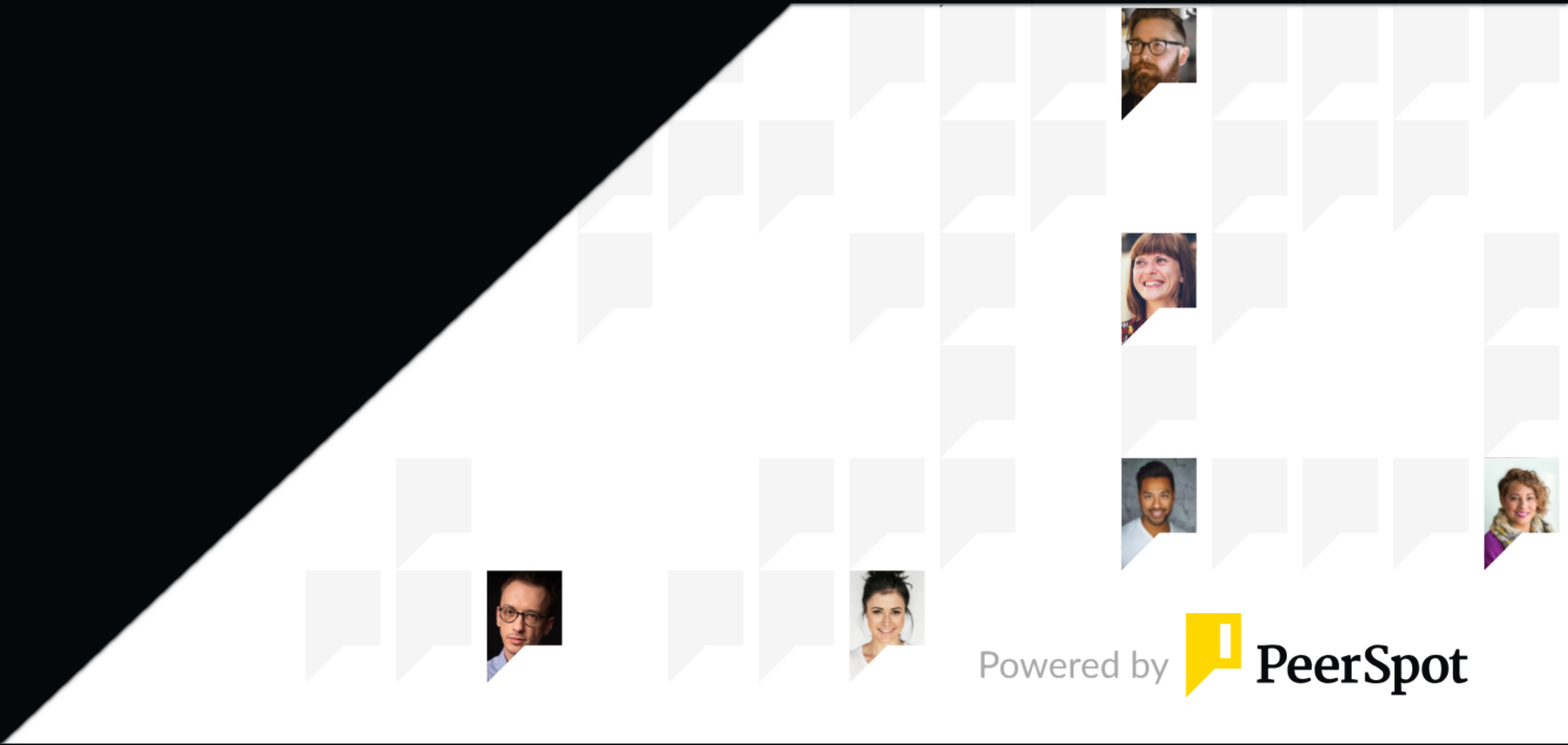
aws marketplace

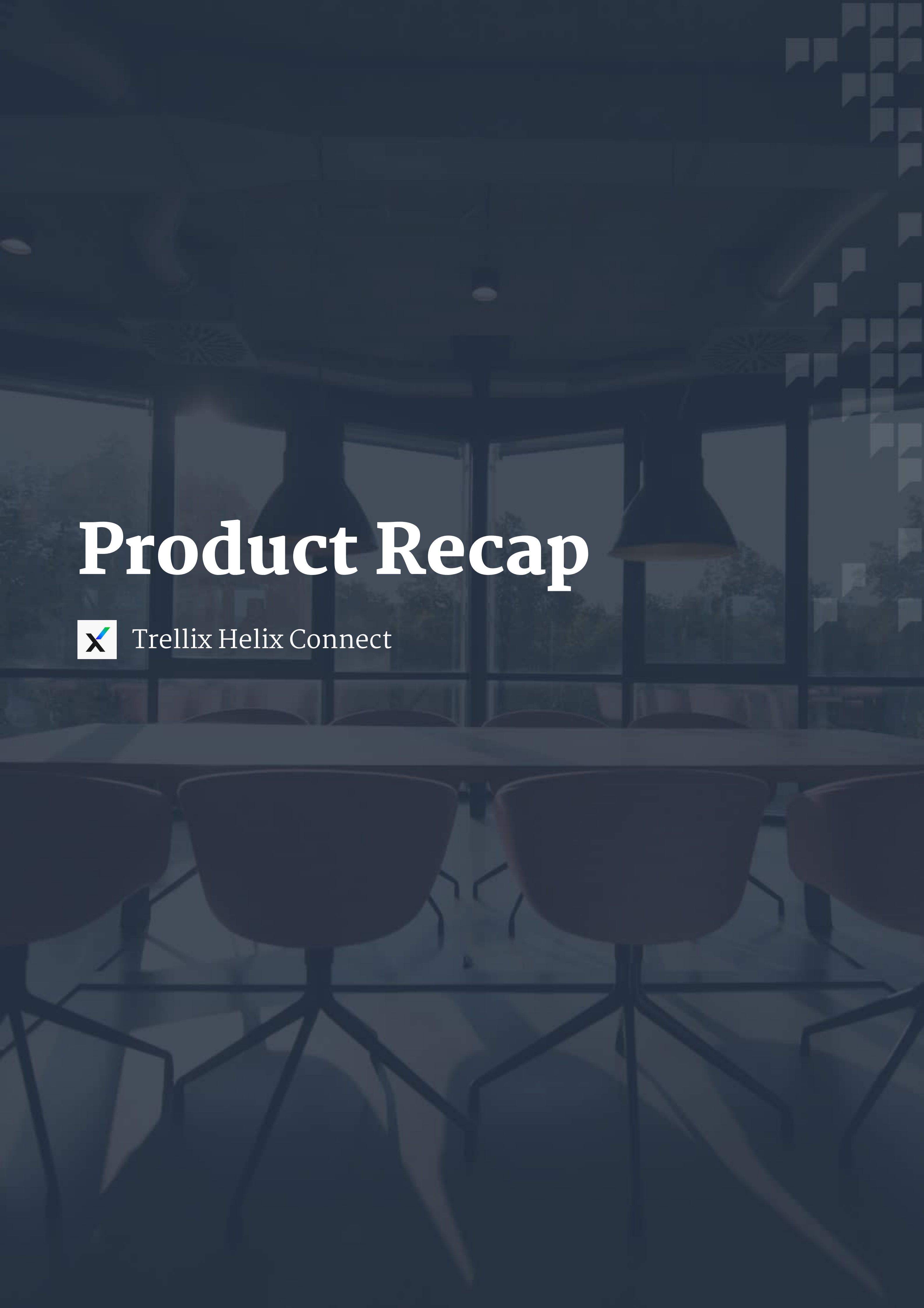
Trellix Helix Connect

Reviews, tips, and advice from real users



Powered by PeerSpot

Contents



Product Recap

Trellix Helix Connect

Trellix Helix Connect Recap

Trellix Helix Connect is known for its seamless API integration, automation capabilities, and efficient data correlation. It offers robust solutions in email threat prevention and malware detection, catering to cybersecurity needs with a user-friendly query language and extensive connector support.

Trellix Helix Connect integrates incident response, centralized SIEM tasks, and data correlation using native support for FireEye products. It rapidly handles alerts, enhances ticket management, and prevents network attacks. Its XDR platform supports a wide range of environments, providing DDI and IOC feeds for comprehensive data, email, and endpoint security. Users appreciate the deployment and API integration, but improvements in graphical interface and pricing could increase satisfaction. Additional infrastructure enhancements and optimized support can address current challenges resulting from recent mergers.

What are the key features of Trellix Helix Connect?

