



Palo Alto Networks Traps

Review From A Customer



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

Review by a Real User

Verified by IT Central Station



Security Consultant at a tech services company with 51-200 employees

ConsulSec67

WHAT IS MOST VALUABLE?

I've found the security protection modules there, have been the most valuable.

WHAT NEEDS IMPROVEMENT?

I started using it from 4.1, but it didn't change that much. Some features and some fixes have been added to 4.2, but not that much. They need to improve reporting, the end-point reporting. They could also enhance their notification statuses. In the current version, you will see some threat alerts, or if anything is executable, but you will not see behavioral analysis. You will see what was being blocked, and that's it. If Traps logs something, you will get a notification. Otherwise, you have to generate the dump file and investigate on your own. In the next release, I would like to see more UI improvements. Their UI is a bit basic. When we are speaking about Palo Alto Networks they are a big company, so they can surely improve the UI a little bit. The UI, the reports, the log system can all be improved. But overall, when we speak about security and protection, they are one of the top providers.

FOR HOW LONG HAVE I USED THE SOLUTION?

I've been using the solution for six months.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's very stable. I've never experienced downtime for the ASM console or ASM core. But we experienced this for the database, and it was not clear in Trap's interface. So, Trap's server stopped working, stopped getting jobs, stopped the enforcing policies because the database was full. We did not get any alert for that, so you will not see any alert on the ESM console that says that your database is about to fill up. It was not reachable and there was no warning or indication for this. You have to go to some tools internally and check in the command line, to see. You will see some errors for the DB, and you will realize that it's a DB issue. I've never experienced any issue with the Traps itself, but with the database.



Palo Alto Networks Traps

[Read 12 reviews of Palo Alto Networks Traps](#)

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

It's very easy to scale if you have file availability. If it's more clear, we can do high availability, but it's a bit tricky. We deployed this for 4,000 endpoints, and it was very easy. Two ASM core servers were enough to deploy it for 4,000 plus endpoints. These are enterprises, not SMBs. They're government institutions.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

I would not say that technical support is bad, but it's not that good. It could be better. Basically, they don't provide customer support tools just to investigate the logs. From a reseller or authorized center for Palo Alto, I can't get that much information from the logs because it's a bit complicated. If they have support tools, for example, to analyze the logs as they have for the Palo Alto firewall. They don't have for this for Traps. They need to have some tools to analyze the logs. We can generate something called tech support files from Traps, but it's useless. Nothing's there. You will not get that much from the tech support file. But for the firewall, if we get the tech support file and upload it to somewhere they have some tools, we can get many useful logs and alerts. For Traps, this is not possible.

HOW WAS THE INITIAL SETUP?

The initial setup was straightforward. They are using MySQL database, and I think it's a disadvantage because you need to buy a license for MySQL also to deploy it. They don't have this concept of file availability between DS and core servers.

WHAT ABOUT THE IMPLEMENTATION TEAM?

We are a reseller. We are implementing it on customer premises for our clients.

WHAT OTHER ADVICE DO I HAVE?

The main advice I can share is to watch out for your database and make sure to give it enough resources. That's it. I would rate this solution eight out of 10.

Learn more: [Read 12 reviews of Palo Alto Networks Traps](#)