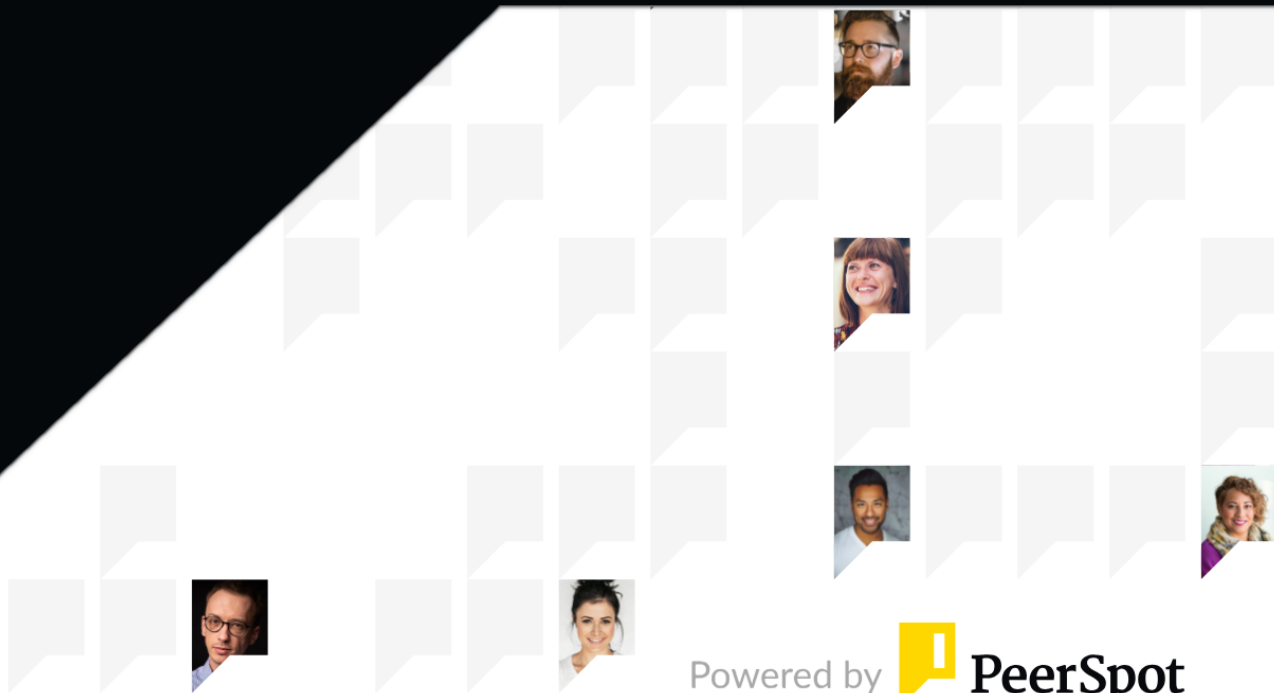




Trellix Helix Connect

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 13

ROI..... 14 - 15

Use Case..... 16 - 19

Setup..... 20 - 23

Customer Service and Support..... 24 - 26

Other Advice..... 27 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

Product Recap



Trellix Helix Connect

Trellix Helix Connect Recap

Trellix Helix Connect leverages automation with playbooks and AI, enhancing incident management, data correlation, and reducing response times while easing integration and improving threat visibility.

Trellix Helix Connect transforms cyber operations with automated workflows, cutting response times and decreasing analyst fatigue. Its ability to integrate seamlessly with existing infrastructures improves incident handling through advanced AI and data correlation techniques. Quick to implement, it enhances threat visibility, enabling faster incident triage, alert correlation, and threat intelligence integration. While the platform excels in these areas, users have noted areas for enhancement, such as integration with third-party tools, better dashboard functionalities, and reduced false positives. Despite concerns over licensing costs and connectivity issues, Trellix Helix Connect remains a valuable asset for centralized security event management and response automation.

What are the key features of Trellix Helix Connect?

- **Automation:** Uses playbooks and SOAR to reduce response times and analyst fatigue.
- **AI Integration:** Enhances incident handling and data correlation.
- **Quick Implementation:** Compatible with existing infrastructures for easy integration.
- **Threat Visibility:** Improves incident triage and threat intelligence integration.

What benefits or ROI should be considered?