- API Integration: Simplifies data exchange with easy-to-use APIs.
- Automation: Offers strong automation for efficient threat management.
- Swift Deployment: Enables rapid setup in diverse environments.
- XDR Platform: Facilitates data correlation for comprehensive threat insights.
- Email Threat Prevention: Protects against phishing and email threats.
- Advanced Malware Detection: Identifies and mitigates complex malware.
- AI Capability: Boosts incident resolution with intelligent analysis.

Which benefits should users consider while evaluating?

- Improved Threat Detection: Enhances security with advanced threat prevention.
- Operational Efficiency: Streamlines incident response with automation and query enhancements.
- Scalability: Supports broad environments with over 400 connectors.
- Adaptability: Predefined use cases increase utilization efficiency.
- Cost Effectiveness: Potential for ROI with streamlined operations and integration capabilities.

Enterprises utilize Trellix Helix Connect for its ability to manage managed detection and response services, logging, and ransomware/ phishing mitigation. It operates efficiently in restrictive environments, enabling cybersecurity functions in industries requiring robust data, email, and endpoint security strategies.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “I advise other customers to choose Trellix Helix, as it improves operations significantly with more efficient responses required for various scenarios they face.”

Verified user

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

✓ “The best feature of Trellix Helix Connect is its quick implementation.”

Daniel_Martins

Head of Management Security Services at NetSafe Corp

✓ “As far as its core functionality goes, it’s spot-on.”

KarimBondok

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

✓ “We are able to block some advanced malware and other things.”

Kumaresan B

Senior Technical Support Engineer at Digitaltrack

✓ “The most valuable features include predefined use cases and threatening states.”

BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

✓ “We have started working with various customers, one of whom is particularly concerned about adjacency. We have identified several use cases where automation is possible.”

Daniel_Martins

Head of Management Security Services at NetSafe Corp

✓ “Trellix Helix helps prevent email attacks, like phishing and email spoofing attacks.”

Abanoub Alfy

Information Technology Security Analyst at EBC

What users had to say about valuable features:

“We are currently working with a provider where I need to send a lot of reports and queries to my customers. Instead, I create reports manually and provide customers with information about the solution..”

Daniel_Martins
Head of Management Security Services at NetSafe Corp

Read full review

“ The most valuable features include predefined use cases and threatening states. If I'm investigating a threat, I can run a query, and it'll suggest the next query I'm supposed to write. And they're making a lot of enhancements..”

BiswabhanuPanda
Senior technical consultant at Hitachi Systems Micro Clinic

Read full review

One of the most valuable features of Trellix Helix is its AI capability for the XDR platform, enabling me to reduce the time to resolve incidents. The software correlates data from the security environment and allows searches in natural language. It is crucial for enterprise companies worldwide, not just in the United States. Trellix Helix offers more than 400 connectors for integration and supports both small and large environments.

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

Read full review

“Enrichments. It's all about enrichments. Helix is a robust solution.

Helix, it's a good solution. Since management, I've been working with the team; I like the Helix ecosystem. .”

KarimBondok

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

Read full review

“We are able to block some advanced malware and other things. I think we use the appliance-based Helix.

It helps us detect some advanced malware. That's one of the major advantages. We also have some automated collaborations enabled internally. So, if there's a new attack or alert, we have visibility on it.

However, we are not experts in automation, but we do get some automation in the Trellix product. We want to test it further..”

Kumaresan B

Senior Technical Support Engineer at Digitaltrack

Read full review

“The best feature of Trellix Helix Connect is its quick implementation.

“The integration with Mandiant is another significant advantage. When investigating an incident, we have access to IOCs and can receive results from Mandiant about these IOCs, similar to what VirusTotal offers. We can search and utilize this integration effectively.

“We utilize the artificial intelligence capabilities in Trellix Helix Connect. We can perform some customization by providing parameters in the YARA from Helix, which provides valuable analysis points.

“The solution allows users to create reports more quickly with comprehensive information, which can be expanded within minutes. This demonstrates the effectiveness of Trellix Helix Connect's automation capabilities for reducing incident response times..”

Daniel_Martins
Head of Management Security Services at NetSafe Corp

Read full review

Other Solutions Considered

“Integrating anything on QRadar is very hard. If you want to upgrade the EPS you have to consider upgrading the appliance but with FireEye, if the customer has to compute, FireEye gives them a file to install on his computer and he can send the logs to my computer.

