Replacing or Augmenting Splunk with Exabeam

Whether you've deployed Splunk and need to augment it or replace it, compare the outcomes for your security team

Splunk: Your Business Intelligence system? SIEM? Both?

Splunk Enterprise is a powerful generic data management, analysis, and visualization tool for big data. The fact is, it was never built with security in mind. The company launched itself as the IT Search Company, focused on IT troubleshooting providing, for the first time, a search mechanism for log data. Splunk has powerful search and data indexing capabilities, but the premise of Splunk — collect everything — is self-serving and defeating.

How many Splunk users currently avoid collecting certain data and telemetry into the system to avoid punitive license increases? We all know the answer to that question and wonder how much security-relevant data is getting missed? Given this, it must be asked if Splunk is the right security information and event management (SIEM) solution to power your Security Operations or Insider Threat teams? Can you afford to bring in the right logs to see a complete security picture across your ecosystem, and drive the strategic outcomes critical to protecting your organization?

Cybersecurity is too important to rely on a swiss army knife — you need a scalpel.

No tool can prevent all attacks. But some can detect intrusions and malicious activity better than others. This detection includes prescriptively bringing in the right data, organized for security use cases using a common information model, storing those logs for compliance, and using advanced and easy query and visualization capabilities to guide any team member to a result of what happened; when, where, and how; and which credentials were involved in events.

This brief will cover the specific needs for security operations where an organization uses Splunk Enterprise or Splunk Enterprise Security, and how teams can supplement or replace Splunk as the main tool if their needs for detecting and responding to credential compromises, insider threats, or zero-day attacks are not being met.

Splunk Enterprise - general purpose does not help the SOC

While Splunk Enterprise is a powerful general-purpose logging tool, there are limitations to using it as a SIEM both in security use cases and visualization. And it can be challenging to compete with the needs and demands of other Operations teams in terms of data sources, customization, and visualization needs. Here's some scenarios where people have found challenges using Splunk Enterprise in their SOC — and how Exabeam can help.

Splunk Enterprise is often "owned" by IT or operations teams outside of security, and there may be license or volume limitations which limit what kinds of logs come in and how long they are stored. This creates the first challenge for security analysts, summed up in a few questions:

- Are you able to bring in all the security logs needed for complete visibility, and that make your workflows complete? (I.e., can you see all authentication traffic wherever it occurs? Web SaaS or public cloud access logs? DLP? Endpoint?)
- Do you have compliance needs to store some kinds of logs for years, and the Splunk cost is prohibitively high?
- Is the hardware cost to run Splunk prohibitive (on-premises customers)? Are you able to see and judge the efficacy of parsing those logs to tell if you are getting all the data you need for queries, correlation rules, and future investigations?
- Are you having data volume issues with events flowing quickly into your operations center, and how long does it take to do each query?
- How many different tools are you currently needing to log into as part of an investigation?

