



**Trellix Endpoint Detection and Response
(EDR)**

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



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 14

Other Solutions Considered..... 15 - 16

ROI..... 17 - 19

Use Case..... 20 - 23

Setup..... 24 - 26

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

Other Advice..... 30 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



Trellix Endpoint Detection and Response (EDR)

Trellix Endpoint Detection and Response (EDR) Recap

Trellix Endpoint Detection and Response (EDR) offers advanced threat detection using AI-driven analytics, real-time monitoring, and integration with the MITRE Framework, enhancing security through comprehensive detection and response features.

Trellix EDR provides users with tools for threat hunting, powerful forensic capabilities, and intuitive dashboards. It integrates with diverse systems and supports cloud-based multi-site configurations, which facilitates a more robust security posture. With features like effective quarantine measures, behavior monitoring, and automation, it enhances operational efficiency. Despite its strengths, areas for refinement include better AI-driven threat analysis, improved resource efficiency, and faster processing times. Enhancing detection capabilities for unknown threats and improving integration with other tools can significantly upgrade performance and usability.

What features define Trellix EDR?

- **Advanced Threat Detection:** Leverages AI analytics for comprehensive threat identification.
- **Threat Hunting:** Empowers users to proactively search for threats.
- **Real-Time Monitoring:** Provides immediate insights into security incidents and status.
- **Integration with MITRE Framework:** Ensures thorough detection and response alignment.
- **Forensic Capabilities:** Offers tools for detailed investigation of security events.
- **Cloud-Based Support:** Facilitates configuration for multi-site environments.

What benefits can users expect?

- **Enhanced Threat Intelligence:** Improved detection capabilities for seamless integration with SIEM systems.
- **Operational Efficiency:** Automation and intuitive dashboards increase productivity.
- **Robust Risk Management:** Comprehensive protection against advanced threats such as ransomware.
- **Zero Trust Compliance:** Telemetry visibility aligns with compliance standards.

Trellix EDR is widely implemented in industries for endpoint protection and incident response. It helps protect workstations and improve threat intelligence by supporting integrations with cloud security and SIEM. Users benefit from its ability to identify malicious files and ransomware while adhering to zero-trust principles through improved telemetry visibility.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Trellix Endpoint Detection and Response (EDR) is valuable because we have a Wide Area Network with many sites, and the EDR is cross-site since it is installed and managed from the cloud.”



CESARCASTRO

Committee Of IT Cybersececurity at a energy/utilities company with 51-200 employees

- ✓ “Trellix Endpoint Detection and Response (EDR) has positively impacted my organization with threat exchange and intel, low false positive ratios, and very high uptime values for both inline and spam modes, along with advanced detection and mitigation capabilities ensuring the highest level of protection and proper detection for command and control and bot attacks.”



Validated user

Business Development Manager at a retailer with 10,001+ employees

- ✓ “Trellix Endpoint Detection and Response (EDR) scores highly because of its sheer depth of endpoint visibility, the precision of its behavior-based detection, and the massive time savings we get from its AI-guided investigations.”



Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

- ✓ “Trellix Endpoint Detection and Response (EDR) does everything; it saves time, it saves money, and of course, it provides peace of mind.”



Abubakar Bello

Security Administrator at a insurance company with 1,001-5,000 employees

- ✓ “Trellix Endpoint Detection and Response (EDR) has positively impacted my organization by improving visibility into security events on endpoints and servers, enabling the early detection of suspicious activities, reducing investigation times, and strengthening our monitoring processes and operational efficiency through analysis, Threat Hunting, and remote response.”



Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

- ✓ “My advice for others considering Trellix Endpoint Detection and Response (EDR) is to use it, or any other Trellix products, as I believe they are excellent.”



Ibrahim Mennanoglu

Senior Information Security Specialist at a consultancy with 51-200 employees



“Trellix Endpoint Detection and Response (EDR) has positively impacted our organization by improving overall efficiency, overall detection and response capabilities, and the capability to improve threat detections as well as the overall efficiency, time utilized, resource management, and analytic use cases review, significantly enhancing the business functionality.”



Vivek_Jaiswal

Security Engineer at LTI Mindtree

What users had to say about valuable features:

Trellix Endpoint Detection and Response (EDR) has a very low false positive rate compared to other products, thus increasing the SOC efficiency in how my team relies on the solution day-to-day.

