aws marketplace

Cisco Secure Workload

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Cisco Secure Workload

Cisco Secure Workload Recap

Cisco Secure Workload is a cloud and data security solution that offers a zero-trust policy of keeping an organization's application workloads safe and secure throughout the entire on-premise and cloud data center ecosystems.

Cisco Secure Workload will consistently provide protection by discovering workload process anomalies, stopping threats immediately, minimizing the risk threat surface, and aborting any lateral movement.

Today's ecosystems are very elastic, and in the application-focused dynamic of today's aggressive marketplace, Cisco Secure Workload delivers a robust security solution that works effectively with today's most popular applications. The solution uniquely surrounds each and every workload to ensure organizations are able to keep their data, network, and applications safe and secure at all times. Cisco Secure Workload ensures that enterprise organizations can maintain secure applications by consistently building firewalls around every workload level throughout the entire ecosystem. The solution can manage applications that are deployed on containers, virtual machines, or bare-metal servers.

Cisco Secure workload is able to meet an organization's busy needs and offers flexible options such as Software-as-a-Service (SaaS) and on-premises options. Using the Secure Workload SaaS options, users receive all the benefits of Cisco Secure Workload protection without the hassle of having to deploy and maintain the platform on premises. Users are responsible for acquiring the necessary software licensing and deploying software agents. Using SaaS, Secure Workload runs in the cloud and is operated and maintained by Cisco. This option offers the ability to scale easily and is a popular choice for SaaS-first and SaaS-only clients. Many organizations find they get the best TCO and achieve the best productivity and profitability using the SaaS options.

When choosing on-premises options, organizations choose between hardware-based appliance models (large or small form factors). Platform selection is dependent on scalability goals, the desired fidelity level of flow telemetry, and the actual number of workloads. When a user chooses to configure Cisco Secure Workload for a conversation-only flow telemetry for all workloads, each platform has the capability to scale up vertically twice the default platform scale. Additionally, with Secure Workload, it is possible for the platform to be scaled horizontally in order to satisfy the demands of extra large widely distributed enterprise environments using federation capabilities.

Cisco Secure Workload also provides a robust disaster recovery (DR) tool, which helps to make it a complete, comprehensive solution. The DR allows for continuous restore and backup capabilities that enable users to quickly remediate operations and data to a standby cluster in the event of a drastic failure or disaster.

Reviews from Real Users

"The solution offers 100% telemetry coverage. The telemetry you collect is not sampled, it's not intermittent. It's complete. You see everything in it, including full visibility of all activities on your endpoints and in your network. Other valuable features include vast support for annotations, flexible user applications, machine learning, automatic classification, and hierarchical policies." - CTO at a tech vendor

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The only use case I can see that makes sense is micro-segmentation. I think there are other use cases for it. The main purpose of the product is to do micro-segmentation by collecting IP. That could be done by installing an agent, and then you have all the communication coming in and out. You could also use some flow sensors installed in the network that receive a copy of the traffic and then report that back to the system."

Torben Nissen Ernst

Technical Solutions Architect - Cyber & Cloud Security Expert at Secure Cloud

- "Generally speaking, Cisco support is considered one of the best in the networking products and stack."

Verified user

Partner at a consultancy with 1-10 employees

- "Secure Workload's best feature is that it's an end-to-end offering from Cisco."

Muhammad Marakkoottathil

Regional Presales Consultant (INS Division) at GBM

"It's stable."

Boris REYES

Sales Manager at Compuequip DOS

"The product provides multiple-device integration."

Sanjay Gaiswal

Technical Presales at Vcom Technologies

"The solution offers 100% telemetry coverage. The telemetry you collect is not sampled, it's not intermittent. It's complete. You see everything in it, including full visibility of all activities on your endpoints and in your network."

Verified user

CTO at a tech vendor with 11-50 employees

"The most valuable feature is micro-segmentation, which is the most important with respect to visibility."

