aws marketplace

Darktrace

Reviews, tips, and advice from real users
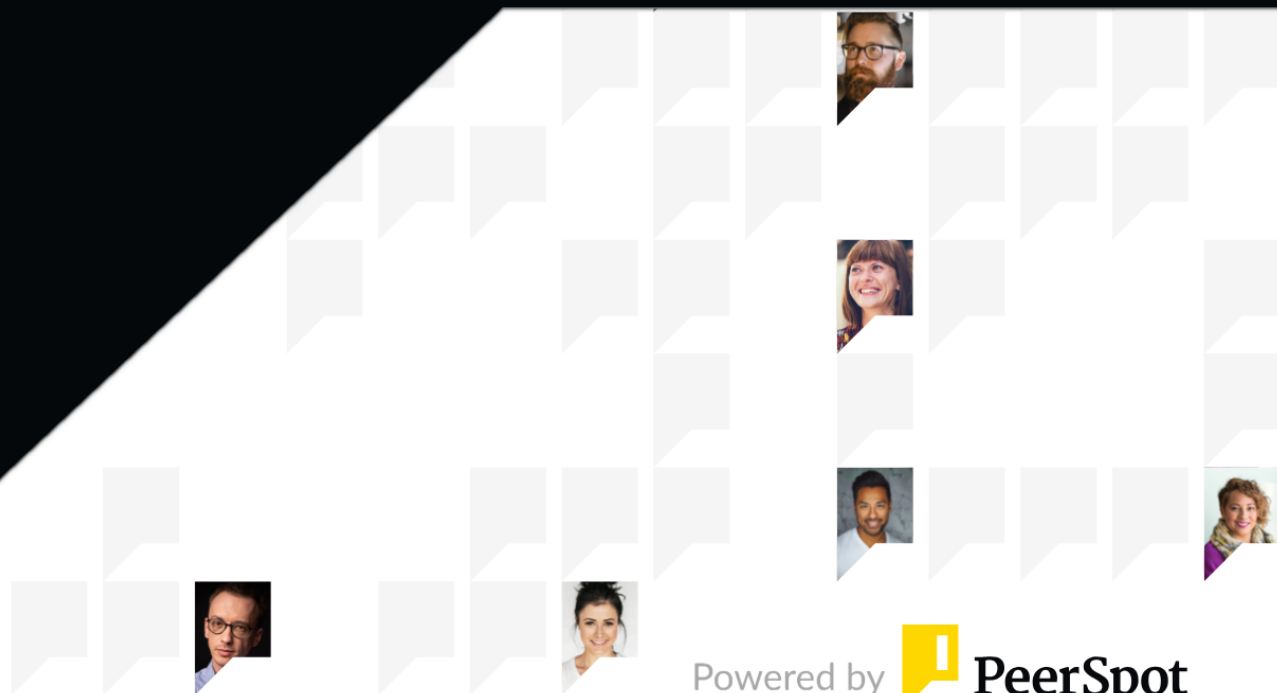
Contents

Product Recap

Darktrace

Darktrace Recap

Darktrace is a leading cybersecurity solution that leverages artificial intelligence and machine learning to provide advanced threat detection, response, and risk management capabilities. Many reviewers find Darktrace's AI and machine-learning capabilities to be valuable. They appreciate its ability to detect anomalies and threats that might go unnoticed by traditional security tools. Overall, the general sentiment towards Darktrace from reviewers is positive. Users seem to appreciate its scalability, stability, AI capabilities, visibility, and ease of use.

Darktrace offers a proactive and intelligent approach to cybersecurity. It utilizes AI algorithms to learn and understand the 'pattern of life' for every user and device within a network. This understanding enables it to detect anomalies that could signify a cyber threat, from subtle insider threats to more obvious ransomware attacks.

Its adaptability, autonomous response features, and comprehensive network visibility make it a top-tier solution for different sizes of organizations and across many industries. It was named one of TIME magazine's 'Most Influential Companies' in 2021 and protects over 8,800 organizations globally from advanced cyber threats.

Darktrace Cyber AI Loop

The Darktrace Cyber AI Loop introduces an advanced artificial intelligence-based system for cybersecurity, designed to build a self-improving defense mechanism. This system functions like a closed loop, where each stage feeds information and insights into the next, amplifying the overall effectiveness of the platform.

