ANOMALI

GUIDE

5 Ways Anomali Delivers Better Security Outcomes than Exabeam

5 Ways Anomali Delivers Better Security Outcomes than Exabeam

Exabeam customers are feeling unsettled following the company's recent acquisition by private equity firm Thoma Bravo and the subsequent merger with former rival LogRhythm. The concern is understandable. This merge opens a host of unknowns, such as:

- Will Exabeam continue to support its Security Operations platform?
- What happens to innovation while these companies figure out integration? How will the product roadmap be impacted?
- Will pricing change?
- Will Exabeam end-of-life any of its legacy products? (We already know LogRhythm UEBA will be EOL.)
- Will you be forced to migrate to a new platform?

This is no longer the same Exabeam organization from which customers originally purchased. The organization's leadership, product innovation, and mission have changed. That's why so many Exabeam customers are exploring alternative solutions.

Security and IT Operations Done Differently

Anomali brings a modern approach to the SIEM market, consolidating security and IT operations into one easy-to-use, AI-powered, integrated platform. It enables you to detect, investigate, respond, and remediate threats at quantum-quick speed at a fraction of the cost of other solutions.

In contrast to the Exabeam products, the Anomali Security and IT Operations Platform provides a user-friendly natural language processing (NLP) interface that empowers a Tier-1 analyst to perform at the level of a Tier-3 — without the learning curve.

Five Ways Anomali Outperforms Exabeam

Below are five reasons why Anomali is superior to Exabeam in terms of cost, ease of use, search speed, threat intelligence, and tools for beginning threat hunters.

1. Straightforward Cost Model

Exabeam's pricing models are confusing, with limits on storage duration and the number of correlation rules allowed. Neither of their SIEM products, Exabeam SIEM nor LogRhythm SIEM, include user and entity behavior analytics (UEBA) functionality, so you'll have to pay extra for it. The self-hosted LogRhythm SIEM also sends local data to the Exabeam GCP instance and back to add UEBA capabilities.

Capability	Exabeam	Anomali
Event flows for UEBA	7GB/day	Unlimited
Full search	Varies from 7-30 days	Unlimited
"Hot" storage	30-45 days	7+ years
Correlation rules limit	100 (add-ons available)	Unlimited
MSSP capability	Not multi-tenant	Yes

2. Wanted: A Simple Interface

The Exabeam Security Operations Platform has separate apps for dashboards, UEBA, case management, correlation rules, search, and more. This is an artifact of the company's disjointed approach to developing its platform, adding one siloed application at a time. Further, there is no way to pull in new threat information or advisories from the web since the platform's threat intelligence service is a black box that feeds the platform. The net result is a woefully disconnected user experience.

As a cohesive platform, Anomali integrates the entire workflow, from threat detection to response. Visualizations allow SOC analysts to pivot around based on event, IP, credential, or indicator of compromise (IoC) before responding. This helps the SOC answer the burning questions faster:

- What activity is critical in priority?
- Have we seen a published attack or advanced persistent threat (APT) group in our environment? If so, when?
- Can we stop this activity right now?

The Exabeam Security Operations Platform's immature SOAR capabilities don't do much more than send cases and events to ITSM and comms systems. In contrast, Anomali Integrator allows analysts to tag indicators to create new rules that are pushed back into the security ecosystem, such as creating a firewall rule to block a known IoC or inbound port/IP combination.

3. Speedy Search

The Exabeam Security Operations Platform advertises a "lightning-fast" speed on searches… but just how fast is it? Promotional videos show a simple search on less than 1M logs less than a month old taking 30 seconds or longer.

Complicating the speed question is the fact that Exabeam defaults to retaining logs for one month unless you pay extra. Long-term search options are limited to one year of data. Access to long-term storage requires a customer support ticket, begging the question, "How long do you want to wait to search your own data?"

In contrast, Anomali's Security Data Lake keeps all your data hot and available, so you can search 7+ years of your data almost instantaneously — no extra charge. It can search up to 100B logs in under 10 seconds. A recent Anomali customer reduced their correlation search time from 48 minutes to 44 seconds!

What makes Anomali so fast?

Anomali's integrated Security Data Lake leverages AI to run queries in the most efficient way possible, dynamically spinning up the processing power for the length of time necessary to obtain results, and then shutting it down when you don't need it anymore. Because Anomali's Security Data Lake is cloud-native and serverless architecture, you won't be running an inefficient environment mismatched to your needs 24x7.

4. Superior Threat Intelligence

Exabeam's threat intelligence service provides five IoC feeds from open source intelligence (OSINT) and ZeroFox for integration into its cloud platform options. There is no option to add premium or ISAC intelligence.

Anomali ThreatStream is the leading Threat Intelligence Platform (TIP), providing curated access to more than 200+ threat intelligence feeds from diverse sources, including OSINT, commercial feeds, dark web monitoring, and proprietary research. Users can also add premium threat intel feeds (often with free trials) via the Anomali App Marketplace. This diverse, customizable library covers a wide spectrum of potential threats and attack vectors mapped to the MITRE ATT&CK® framework.

What's more, Anomali's threat intelligence doesn't live in a silo. The Anomali Security and IT Operations Platform infuses it into all alerts and incidents. This integration ensures seamless data analysis and better contextualization of threats, leading to more efficient detection and response.

Anomali is also an active member of the threat-sharing community. ThreatStream's Trusted Circles feature facilitates secure and efficient threat intelligence sharing among predefined groups, such as industry-specific consortia, government bodies, or partner organizations. These circles enable participants to immediately share relevant threat data while maintaining control over what is shared and with whom. This collaborative approach improves individual organizations' security while contributing to the broader cybersecurity ecosystem.

5. Tools for the Tier-1 Analyst

The Exabeam's tools for search and correlation rule writing can help experienced analysts and threat hunters find hidden threats. However, they may be too advanced for junior personnel. While it does include an AI-driven copilot built on a generic large language model (LLM) — albeit without specific threat information — inexperienced analysts and threat hunters may not know the right questions to ask, diminishing the feature's value.

Anomali Copilot is built on an LLM with access to the industry's largest repository of curated global threat intelligence, providing actionable insights in plain language. It bridges the gap between lower tiers of SOC analysts and threat hunters with easy-to-use AI-based tools and automated threat summarization. Analysts can pull web-based threat summaries into Anomali to compare with internal telemetry, enabling them to flag suspicious events as soon as they occur.

Anomali's AI empowers your Tier-1 analysts to be more proactive in fighting threats.

Anomali: The Future of SIEM

Anomali's groundbreaking AI-Powered Security and IT Operations Platform provides comprehensive visibility, speed, AI, and world-class threat intelligence in one, easy-to-use integrated platform. Anomali delivers first-in-market speed, scale, and performance, consolidates your tech stack, and empowers your team to do more with less.

Innovative, Effective Technology

Cybersecurity solutions for organizations of all sizes. AI-powered intelligence-driven solutions for a more secure world. That's Anomali.

Discover how Anomali can help you create a robust, highly adaptive security solution. Schedule a demo of Anomali's Security and IT Operations Platform to see why it's different and how it can transform your organization's security posture.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security and IT Operations Platform.

ANOMALI