Verified user

Solutions Architect at Liberty Global

What users had to say about valuable features:

"The most valuable feature is micro-segmentation, which can be used to deploy endpoint security along with the visibility of application and connection matrix

This product is simple to deploy, and provides visibility of connectivity between the endpoints/application.."

Verified user
Solutions Architect at Liberty Global

Read full review

"The most valuable feature right now is to do with having visibility on the network — especially on our servers — and to be able to enforce some type of security measures. This is mostly to combat processes that shouldn't be running on the servers.

The data analytics and all the data that it gathers are very useful. It creates a fast turn around to improve the speed of decision making so we can decide what we need to do to remain secure.."

Verified user
Network Engineer at a media company with 1,001-5,000 employees

Read full review

“The solution is very user-friendly, which clients appreciate.

The UI and GUI are fine.

It's stable.

We can scale the product.

Technical support is helpful and responsive. .”

Boris REYES
Sales Manager at Compuequip DOS

Read full review

“I used to be a big fan of Cisco Secure Workload and Cisco Tetration Platform. I used to really like it. However, the product has undergone significant modifications since then. Certain pieces of it have been moved into Cisco SD-Access, and the original DVR of the network functionality has been moved. As a result, the product has changed a lot since I was most familiar with it.

Regarding features, it's quite similar to scanning tools as it catalogs vulnerabilities and identifies their locations on your endpoints within the network. It operates on an agent-based system and uses a catalog and scoring function to determine where known vulnerabilities exist..”

Verified user
Partner at a consultancy with 1-10 employees

Read full review

"The most valuable feature of Cisco Secure Workload is its ability to streamline policy discovery. Once you create the workspace, it automatically identifies policies at various levels, whether you need finely-tuned micro-level or broader group policies. As data is gathered from all the agents, the system presents these policies, significantly reducing the need for multiple engineers who typically take much longer to create them. My IT risk colleagues utilize a process we call ADM, where they discover policies over a three to six-month period and present them to application owners. Once the application owners approve the policies, they can switch to enforcement mode in Cisco Tetration. This automation in policy presentation and access is incredibly valuable, as it minimizes manual intervention and the time required for policy discovery.

Micro-segmentation allows for precise enforcement of policies based on specific needs. You can implement tight risk postures, defining policies per IP, server, or port. This enables granular control or broader policies at the group level, grouping similar types of servers. The system automates this process; you specify your risk appetite and how detailed or general you want the policies to be. This approach protects servers that sit next to each other on the same VLAN without requiring large network firewalls to create multiple dependencies or DMZs. Instead, it leverages the existing firewalls on each server, allowing you to control policies centrally.."

Raj Metkar
Director, Head of Networks at MUFG, EMEA

Read full review

“The only use case I can see that makes sense is micro-segmentation. I think there are other use cases for it. The main purpose of the product is to do micro-segmentation by collecting IP. That could be done by installing an agent, and then you have all the communication coming in and out. You could also use some flow sensors installed in the network that receive a copy of the traffic and then report that back to the system.

No matter where you're getting the flow from, the system calculates all those flows. You know what the front end, the middleware, the back end, the database, and so on are so that you can group them. The system's strength is actually in proposing the policy. So, all web servers need to have HTTPS access to it.

Then, you can start building the policy for your application. When you have a policy, you can push that situation for self-service, which means you're trying out the policies you created in a real environment. Then, you can spend time trying to see if you have any escaped traffic, which means you have traffic that does not match the policy. If you were in enforcement mode, that traffic would be dropped. So you have a period where you can monitor if you have done the correct mode, seen all the traffic, and so on. That could be for a couple of weeks, that could be a month, or it could be half a year, depending on the criticality and how important your system actually is.

From my point of view, the strength is the policy proposal you're receiving. It's really good. That's the biggest challenge for everybody - creating a policy you could use in Cisco Secure Workload itself. You could also export it and use it in your firewall if you want to do that if you have a Cisco firewall setup. But you could also use it in every other enforcement part. I'm seeing what people are struggling with in companies - to actually restructure your CMDB data correctly, then get a policy that you can use in your network. I think that the tool is good at that..”

