

# Looking for an Alternative to Splunk, Elasticsearch, Sumo Logic, or Datadog?



Consider Running Multiple Log Management Systems Instead

Let's start with a given: log collection and analysis is an increasingly essential function for enterprises across virtually every market. Strengthened security, enhanced productivity, and lower operating costs are just some of the benefits offered by log management solutions. Vendors like Splunk, Elastic, Sumo Logic, and Datadog have significant user bases.

That said, we're still in the early days of log management. And attractive alternatives are available. Users who are open to next-generation approaches have a greater opportunity to be rewarded with better price-performance, enhanced ROI, and greater benefits to the enterprise. It's not too early to make a change, but it can be too late. Preserving investment in traditional systems is not a good strategy if it means being locked into high costs and limited features that prevent organizations from adopting a "log everything" strategy.

Understandably, enterprise IT managers may have legitimate concerns about adopting a second log management solution, such as:

- investment in and familiarity with the current solution;
- uncertainty whether a new solution will perform as promised; and
- concern about the added cost of maintaining parallel solutions.

**“ We know we should be logging more, but we just can't afford it. We have to decide what we log. ”**

## Believe It or Not, You Can Lower Costs and Log More

Even as these questions are posed, managers should also consider the potential upside of replacing or supplementing their current log-management solutions: lowering the costs and expanding the use of logging.

The usage-based business model of traditional log-management solutions deters the use of logging on a scale that most enterprises want to or should perform. One of the most common complaints we hear is: “We know we should be logging more, but we just can't afford it. We have to decide what we log.”

So, if there were an option to reduce the cost of logging, enterprises would have a reason to expand their collection and analysis of log data, thus reaping more benefits across a widening range of use cases.

## Enter Humio: Enterprises Can Log Everything

Such an option exists in Humio, which provides the two most important elements that allow enterprises to “log everything” – a flat-rate pricing model and scalable performance capable of supporting the largest and most challenging log-collection environments.

Humio provides a modern approach to log management that delivers significant benefits to customers. Managers and end-users of logging workloads should ask themselves and their colleagues three key questions:

1. Are we placing any limits on the volume of logs we collect because of costs?
2. Are there places in our organization where we would like to start collecting logs but have not done so because of costs?
3. Is it likely that future growth in the volume of logs to be collected will bump up against budget limitations, causing us to place limits on the volume of logs we collect?

If the answer to any of these questions is yes, then it is important to select a new log-management system that will:

- not impose any cost penalties for collecting as much data as you want or need;
- allow you to add new applications and use cases for log collection;
- scale cost-effectively to accommodate all future log-collection requirements; and
- not impose additional financial or resource burdens on the IT organization.

Humio meets all four of those requirements.

## The Best Way To Start With a Humio Solution

Why start with a Humio solution, either in parallel with a traditional platform or as a replacement for one? See if you recognize any or all of these situations:

- A desire or need to begin log collection in a new part of the organization. For example, if your DevOps team is adopting containerization or a cloud native approach; or if some of your IT systems are not currently monitored for threats.

- Instances in the recent past where a proposal for increasing log collection was turned down because of a forecast rise in costs. (Ask Humio for a comparative TCO analysis.)
- Use cases where observability is the essential requirement, rather than task-specific analytic tools.
- You foresee a time where log-management requirements (in terms of volume, cost, or both) will exceed your organization's ability to pay for it and/or manage it with existing staff.

Now, it's perfectly understandable that IT managers might feel overwhelmed at the thought of ripping out an existing system and replacing it with an entirely new one. But that isn't necessary. Humio's ease of deployment and management means it can be installed alongside an existing solution. Enterprises can keep using what they are comfortable with, and either add new applications on the Humio platform or gradually transition current workloads onto it.

### Next Steps: Timing Your Move

The final question to be asked in the process of evaluating a parallel or replacement solution concerns timing. Should you replace your traditional solution right now, immediately cutting costs and increasing the volume of logs collected? Or, do you feel more comfortable trying a new solution in an isolated test bed, where staff can become familiar with how the new solution works? Or, should you revisit your entire logging strategy to determine if a commitment to "log everything" is the right approach for your enterprise?

Each of these is a valid approach, and the answer depends on many factors unique to your organization. Contact Humio to engage with experienced professionals who can help you determine the best strategy.

#### **Schedule a Demo**

To schedule a private demonstration, visit [humio.com/request-demo](https://humio.com/request-demo).

#### **About Humio**

Humio is a real-time observability solution for DevOps, ITOps, and Security Professionals focused on changing the way users view all data across entire complex, distributed systems.

The platform empowers teams to log all their data to gain instant visibility into their entire system and instantly identify and address concerns or vulnerabilities in a complex computing environment.

