aws marketplace

TrendAI Deep Security

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

TrendAI Deep Security

TrendAI Deep Security Recap

TrendAI Deep Security offers advanced protection with anti-malware, virtual patching, and intrusion prevention. It supports hybrid and cloud environments, providing comprehensive security solutions for large organizations.

TrendAI Deep Security provides a robust suite of features tailored for defending systems against evolving threats. With centralized management, it seamlessly integrates with hybrid and cloud environments. Notable is its virtual patching, which reduces zero-day vulnerability risks and downtime, making it an optimal choice for large corporations seeking extensive protection. Despite challenges like less intuitive dashboards, compatibility, and performance issues during scanning, it excels in server and endpoint protection, intrusion detection, and application control. It's particularly effective in financial sectors and integrates with cloud platforms to automate security policy deployment.

What are TrendAI Deep Security's most significant features?

- **Anti-Malware:** Guards against modern threats across multiple environments.
- **Virtual Patching:** Shields systems from zero-day vulnerabilities without immediate updates.
- **Intrusion Prevention:** Detects and prevents unauthorized access attempts.
- **Firewall Capabilities:** Ensures network safety by regulating data across systems.
- **Cloud Integration:** Provides seamless operations with automated policy application.

What benefits should users look for in reviews?

- **Comprehensive Protection:** Users should expect robust security for both physical and virtual environments.
- **Operational Efficiency:** Look for improved efficiency due to automated processes and policy applications.
- **Zero-Day Protection:** Consider the benefits of virtual patching in minimizing downtime and security risks.
- **Compliance Support:** Ensure the feature aids in adhering to industry-specific regulations.
- **Centralized Management:** Centralized control simplifies security management across infrastructures.

Organizations in sectors like finance deploy TrendAI Deep Security for its virtual patching and hybrid environment support. The solution's adaptability across cloud platforms ensures secure workloads, making it essential for environments requiring robust threat detection and monitoring.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The best features Trend Micro Deep Security offers include virtual patching and comprehensive protection from multiple modules such as anti-malware, web reputation, firewall, integrity monitoring, and log inspection."

Verified user

Information Technology Service Desk Manager at a tech vendor with 5,001-10,000 employees

- "The protection layer and total control features of Trend Micro Deep Security provide comprehensive protection, with multiple security layers including anti-malware, intrusion prevention, integrity monitoring, web reputation, application control, firewall, and log inspection, all accessible through a single lightweight agent and manageable across Windows, Linux, and cloud workloads."

MojammelHossain

Microsoft Security Department at a financial services firm with 501-1,000 employees

"Trend Micro Deep Security has positively impacted my organization by reducing risk and response times while being cost-effective and saving on operational efficiency, compliance, audit readiness, scalability, and business agility, supporting both on-premise and container workloads."

PrashantSharma6

Senior Professional 2 at Capgemini

"Trend Micro Deep Security has positively impacted my organization by being a mature tool and a stable platform, and its virtual patching capability is very strong, with good visibility and reporting features that I find beneficial."

Abhishek Motla

Senior Cyber Security Engineer at Capgemini

"Trend Micro Deep Security is an advanced threat protection product that helps our servers prevent upcoming attacks and also logs inspections and firewall preventions, helping our servers in daily life by protecting them from advanced cyber attacks."

Manish Kumar Twinkle

Security Engineer at itsipl

"Trend Micro Deep Security's best features include the IPS module, which stands out because it is not just an AV product but operates as the latest AV or EDR product, provides details, and handles patches related to vulnerabilities."

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

"Virtual patching stands out as the best feature Trend Micro Deep Security offers, allowing us to virtually patch servers without downtime, which is critical given our limited patching windows, and helps prevent servers from being exploited."

Harshit Tiwari

Web develope analyst at a tech vendor with 10,001+ employees

What users had to say about valuable features:

"Trend Micro Deep Security has fantastic and very advanced features. The most valuable and advanced feature of the solution is the ability to check vulnerabilities. The solution's real-time scanning allows me to monitor my entire network.."