Torben Nissen Ernst

Technical Solutions Architect - Cyber & Cloud Security Expert at Secure Cloud

Read full review

Other Solutions Considered

"We did not evaluate other options because there are not many products in the market that offer this functionality. In fact, I think that Cisco is specifically covering the market for micro-segmentation and visibility of applications.."

Verified user
Solutions Architect at Liberty Global

Read full review

"The only other product we considered before deciding on Cisco Tetration is Illumio, which is a direct competitor. It is possible to string together multiple tools from the VMware side that can create similar functionality.."

Verified user
Sr. Regional Director, US East at a tech services company with 11-50 employees

Read full review

"We possible looked at a vRealize solution, but our customer did not want to consider VMware because it was not Cisco. The customer was a Cisco shop and did not even inquire regarding the price of the Tetration solution.."

Darko Petrovic
Brand Manager at Comtrade Group

Read full review

"We considered tools from Nutanix and ESX but decided to move away from ESX due to its vendor-specific nature. Each tool had its challenges, especially if we were to invest in a Nutanix solution. We wanted to avoid being locked into a single vendor's ecosystem. We quickly evaluated and eliminated those solutions, as we needed a technology-agnostic option that could operate across all our platforms.."

Raj Metkar
Director, Head of Networks at MUFG, EMEA

Read full review

"We initially only had the network monitoring and insight software. The network monitoring solution, SolarWinds, was the first. We also went back with Riverbeds as a unit model draft of the quality but that did not make sense to us. We tried integrating the application monitoring along with the network itself using a net flow but we were still not able to get the regular insights and the regular results that we're getting right now with the Tetration solution.."

RahulRao
Senior Manager Cloud Ops and Engineering at a comms service provider with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

"There is an immediate ROI when deploying this product. While it is hard to count in dollars, an organization will experience functionality that they never had before. The product creates cost savings in the allocation of resources but that goes much further than that. As an example, it is possible to recreate a database server that had no documentation and no backup. If that database were to go down, it would cost a company millions. Tetration can gather enough information to be able to rebuild that same database server and have immediate tell over and avoid that type of disaster.."

Verified user

Sr. Regional Director, US East at a tech services company with 11-50 employees

Read full review

Use Case

"The primary use case for us and our clients is to give the auditors the tools and the view on the network that we're in sync and that we're audible in what we do.."

fhofman
Works at a comms service provider with 10,001+ employees

Read full review

"Our primary use case of this solution is to analyze traffic. We have a route cluster of 2,500 nodes right now just in case the application is facing any delay or latency we wanted to have the visibility. It allows for insight into our data center.."

RahulRao
Senior Manager Cloud Ops and Engineering at a comms service provider with 10,001+ employees

Read full review

"We offer this solution to financial institutions. It complements the infrastructure of Cisco, routers, switches, and endpoints.

This is part of the suite of solutions that we offer.."

Boris REYES
Sales Manager at Compuequip DOS

Read full review

“When we onboarded Cisco Secure Workload, the usual use case was to discover internal application dependencies and create a dependency map for Cisco ACI. As the network team, we chose to implement ACI in a network-centric mode rather than an application-centric mode. However, we soon realized that Cisco Secure Workload's capabilities extend far beyond discovering dependency maps.

We use it for internal micro-segmentation. After evaluating it, we began using the agent-based solution across our server estate to protect our internal servers from each other and internal users. Today, our primary use case for the product is micro-segmentation within our internal network..”

Raj Metkar
Director, Head of Networks at MUFG, EMEA

Read full review

Setup

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

“The initial setup is straightforward. It doesn't take long to deploy. You just need to install the agents on the machines and if you want to install it on-premises then you use the cloud servers to help with the setup. The entire process takes a week or two. .”

Verified user

Solutions Architect at Liberty Global

Read full review

“The initial setup was straightforward. It took us about three days to deploy the solution. To reach your first operational capability, from then onwards, it depends on the scenario. We usually spend weeks, if not months, in order to adapt the system to the customer's use case and this requires professional services, specific for the situation..”