The key components of the loop are:

- DETECT- An AI engine that monitors your network and endpoints for anomalous activity, constantly learning the normal behavior of your users and devices. It identifies suspicious patterns and potential threats in real-time, even from never-before-seen attacks.
- PREVENT - This proactive arm analyzes vulnerabilities and identifies weaknesses in your IT infrastructure. It prioritizes patching and configuration changes to harden defenses before attackers can exploit those vulnerabilities.
- RESPOND - When DETECT identifies a threat, RESPOND takes immediate action to contain and neutralize it. This can involve isolating compromised devices, disrupting attacker activity, and automatically escalating critical incidents to human analysts.
- HEAL - This newest addition to the loop focuses on post-incident recovery. It automatically restores compromised systems, cleans infected files, and helps to prevent the attack from spreading further.

Darktrace's AI algorithms can identify threats that traditional security tools might miss. It

continuously learns and updates its understanding of what is normal for each environment, ensuring that it can quickly detect and respond to unusual activities that could indicate a breach. Darktrace's Antigena module can autonomously respond to threats in real time. This is particularly crucial in containing fast-moving threats like ransomware, where every second counts.

Darktrace's solution provides unparalleled visibility into all parts of the network, including cloud services, IoT devices, and industrial control systems. This comprehensive coverage ensures that no part of the network is left unprotected. However, while the Darktrace Cyber AI Loop offers a robust solution, it is not a complete cure-all and requires careful implementation and integration with existing security frameworks.Darktrace offers a comprehensive and unified approach to cybersecurity. It provides continuous protection against known and unknown threats, regardless of where they emerge. Darktrace's solutions provide visibility into your cloud infrastructure, continuous monitoring of application usage and communication patterns (e.g., identification of suspicious actions like unauthorized data access), comprehensive email security that goes beyond traditional spam and phishing filters, real-time protection for endpoints, and continuous monitoring of network traffic and device activity.

Darktrace also provides specialized coverage to secure your zero-trust architecture. Identifies compromised identities, unauthorized access attempts, and risky data exfiltration within a least-privilege environment. Finally, it has a dedicated solution for safeguarding industrial control systems and critical infrastructure. Monitors communication patterns, device behavior, and physical access within OT environments, protecting against operational disruptions and cyberattacks.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✔ "I can rate Darktrace's technical support as one of the best products in the world."

> **Anil M**
> Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

✔ "The technical support from Darktrace is very good, including support from their resellers."

> **Malebo Lethoba Group**
> Security Analyst at a healthcare company with 10,001+ employees

✔ "The most valuable feature of Darktrace is its ability to detect and counter threats before they occur."

> **Peter-Murphy**
> Head of Technology Operations at Pobl Group

✔ "The most beneficial feature in Darktrace is identifying phishing emails with the help of the AI engine and machine learning."

Waleed Omar

Information Security Specialist at Arab Open University

✔ "The autonomous mode, which is the Antigena AI response, is particularly valuable."

ChristopherMangava

Group Cybersecurity Administrator at Tharisa

✔ "Darktrace is valuable since it offers full packet capture and detailed metadata."

Magdy Ali

Network & Security Section Head/Digital Transformation at City Edge

✔ "The most valuable features are the AI and advanced learning tools that distinguish it from other products."

Zia Syed

Systems Specialist/ Administrator at ALFA International Company Limited.

What users had to say about valuable features:

The autonomous mode, which is the Antigena AI response, is particularly valuable. It is capable of responding to lateral movement and ransomware deployment within environments where there is data exfiltration. For example, if more than 2.5 gigabytes of data have been pulled in a few minutes, it engages by blocking for one-hour intervals, alerts, and extends the block until it goes into full isolation if the violation continues.

ChristopherMangava   Read full review ↗
Group Cybersecurity Administrator at Tharisa

The AI analysis and AI investigation features are incredibly effective. I do not need to manually process incidents as Darktrace provides an incident summary, potential detection paths, and other details, all exportable with just a click. The tool is very powerful and saves a lot of time. The autonomous response technology eliminates the need for human intervention by automatically handling incidents even during off hours.

Verified user   Read full review ↗
Security Information & Incident Analyst at a financial services firm with
1,001-5,000 employees

"The features that are most valuable to me include detection, response with analytics, and network detection. These features are particularly effective because they provide comprehensive security analytics. Additionally, the analytics aspect is highly appreciated for its effectiveness.

I do not use the automation response since I have another product handling automation. Furthermore, I believe that the reporting needs enhancement for better performance.."