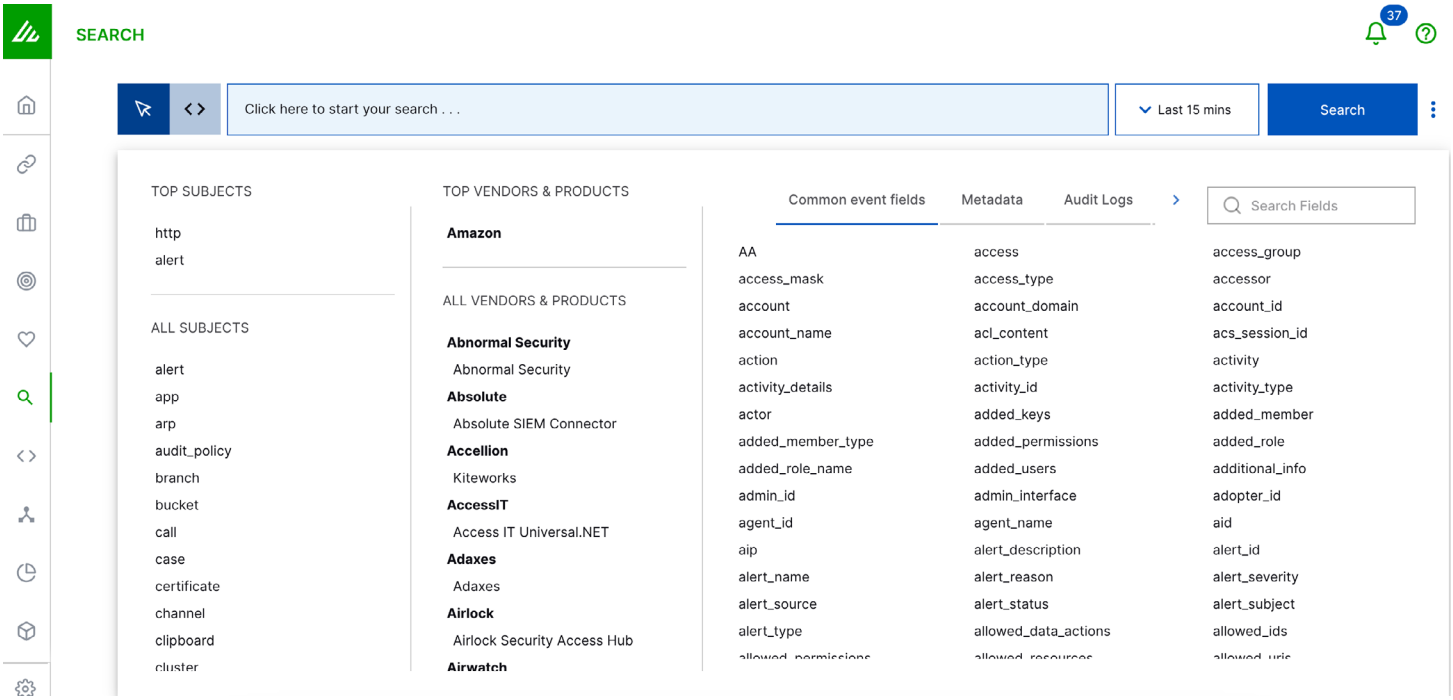
Security analysts and SOCs who have specific security needs can replace their Splunk Enterprise use for security with Exabeam Security Log Management or Exabeam SIEM — both purpose-built for security.

Exabeam Security Log Management can bring in logs from a variety of log sources including Splunk Enterprise, with cost-effective storage over long-term needs to meet Compliance requirements. Exabeam allows the mapping of use cases to data sources and shows use case coverage gaps. Bringing the right data helps not only manage costs but also provides actionability. We cost-effectively move your security logs into the same system, offering ease of Search and Correlation Rule building. Exabeam Log Stream makes it easy to bring in new log sources, then parses them using a Common Information Model that creates security events, allowing you to search for events across multiple log sources — from endpoint to AD. Exabeam can also help you eliminate noisy fields in your data that have no relevance to security outcomes. Exabeam enriches the logs with context data including third-party threat intelligence, offering a one-stop-shop for your SOC to see all their security events in one interface.

When Security doesn't own the Splunk implementation and has investigation tracking and escalation needs, there's Exabeam SIEM. Exabeam SIEM offers all the features of Exabeam Security Log Management, and adds Alert and Case Management for creating incidents and managing them through to completion. Whether your team is local or distributed, or needs Search exports to other tools like ServiceNow via API for automation, Exabeam can help you get the right data into the right hands quickly. And if a log source goes silent, troubleshooting via Log Stream makes things easy.

Exabeam is easy to use too — no Ninjas required. The Search function is a simple wizard with drop-down options prompted by the analyst typing. Once complete, a Search can be saved or even converted to a Correlation Rule. Finding and training analysts can be hard — Exabeam is working to make it easier and faster for new security analysts to do their jobs and find issues. The required experience or training needed of a security team shouldn't hold an organization hostage.

Figure 1.
Simple Search capability, showing common event fields, vendors, and subjects.



Fast Search, Correlation Rules, and Dashboards with Alert and Case Management provide security teams with the specific tools that Splunk Enterprise doesn't offer, as well as the compliance controls and speed of high-volume searches across the storage life of your logs.