With the best features Trellix Endpoint Detection and Response (EDR) offers, ease of SOAR integration helps to automate the IOC distribution, and our security team and management trust the product. Advanced detection capabilities ensure that targeted attacks will be detected and blocked before they arrive at our network.

“SOAR integration has assisted our security team and management in trusting the product. .”

Validated user

Business Development Manager at a retailer with 10,001+ employees

[Read full review](#) 

“First, it is user-friendly. Second, it works with a lot of products and many different versions of Windows. Third, the reporting module is very good. Because if you are using Endpoint Protection with ePO, it has a central console that is quite easy to manage all endpoints at a single dashboard. It has very good threat intelligence.

“In addition to the threat intelligence, it is easy to manage and granular. We can easily manage products up to the client level, and we know what is happening, then we do a lot of threat analysis. There are many resources that we can use. They also have very good support.

“Trellix Endpoint Detection and Response (EDR) has very good threat hunting capability. We can use the logs to see when a process starts and what it hits, and the other processes or services it has affected. This is quite encouraging..”

Abubakar Bello

Security Administrator at a insurance company with 1,001-5,000 employees

[Read full review](#) 

“The best features Trellix Endpoint Detection and Response (EDR) offers me are the management of all hosts from the EDR, allowing me to disable the network to a computer when necessary. I can check all processes and do what I want from the EDR tools, eliminating the need to physically go to the computer.

“I think the reporting part is the best feature of Trellix Endpoint Detection and Response (EDR), as it is very useful for reporting. The Trellix reporting site is easy to manage, with useful menus and a user-friendly interface.

“Trellix Endpoint Detection and Response (EDR) has positively impacted my organization by allowing us to protect our servers from malware and attacks, ensuring we can safeguard our clients. We can trust Trellix Endpoint Detection and Response (EDR) and conduct weekly or monthly scans to see what we have on our file servers and what clients save or download, including identifying malware behavior files. This is useful for us, providing a benefit where we can report and then take action..”

Ibrahim Mennanoglu

Senior Information Security Specialist at a consultancy with 51-200 employees

[Read full review](#) 

“The best features Trellix Endpoint Detection and Response (EDR) offers primarily include advanced threat detection, which utilizes AI-driven analytics and capabilities to identify and respond to threats. It continuously collects data from different sources to perform a comprehensive analysis to identify endpoints. Another key feature is its forensic capability, which captures critical data, files, memory, and processes running on the host, allowing it to quickly take action in terms of containment, investigations, and automated responses, including integration with MITRE ATT&CK framework.

“Out of the features I mentioned, I find myself relying on advanced threat detection the most because it quickly identifies emerging threats across the business and takes action in terms of detection as well as the response, also identifying the containment of devices, isolating devices, and taking IOCs blocking to the global organization level, which is enhanced by great forensic capabilities as well.

“Trellix Endpoint Detection and Response (EDR) has positively impacted our organization by improving overall efficiency, overall detection and response capabilities, and the capability to improve threat detections as well as the overall efficiency, time utilized, resource management, and analytic use cases review, significantly enhancing the business functionality..”

Vivek_Jaiswal

Security Engineer at LTI Mindtree

[Read full review](#) 

“The best features offered by Trellix Endpoint Detection and Response (EDR) include complete visibility on the endpoints, allowing real-time monitoring of activities, workstations and servers. Advanced incident investigation facilitates analysis through a process tree, timeline, and complete traceability. Another valuable feature is the detection of advanced threats, seeing beyond traditional signatures, detecting fileless malware and lateral movement. Threat Hunting allows proactive searches for indicators of compromise. Remote response allows an analyst to act quickly through isolation, termination of processes, and the integrations that the platform also has.

