IT Central Station
Unbiased reviews from the tech community

Case Study

Vectra AI

VECTRA

reviewer1444719

Project Manager at a university with 1,001-5,000 employees

✓ Review by a Real User

✓ Verified by IT Central Station

What is our primary use case?

We use it to monitor what is happening on our network, especially to protect our network from malicious activity.

We also have the sensor into Office 365, so we can also monitor everything that is happening in there.

At the moment, we use it to monitor all our endpoints.

How has it helped my organization?

The solution's Privileged Account Analytics for detecting issues with privileged accounts is critical for our organization. Because of risk, we scan our entire network. We have a lot of segmented networks where clients can almost do nothing. If we just look into everything, then sometimes there is a bit of noise. When you select your privileged hosts or accounts, you can see how many things are left over and which are the most critical that need to be solved as soon as possible.

It notifies us if our Office 365 has been compromised. Even after business hours, I get personal emails. This is a temporary solution because we are working doing repetitive alerting, but that's a work in process. We are working on an integration with our authentication system that will be able to detect an account or device. We want to automate that process so the account will be locked out for a period of time.

Vectra is a detection system on top of our protection system. We do a lot of protection on our network, but that protection is a configuration based on human interaction, where there can also be human faults or errors in the system.

The solution captures network metadata at scale and enriches it with security information, e.g., we have sensors for Symantec antivirus and our virtual infrastructure. We are looking into extra sensors for enabling some things from Microsoft Defender. We integrated it into our Active Directory so we can do some user correlations, etc. It enriches the metadata on hosts and accounts, but that is mainly informative. It is good for us when making a final decision about some detections.

It has helped us to organize our security. We get a better overview on what is happening on the network, which has helped us get quicker responses to users. If we see malicious activity, then we can quickly take action on it. Previously, we weren't getting an overview as fast as we are now, so we can now provide a quicker response.

The visibility is much greater because of the behavior analysis and details that sometimes we have to put into it. On the firewall that we already have, sometimes we do manual lookups and check if everything is okay, then do research into it. Now, we put less effort into trying to manually do things to ensure that we have a good security model. We can see more how behavior changes with time, but that also requires us to put more time into the solution.

The solution gives us a baseline for users and their behaviors. We are able to establish which users have risky behaviors, then reach out to them and recommend better ways of doing things.

What is most valuable?

The hosts are critical hosts, which are really good when used to look up things as fast as you can because these could be very risky situations. Furthermore, within detections, we try to clean up a lot of things that are low in priority. It is same thing for the accounts within Office 365: Everything that is critical has to be solved as fast as possible.

The triaging is very interesting because we can do more with less work. We have more visibility, without too many false positives. It is a work in process because there are a lot of clients in the network, and everything has to be researched to see if it is valid, but most alerts and detections are solved with a bit of triaging.

The interface is very intuitive and easy to use. It gives a good overview, and it is important to understand what is happening on the network.

The integration within our virtualization infrastructure allows us to see the traffic that is going between virtual machines, even within our host. That gives us a lot more insights.

What needs improvement?

The solution’s ability to reduce false positives and help you focus on the highest-risk threats is mostly good. It is still a bit of work in process, but I can give feedback to the company from the help desk. There is follow-up from the Vectra team who follows it closely. We can also give a lot of inputs to make it still a better product. It's already a very good product, but in comparison with a lot of systems I used in the past, the false positives are really a burden because they are taking a lot of time at this moment.

The Office 365 integration is still a pretty new feature. I also have seen some improvements, and they email us with every step in the improvement process. I think that this integration will grow.

Every area has room from improvement. Security is an ongoing process. It is important for Vectra to keep updating their system based on new behaviors.

We would like to see the combination of the cloud with on-premise, e.g., what's happening in the cloud versus what's happening in the on-premise situation. If there is a phishing mail in the cloud, then the phishing mail comes in and a colleague clicks on that mail. Normally, it would be blocked by the system. However, when it's not blocked, then there can be malware on the system locally. We think it's important to get the integration of what's happening on Office 365 with phishing mails.

