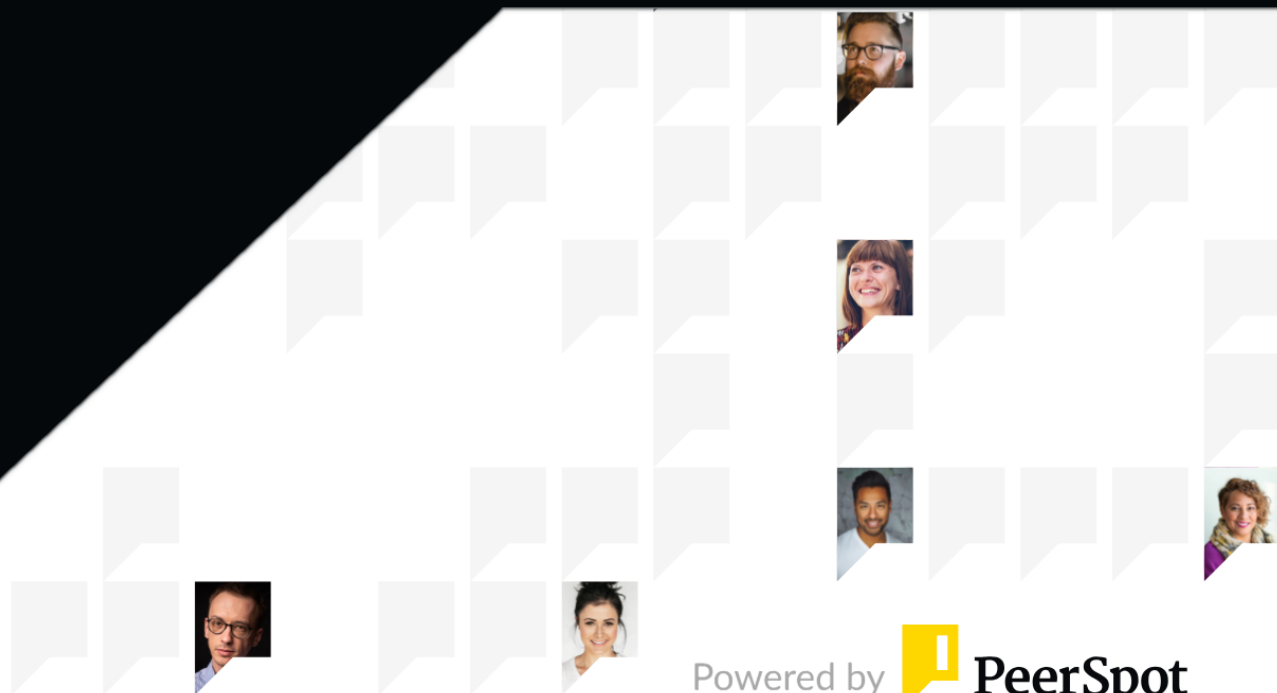




**Trellix Network Detection and Response**

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



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 16

ROI..... 17 - 19

Use Case..... 20 - 23

Setup..... 24 - 26

Customer Service and Support..... 27 - 29

Other Advice..... 30 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

# Product Recap



Trellix Network Detection and Response

# Trellix Network Detection and Response Recap

Trellix Network Detection and Response provides robust threat protection with advanced detection of zero-day attacks and APTs. Its user-friendly dashboard and real-time response capabilities enhance security and visibility across networks.

Trellix Network Detection and Response stands out with its MVX engine, leveraging virtual machines for comprehensive behavioral analysis. The solution supports detection of advanced cyber threats through features like sandboxing and application filtering, offering real-time response and packet capture for detailed contextual insights. Companies benefit from seamless integration with other platforms, enhancing usability and overall protection. User-friendly interfaces improve network visibility, while stability and ease of configuration safeguard against both signature-based and signature-less threats.

## What key features does Trellix offer?

- **Zero-Day Attacks Detection:** Identifies and mitigates unknown threats.
- **APTs Detection:** Detects advanced persistent threats through sophisticated techniques.
- **MVX Engine:** Uses virtual machines for behavioral analysis.
- **Sandboxing:** Adds a layer of threat protection.
- **Real-Time Response:** Offers immediate threat mitigation and context.
- **User-Friendly Dashboard:** Enhances visibility with application filtering.