Mohamed Eletreby   Read full review ↗
Solution Architect at a tech services company with 51-200 employees

The most beneficial feature in Darktrace is identifying phishing emails with the help of the AI engine and machine learning. In case it does not identify something, we can automatically make Darktrace learn from selections and other functionalities.

Regarding the ROI, we have experienced a significant reduction in phishing emails and have utilized our time efficiently, resulting in approximately 70% ROI. ."

Waleed Omar   Read full review ↗
Information Security Specialist at Arab Open University

The functions I find most valuable in Darktrace are the AI analyst as well as the detection.The autonomous response capabilities of Darktrace are not crucial for me because it doesn't work in a network where there are no core switches. In a modern network, the autonomous response doesn't work, especially when sitting in a shared data center.If I'm running a traditional network where I am not in a shared data center with a layer two dedicated for my resources, then it can work for me. However, if I am in a data center where I don't have layer two, it becomes an issue because the autonomous response is reliant on sending spoofed TCP resets to my core switch to block traffic, which is a major issue.

Malebo Lethoba Group
Security Analyst at a healthcare company with 10,001+ employees

Read full review ⬈

"The features I find most effective in Darktrace include anomaly detection. The machine learning model provides accurate alerts after the learning period of 1 or 2 weeks, especially for network anomalies or something that the user is trying to access, which can include trying to visit unknown sites or botnets, and those things get detected and represented in a very good dashboard.

"Darktrace positively impacts my organization by enhancing threat hunting, particularly in east-west traffic within the same subnet. Previously, we only used traditional firewalls that cannot catch this lateral traffic. After deploying Darktrace, we gain insights into machine-to-machine communication, which adds more value to the organization and is especially beneficial for the SOC team.."

Anil M
Technical Consultant - Unix Platform Services at BITS AND BYTE IT
CONSULTING PVT LTD

Read full review ⬈

Other Solutions Considered

"I previously checked with different solutions.I decided to go with Darktrace. However, it offers complete packet capture and metadata, unlike other vendors.."

Magdy Ali
Network & Security Section Head/Digital Transformation at City Edge

Read full review [↗]

"Before working with Darktrace, I did not use any similar solution in the same category. Earlier, I was using something called decepters, and my organization may have explored different products, but I learned about network detection and response through Darktrace about 5 to 6 years ago.."

Anil M
Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

Read full review [↗]

"I have experience with other solutions such as Morphisec Endpoint Protection, DeepInStink, Darktrace, Check Point, Defender, Veronis, ForcePoints, Odyxx, and SALT API security.."

Verified user
Programma / Project Manager at a tech services company with 1-10 employees

Read full review [↗]

"I did not evaluate other options when looking into Darktrace, but some customer preferences led us to consider other NDR solutions, such as 40 NDR. Our customers had a Fortinet setup with various products, and they preferred the 40 NDR for proprietary visibility when collecting logs from Fortinet devices.."

Anil M
Technical Consultant - Unix Platform Services at BITS AND BYTE IT
CONSULTING PVT LTD

Read full review ↗

"We evaluated Vectra AI alongside Darktrace as a potential network NDR solution, but other competitors are in the market. Trellix also offers an NDR solution, and any cybersecurity product with strong NDR capabilities competes with Darktrace. Since Vectra AI was relatively new and not yet stable at that time. Metrix also offers an NDR solution, but its product lineup is too complex, requiring the purchase of multiple components to access NDR capabilities. This didn't align with our approach of selecting best-in-class products for specific functions rather than opting for an all-in-one solution.."

ADITYA KAUSHIK
Director Of Information Communication Technology (ICT Head) at a
maritime company with 1,001-5,000 employees

Read full review ↗

The main competitor of Darktrace at the moment, based on how long they've been in the market, would be Vectra. Vectra does a similar thing, but Darktrace would beat Vectra based on the algorithms that Darktrace is using because Darktrace's algorithms in terms of AI and ML are quite good.Cisco is also coming with some technologies such as Cisco Secure Analytics, network analytics, and Cisco Secure Cloud Analytics. That technology is quite good because if running mainly on Cisco, such as SD-WAN Meraki devices with remote workers using Cisco Umbrella or AnyConnect, pulling data from them and pushing it into an XDR or Secure Analytics can be quite effective, providing reachability, visibility, and scalability.

Malebo Lethoba Group   Read full review [↗]
Security Analyst at a healthcare company with 10,001+ employees

ROI

Real user quotes about their ROI:

"The organizational value gained from Darktrace is securing the business against potential threats. A tangible return on investment is only noticeable if facing an actual cyber attack.."

