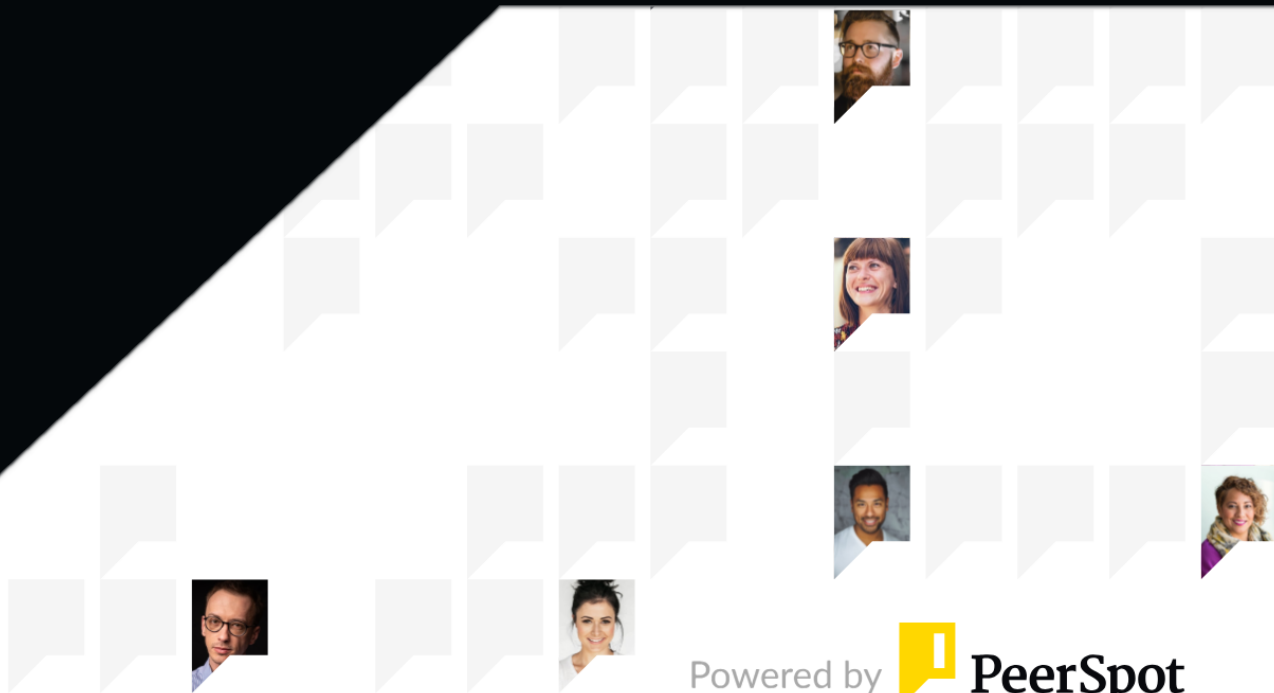




Vectra AI

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 11

Other Solutions Considered..... 12 - 14

ROI..... 15 - 17

Use Case..... 18 - 21

Setup..... 22 - 25

Customer Service and Support..... 26 - 27

Other Advice..... 28 - 31

Trends..... 32 - 33

About PeerSpot..... 34 - 35

Product Recap



Vectra AI

Vectra AI Recap

Vectra AI delivers hybrid network and identity security that stops advanced threats others miss. Unlike traditional NDR or IDPS tools, Vectra is purpose-built for the modern AI-enabled enterprise where attacks move laterally, exploit stolen credentials, and evade agent-based controls.

The Vectra platform uses AI-driven behavioral detection and real-time correlation of attack signals across network, cloud, and identity layers. This gives security teams visibility where EDR and SIEMs fall short, enabling faster, more confident decisions with fewer resources.

