



Trellix Network Detection and Response

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 10

Other Solutions Considered..... 11 - 12

ROI..... 13 - 14

Use Case..... 15 - 17

Setup..... 18 - 21

Customer Service and Support..... 22 - 24

Other Advice..... 25 - 27

Trends..... 28 - 29

About PeerSpot..... 30 - 31

Product Recap



Trellix Network Detection and Response

Trellix Network Detection and Response Recap

Detect the undetectable and stop evasive attacks. Trellix Network Detection and Response (NDR) helps your team focus on real attacks, contain intrusions with speed and intelligence, and eliminate your cybersecurity weak points.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “We wanted to cross-reference that activity with the network traffic just to be sure there was no lateral movement. With Trellix, we easily confirmed that there was no lateral network involvement and that nothing else was infected. It helped us correlate the events and feel confident in our containment.”



BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

- ✓ “Trellix NDR provides an essential defense by automatically responding to network incidents that firewalls may not catch.”



Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

- ✓ “Over the thirteen years of using the product, we have not experienced a single compromise in our environment. During the COVID period, we faced numerous DDoS attacks, and the tool proved highly effective in mitigating these threats.”



Archie Scorgie

Information Security Senior Advisor at Eskom Ltd



“The installation phase was easy.”



YaserAljohani

OT/ICS Information Security Specialist at SANS



“Support is very helpful and responsive.”



Kumar_V

Senior Manager at a financial services firm with 10,001+ employees



“The sandbox feature of FireEye Network Security is very good. The operating system itself has many features and it supports our design.”



Hamada Elewa

System Engineer - Security Presales at Raya Integration



“The most valuable feature of the solution stems from how it allows users to do the investigation part. Another important part of the product that is valuable is associated with how it gives information to users in the form of a storyline.”



Verified user

information security at a insurance company with 201-500 employees

What users had to say about valuable features:

“Trellix Network Detection and Response helps increase response to attacks. One benefit is increased visibility and simplicity in maintaining it. AI analyzes and relates data based on past performance over the last five days. .”

Daniel_Martins

Head of Management Security Services at NetSafe Corp

[Read full review](#) 

“Trellix NDR provides an essential defense by automatically responding to network incidents that firewalls may not catch. When users break firewall rules, the solution identifies affected areas for immediate action, helping determine the actual reason for attacks. Its ability to report incidents like network paths makes it invaluable in securing the environment. With eight years of experience, I can attest that Trellix NDR is effective in detecting and protecting networks..”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[Read full review](#) 

“Over the thirteen years of using the product, we have not experienced a single compromise in our environment. During the COVID period, we faced numerous DDoS attacks, and the tool proved highly effective in mitigating these threats. The IP devices played a crucial role in blocking and reducing the amount of malicious traffic entering our company. Its endpoint security, EDR, and insights are valuable. The automation functionality, particularly the ability to automatically handle and mitigate detected threats, has proven to be immensely beneficial for our security operations..”

Archie Scorgie

Information Security Senior Advisor at Eskom Ltd

[Read full review](#) 

“The NTAP features are the most valuable aspects of the product. Other features, like ITS, are there, however, the primary value is in the NTAP protocols.

It is an easy product to set up.

The product has been quite stable.

Support is very helpful and responsive. .”

Kumar_V

Senior Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“There are sandbox capabilities. You can submit malicious files and great feedback, including if there is malware, what it is doing, et cetera.


The way it works is better than others thanks to the sandbox. It can give you simulations in different operating systems and applications and give your real insights from the perspective of a real environment. You gain insights into evasion techniques.

It's not just running in the background on an endpoint. You can do tests and learn. You can do behavior analysis. That's the main feature.

The solution can scale. .”

AmgadYousry

Head of Infrastructure at a tech services company with 11-50 employees

[Read full review](#) 

“The **in-depth investigation capabilities** are a major advantage. When the system flags something as malicious, it provides a packet capture of that activity within the environment.

That helps my team quickly identify additional context that most other tools wouldn't offer – like source IP or base64 encoded data. We can also see DNS requests and other details that aren't readily available in solutions like Check Point or others that we've tried.

The detection itself is solid, and their sandboxing is powerful.

There's a learning curve – you need a strong grasp of OS-level changes, process forking, registry changes, and the potential impact of those. But with that knowledge, the level of information Trellix provides is far greater than what we've seen elsewhere.

The real-time response capability of Trellix has been quite effective, although it's not very fast. The key is this solution's concept of 'preference zero.' They don't immediately act on a zero-day. For example, the solution has seen a piece of malware for the first time. It'll let it in, then do sandboxing. Maybe after four or five minutes, it identifies that specific file's DNX Secure Store as malicious. At that point, they update the static analysis engine, and it gets detected if anything else tries to download the same file.