Peter-Murphy   Read full review [↗]
Head of Technology Operations at Pobl Group

"Using this solution provides financial benefits by securing from server attacks, which offers indirect savings. The percentage of budget savings can range from 30% to 40% for online businesses and five to ten percent for in-house processes.."

Zia Syed   Read full review [↗]
Systems Specialist/ Administrator at ALFA International Company Limited.

"The solution improved our visibility. Earlier, we couldn't visualize some threats on the internal network level. With Darktrace, we were able to spot some deficiencies and certain vulnerabilities.."

Marcelo Zuniga
CISO at a financial services firm with 1,001-5,000 employees

Read full review ↗

"The return on investment is really high in terms of detecting bad actors or bad threats in the organization. In addition, I have discovered that when we negotiate a bundle package with Darktrace, they are really considered as affordable.."

Manjunath_P
CISO at Interplex Electronics Malaysia Sdn. Bhd.

Read full review ↗

"The benefit is the security. You probably have a security case, an alarm system, and one or two locks. You don't rely on one security device; you have different layers. Darktrace is just one of those layers.."

AntonGeijsendorpher
IT Network Administrator at Foord

Read full review ↗

"When considering return on investment for organizations using Darktrace, the disadvantage lies in having to use a physical appliance. Running a quick POC is not possible since the hardware has to be shipped from the UK or elsewhere, but other NDR solutions provide virtual appliances that can be deployed on virtualization servers to get up and running quickly.."

Anil M
Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

Read full review ⬈

Use Case

We use Darktrace for network detection and response, specifically for monitoring the network for any malicious activities, anomalies, and lateral movements.

ChristopherMangava

Group Cybersecurity Administrator at Tharisa

"The typical use case for Darktrace is for threat vector scanning, detecting any unusual activity, and anomaly detection. Apart from that, it is very helpful in incident response.."

Anil M

Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

"I am using it for network and email security. I am a systems administrator overseeing cybersecurity at Alpha International Company Limited. We have been using it for about two years, focusing on the latest version.."

Zia Syed

Systems Specialist/ Administrator at ALFA International Company Limited.

"The primary use case for Darktrace includes network monitoring, endpoint monitoring, and email scanning. I integrate it into our cybersecurity strategy and use it to monitor everything happening on the network.."

Peter-Murphy
Head of Technology Operations at Pobl Group

Read full review [↗]

"I am a distributor for several vendors and act as a trusted adviser. Although I do not have an official relationship with Darktrace, I know the product and vendor from working with some organizations in the Netherlands. My clients vary from two hundred fifty seats to fifteen hundred.."

Verified user
Programma / Project Manager at a tech services company with 1-10 employees

Read full review [↗]

"The primary use case for Darktrace is to gain full visibility into the network traffic. Darktrace provides complete packet capture and metadata analysis, unlike other solutions that offer only specific metadata. This comprehensive view allows for better assessment and monitoring of the network environment.."

Magdy Ali
Network & Security Section Head/Digital Transformation at City Edge

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.

The initial setup is straightforward. The machine needs time to learn the environment before entering active mode. It needs to learn traffic flows and what is considered normal before activating full autonomous mode.

ChristopherMangava   Read full review ⬈

Group Cybersecurity Administrator at Tharisa

"The initial setup was straightforward, however, there were some connection issues when deploying the VM on the cloud. Overall, the setup process was easy.."

Magdy Ali   Read full review ⬈

Network & Security Section Head/Digital Transformation at City Edge

"The initial setup can be rated as a seven out of ten because it involves going into the console and ensuring that the network settings are correctly configured.."

Verified user   Read full review ⬀

IT Engineer at Cellfind (Pty) Ltd.

"Deploying Darktrace is quite easy and plug and play, wherein all we need is to put it in a data center, rack up, and do some switch configuration. The learning would take a week time, and once the data gets populated, we get a very good dashboard.."

Anil M   Read full review ⬀

Technical Consultant - Unix Platform Services at BITS AND BYTE IT
CONSULTING PVT LTD

"The initial setup can be rated as seven out of ten. The main challenge was time as the system takes about three to six months to learn the network before it becomes fully effective.."