Verified user

CTO at a tech vendor with 11-50 employees

Read full review

“The solution's setup process isn't too easy or hard. It is moderate in terms of ease of implementation.

It's best to have one to two people available to handle deployment and maintenance. Even though one person can handle the process, it's good to have a backup if they go on vacation or take PTO. Usually, engineers can handle any task. .”

Boris REYES

Sales Manager at Compuequip DOS

Read full review

“The cloud-based solution is much easier to use than the on-premises solution. But if you want it on-premises, it could be a complex case to keep that up to date.

If you order a proof of concept or value, you'll get access to a cloud-based version if that's what you want to do. That's the easiest one. You'll get access to maybe 50-100 clients, and then you can start to install it. That's really easy. But the difficult thing is to provide the solution with the correct tags, and that's what everybody is struggling with - actually getting a good asset database. Usually, banks and the financial sector have a really good overview and registration for all the different services. A lot of other companies out there don't have that..”

Torben Nissen Ernst

Technical Solutions Architect - Cyber & Cloud Security Expert at Secure Cloud

Read full review

"I am not familiar with the current deployment options for Cisco Secure Workload, but it seems to involve deploying an agent, which is about as complex as other solutions. One significant difference among these products is how much they enable you to manage noise. Some criticisms of products like Palo Cortex or Rapid7 are that they are very noisy, with lots of false positives and alerts that customers do not consider actionable. In order for an alert to be actionable, customers need to know what steps to take to resolve it, and sometimes the products are not clear enough. Wiz has been differentiating itself recently by adding extra controls in the scoring, allowing for a custom component to the security scoring. This makes alerts less noisy and easier to focus on for customers who want fewer alerts coming out of the product. Security is a problem that never ends, and customers appreciate the ability to focus their activity since their teams can only handle so much at a time. Therefore, the more these products can do to be less noisy and provide clarity and focus, the better they will perform.."

Verified user

Partner at a consultancy with 1-10 employees

Read full review

“The concepts can be quite new without the right professional services support from Cisco, and security teams might struggle. Cisco's professional services team guided us through the process, helping us implement around twenty critical applications within the micro-segmentation framework.

Our deployment was straightforward. We simply connected two network cables and assigned some IP addresses, and the platform was operational within a day or two. However, the micro-segmentation of each application and the automatic discovery of rules took about a year to fully deploy for all twenty applications.

The process involved collaboration between two teams: the network team, which manages the Tetration platform, and the IT risk team, which focuses on policy decisions. We maintained the Tetration platform, handled updates, and engaged our IT risk colleagues to determine which IT risk policies needed implementation for various applications. They maintained a list of critical applications that required segregation.

Once we established this partnership, the IT risk team worked with application teams on auto-discovery and policy presentation. After deliberation and agreement on the policies, the network team enforced them. Our role primarily involved overseeing Tetration as a secure on-premises platform while assisting our IT risk colleagues, who were still learning, with decision-making supported by Cisco Professional Services.

At the senior management level, we decided which applications to include within the scope of Cisco Tetration. The process was structured to involve one application team at a time, helping them build confidence through testing. Once successful on day one, we deployed the application into production and established policies for service and request flows.

We also implemented a process for handling changes at the application level, using ServiceNow for requests to modify existing policies, similar to changing firewall rules. Additionally, we created a RACI matrix to clarify responsibilities: defining who was accountable for deploying agents, monitoring their

performance, and managing policy enforcement.

I would rate the experience a ten out of ten. .”

Raj Metkar

Director, Head of Networks at MUFG, EMEA

Read full review

Customer Service and Support

"Cisco's technical support has always been quite reliable since Cisco manages our rack. Whenever there was an issue, whether it involved replacing a switch or a physical server in a cluster, their support was helpful, and all replacements were completed on time.."

Raj Metkar
Director, Head of Networks at MUFG, EMEA

Read full review

"Cisco support has been really good. We have access to the guys who are programming or developing it. We've had good contact, and that helped us encounter all those issues we were facing, both bugs and knowledge around how to do stuff correctly.."

