aws marketplace

Unified Vulnerability Management

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Unified Vulnerability Management

Unified Vulnerability Management Recap

Unified Vulnerability Management provides comprehensive capabilities to identify and address security threats, offering detailed insights and proactive risk management within one platform.

Its integrated approach enables businesses to efficiently detect vulnerabilities across their digital landscape. With real-time analytics and robust reporting, Unified Vulnerability Management helps organizations prioritize security measures, ensuring critical vulnerabilities are addressed promptly. Its adaptable framework delivers seamless threat mitigation by aligning operational activities with cybersecurity goals.

What are the main features of Unified Vulnerability Management?

- Comprehensive Threat Detection: Identifies vulnerabilities in real-time across all systems.
- Integrated Risk Assessment: Prioritizes threats based on potential impact and exposure.
- Automated Reporting: Streamlines documentation for compliance and risk management.
- Scalable Architecture: Accommodates growing enterprise security needs efficiently.

What benefits should users consider in reviews?

- Improved Security Posture: Enhances threat detection and response strategies.
- Cost Efficiency: Reduces the need for multiple tools through integrated functions.
- Time Savings: Automates routine security tasks to focus on critical vulnerabilities.
- Enhanced Compliance: Simplifies meeting security standards and regulations.

In sectors like finance and healthcare, Unified Vulnerability Management tailored integrations align with unique security requirements. Its capability to adapt ensures that industry-specific standards are met while maintaining high operational security levels, delivering adaptable threat solutions tailored to specific sector needs.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- “Unified Vulnerability Management has centralized the process of identifying, assessing, prioritizing, remediating, and monitoring vulnerabilities across my organization's entire IT ecosystem through a single integrated platform and governance framework, making this the most significant advantage.”

Shaamim Ahmed

Director, Technology at AmericaTech, Inc.

- “In Unified Vulnerability Management, the best features include the ability to consolidate each and every device without dependency on other patch vulnerability management software, such as Qualys and SolarWinds, which have limited modules.”

Utpal Sinha

Sr Manager at HCL Tech

- “Based on my experience, the visibility and zero trust that Unified Vulnerability Management provides brings the biggest benefit.”

ADEOYE-AFOLABI

Head Of Network And Security at Nigeria LNG Limited

"The best feature of Unified Vulnerability Management is that it never shows actual details publicly and provides different virtual information to those coming from outside the company."

Bhaskar Rao

Network Manager Admin at Yamaha

"Unified Vulnerability Management gives a good overview and detailed visibility of all traffic, which allows me to easily find bottlenecks or issues."

Ahmed Azzuz

Service And Contract Manager at Colt Technology Services

"For me, the most appealing aspect of Unified Vulnerability Management for a customer or potential customer is the functionality."

Verified user

Cyber Security Architect at a manufacturing company with 1,001-5,000 employees

"Unified Vulnerability Management has positively impacted my organization by improving our response time to vulnerabilities significantly, reducing our average response time by 40% and delivering measurable improvements in our security posture."

Marco Spagnoletti

Shift Lead SOC Analyst at CYBEROO

What users had to say about valuable features:

"The best feature of Unified Vulnerability Management is that it never shows actual details publicly and provides different virtual information to those coming from outside the company. It does not give any actual information about any companies, making it very safe for any organization to protect their networks, which is why it is in high demand right now.."

Bhaskar Rao
Network Manager Admin at Yamaha

Read full review

"The best features Unified Vulnerability Management offers include comprehensive scanning and detailed reporting.

"The risk-based prioritization helps my team by allowing us to focus on the most critical vulnerabilities first.

"One aspect that stands out is the user-friendly interface, though there are enhancements I wish it had.."

Marco Spagnoletti
Shift Lead SOC Analyst at CYBEROO

Read full review

“Based on my experience, the visibility and zero trust that Unified Vulnerability Management provides brings the biggest benefit.