Why security leaders choose Vectra AI:

- Continuous observability across hybrid environments spanning data center, cloud, SaaS, and OT
- AI-powered Attack Signal Intelligence that filters noise and surfaces true threats in minutes
- Automated SOC workflows that reduce manual triage and analyst fatigue

What makes Vectra different

- Proactive protection with AI: Vectra provides real-time, AI-driven observability across hybrid environments, enabling security teams to see emerging threats before they become incidents.
- Preemptive detection and response: By correlating signals across network, cloud, and identity, Vectra uncovers stealthy lateral movement, credential misuse, and privilege escalation attempts before damage occurs.
- Automated SOC operations: Vectra automates triage, investigation, and reporting, transforming SOC workflows from manual and reactive to efficient and intelligent — reducing time to respond and freeing analysts for higher-impact work.
- AI with context: Our Attack Signal Intelligence filters noise and delivers high-fidelity alerts, accelerating detection while eliminating alert fatigue.
- Built for hybrid complexity: Vectra thrives in environments that challenge other tools — encrypted traffic, unmanaged assets, cloud services, and identity systems.
- Measurable resilience, not alert noise: Vectra equips SOC teams to outpace adversaries, reduce reliance on manual processes, and drive measurable improvements in MTTD, MTTR, and analyst efficiency.

Industry recognition

- Named a Leader in the 2025 Gartner Magic Quadrant for Network Detection and Response
- The only vendor recognized as Customers' Choice in the 2024 Gartner Peer Insights for NDR
- Winner of Best Behavioral Analytics at the SC Awards Europe
- Cited in GigaOm, SPARK Matrix, and other analyst reports for technical strength and customer satisfaction

Get the [Vectra AI Buyer's Guide](#) and find out what your peers are saying about Vectra AI, Fortinet FortiGate, CrowdStrike Falcon and more!

For more information, visit www.vectra.ai.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Vectra AI has positively impacted my organization; last year while using it, we received many malicious email threats and virus incidents, including a trojan virus that had reportedly been deployed by someone, and our company used Vectra AI to detect the malicious threats and viruses before they could cause more damage, and we successfully stopped the threats.”



Rahul Reddy

Consultant at a retailer with 5,001-10,000 employees

- ✓ “Attack Signal Intelligence helped reduce irrelevant alerts by 80% to 90%, with metrics showing a 100-plus reduction in investigation workloads and roughly saving about 55,000 hours of investigation time.”



Verified user

Strategic RAN Lead | Network Transformation & Optimization | Philippines & South Africa at a tech vendor with 10,001+ employees

- ✓ “The intuitive dashboards are incredibly useful, with both the Quadrant UX and the Respond UX, so whether looking from a management point of view or an analyst point of view, both dashboards are very intuitive.”



Drystan Govender

CTO at Cyber Retaliator Solutions



“There are many detection features available.”



Mohammad Alkurdi

Owner at Fortibits



“Using this tool for automation has provided more benefits to our processes.”



Nawaf Fawaz

Planning& Performance Analyst at National Information Center, Ministry of Interior, Saudi Arabia



“The most useful feature is the anomaly detection because it's not signature-based. It picks up the initial part of any attack, like the recon and those aspects of the kill chain, very well.”



Verified user

Sr. Specialist - Enterprise Security at a mining and metals company with 5,001-10,000 employees



“The packet-capturing feature is very useful.”



Naveen Hariharan Vijaya

Security Consultant at IBM Thailand

What users had to say about valuable features:

The main feature of Vectra AI that I find valuable is its focus on the user interface and its approximately two hundred algorithms based on artificial intelligence and machine learning. It allows me to create automations easily. Using this tool for automation has provided more benefits to our processes.

Nawaf Fawaz

Planning& Performance Analyst at National Information Center, Ministry of Interior, Saudi Arabia

[Read full review](#) 

“The packet capturing feature is very useful, and as the name suggests, AI uses models to detect abnormal behavior. Some of the patent-matching algorithms they use are very advanced and detect threats at a very early stage.

For me, detections from unmanaged networks are one of the greatest values. You can identify threats from BYOD or even mobile devices, which were not handled before..”