Vikas Saxena
Information Technology Manager at BCML

Read full review

"The most valuable features of Trend Micro Deep Security first of all include anti-malware. Second, as I mentioned, virtual patching is very critical. If a customer has a business and needs to patch one of their critical servers, but due to business requirements, they cannot patch the systems immediately, this virtual patching will help the servers avoid exploit. Trend Micro Deep Security will cover it as a patch: when an attacker tries to exploit a particular CVE, it will block and secure the system from that exploit. Vulnerabilities will be virtually patched, making it the main and most helpful feature. Additionally, this anti-malware finds any malware or spyware, fulfilling all anti-malware functions. It also has a File Integrity module; if I provide a custom file path, it will give alerts if there are any changes to those particular files.."

Verified user
Security Consultant at a tech vendor with 10,001+ employees

Read full review

"The best features Trend Micro Deep Security offers include virtual patching, which is well-known to protect against zero-day vulnerabilities, integrity monitoring, which is useful for monitoring unauthorized config changes, and anti-malware and firewall that helps to reduce noise, along with cloud integration that assists in the auto-discovery of different workloads.

"In my experience, virtual patching has been the most valuable feature because Trend Micro Deep Security is well-known for this capability, and it helps clients using legacy servers who do not want to upgrade as their applications require that functionality. Virtual patching helps us by providing the necessary security to protect those servers.."

Abhishek Motla
Senior Cyber Security Engineer at Capgemini

Read full review

"The best feature of Trend Micro Deep Security is Application Control, where we can put it in lockdown mode, and applications that are already applied or installed will be executed, while new ones will be blocked automatically.

Trend Micro Deep Security is an advanced threat protection product that helps our servers prevent upcoming attacks and also logs inspections and firewall preventions, helping our servers in daily life by protecting them from advanced cyber attacks.

With the help of Application Control, we first scan the inventory of our applications that are installed on the server. After that, we get a scanned and checked inventory where all the executable files of the servers are present with the help of hashes. By putting application control in lockdown mode, all the applications that pre-exist in the file will execute at any time. However, when a new file or new update comes to the server, it will be denied due to the lockdown policy. If any attack comes, the new hashes will be found and blocked, making it a very good feature of Trend Micro Deep Security.."

Manish Kumar Twinkle
Security Engineer at itsipl

Read full review

The best features of Trend Micro Deep Security include virtual patching, which is IPS, and multi-layer protection that encompasses anti-malware, firewall, integrity monitoring, and log inspection. Furthermore, it offers cloud and hybrid support, centralized management, compliance assistance with built-in tools including PCI DSS, HIPAA, and GDPR, along with application control, scalability, and automation.

Trend Micro Deep Security has positively impacted my organization by reducing risk and response times while being cost-effective and saving on operational efficiency, compliance, audit readiness, scalability, and business agility, supporting both on-premise and container workloads.

“Virtual patching via IPS protects all servers instantly, resulting in no downtime and eliminating overtime labor, saving around $50,000. Additionally, there is a reduced risk of breach. For improved efficiency, with Trend Micro Deep Security, I built 100 new cloud instances without needing manual agent installations and policy assignments, which would have taken hours and delayed securing workloads, ultimately increasing risk. With Trend Micro Deep Security automation, agent deployment occurs automatically via AWS and Azure integration, and policies are applied instantly based on tags, saving eight to ten hours per deployment cycle, allowing my team to focus on more strategic tasks instead of manual deployment and patching. .”

PrashantSharma6
Senior Professional 2 at Capgemini

Read full review

"Trend Micro Deep Security offers several powerful features, with the Intrusion Prevention System module standing out as one of the most valuable. Unlike a typical antivirus product, Deep Security functions more like an advanced AV or EDR solution. It not only provides protection but also assists in managing vulnerability patches. The IPS module delivers virtual patching that mitigates risks immediately, making it an especially effective tool for securing servers.

The virtual patching capability has been highly beneficial for our organization. On Windows platforms, not all vulnerabilities can be patched through standard updates, but the IPS module typically offers virtual patches to close those gaps. This helps maintain system stability and protection without requiring disruptive updates.