There is that initial 'preference zero' concept, like with Panda. You may not hold traffic in the network. That's standard in the industry; we don't do much about it. To address that, we also have endpoint solutions. We use SentinelOne in our environment, which helps us identify threats like Western Bureaus and others..”

BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

[Read full review](#) 

Other Solutions Considered

“I have almost four years of experience in the area of cybersecurity, and I have used many EDR solutions before Trellix, like Kaspersky and Cybereason. My company decided to use Trellix Network Detection and Response..”

Verified user

information security at a insurance company with 201-500 employees

[Read full review](#) 

“Of course, we had to check all other products available in the market, research their features, and then we had to compare these products based on benefits to our clients, and the expected ROI. .”

Verified user

Sr. Network Engineer at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“We've used Forcepoint, NetFlow, SentinelOne, Trellix, Arista...some Splunk, and some Elastic as well. It's a mix of tools across different security domains.

These are all security-focused products. Security is my primary focus..”

BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

[Read full review](#) 

“I compared this product with something like MD, for example, Forcepoint.

It's about how you are using the solution. If you don't have a Forcepoint Next Generation Firewall proxy you shouldn't go for MD. You should go for FireEye. If you need to use MD, you need to have the other solution as well. It's not working as a standalone. It feeds from other solutions..”

AmgadYousry

Head of Infrastructure at a tech services company with 11-50 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I was with one of my clients last week and he told me that he's satisfied with the solution because they prevent a lot of attacks and a lot of breaches. .”

Antonio El Khoury

System Engineer at IRIS

[Read full review](#) 

“We see ROI in the sense that we don't have to react because it stops anything from hurting the network. We can stop it before we have a bigger mess to clean up..”

Verified user

Deputy Assistant Secretary with 201-500 employees

[Read full review](#) 

“We have seen ROI.

Because of what the FireEye product does, it has significantly decreased our meantime in being able to identify and detect malicious threats. The company that I work with is a very mature organization, and we have seen the mean time to analysis decrease by at least tenfold..”

Verified user

CEO at a tech services company with 1-10 employees

[Read full review](#) 

Use Case

“We use FireEye Network Security to secure the internet link. The solution works as an inline sandbox. Additionally, it can scan and monitor all uploads and downloads, and internet browsed links..”

Hamada Elewa

System Engineer - Security Presales at Raya Integration

[Read full review](#) 

“The solution can be used for detecting malicious traffic based upon known IOCs and it's integrated with the artificial intelligent speed, so we're able to recognize which IOCs are matching and their threat attribution..”

Verified user

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

[Read full review](#) 

“Our primary use case is for endpoint protection. We need the solution to integrate with the firewall so that we could get some threat intel based on the kinds of malicious factors that we are getting on the internet at work. We are working to optimize it with the firewall and the other tools we are using for network protection..”

Harneet Kaur

Information Security Consultant at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“We are using it from the perspective of data protection. We have two types of data that is coming. One is the actual data or the customer data that comes into our premises, and the second is the internet traffic that comes into our organization. FireEye devices scan all the traffic that comes through the tools on which we have configured FireEye, and they also analyze a lot of traffic..”

Verified user

[Read full review](#) 

Lead Program Manager at a computer software company with 10,001+ employees

“The primary use case for Trellix Network Detection and Response is network intrusion detection, which is crucial for protecting environments. It helps secure networks and defend against phishing and other attacks created by the networking sector. We use the solution for detection and forensics investigation, reporting incidents such as the source and network path of attacks..”

Abdullah Al Hadi

[Read full review](#) 

Information Security Engineer at Nhq Distribution Ltd

“The solution has been in place for quite some time – three or four years. We've renewed it several times, and we upgraded from Gen 3 to Gen 4 hardware at one point as well.

Currently, it's integrated with our firewall and McAfee IPS. We also have network-based sandboxing deployed. It uses static and dynamic analysis engines, so we get alerts if malicious traffic is detected or harmful objects are downloaded.

We've been using their PX solution for packet capture, which is the core of their NDR functionality. But we haven't fully adopted the combined product – NX and PX – yet because they are still separate.

The storage requirements for raw packet capture, especially with our traffic levels, make it quite expensive. And that's true for many security products. I feel like NDR is pretty expensive.

However, this is especially true about raw packet capture for network telemetry – the storage requirements with RAID 0 become quite expensive, regardless of the solution..”

Biswabhanu Panda

Senior technical consultant at Hitachi Systems Micro Clinic

[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. There is one template for location where we installed the virtual appliance and once that was up and running, it was fine. We had four or five people in the network team that set up the appliances..”

