aws marketplace

Trellix Endpoint Detection and Response (EDR)

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Trellix Endpoint Detection and Response (EDR)

Trellix Endpoint Detection and Response (EDR) Recap

Reduce Alert Noise

Reduce the time to detect and respond to threats. Trellix EDR helps security analysts quickly prioritize threats and minimize potential disruption.

Do More with Existing Resources

Guided investigation automatically asks and answers questions while gathering, summarizing, and visualizing evidence from multiple sources—reducing the need for more SOC resources.

Low-Maintenance Cloud Solution

Cloud-based deployment and analytics enables your skilled security analysts to focus on strategic defense, instead of tool maintenance. Benefit from implementing the right solution for you.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The product and the services we have are quite good."

CESARCASTRO

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

- "The product's initial setup phase was very straightforward since you just need to install it, and it works."

Ramy Ragab

Head of Data Link at Telecom Egypt

- "Trellix Endpoint Detection and Response (EDR) offers endpoint protection and helps collect information while also allowing users to investigate malicious files in an IT environment...It is a stable solution...It is a scalable solution."

Hung-LE

Group IT Manager at Discova

"The dashboard makes it easier and more effective to analyze data."

Abdullah Al Hadi

Information Security Engineer at Nhq Distribution Ltd

"When Trellix detects some threats, the device is isolated in a quarantine zone for examination."

Juan Muriel

IT Management Specialist at a computer software company with 10,001+ employees

"The most valuable feature of the solution is its area for threat detection."

Sampath Acharya

Technical Associate at Valuepoint Systems

"It relies on external systems for detection and then asks the endpoint to handle blocking. However, the most crucial feature is its investigative capabilities. With real-time search and other functionalities, it enables comprehensive detection and response."

ObaseunAwoyinfa

Security Consultant at Trinexia

What users had to say about valuable features:

"Trellix is a good solution. It helps with real-time monitoring and alerts. We are pretty satisfied with it. The product is user-friendly. It improves our security posture.."

Muniyappan Vk
Senior IT Support Engineer at Mu Sigma Inc.

Read full review

"The most useful features are behavior monitoring, DLP, and access control. The automation has gotten much better in the last two years than when it was McAfee. It works better now and integrates more smoothly.."

RiaanDu Preez
Senior Cyber Security Specialist Architect at a tech consulting company with 11-50 employees

Read full review

"Trellix Endpoint Detection and Response is a user-friendly solution. The biggest strength of the solution is that it's an integrated product that includes EDR and antivirus. It's not like you have different technologies for different solutions.."

Bernard Van Den Heuvel
Professional Services Manager at Concanon LLC

Read full review

"The dashboard makes it easier and more effective to analyze data. It also allows us to access the AWS analytics and system features in one place. If we need to find specific details about an endpoint, we can determine what is happening and how any organization is affected by the data provided.."

Abdullah Al Hadi
Information Security Engineer at Nhq Distribution Ltd

Read full review

"The antivirus and DLP features are valuable. Now, we have a campaign to encrypt all the drives of the company. We have a solution for network access control from Fortinet. When Trellix detects some threats, the device is isolated in a quarantine zone for examination. We integrate Trellix Endpoint Detection and Response with other solutions to perform such isolations. We also use products for log monitoring and correlation and create use cases for automatic response.."

Juan Muriel
IT Management Specialist at a computer software company with 10,001+ employees

Read full review

"The product and the services we have are quite good. However, I cannot stay at this level forever. I have to improve continuously and dynamically.

Everything is working, and the company is training its personnel. I have had in a few months in the past some attacks on personnel—so phishing, for example. I have spent efforts on training our managers and others - what can software do if the knowledge base is low?."

CESARCASTRO

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

Read full review

Other Solutions Considered

"In my previous organization, I used to work with Cybereason instead of Trellix Endpoint Detection and Response (EDR). My present company prefers to use Trellix Endpoint Detection and Response (EDR), so I switched. ."

Verified user
information security at a insurance company with 201-500 employees

Read full review

"We have been looking at replacing McAfee with Trend Micro, but to change our setup is a big task. It is very complex and we need a plan, so are just upgrading instead of changing at this time.."

Pankaj Nagpal
Chief Information Security Officer at Romsons

Read full review

ROI

Real user quotes about their ROI:

"There has been a return on investment since it is a good business. Hence, we embedded the solution in our services. So, I know that this is a good investment.."

Christian Guillén
Sales Manager at Last call

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

"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.."

ObaseunAwoyinfa
Security Consultant at Trinexia

Read full review

Use Case

"I use César for our endpoints, our users, and the services from email and web services, back and forth, and also at the edge of our network. We have contracted firewalls and everything else for networking.."

CESARCASTRO

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

Read full review

"The solution is used to search the IOCs. We use it in our company when we are unable to search for multiple hashes at a time for a particular file. Without Trellix Endpoint Detection and Response (EDR), each hash needs to be executed individually in the search parameter. ."