## What are the benefits of Trellix Network Detection and Response?

- **Enhanced Usability:** Integrates easily with other platforms for seamless operations.
- **Detailed Context:** Real-time packet capture provides in-depth threat analysis.
- **Comprehensive Threat Protection:** Covers both signature-based and signature-less threats.
- **Improved Visibility:** Offers clear dashboard analytics for network monitoring.

Companies in sectors like finance, healthcare, and enterprise security utilize Trellix Network Detection and Response for tasks such as network intrusion detection, endpoint protection, and securing data transmission paths. It aids in threat investigations, pre-sales demos, and network forensics, reducing risks by protecting against cyber threats like phishing.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “We have seen several positive impacts since implementing Trellix Network Detection and Response, particularly in the areas of threat detection, intelligence, response, and operational efficiency.”



**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

- ✓ “Trellix Network Detection and Response offers excellent diversity and support for different capabilities because it is built and composed of different services.”



**Saja Matar**

CyberSecurity Architect at a comms service provider with 51-200 employees

- ✓ “Trellix Network Detection and Response has positively impacted my organization by addressing performance issues, specifically by offloading heavy traffic inspection and SSL inspection through sensors due to the limitations of the firewall.”



**Hassan Sheikh**

Network & Security Lead at Net-International



“Trellix Network Detection and Response definitely helps make investigations faster and more efficient.”



**Mahesh Malve**

Senior Business Development Associate at DigitalTrack Solutions ind pvt ltd



“The real-time alerts from Trellix Network Detection and Response reduced our average incident detection time from several hours to under thirty minutes, allowing the team to contain threats much faster.”



**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.



“Trellix Network Detection and Response has positively impacted my organization by significantly reducing the time to detect as we also were experimenting with the automation systems.”



**Verified user**

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



“Trellix Network Detection and Response has positively impacted my organization by creating a better safeguard and protecting us from threats.”



**Verified user**

Cyber Security Engineer at a retailer with 51-200 employees

What users had to say about valuable features:

“The best features I found most valuable in Trellix Network Detection and Response are anomaly detection, network traffic analysis, threat prioritization, and centralized visibility into security events.

“The most valuable feature for me in Trellix Network Detection and Response is network traffic analysis because it provides detailed insight into how devices communicate across the environment and helps identify abnormal patterns quickly..”

**Karan Pichlangia**

Assistant General Manager at Sunteck Realty Pvt Ltd

[Read full review](#) 

“The best features Trellix Network Detection and Response offers are real-time threat detection, traffic analysis, and the way it breaks down alerts in a clear and simple way.

“The feature we rely on the most day-to-day is real-time threat detection because catching a threat early makes a huge difference, and this product does that very well.

“Trellix Network Detection and Response has positively impacted our organization by making our security team more confident and responsible, knowing that the network is being watched all the time, allowing us to respond to threats much faster than we used to.

“Our team now responds to network threats much quicker than before, and we have managed to stop a few suspicious activities early that could have caused bigger problems..”

**Dhanaji Mali**

Technical Specialist at VDA Infosolutions Pvt. Ltd.

[Read full review](#) 

“Based on the scenarios I recently mentioned, one valuable feature is the real-time threat detection of Trellix Network Detection and Response. It detects advanced threats, malware, and lateral movement using AI, ML, and behavior analytics. This is where I used it in two different scenarios that I have mentioned earlier. Another feature would be the network visibility where it provides deep visibility across on-premises, cloud, branch, and hybrid environments. The last feature would be the lateral movement detection, which is particularly useful for identifying attackers moving between internal systems after initial compromise.

“Regarding business impact, the real-time threat detection successfully reduced our mean time to detect and response time. Instead of discovering threats during periodic reviews, Trellix Network Detection and Response alerts us immediately when it detects suspicious network behavior such as lateral movement or unusual outbound traffic. This allows the SOC team to investigate and contain incidents faster, reducing potential business impact and minimizing downtime. The key workflow benefits include faster threat detection, reduced manual monitoring, and better alert prioritization, which helps in quicker incident response and lower risk of business disruption. Both I and the organization have benefited from this.

“The real-time alerts from Trellix Network Detection and Response reduced our average incident detection time from several hours to under thirty minutes, allowing the team to contain threats much faster. Improved alert prioritization reduced manual triage effort by around thirty to forty percent, allowing analysts to focus on genuine threats. Each detection of lateral movement enabled containment before additional systems were affected, reducing the scope and cost of investigation..”

