections with business context. It builds behavioral profiles with attributes such as executive status, system function, privilege level, access scope, and usage patterns for human users, service accounts, and AI agents.

This context feeds the machine-learning engine so risk scores reflect potential impact, not only event frequency. Continuous risk scoring also incorporates late-arriving data, giving analysts an updated view of emerging risk without depending solely on static correlation.

Search and Investigate With Exabeam Nova

The Exabeam Nova Search Agent uses natural language processing (NLP) to convert plain-language queries into structured searches. It also generates dashboards and reports and provides persistent, platform-wide access from the analyst sidebar. Analysts can investigate threats and generate insights without specialized query syntax, accelerating threat hunting and reporting workflows.

Measure Coverage and Guide Improvement

The Exabeam Nova Advisor Agent in Outcomes Navigator provides measurable insight into security program performance. It benchmarks coverage and effectiveness against:

- Strategic use cases
- MITRE ATT&CK® techniques
- Industry peers
- Compliance frameworks
- OWASP Agentic Top 10

These insights help you identify coverage gaps, prioritize improvements, and communicate security outcomes in executive terms.

Extend Existing Security Investments

New-Scale Analytics adds advanced behavioral analytics to current environments without requiring SIEM replacement. It strengthens detection for insider threats, credential misuse, and AI agent misuse while providing a unified behavioral view of humans and AI agents.

Built on New-Scale Fusion

New-Scale Analytics runs on New-Scale Fusion, a cloud-native foundation designed for scale and operational efficiency. It centralizes:

- Data collection
- Behavioral analytics
- Investigation workflows
- Response automation

Embedded Exabeam Nova agents automate threat detection, investigation, and response tasks using behavioral context from UEBA and ABA models.

Benefits of New-Scale Analytics

Complete Threat Visibility

Automatically assemble related activity into investigation timelines and apply dynamic risk scores to users, service accounts, and AI agents. Persistent, platform-wide search is available from the analyst sidebar.

Streamlined Data Integration

Onboard and monitor data sources through the Common Information Model (CIM) to maintain consistent data structures across analytics pipelines.

Accessible Threat Hunting

Use natural-language queries through Exabeam Nova so analysts at any skill level can investigate threats without specialized query syntax.

Accelerated Detection Engineering

Deploy curated detection content with automatic rule variations. Exabeam Nova assists with rule creation and Sigma-to-native conversion.

SIEM Interoperability

Extend an existing SIEM with behavioral analytics and unified detection workflows without replacing current infrastructure.

Reduced Data Movement

Use federated search and flexible forwarding to analyze data without relocating it, helping optimize storage architecture and cost.

Machine and Agent Behavior Monitoring

Use ABA to monitor applications, service accounts, and AI agents and identify deviations that indicate compromise or misuse.

Optimized Security Coverage

Map data sources to security use cases and receive recommendations to improve correlation, visualization, and detection coverage. Outcomes Navigator Overrides let teams manually map custom data sources to specific use cases. The Exabeam Nova Advisor Agent extends coverage mapping to frameworks such as the OWASP Agentic Top 10.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

exabeam

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.