In addition to IPS, the platform includes strong features such as the anti-malware module, firewall, and application control modules—all of which enhance system security and help prevent unknown or suspicious activities. Web reputation capabilities further strengthen protection and assist our team in daily operations.

Trend Micro Deep Security has positively impacted our organization by supporting both Windows and non-Windows environments, including Linux and AIX. Its cross-platform compatibility simplifies deployment and monitoring. The product performed exceptionally well even on older systems such as Windows Server 2003, where many antivirus solutions often struggled.

From an operational perspective, Deep Security also improves compliance outcomes. Unlike many tools that require reinstallation for issue resolution, most problems can be fixed by reactivating the agent or using simple troubleshooting commands. Moreover, its integration with Trend Micro Vision One provides comprehensive visibility across the environment, helping our team maintain better oversight and security posture.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

Other Solutions Considered

Before choosing Trend Micro Deep Security, we evaluated the Defender solution, but it was not as cost-effective, leading us to select Trend Micro Deep Security instead.

PrashantSharma6
Senior Professional 2 at Capgemini

Read full review

"Previously, I was using Sophos Server Security and switched to Trend Micro Deep Security because Sophos Server Security got stuck in some cases, slowing down our servers.."

Manish Kumar Twinkle
Security Engineer at itsipl

Read full review

"Before choosing Trend Micro Deep Security, I evaluated other options and have used features from all the tools, including integrity monitoring, anti-malware, cloud, virtual patching, IPS, and IDS, so I have experience with all the features of this tool.."

Abhishek Motla
Senior Cyber Security Engineer at Capgemini

Read full review

"Before Trend Micro Deep Security, I was using solutions like Symantec and McAfee on the servers. After implementing it for one client, that client felt happy due to the many new modules available. I explained these to them and implemented them, which made the client feel their servers were secured using Trend Micro Deep Security.."

Verified user
Security Consultant at a tech vendor with 10,001+ employees

Read full review

"We previously used a different solution. We switched to Trend Micro Deep Security because we wanted cloud deployment and more advanced security. Trend Micro Deep Security has modules like vulnerability assessment and TAC mode, which were not available in our previous tool.."

Vikas Saxena
Information Technology Manager at BCML

Read full review

"I evaluated other options and other vendors before choosing Trend Micro Deep Security. As mentioned, in a few clients, other solutions were already present, but due to the features, modules, and functionality, a few customers migrated from other solutions to Trend Micro as well.

To be frank, I have not personally compared Trend Micro Deep Security with other vendors; customers have compared them and chosen.."

Verified user

Security Consultant at a tech vendor with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

Regarding return on investment, my organization absolutely sees a positive return because we have reduced breach risks and cut operational costs through automation, which eliminates downtime during patching, making it a single platform that saves on licensing costs while improving compliance efficiency.

PrashantSharma6
Senior Professional 2 at Capgemini

Read full review

"Trend Micro Deep Security saves money. It is a costly product, but with the help of this, we secure our organization's infrastructure very much and also get real prevention with the help of these features.."

Manish Kumar Twinkle
Security Engineer at itsipl

Read full review

"I have experienced a strong return on investment with Trend Micro Deep Security, as it has helped save both time and money. Several people I know have also invested in it, and they have found it equally beneficial in both aspects.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"I have seen a return on investment with Trend Micro Deep Security. It is a time-saving and money-saving product. The management console is very useful and easy to operate, allowing policy deployment in a minimal amount of time.."

Verified user
Information Technology Service Desk Manager at a tech vendor with 5,001-10,000 employees

Read full review

"We give the comparison and demo to the customer. If the customer is interested in technical capabilities, we demonstrate the tools, setup, implementation, and their working. At the end, the customer is more interested in the cost.."

M-Saleem
Manager, Technical Microsoft at a computer software company with 201-500 employees

Read full review

"I have seen a return on investment with Trend Micro Deep Security because its deployment feature is very effective, and the single agent helps monitor multiple things while ensuring employees were not affected during the deployment, as the downtime was minimal, so much so that they did not notice when it happened.."

