



**Vectra AI**

# **Reviews, tips, and advice from real users**



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 12

ROI..... 13 - 17

Use Case..... 18 - 20

Setup..... 21 - 24

Customer Service and Support..... 25 - 26

Other Advice..... 27 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

# Product Recap



Vectra AI

# Vectra AI Recap

Vectra AI is used for detecting network anomalies and potential malicious activities, providing visibility into network traffic and enhancing threat detection across environments.

Organizations deploy Vectra AI mainly on-premises with additional cloud components. It helps with compliance, incident response, security monitoring, detecting insider threats, and correlating network events. Vectra AI captures and enriches network metadata, provides detailed dashboards, reduces false positives, and supports cross-environment behavioral analysis to enhance threat detection and prioritization. While valued for its high accuracy and alert aggregation, it has room for improvement in UI/UX, packet management, and integration with SIEMs and other tools. It is noted for expensive pricing and limited proactive threat response features.

## What are Vectra AI's most valuable features?

- High accuracy in identifying threat locations
- Aggregation of alerts into single incidents
- 24/7 threat detection
- Visibility into the entire attack lifecycle
- Risk score aggregation
- Effective triaging of alerts
- Integration with other tools

## What benefits or ROI should users look for?

- Enhanced threat detection and prioritization
- Comprehensive network visibility
- Reduction in false positives
- Better incident response capabilities
- Improved compliance monitoring

In specific industries, Vectra AI is deployed to monitor complex networks and alleviate challenges in threat detection. It is particularly effective in sectors requiring stringent compliance and security measures, offering insights and capabilities crucial for protecting sensitive data and maintaining operational integrity.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“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



“It provides various dashboards that facilitate the identification of connections and can detect data exfiltration, meaning data sent from your environment to another.”



**Sajid Mukhtar**

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



“The solution is currently used as a central threat detection and response system.”



**Drystan Govender**

Senior Sales Engineer | Product Lead: TOPIA at Cyber Retaliator Solutions



“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



“The biggest feature for us, because we are heavy Microsoft users, is its integration with Office 365. On top of Vectra AI, we use all of the Microsoft security platforms, such as Defender ATP and Sentinel. Having full integration and a central platform to look at all of the threats that are coming through from the different platforms is a huge benefit for us.”



**Tony Whelton**

Director IT at Wellington College

## What users had to say about valuable features:

“Vectra AI can bring the ability to detect intrusion on the network more so than legacy IDS tools. It goes beyond just doing sample packet capture as Corelight does and provides value to the customer regarding their reporting and what the tool is doing..”

**Dan Jeske**

Account Executive at Fishtech Group

[Read full review](#) 

---

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](#) 

“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](#) 

---

“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](#) 



“The most valuable feature of the solution is that it only shows us the events that are actually critical. The solution is currently used as a central threat detection and response system. It ingests every bit of information from the SIEM, does AI triaging and detection, and sends incredibly high-fidelity alerts to the SIEM for investigation..”

**Drystan Govender**

Senior Sales Engineer | Product Lead: TOPIA at Cyber Retaliator Solutions

[Read full review](#) 

“Vectra AI offers a range of valuable features. Firstly, it utilizes its own AI-based tools. Secondly, it provides various dashboards that facilitate the identification of connections and can detect data exfiltration, meaning data sent from your environment to another. The tool operates based on metadata, offering comprehensive information about traffic between source and destination. Some key features include the ability to integrate with EDR or EPP solutions, allowing you to secure servers with stability issues or infections. Alternatively, you can use Active Directory to lock down infected hosts if you choose not to incorporate EPP or EDR. These features provide insights into your network, showing connection details, data transfers, VPN connections, and the number of connected EDS event hosts, among other things. .”

**Sajid Mukhtar**

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

[Read full review](#) 

# Other Solutions Considered

“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](#) 

---

“We evaluated Darktrace and one more solution. We also evaluated some SOC and SIEM systems, but we found Vectra AI to be better in comparison to other solutions. It was simple to implement and analyze..”