Torben Nissen Ernst
Technical Solutions Architect - Cyber & Cloud Security Expert at Secure Cloud

Read full review

"Generally speaking, Cisco support is considered one of the best in the networking products and stack. However, their support is not as good when it comes to higher layer products, such as software and application layer products.."

Verified user
Partner at a consultancy with 1-10 employees

Read full review

"We augment Cisco customer service and support for the product, so we generally do not require support. However, Cisco support is excellent and we never have any issues. We will always get the support that we need, whether it be from the business unit that developed it directly, or from the Cisco TAC.."

Verified user
Sr. Regional Director, US East at a tech services company with 11-50 employees

Read full review

"Technical support for this solution is really good. For this kind of solution, you have cutting-edge support. The only problem is that many of the specialists only speak English, which sometimes makes it difficult as we are a French company. Aside from the interaction with people, however, the support is really good. If you have a complex case then they work with you until you have a solution.."

Brice ABRIOUX
Information Security Engineer at ENEDIS

Read full review

Other Advice

“For me, the solution is a nine out of ten. I really like it. It's a great tool that will help give visibility to a data center and network, understand processes that are running within the data center and be able to enforce rules and regulations for all your processes..”

Verified user
Network Engineer at a media company with 1,001-5,000 employees

Read full review

“The suitability of Cisco Tetration depends on the strategy of any given organization. If your organization has a micro-segmentation strategy then this is a good solution. It works to improve visibility by creating connection metrics between applications and having the proper policy in place.

Overall, this is a really good product and I am happy with it.

I would rate this solution a nine out of ten..”

Verified user
Solutions Architect at Liberty Global

Read full review

“We are Cisco partners and resellers.

Normally, we deal with the most up-to-date version of the solution. It's typically a requirement of the client that we provide the latest.

I'd advise potential users to watch some webinars in order to understand the tool. Normally, we offer these solutions with training. That paying a premium for a new tool is always very good advice.

I'd rate the solution eight out of ten.."

Boris REYES
Sales Manager at Compuequip DOS

Read full review

"You need to have a team with a good understanding of your information systems in order to have benefits with this kind of solution.

My advice for anybody who is implementing this solution is to define what you want to use, and what you need from the tool. You can't have rules that are too strict in the beginning because otherwise, you can't go to production. Over time, you will have a clear view of what is ongoing with your information system. This allows you to improve step-by-step. This is a long-term approach.

This is a good solution, but it should be more user-friendly and easier to deploy agents.

I would rate this solution an eight out of ten.."

Brice ABRIOUX
Information Security Engineer at ENEDIS

Read full review

"We need two people, one from the IT risk side and one from the network side, for the maintenance.

Since deploying the Cisco Secure Workload, we haven't experienced any security incidents with our internal critical systems. While this implementation has increased our maintenance costs due to introducing a new product, it was necessary to meet internal segregation regulations. Without Cisco Tetration, we would likely have been forced to purchase multiple firewalls and create various DMZs, which would have consumed significant time and resources in networking and security maintenance. Traditional hardware solutions wouldn't have offered the same flexibility as Tetration, which allows us to use distributed firewalls on each server.

Deploying this platform across 20 applications has been much quicker than relying on physical firewalls, which would have led to a more macro-segmentation approach.

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

Raj Metkar
Director, Head of Networks at MUFG, EMEA

Read full review

"The tool is a complex system. I've been trying to install it myself. Normally, you can get a virtual edition. You can also buy a whole rack for it, where it ships all the appliances we need. And you can get it as a cloud version. Maintaining a system like that, upgrading it and patching it, keeping it running, and all those things are huge tasks. From my current view, because the pricing for it is almost the same for getting it on-premises compared to the cloud version, and all the services you're receiving around it, getting updates, patches, support, and all those things, it's a much better solution compared to having it on-site. Also, you need all the skills for actually keeping that system alive.