Abhishek Motla
Senior Cyber Security Engineer at Capgemini

Read full review

Use Case

“Trend Micro Deep Security serves as my main solution for antivirus and endpoint security. In this use case, we manage security policies, file protection, and scanning activities with Trend Micro Deep Security..”

Harshit Tiwari
Web develope analyst at a tech vendor with 10,001+ employees

Read full review

“My main use case for Trend Micro Deep Security was that I worked as an implementation engineer, and I was responsible for managing the tool in the client environment, so it served as a main resource for that and a single point of contact.

“I managed Trend Micro Deep Security in my client's environment by implementing the project and the policies based on their environment, such as when any server was going to upgrade or some activity was going to happen..”

Abhishek Motla
Senior Cyber Security Engineer at Capgemini

Read full review

“The usual use cases for Trend Micro Deep Security that I have been working with mostly involve server security, and like anti-virus, I use it for the endpoint. I will also have Trend Micro Deep Security solution for the servers. The good thing, as I compared it with other solutions related to server security in the form of anti-virus, is that Trend Micro Deep Security is very good. It has multiple features available, not only anti-malware but also an anti-ransomware feature as well. Apart from that, it acts as a firewall with IPS and IDS kind of features. IDS works as IDS with signatures. The main feature that other solutions didn't have is virtual patching, which provides the best help for vulnerabilities available on the server. Besides that, it has other modules like application control, which I can use to restrict the installation of new software. Multiple modules are available, and this again depends on the licenses and other factors. The customer who purchases must take all the licenses and implement them properly to gain from the solution. If I have taken the solution but have missed application control, it will not function. Therefore, the multiple modules team must evaluate, and the settings or configurations must be made according to best practices to help as a security tool and prevent many attacks..”

Verified user

Security Consultant at a tech vendor with 10,001+ employees

Read full review

"Trend Micro Deep Security is used in our environment for monitoring and incident response to detect any malicious activity. We utilize the Intrusion Prevention System module, virtual patching, and application control features to manage and secure our applications effectively.

Incident response and monitoring through Trend Micro Deep Security are integrated with Trend Micro Vision One. When an alert is triggered, such as a workbench ID being created for detected malware activity, we receive the alert and begin our investigation in Vision One. We identify the source of the alert, verify associated indicators such as the SHA value, and determine whether the file is malicious. A detailed investigation is conducted to understand the threat, assess its impact, and implement preventive measures. If the file has not been quarantined automatically, we collect and submit it to Trend Micro for further analysis before assessing its severity.

On a daily basis, Trend Micro Deep Security supports our operational activities. We add exclusion files as needed, monitor all malware-related activity, and review application control data to ensure that only approved applications are whitelisted while any unauthorized or risky applications are blocked.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"My main use case for Trend Micro Deep Security is its best feature, virtual patching, which allows us to secure our server against known vulnerabilities without having to immediately apply OS or application patches. This has helped reduce downtime, improve compliance, and safeguard critical workloads. The solution has seven modules, including anti-malware, web reputation, firewall, integrity monitoring, and log inspection, but its best feature remains virtual patching.

"I use Trend Micro Deep Security in multiple organizations, primarily in the financial sector and multiple banks, where I have protected both our physical and virtual servers from vulnerabilities. Its role is primarily virtual patching, meaning if our server is vulnerable due to a zero-day attack and a patch is not applied, Trend Micro Deep Security creates a virtual patch. That remains the best feature. I perform day-to-day operations with it.

"I have implemented and tested multiple use cases on Trend Micro Deep Security solution for different modules, including intrusion prevention and integrity monitoring. For the anti-malware module, I have tested and observed how this product protects against any malicious or suspicious activity.."

Verified user

Information Technology Service Desk Manager at a tech vendor with 5,001-10,000 employees

Read full review

Trend Micro Deep Security serves as my main solution for server and workload protection, including intrusion detection and prevention for known and unknown threats, and integrity monitoring, which detects unauthorized changes to critical systems and configurations. Anti-malware and ransomware protection secures workloads from malicious files and processes, along with host-based firewall protection to control inbound and outbound traffic. I rely on Trend Micro Deep Security for day-to-day monitoring of alerts and events, applying security policies, updating security rules, ensuring compliance, and responding to incidents.