The scanning in Unified Vulnerability Management helps with vulnerability management by scanning applications and users' internet-bound traffic as well as data center traffic. It flags anomalies and measures against known vulnerabilities, known CVEs, and vulnerabilities, making it a process of filtering, scanning, and reporting of anomalies.

We are using the automated scanning feature in Unified Vulnerability Management..”

ADEOYE-AFOLABI
Head Of Network And Security at Nigeria LNG Limited

Read full review

"For me, the most appealing aspect of Unified Vulnerability Management for a customer or potential customer is the functionality. It is the grouping of numerous inputs into the solution.

"Unified Vulnerability Management collects information from other products and aggregates that information. The other products are the ones that perform all the scanning. Unified Vulnerability Management takes all of those inputs, bundles them into one platform. For instance, I have an antivirus solution that collects information about my workstations and provides the workstation name. I also have a vulnerability management solution that collects information about that laptop. Unified Vulnerability Management joins them all together using the key that is the laptop name and combines all that information from different sources.."

Verified user

Cyber Security Architect at a manufacturing company with 1,001-5,000 employees

Read full review

"In Unified Vulnerability Management, the best features include the ability to consolidate each and every device without dependency on other patch vulnerability management software, such as Qualys and SolarWinds, which have limited modules. It can work on both web and on-premises servers through a single centralized module that scans all platforms, including cloud and Software-as-a-Service, and can assess vulnerabilities related to TLS and DTLS, while on-premises scanning is also possible with a simple connector.

"We have configured automated scanning in Unified Vulnerability Management, but we also take precautions during this process. We implement temporary firewall blocks for specific ports that could damage the product, such as Portwide, which acts like a trojan; thus, we maintain limited automation, scanning for a specific duration on particular TCP ports within a determined IP range. The software includes an exclude option, which we utilize to avoid certain IP addresses or URLs.

"I can assess the ability to generate customizable compliance reports as effective; internally, it includes a tool, and if necessary, we export these reports into CSV format. Once in CSV format, we use Power BI for graphical presentation to stakeholders.."

Utpal Sinha
Sr Manager at HCL Tech

Read full review

“From Unified Vulnerability Management, credential scanning emerged as the most significant feature. Credential scanning identifies when someone attempts to log in to our network from outside, a capability that no other application recognizes. If someone tries to log in inside our network from outside, it will not be recognized by any other application, but Unified Vulnerability Management, especially through credential scanning, recognizes and prevents the operation.

“Credential scanning is important for Unified Vulnerability Management as it serves as the first line of defense against hackers attempting to enter your network. From my role as a cybersecurity design architect, this capability is crucial. Most EDR, XDR, and other protection tools may not catch these sophisticated attacks because hackers use AI and different methodologies to gain access. They act as real users, injecting usernames and passwords, which can easily compromise credentials and allow them inside the network. Other tools cannot detect such activity, which is why I focus intently on this and secured my credential environment.

“Unified Vulnerability Management is a very important part of my security strategy. My understanding shows that I have worked with many complete security postures, and vulnerability management is one of my areas of expertise. I believe that Unified Vulnerability Management is the backbone of any organization's security posture.

“Unified Vulnerability Management means a comprehensive security approach that combines vulnerability discovery, assessment, prioritization, remediation, validation, and reporting into a single centralized program platform. I can secure servers, workstations, network devices, and cloud resources including Azure, AWS, and GCP, especially from an American market perspective. It also includes applications, APIs, containers, Kubernetes, mobile devices, IoT, and DevOps elements. Unified Vulnerability Management prioritizes vulnerability scans to detect CVEs, ensuring continuous monitoring and assessment, tracking remediation progress, and automating patch deployment. It integrates threat intelligence and complies with standards including NIST CSF, 853, CIS control, ISO 27001, PCI DSS, and HIPAA.

