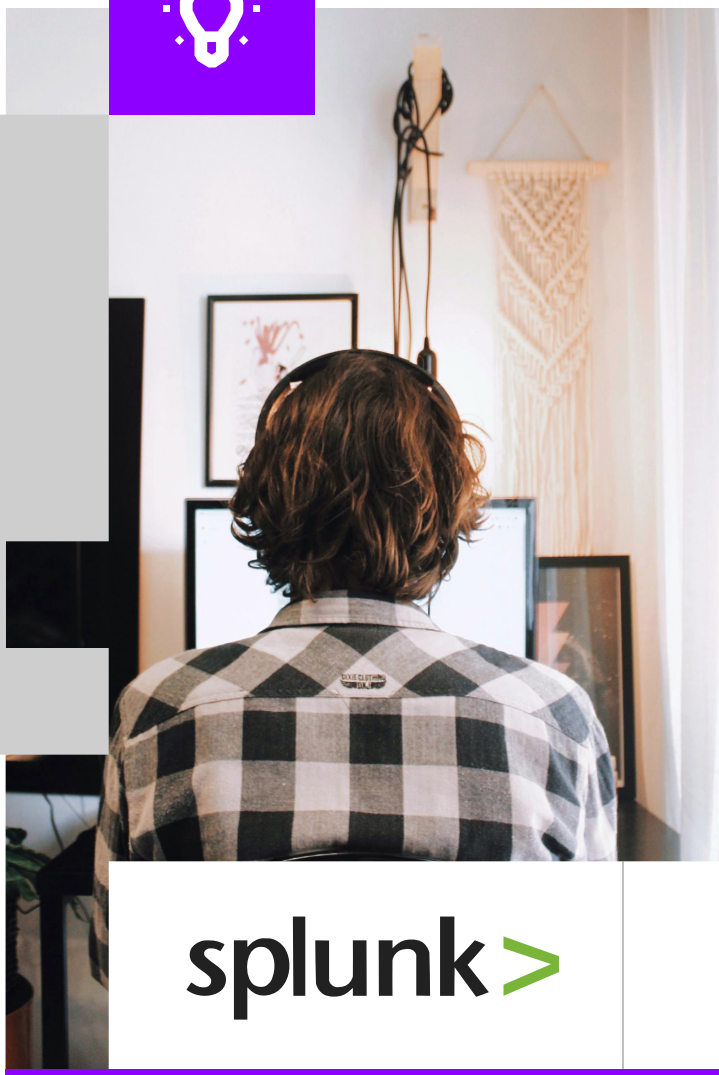
exabeam

Solution Brief

Augmenting Splunk with Exabeam

Improve Threat Detection, Enhance Cloud Security, and Reduce Incident Response Times



Security leaders are tasked with building world class programs capable of defending against both today's threats and tomorrow's attacks—all on a fixed budget. Unfortunately, traditional SIEMs like Splunk—while offering powerful data centralization capabilities—often require arcane query language knowledge, extensive customization and maintenance, and exhaustive analyst cycles to perform triage and investigation.