A specific example of how I use Trend Micro Deep Security in my daily work involves a critical vulnerability related to Apache Log4j that was recently announced. Before the patching, I checked the IPS module and had a virtual patch available. By enabling that rule for Log4j, all servers were protected from exploitation without waiting for vendor-released patches, preventing potential data breaches and downtime during the patching window.

“I use zero-day exploit mitigation with Trend Micro Deep Security. Whenever a zero-day vulnerability is announced, Trend Micro Deep Security's virtual patching via the Intrusion Prevention System protects workloads before vendor patches can be applied, and ransomware protection is also available. My team manages hundreds of servers across on-premise and cloud environments, and when a critical vulnerability is announced, applying OS patches manually would take days and require downtime. As a Trend Micro Deep Security engineer, I have virtual patching via IPS that instantly protects all workloads and systems without scheduling maintenance windows, eliminating emergency patching chaos, preventing downtime, and allowing faster compliance reporting. This enables my team to focus on strategic tasks instead of manual patching. The centralized dashboard also makes work much easier.

“In terms of automation, auto-deployment of agents integrates with cloud APIs and orchestration tools including Chef, Puppet, and Ansible to automatically install and configure the agents on new workloads. Policy automation applies protections based on tags or templates, ensuring that whenever a new server is created, it receives the right protection without manual intervention. Scheduled tasks automate malware scans, log inspections, and integrity checks at predefined intervals, and CI/CD pipeline integration allows checks to be embedded into

DevOps workflows, ensuring containers and workloads are scanned before deployment. .”

PrashantSharma6
Senior Professional 2 at Capgemini

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

The initial setup is easy, taking only about twenty to thirty minutes per server. I download the script, share it with the IT team, and either push the script to the centralized management console or deploy them on servers.

Ramesh Elayarajendiradoss Read full review

Endpoint Solutions Support at Compass Group

"In one premises, we deployed it on the cloud, which was challenging at the start, while on another it was set on TensorFlow, which was comparatively easy.."

Muhammad Huzaifa Khan Read full review

IS Analyst at a financial services firm with 1,001-5,000 employees

"It's not difficult to maintain because we have experience that when the customer is trained adequately, and if they are really concerned about security, they maintain it properly. They have the IT teams, security teams to look after the server endpoints and monitor them, patch them and if there is any vulnerability or any detection found on the endpoints, they try to mitigate that.."

M-Saleem

Read full review

Manager, Technical Microsoft at a computer software company with 201-500 employees

"Setting up Trend Micro Deep Security was fairly easy with proper preparation. The process required ensuring that the system met all requirements and that the network was correctly configured. You had to install the manager, set up the database, open the necessary ports, and deploy agents on each machine. A few steps, such as verifying software authenticity and synchronizing system clocks, required attention. Overall, with the installation guide and a bit of planning, the setup went smoothly, and once everything was configured, the solution started protecting the environment seamlessly.."

Abhimanyu Das

Read full review

Senior Cybersecurity Engineer at Kyndryl

“The product's initial setup phase was super easy. Trend Micro's team was there to support us when we were setting it up. The sales team and sales engineering team were also helpful.

If ten means very easy setup and one means difficult, I rate the setup phase a seven to eight.

Within business hours, the solution was deployed in two days, considering that there was a need to set up policies and servers..”

Anil Chauhan

Information Security Specialist at SG Fleet Group Ltd

Read full review

“I participated in the initial setup and deployment of Trend Micro Deep Security.

The setup process I participated in for deploying Trend Micro Deep Security involved first opening the necessary ports. For any solution to implement, I need to identify what ports are required for communication. Since it is Trend Micro, I need a connection to the Trend Micro database, where signatures and IOC details get updated. I also need a custom port or can use a default port for the console, which can be decided while configuring, and those ports must be accessible for the administrator of Deep Security. Additionally, I require bi-directional communication from the agent to the console where I install the Trend Micro Deep Security agent on the server. For installing Trend Micro Deep Security agent, a requirement is that it should have one GB of free space; those prerequisites are necessary for every solution, and similarly, Trend Micro Deep Security has its prerequisites that I must ensure before going for installation. Trend Micro Deep Security is available in both on-premises and cloud-based formats. For the cloud-based version, the console will be deployed in the back-end, and I only install the agent and ensure communication towards that URL. If it is on-premises, as I mentioned, I need to open the ports internally and towards Trend Micro. Trend Micro refers to the cloud version as Workload.