“Regarding features or any functionality that I consider especially valuable, the mapping to MITRE ATT&CK, the retention of historical telemetry, advanced behavioral detection, forensic capabilities, and centralized management can be noted. Trellix Endpoint Detection and Response (EDR) has positively impacted my organization by improving visibility into security events on endpoints and servers. The platform has also enabled the early detection of suspicious activities, reducing investigation times. Another of its capabilities is analysis, Threat Hunting and remote response, where we have strengthened our monitoring processes and improved operational efficiency. Additionally, as it is a SaaS platform, a management of security infrastructures has been implemented, allowing the team to focus on activities of greater strategic value and continuous protection..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“The integration capability through Trellix Endpoint Detection and Response (EDR) is seamless because we have installed native solutions that correlate endpoint data with threat intelligence. It effectively eliminates the usual noise and alert fatigue that plagues many SOCs today.

“The best features Trellix Endpoint Detection and Response (EDR) offers are the advanced telemetry and behavior-based detection, high-fidelity alerts, and native ecosystems with in-depth forensics and rapid remediation.

“The behavior-based detection engine in Trellix Endpoint Detection and Response (EDR) is incredibly precise. It monitors many different telemetry sources across endpoints and actively maps attacker tactics, techniques, and procedures (TTPs) directly to the MITRE ATT&CK framework. This allows us to think in the mindset of an attacker and catch sophisticated living-off-the-land techniques or data exfiltration attempts before they cause real damage.

“Another massive advantage of Trellix Endpoint Detection and Response (EDR) is how it correlates endpoint data with threat intelligence to deliver high-fidelity alerts. It filters out the noise because we distribute and use the broader Trellix ecosystem. We see firsthand how smoothly it integrates with network, cloud, and third-party solutions. It gives us an enterprise-wide, unified security posture from a single console.

“The in-depth forensics and real-time search capability in Trellix Endpoint Detection and Response (EDR) are outstanding. We can instantly take a non-persistent endpoint snapshot, capturing an up-to-the-moment view of active processes, network connections, services, and autorun entries, even if the machine goes offline. This allows us to confidently isolate threats, find indicators of compromise (IOCs), and rapidly execute a pre-configured response to return the device to a known good state.

“For our SOC team, the absolute best feature of Trellix Endpoint Detection and Response (EDR) is AI-guided investigations. Unlike traditional playbooks that just automate simple scripted tasks, Trellix uses AI to automatically ask and answer questions behind the scenes. It tests multiple hypotheses in parallel, gathers and visualizes the evidence, and presents a summarized case to the analyst. It

drastically cuts down investigation time and fights analyst burnout..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

Other Solutions Considered

Before choosing Trellix Endpoint Detection and Response (EDR), I evaluated other options including Bitdefender, Kaspersky, ESET, SentinelOne, and Sophos.

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“We evaluated other options, including CrowdStrike, Microsoft Defender, SentinelOne, and Trend Micro, in addition to Trellix Endpoint Detection and Response (EDR)..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“We previously used Cisco AMP EDR solution, but we prefer Trellix Endpoint Detection and Response (EDR) as it is more effective in detecting emerging threats..”

Vivek_Jaiswal

Security Engineer at LTI Mindtree

[Read full review](#) 

“Before choosing Trellix Endpoint Detection and Response (EDR), we evaluated other options including Cisco Antimalware protections and Symantec Endpoint Protection, but Trellix Endpoint Detection and Response (EDR) turned out to be a much better solution..”

Vivek_Jaiswal

Security Engineer at LTI Mindtree

[Read full review](#) 

“We are a government company, so we ask the system to contract a company that is resourceful with cybersecurity without mentioning the name or mark. We had been using Trellix since it was McAfee. But I had evaluated solutions from Microsoft, Panda, ESNET, as general malware tools..”

CESARCASTRO

Committee Of IT Cybersecurity at a energy/utilities company with 51-200 employees

[Read full review](#) 

“While choosing Trellix Endpoint Detection and Response (EDR), I evaluated other options, but I prefer to use Trellix Endpoint Detection and Response (EDR) as it is very good and useful. I manage Trellix Endpoint Detection and Response (EDR) easily, and it effectively protects our clients and servers, achieving high scores from outsourced scanning companies that assess our systems..”

Ibrahim Mennanoglu

Senior Information Security Specialist at a consultancy with 51-200 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen a return on investment with Trellix Endpoint Detection and Response (EDR); a lot of time is saved as it minimizes the efforts of manual work, requiring very few analysts to process all those alerts, thus improving operational efficiency and overall..”

