# Article information:

Elastic (ELK) Stack vs Splunk Enterprise 2023 | Gartner Peer Insights  
<https://www.gartner.com/reviews/market/security-information-event-management/compare/product/elastic-elk-stack-vs-splunk-enterprise>

# Article summary:

1. Elastic (ELK) Stack and Splunk Enterprise are both popular event management and security information tools.

2. Users appreciate the powerful capabilities of both tools, but some have criticized the support provided by Splunk Enterprise.

3. The article includes reviews from users in various markets, highlighting the strengths and weaknesses of each tool.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article compares Elastic (ELK) Stack and Splunk Enterprise, two popular tools for event management and security information. The comparison is based on user reviews from Gartner Peer Insights, which provides insights into the strengths and weaknesses of each tool.

One potential bias in the article is that it relies solely on user reviews, which may not be representative of the entire user base. Additionally, the article does not provide any context or background information about the tools, assuming that readers are already familiar with them.

The article also appears to be one-sided in favor of Elastic (ELK) Stack. While there are both favorable and critical reviews for both tools, the favorable reviews for Elastic (ELK) Stack are highlighted more prominently than those for Splunk Enterprise. This could suggest a promotional bias towards Elastic (ELK) Stack.

Furthermore, some claims made in the article are unsupported or lack evidence. For example, it is stated that Elastic SIEM is "the best and most open-source SIEMs," but no evidence is provided to support this claim. Similarly, it is claimed that Splunk support is lacking without any evidence to back up this assertion.

The article also misses some important points of consideration when comparing these tools. For example, it does not discuss pricing or licensing options for either tool, which could be a significant factor for organizations considering them.

Additionally, unexplored counterarguments or alternative perspectives are missing from the article. For instance, while users praise Elastic (ELK) Stack's flexibility and customization options, there may be concerns about its complexity and steep learning curve.

Overall, while the article provides some useful insights into user experiences with these tools, its potential biases and limitations should be taken into account when evaluating its conclusions.

# Topics for further research:

* Pricing and licensing options for Elastic (ELK) Stack and Splunk Enterprise
* Comparison of the learning curves for Elastic (ELK) Stack and Splunk Enterprise
* Features and capabilities of Elastic SIEM and how they compare to other SIEM solutions
* User experiences with Splunk support and how it compares to other support options
* Integration options for Elastic (ELK) Stack and Splunk Enterprise with other security and event management tools
* Comparison of the scalability and performance of Elastic (ELK) Stack and Splunk Enterprise in large enterprise environments.

# Report location:

<https://www.fullpicture.app/item/5bd315647c0a5d0a2f648a4274b8a260>