MICRO FOCUS

ArcSight

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

ArcSight

Read 9 reviews of ArcSight

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

Review by a Real User

Verified by IT Central Station

Manager at a financial services firm with 1,001-5,000 employees

it_user597603

WHAT IS MOST VALUABLE?

Event correlation across multiple device categories: It allows us to have a full picture of what is happening in the environment. Flexible event collection: Besides hundreds of standard devices, you can send custom CEF Syslog prepared with your own scripts. Customization of alerts: Velocity macros allows you to send very clear and user-friendly alerts.

HOW HAS IT HELPED MY ORGANIZATION?

This product gave us a clear picture of the network traffic, including the useless parts. It also allowed us to detect a large range of threats, starting from the malware infected workstations to misconfigured devices.

WHAT NEEDS IMPROVEMENT?

The web console should have all the features of the standard console. In addition, the upgrade process should be simpler.

FOR HOW LONG HAVE I USED THE SOLUTION?

I have used this solution for 10 years and 8 months.

WHAT WAS MY EXPERIENCE WITH DEPLOYMENT OF THE SOLUTION?

I did have some small issues at the beginning. It was mostly due to not reading the documentation or sending too many events in the HPE ESM solution.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

Scalability was not an issue. The environment was relatively stable and we filtered out non-security events using custom scripts.

ArcSight

Read 9 reviews of ArcSight

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

I have had mixed experiences over the years. Customer service was good, while the technical support was mostly great. There were a few glitches, like assigning our trouble ticket to a support specialist in an impossible time zone.

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

I have not used any other solution. In 2005, we started directly with the HPE ArcSight solution because our company security consultant recommended it.

HOW WAS THE INITIAL SETUP?

In 2006, when we first installed HPE ArcSight into production, we disabled most of the default rules and other object categories. Today, this may not apply. After which, we designed and implemented our own rules, filters, field sets, active lists, session lists, reports, alerts, etc. The first year was hard. In the following years, we mainly did the fine tuning, added new event categories and also did a lot of updates/upgrades.

WHAT ABOUT THE IMPLEMENTATION TEAM?

We carried out a pilot implementation based on the initial SOW, including several basic use cases. This allowed us to understand what is really happening in the environment and we learned that most of the default rules are not appropriate for us. After the pilot was successful, we bought the solution.

WHAT WAS OUR ROI?

Calculating ROI is tricky and was never a concern for us. The simple fact that HPE ArcSight helped us several times to survive malware attacks (Conficker was one such attack) and it also helped a lot with different compliance audits, which was enough for us.

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

In order to avoid huge licensing costs, you should use pre-filtering of events, outside the ArcSight solution. We did this for Cisco ASA firewalls, Microsoft TMG proxies, etc. Of course, this approach may not work, if you have regulatory constraints and have to collect everything.

WHAT OTHER ADVICE DO I HAVE?

You must understand your environment and its dynamics. Talk with IT people, write down the most important use cases, shortlist at least three SIEM solutions, do several pilots and then choose well.