“The features I rely on most day-to-day in Unified Vulnerability Management are

asset discovery, vulnerability management, patching, remediation, and threat intelligence. These are the most significant aspects for me. Additionally, I work to reduce security tool sprawl, achieve faster remediation patching, improve compliance readiness, enhance risk-based decision-making, and maintain visibility across hybrid and multi-cloud environments.

“I have used various solutions including Microsoft Defender Vulnerability Management, Tenable One, Rapid7, InsightVM, and CrowdStrike Falcon for vulnerability management. Additionally, I also utilize Wiz for cloud vulnerability management tools.

“Unified Vulnerability Management has centralized the process of identifying, assessing, prioritizing, remediating, and monitoring vulnerabilities across my organization's entire IT ecosystem through a single integrated platform and governance framework, making this the most significant advantage.

“I observe that Unified Vulnerability Management provides significant asset discovery, vulnerability scanning, and the capability to detect vulnerable CVEs, ensuring continuous monitoring and assessment that creates alerts if anything occurs. It also uses risk prioritization based on CVSS scores, threat intelligence, exploit availability, and business impact while emphasizing patching prioritized exploiting vulnerabilities..”

Shaamim Ahmed
Director, Technology at AmericaTech, Inc.

Read full review

Other Solutions Considered

More AI features would be welcome, and the price should be lower because it is becoming more expensive, and customers are already looking for alternatives because of the pricing.

Ahmed Azzuz
Service And Contract Manager at Colt Technology Services

Read full review

"I would compare Unified Vulnerability Management with other solutions and rank it around eight or eight point nine, definitely not reaching nine. Qualys is a good product in this space, but the challenge with Qualys is that multiple modules need to be purchased.."

Utpal Sinha
Sr Manager at HCL Tech

Read full review

"Comparing Unified Vulnerability Management with Cisco, there are crucial differences. For Cisco, you have more skilled engineers available to manage Cisco enterprise and technologies, but for Unified Vulnerability Management, you require training and a specific skill set. Support from Cisco is better from my experience.."

ADEOYE-AFOLABI
Head Of Network And Security at Nigeria LNG Limited

Read full review

"I previously used other solutions before Unified Vulnerability Management, particularly Tenable products including Tenable, Tenable IO, and Tenable vulnerability management for vulnerability scans.

"Before using Unified Vulnerability Management, I evaluated options including Azure Security Center, Microsoft Defender, Qualys, and Splunk, integrating these to enhance capabilities for vulnerability management. My primary focus is on Microsoft and Tenable, with limited use of Microsoft Defender vulnerability management before switching.."

Shaamim Ahmed
Director, Technology at AmericaTech, Inc.

Read full review

ROI

Real user quotes about their ROI:

"I see a very high return on investment with Unified Vulnerability Management.

The ROI with Unified Vulnerability Management is approximately 60 percent so far, given one year in the deployment. We have used Unified Vulnerability Management for less than one year, so I would say 60 percent so far.."

ADEOYE-AFOLABI
Head Of Network And Security at Nigeria LNG Limited

Read full review

"In terms of return on investment, I estimate it at around thirty percent annually. In a five-year period, we can see a full payback; for instance, comparing the cost with vendors such as Secureworks, hiring them for monthly scanning would yield higher expenses than maintaining Unified Vulnerability Management. Thus, we save around thirty to forty percent over five years.."

Utpal Sinha
Sr Manager at HCL Tech

Read full review

"I observe that Unified Vulnerability Management leads to significant returns on investment, in which automation reduces the need for human intervention. I can configure everything to operate on schedule; therefore, no need for manual operation is required. Everything scans automatically, creates reports, and generates ServiceNow tickets for remediation. It becomes a hands-free application that streamlines my processes greatly.."

Shaamim Ahmed
Director, Technology at AmericaTech, Inc.

Read full review

Use Case

"My main use case for Unified Vulnerability Management is to identify and mitigate vulnerabilities effectively. We have a unique workflow that helps streamline our vulnerability management process.."