- **Reduced Response Times:** Streamlines alert management with rapid automation.
- **Analyst Efficiency:** Alleviates fatigue through automated workflows and data handling.
- **Improved Security:** Enhances threat visibility and incident management capabilities.
- **Cost Efficiency:** Offers a comprehensive threat management solution despite licensing concerns.

Organizations rely on Trellix Helix Connect for centralized correlation and security event management, integrating it with existing tools for streamlined alert management and enhanced cybersecurity measures. It supports tasks like phishing detection, data protection, and endpoint security, essential in industries facing persistent network threats, including managing logs, detecting malware, and automating responses, reducing investigation times and improving notification efficiency.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“The pre-built rules and analytics save us a lot of time and have positively impacted my team's workflow because whenever we migrate to a new tool, we basically have to sit for months to form the rules and alerts.”



Validated user

Associate Cybersecurity Analyst at a tech vendor with 10,001+ employees



“We estimate that security investigation and incident response activities are approximately 40 to 45% faster compared to before implementing Trellix Helix Connect.”



Hitesh Singh Thakur

Mentor Operations at eClinicalWorks



“In general, I can say that Trellix Helix Connect impacted my organization positively.”



Melih Karasu

Director at Natica IT Consulting



“Trellix Helix Connect is the overall complete cybersecurity solution, covering all aspects in one package, which is why I prefer it for cybersecurity.”



Sheikh Abdul Hannan

Technical Manager at Jlogic Innovations



“The features that I find most valuable in Trellix Helix Connect are the incident response capabilities, which include EDR and XDR, along with the SoC capabilities added in the new advanced Trellix AI intelligence.”



Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd



“Trellix Helix Connect has positively impacted my organization as it is the most important tool to provide MDR service to our clients, which has resulted in specific outcomes and improvements.”



Validated user

Presales Lead at a outsourcing company with 11-50 employees



“Trellix Helix is an excellent product that I would advise others looking into using for the first time because FireEye provides documentation on setup and how to create queries, and they also have a YouTube channel explaining all involved queries, and I have not found anything lacking in the training for implementation.”



Sourabh Pardhi

Senior Information Security Analyst at Everbridge

What users had to say about valuable features:

“The area I found to be of value is the file rate capability in Trellix Helix, which is the primary feature I appreciate. For example, if we received any traffic, I could obtain a PDF file that could be analyzed in the EDR tool of FireEye. I have used multiple tools after that as well, but none of them have the same capability. If you obtain the PKS, you will not be able to analyze it, so that is the major thing I appreciate..”

Sourabh Pardhi

Senior Information Security Analyst at Everbridge

[Read full review](#)

“Correlating the alarms is the priority for us, and Trellix Helix Connect was capable of doing that, and we were happy for this feature because we connect some third-party resources as well. We are not only using Trellix products but also other third-party firewalls and other security tools.

It helped streamline our incident management by reducing our investigation time; not extremely, but it helped..”

Melih Karasu

Director at Natica IT Consulting

[Read full review](#) 

“The main advantage of Trellix Helix Connect is the vast integration with over 4,000 applications. This extensive support for integration is a major advantage of this product.

“Trellix Helix Connect easily integrates with Office 365 and also integrates well with FortiGate, Palo Alto, and Barracuda, especially within AWS environments..”

Sheikh Abdul Hannan

Technical Manager at Jlogic Innovations

[Read full review](#) 

“The best features Trellix Helix Connect offers are centralized visibility, security event correlation, threat intelligence integration, automated workflow, and incident investigation capability.

“The most valuable feature out of those is security event correlation because it helps connect information from multiple security tools and provides better context for our investigation.

“Trellix Helix Connect has positively impacted our organization by improving our threat detection capability, reducing investigation time, and providing better visibility across our security environment.

“We estimate that security investigation and incident response activities are approximately 40 to 45% faster compared to before implementing Trellix Helix Connect..”

Hitesh Singh Thakur

Mentor Operations at eClinicalWorks

[Read full review](#) 

The features that I find most valuable in Trellix Helix Connect are the incident response capabilities, which include EDR and XDR, along with the SoC capabilities added in the new advanced Trellix AI intelligence. These things are very important to all organizations.

Additionally, DLP is also very essential for our organization, as they are already using it. We are trying to introduce the Trellix layer security, but we still need some time to introduce all aspects to our own customers. We are working at our level best to achieve that.

