6 Ways Exabeam Delivers Better Security Outcomes Than Splunk

While no tool can prevent all attacks, some can detect intrusions and malicious activity better than others. Far too often, security information and event management (SIEM) solutions are challenging due to a lack of specialized expertise to customize and maintain the system. Add to this the astronomical cost to maintain and analyze all the logs that might help your teams discover what happened; when, where, and how; and which credentials were involved. Combating these challenges requires a system equipped with prepackaged rules, timelines, and suggested guidelines for purpose-built security investigation, to find the true gems of discovery amidst the noise of alerts.

Exabeam provides customers with this very set of tools to defend against the endless threats posed by attacks such as ransomware, phishing, and brute force attacks. We are leading the industry with tools 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.

There are a lot of SIEMs in the marketplace from which to choose. But how do you distinguish between Exabeam and solutions such as Splunk to find the right fit for your organization? Here are six reasons why Exabeam stands out as a superior SIEM choice:

1. Splunk is expensive

The cost of deploying a SIEM can be an expensive undertaking for any organization. Not only do you need to find the most cost-effective solution, but you need to quickly realize value and earn a return on investment. The cost of deploying and operating Splunk is significant, and many organizations are slow to realize true security value from its use.

Why not deploy a solution that uses automation to cut the time spent on security tasks by 51%? Through natural language querying, context-enhanced parsing, and data presentation, Exabeam improves analyst investigation efficiency and effectiveness — from collection to response. **See how much you can save with the Exabeam Fusion SIEM ROI calculator from Forrester Consulting.**

2. Splunk often requires ninjas, and they're unicorns – costly unicorns

The industry-wide shortage of cybersecurity professionals, coupled with the need for unique expertise, training, and customization to operate Splunk, creates a very complicated scenario. The constant need to demonstrate fast time to security value for tools and the people that operate them can make properly staffing your security team even more complicated.

Using Exabeam, your team can fully protect your systems without the need for large, expert-level staff or a specialized set of skills. This allows you to do more and protect your organization with fewer resources — working smarter, not harder. Let your would-be ninjas do actual threat hunting, rather than constant tool tinkering.

3. With Splunk, you need to know what to look for

At Exabeam, we say you can't fight what you can't see. Compromised credentials are associated with 80-90% of breaches, and almost always involve lateral movement (for which Splunk doesn't have prepackaged detections). Seeing lateral movement from device to device — let alone from device, to cloud, to on-premises resources — is nearly impossible without robust behavioral models and correlation rules.

At Splunk, user behavior analytics (UBA) is a disparate bolt-on product sold separately from their legacy SIEM — and lacks the refinement, detail, and visualization strengths of Exabeam Smart Timelines™. Splunk correlation rules are noisy, as well, with lots of irrelevant alerts to investigate. Tailoring the Splunk UBA to match your needs and environment? Well, see points 1 and 2.

4. Splunk stopped cloud-native innovation years ago

Splunk was successful because they solved the challenges of the legacy set of founding SIEM tools. They offered a better solution for search, correlation, and managing data at scale in an on-premises world. Splunk Cloud does not enjoy the benefits of a cloud-native architecture, including elasticity, fast engineering and releases, and remains slow to roll out new features, new connectors, and new log sources. The incumbent is ripe to be challenged.

As a Next-gen SIEM, Exabeam uses a behavior-based approach to threat detection, investigation, and response (TDIR). By aggregating all relevant events and weeding out the noise, Fusion SIEM is proven to boost analyst productivity and detect threats missed by other tools. This improves detection rates and response times, as well as team morale.

5. Splunk offers no easy path to advanced analytics, security visibility, or threat hunting capabilities

Exabeam delivers prepackaged correlations, integrations with hundreds of security tools and log sources, along with 1,900 rules and models, reports, and threat intelligence. **Focusing on high-value events, improving attack chain visibility, and use-case enrichment of events offer your team a focused, repeatable threat-hunting capability.**

6. Static correlation rules and limited threat behavior models are incomplete for effective threat detection

Splunk is a search tool and will seek for whatever you want to find. The problem is, you need to know what to look for — an improbable task with most zero-day attacks designed to evade detection methods based on correlation rules. Splunk offers a bunch of noisy correlation rules that generate expensive, irrelevant alerts while the true attacks go undetected.

With Advanced Analytics, Exabeam defines baseline normal activity for users and entities to detect deviations compared to that baseline, the baseline of a peer group, and the organization. Anomalies are placed into our machine-learning-based Smart Timelines to provide a full chronological picture of all associated events. Exabeam offers more than 1,900 models for anomalies, powering superior security risk management based on risk scores, timelines, and use cases — in a world where the first instance of any new behavior should be considered unusual. **All of this comes prepackaged. #NoNinjasRequired.**

	exabeam	Splunk
Detection Content		
Behavior-Based Models to Detect Abnormalities	750+ Behavioral Models	85+ Behavioral Models
Detection Rules to Detect Known Threats	1,800+	✓
Integrated Commercial-Grade Threat Intelligence	✓	Open Source
Detection Content Mapped to Use Cases	✓	X
Investigative Automation		
Automatically Generated Smart Timelines	✓	Query-Based Workflows
ML-Based Alert Prioritization	✓	Static Rule Severity Scoring
Pre-Built Watchlists for Risky Users and Entities	✓	Partial
Granular Risk Based Scoring	✓	X
Log Management		
Self-Service Data Collection Interface	✓	X
Search Query Builder Assistant	✓	X
Up to 10 Years of Searchable Data Without Rehydration	✓	X
Deployment Architecture		
Fully Cloud Native	✓	"Lift and Shift"
Multitenant	✓	✓
Integrated SIEM + UEBA + SOAR	✓	Must purchase UBA and Phantom – On-Prem Only

Conclusion

Splunk was not founded as a security company and never intended to provide security functionality. Splunk is, no argument, a fine tool for searching, sorting, and monitoring big data for many businesses. From application troubleshooting, to supply chains and distribution models, to moving goods, inventory, and other business intelligence functions, Splunk remains a good solution. But the truth is, Splunk was never built for security, and instead has relied on bolt-on features through their UBA and SOAR acquisitions. That's not a lot of security value for the money required to own and operate it. Isn't it time you got a great tool to Detect the Undetectable™? As important as cybersecurity is to an organization, doesn't it make sense to look for solutions and providers that are purpose-built for this critical area?

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