Naveen Hariharan Vijaya

Security Consultant at IBM Thailand

[Read full review](#) 

“There are many detection features available. There are extensive out-of-box detection capabilities. I cannot mention just one or two at the moment. There are multiple detection rules, and its integration with ADR and Office 365 AI is very nice, to be honest with you. It is scalable, and they have their own appliance that can handle multiple locations. You can deploy it for enterprises with multiple sites..”

Mohammad Alkurdi

Owner at Fortibits

[Read full review](#) 

“Vectra AI offers artificial intelligence capabilities with visibility that can be integrated into our day-to-day operations and other tools, including malware detection tools and cyber threat tools.

“Vectra AI has positively impacted my organization. Last year while using it, we received many malicious email threats and virus incidents, including a trojan virus that had reportedly been deployed by someone. Our company used Vectra AI to detect the malicious threats and viruses before they could cause more damage, and we successfully stopped the threats.

“Using Vectra AI, I notice that server downtime has decreased significantly. We now experience only two to three hours of downtime, whereas without Vectra AI and other tools, our downtime would exceed 48 to 72 hours..”

RahulReddy

Consultant at a retailer with 5,001-10,000 employees

[Read full review](#) 

“The most valuable features I find are the threat signal intelligence and the ability to build high-fidelity alerting for customers, which is one of the biggest value adds.

“Cognito Detect is quite useful, but it has only been used in a few companies that have required deeper insights into their network analytics, so not all customers have it. However, the ones that do have found a lot of value in it.

“Vectra AI helps in identifying malicious network activities by enabling threat hunting and providing security enriched network analytics, giving considerable visibility over that aspect.

“I am evaluating Cognito Recall's impact on my customers' threat investigation processes by noting that the ones using it are quite intensive. They can use Cognito Recall to look back further in time on events raised from a SIEM perspective..”

Drystan Govender

CTO at Cyber Retaliator Solutions

[Read full review](#) 

“The best features of Vectra AI are related to AI. For the NDR part, Attack Signal Intelligence features were mainly responsible for behavior AI, high-fidelity signaling, and prioritization. These features were great for anomaly detection and behavioral-based detection, able to catch zero-day attacks and living-off-the-land attacks. For high-fidelity signaling, it automatically triaged, filtered, and correlated signals, which dramatically reduced alert fatigue noise on the customer side by approximately 80% and eliminated alert fatigue on the SOC teams. Regarding the identity detection and response IDR solution, it monitored Active Directory and Entra ID for any attacks, allowing the SOC to detect any compromised credentials.

Alert noise was dramatically reduced by nearly 80%, allowing SOC analysts to focus more on true threats, which made them more productive and resulted in higher operational efficiency. Attack Signal Intelligence helped reduce irrelevant alerts by 80% to 90%, with metrics showing a 100-plus reduction in investigation workloads and roughly saving about 55,000 hours of investigation time. Investigation time has decreased significantly, empowering analysts with detection and advanced unknown threats that Vectra AI provided. Its knowledge base and database are very up to date, allowing for spotting zero-day attacks with full visibility and helping to stop attacks in minutes.

Vectra AI has reduced the MTTD and MTTR, increasing operational and process efficiency, and has helped reduce the number of SOC analysts that needed to be hired. Thanks to the AI features, the number of employees and SOC analysts hired has been reduced..”

Verified user[Read full review](#) 

Strategic RAN Lead | Network Transformation & Optimization | Philippines & South Africa at a tech vendor with 10,001+ employees

Other Solutions Considered

“Other options were not evaluated, as at that time, Vectra AI was the only NDR solution that had AI features. They began with the AI concept that was being sought..”

Verified user

Strategic RAN Lead | Network Transformation & Optimization | Philippines & South Africa at a tech vendor with 10,001+ employees

[Read full review](#) 

“We weren't using any solution before. We went for Vectra AI because we wanted something to have visibility. We were completely blind to what could happen on the network. With Vectra AI, we aren't so blind..”