Verified user

[Read full review](#) 

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

“I rate the product's initial setup phase a seven on a scale of one to ten, where one is difficult, and ten is easy.

The solution is deployed on an on-premises model. .”

Verified user

[Read full review](#) 

information security at a insurance company with 201-500 employees

“The tool's integration with our existing security infrastructure was not difficult. Following the provided processes made the integration relatively straightforward. Its deployment was not difficult for us. We received support from Trellix professional services, which made the process smoother. The process took two months to complete. .”

Archie Scorgie

Information Security Senior Advisor at Eskom Ltd

[Read full review](#) 

“The product is plug-and-play so there is no complication regarding the setup of the solution. It's very simple and straightforward. I wouldn't describe the process as complex.

In terms of maintenance, only some support is required occasionally. You do not need a dedicated staff member constantly on the product to maintain everything. .”

Kumar_V

Senior Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“The installation phase was easy.

The solution is deployed on an on-premises model.

The solution can be deployed in a couple of days.

There are around 15 engineers in my company to take care of the product's deployment and maintenance areas..”

YaserAljohani

OT/ICS Information Security Specialist at SANS

[Read full review](#) 

“The initial setup was really straightforward. It took maybe a day to complete the upgrade.

We spent some time getting the prerequisites ready, which took a bit longer, but the actual deployment was very fast.

So you just identify the network where you want to connect it and just plug it in. It only took half a day.

Therefore, the preparation took some time, but the deployment itself was quick.

Handling upgrades:

We have a practice where network device upgrades take priority – starting with the App Firewall and working our way through Web Proxy and so on. We avoid parallel endpoint upgrades as we've had challenges with those.

Trellix releases sandbox system updates yearly, which are fine. Those don't require downtime. However, operating system upgrades are a factor.

We review KBR details thoroughly. Three or four months ago, we went from 9.1.4 to 9.1.5, and we're evaluating a possible upgrade to version 10, perhaps next month.

Generally, we follow the n-1 version strategy. But if there are significant new features in a release, we might upgrade sooner. Overall, it's manageable – we upgrade frequently, and this particular solution hasn't caused downtime issues. Plus, we use DNS-based global [settings/configuration?], so downtime isn't a major concern..”

BiswabhanuPanda

[Read full review](#) 

Senior technical consultant at Hitachi Systems Micro Clinic

Customer Service and Support

“In my company, if you face issues with Trellix Network Detection and Response or Trellix EDR, there is a separate team in my organization that offers technical support..”

Verified user

information security at a insurance company with 201-500 employees

[Read full review](#) 

“We handle the first-line support for Trellix Network Detection and Response on our own, performing troubleshooting and maintenance. For more advanced issues, we rely on Trellix Network Detection and Response's classic support as the third-line support..”

Archie Scorgie

Information Security Senior Advisor at Eskom Ltd

[Read full review](#) 

“The support from FireEye Network Security is not very good. Palo Alto and Fortinet have better support.

I rate the support from FireEye Network Security a six out of ten..”

Hamada Elewa

System Engineer - Security Presales at Raya Integration

[Read full review](#) 

“Technical support is rather good. But it's very restrictive, it's false of maintenance.

If you're don't authenticate it each month, you have to ask for another password and it's a little bit repressive..”

Philippe Panardie


RSSI at SDIS49

[Read full review](#) 

“Technical support needs improvement as sometimes engineers are not available promptly, especially during high-severity incidents. There is a need for technical expertise, specifically in device control and DLP issues..”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[Read full review](#) 

“The customer service and support are really good. Trellix offer multiple contact options – you can call and get immediate assistance from someone in Israel, Singapore, Japan, or even India. Plus, they offer chat support through Teams or Webex.

Trellix's documentation portal is also good..”

BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

[Read full review](#) 

Other Advice

“I was involved in the proof of concept. If someone requires the tool for their environment, they can use it. Overall, I rate the solution a ten out of ten..”

Mohd Fadhil

Security Engineer at Mavisco Resources Sdn Bhd

[Read full review](#) 

“Currently, I would rate Trellix NDR as an eight out of ten. There are various opportunities for improving its response capabilities and dashboard visibility to quickly address incidents, which could improve the overall effectiveness of the solution..”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[Read full review](#) 

“The product's response capabilities were good. In general, I can say that the solution's response capabilities are neither too good nor very bad, so I can place it somewhere in the medium range.

I rate the tool a five out of ten..”

Verified user

information security at a insurance company with 201-500 employees

[Read full review](#) 

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

Potential customers should definitely evaluate their specific use cases, budget, and commercial considerations. The product itself is good, there's no doubt. But it's essential to understand your use cases – then I'd definitely recommend it..”

