New-Scale Fusion

New-Scale Fusion is a cloud-native security operations platform built for speed and scale. It unifies threat detection, investigation, and response (TDIR) by combining security information and event management (SIEM), user and entity behavior analytics (UEBA), and automated response in one platform. Expanded Agent Behavior Analytics (ABA) adds visibility into both human users and AI agents operating in your environment. Native telemetry from generative AI systems, including OpenAI Chat GPT, turns previously opaque AI activity into structured data your team can search, analyze, and investigate

The platform provides an intuitive experience that simplifies log onboarding and helps teams gain value sooner. Behavioral analytics, dynamic risk scoring, and automated workflows reduce alert fatigue and elevate real threats so analysts can focus on high-value work.

Benefits

- **Unify data for TDIR:** Use a centralized workbench for search, dashboards, case management, and coordinated response.
- **Detect advanced threats:** Apply behavioral analytics to identify anomalous activity from users and AI agents and reveal full attack paths.
- **Accelerate TDIR with AI:** Use Exabeam Nova agents to automate evidence collection, correlate detections, and present recommended actions.
- **Gain visibility into AI-driven workflows:** Ingest native ChatGPT telemetry to observe AI agent activity and user-agent interactions.
- **Automate response actions:** Use Automation Management to standardize workflows, orchestrate actions, and notify teams when threats require action.
- **Enable secure AI innovation:** Use the MCP Server to expose case data, scores, and Exabeam Nova investigation summaries to custom enterprise AI agents through monitored, controlled interfaces.
- **Simplify integrations:** Support for the OpenAPI Standard (OAS) accelerates onboarding for data sources, workflows, and automation.
- **Map coverage to frameworks:** Outcomes Navigator shows how your data sources support security use cases and MITRE ATT&CK® techniques, and highlights areas for improvement.
- **Monitor security operations health:** Track uptime, parser performance, and license usage from a unified view to support capacity planning.
- **Scale with confidence:** A cloud-native, microservices-based architecture delivers performance and elasticity for enterprise environments.

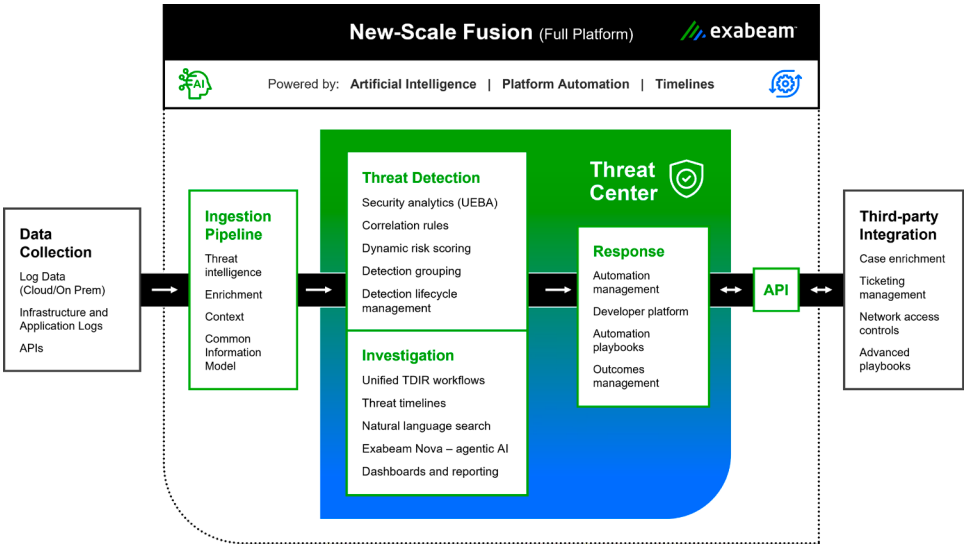

Figure 1.

New-Scale Fusion combines data collection, detection, investigation, and response into one cloud-native workflow.