Vivek_Jaiswal

Security Engineer at LTI Mindtree

[Read full review](#) 

“Of course this is a yes. I had called the US partner during the past years when I need the support directly from the manufacturer and I got all the help to workaround or overcame issues. That had happended when my local partner company was not enough..”

CESARCASTRO

Committee Of IT Cybersececurity at a energy/utilities company with 51-200 employees

[Read full review](#) 

“Some benefits are available for the users from the use of the solution as it provides nice visibility of the whole environment and the endpoints in an environment, but there is a need to have someone with the technical background to manage it..”

Ramy Ragab

Head of Data Link at Telecom Egypt

[Read full review](#) 

“A concrete result of using Trellix Endpoint Detection and Response (EDR) is that there is a significant reduction in investigation and response times in the event of a security incident. Before its implementation, collecting and correlating evidence across multiple machines required more time. Nowadays, the security team can identify, analyze and contain threats from a single console, considerably reducing the time needed to take corrective actions..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

Trellix Endpoint Detection and Response (EDR) has positively impacted my organization with threat exchange and intel, low false positive ratios, and very high uptime values for both inline and spam modes, along with advanced detection and mitigation capabilities ensuring the highest level of protection and proper detection for command and control and bot attacks.

I have noticed a decrease in attacks as a specific outcome that shows the positive impact of Trellix Endpoint Detection and Response (EDR). .”

Validated user

[Read full review](#) 

Business Development Manager at a retailer with 10,001+ employees

“Trellix EDR provides capabilities similar to AI, significantly aiding your software or IT support team in conducting investigations rapidly. Tasks that might have taken months can now be resolved quickly using the platform. This ability to swiftly identify and address the root causes of attacks is a major advantage. Moreover, by preventing breaches, Trellix EDR helps safeguard data and avoids the need for compliance measures with regulatory bodies. This security is crucial because, in regions like Africa or Nigeria, where certain breaches may go unnoticed, Trellix ensures compliance and transparency, such as mandatory breach reporting in other jurisdictions. Maintaining trust with customers is paramount, as damage to brand reputation can be difficult to repair. Therefore, investing in a solution like Trellix EDR not only protects your organization but also enhances its credibility and operational resilience..”

ObaseunAwoyinfra

[Read full review](#) 

Security Consultant at Trinexia

Use Case

“My main use case for Trellix Endpoint Detection and Response (EDR) is for blocking malware and catching unusual behavior to process, while also monitoring all processes we have for our company, the clients, the computer, and the servers. Our process behavior is crucial, and Trellix Endpoint Detection and Response (EDR) helps to protect our systems from malware..”

Ibrahim Mennanoglu

Senior Information Security Specialist at a consultancy with 51-200 employees

[Read full review](#) 

“I am using Trellix Endpoint Detection and Response (EDR) for threat detection and response and incident response. In Mexico, I am looking for robust and scalable protection and deep visibility without overwhelming my security teams. Trellix Endpoint Detection and Response (EDR) is not just a product we sell; it is the solution we trust to protect our own business in Grupo Salinas every single day. Trellix Endpoint Detection and Response (EDR) is deployed in my organization in the public cloud..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“We use routing and switches, IP phones, routers, switches, and a core switch. We also have Identity Services Engine, but it is end of life or end of support now, so we are working on replacing it.

“Our solutions cut across various security products from Sophos and Trellix. We started with McAfee for 15 years and have now transitioned to Trellix, which acquired McAfee.

“Basically, we use this to protect our endpoints..”

Abubakar Bello

Security Administrator at a insurance company with 1,001-5,000 employees

[Read full review](#) 

“My main use case for Trellix Endpoint Detection and Response (EDR) is the automatic detection of threats and automatic threat detections and response, as there are many use cases that we are currently working with for this Trellix Endpoint Detection and Response (EDR) solution.

“For a quick specific example of how I use Trellix Endpoint Detection and Response (EDR) for threat detection and response in my day-to-day work, Trellix Endpoint Detection and Response (EDR) solution is integrated with our organization's endpoint, monitoring all endpoint activity and detecting advanced threats such as ransomware, fileless malware, exploits, and living-off-the-land attacks. It uses behavior-based analysis as well as machine learning advanced threat intelligence to identify suspicious activity across the traditional antivirus solutions, making it a really great solution for threat protections and detections..”