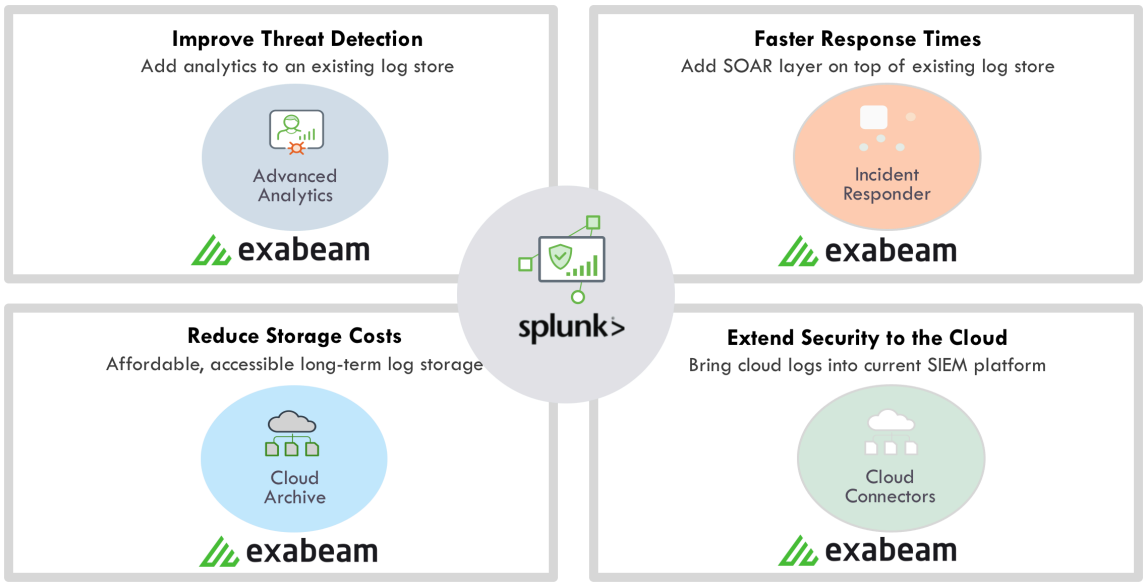
Exabeam solves these problems by augmenting Splunk's SIEM and log management solutions, enabling security teams to make the most out of their existing investment. Exabeam accomplishes this by deploying alongside and ingesting data from Splunk to provide joint customers with improved threat detection, enhanced visibility of cloud services, and reduced incident response times; all without needing to make architectural changes to their Splunk deployment.

"Exabeam helps organizations of all sizes make the most of their existing SIEM investment, this makes it a natural complement to any Splunk Deployment," Orion Cassetto, Director of Product Marketing at Exabeam.

splunk>

> Two years ago we began working with Exabeam and have seen the value it can bring to organizations using Splunk. I recommend any SIEM customer should at least take a look what's possible with the combination.

Oseloka Obiora
Director of Operations
RiverSafe



Four ways customers benefit by augmenting splunk deployments with exabeam.

Improve Threat Detection

A primary way that organizations look to enhance the capabilities of their existing Splunk deployment is by improving its ability to detect threats. Exabeam's threat detection is powered by user and entity behavior analytics (UEBA); which helps analysts find threats by learning user and machine activity, then automatically identifying risky, abnormal behavior. This comes in stark contrast to the SPL query and correlation rulebased approach employed by Splunk and Splunk ES.

Exabeam starts by ingesting and aggregating events and alerts—from Splunk, other data lakes, and directly from security point products themselves—into machine built timelines called Smart Timelines™. It then assigns risk scores to abnormal or anomalous activities within those timelines which may be indicative of threats or security incidents.

Exabeam Smart Timelines automate incident investigation by gathering evidence and assembling it in a chronological order that represents the scope and sequence of an event. Smart timelines contain both normal and abnormal behavior and follow attacks that move laterally to ensure that parts of complex attacks do not go unnoticed.

These timelines also help analysts prioritize incidents as they are automatically presented to analysts in order of highest risk to help focus analyst cycles where they matter most.

Finally, to proactively hunt for threats, Exabeam provides a simple point-and-click interface, which enables analysts to simply string together conditions from the available menus to make the search criteria which would be difficult or impossible to create with Splunk's SPL query language.

Quick Facts

Research by the Exabeam research team found that using Exabeam Smart Timelines can automate 1.7 Billion queries per year for every 5,000 employees at a company.

Achieve Faster Incident Response Times

Exabeam's Incident Responder, a security orchestration, automation, and response (SOAR) solution provides faster incident response as it provides hundreds of out-of-the box actions via pre-built service integrations. These actions can be run one-off or as part of playbooks. Response playbooks string together actions to automate containment, mitigation or response workflows.

In stark contrast to bolt-on SOAR solutions—which may effectively perform remediation, but lack the full scope of an attack— Incident Responder has native integration with Exabeam's behavior analytics solution to ensure full attack visibility. This is crucial for proper incident response, because the ability to detect an attack is a prerequisite to its resolution; automated or otherwise. Tight integration between Exabeam's behavior analytics and SOAR capabilities ensure that attacks aren't overlooked, no matter how complex or sprawling their nature; and that automated response can be effective.