Martin Bruno

CIO at General Transmissions

[Read full review](#) 

“Previously, we used Darktrace. Though it is a good platform, because there were so many false positives coming through, we found that we were neglecting it and not investigating the alerts. After less than a year of using Vectra, we've managed to tailor our dashboards to a point where we just see the high-volume or high-risk alerts coming through, and we act on those on an instant basis. Vectra AI has helped me get my time back. .”

Tony Whelton

Director IT at Wellington College

[Read full review](#) 

“We evaluated other options very thoroughly. It became a two-horse race between Vectra and Darktrace. The differentiators for us were the UI experience, the MDR, and we felt that there was better engagement with the Vectra presales team. They better understood our needs and how Vectra would fit as a solution..”

Verified user

Head of ICT Security & Governance at a construction company with 501-1,000 employees

[Read full review](#) 

“We had a SIEM solution that was mainly focused on event-based logging, not necessarily on the network part. We were looking at more of a network IDS solution, and that's where Vectra came in. We wanted something that was easy to use as we didn't want too much platform maintenance. We wanted something to plug into the box and make it work. At first, we didn't believe that we would be able to find something like that after we had seen Darktrace, their biggest competitor, but in the end, Vectra was a perfect fit for us because it made it very easy to insert it into our branch offices as well..”

Verified user

[Read full review](#) 

Security at a financial services firm with 201-500 employees

“We looked at ExtraHop, a VMware NDR solution, Carbon Black, and a solution from a French organization.

Carbon Black is oriented around VMware products. As such, it would have been okay for the data center, but we would have had to upgrade the entire physical infrastructure inside the data center. It would have been very expensive, and thus, we eliminated Carbon Black. The French competitor was eliminated because the solution was a few years behind.

We then talked with Vectra AI and were happy with what they offered us. We spoke with other companies that use it and found out that they were happy with it. Thus, Vectra AI got the opportunity to do the proof of concept..”

Verified user

[Read full review](#) 

Cybersecurity Consultant at a tech services company with 201-500 employees

ROI

Real user quotes about their ROI:

“A good return on investment has been seen. For cost savings over a period of three years, it could be about 350%. The payback period is roughly six months. Productivity savings could be about 800,000, with SOC efficiency increasing nearly 40%. Workload reduction on the SOC side is now 100% lighter than previously..”

Verified user

[Read full review](#) 

Strategic RAN Lead | Network Transformation & Optimization | Philippines & South Africa at a tech vendor with 10,001+ employees

“When it comes to ROI, in certain places we saw the return and in certain places we didn't. When it comes to security investments and tooling of security, the return on investment takes a bit longer and you always see your investment back. At one point something will happen and you will start using the tool for the reason you bought it..”

Verified user

[Read full review](#) 

Security Engineer at a legal firm with 1,001-5,000 employees

“From a security perspective, it's always hard to find a return on investment. If you look from the risk mitigation perspective and what's the worst that can happen, if we can stop attacks sooner, it would result in lesser costs on remediation afterward because we were fast on the initial attack..”

Verified user

[Read full review](#) 

Security at a financial services firm with 201-500 employees

“After deploying Vectra AI in our network, it began to add value to our security operations within a week.

We have not yet seen ROI, but we are growing our usage. We need to offload at least one analyst or have it do the work of a couple of analysts over time. .”

David Heed

[Read full review](#) 

Security Center Coordinator at a comms service provider with 1-10 employees

“We stopped some attacks. An attack could cost a lot more than the cost of Vectra. For example, we got an attack before that cost us \$100,000. So, Vectra's cost is not so high. The cost of an attack could be worse. If we got encrypted data, it could be worse because we would have to stop the factory, which would cost a lot..”

Martin Bruno

CIO at General Transmissions

[Read full review](#) 

“I haven't gotten much feedback about the return on investment. Because nothing is happening yet, we need some reassurance that we can see when it does. We must feel confident that it will actively respond when something happens.