It is very easy to scale with FireEye. It can be upgraded to any number of EPS..”

BiswabhanuPanda
Senior technical consultant at Hitachi Systems Micro Clinic

Read full review

“We chose Trellix among the variety of products on the market because other vendors support cloud-based threat intelligence, requiring us to interact with the cloud.

With Trellix Helix, we have on-premises offerings and we are able to collaborate on our logs within our premises. We don't want to send data outside our organization because we support banking customers. We can maintain everything internally..”

Kumaresan B
Senior Technical Support Engineer at Digitaltrack

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

Use Case

I am a presales manager for a cybersecurity company, and I use Trellix Helix to manage software for cybersecurity. I sell software to enterprise customers, and my main use case involves data protection, email security, and endpoint security.

Verified user

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

Read full review

“We work for a company that provides secret services related to XDR and NSS. We offer the Helix solution to many companies in Brazil. We manage the implementation and provide solutions to our customers. We are a Helix service provider for ten companies in Brazil..”

Daniel_Martins

Head of Management Security Services at NetSafe Corp

Read full review

“The solution is typically used for sub-services, managed detection, and response services as well as advanced sub-services. The solution was managed by the company where I worked and we offered the services to the customer..”

Verified user

CTO & CISO at a tech vendor with 51-200 employees

Read full review

“We use it for everything like our logs, data allocation, and ransomware. We basically do malware objects and malware callbacks. I think it's our integration tool. It's our centralized SIEM where we look at all the events, alerts and then do a tryout. The major playbooks that we use are ransomware and phishing campaigns. We basically use it for our PTI-based credit card fraud detection. .”

Verified user

Sr Manager - Information Security & Researcher at a tech services company with 1,001-5,000 employees

Read full review

“We use Helix in a very restrictive environment that doesn't allow solutions to be connected to the cloud. Some solutions, like CrowdStrike and some XDR solutions, need to be connected to an external cloud. The same goes for Trellix, but with Helix, we have one option.

If we need DDI feeds or IOC feeds from vendors or customers, Helix will provide these IOCs via DDI push from Trellix to our side, even if we haven't faced any incidents..”

KarimBondok

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

Read full review

“We use Trellix Helix Connect because it is a SaaS solution. I think it has its own infrastructure rather than AWS or another provider. We use the Helix SaaS and a component called Evidence Collector that gets the logs from on-premise infrastructure and sends them to SaaS. I believe everything about Trellix Helix Connect is SaaS-based.

“We use Evidence Collector which can be installed with the on-premise infrastructure to collect components such as files and IPS. This product receives the logs from the infrastructure and sends the information to Helix..”

Daniel_Martins
Head of Management Security Services at NetSafe Corp

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.

Verified user

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

Read full review

“It is very easy to deploy. Most of its maintenance is automatic. We just get the notification that it is going to happen. So far, we haven't faced any issues..”

Verified user

SOC Services Manager at a healthcare company with 10,001+ employees

Read full review

“I won't say setup was difficult, but I would say that integration-wise, there are certain challenges regarding the passing of top logs. Providing and collecting the logs is easy and pushing the logs, but pulling logs is difficult in Helix.

We have a very large setup. So it took us around three or four weeks..”

BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

Read full review

“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

Senior Technical Support Engineer at Digitaltrack

Read full review

“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

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

Read full review

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.

Verified user

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

Read full review

"The customer service and support are very fast. Trellix's vendor support is excellent. They have responsive experts who can assist us without delay. We don't need to go through lengthy processes; our local support team handles Helix cases efficiently. For critical issues, they usually respond within thirty minutes to an hour. Overall, their professionalism stands out.."

KarimBondok

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

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

I advise moving quickly to adopt Trellix Helix to improve operations and get faster response times for incidents. I rate Trellix Helix overall ten out of ten.

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

Read full review

“FireEye Helix is best suited to enterprise companies. I recommend it as an easily implemented solution with a user-friendly web UI and good support. I'd give it a rating of seven out of ten..”

Verified user
Cyber Security Manager at a tech services company with 51-200 employees

Read full review

“I recommend Helix. I have a good experience with it. If I get a POC, I can easily give it to the customer and evaluate it.

The solution is stable and addresses advanced malware. It's also easy to access support in India.

Overall, I would rate it a nine out of ten. .”