**Martin Bruno**

CIO at General Transmissions

[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](#) 

“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 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**

Security at a financial services firm with 201-500 employees

[Read full review](#) 

“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**

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

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“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**

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

[Read full review](#) 

---

“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**

Security at a financial services firm with 201-500 employees

[Read full review](#) 

“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**

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

[Read full review](#) 

---

“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**

[Read full review](#) 

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

---

“The capturing of network metadata at scale reduces the time of investigations when researching incidents. Instead of having to look over multiple tools, that data can be somewhat aggregated, from a Vectra perspective. The time to detect and understand a threat has been reduced.

Vectra AI has reduced the time it takes us to respond to attacks. The amount of time depends on the specific detection or circumstance around it. Some things have been raised previously, then we would have good knowledge about what that detection meant and how to investigate it effectively. Other times, a detection might be viewed as more novel, where there may not be the immediate skills in place to investigate it effectively, whether that is the security team or me. There is a whole lot of research that needs to go into this to make sure that you have the knowledge to actually verify whether a thing needs to be dealt with.

Vectra AI provides you this information very well, with more context around the detection. Someone with a more general knowledge of some of these things can look at all the factors rather than just the detection to make a determination of how risky it is and how you might start investigating it. For example, with autodetection in an account, if it was just that detection, then your initial response might be to lock that account out. However, if you get a bit more context about it and can see what other activities were happening on the same asset around the same time, then you might not lock that account. You might just reach out to that user, and say, "Hey, what was this about?" because you are not so concerned about an immediate threat.

There is ongoing maturity from our security strategy, which this solution introduces. Down the track, we could look to extend this from an agent perspective to our cloud platforms in a more rigorous way than what has already been implemented. It gives us increased confidence over time as we do get these detections and alerts that are valid, so we are able to accurately resolve and stop them quite quickly. That is where we will see the bigger benefit. It will tick something and alert us as quickly as possible, then we can get to it and shut it down as quickly as possible. That means our security maturity is only strengthening, and we can respond and have visibility over events in the future.



The return on investment was passed over to our SOC. They were using our previous tool, DarkTrace, and now they are using Vectra. There will be a lot less in future reports because there will be a lot less that they are actually investigating..”

**Dave Wallace**

Operations Manager at a healthcare company with 51-200 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](#) 

“We have a basic Vectra environment because we mainly only use the NDR for the solution's options. We do mainly filled logins, anomalies, and network flow monitoring..”

## Verified user

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

## Sajid Mukhtar

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

[Read full review](#) 

“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**

Technical Sales Engineer at Barikat Cyber Security WLL

[Read full review](#) 

---

“Our company is in the retail arena, and we have stores, warehouses, and a data center. Right now, we're using Vectra AI in our offices and the data center. The major issue we had was that we were completely blind inside our data center in terms of seeing what traffic we had. Our main focus with Vectra AI was to see what's happening inside the data center through virtual sensors. We're going to expand it to include our stores because the franchisees requested that we monitor the networks in all of the stores. Every shop in our company is a franchise, and they can do whatever they want to in their shops. We won't have any idea as to what's on the network in the shops. By using Vectra AI, we will have visibility into the network.

We have started the proof of concept for our warehouses as well..”

**Verified user**

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

[Read full review](#) 

“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](#) 

# 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.

**Sajid Mukhtar**

[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..”

**Sajid Mukhtar**

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

[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**

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

[Read full review](#) 

“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. It 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

---

“I would rate their support a ten, on a scale from one to ten, with one being the worst and ten being the best. The reason for this rating is that they were with us every step of the way to help and guide us through the process seamlessly..”

**Verified user**

[Read full review](#) 

CyberOps at a manufacturing company with 10,001+ 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

“The technology is strong, but everything around the technology outside of support is weak. Vectra AI needs to find a way to make it more cost-effective for customers to compete with some of the other tools on the marketplace that customers are buying. Vectra AI should do sample packet captures for clients with different use cases. They're trying to forcefully push their tool on the market when the market wants something else.

Overall, I rate Vectra AI a five out of ten..”

**Dan Jeske**

Account Executive at Fishtech Group

[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.

.”