We can use Vectra to create visibility, like Microsoft coming out with end-of-life PCERPC integrations. We can help the clients even though it's not on the security operations team. You can utilize the network data once you have it and we can build the services to provide assistance above and beyond detection..”

Verified user

Product Owner NDR at a tech vendor with 201-500 employees

[Read full review](#) 

Use Case

“As an end user, I do not have to commit manpower to manage Vectra since most of their use cases are managed by them. It's a hands-off kind of deployment..”

Verified user

Cyber Security Engineer at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“Vectra AI is my main cybersecurity tool, and we use the AI data in our company. For example, when we discovered a malicious email, Vectra AI helped us identify that it was not a legitimate email, and we successfully stopped the threats..”

RahulReddy

Consultant at a retailer with 5,001-10,000 employees

[Read full review](#) 

“This tool operates on machine learning principles, utilizing its own AI-based models and rules to detect activity within your environment. Initially, Vectra AI observes and monitors your organization's behavior for a two-week period, identifying legitimate services operating within your environment. Once it completes this monitoring phase and detects all services, it begins to assign certainty and severity levels to the network traffic it observes..”

Verified user

[Read full review](#) 

Associate Director Security at a outsourcing company with 10,001+ employees

“Our primary focus lies in identifying weaknesses to address customer concerns regarding visibility into network operations. This is especially crucial due to the presence of various managed devices within the network. Detecting and managing these devices and enhancing visibility is done by Vectra AI. It also has the capability to detect potential threats and correlate diverse events that occur on the network. Hackers often target systems from different domains, requiring cross-domain correlation. Net NDR solutions, particularly Vectra, excel in fulfilling these needs using AI-driven algorithms. Over time, these algorithms learn from the data, aiding in automatic post-event analysis. .”

Atakan Oztuna

[Read full review](#) 

Technical Sales Engineer at Barikat Cyber Security WLL

“We use Vectra AI for endpoints where we are unable to install agents, like endpoint agents, EDR agents, or antivirus tools. For example, BYOD devices or routers in our network. We don't have any control over those, but we need monitoring capability.

Vectra AI can monitor the traffic from the wireless router to the firewall or any outgoing traffic. It can give us an idea of whether there is any C&C or C2 communication or any botnet activity from those source IPs. Without having any agents in the endpoint, it is a network monitoring tool. We use this tool to detect threats within the environment where the assets are unmanaged.

Also, since we tap into certain network points such as firewalls or IDSs, we get more visibility from managed assets as well. So before the endpoint notices the behavior, Vectra notices some of the exfiltration techniques and alerts us..”

Naveen Hariharan Vijaya

Security Consultant at IBM Thailand

[Read full review](#) 

“Vectra AI is being used as an NDR solution to sell to customers as a managed service. The product has been productized to sell to customers as an NDR solution. The network is scanned for any anomalies or threats that are detected and fed to the customer's SIEMs and SOARs.

In one financial sector scenario, a customer was complaining about reduced alert fatigue and detecting an attack missed by traditional tools. They wanted an AI solution that could detect anomalies with the best MTTD and MTTR response times to reduce overhead over the SOC teams.

Vectra AI has been used for identity management, which was integrated with Microsoft Entra ID and Active Directory to monitor account activity. A customer wanted in-depth analysis on their identity management solution. Another scenario involved integrating with the customer's cloud solutions, where they wanted a solution that provided cloud detection and response through AWS and Microsoft 365 environments..”

Verified user

[Read full review](#) 

Strategic RAN Lead | Network Transformation & Optimization | Philippines & South Africa at a tech vendor with 10,001+ employees

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

Setting up Vectra AI is more complicated compared to other tools like ExtraHop. It requires multiple appliances for different functions, whereas ExtraHop requires only one sensor.

Nawaf Fawaz

[Read full review](#) 

Planning& Performance Analyst at National Information Center, Ministry of Interior, Saudi Arabia

“Vectra AI didn't have a SaaS model until recently. Companies don't like deploying something complex that'll turn customers away. From what I understand, Vectra AI is somewhat complex in its deployments..”