**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“Trellix Network Detection and Response offers excellent diversity and support for different capabilities because it is built and composed of different services. Trellix Network Detection and Response provides an all-in-one package with services such as Yara detection, Zeek detections, IPS, and IDS capabilities, all presented not as lazily implemented features but as standalone services that could be sold individually. The service that stands out the most for us is detecting and applying Riskwhere capabilities to see how our environment complies with standards, making it the full package for us. It supports compliance, security, and detection capabilities.

“Trellix Network Detection and Response allows for configuration of sandboxes, known as MVXes, which are separate standalone services that can be scaled up or down depending on your workload. For example, a smaller environment might only need one sandbox, while a larger one can set up a cluster of instances for sandboxing. It offers flexibility for inbound or outbound traffic by allowing you to set it inside the network to actively block or drop traffic, or simply mirror traffic for detection without prevention. The detection engine and services are powerful because they integrate different resources, enabling me to apply different integrations, such as Zeek integrations, for direct rule application.

“Trellix Network Detection and Response positively impacts my organization by providing an all-in-one package rather than requiring us to buy separate products from companies like FireEye or McAfee, which support different features. Multi-tenancy is critical for us as an MSSP, and Trellix Network Detection and Response's central management allows me to manage all appliances through a single UI, which is helpful despite some intricate configurations needing to be done on the appliance itself..”

**Saja Matar**

CyberSecurity Architect at a comms service provider with 51-200 employees

[Read full review](#) 

“Trellix Network Detection and Response definitely helps make investigations faster and more efficient. One of the biggest advantages is the visibility it provides into network activity, which allows me to quickly understand what happened and determine whether an alert requires immediate action. Instead of manually collecting data from multiple sources, I can use the platform to view relevant network communications, identify suspicious connections, and trace activity associated with a particular host or user. This significantly reduces the time needed for initial triage and investigations.

“Trellix Network Detection and Response has become a regular part of my daily security monitoring workflow, not just a tool I use when there is an incident. Beyond investigating alerts, I use it to maintain visibility into network activity, validate suspicious events identified by other security tools, and proactively look for unusual behavior that could indicate emerging threats. I also appreciate the context it provides during investigations. Having access to detailed network insights helps me make more informed decisions and collaborate more effectively with other teams when an issue needs to be escalated or remediated.

“The features I find most valuable in Trellix Network Detection and Response are the network visibility, threat detection capabilities, and the investigation tools that provide context around security events. One of the biggest strengths of Trellix Network Detection and Response is the ability to analyze network traffic and identify suspicious behavior that may not be obvious through traditional security monitoring. The alerting and detection capabilities help surface potential threats early, which allows us to investigate and respond more quickly. I also appreciate the level of detail available during investigations. Being able to view communication patterns, affected systems, and related activity in one place makes it much easier to understand the full scope of an incident. This saves time and reduces the effort required to manually correlate information from multiple sources..”

**Maresh Malve**

Senior Business Development Associate at DigitalTrack Solutions ind pvt ltd

[Read full review](#) 

“A few features of Trellix Network Detection and Response stand out for their particular value. First is the advanced threat detection capacity, which is very important. This platform uses behavioral analytics, machine learning, and threat detection to identify suspicious activity that traditional signature-based tools might miss. This is particularly useful for detecting zero-day threats, insider trading, and suspicious attacks. Secondly, I really appreciate the deep network visibility it provides.

“Deep network visibility has been one of the most valuable aspects of Trellix Network Detection and Response for our team because it allows us to see what is happening across the network in much greater detail than traditional monitoring tools. For example, we had a situation where there was unusual communication between an internal endpoint and an external server IP address. At first, the activity did not appear malicious because there were no adverse malware signatures or policy violations. However, using the network visibility provided by Trellix Network Detection and Response, we were able to communicate with partners, identify the affected device, review the timeline of events, and understand exactly how the traffic was moving through the environment.

“We have seen several positive impacts since implementing Trellix Network Detection and Response, particularly in the areas of threat detection, intelligence, response, and operational efficiency. One of the biggest improvements has been our ability to detect threats earlier. Previously, some suspicious activity might go unnoticed until it triggered an alert from other security tools or we discovered it during a manual investigation. With Trellix Network Detection and Response continuously analyzing network behavior, we can identify potential threats sooner and more effectively, which reduces the overall risk to our organization. We have also seen a noticeable improvement in incident response times because Trellix Network Detection and Response provides detailed context around alerts.