Kumaresan B
Senior Technical Support Engineer at Digitaltrack

Read full review

“The solution can be challenging for analysts with lower skill levels. The syntax for finding findings requires specific knowledge, making it more difficult for initial users.

“Trellix Helix Connect is generally easy to use, but the Evidence Collector component presents more challenges.

“This review rates Trellix Helix Connect as 6 out of 10..”

Daniel_Martins
Head of Management Security Services at NetSafe Corp

Read full review

“I have numerous advantages with ten client customers who use our services. We have a dedicated team working directly with the Helix system at PeerSpot within our company, providing maintenance and generating reports for our customers.

The solution offers extensive platform visibility, event tracking, and integrations. While we explore other integration possibilities like CNA, we haven't found a comparable solution yet. Integrating with other vendors and multi-platform environments presents challenges, especially in ensuring API compatibility and staying current with integrations.

I strongly recommend Helix to our new customers for its capabilities and reliability.

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

Daniel_Martins
Head of Management Security Services at NetSafe Corp

Read full review

“I would give the product an overall rating of eight out of 10.

We have 10 people currently using this software. Six are on the list, plus two managers and two IR experts.

It's not possible for just one person to maintain the solution, and it's not really allowed. It has to be a team effort, with two or three people.

It's not about users. Helix works differently, collecting logs from 6,000 different sources integrated with the solution.

The licensing is not based on users; it's based on APIs. It's more of a SIEM SGL type of platform. It collects logs from around 6,000. But have around 10
people maintaining that..”

BiswabhanuPanda
Senior technical consultant at Hitachi Systems Micro Clinic

Read full review

Top Industries

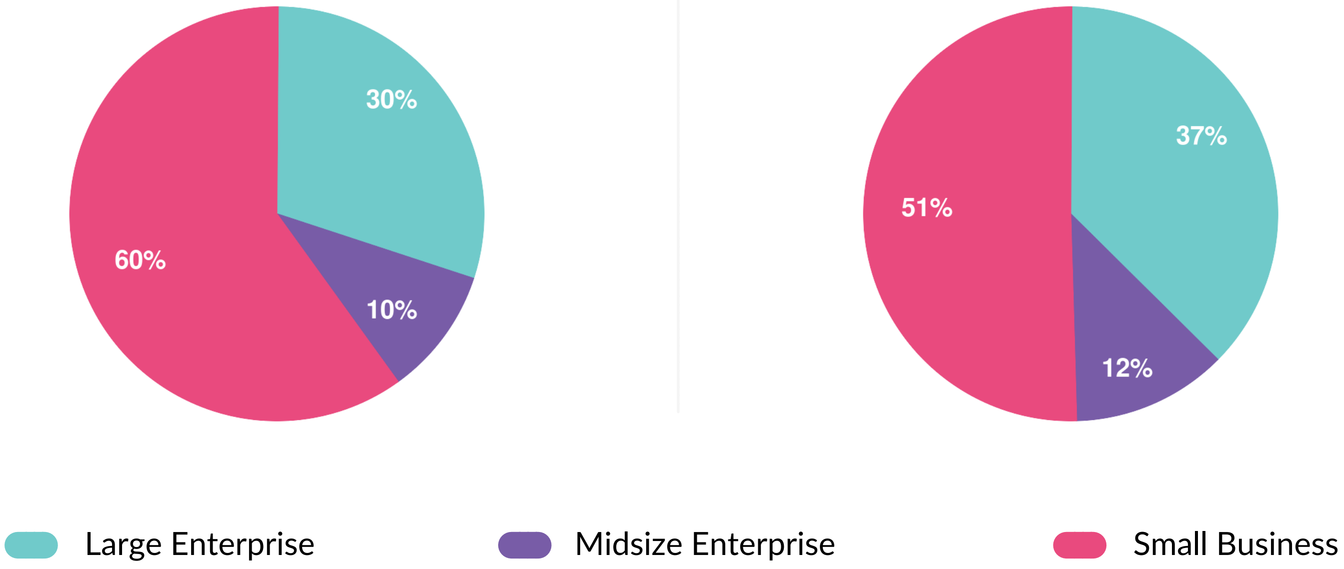
by visitors reading reviews

Comms Service Provider	18%
Manufacturing Company	13%
Computer Software Company	11%
Financial Services Firm	5%

Company Size

by reviewers

by visitors reading reviews



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