Sometimes, it is a bit noisy on the dashboard because all the systems are on one field. On the dashboard, we have a complete overview of high, medium, and low risks. However, it would be more interesting for us if they could split that dashboard into high, medium, and low devices. For example, there is a dashboard on a device with a complete overview specifically for high-risk.

For how long have I used the solution?

It has been operational for a few months.

What do I think about the stability of the solution?

It runs very smoothly. It is stable.

We haven't had any issues in regards to the stability or performance. The interface works very quickly. There is no latency on the traffic.

What do I think about the scalability of the solution?

It scales well.

For end users, we have about 10,00. On the administrative side, there are five to 10 system admins who use the information from the system for configuration and monitoring tasks.

How are customer service and technical support?

The technical support is very good with fast responses. They reach out if they see there might be more questions. So, if you have a simple question, it could be that they elevate it to a more complex question to see what you really mean.

Seeing all the malware reaching out to CMC services from within our network, we reach out to those people via the help desk, and tell them, "Maybe you can scan this or that because those systems are managed by us." We get a lot of thanks from those people, which are often saying, "I did have some strange behavior on our systems, but I didn't know what it was. I wasn't doing anything about it, but thank you. It helps when you scan it, and the system is running better at the moment." In a completely unmanaged network with a lot of devices bring your own devices), it helps everybody.

The way that we can work with support to add feature requests is very interesting because it is an evolving world.

Which solution did I use previously and why did I switch?

We didn't have a solution like Vectra previously.

How was the initial setup?

The initial setup was completely straightforward. I didn't need any help. They delivered the device within the first weeks of COVID-19. The system is preconfigured from Vectra. I placed it in the server home, configured the network, and moved the Internet traffic out of the mailboxes, then I put it onto network so it was visible. In 30 minutes to an hour, everything was running.

What was our ROI?

We can sleep better.

As long as there is no full cycle attack, we will earn our money back.

Efficiency increased. There is less technical work to be done to ensure that nothing is happening from threats. Now, the system gives us the transparency that we need.

The solution has reduced the time it takes us to respond to attacks. In the past, it was difficult to know if something was happening because we didn't have an overview. Now, we know it very quickly because we have an overview of what is happening.

What's my experience with pricing, setup cost, and licensing?

The pricing is high.

Darktrace was also pricey.

Which other solutions did I evaluate?

We also evaluated Darktrace. We made a decision to stop testing Darktrace very early on, so it is difficult to compare to Vectra.

We chose Vectra because of the solution's simplicity; it is more straightforward. Also, we liked Vectra's support, visibility, and implementation. The solution comes to a conclusion within Vectra about some detections. It was easier to find the technical details which were interesting without looking too deep. The correlation was good too. At the end of the proof of a concept, Vectra added some extra features. However, for finding the way into the system, it took us a lot more time.

We found that Vectra enables us to answer investigative questions that other solutions are unable to address. They provide a checklist regarding what we can do about detections. Because of this visibility, we don't have to do more investigations.

We have other systems, like Office 365, which do behavior analysis and some signature behavior analysis. However, Vectra does not gives that many false positives in comparison with other solutions. Also, we are now able to see the entire network and cloud.

What other advice do I have?

If you are looking into this type of solution and have the money, then you certainly need to look into Vectra.

The campaigns are interesting when looking at the beginning of a campaign. The scope of false positives is a real issue in a network that continuously has a lot of new hosts, but we can cope with it. We have given some feedback to the help desk regarding coping with this matter.

We hope that we can keep it so we don't see a complete lifecycle of an attack.

We are planning to use more features of the solution in the future, e.g., automation. We also want to integrate it with more advanced client security features.

I would rate this solution as an eight of 10. There is still a lot of development going on with it.

Which deployment model are you using for this solution?

On-premises

Read 12 reviews of Vectra AI

See All Reviews