**Sajid Mukhtar**

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

[Read full review](#) 

“Vectra faces robust competition, but it substantiates its abilities. Depending on client needs, it can easily work with other IT solutions. Yet, for pure network detection and response, Vectra excels, particularly for enterprises demanding very good solutions. It offers superior detection coverage for heightened security. It has an encryption-based approach, enabling threat detection without decrypting any data. Moreover, Vectra stands out with its broad integration capabilities with third-party tools and I personally find it a successful feature.

Overall, I would rate Vectra AI an eight out of ten. .”

**Atakan Oztuna**

Technical Sales Engineer at Barikat Cyber Security WLL

[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](#) 

“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**

Senior Sales Engineer | Product Lead: TOPIA 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..”

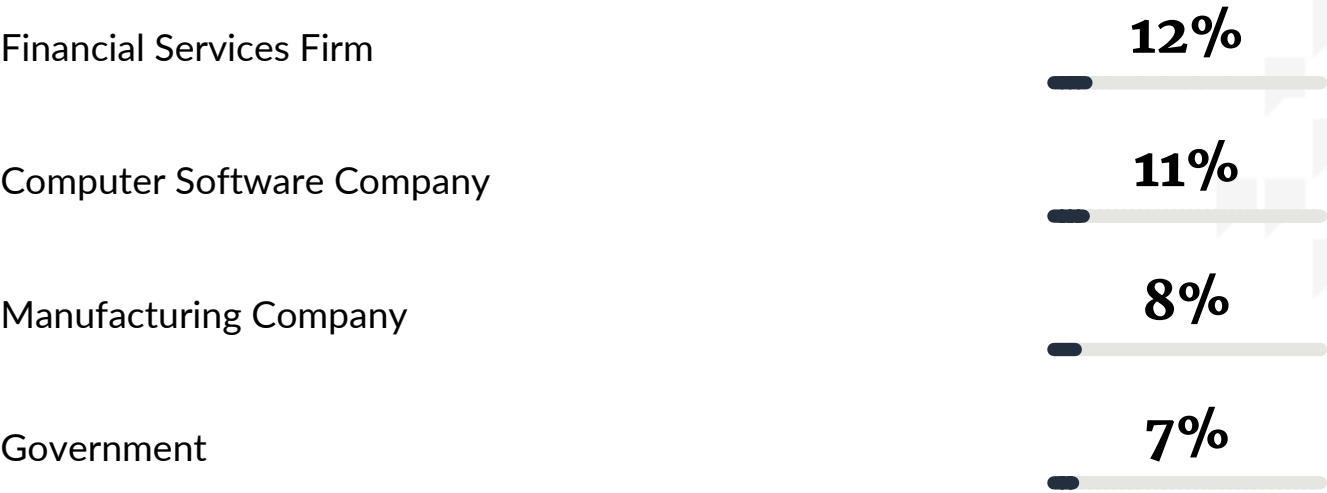
**Naveen Hariharan Vijaya**

Security Consultant at IBM Thailand

[Read full review](#) 

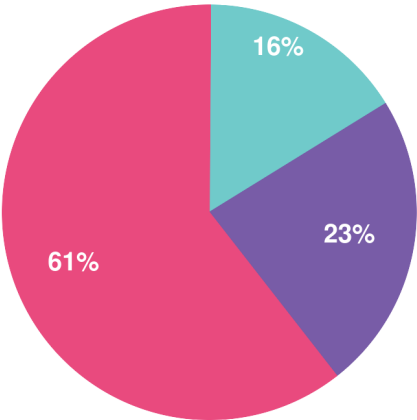
# Top Industries

by visitors reading reviews

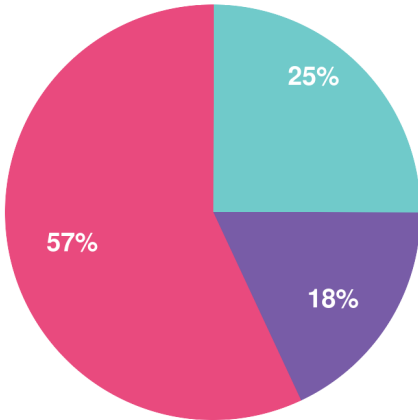





# Company Size

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 software running on AWS and other platforms. 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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944