I have faced no issues during the initial setup of Trend Micro Deep Security. No issues have arisen because I understand the prerequisite requirements. Before proceeding, I review that Trend Micro has vast documentation available for known issues, along with implementation guides, user guides, and admin guides. With this information, I did not face any challenges. The only occasional issue arises when the agent becomes corrupted; they provide a solution by uninstalling it or using the cut tool from Trend Micro to remove the agent. Afterward, I reboot the server and reinstall it. Other than that, I have not encountered significant difficulties..”

Verified user

Security Consultant at a tech vendor with 10,001+ employees

Read full review

Customer Service and Support

"In terms of customer support, I think they need to exhibit more proactiveness. That is the lacking we are facing, and thus I believe they need improvement in customer support.."

MojammelHossain
Microsoft Security Department at a financial services firm with 501-1,000 employees

Read full review

"Customer support is very responsive and technically strong, and the ticket resolution time is very acceptable, as the engineers are knowledgeable and help resolve issues as soon as possible.."

Abhishek Motla
Senior Cyber Security Engineer at Capgemini

Read full review

"In my opinion, we have very good articles for customer support, and most of the issues have been solved with the help of these articles. If we do not get any resolution from KB articles, we can create a case. According to my service experience with normal support, an engineer is assigned to the case in 12 hours, and we get a resolution as soon as possible.."

Manish Kumar Twinkle
Security Engineer at itsipl

Read full review

"I have had a positive experience with Trend Micro Deep Security's customer support. The platform offers two types of support: normal and premium. I have used the premium support, which ensures immediate and efficient assistance. Even the normal support is far superior to that of other providers, such as Microsoft, whose response times are often much longer.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"I have interacted with customer support mostly for analysis when we encounter issues. About eighty percent of the time, we receive satisfactory responses, with the remaining twenty percent reflecting delays or the necessity for their internal engineering team to provide assistance.."

Harshit Tiwari
Web develope analyst at a tech vendor with 10,001+ employees

Read full review

"I often communicate with the technical support team of Trend Micro Deep Security; to be frank, I have not faced any recent technical challenges, so I have not raised any issues. I mentioned earlier that I possess considerable experience with this solution, allowing me to resolve many issues independently. In earlier stages, I faced challenges and raised multiple technical calls, receiving perfect resolutions on time, and the issues were fixed.

For the technical support received, I would rate them an eight from one to ten.."

Verified user

Security Consultant at a tech vendor with 10,001+ employees

Read full review

Other Advice

I believe my company is a partner with Trend Micro. I have been contacted regarding an incentive or a gift card for this review. I recommend everyone use Trend Micro Deep Security, as it is the industry leader at this moment and provides better security. My review rating for Trend Micro Deep Security is eight.

PrashantSharma6
Senior Professional 2 at Capgemini

Read full review

"My advice for others looking into using Trend Micro Deep Security is that they can proceed with the solution if they have a hybrid environment or a cloud environment, as it is suitable for all types of environments, and I would recommend it. My overall rating for this solution is 8.5 out of 10.."

Abhishek Motla
Senior Cyber Security Engineer at Capgemini

Read full review

"We are using Trend Micro Deep Security on our servers, which are in TAC mode. We can only monitor them, and the servers are behind the firewall. We are using the solution only in our LAN environment. There is no direct internet traffic on that server. Since we only work in the LAN environment, we don't get any IPS events. It is very easy to deploy the client and manage the console.