Dan Jeske

[Read full review](#) 

Account Executive at Fishtech Group

“The setup is a very straightforward process. You need to tap the network traffic at your desired point, and it has two components: a sensor and a brain. The sensor collects the logs and forwards them to the brain, which does the detection and everything. They offer a virtual appliance that you can run in your environment.

The setup process is usually very simple. It took only two days to set up. But, initially, deciding the location of the sensor and other factors took more time. The threat team at Vectra AI engaged with us effectively, provided all the support, understood our architecture and advised us on placing the sensors..”

Naveen Hariharan Vijaya

Security Consultant at IBM Thailand

[Read full review](#) 

“We started with a proof of concept and then we committed to the Vectra solution. That's when we began the formal implementation. From the very initial engagement to the proof concept and through the transition to service, it took approximately six months.

The deployment went very well and that was a real positive in terms of the engagement with the onboarding and the customer experience.

Across our ICT team, six individuals were involved in security, infrastructure, project management, and service transition.

There is no maintenance of the solution on our side..”

Verified user

Head of ICT Security & Governance at a construction company with 501-1,000 employees

[Read full review](#) 

“ The on-prem setup requirement is something easy. However, the cloud's environment setup is a bit tricky and complex. Not only because of the Vectra but also due to the some limitations of the cloud setup. The deployment process varies depending on the organization's size and footprint. It typically takes about one week for data centers with a dispersed network across different regions. For Vectra, on-premises deployment is relatively straightforward, but the cloud deployment can be more complex.

The deployment process involves adhering to ITIL processes, including change management. This entails creating change requests and engaging Smart Hands for physical sensor deployment or allocating VM resources for virtual sensors. Network availability and coordination are essential aspects of the deployment process. In simple terms, it involves a well-defined change management process and various steps to ensure a successful deployment. I would rate it a six out of ten.

Verified user

[Read full review](#) 

Associate Director Security at a outsourcing company with 10,001+ employees

“The initial setup is straightforward. I would rate the setup an eight out of ten.

In the case of deployment, 70% of the public prefers the public cloud while the rest prefer private. These are the only two forms of deployment.

The initial deployment should ideally be completed within two weeks. However, due to the need for fine-tuning, false positive elimination, and deriving enhanced value, an extended period of around two months is necessary. This allows users to cover all the potential threats and risks, ensuring comprehensive coverage

.”

Atakan Oztuna

Technical Sales Engineer at Barikat Cyber Security WLL

[Read full review](#) 

Customer Service and Support

When I create tickets, the response is fast, and issues are solved promptly. However, more technical queries may take two or three days, or up to a week.

Nawaf Fawaz

Planning& Performance Analyst at National Information Center, Ministry of Interior, Saudi Arabia

[Read full review](#) 

“From what I've heard, the support team is responsive and helpful. However, I haven't had the opportunity to directly interact with the technical support team..”

Verified user

Associate Director Security at a outsourcing company with 10,001+ employees

[Read full review](#) 

“I would rate their technical support a 10, as we have local support in South Africa and the ability to reach out to the teams quickly and effectively when they are in similar time zones, leading to great support globally..”

Drystan Govender

CTO at Cyber Retaliator Solutions

[Read full review](#) 

“We are very satisfied with the support. It has been excellent so far. It has been very timely, very personalized, and always quick to find solutions. We've been really pleased with it..”

Verified user

[Read full review](#) 

Head of ICT Security & Governance at a construction company with 501-1,000 employees

“Two months ago, we had a small incident, and we used their technical support. A colleague of mine interacted with them, and it was perfect. I t was done flawlessly, and everything worked. I'd rate them a nine out of ten..”

