Fidelis Elevate

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Fidelis Elevate

Read 2 reviews of Fidelis Elevate

Review by a Real User

Verified by IT Central Station

IT Security Coordinator at a healthcare company with 1,001-5,000 employees

ITSecuri7cfd

WHAT IS OUR PRIMARY USE CASE?

It is used as our primary in-line IDS/IPS system, replacing FireEye NX. It catches more, looks at more ports than Fireeye NX, and is a scalable appliance, unlike our NX which was saturated and shut itself down.

HOW HAS IT HELPED MY ORGANIZATION?

Increased our ability to stop malware before it hits workstations. That ability increased by 200% due to the number of ports it monitors, over the FireEye NX product. It has also improved our hunt ability with quick search tools, to zone in on malware or other anomalies. It is able to link items to incidents from other consoles, and works natively with the SIEM.

WHAT IS MOST VALUABLE?

IPS and reporting. It catches more inline than the FireEye NX even looked at. It has a rating system now so you can rate things up or down, depending on your environment. This means alerting can be customized, yet still pick up anomalies. Reporting has been great and it is easy to do a quick search through 45 days of data for something of interest.

WHAT NEEDS IMPROVEMENT?

Update: The interface bug issue hasn't happened in last three months. This may be solved now, we hope. Support seems better.

FOR HOW LONG HAVE I USED THE SOLUTION?

Four years

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

There was a bug issue for more than a year, but seems resolved with last patch, last reboot occured over 3 months ago.

Fidelis Elevate

Read 2 reviews of Fidelis Elevate

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

No issues with scalability. In fact, we've added a datacenter, purchased new gear, and scaled out two more units for the active/standby site to take over the load, should a DR be required.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Tech support is competent, usually responds within a few hours, can escalate anything urgent to technical account rep for immediate handling.

IF YOU PREVIOUSLY USED A DIFFERENT SOLUTION, WHICH ONE DID YOU USE AND WHY DID YOU SWITCH?

We used a different solution. We switched due to flexibility, expandability, and cost. Limitation in old hardware appliance would not scale without major costs.

HOW WAS THE INITIAL SETUP?

A breeze. After rack and stack, devices were up and running base configurations within two hours. As with any IPS, tuning is required to stop false positives. This is no different, but the ease of use of the interface allowed my team to start making adjustments within a few hours. With the latest version this is even easier, given the new rating system. You can tweak your environment on the fly, as your ops look at alerts to lower thresholds, raise them, or reduce false positives.

WHAT ABOUT THE IMPLEMENTATION TEAM?

we always use 1 of 2 partner implementer. I rate our partner a 9/10.

WHAT WAS OUR ROI?

More visibility at the north-south network layer, automation of security event/incident handling.

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

Company came from government space. You license by the number of days of logs you need to maintain visibility for. Forty-five days is a good solid number for a company with around a 10k user base.

WHICH OTHER SOLUTIONS DID I EVALUATE?

Tipping Point, Cisco

WHAT OTHER ADVICE DO I HAVE?

The product itself works fine, support is pretty good.

Read 2 reviews of Fidelis Elevate