BiswabhanuPanda

Senior technical consultant at Hitachi Systems Micro Clinic

[Read full review](#) 

“I am a deployment engineer. We are not using FireEye for ourselves. We are deploying it to our customers.

We are usually using the latest version since the database will be updated, and the images of the box itself will be updated regularly. It's always better in this kind of solution to have the latest update.

You can get it as a service provided by your cloud provider. With the on-premise, you will get the box, and each type of box has its deployment methodology or deployment technique. For example, if you are going to deploy the NX, you can make it online, and your networking can give it a motherboard from your switch.

I'd rate the solution nine out of ten. It's just a bit complex to set up..”

AmgadYousry

Head of Infrastructure at a tech services company with 11-50 employees

[Read full review](#) 

“Trellix Network Detection and Response has enhanced our organization's in-house capability in the area of threat detection.

Trellix Network Detection and Response worked very well in a scenario where it was used to help my company respond to a network incident efficiently.

The network detection and response capabilities of the product are the most valuable for our company's security operations.

The operation of the dashboards is not problematic in the product.

The network analytics feature of the product helps me in my daily tasks.

The product is user-friendly.

The product did improve my company's time to detect and respond to threats.

My company takes care of the maintenance of the product.

I rate the overall tool a seven out of ten..”

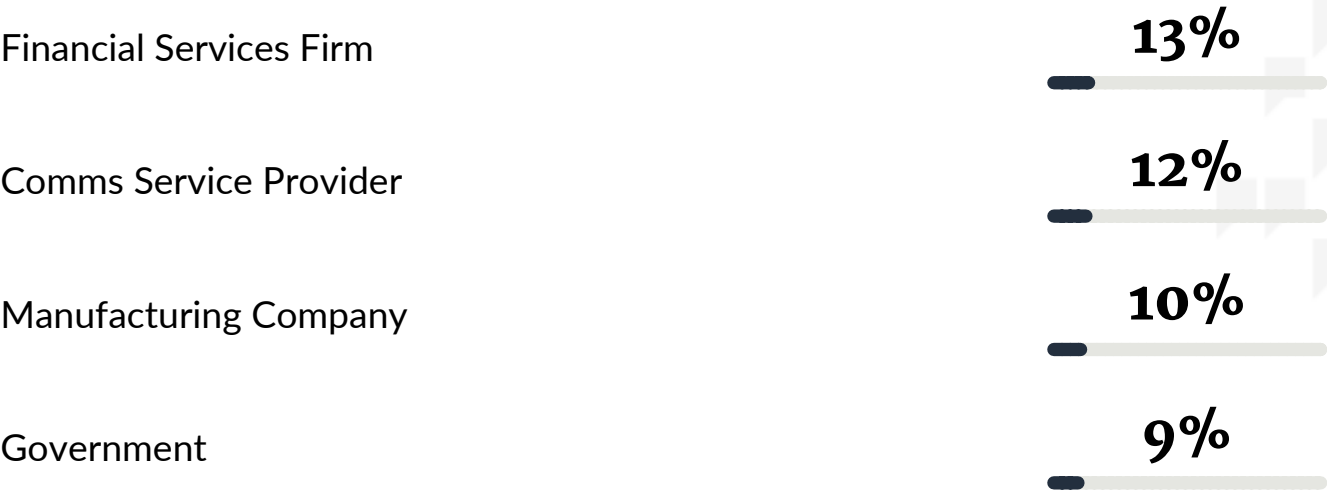
YaserAljohani

OT/ICS Information Security Specialist at SANS

[Read full review](#) 

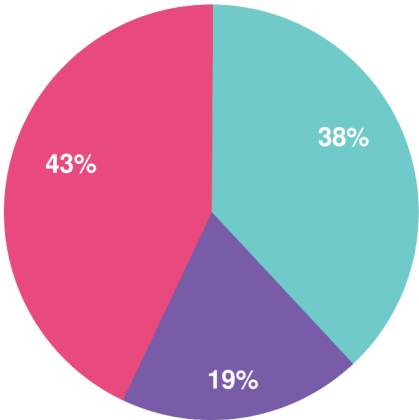
Top Industries

by visitors reading reviews

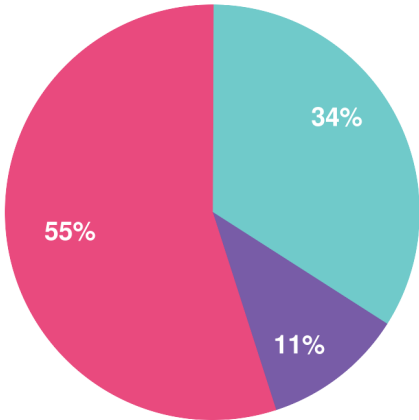


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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