Have Splunk as a SIEM, but still coming up short

Splunk Enterprise Security offers good legacy SIEM features, but has limitations in both implementation and constraints on the people operating it. The care and feeding of a Splunk Enterprise Security SIEM requires skills and resources that are harder to find and hire in the wild — and making your own Splunk Ninjas is an investment in human resource capital that you may not have time or budget to spare.

Other challenges include:

- Similar to the points above, for Splunk Enterprise, are you sure you're seeing all the right logs needed for your intended security outcomes and use cases?
- Resources for security teams are limited and those using Splunk are overwhelmed; who has the money or space for a specific Splunk expert when you can have a cross-functional person?
- Splunk Enterprise Security and Splunk UBA are separate logins — even with SSO enabled, they are still two distinct places a security operator needs to check and review for data and information. Integration is key.
- Seeing the relationship between the log coming into SIEM, the quality of the fields parsed, and how they support the use cases (e.g., malware, malicious insider, compromised credentials, etc.) has no closed circuit for improvement.
- Manual threat detection and especially investigations can take time and resources. Building a timeline requires ~300 queries in Splunk. Experts building the queries are not easy to find and typically quite expensive.

Still, sometimes you have reasons why you cannot simply replace the security log ingest from your Splunk Enterprise instance entirely. In those instances, and where you want to add the industry best-in-breed UEBA system, there is an option to take your current Splunk ES security data and port it entirely into Exabeam Fusion.

Exabeam Fusion is cloud-native with hyper-quick query performance, powerful behavioral analytics for next-level insights that other tools miss, and automation that changes the way your analysts do their jobs. Exabeam UEBA contains over 1,800 rules, including public cloud infrastructure security, with over 750 behavioral model histograms that automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. Exabeam Smart Timelines™ convey the complete history of an incident and highlight the risk associated with each event. These automated event enrichment and investigation features reduce manual tasks from alert triage to incident response across your defense in-depth stack — all in one interface.

Exabeam Outcomes Navigator offers the industry's first mapping of log sources to use cases and outcomes. This means that you can look at each phase of the MITRE ATT&CK™ framework, as well as against common use cases (malware, compromised credentials, malicious insiders). SOC leaders and engineers can look back at the log sources to judge their coverage against this common framework, as well as be directed back into Log Stream to make adjustments appropriate to bring logs to a higher Tier or completeness.

Exabeam Threat Intelligence Service is included with all products, bringing in third-party threat intelligence to enrich data with known indicators of compromise (IoCs) that add to risk scores when seen. Analysts can easily construct dashboards based on any outbound IoC activity, identifying potentially compromised entities and credentials at a glance — or create rules for automating responses and escalation via APIs or Incident Responder.

Splunk SOAR is an add-on that you need to purchase separately from Splunk Enterprise Security or Splunk UBA. Isn't it time for a fully integrated solution? Exabeam Fusion contains all three of these capabilities in one platform with role-based access controls. Serve the needs of your insider threat team and your SOC with a single solution.

