4 Ways Exabeam Delivers Better Security Outcomes Than Securonix

While no solution can prevent all attacks, some can detect intrusions and malicious activity better than others. Far too often, your security information and event management (SIEM) solution is challenging due to a lack of specialized expertise to customize and maintain the system — or it's too costly to maintain and analyze all the logs that might help your teams discover what happened; when, where, and how it happened; and which credentials were involved.

Combating these challenges requires a system equipped with pre-built rules, timelines, and suggested guidelines for purpose-built security investigation — to find the true gems of discovery amidst the noise of alerts.

There are a lot of SIEMs in the marketplace from which to choose. But how do you distinguish between Exabeam and solutions such as Securonix to find the right fit for your organization?

Here are four reasons why Exabeam stands out as a superior SIEM choice:

1. Securonix does a poor job of providing full visibility to analysts

With Securonix, user and entity timelines are only generated when a policy violation has occurred; if a user or entity has no violation, they do not have a timeline in the solution. Securonix shows violations, but not what normal behavior looks like for individual users. It would take a Securonix analyst ~700 queries to make one Exabeam Smart Timeline™, which is automatically created for every user and entity.

Exabeam Smart Timelines reduce the time required to detect, investigate, and respond to security incidents.

2. Securonix use cases fail to cover the entire TDIR lifecycle

Securonix's standard use cases (Insider Threat and Cyber Threat Analysis) focus onthreat detection, dashboards, and reporting, and fail to cover thorough investigation and response.

Exabeam use case packages span the entire threat detection and incident response (TDIR) workflow and include detection rules and models, investigation and response checklists, and automated playbooks with pre-built checklists to guide consistency in response.

3. Securonix pricing passes on hidden search fees and slower query times

Securonix's bring-your-own data lake option allows customers to use their existing AWS/Snowflake instance; however, customers incur a per query fee of $5/TB scanned, which can add up fast with Securonix services like Autonomous Threat Sweep. To keep costs down, we've seen Securonix quoting zero-days of hot retention; this impacts search speeds significantly.

Exabeam offers transparent consumption pricing with no hidden fees passed on to customers; cloud archive provides low-cost long-term storage with rapid search capabilities.

4. Securonix white-labeling hides platform complexity prior to purchase

While Securonix claims they are working on a native security orchestration, automation, and response (SOAR), for the time being, they still white-label their SOAR capabilities from CyberSponse.

Exabeam Incident Responder Turnkey Playbooks™ maximize SOC efficiency, allowing even junior analysts to automate actions ensuring consistent investigation workflows.

	exabeam	Securonix
Metrics		
EPS	1M+	100K
# Integrations	549	180
# Pre-Built Detection Rules	1,800+	450
# Pre-Built Models	750	190
# MITRE Techniques	101	133
# Parsers	7,937	532

Conclusion

Securonix offers three cloud-native deployment models to meet data security and privacy requirements for a variety of customers. Their shared multi-tenant option is the most cost-effective, with only logical separation of customer data; this keeps costs low and allows MSSPs visibility across tenants. Securonix visualizes alerts in a way familiar to legacy SIEM/EDR users via individual alerts, allowing analysts to triage them using a familiar workflow. They also display violations by users ranked by risk, allowing investigators to use whichever workflow is more comfortable to them.

Exabeam provides customers with pre-built rules, timelines, and suggested guidelines for purpose-built security investigation to defend against the endless threats posed by attacks such as ransomware, phishing, and brute force attacks. We are leading the industry with solutions to help you constantly adapt to the evolving world of cyberthreats.

Whether it's compromised (or malicious) insider credentials abused by Lapsus$, zero-day attacks from nation states, or organized crime, Exabeam helps your team to keep up with the growing number of daily threats via our cloud-native solutions and security tactics focused on generating incident resolutions, consistently and repeatedly.

Exabeam offers cloud-native log management with long-term search of events and anomalies at the same speed as yesterday. Exabeam defined the business of UEBA in the market, and the Smart Timelines are key to pivot to MITRE use cases, cumulatively saving hundreds of hours of investigation per year. Exabeam builds enriched events — not just sorting logs — offering correlation rules that are easy to create without requiring expertise.

Exabeam makes it easy to automate alerting and escalation, with both internal case management and automation, as well as optional external incident response custom automation. Visualization is key. Exabeam makes it easy to see what's going on locally, in the cloud, and on people's endpoints.

Exabeam was built by security people for security people, a pioneer of the UEBA market and one of the world's most successful standalone security companies.

Get an Exabeam Fusion SIEM demo today, and think of us when it's time to renew!

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now