“Measurable improvements have been observed since implementing Trellix Network Detection and Response. For example, our mean time to detect and investigate security incidents has improved significantly. Before implementing the solution, analysts often had to gather data manually from multiple tools to understand the scope of the impact of an alert. The visibility and context provided

by Trellix Network Detection and Response have made that process much faster. Specifically, we have seen investigation times reduced by around thirty to forty percent for many security events..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

# Other Solutions Considered

“Before implementing Trellix Network Detection and Response, we used a combination of traditional network monitoring tools, which were signature-based in alerting and security controls but lacked the capabilities of a dedicated NDR platform..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

---

“When I joined this organization, we worked with Trellix Network Detection and Response only. I am not sure what they used before this, but I know why we switched. We switched because the existing system had poor visibility, high false positives, and limited ability to detect advanced or unknown threats, which slowed down detection and response. That is why we switched to Trellix Network Detection and Response..”

**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“We previously relied on a different solution for network monitoring and threat detection before Trellix Network Detection and Response. One of the reasons for moving to Trellix Network Detection and Response was the need for improved visibility, stronger investigation capabilities, and better integration with our overall security operations workflow. From my experience, Trellix Network Detection and Response provides valuable context around alerts and helps streamline investigations, which has improved efficiency for the security team..”

**Maresh Malve**

Senior Business Development Associate at DigitalTrack Solutions ind pvt ltd

[Read full review](#) 

---

“We evaluated several network detection and response solutions before selecting Trellix Network Detection and Response as part of our assessment process. We looked at platforms such as Cisco, Secure Network, and others that offered network visibility and threat detection. We wanted to compare their detection capacities, network visibility, investigation workflows, and the overall operational value. While all the solutions had strengths and positive aspects, Trellix Network Detection and Response stood out the most..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

“I was not directly involved in the formal evaluation and procurement process, so I cannot say with certainty which products were shortlisted or compared in detail before selecting Trellix Network Detection and Response. By the time I started working with the solution, Trellix Network Detection and Response had already been selected and deployed. From a user perspective, I have found it effective for network visibility, threat detection, and investigation support. While I am aware there are several strong solutions in the NDR market, I was not personally part of the product evaluation process..”

**Mahesh Malve**

[Read full review](#) 

Senior Business Development Associate at DigitalTrack Solutions ind pvt ltd

---

“I still run Corlight in parallel alongside Trellix Network Detection and Response. While Trellix Network Detection and Response limits access and navigation through alerts, making full investigations difficult, Corlight enables such investigations with customizable components including Suricata, Zeek, Yara, and smart Pcap features.

“We evaluated Corlight, which, while effective, necessitated extensive manual labor for setup, unlike Trellix Network Detection and Response..”

**Saja Matar**

[Read full review](#) 

CyberSecurity Architect at a comms service provider with 51-200 employees

# ROI

Real user quotes about their ROI:

“We have seen a positive return on investment with Trellix Network Detection and Response through the improved investigation efficiency, reduced manual effort, and faster threat identification..”

**Karan Pichlangia**

Assistant General Manager at Sunteck Realty Pvt Ltd

[Read full review](#) 

---

“I have seen a return on investment with Trellix Network Detection and Response, particularly in terms of time saved; since I manage the solution, I spend significantly less time on it..”

**Verified user**

Cyber Security Engineer at a retailer with 51-200 employees

[Read full review](#) 

“We have seen a positive return on investment, although it is sometimes easier to measure in terms of operational efficiency and risk reduction rather than direct cost savings. From an efficiency perspective, we have seen investigation and incident response times improve by thirty to forty percent within our operational team..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

---

“I have not seen a return on investment in terms of reducing employees, since Trellix Network Detection and Response actually necessitates more team members to operate it. However, it saves time by consolidating what would have been multiple setups with different providers. The setup was complex and time-consuming, yet once operational, daily use becomes much easier, though overall cost savings remain unclear due to their pricing lack of transparency..”

**Saja Matar**

CyberSecurity Architect at a comms service provider with 51-200 employees

[Read full review](#) 

“I do not have official ROI metrics, but from what I have seen, the biggest return has been in time-saving and operational efficiency. Investigations are generally faster because analysts have immediate access to relevant network context instead of manually piecing together information from multiple sources. I also think there is a value in detecting and understanding threats earlier. It is difficult to quantify exactly, but faster detection and response can help reduce the potential impact of incidents. While I cannot point to a specific dollar amount or reduction in staffing, the platform has helped the team work more efficiently and strengthen our overall security operation..”