Verified user

information security at a insurance company with 201-500 employees

Read full review

"As a user, I didn't have any concerns about technical aspects where I was working previously. Working together. So, we sell licenses of McAfee. We had a promotional activity in which when you buy a cell phone, you get a McAfee subscription for mobile, and we used to offer a license of McAfee with an internet connection.."

Christian Guillén
Sales Manager at Last call

Read full review

"Trellix Endpoint Detection and Response (EDR) is a very advanced solution, and it can work very well since it helps a user get very deep and very detailed information. With Trellix Endpoint Detection and Response (EDR), I can collect everything from the client without any problem. Trellix EDR API rate is very high, and they cover a very large number of attacks and IOCs because it stands as a highly corrected product with the help of a very high-level research and development team.."

Ramy Ragab
Head of Data Link at Telecom Egypt

Read full review

"We use the solution to detect and identify critical management activities. Within the network level, you can understand what is happening in the environment. Organizations using complex systems for various purposes can easily identify shared activity within the environment. There is a detection base that allows us to identify and manage threat events. The solution also includes licenses for forensic investigations of any attack that occurs. Details can be found within the platform's release at the end of the month or whenever needed. Any Trellix malware activity will be displayed on the dashboard, and the moderating services will be integrated into everything we have built.."

Abdullah Al Hadi
Information Security Engineer at Nhq Distribution Ltd

Read full review

"In my company, we use Trellix Endpoint Detection and Response (EDR) since it is a very helpful product. In my company, we install Trellix Endpoint Detection and Response (EDR) for all our machines and endpoints, along with Trellix Cloud Security. Trellix EDR can be integrated with Trellix SIEM. Trellix and McAfee Endpoint Security are used in our company as they offer endpoint protection.

Trellix Endpoint Detection and Response (EDR) offers endpoint protection and helps collect information while also allowing users to investigate malicious files in an IT environment.."

Hung-LE
Group IT Manager at Discova

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.

"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

Read full review

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

"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

Read full review

Technical Associate at Valuepoint Systems

"Administering Trellix EDR involves specific procedures. For instance, real-time searching requires using predefined keywords, which aren't readily visible unless you consult with Trellix support or a SE. A comprehensive manual simplifying these administrative tasks would greatly enhance usability. Despite this, setting up the product is straightforward and quick, since it operates in the cloud. Connecting to either cloud-based or on-premises APIs is seamless. However, the challenge lies in product administration, which some users might find complex, leading them to opt for alternative solutions over Trellix EDR.."

ObaseunAwoyinfa

Security Consultant at Trinexia

Read full review

"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

Information Security Engineer at Nhq Distribution Ltd

Read full review

“The product's initial setup phase was very straightforward since you just need to install it, and it works.

The product's deployment phase had very few steps because it was made available as a preconfigured device without the configurations, and with the network configuration, everything works fine.

The solution is deployed on an on-premises model.

The solution can be deployed in an hour.

The maintenance and deployment of the solution require the same number of people as for Kaspersky..”

Ramy Ragab

Head of Data Link at Telecom Egypt

Read full review

“Speaking about the product's setup phase, in our company, we deploy it with the endpoint management setup system. When in our company, we have any new applications, the endpoint management setup system automatically deploys for all the agents.

The solution can be deployed in twenty minutes to complete all the components of the installation phase.

For deployment, my company uses a deployment application since we have to deal with endpoints in my organization, and other than that, if there is a requirement for deployments, then we use it to take care of such a setup phase. The deployment can be done automatically for the endpoint.

The solution is mostly deployed on the cloud, but at times, it may be deployed on a hybrid cloud..”

Hung-LE

Group IT Manager at Discova

Read full review

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

"Their technical support is better than some of the competitors in the space. To make a direct comparison, it's definitely better than Symantec Broadcom.."

RojeHay
Senior Security and Risk Management Analyst at National Commercial Bank Jamaica Limited (NCB)

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 tech consulting company with 11-50 employees

Read full review

"I've contacted the technical support for McAfee MVISION Endpoint Detection and Response many times. It takes time for the team to respond to the cases, but at the end of the day, you do get a response.."

Aggry Motlhwa
IT Security Specialist at Commercial Bank of Ethiopia

Read full review

"They had pretty good tech support. I think a lot of what happened to McAfee, from my perspective, was everything went offshore to India and for US customers, there is a language barrier that created problems.."

Verified user
Sr. Sales Engineer at a tech services company with 11-50 employees

Read full review

"Support for Trellix EDR is not great. There have been instances where we encountered issues that required support intervention. In some cases, we were unable to resolve the problem ourselves, and escalated it to support. Unfortunately, there were delays in getting responses from support, which sometimes led to frustration and caused us to consider alternative solutions. ."