We have encountered a couple of issues normally based on the platform. We've seen a couple of issues on the Windows platform. We've solved some bugs during

the years we've worked with them. Some are related directly to ops, but some are also related to how we use the technology.

If you're interested in using Cisco Secure Workload for the first time, I'd ask you a few questions about what you want to achieve. Many customers say they have some crown jewels for which they need to do micro-segmentation. That makes sense. But at some point, you need to look at all your other systems. You could have a management backend setup or environment connecting to all your networks, your servers, and so on. Those environments must be in place, and micro-segmentation must be done on them. Otherwise, if people get access or hack those systems, you're in trouble because they have access to all your different systems, no matter what you're actually doing for micro-segmentation.

Before installing the agent on all hosts and starting to do micro-segmentation, you must look at your CMDB and asset database. Try to get the best quality. When you have that available and refined, you can start micro-segmentation. We need to ensure that every time you deploy a new server, it must be propagated into the system automatically. Otherwise, you could end up in a situation where you're blocking your traffic and denying service to yourself.

It would help if you had all those workflows in place. The next time a server is deployed, it needs to be propagated automatically into the system. So, all DNS servers, for example, are in one group. If they decide to deploy a new DNS server, that will automatically propagate into the system. So, others who are on micro-segmentation have access to it. Otherwise, it'll only be a static solution that you must maintain daily to see if something has been dropped. You need to monitor the system for dropped traffic, but you also need to automate everything.

I'm unsure I would want to apply Cisco Secure Workload on all hosts. What I would do is create or allow the application owners themselves. They could use Cisco Secure Workload or they could use another technology. It could also be using containers and stuff like that, Kubernetes, and so on. But I'd use Cisco Secure Workload to define a policy together with the application owners. Then I'd give that policy to the application owners and ask them if they want to use Cisco Secure Workload, or if they have another enforcement mechanism they want to use.

Here's the policy, then we need to enforce it. You can export that, put it in your documentation for the design document for the application and work with that.

That makes a huge difference for the application owners if they don't know what's going on in the application. When you're done with that, either you're going to keep the agent there and enforce it, or you can uninstall it and move to another target, a new application, and do the same thing. Depending on the criticality of the application, you could maybe use some of the policy in Cisco Secure Workload, or you could use it in other enforcement points out there.

Based on the way that you're collecting all the flows and can create a policy for you, I think that is really good compared to a lot of other systems that I have seen out there. So based on that, I would give it a nine out of ten. It's really good. There could be something with the price, maybe. But it depends on how you're using it..”

Torben Nissen Ernst
Technical Solutions Architect - Cyber & Cloud Security Expert at Secure Cloud

Read full review

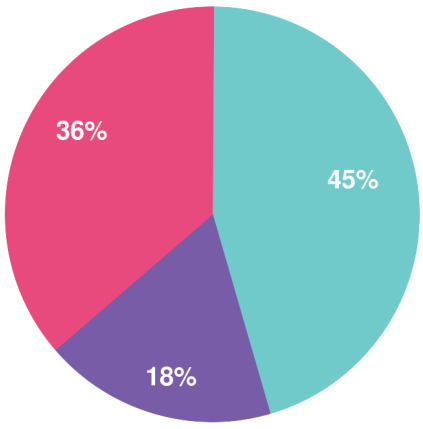
Top Industries

by visitors reading reviews

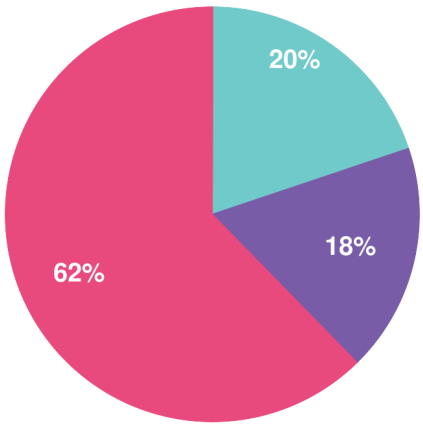
Manufacturing Company	13%
Financial Services Firm	10%
Computer Software Company	8%
Government	8%

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