A Unified Security Operations Platform

New-Scale Fusion combines SIEM, UEBA, and automation into a single workflow built for every security operations role. Its open architecture reduces skill requirements, speeds data ingestion, and helps teams onboard new sources quickly. Natural-language queries, advanced analytics, and behavioral models uncover threats traditional tools miss, including subtle activity from AI agents that appears legitimate at the event level but deviates from learned behavioral baselines.

The platform includes:

- **Threat Center:** A unified workbench for detection, investigation, and case management
- **Exabeam Nova:** A team of AI agents integrated into the platform
- **Outcomes Navigator:** A coverage mapping and benchmarking application
- 600+ product integrations for critical security technologies

Threat Center

Threat Center centralizes threat management, investigations, and automation. Intelligent correlation reduces noise so analysts can focus on meaningful activity. Automated evidence collection and timeline creation present full incident narratives in seconds. Behavioral detections for AI agents are grouped and scored with the same workflow used for human-driven threats, enabling consistent handling of both.

Exabeam Nova

Exabeam Nova is a team of AI agents that consume behavioral detections for human and non-human identities. They support analysts by automating analysis, correlating events, and presenting the most relevant details for response.

- **Investigation Agent:** Creates case summaries, highlights attack vectors, and recommends next steps.
- **Advisor Agent:** Delivers daily reports on security posture, coverage, and use case alignment; integrates with Outcomes Navigator for program insights.
- **Search Agent:** Converts natural language into Exabeam Query Language (EQL) queries mapped to the Common Information Model (CIM) for precise results.
- **Visualization Agent:** Builds charts and dashboards from natural-language prompts to show trends and patterns.
- **Analyst Assistant Agent:** Provides fast, context-aware answers to investigation questions.
- **Threat Scoring Agent:** Applies dynamic risk scoring to surface the most urgent events.

Automation Management

Automation Management includes prebuilt playbooks and a no-code editor to standardize response workflows, automate repetitive tasks, and accelerate incident resolution.

With hundreds of prebuilt integrations and drag-and-drop orchestration, you free analysts from manual work and improve consistency across all response actions.

Platform Capabilities

Behavioral Analytics

Applies machine learning to establish behavioral baselines for every user and entity, including AI agents. Dedicated models identify anomalies tied to cloud, identity, and AI activity. Native ingestion of Google Gemini and ChatGPT logs converts AI actions into structured analytics and investigation data.

Collectors

Configure and manage log ingestion from cloud, on-premises, and contextual sources through a single interface.

Common Information Model (CIM)

Normalizes raw logs for faster correlation, rule building, and search accuracy

Context Management

Enriches logs with threat intelligence, geolocation, and user-host-IP mapping to improve investigations and detection logic.

Multi-Layer Risk Scoring

Applies adaptive scoring based on behavioral deviation, business context, and evolving AI agent activity.

Outcomes Navigator

Map log sources to use cases, ATT&CK techniques, and compliance requirements. Generates board-ready insights and peer benchmarks.

Search

Supports natural-language queries that translate to EQL with CIM alignment for reliable results.

Dashboards

Use prebuilt or custom dashboards to observe detection patterns, monitor investigations, and track compliance.

Log Stream

Supports large-scale ingestion with real-time parser monitoring through Live Tail.

Service Health and Consumption

Tracks uptime, data flow, and license consumption to support availability and capacity planning.

Threat Intelligence Service

Aggregates commercial and open-source threat intelligence, ranks indicators, and supports custom feeds through a STIX/TAXII Cloud Collector.

Notifications Service

Sends alerts and updates through email, Microsoft Teams, or Slack.

New-Scale API and MCP Server

Extends automation into third-party tools. The MCP Server provides secure access for custom enterprise AI agents using monitored queries.

Federated Search and Third-Party Data Storage

Enables federated search and external storage through add-on capabilities.

New-Scale Fusion includes core capabilities for detection, investigation, and response, with optional add-ons that expand retention, analytics depth, and data workflow flexibility. Your team can tailor coverage to your environment without adding unnecessary complexity.

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).

exabeam

Learn more at
www.exabeam.com →