Marco Spagnoletti
Shift Lead SOC Analyst at CYBEROO

Read full review

"Our major use cases for Unified Vulnerability Management include user identity, endpoint management, security management for endpoints, authentication, and authorization. We also use it to filter internet traffic from end users.."

ADEOYE-AFOLABI
Head Of Network And Security at Nigeria LNG Limited

Read full review

"We integrated Unified Vulnerability Management with the FortiGate firewall, and as of now, there are no challenges found. It is very easy to implement Unified Vulnerability Management with the FortiGate firewall.."

Bhaskar Rao
Network Manager Admin at Yamaha

Read full review

"Unified Vulnerability Management is used for vulnerability management, involving finding vulnerabilities on devices and providing recommendations. Based on these recommendations, we manually check the vendor pages for the necessary patches and version upgrades, and that work is manual, as we are not using any software for it.."

Utpal Sinha
Sr Manager at HCL Tech

Read full review

Unified Vulnerability Management provides a good overview and detailed visibility into all traffic, allowing me to easily identify bottlenecks or issues.

The platform's ability to generate customizable compliance reports is valuable because they are always available, and I can request the latest report with the most current data and upload it directly from the platform.

“Risk-based prioritization is very important for my resource allocation. .”

Ahmed Azzuz
Service And Contract Manager at Colt Technology Services

Read full review

“I am familiar with Unified Vulnerability Management through Tenable, which serves as my primary tool and playground. Unified Vulnerability Management is a universal vulnerability management tool. I have been using Tenable AI, Tenable AD, and Tenable IO for more than eight to nine years, approaching close to ten years of experience.

“I worked for TD Synnex, the largest distributor in the USA and globally. In my role as a senior cyber security architect, I implemented their Unified Vulnerability Management application across approximately 9,000 servers with global operations. I also worked for Caterpillar as a data security admin level four, which is the highest level of engineering role beside the America Tech. I found that they used vulnerability tools including Tenable and other vulnerability management solutions. Based on my understanding of the rhythm of business, I applied Unified Vulnerability Management principles and evaluated their capabilities from an engineering perspective..”

Shaamim Ahmed
Director, Technology at AmericaTech, Inc.

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 deployment process of Unified Vulnerability Management is straightforward because it primarily involves cloud support or deployment with few changes to the infrastructure.."

ADEOYE-AFOLABI

Head Of Network And Security at Nigeria LNG Limited

Read full review

Implementation is provided by Unified Vulnerability Management in my customer's environment. The time for implementation varies depending on the customer, but on average, it takes a few hours. More people are needed for implementation, and a project manager is assigned. It is necessary to have at least basic knowledge of the product, otherwise it is difficult to handle it easily.

Ahmed Azzuz

Service And Contract Manager at Colt Technology Services

Read full review

"Regarding implementation, I can say it is moderate, not easy and not very difficult. It should be a knowledgeable person who can deploy it easily, but for a non-knowledgeable person, it is difficult. I did not face any problems.

"Deployment for Unified Vulnerability Management may take a couple of months after planning, which takes about one and a half months. After planning, the deployment is a one-day job. Impact analysis, reviewing changes, and risk analysis take time, but with proper planning, the job for deployment will take one day.."

Bhaskar Rao

Network Manager Admin at Yamaha

Read full review

Customer Service and Support

Unified Vulnerability Management's support could always be better, and it would be beneficial to have an external party providing that service. I understand that Unified Vulnerability Management is exploring external parties to provide support as well. Currently, I would rate the support a seven.

Ahmed Azzuz
Service And Contract Manager at Colt Technology Services

Read full review

"I rate the technical support at Unified Vulnerability Management as very good; they respond immediately when I call for assistance. If necessary, they escalate issues to senior staff, and I have seen R&D personnel come and help us with problems, such as fixing certificate issues during calls. I give the support a rating of ten.."

