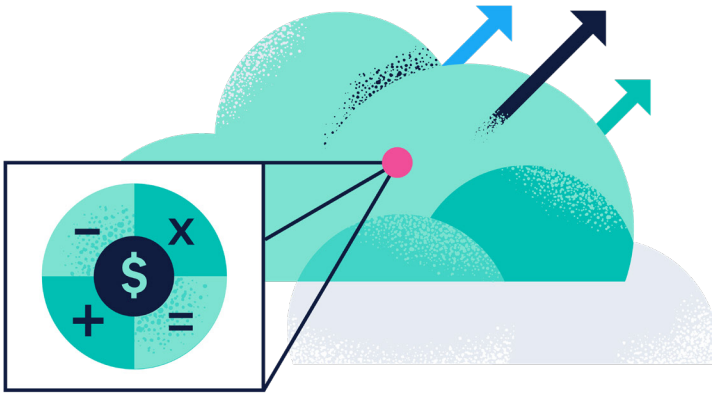
elastic | The Search Analytics Company



Cut your costs by migrating from Splunk to Elastic

How Elastic lowers your costs compared to Splunk

Elastic is the perfect solution for many challenges that Splunk customers are facing. Customers who migrated from Splunk to Elastic stated that Elastic lowers costs in the following ways:

Unified solution for observability & security with simple pricing

Elastic customers get comprehensive and powerful capabilities, including security and observability, in one integrated solution at lower cost. All your data resides in one highly resilient and scalable data lake. Our single resource-based pricing is simple and predictable while providing flexibility.

With Splunk, customers reported it was difficult to predict costs:

- Splunk has **fragmented solutions** (Splunk Enterprise Security, Observability, Splunk Cloud, etc.) for metrics, logs, traces, and security data, plus many disparate solutions from numerous acquisitions. Customers must buy different products with different pricing and pay extra to get capabilities close to Elastic.

 |

elastic

- Splunk requires Splunk Cloud for logs, and Splunk Observability Cloud for APM-based data. **Your data is separated across multiple products.**
- Splunk historically charged by ingested data. Customers' costs grew exponentially as logs grew. Now Splunk **offers 4 pricing structures:** workload pricing, ingest pricing, entity pricing, and activity-based pricing. While claimed to be "flexible", this is very confusing. It's hard to figure out which pricing is more economical, especially when both logging and security workloads scale fast.

Innovative AI capabilities enabling higher productivity

Elastic is a next-generation, performant, open and flexible search analytics platform, integrated with innovative AI capabilities without extra charge, including:

- **A new AI Assistant, leveraging generative AI**. This industry-leading AI Assistant uses LLM with Elastic's search capabilities, while leveraging your proprietary data, such as run-books, customer issues, and other internal contextual information. It enables:
  - Accelerated incident management and root cause analysis
  - Interactive exploration of problems and execution remedies
  - Context-aware, business-specific, and organization-specific output
- **Industry-leading machine learning** with 100+ built-in models, and the ability to bring your own, enables rapid time to insight and incident resolution.

Splunk's ML/AI capabilities are behind. Their AI Assistant is still in preview while Elastic had introduced our industry-leading AI Assistant last year. Customers who migrated to Elastic reported significant productivity improvements and MTTR reduction, which lowers TCO in addition to savings in licensing costs.

Superior performance on all your data at a lower cost

Elastic offers **low latency search across all data tiers**. All data in Elastic is normalized. Searches are real time in hot/warm tiers and near real time for cold/frozen tiers, without rehydration. As a comparison, Splunk's data is disjointed on legacy architecture, which may result in slow performance. Data in the "frozen" layer is not searchable, and needs to be rehydrated. Splunk Cloud Dynamic Data Active Archiving is slower at higher cost. All this in turn can make speedy queries more expensive.

Our new **piped query language**, **ES|QL**, **further enhances performance and lowers cost**. It provides a fast single method to interact with data in Elasticsearch, removing the costly need to transfer data to external systems for specialized processing.

Strong partnership focused on your time-to-value and overall success

Elastic builds long-term partnerships with customers. Our account teams are dedicated to customers' time-to-value and their overall success. Many of our customers who swapped out of Splunk stated that Splunk account teams were relatively unstable and less responsive. Issues in deployment and support are not resolved in time, therefore becoming costly.

 |

elastic

Significant Costs Reduction Proven by Customers

Because of the above reasons, **customers of various sizes and industries, with observability or security or both use cases, reported achieving significant TCO reductions migrating from Splunk to Elastic**. The following are a few examples:

A leading multinational telecommunication company gained significant business benefits at 30–50% lower cost

This customer moved off Splunk on-prem and implemented Elastic Observability platform for logging. The primary reason to migrate is the cost. The customer saw immediate 30-50% license cost reduction, saving millions of dollars a year. With more than 50,000 software builds, Elastic ingests 400TB of telemetry data per day, helping the customer to see what's occurring at the application layer all the way down through hardware.

In addition to much lower licensing costs, the customer especially likes Elastic's modern architecture with all data normalized. They found that Splunk's legacy architecture with disjoint data made it hard for them to quickly perform analytics on all data. They believe Elastic's ML/AI features are more advanced than Splunk, used for anomaly detection, APM, response time, etc. By year 3, they have gained the following benefits:

- 85% time identifying and resolving incidents
- 75% reduction in application deployment time
- 22,000%+ data analyst hours saved
- 3% increase in customer retention rate
- 25% reduction in customer support calls
- $1.2M savings from tool consolidation

These business benefits, in addition to lower licensing costs, further reduced TCO.

elastic

A leading American financial company cut cost by 49% per node and enabled $11M–$27M annual benefits after migration

This customer wanted to consolidate their observability tools to one vendor. Since their Splunk account team was viewed as not stable or responsive, while Elastic built a strong long-term partnership with them, the customer migrated their observability platform from Splunk on-prem to Elastic Cloud.

The customer projected an immediate 49% cost reduction per node. They believe the new observability implementation on Elastic Cloud is built for the future. The total annual benefits from leveraging the consistent orchestration, maintaining compliance certifications and the reduced risk of downtime, in addition to the infrastructure cost savings, added up to $11M in year 1, and is projected to be $27M in year 3.

A US data management leader cut costs by 50% and accelerated MTTR after consolidating observability and security solutions

With Elastic, this customer benefits from a single pane of glass for insights into their applications hosted in multiple regions and across their four cloud partners: AWS, Azure, Google Cloud, and Oracle. This has delivered efficiencies and cost savings that result from a single vendor relationship. The customer has reduced observability and security costs by 50% compared with Splunk and other solutions they were using before, including reduced costs from taking advantage of **Elastic Searchable Snapshots**. This enables them to retain data in a searchable form for 90 days while reducing dependency on expensive 'hot' storage.

The customer is now seeking added value from Elastic's leading generative AI features including **Elastic AI Assistant for observability**. This AI Assistant provides automated explanations for complex information, and improves troubleshooting processes, which boosts productivity and further lowers TCO.