“The customizable alerts and reports in Trellix Helix Connect assist my team in adapting security strategies. When using cloud sites with products such as EDR and XDR, you are not left with vulnerabilities, but when you are using third-party tools, you can analyze that your site is totally secured. This is something customers sometimes require. For example, with this type of report submitted to CrowdStrike, that product shows their reporting and sends the email to that customer particularly, and they are very happy about that. In Trellix, we need these types of reports where you are giving information for analyzing or reporting, and scanning shows that your site is very secure and you are using a high-level, advanced-level threat protection detection product. This type of report could sometimes be sent to the customer, stating that you are using it and you are totally secure. This would be helpful for us. .”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[Read full review](#) 

“The best features Trellix Helix Connect offers are that it provides readily available connection and the speed of deployment. It comes with a set of pre-built rules, integrations, and analytics which eliminate months of hard work and research that we have to do on the rule-making part. Trellix Helix Connect is also easy to implement and integrate as both come from the same parent company. With the existing data sources, we can connect it, and it also has many connectors and over 490 third-party connectors which help us get prioritized AI-guided responses. The GenAI triage, which used to be called Trellix Wise before, is now accessible to both current and new customers. This GenAI-powered alert triage helps us in the automation of triaging the detections.

“The pre-built rules and analytics save us a lot of time and have positively impacted my team's workflow because whenever we migrate to a new tool, we basically have to sit for months to form the rules and alerts. Trellix Helix Connect provided a very ready-to-go data source with connectors, which made it easy for us to implement the things from the start. It did not take a long time for us to set it up and launch into operations practically.

“Trellix Helix Connect has positively impacted our organization by helping us quarantine and un-quarantine files and manage our full asset inventory. We can watch every host and what is happening with them, whether the host is being deleted, onboarded, or off-boarded. It has also helped with our monthly reviews and the reports through which we can observe the types of malware affecting us, the malware that is not impacting us anymore, and the trends in malware activity..”

Validated user[Read full review](#) 

Associate Cybersecurity Analyst at a tech vendor with 10,001+ employees

Other Solutions Considered

“Before Trellix Helix Connect, we relied on multiple monitoring and log management tools that lacked centralized correlation and visibility, but after Trellix Helix Connect, everything was centralized..”

Hitesh Singh Thakur

Mentor Operations at eClinicalWorks

[Read full review](#) 

“Because of the budget, we are not using any XDR right now.

We stopped using FireEye Helix six or seven months ago.

I only used Trellix XDR, Helix Connect before Trellix Helix Connect..”

Melih Karasu

Director at Natica IT Consulting

[Read full review](#) 

“I worked with a customer that had a McAfee EDR from Kaspersky and another vendor's NDR. They faced many issues, and eventually, they paid much money for little value.

The main competitors are CrowdStrike and Fidelis. In terms of customers, they don't have a problem with cloud connection. We will put CrowdStrike as the first competitor because of customers' worries about the cloud connection. Most of the POCs I saw were Fidelis and Trellix, or Cortex, against Linux. I see these two at customers all the time..”

KarimBondok

Cyber security team lead at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“I am currently also working with Microsoft, Kaspersky, and Symantec, along with Trellix Helix Connect.

“I also work with Kaspersky and Symantec because they are cheaper solutions, but Trellix Helix Connect is the overall complete cybersecurity solution, covering all aspects in one package. That is why I prefer Trellix Helix Connect for cybersecurity..”

Sheikh Abdul Hannan

Technical Manager at Jlogic Innovations

[Read full review](#) 

ROI

Real user quotes about their ROI:

“We have seen a return on investment with Trellix Helix Connect, and we can share relevant metrics as we reduce the MTTD and MTTR and have KPIs indicating our ROI..”

Validated user

Presales Lead at a outsourcing company with 11-50 employees

[Read full review](#) 

“We have seen a positive return on investment through the faster incident investigation and improved operational efficiency, as well as the reduced manual effort for security monitoring. Before Trellix Helix Connect, we were doing everything manually, but after that, it has become automatic, allowing us to save about 40 to 45% time and reduce operational inefficiencies..”

Hitesh Singh Thakur

Mentor Operations at eClinicalWorks

[Read full review](#) 

“I have not seen explicit ROI metrics since that part was handled by the sales representatives of our company and the client's company. However, from an analyst's perspective, it has required fewer L2 operators since we already have a broader view of what is happening with the endpoint machines, which helps us form a verdict quickly and results in fewer employees needed..”

Validated user

Associate Cybersecurity Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

Use Case

“Trellix Helix was used to retain all logs, where I created multiple alerts based on organizational requirements. These alerts would trigger when conditions matched specific criteria. Multiple data centers shipped logs through Trellix Helix, and those data centers were monitored through the platform. These were the fundamental use cases I utilized..”