**Maresh Malve**

[Read full review](#) 

Senior Business Development Associate at DigitalTrack Solutions ind pvt ltd

---

“If I consider the return on investment concerning Trellix Network Detection and Response, I mostly measure it by our time saving. Faster detection of threats, reduced mean time to detect and response time, and faster investigation using Trellix Network Detection and Response alerts have resulted in time savings. Analysts no longer need to perform extensive manual log analysis, so they can handle more incidents in less time. Regarding security cost, a reduction in security cost occurs because early detection prevents major breaches and avoids data loss, downtime, and recovery costs. Fewer false positives provide better alert accuracy, which reduces analyzing time..”

**Dhanesan Sridhar**

[Read full review](#) 

Decision Scientist 3 at Mu Sigma Inc.

# Use Case

“My primary use case for Trellix Network Detection and Response is network threat monitoring and incident investigation. I use it to identify suspicious network activities, detect potential threats, and gain visibility into traffic patterns across the environment. On a day-to-day basis, I review alerts generated by the platform, investigate unusual communications, analyze indicators of compromise, and validate whether an alert represents a genuine security risk or a false positive..”

**Maresh Malve**

Senior Business Development Associate at DigitalTrack Solutions ind pvt ltd

[Read full review](#) 

---

“Our main use case for Trellix Network Detection and Response is to maintain oversight of our network traffic and catch any threats or unusual activity as early as possible.

“Trellix Network Detection and Response runs in the background monitoring all network traffic, and whenever something unusual comes up, it sends us an alert and we look into it straight away without any delay..”

**Dhanaji Mali**

Technical Specialist at VDA Infosolutions Pvt. Ltd.

[Read full review](#) 

“My main use case for Trellix Network Detection and Response is to continuously analyze network traffic and identify suspicious activity that may indicate security threats. It helps us gain deeper visibility into network behavior and improve our overall threat detection capability.

“During routine monitoring with Trellix Network Detection and Response, the platform identified unusual communication between internal systems and external destinations. The activity appeared normal at first glance, but Trellix Network Detection and Response highlighted it as anomalous, allowing us to investigate and address the issue before it escalated..”

**Karan Pichlangia**

Assistant General Manager at Sunteck Realty Pvt Ltd

[Read full review](#) 

---

“My primary use case for Trellix Network Detection and Response is real-time threat detection, network traffic monitoring, and rapid incident response. I use it to identify malicious activity, prevent unauthorized access, and improve overall network security visibility across the organization.

“A practical example of how I have used Trellix Network Detection and Response in my daily work was detecting unusual outbound traffic from a user endpoint. The solution quickly identified the suspicious behavior, generated an alert, and helped us isolate the affected device before any data loss occurred. This significantly reduced investigation time and minimized the security risk..”

**Jatin Sharma**

Security Engineer at Digitaltrack

[Read full review](#) 

“A situation where I used Trellix Network Detection and Response is malware detection, where Trellix Network Detection and Response generated alerts for unusual outbound traffic from a user workstation. The investigation showed malware attempting to communicate with a known malicious IP. I isolated the endpoint and coordinated remediation with the endpoint security team. This is one of the major things that I worked on recently.

“Another use case would be lateral movement investigation. During a security incident, I used Trellix Network Detection and Response to analyze internal network traffic and identify suspicious RDP connections between multiple servers, which helped determine the scope of lateral movement. This helped me investigate further in detail using Trellix Network Detection and Response for lateral movement investigation..”

**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“Our primary use case for Trellix Network Detection and Response is to enhance network visibility and strengthen our threat detection capacity. We use it mainly for monitoring network traffic in real-time, identifying suspicious activity, and detecting advanced threats that may bypass traditional security controls. One of the key benefits for us is the ability to leverage behavior and machine learning for identifying abnormal activity, which helps to detect potential malware attacks and movement, command and control conversations, and other indicators of compromise at an earlier stage.