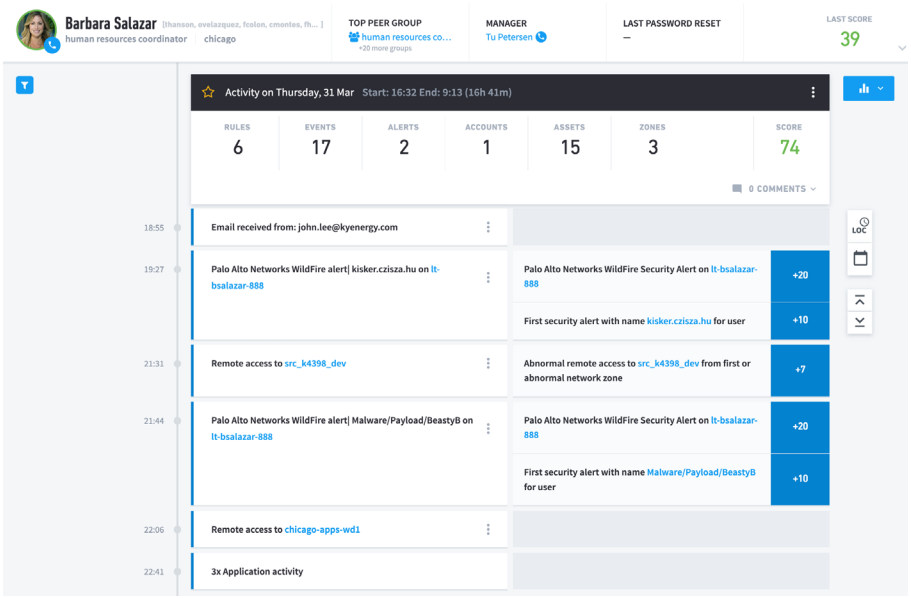


Figure 2.
Exabeam Smart Timeline showing how a malicious email caused a malware payload drop.

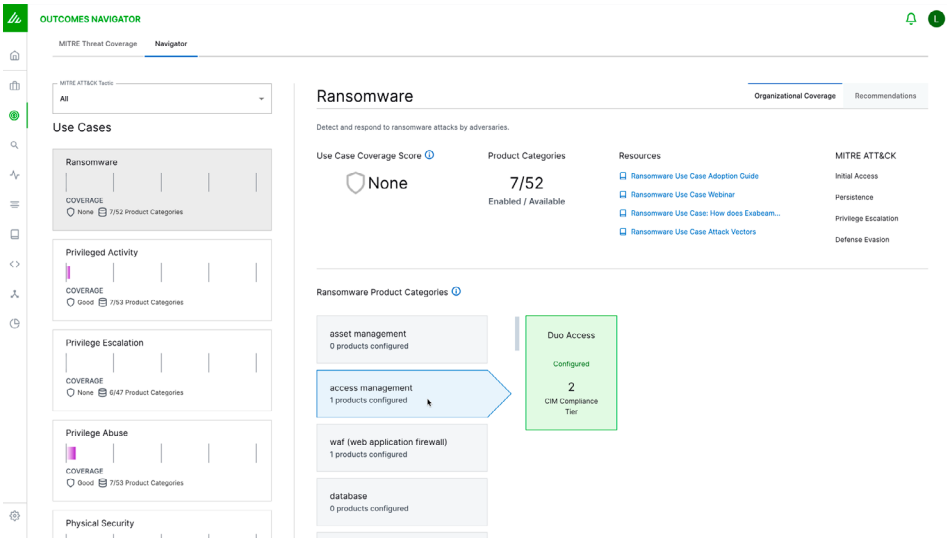


Figure 3.
Picture of Outcomes Navigator showing log sources that can indicate Ransomware, and the quality or Tier of the log source.

	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

Figure 4. Exabeam and Splunk comparison

Key capabilities

- **Ease of Search**
  - Analysts want an easy-to-use search capability that will allow them to filter down to the most important information.
  - Test your Splunk user today — how long does it take to create a query for any TOR endpoints accessed from your network or remote users?
- **Visualize what you Search for**
  - Quickly construct a centralized search dashboard with an easy-to-use interface that will display actual vendors
  - See all failed logins, denied multi-factor authentication, or other key incident indicators in visual format — and turn them into Correlation Rules
- **End-to-end log management**
  - Bring in new log sources fast to support your whole environment
  - See how the logs measure up against your coverage needs and SOC workflows
- **Easy Timelines for all Incidents**
  - Exabeam Fusion lets you see all associated events for every user and device on your network
  - Quickly identify where the risky activity was, quantify it, open cases, and resolve with prescriptive guidance from Exabeam
  - Case management and incident response — together

Next Steps

Organizations choose Exabeam Fusion over legacy Splunk installations to boost threat detection, investigation, and response (TDIR) capabilities with advanced UEBA technology to expedite processes, reduce their manual workloads, and align security with the company's business goals.

"We've strengthened our processes with workflows that have helped our team become far more effective as a result of the Exabeam partnership. Our team members can now ask the critical questions connecting security to business function." says a Cybersecurity Operations Manager at power network supplier who uses Exabeam software,

Reach out today for a discussion and demo on how Exabeam can augment your Splunk Enterprise installation — or replace it.

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 →