exabeam™

Exabeam
Solution Brief

Exabeam and Trellix

Enhanced Endpoint Security With Machine-Learned Detection and Context-Rich Investigations

Executive Summary

Endpoint detection and response (EDR) tools play a critical role in identifying threats at the edge, but without broader visibility security teams miss the full picture. By integrating Trellix Endpoint Security with the Exabeam New-Scale Security Operations Platform, you gain unified threat detection, investigation, and response (TDIR) powered by behavioral analytics, correlation, and automation.

Market Challenge

Endpoint data alone can't reveal the full scope of an attack. To respond effectively, security teams need context from the entire environment—including users, assets, networks, and cloud workloads—unified in a centralized platform built for TDIR.

Complete Threat Detection, Investigation, and Response

The New-Scale Platform combines SIEM, machine-learned detection, and automated workflows to give you full visibility into threats across your environment. Its cloud-native design supports rapid data ingestion, lightning-fast queries, and automated investigations—empowering analysts to detect, investigate, and respond faster and more accurately.

The integration with Trellix Endpoint Security strengthens these capabilities by enabling log ingestion and automated response actions. Exabeam ingests Trellix Endpoint Security alerts and enriches them with behavioral context and correlation, helping security operations teams spot attacker behavior early, understand it faster, and act decisively. Built-in low-code and no-code SOAR capabilities in Exabeam Automation Management allow security teams to build, test, and deploy playbooks that automate containment, ticketing, and triage.

Together, Exabeam and Trellix simplify security operations, reduce manual work, and improve cloud security posture so your team can focus on what matters: stopping threats before they escalate.

Key Integration Benefits

- **Faster threat detection** with automated correlation and investigation workflows
- **Stronger visibility** across cloud and endpoint infrastructure
- **Streamlined operations** with a preconfigured Trellix tile and API-based collector

Top Use Case: Situational Awareness

- **Definition:** The ability to quickly understand your current threat posture, identify risks, and measure how well your defenses are working
- **Challenge:** Without centralized visibility, analysts must manually pivot between Trellix, Exabeam, and other tools—slowing investigations and increasing risk.
- **Solution:** Ingest Trellix alerts into Exabeam to view endpoint and behavioral data from a single console. Track threats and response actions in real time with contextual timelines.

Integration Overview

Integrated Product: New-Scale Security Operations Platform (sold as Exabeam Fusion)

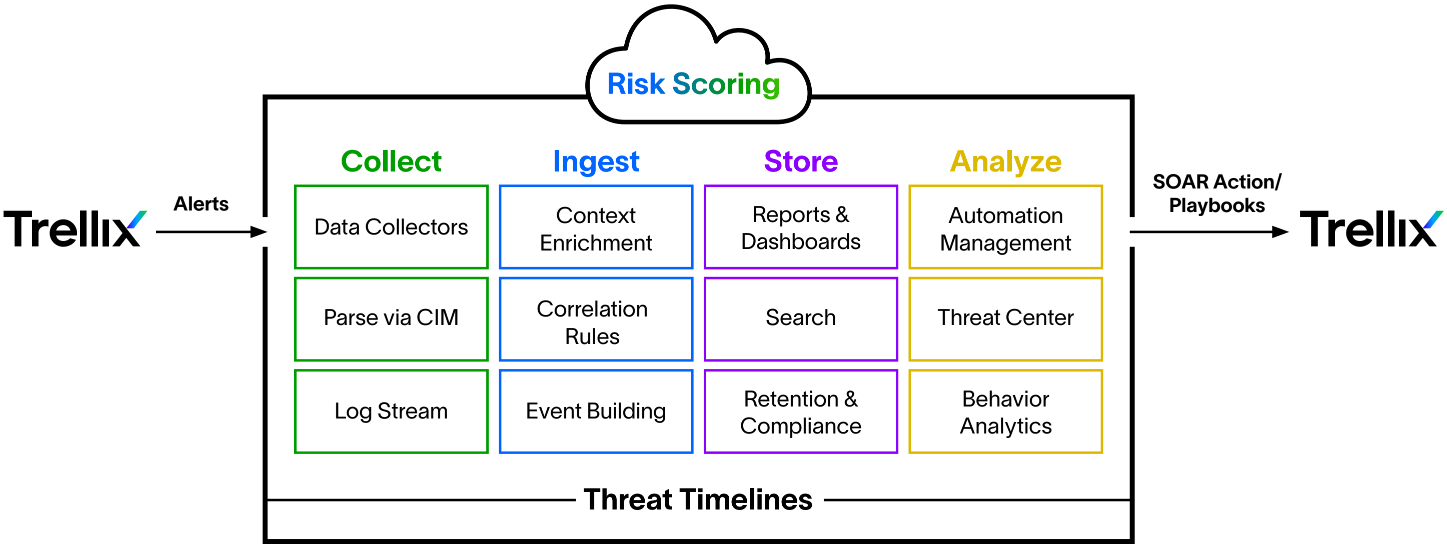

Figure 1. Trellix Endpoint Security alerts are ingested into Exabeam, enriched with behavioral context, and correlated across the environment to support threat detection and automated response. Automation Management enables custom notification and sends webhooks back to the Trellix console.

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 →

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.

2025 Exabeam, LLC. All rights reserved.