Sourabh Pardhi

Senior Information Security Analyst at Everbridge

[Read full review](#) 

“Trellix Helix Connect is typically used for monitoring hidden events, such as malware events that a normal team might not detect, including phishing attacks. This is the most powerful case of an XDR, enabling easy detection of phishing scams and malware events..”

Sheikh Abdul Hannan

Technical Manager at Jlogic Innovations

[Read full review](#) 

“Correlating the alarms is the priority for us, and Trellix Helix Connect was capable of doing that, and we were happy for this feature because we connect some third-party resources as well. We are not only using Trellix products but also other third-party firewalls and other security tools.

It helped streamline our incident management by reducing our investigation time; not extremely, but it helped..”

Melih Karasu

Director at Natica IT Consulting

[Read full review](#) 

“Our main use case for Trellix Helix Connect is centralized security monitoring, threat detection, security event correlation, and incident response, which helps us to collect and analyze security events from multiple sources through a single platform.

“One example of how I use Trellix Helix Connect for threat detection or incident response in my day-to-day work was when Helix correlated alerts from multiple security tools and identified a potential security incident that would have been difficult to detect by reviewing individual alerts separately, helping us investigate and respond much faster..”

Hitesh Singh Thakur

Mentor Operations at eClinicalWorks

[Read full review](#) 

“I have been using Trellix Helix Connect for about 1.5 years now.

“The main use case for Trellix Helix Connect is to see the detections and the endpoint results of the endpoints involved in those detections. For example, if a user generates an alert by doing something suspicious, we get the alert on Trellix EDR, and then we get a link to Helix Connect through which we can check the details about the user and their machine.

“Checking those details in Helix Connect helps me in my day-to-day work because, for example, if someone downloaded something that they were not supposed to download and we get a flag on the EDR, we see that person is the user on the EDR system and we go to Helix Connect to search out the username or maybe the hostname. We get the full device details, and from the device, we can contain the device, restrict the device, or delete that file from the device. We can also quarantine or un-quarantine the particular file based on the business needs of the company. This is how it makes it easier for us to mitigate things..”

Validated user

[Read full review](#) 

Associate Cybersecurity Analyst at a tech vendor with 10,001+ employees

I have been working with Trellix Helix Connect for a long period of time, almost nine years. I have worked on different products including Application Control, encryption, email security, EDR, XDR, and all the newly added products in Trellix.

The orchestrated workflows in Trellix Helix Connect have helped enhance my threat response. In the orchestration, we are getting the reporting site and an investigation report. If you are using DLP or XDR, we get the DLP report on the orchestrated platform. For SaaS-based EPO that is already in the cloud, customers have no hassle because all upgradations and products are upgraded automatically on the cloud side. However, for on-premises platforms, customers want different types of reporting. For example, if any incident happens, it instantly shows in the dashboard, and from this, we can get detailed reporting on that attack surface and incident report. I think if these types of things are added to the platform, it would be helpful for customers and for us. .”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[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 of Trellix Helix was rated nine and a half out of ten. Although no software is ever one hundred percent, my experience was good and easy to use. The installation process is simple with straightforward configuration.

Validated user

[Read full review](#) 

Senior Value Engineering at a tech vendor with 5,001-10,000 employees

“The initial deployment of Trellix Helix Connect is neither easy nor complex; I would rate it as medium because if you are a technical person familiar with antivirus and security products, you can handle it..”

Sheikh Abdul Hannan

[Read full review](#) 

Technical Manager at Jlogic Innovations

“If you understand the concept of Trellix Helix, it's easy to deploy.

It took a couple of days. We haven't integrated it with any solutions yet. We just have some minimal solutions that need to be integrated. If we have any issues in the future, we'll let you know.pen_spark.”

Kumaresan B

[Read full review](#) 

Senior Technical Support Engineer at Digitaltrack

“I found the initial setup to be easy; it was not difficult because we deployed it on multiple data centers. Creating the rules was also very easy, and it is a user-friendly tool. Initially, I struggled with it but later found it enjoyable writing the queries and getting the results.

The deployment for four data centers took a few hours; we had everything configured, but one data center was not receiving proper logs. We later found that there was an issue with the data center itself, but overall it did not take much time, so that was positive..”