ObaseunAwoyinfa
Security Consultant at Trinexia

Read full review

Other Advice

“Our clients are usually medium-sized and enterprise businesses. Overall, I would recommend Trellix EDR to others. I'd rate it eight and a half out of ten. No EDR or XDR solution gets a nine from me right now because they all have room for improvement. .”

RiaanDu Preez
Senior Cyber Security Specialist Architect at a tech consulting company with 11-50 employees

Read full review

“Trellix Endpoint Detection and Response (EDR) handles security incidents but generates multiple false positive alerts. If the solution is fine-tuned from time to time, then true positive results can be expected accurately. After implementing Trellix Endpoint Detection and Response (EDR) in our organization, we have witnessed great security efficiency.

I would recommend the solution to others as it's very easy to use. I would rate the solution a seven out of ten. .”

Verified user
information security at a insurance company with 201-500 employees

Read full review

“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

"Its machine learning capability is strong, and the AI configurations and system integration enhance its effectiveness. The API solutions added to this system allow us to detect and respond to incidents quickly. The quick response is also due to Edge Solutions and specific-type solutions, enabling us to conduct thorough investigations and generate reports on the platform.

I recommend Trellix Endpoint Detection and Response (EDR) because it offers strong capabilities. It's worth noting that XDR solutions are also available and might be more effective. These XDR solutions are advanced technologies with enhanced features, including improved API integration.

Overall, I rate the solution an eight out of ten.."

Abdullah Al Hadi
Information Security Engineer at Nhq Distribution Ltd

Read full review

"I haven't worked on the tool to see how it works for security workflow.

My customers have not seen any challenges while working with Trellix Endpoint Detection and Response (EDR) in terms of integrations.

The tool does not support any AI and security initiatives.

The tool is suitable for enterprise companies.

If businesses are completely on the cloud, then the tool is not required. If a company has a hybrid cloud model with an on-premises model, then it will be a good tool to use.

I rate the tool an eight out of ten.."

Sampath Acharya
Technical Associate at Valuepoint Systems

Read full review

"Technical personnel often recommend Trellix Endpoint Detection and Response (EDR) for environments that are not necessarily small, but rather SMBs, those with around 50 computers. EDR solutions are increasingly aligned with the evolving threat landscape.

Trellix EDR provides advantages beyond just detection and response; it facilitates thorough investigation. It operates more like a layered approach, enabling detailed investigation through Trellix Investigator. This allows you to drill down into threats. With real-time search capabilities, you can monitor threats as they occur. Historical search features let you trace when a threat entered the environment and its progression. This granularity extends to file searches and other detailed inquiries, simplifying and enhancing threat management tasks.

In terms of integration, there is still room for growth. Currently, apart from basic anonymized data sharing, there isn't much integration visible. The ability to leverage EDR with other security solutions seems limited, except perhaps through programming.

Trellix EDR has the potential to be among the top EDR solutions with a few adjustments. It could become the best out there. When considering factors like support, pricing, and ease of use, Trellix EDR has the opportunity to excel. However, currently, there are areas where it can enhance user experience, particularly in simplifying tasks that end users might find challenging on the EDR platform. While it promises to enhance security posture and threat detection speed, these improvements may not be immediately apparent to users, impacting their confidence in the product.

Overall, I rate the solution a seven out of ten.."

ObaseunAwoyinfa
Security Consultant at Trinexia

Read full review

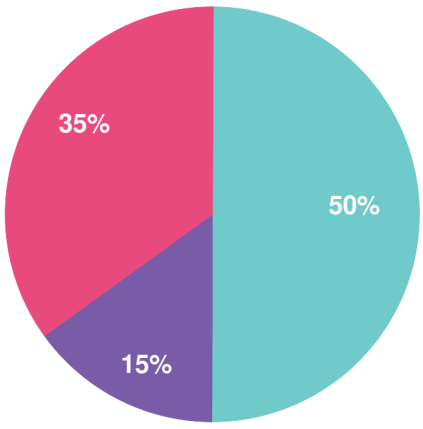
Top Industries

by visitors reading reviews

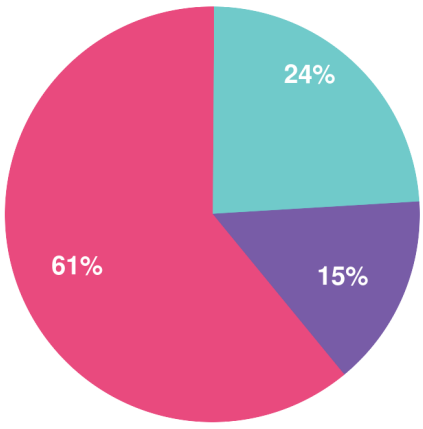
Financial Services Firm	12%
Computer Software Company	11%
Government	11%
Manufacturing Company	10%

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 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