Vivek_Jaiswal

Security Engineer at LTI Mindtree

[Read full review](#) 

“The main use case for Trellix Endpoint Detection and Response (EDR) in my organization is for continuous monitoring of user machines and servers, detecting suspicious activities, investigating security incidents, and responding quickly to potential compromises. Trellix Endpoint Detection and Response (EDR) provides detailed visibility of events on the endpoints, significantly reducing the time to detect and remediate threats.

“One concrete example of how I have used Trellix Endpoint Detection and Response (EDR) to investigate or respond to a security incident in my company occurred when we implemented a detection and response strategy, especially for workstations and critical servers, which has allowed us to centralize that visibility of security events on the endpoints and improve those investigation processes in the event of an incident. In one of the most relevant cases, Trellix Endpoint Detection and Response (EDR) identified the execution of a suspicious process that was attempting to establish connections to some unusual external IP addresses..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

Trellix Endpoint Detection and Response (EDR) is my organization's main solution for threat detection and mitigation of zero-day and advanced persistent threats in the network, and it is being used throughout the company.

It is highly effective and scalable in terms of detection and prevention, and our usage within Trellix Endpoint Detection and Response (EDR) enhances the value. The SOC team is constantly monitoring Trellix Endpoint Detection and Response (EDR) alerts, in addition to SIEM-generated incidents.

“Inline mitigation capabilities work particularly well, and different deployment models cater to specific needs, along with frequent updates, low false positive rates, and advanced detection of targeted attacks.

“Trellix Endpoint Detection and Response (EDR) is deployed in my organization using a hybrid cloud.

“I purchased Trellix Endpoint Detection and Response (EDR) through the AWS Marketplace.

“Advanced detection of targeted attacks has reduced the attacks, and I have seen low false positive rates as relevant metrics that show the return on investment. .”

Validated user

[Read full review](#) 

Business Development Manager at a retailer with 10,001+ employees

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.

“Setting up the solution is easy for me because I've been in cybersecurity for almost 30 years, but new users might find it hard. Depending on the client's needs, it can be set up on-premises, in a private or hybrid cloud, or fully in the cloud. Setting it up can take a few days for small environments or months for big companies with thousands of endpoints..”

RiaanDu Preez

Senior Cyber Security Specialist Architect at a outsourcing company with 11-50 employees

[Read full review](#) 

“The solution is SaaS-based, and we have deployed it using the hybrid cloud model.

The tool's deployment phase is a lengthy process. For one endpoint, it takes 15 to 20 minutes..”

Sampath Acharya

Technical Associate at Valuepoint Systems

[Read full review](#) 

“My first piece of advice is to go cloud-native with Trellix Endpoint Detection and Response (EDR) ePO SaaS if your compliance allows it. By basing the configuration on cloud infrastructure rather than traditional on-premises infrastructure setup, it removes a massive amount of engineering overhead. It allows your team to focus entirely on threat monitoring and response from day one, rather than patching servers or managing database sizing..”

Domit-Molina

[Read full review](#) 

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

“I have seen a return on investment with Trellix Endpoint Detection and Response (EDR), as the money saved is satisfactory. They also assist us with licensing and provide timely reminders for license renewals, which means we require fewer employees to manage these tasks. I find it easy to locate what I need on Trellix Endpoint Detection and Response (EDR), such as articles in the knowledge base and documents on their portal..”

Ibrahim Mennanoglu

[Read full review](#) 

Senior Information Security Specialist at a consultancy with 51-200 employees

“We operate within our environment and country. One of our clients, is interested in using our on-premises solution. They are hesitant to adopt a cloud-based solution due to concerns about data security. They worry that storing data in the cloud could expose it to unauthorized access. They are confused about how the cloud handles sensitive data like CPU data and prefer to keep their information on-premises. However, other banks have embraced cloud solutions and understand their value. Over time, as more companies study and become comfortable with cloud technology, we believe others will also follow and move to the cloud. We hope to maintain their interest in our services..”

Abdullah Al Hadi

[Read full review](#) 

Information Security Engineer at Nhq Distribution Ltd

“It is straightforward. The only little challenge is that you have to get all the necessary updates for it to connect to the database.