Exabeam Smart Timelines further reduce response times by automating evidence gathering typically performed in early stages of response efforts. A study by the Exabeam research team found that each machine-built Smart Timeline can replace as many as 700 manual queries which would otherwise be required to obtain similar visibility.

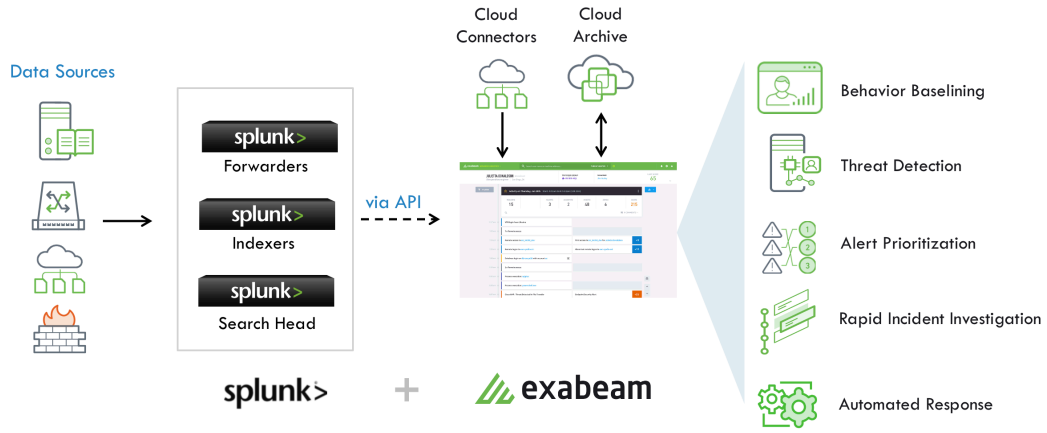
Bring the Cloud Solutions in Scope

Exabeam extends security to the cloud via Cloud Connectors which help organizations monitor activity taken in cloud services and cloud infrastructure providers. Cloud Connectors are pre-built connectors that enable security teams to easily collect logs from dozens of popular cloud services—such as AWS, GitHub, Google, Microsoft Office 365, Salesforce and many others. This allows enterprises to detect threats using behavior analytics on their cloud applications, along with extending any compliance-based security requirements to the cloud. Cloud Connectors automatically adapt to any API changes, so you can rest assured that the connector is always operating as intended.

Reduce Storage Costs

Exabeam Cloud Archive provides a low-cost, long term storage solution for log data. In many SIEMs, customers are provided two options: expensive hot data, or frozens offline storage. Each of these options has serious implications on user experience, as customers must choose between consuming large swathes of their security budget to keep data online in hot storage, suffer through painfully slow search times, or resurrect their data from offline storage repositories to make it accessible. With Cloud Archive, customers can retain months, years, or decades of data in an online, searchable format that can be researched in minutes.

Cloud Archive can be used alongside Splunk such that data ingested into Exabeam for threat detection can be automatically stored for future compliance and forensic needs. Furthermore, analysts no longer have to wait hours to obtain search results from NAS or other offline storage. Instead, analysts can easily search archived data at will using simple text search or the Lucene query syntax, and customize results with additional fields and filters.



A high-level overview of a splunk and exabeam integration.

How it Works

- Splunk acts as a centralized log management platform to ingest logs from disparate sources.
- Exabeam is configured to fetch logs along with historical data from Splunk via its API.
- Exabeam Cloud Connectors collect logs from cloud services (e.g. SFDC, Box, Google apps, etc.) and cloud infrastructure providers (e.g. AWS, GPC, Azure).
- Exabeam automatically synthesizes ingested data to baseline user and machine behavior into Smart Timelines. This helps to detect any deviation from the baseline.
- Exabeam detects threats associated with anomalous, high-risk behavior and automatically prioritizes them by risk score.
- Exabeam Smart Timelines automate incident investigation by gathering data and evidence and assembling it into an incident timeline. This obviates the need to query and pivot through raw logs in Splunk to create timelines.
- Response workflows are automated with SOAR, via pre-built connectors and response playbooks to lower mean time to respond (MTTR).
- Data is sent to Cloud Archive for long term storage, where it can remain online and accessible but in a cost effective manner.

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.