Splunk

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Splunk

Read 58 reviews of Splunk

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

Foundation Technology Specialist at a insurance company with 1,001-5,000 employees

it_user635271

HOW HAS IT HELPED MY ORGANIZATION?

MTTR is drastically reduced, because the developers and other IT support staff have instant access to log events. People costs are saved by not having to involve the domain developers from multiple teams, when tracing a problem that spans multiple platforms. Security is improved by not having to give as many people access to log on to the servers.

WHAT IS MOST VALUABLE?

The ability to rapidly diagnose problems in production and non-production, across hundreds of log files, is the most valuable feature.

WHAT NEEDS IMPROVEMENT?

Official training, even CBT, is expensive so not many people are able to get certified. This leads/causes the users to make use of the most basic functionality only. It is a challenge to manage the environment in such a way, that one's log, even with the bandwidth license, isn't exceeded. Splunk has moved towards not applying hard caps in data ingestion, and this will help us in the future. However, I'd like an easier way to flag certain source log files as non-critical and have Splunk automatically disable those event sources when the license capacity exceeds an arbitrary value.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

There were no stability issues.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

There were no scalability issues.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Customer Service:
I haven't had the need to log any critical issues. Most of my support tickets have been revolved around configuration questions. I'm very happy with the way Splunk's support staff respond - they're pretty helpful. I think I've only had one situation where the response was acceptable, but not stellar. Technical Support:
The technical support is good. I'm sometimes surprised when the support engineer doesn't immediately know the answer to my questions (as I feel they must be fairly common queries). But, this can probably be excused because of the breath of features Splunk Enterprise has.

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

We were not using any other solution previously. I evaluated ELK Stack but at the time, Splunk offered more flexibility, better support and was easier for us to implement.

HOW WAS THE INITIAL SETUP?

Initial setup was fairly straightforward, but we used an experienced implementation partner and ensured that our team was intimately involved in the installation/configuration process on a technical level.

WHAT ABOUT THE IMPLEMENTATION TEAM?

We used a combintation of in-house (ie. myself) and an experienced Splunk partner.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

The product has a lot of value, and I feel that we're getting the value that we're paying for. Splunk Enterprise becomes extremely expensive after the 20GB/month license, but if you take care of what you log, i.e., by not logging excessive application events, then that license will get you a long way.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We looked at ELK Stack.

WHAT OTHER ADVICE DO I HAVE?

Use an experienced Splunk architect to design your infrastructure configuration. Ensure that your tech leads are intimately involved and understand exactly how the product fits together. Manage your Splunk configuration in a repository (Git). Educate the end users as quickly as possible to use the tool effectively. Change practices and encourage staff to use Splunk instead of old ways of getting the data they need. Prevent, or limit, direct access to the servers or server log files if you can.

Learn more: Read 58 reviews of Splunk