“I am using on-premises with the ePolicy Orchestrator and then we apply the license. After the product is already installed, we do the necessary upgrade, restart the system, and then push the agents to the endpoints. Then we receive updates and manage our clients..”

Abubakar Bello

[Read full review](#) 

Security Administrator at a insurance company with 1,001-5,000 employees

Customer Service and Support

“There are multiple ways to get support. You can create a case through your partner or support portal by calling. If necessary, you can raise a call and follow up immediately..”

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

[Read full review](#) 

“My opinion about technical support might be biased because I have direct access to top-level senior staff. I know some people struggle with support if they go through normal channels..”

RiaanDu Preez

Senior Cyber Security Specialist Architect at a outsourcing company with 11-50 employees

[Read full review](#) 

“Customer support is a critical component of any enterprise EDR deployment, and my experience with Trellix has been highly positive, largely because of how they structured their ecosystem through Trellix Thrive..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“We do a lot of research. Our only problem with Trellix is that it is resource intensive and takes a lot of resources. However, we found out that it works on our systems and on our desktops. But on our servers, we do not want it to touch our resources, so we deployed Sophos XDR on the server..”

Abubakar Bello

[Read full review](#) 

Security Administrator at a insurance company with 1,001-5,000 employees

“Tech support may be tricky if the support comes from Asia experts. Eeveryone here speaks spanish and I are not affordable most of time. The tech is interesting when a high support level is called. Once someone from Argentina helped me that has excellent skills. We need more like her..”

CESARCASTRO

[Read full review](#) 

Committee Of IT Cybersececurity at a energy/utilities company with 51-200 employees

“I would rate Trellix Endpoint Detection and Response (EDR)'s customer support as very good. The support has been professional, with good product knowledge and adequate follow-up of cases. The attention we have received has allowed us to resolve some incidents and queries efficiently, contributing to a positive experience with the platform. On a scale from one to ten, I would rate that support nine out of ten. The support team has demonstrated solid knowledge, providing adequate follow-up to cases and maintaining effective communication..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

Other Advice

“I have seen companies without any EDR services, and we were lacking information. I started with IDR around four years ago, and the support services were very light. I remember doing many tickets for Trellix support, and my EDR was not properly functioning. I didn't feel the detection or the real protection. My company is one among 17 others that are part of a corporation. I am a member of the IT Security Council.

Overall product rating is five out of ten..”

CESARCASTRO

Committee Of IT Cybersececurity at a energy/utilities company with 51-200 employees

[Read full review](#) 

“In my day-to-day work, I also use Trellix Endpoint Detection and Response (EDR) for the Threat Hunting part, the continuous monitoring of indicators of compromise and the generation of reports for the security and management teams, allowing detection and investigation times to improve the visibility of the environment, strengthening the cybersecurity posture. I would recommend properly planning the implementation of Trellix Endpoint Detection and Response (EDR), training the security team, and taking advantage of the investigation and Threat Hunting capabilities from day one. When integrated with a SOC process and other security tools, Trellix Endpoint Detection and Response (EDR) can provide excellent visibility and a significant improvement in detection and response capabilities against any threat. I would rate this product nine out of ten overall..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“When evaluating the AI capabilities in Trellix Endpoint Detection and Response (EDR), specifically Trellix Wise, governance and data security are actually its strongest selling points. Trellix has built its GenAI framework with a strict, responsible AI approach that directly addresses the main concerns of corporate legal and security teams.

“When it comes to the accuracy and reliability of Trellix Wise within the EDR platform, I would rate it as exceptionally high, but it is important to understand why it is reliable. In cybersecurity, generic AI often struggles with accuracy because it lacks context. Trellix solves this by anchoring its AI to three specific guardrails that ensure reliable outputs. I rate this solution with a review rating of 9..”

Domit-Molina

Especialista Seguridad Endpoint at a tech services company with 51-200 employees

[Read full review](#) 

“This EDR solution stands out through its automated threat response, forensic investigation capabilities, and integration with the MITRE ATT&CK framework. Compared to other solutions, such as Cisco Antimalware protections and Symantec Endpoint protections, Trellix Endpoint Detection and Response (EDR) is not just behavior-based analysis but also supports signature-based analysis.