“One specific example was when Trellix Network Detection and Response identified unusually outbound network traffic originating from an employee's workstation. This activity did not trigger our traditional signature-based security tool because it was using legitimate protocols and appeared normal at first glance. However, Trellix Network Detection and Response detected the behavior and flagged the communication as suspicious. Our security team investigation and alert discovered that our endpoint had been compromised through phishing emails, and the attackers were attempting to establish command and control conversations and leverage across the network..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt 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.

“Regarding my day-to-day work with Trellix Network Detection and Response, it is simple; the implementation part has been completed, and now I just monitor the logs and check for any recent alerts or any critical threats that are detected, and I work on them..”

## Verified user

Cyber Security Engineer at a retailer with 51-200 employees

[Read full review](#) 

“My advice to others looking into using Trellix Network Detection and Response is to prepare for an initial time-intensive setup, as it has many features that require time to configure properly. However, once past the setup phase, operations will run smoothly with patience..”

## Saja Matar

CyberSecurity Architect at a comms service provider with 51-200 employees

[Read full review](#) 

“The experience with Trellix Network Detection and Response regarding pricing, setup cost, and licensing was that the implementation process was manageable, and the licensing model aligned well with our operational requirements. Overall, the value provided by the solution justifies the investment..”

**Karan Pichlangia**

[Read full review](#) 

Assistant General Manager at Sunteck Realty Pvt Ltd

---

“My advice for others looking into using Trellix Network Detection and Response is to take some time to set it up properly, fine-tune the alerts to suit your environment, and once that is done, it runs very smoothly and gives your security team a much stronger grip on what is happening across the network..”

**Dhanaji Mali**

[Read full review](#) 

Technical Specialist at VDA Infosolutions Pvt. Ltd.

---

“We purchased and deployed Trellix Network Detection and Response through Azure Marketplace by selecting the product and configuring the subscription and network settings, then deploying it into a resource group. After deployment, we integrated it with our environment for monitoring and security operations. This is the current approach we are following..”

**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

---

“Our experience with pricing, setup costs, and licensing has been positive. Trellix Network Detection and Response is an enterprise-grade security solution, so it represents a significant investment, but we believe that the value it provides in terms of threat detection, network visibility, and incident response justifies the cost. From a licensing perspective, the model was straightforward and aligned well with our organizational requirements. We were able to scale the deployment based on our environment and security needs, which gave us some flexibility based on the infrastructure involved. The initial setup required planning and coordination between our security and network infrastructure teams, but overall, it has delivered good value as part of our security product stack..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

# Customer Service and Support

“Customer support for Trellix Network Detection and Response is very excellent, as they provide thorough troubleshooting steps to overcome any technical issues..”

**Dhanaji Mali**

Technical Specialist at VDA Infosolutions Pvt. Ltd.

[Read full review](#) 

---

“Trellix Network Detection and Response cannot be operated without customer support, especially during the first year and a half of use. Their support is helpful, providing necessary training and sessions to understand the system better..”

**Saja Matar**

CyberSecurity Architect at a comms service provider with 51-200 employees

[Read full review](#) 

---

“Customer support for Trellix Network Detection and Response works as the first point of contact for users, and the support team handles technical issues and escalation to ensure problems are resolved efficiently..”

**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“The customer support for Trellix Network Detection and Response is very good. They help and support us promptly, allowing us to resolve issues immediately. I would rate customer support an 8 on a scale of 1 to 10..”

**Hassan Sheikh**

Network & Security Lead at Net-International

[Read full review](#) 

---

“Customer support for Trellix Network Detection and Response is good, providing me with accurate results or accurate troubleshooting.

“I would rate the customer support of Trellix Network Detection and Response an eight out of ten..”

**Jatin Sharma**

Security Engineer at Digitaltrack

[Read full review](#) 

“Overall, our experience with Trellix customer support has been positive. We have not needed customer support very frequently because the platform has been stable, but when we have reached out, the assessment has been generally good. Most of our integrations have involved resolving implementation guidance, configuration questions, product updates, and troubleshooting specific issues. In those situations, the support team was responsive and knowledgeable, and they were able to help resolve our problems within a reasonable time frame..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

## Other Advice

“Regarding Trellix Network Detection and Response's AI capabilities, I think the governance side is well thought out, keeping everything in check and ensuring that detection is handled in a controlled and secure manner.

“As for Trellix Network Detection and Response's accuracy and reliability of output, it has been quite accurate in the detection of real threats, and we have not seen any false alarms, so the alerts have been mostly relevant and actionable.

“I would rate this product overall as a 9..”

