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), behavioral analytics, and automated response in one platform.

Agent Behavior Analytics (ABA) extends visibility beyond human users to include AI agents operating in your environment. Native telemetry from generative AI systems, including Claude, ChatGPT, Gemini, and Microsoft Copilot, converts previously opaque activity into structured data your team can search, analyze, and investigate.

You get an intuitive experience that simplifies log onboarding and reduces time to insight. Behavioral analytics, dynamic risk scoring, and automated workflows reduce alert noise and prioritize the most critical threats first, so your team can focus on high-impact investigations.

Benefits

- **Unify data for TDIR:** Work from a centralized platform for search, dashboards, case management, and coordinated response.
- **Detect advanced threats:** Use behavioral analytics to identify anomalous activity from users and AI agents and reveal full attack paths.
- **Accelerate TDIR with AI:** Exabeam Nova agents automate evidence collection, correlate detections, and present recommended actions.
- **Gain visibility into AI activity:** Analyze telemetry from Claude, ChatGPT, Gemini, Microsoft Copilot, and open agent sources (BYO-AI).
- **Automate response**: Standardize workflows, orchestrate actions, and notify teams when action is required.
- **Enable secure AI innovation:** Use the MCP Server to expose case data, risk scores, and investigation summaries to enterprise AI agents through 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 supports use cases and ATT&CK techniques, and highlights gaps. It also maps coverage to frameworks such as the OWASP Agentic Top 10, with recommendations from the Exabeam Nova Advisor Agent.
- **Monitor platform health:** Track uptime, parser performance, and license usage in a unified view.
- **Scale effectively:** A cloud-native, microservices-based architecture delivers elasticity for enterprise environments.

A Unified Security Operations Platform

New-Scale Fusion combines SIEM, UEBA, and automation into a single experience for all security operations roles. Its open architecture reduces onboarding friction and helps your team add new data sources quickly.

Natural-language queries, advanced analytics, and behavioral models uncover threats traditional tools can miss, including subtle activity from AI agents that may appear legitimate at the event level but deviate from expected behavior.

Core components include:

- **Threat Center:** A unified workbench for detection, investigation, and case management
- **Exabeam Nova:** A team of AI agents embedded in the platform
- **Outcomes Navigator:** A coverage mapping and benchmarking application
- **Prebuilt integrations:** A broad set of integrations and detection content for rapid onboarding and coverage

Threat Center

Threat Center centralizes threat management, investigations, and automation. Intelligent correlation reduces noise and highlights meaningful activity. Automated evidence collection and timeline creation present full incident context quickly.

Behavioral detections for AI agents are grouped and scored using the same workflows applied to human-driven threats, enabling consistent response.

Exabeam Nova

Exabeam Nova is a set of AI agents that analyze behavioral detections for human and non-human identities. These agents automate analysis, correlate events, and surface the most relevant details to guide investigation and response.

Investigation Agent: Creates case summaries, identifies attack paths, and recommends next steps

Advisor Agent: Delivers reports on posture, coverage, and use case alignment, with integration to Outcomes Navigator for program insights

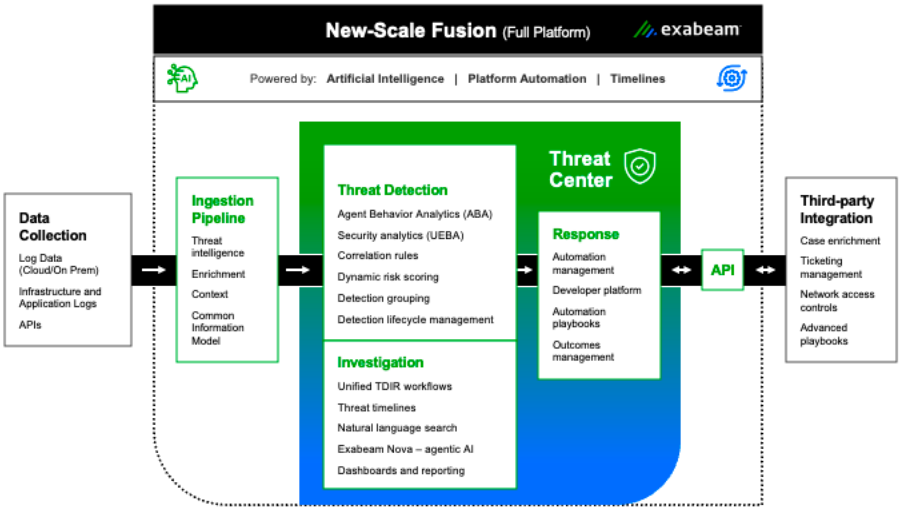

Figure 1.

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

Search Agent: Translates natural language into Exabeam Query Language (EQL) queries, aligned to the Common Information Model (CIM) for accurate results

Visualization Agent: Builds charts and dashboards from natural-language prompts to highlight trends and patterns

Analyst Assistant Agent: Answers investigation questions quickly and with context

Threat Scoring Agent: Prioritizes activity using dynamic risk scoring

Rule Creator Agent: Automates rule creation and converts Sigma and YARA rules to streamline detection development

Automation Management

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

With extensive integrations and drag-and-drop orchestration, your team can reduce manual work and improve consistency in response actions.

Platform Capabilities

Security Analytics for Human and Non-Human Identities

Applies machine learning to establish behavioral baselines for users, entities, and AI agents. Specialized models detect anomalies across cloud, identity, and AI activity.

Ingests telemetry from Claude, ChatGPT, Gemini, Microsoft Copilot, and open agent sources, converting AI activity into structured data for analytics and investigation.

Data Ingestion and Collectors

Collect and manage logs from cloud, on-premises, and contextual sources through a single interface.

Common Information Model (CIM)

Normalizes raw data to improve correlation, rule creation, and search accuracy.

Context Enrichment

Adds threat intelligence, geolocation, and user-host-IP mapping to improve detection and investigation.

Dynamic Risk Scoring

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

Outcomes Navigator

Maps log sources to use cases, ATT&CK techniques, and compliance requirements, including coverage mapping to the OWASP Agentic Top 10 with Exabeam Nova Advisor Agent recommendations. Provides insights and benchmarks to track program maturity and identify areas for improvement.

Search

Natural-language queries convert to EQL using CIM alignment for accurate results.

Dashboards and Reporting

Use prebuilt or AI-assisted dashboards to track detections, investigations, and compliance metrics.

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.

Threat Intelligence Service

Aggregates commercial and open-source 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 enterprise AI agents using monitored queries. Open agent telemetry, including Observra, enables structured visibility into agent interactions across integrated environments.

Federated Search and External Storage

Supports federated queries and external storage through add-on capabilities.

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 →