“My advice for others looking into using Trellix Endpoint Detection and Response (EDR) is that they should work with the vendor on deployment and integrations with the EDR agent, ensuring complete discussions with the vendor for better results.

“I think Trellix Endpoint Detection and Response (EDR) is a really good solution, with no performance glitches, performance behavior gaps, or discontinuities. I would rate this solution a 10 on a scale of one to ten because it not only serves as an EDR solution but also excels in detecting and responding to behaviors based on data, quickly identifying processes running on the host and correlating the data, taking action very quickly, making it a very good solution without any gaps that I see..”

Vivek_Jaiswal

Security Engineer at LTI Mindtree

[Read full review](#) 

“I have seen faster response times with Trellix Endpoint Detection and Response (EDR); for example, when I receive alerts for malware detection, I can immediately take action directly from Trellix Endpoint Detection and Response (EDR), starting by disabling the network to the affected machine and then investigating further.

“My advice for others considering Trellix Endpoint Detection and Response (EDR) is to use it, or any other Trellix products, as I believe they are excellent. It is easy to set up, share the models, follow necessary steps, and its effectiveness in protecting against malware, ransomware, and other threats is remarkable for all clients and servers, which I find manageable.

“I appreciate Trellix Endpoint Detection and Response (EDR). I have managed Trellix modules for almost seven years, not just EDR, but also [DLP](#), ATP, TAI, and others. We find it useful, and the best part is that I can easily find the answers I need from Trellix Endpoint Detection and Response (EDR) document systems, which is very beneficial. I have given this review a rating of 8 out of 10..”

Ibrahim Mennanoglu

Senior Information Security Specialist at a consultancy with 51-200 employees

[Read full review](#) 

“This year, I am planning to have a training for all the personnel of the company in every department so they can learn the basics of the endpoint tool. They can have more actions for possible threats or everything so they can help my department to make a better and faster action if something real is happening. Something like ethical hacking or a service, but using my own personnel in the company. I know that it is difficult, but I want to try to make that this year.

I have evaluated many products including Fortinet environment and a lot of appliances, and also many other products that we have now. I have evaluated around six or seven other brands or other products. However, I have learned Trellix Endpoint Detection and Response (EDR) tools and before that McAfee, around two decades. It is enough expertise that we have made. I do not want to lose that with maybe another interesting tool. For example, what would be interesting is if an [XDR](#) tool that can help us in managing the threats of the cybersecurity environment uses AI as an agent, a trained agent that helps our department, so it has to be trained first by a company like Trellix or another with the expertise or the capacity to help us actually. That is one thing I can recommend.

In February or March, I am signing a new contract with five levels, three more levels of security that we have now. We will have the tool, the SOC, the operating center service, and we need to manage applications firewall, web filtering, and XDR, and maybe next year also PAM and so on. I rated this solution an 8 out of 10..”

CESARCASTRO

Committee Of IT Cybersecurity at a energy/utilities company with 51-200 employees

[Read full review](#) 

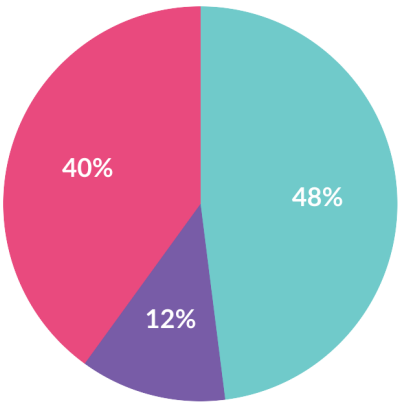
Top Industries

by visitors reading reviews

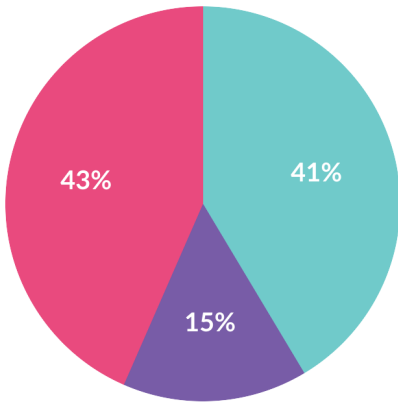


Company Size

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