Verified user

[Read full review](#) 

System Engineer at a computer software company with 1,001-5,000 employees

“We have a strong local presence and support in this market, and our company's origins in Turkey also contribute to robust local assistance. While comprehensive support is provided during major incidents and upgrades, we excel in offering immediate assistance for failover situations and downtime prevention. The team is highly specialized in cyber security and SOC technologies. We are quite strong and are able to help ourselves in the field of technical support.

.”

Atakan Oztuna

[Read full review](#) 

Technical Sales Engineer at Barikat Cyber Security WLL

Other Advice

“Vectra AI should be considered if looking for an NDR solution and not just an EDR solution only. It provides great value and quality, provided that customers can pay for the licenses, which are quite expensive. Vectra AI is represented as a partner and reseller in business with this vendor. This review has been given a rating of eight out of ten..”

Verified user

Strategic RAN Lead | Network Transformation & Optimization | Philippines & South Africa at a tech vendor with 10,001+ employees

[Read full review](#) 

“At the end of the day, it's written rules in such a way. The trend in the market is something I did not consider much. The detection rules are written in the back end. There is something happening in such a way to do it again. AI is mentioned too much, and for me, it is only marketing talk. At the end of the day, there is no one hundred percent AI in security. Detection requires manual writing at times. They already handle back-end processes but vendors won't show this. AI is not targeting a specific vendor. AI, for me, is just a trend. It depends on the client. I tailor solutions to client requirements. For visibility and monitoring, I choose the best products. Every application, every NDR solution has its capabilities. It varies by client because I must advise clients on solutions they can use and benefit from. I sometimes advise clients about Vectra as it still serves my clients well. It's fair enough for now. The overall product rating is seven out of ten..”

Mohammad Alkurdi

Owner at Fortibits

[Read full review](#) 

“I would advise other organizations using Vectra to ensure they fine-tune their service groups, correctly label their services, and integrate their firewalls and [AWS](#) systems. This will help obtain accurate and updated information about DMZ tools, VPN tools, and [EC2](#) tools, allowing Vectra to have better visibility into the services running. This, in turn, can improve the accuracy of the scan feed and provide more precise results, reducing false positives.

Overall, I would rate it seven out of ten.

.”

Verified user

Associate Director Security at a outsourcing company with 10,001+ employees

[Read full review](#) 

“The solution had some very good integrations with firewalls and EDR solutions. Since Vectra AI is more of an internally-detection and response tool, it detects insider threats extremely well.

Before choosing Vectra AI, ensure you have a proper architect for your environment that shows you where all your blindspots could be. This makes the deployment a lot easier. Vectra AI detects threats that people miss, especially manual operators.

Vectra AI has helped save a lot of log analysts time because they don't have to deal with a lot of alert noise and false positives. Using Vectra AI for detection, triaging, and responses speeds up your soft response mechanism and makes the responses much quicker.

Overall, I rate the solution an nine out of ten..”

Drystan Govender

CTO at Cyber Retaliator Solutions

[Read full review](#) 

“I would rate it at nine out of ten. The one point I'm reducing is because the model can learn itself. If no one is fine-tuning it, for example, every time we find a huge number of alerts, then only we go and look it up and fine-tune the product.

If no one is acknowledging it or it seems like regular traffic, then the product can understand that behavior and have a feedback mechanism to correct it, mark it as a false positive, or whitelist it.

My recommendation:

[Understand](#) your network first, and place the sensors in the correct position to receive all kinds of traffic: THC, PDNS, and all those things. If you place the sensors at the egress traffic, you may not receive some of the packets, and you will not have overall visibility.

So the placement of sensors is very important; you need to understand your network to place them correctly..”

Naveen Hariharan Vijaya
Security Consultant at IBM Thailand

[Read full review](#) 

“The intuitive dashboards are incredibly useful, with both the Quadrant UX and the Respond UX, so whether looking from a management point of view or an analyst point of view, both dashboards are very intuitive.

“The biggest metric I use to demonstrate the dashboard's effectiveness is the ability to respond to an alert effectively, particularly within the SLA timeframe. Many of our customers have an SLA with our partners, and if they keep to that SLA, it means the tool performs effectively. We have not had instances of it not working among our partners.