Peter-Murphy   Read full review ⬀

Head of Technology Operations at Pobl Group

The initial setup process for Darktrace is complex because I need a network technician or engineer to configure the span port on my core switches, and I need assistance to choose which VLANs I want to ingest traffic from. Beyond that, everything is easy; the management of Darktrace is quite easy. Making exclusions is easy, and investigating within the platform is quite easy. However, the initial setup becomes complex due to the requirement of getting someone to create the span, and needing a dedicated span for Darktrace on the switch.

Malebo Lethoba Group   Read full review [↗]
Security Analyst at a healthcare company with 10,001+ employees

Customer Service and Support

The technical support from Darktrace is very good, including support from their resellers. We worked with Grove, who are with 360 Integrity now, and they are quite good.

Malebo Lethoba Group   Read full review [↗]
Security Analyst at a healthcare company with 10,001+ employees

I would rate it a nine. The challenge lies in waiting for a response after logging a ticket. Sometimes it requires back-and-forth responses before having an actual conversation with technical consultants via calls or video conferencing.

ChristopherMangava   Read full review [↗]
Group Cybersecurity Administrator at Tharisa

"The support provided by Darktrace is very good. We had issues with Darktrace Mobile, and they assisted us with a solution, even allowing us to test new features.."

Verified user   Read full review [↗]
IT Engineer at Cellfind (Pty) Ltd.

"Darktrace provides excellent technical support with a monthly meeting to review platform incidents, ensuring the system functions as expected. I would rate their customer service at nine out of ten.."

Peter-Murphy
Head of Technology Operations at Pobl Group

Read full review ↗

"Technical support is good. They always coordinate with the CISO. If any of the sensors are down, they immediately notify the CISO, since I work via the CISO as well as the chief security architect for the entire organization.

At any moment the sensors are down or the availability of our monitoring solutions are not reachable to their security backend team, their support team immediately notifies us. Their customer support is very helpful.."

Manjunath_P
CISO at Interplex Electronics Malaysia Sdn. Bhd.

Read full review ↗

"I can rate Darktrace's technical support as one of the best products in the world. We have seen satisfaction reflected on our customers' faces after deployment when they start seeing the data and the dashboard, and they often express surprise at the network traffic visibility that Darktrace provides.

"I would rate the technical support of Darktrace between 6 to 8, as the support is good and we receive timely assistance whenever we raise an issue.."

Anil M
Technical Consultant - Unix Platform Services at BITS AND BYTE IT
CONSULTING PVT LTD

Read full review ↗

Other Advice

I would recommend Darktrace and rate it a nine. I have not evaluated many other competitors, other than LinkShadow, considering our budget constraints.

ChristopherMangava   Read full review ↗
Group Cybersecurity Administrator at Tharisa

I would 100% recommend Darktrace. The product is autonomous, detecting and preventing threats effectively, unlike many competitors that are stuck only at detection. The visuals and the conceptualized views for connections greatly assist in threat analysis. My rating is eight out of ten.

Verified user   Read full review ↗
Security Information & Incident Analyst at a financial services firm with
1,001-5,000 employees

"For new users of Darktrace, it is important to be patient and set up the system properly. Follow Darktrace's advice throughout the setup process, which is crucial for effectiveness. Overall, I rate Darktrace at eight out of ten.."

Peter-Murphy   Read full review ↗
Head of Technology Operations at Pobl Group

"We are using the latest version of Darktrace. I have not used Darktrace's

Enterprise Immune System. Antigone is the feature of Darktrace that we have recently experienced. At the moment, I have not encountered a situation where Darktrace's self-learning capabilities reduced the risk of data breaches, but it performs very effectively overall. It requires some time to adapt; initially, when we deploy, it takes weeks. On a scale of 1-10, I rate Darktrace a 9.."

Anil M
Technical Consultant - Unix Platform Services at BITS AND BYTE IT
CONSULTING PVT LTD

Regarding the number of IPs monitored using Darktrace, they provide licenses that allow monitoring of around 16,000 IP addresses, and they give a buffer. Monitoring is possible for as many devices as long as they are in line with the traffic. However, devices that are not in line with the spanning won't be visible, which means there is no visibility.My recommendation for Darktrace would be based on the kind of network someone is running. If someone is running a network where they have dedicated layer two switches, I would most definitely recommend Darktrace as it's a good product. However, if someone is running in a shared environment where they share the layer two with other customers in that data center, then Darktrace wouldn't be suitable.For an overall rating, I would give Darktrace an eight out of ten.