Sourabh Pardhi

[Read full review](#) 

Senior Information Security Analyst at Everbridge

“When we undertake projects to install Helix, initially, our company had all the logistical information needed from the installation guide. However, there are details not included in the manuals that we sometimes discover only through direct communication with Trelix experts. This process has become more manageable over time, but initially, we encountered significant challenges, such as issues with connectors, which handle different log formats. These discrepancies weren't clearly outlined in the manuals and caused delays.

For instance, it took about a month to deploy components like SSO and group collection for our customer's infrastructure. Each deployment involves specialized roles—one focusing on connections and another on development and automation with CFA. With these two roles, we can effectively implement Helix..”

Daniel_Martins

Head of Management Security Services at NetSafe Corp

[Read full review](#) 

“The initial setup is very simple. Before we bought Trellix, we had some other competitors like Kaspersky and Fidelis. During the proof of concept (POC), we found it very hard to integrate in that situation.

And capability-wise, Fidelis is also big for enterprises, but the main issue was integration and management, especially that the appliance management of services is not that good.

On the other hand, Trellix has the SIEM appliance, which can create custom rules and make your EDR and NDR talk to each other and provide more enrichments and more insights into incidents, whether it is a true positive or false positive. But it's good to have, especially when we talk about EDR and NDR, it is very recommended to have both solutions from the same vendor to avoid any integration and configuration issues.

We primarily manage Helix software for API cloud. The appliances are physical and managed in the data centre. .”

KarimBondok

[Read full review](#) 

Cyber security team lead at a financial services firm with 1,001-5,000 employees

Customer Service and Support

The technical support for Trellix Helix is rated four out of five. Despite the ongoing transformation due to a fusion and merger of the company, the support could be better as there have been some challenges with staffing and information.

Validated user

Senior Value Engineering at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“The customer support is not very good, not that responsive, and not that fast either. We often wait for weeks to get a response from the engineering team due to a long relay process from customer representatives to the engineering team and then back to us..”

Validated user

Associate Cybersecurity Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“I would rate the technical support an eight from one to ten.

SLA times were okay for us; I cannot complain about anything for support. However, sometimes we can face some level one support engineers, at which point we had some problems..”

Melih Karasu

Director at Natica IT Consulting

[Read full review](#) 

“I had to contact technical support a few times when the data center went down or when I was not receiving the EPS count on the ADCs. Initially, when the product was deployed, it was difficult to get a response, but later the response time became very fast.

My experience with the support team was very good; they were cooperative and demonstrated good knowledge of how things worked. Excluding my first experience, I would rate their support team a nine..”

Sourabh Pardhi

Senior Information Security Analyst at Everbridge

[Read full review](#) 

“Earlier, the technical support from Trellix was not good, but currently, there has been very significant improvement in technical cases, and the responses are strong and very helpful.

“I assess the effectiveness of Trellix Helix Connect's threat detection capabilities as robust, making it more powerful than Trend Micro and other solutions like CrowdStrike. It provides detailed visibility reports and granular reporting..”

Sheikh Abdul Hannan

Technical Manager at Jlogic Innovations

[Read full review](#) 

“The support for Trellix Helix Connect is not satisfactory. We experience difficulties accessing personnel with deep knowledge of Helix. We have numerous tickets to understand and resolve problems. It is not an easy product to support on a daily basis.

“The support would rate a three out of ten. It can take one to four weeks to connect with someone who truly understands Helix and can provide solutions. This makes the product difficult to maintain..”

Daniel_Martins

Head of Management Security Services at NetSafe Corp

[Read full review](#) 

Other Advice

“Trellix Helix is an excellent product that I would rate a nine on a scale from one to ten, with ten being the best. I would advise others looking into using Trellix Helix for the first time that it is very good because FireEye provides documentation on setup and how to create queries. They also have a YouTube channel explaining all involved queries, and I have not found anything lacking in the training for implementation. Only the cloud part could be improved, particularly shipping logs and configuring the AWS or GCP console..”

Sourabh Pardhi

Senior Information Security Analyst at Everbridge

[Read full review](#) 

“My advice to others considering Trellix Helix Connect is to proceed only if you are getting competitive pricing; otherwise, it is nothing special and simply offers what many other connectors, such as CrowdStrike, Palo Alto, and Defender, already offer. Those options are far superior in terms of GUI and UI/UX standards. If you find competitive pricing that seems worthwhile, then proceed; otherwise, I would not recommend it. I gave this product a rating of 7 out of 10..”