“I assess the benefits of integrating Cognito [Stream](#) with existing [SIEM](#) systems by

noting that Cognito [Stream](#) is very similar to Cognito Recall and provides enriched details around the network side in real-time. However, it is not for investigation purposes but rather for visibility purposes over the network.

“My overall rating for Vectra AI is 10..”

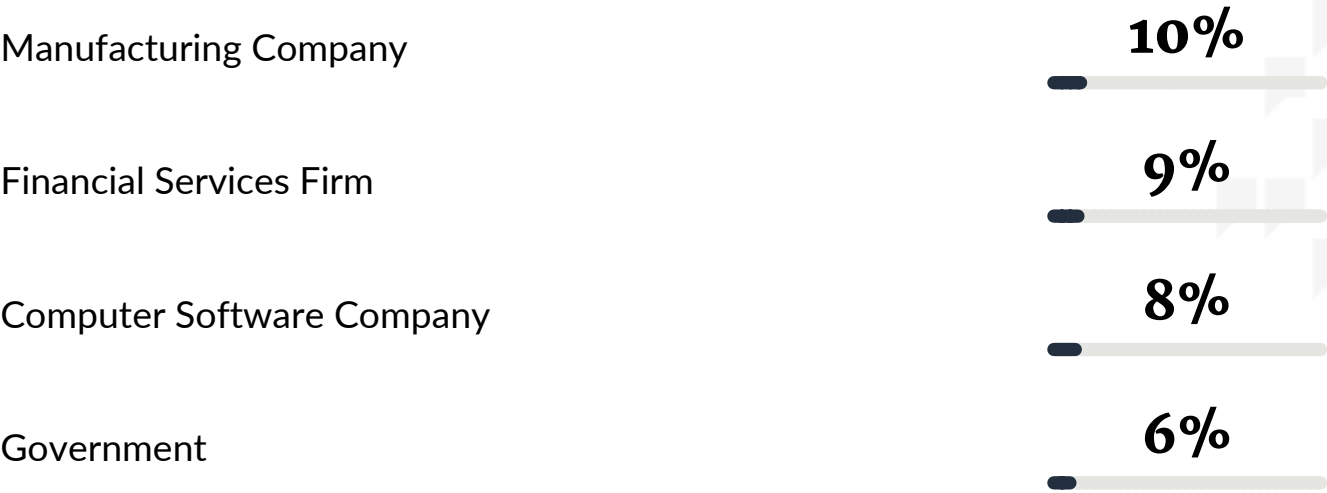
Drystan Govender

CTO at Cyber Retaliator Solutions

[Read full review](#) 

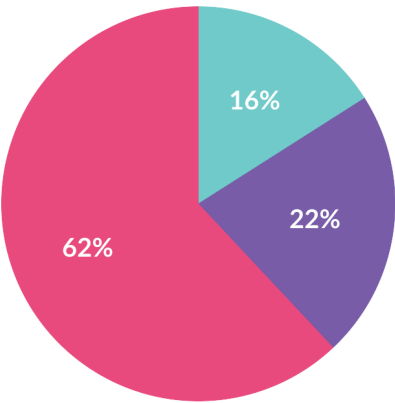
Top Industries

by visitors reading reviews

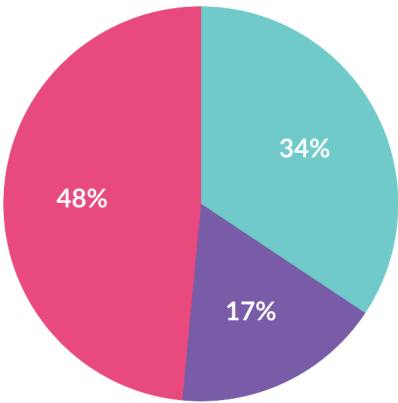


Company Size

by reviewers



by visitors reading reviews



 Large Enterprise  Midsize Enterprise  Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944