**Dhanaji Mali**

Technical Specialist at VDA Infosolutions Pvt. Ltd.

[Read full review](#) 

---

“Organizations should integrate Trellix Network Detection and Response with their existing security ecosystem and establish a clear investigation workflow to maximize the value of the platform.

“Trellix Network Detection and Response applies advanced analytics within a controlled security framework, helping organizations maintain visibility and governance while improving threat detection capability. In our experience with Trellix Network Detection and Response, the analytics and threat detection have been consistent and reliable. The alerts are generally meaningful and help us focus on high-priority security events.

“I would rate this product a 9 out of 10..”

**Karan Pichlangia**

Assistant General Manager at Sunteck Realty Pvt Ltd

[Read full review](#) 

“Instead of relying only on signatures, Trellix Network Detection and Response baselines normal network behavior and alerts on deviations such as unusual outbound connections, lateral movement, or command and control traffic. The specific feature impact would be behavior analysis to detect unknown threats and insider activity, and threat intelligence integration to identify communication with known malicious IPs or domains. The threat hunting tools help us find hidden or low and slow attacks missed by traditional tools. I recommend putting in reduction with tuning behavior analysis policies, leveraging threat intelligence feeds, and monitoring east-west traffic. This reduces false positives and helps identify suspicious activities such as lateral movement communications.

“My main advice regarding Trellix Network Detection and Response is to properly tune the system during initial deployment. Without tuning, you may get many false positives. It is also important to integrate threat intelligence feeds and align detection with MITRE ATT&CK so alerts are meaningful and easy to investigate. I have rated this product an eight out of ten..”

**Dhanesan Sridhar**

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

---

“Something unique for our environment regarding how we use Trellix Network Detection and Response is how it is implemented and managed. Because we use two appliances for network detection, one for users for everyday use and another for servers, we ensure they have separate traffic and can control and apply different controls to each appliance.

“For the flexibility of sandbox configuration in Trellix Network Detection and Response, it has helped my team day-to-day by matching our exact workload. For example, in the data center environment where we have a lot of traffic needing processing, we can add three or four MVXes for sandboxing capabilities, without having to mirror those configurations for the disaster recovery center, allowing each appliance its own sandboxing configurations. For compliance, the compliance

team checks network detection configurations, but there is no automation currently, though Trellix Network Detection and Response has a component called Riskwhere that performs risk assessments and covers configurations to benchmark our environment. However, it is important to note that Riskwhere still generates many false positives, requiring manual tuning to fit our environment.

“Regarding specific outcomes since using Trellix Network Detection and Response, the compliance scores have not improved yet since it requires manual configuration tailored to our needs. However, incidents have decreased because both solutions operate on a static basis, whereas Trellix Network Detection and Response utilizes sandboxes for dynamic analysis. It saves us a lot of time thanks to its central management, although some configurations sometimes conflict in application between central management and the appliances themselves. Trellix Network Detection and Response still needs more work for better unification of service management to clarify each service provided. The network detection component tends to have the most integrated services, featuring MVX, IPS, Malware Guard, and Smart Vision. I would rate this solution an eight overall..”

---

**Saja Matar**

CyberSecurity Architect at a comms service provider with 51-200 employees

[Read full review](#) 

“A quick specific example of how I use Trellix Network Detection and Response for threat detection and response is that I received a malicious file; some of my teammates downloaded a malicious file that contained a Trojan horse from a malicious website. Trellix endpoint was successfully able to detect it and also remove it, and it is installed in each person's systems across the organization.

“When I say the number of threats detected is getting less, I can share that around five to six months back, I was regularly getting a specific type of threat from the same zip file, which was spreading across the organization. The tool helped me find the root cause, which was an infected file stored in the server, and whenever someone accessed it, it used to spread to that system.

“I rated Trellix Network Detection and Response eight out of ten because the two areas where it can be improved are reporting, as the reports can be much better and easier to understand, and second, the support could be better. Due to these two areas, I deducted two points from the overall score.

“Regarding Trellix Network Detection and Response's AI capabilities, I think its governance and security are quite good; the AI is working fine, and I receive its logs and analysis, which makes me quite happy with this new AI and ML integration. It helps me in governance as well.

“The accuracy of Trellix Network Detection and Response is quite good.