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

Vikas Saxena
Information Technology Manager at BCML

Read full review

I highly recommend Trend Micro Deep Security to anyone considering it. If you have prior experience with security solutions such as Microsoft Defender, Symantec, or Trellix, you will appreciate its user-friendly interface and straightforward management. The platform stands out for its simplicity, efficient policy deployment, and excellent technical support. It is definitely worth trying to experience the difference compared to other tools.

Although our organization purchased Trend Micro Deep Security through another channel, I do not recall the exact source. Overall, I rate this solution a solid ten out of ten.

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"I often utilize documentation, guides, or manuals for Trend Micro Deep Security. As mentioned earlier, prerequisite documents are always available. If I proceed with upgrades as well, I check the release notes provided by Trend Micro, detailing

the advantages, fixes from older versions, and known issues. Upgrade and installation guides are also accessible. When planning an upgrade, the upgrade guide specifies which version can be upgraded to and any installation details for later versions. There are numerous documents available, and as I mentioned, I ensure to go through those documents to perform upgrades, implementations, or configurations accordingly.

I am happy with the official documentation provided by Trend Micro.

I also work with a few more products including Zscaler and others from Trend Micro. At this moment, I collect reviews for Trend Micro InterScan Message Security, and I do work with that as well.

I gave this review an overall rating of nine.."

Verified user
Security Consultant at a tech vendor with 10,001+ employees

Read full review

"Trend Micro Deep Security prevents advanced attacks from third parties or attackers, and it helps us get log analysis of our applications and operating system.

Trend Micro Deep Security has eight modules: anti-malware, web reputation, device control, log inspection, integrity monitoring, firewall, and IDS/IPS rules. It essentially provides virtual patching, preventing our servers from all channels. When a signature-type attack or pattern-type attack happens, anti-malware will block it. When a user goes through a browser, web reputation will block threats. When any person executes something with the help of a pen drive, device control will block it. When a firewall pre-existing rule is there, it will block malicious sites, URLs, and IPs. Additionally, with the help of IDS/IPS rules, it will virtually patch our application or system.

In our organization, we must monitor the logs to see what is blocked or we get notifications of alerts that something is being blocked or some files are being affected, so we get an analysis of that part.

We have also used Trend Micro XDR, so it reduces the alerts. However, I believe we must check manually to determine whether a file is genuine or not. It reduces alerts, but we must check and apply false positives with trusted vendors, trusted sources, or trusted destinations.

Because we need to achieve a 10 out of 10 score, one point I deducted was for its long-term support. It provides new patches of agents to upgrade in one to two months, which is why I took off that one point.

For server security, I would advise others to try Trend Micro Deep Security with the full features, as you will definitely see an increase in performance. This review has a rating of 9 out of 10.."

Manish Kumar Twinkle
Security Engineer at itsipl

Read full review

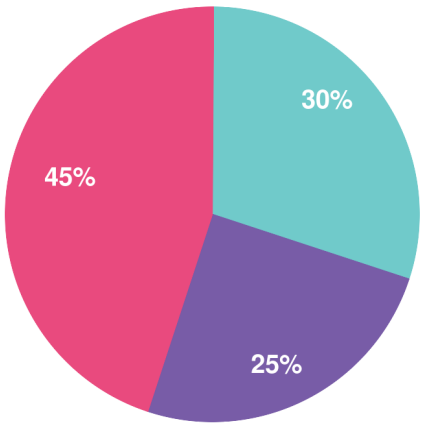
Top Industries

by visitors reading reviews

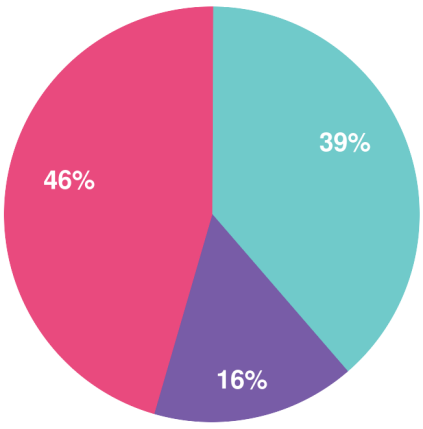
Financial Services Firm	16%
Manufacturing Company	9%
Computer Software Company	7%
Outsourcing Company	6%

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