Malebo Lethoba Group
Security Analyst at a healthcare company with 10,001+ employees

The Autonomous Response capability in Darktrace handles real cyber threats quite efficiently. The Autonomous Response is excellent at identifying phishing emails and suspicious emails accurately, and it automatically sends a response to users that certain emails were blocked by Darktrace, helping users identify whether it

was done correctly or incorrectly. If it was done incorrectly, the user can submit a request, and we can perform human analysis and then add it to a whitelist or blacklist.

In terms of AI functionality, I have seen some AI integrations overall. Darktrace is completely designed based on AI and machine learning, making it very efficient in identifying suspicious behavior and suspicious emails.

We are using the Securonix SIEM solution, and from ManageEngine, I use Help Desk and the Patch Manager.

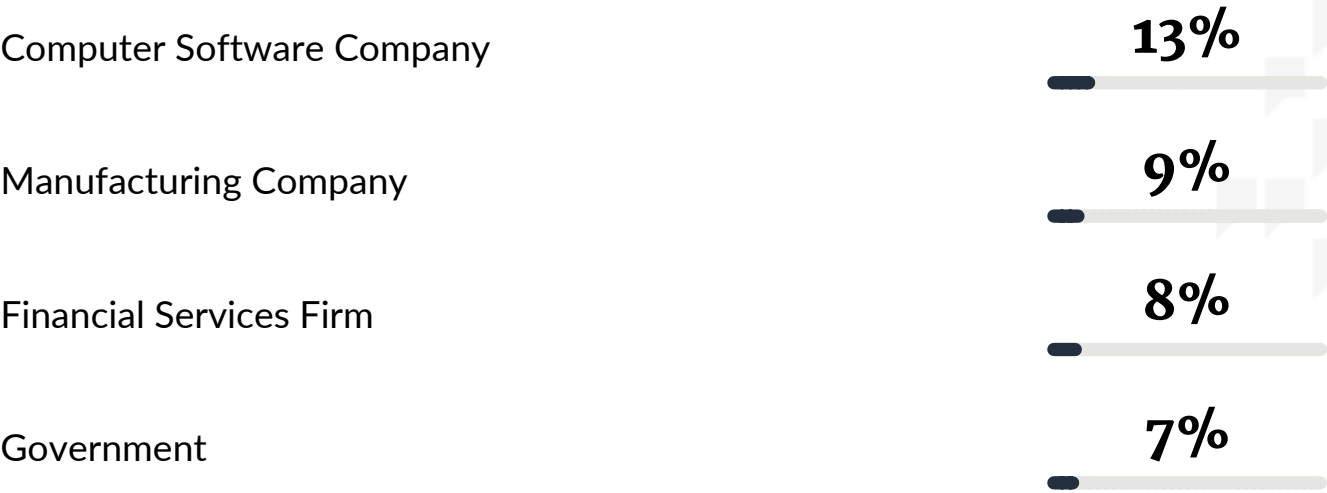On a scale from 1 to 10, I would rate Darktrace as six points. ."

Waleed Omar
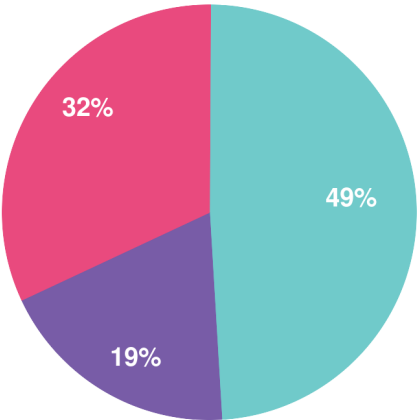Information Security Specialist at Arab Open University

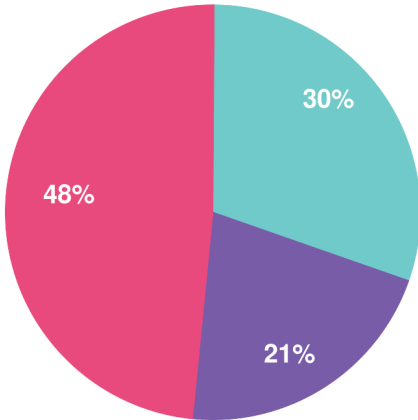Read full review ↗

Top Industries
by visitors reading reviews

Computer Software Company

13%

Manufacturing Company

9%

Financial Services Firm

8%

Government

7%

Company Size
by reviewers

by visitors reading reviews

32%
49%
19%

30%
48%
21%

● 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

PeerSpot

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

reports@peerspot.com

+1 646.328.1944