Validated user

Associate Cybersecurity Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“The orchestrated workflows of Trellix Helix Connect enhance threat response by providing detailed reporting, integration dashboards, and detailed feature reporting through Trellix [ePolicy Orchestrator](#).

“I rate the technical support from Trellix an eight out of ten.

“I rate Trellix Helix Connect a nine out of ten as a product in general..”

Sheikh Abdul Hannan

Technical Manager at Jlogic Innovations

[Read full review](#) 

“Trellix Helix Connect's governance and security features provide strong assurance, ensuring that AI-driven insights and automated actions remain aligned with our organizational security policy.

“The accuracy and reliability of Trellix Helix Connect's AI capabilities are impressive, as the AI-driven insight and correlation have been accurate and reliable, helping our team prioritize threats and focus on the most important security events.

“My advice to others looking into using Trellix Helix Connect would be to integrate it with all major security tools and establish a clear incident response workflow to maximize the value of the platform. I would rate this product a 9 out of 10..”

Hitesh Singh Thakur

Mentor Operations at eClinicalWorks

[Read full review](#) 

“I can say that I was working with Trellix Helix Connect overall, and the product was great; on the other hand, the concept has changed a little bit. We do not have any issue with the product. I was okay.

I used the integration feature of Trellix Helix Connect.

We also use NX, network security, and email security appliances and solutions as well, so with the ecosystem, it was excellent.

I leveraged some reports, and I can say that is all.

In general, I can say that Trellix Helix Connect impacted my organization positively.

I tried to integrate with Check Point and also Symantec mail security product, Secure Mail Gateway, which were the most problematic vendors..”

Melih Karasu

Director at Natica IT Consulting

[Read full review](#) 

I do use the integration feature in Trellix Helix Connect. Trellix is now not only on-premises but also working on the SaaS base. In the SaaS-based EPO, we are integrated with the on-premise or SaaS base, and we are transferring the system to the SaaS base. Some clients are trying to transfer their system to the cloud and some are using that cloud DLP. The problem is with the DLP integration. Another product is Solidcore, which is related to [Application Control](#), [Change Control](#), and Execution Monitoring, and it is not properly integrated with the SaaS-based EPO. It is a main concern that we need proper integrations to the cloud services for Application Control, [Change Control](#), and integrity monitoring for Solidcore devices.

I can share that the efficiency improvement Trellix Helix Connect brought to my customer's security operations varies because for different customers, their expectations, design, and requirements are different. For example, banks have different requirements than customers on the medical side, such as pharmaceuticals. In some banking sectors, they want proper visualization, reporting, and a customized dashboard that can help them submit their report to higher authorities. On the other hand, if you consider the pharmaceutical sector,

they want total security where nobody can access and nobody can get any internal report or internal information. They want to secure their site. This is the difference between companies using it, as their requirements are totally different. Some use Application Control for ATM security for banks, but on the other hand, if you consider pharmaceuticals, they do not need any ATM security level of protection. They need high-level data protection as that is a high concern for them. Overall, the different products and their working capabilities are different, and customers want to get their organization secure in that way. I think penetration testing and other things could be added which would be helpful for customers for future reporting purposes, protection purposes, or detection purposes. My overall rating for Trellix Helix Connect is eight out of ten. .”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[Read full review](#) 

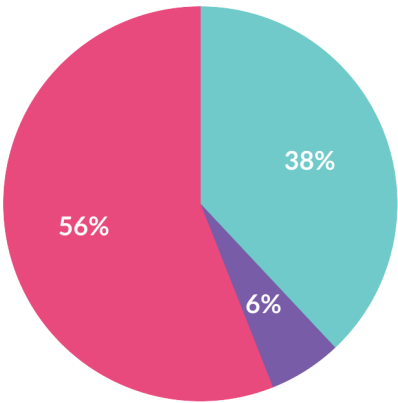
Top Industries

by visitors reading reviews

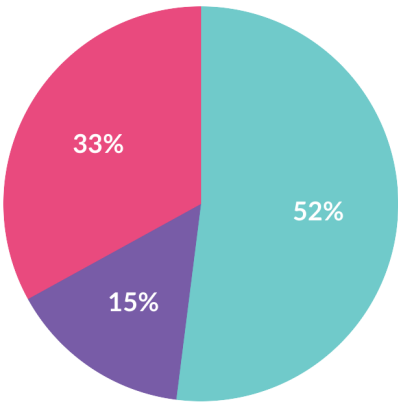


Company Size

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