“My advice for others looking into using Trellix Network Detection and Response is to be aware that the implementation part can be a lengthy process; endpoints are not installed in a day or a week, and it will take some time. Getting used to it takes around one to two months for the cybersecurity engineers managing the solution. I also recommend setting up logs and alerts on your emails so you do not have to open the dashboard daily, which helps save a lot of time.

“Trellix Network Detection and Response is a good mid-budget product that provides quite good security, and I have positive reviews about it..”

**Verified user**

Cyber Security Engineer at a retailer with 51-200 employees

[Read full review](#) 

---

“Trellix Network Detection and Response has become an integral part of our day-to-day security operations rather than just a tool we are using for major incidents. On a daily basis, our security team relies on it for continuous network monitoring, threat hunting, visibility, and security alerts. It provides valuable visibility into network activity across our environment, helping us identify unusual behavior that may indicate potential security risks. This proactive approach allows us to investigate and address issues before they develop into serious incidents.

“Another important aspect is integrating with our border security ecosystem. The alerts generated by Trellix Network Detection and Response complement data from our endpoints, [SIEM](#), and other security platforms, giving us a more complete view of potential threats. This improves investigation efficiency and helps reduce the time required for detecting, responding to, and managing security events.

“I would rate Trellix Network Detection and Response as nine out of ten overall.

“I choose nine out of ten because it delivers very strong value in areas that matter most to security operation teams, such as threat detection, network visibility, and investigation support. What stands out the most is its ability to detect suspicious threats that might not be identified by traditional security tools alone. Its behavioral analytics and machine learning capabilities, along with its network-level visibility, help uncover suspicious activity earlier, which is critical in today's threat landscape. Another reason for the high rating is the depth of context it provides during investigations when an alert is triggered. It also helps with a quick understanding of what happened in a system involved in suspicious activity across the network, thus reducing investigation time and enabling teams to respond more effectively.

“From a governance and security perspective, I think Trellix Network Detection and Response handles AI capabilities quite well. One thing I appreciate is that AI is used to enhance operations rather than replace human decision-making. The platform provides risk scoring and behavioral analytics, enabling abnormal detection and reconciliation while still allowing security teams to validate findings or make decisions. From a security standpoint, the AI helps identify threats that might otherwise be missed by traditional rule-based detection methods by analyzing network behavior and activity. It can uncover suspicious behavior earlier in the attack life cycle, which strengthens overall security posture and improves threat detection capabilities.

“Overall, the AI capabilities in Trellix Network Detection and Response have been both secure and reliable. In our experience, the platform consistently identifies suspicious behavior and potential malware attacks that warrant investigation. One of the strengths of the AI is its ability to analyze behavior patterns rather than relying solely on signatures or predefined rules. This helps it identify unusual

activity that may indicate a compromise, even when the threat is new or previously unseen. We have found that many high-priority alerts generated by the platform have also been related to actionable items with increased confidence. In terms of reliability, the platform has provided accurate insights during investigations. The AI's detection capabilities generally include context that supports the identification of suspicious activity..”

**Twinkle Solanki**

Business development executive at Digitaltrack solution Pvt Ltd

[Read full review](#) 

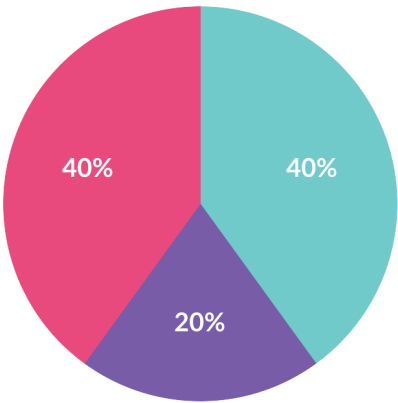
# Top Industries

by visitors reading reviews



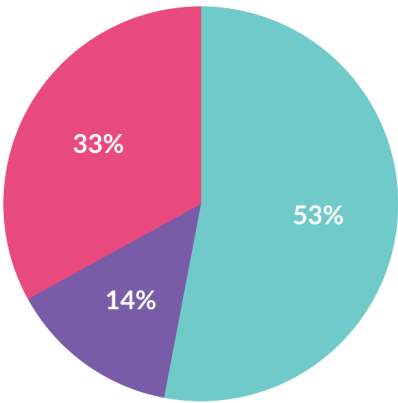
# Company Size

by reviewers



# Company Size

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](https://www.peerspot.com)

## PeerSpot

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

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

+1 646.328.1944