Utpal Sinha
Sr Manager at HCL Tech

Read full review

"Customer support varies. After COVID, I find customer support lacking, and I am not sure why the principals do not prioritize it more. They focus on technology but also created community sites for users to ask questions, which often provides automated responses for common queries. For new issues, there might be a delay in receiving help, and sometimes it involves answering machines when calling for support, which can be frustrating. I believe OEM should consider refining their support strategies, employing better AI agents that can cover frequent questions and enhance their response to users.."

Shaamim Ahmed
Director, Technology at AmericaTech, Inc.

Read full review

"The technical support from Unified Vulnerability Management is adequate, but not as robust as Cisco; we still experience delays.

Regarding improvements to support, the response time could be better, but not the quality of support.

I would rate the support from Unified Vulnerability Management at six out of ten points.."

ADEOYE-AFOLABI
Head Of Network And Security at Nigeria LNG Limited

Read full review

Other Advice

"My advice for others looking into using Unified Vulnerability Management is to fully understand their specific needs and tailor the implementation accordingly. Overall, I have found it to be an invaluable tool in our security arsenal. I would rate this product a 9 out of 10.."

Marco Spagnoletti
Shift Lead SOC Analyst at CYBEROO

Read full review

"We do use automated scanning, and it will generate a report if any of our organization's assets have some unauthorized software that is non-compliant. Based on the report, we will work on understanding why it is non-compliant and what the reason is for its installation on end user assets, and we will mitigate that.

"I have not yet used Unified Vulnerability Management's remediation workflow tools, but we are working on it right now as that project is ongoing.

"About pricing, it is higher compared to others because Unified Vulnerability Management is demanding and more secure than other products since it does not give actual information of the customer, so it is a bit expensive. Organizations should choose to work on the pricing.

"I rate this solution an 8 out of 10.."

Bhaskar Rao
Network Manager Admin at Yamaha

Read full review

"For remediation, we do it manually, which is handled by another team. We have not used the remediation workflow tools in Unified Vulnerability Management.

The integration capabilities of Unified Vulnerability Management impact our overall IT security strategy positively. It integrates seamlessly with other systems and applications using APIs, and we do not have issues with integration, even with tools to generate tickets and reporting.

Risk-based prioritization is important for our resource allocation. When you refer to critical and non-critical vulnerabilities, we know what to focus on and what to tackle at any point in time.

With risk-based prioritization in Unified Vulnerability Management, it makes attention-driven decisions possible. We eliminate critical vulnerabilities as soon as possible using an agile process. Other vulnerabilities are worked on based on availability, so critical ones come first, then low and medium risks follow. It is really important.

I would rate this review at seven out of ten points.."

ADEOYE-AFOLABI
Head Of Network And Security at Nigeria LNG Limited

Read full review

"My advice to others looking into Unified Vulnerability Management is to consider Tenable One as my first choice. I tend to favor Tenable and its different use cases. For example, Microsoft Defender is advantageous only within Microsoft platforms, whereas Wiz is beneficial for cloud-only environments. Given more comprehensive needs, Tenable One stands out as compatible with most infrastructures. ServiceNow has a vulnerability response function, but I have limited experience with that. I have also looked into CrowdStrike, particularly their Exposure Management, but I have not explored it fully as it is newly released.

"Every technology is developing rapidly, and there is a growing emphasis on AI within this evolution. Just three years ago, AI was not as prevalent, but now it significantly enhances productivity and efficiency. However, it represents a double-edged sword; while largely beneficial, AI can also create risks. It learns from inputs, and if anyone employs bad prompts within an enterprise context, they might expose vulnerabilities without recognizing it. Therefore, I need to safeguard AI use alongside utilizing DLP systems to protect such instances, ensuring protective measures are in place for any potentially harmful inquiries made to AI.

"I rate this solution a nine out of ten based on my overall experience.."

Shaamim Ahmed
Director, Technology at AmericaTech, Inc.

Read full review

"I have not gone any further than initial awareness regarding Unified Vulnerability Management. I must admit that I did not know they even had an on-premises version.

"I have no idea if there were any challenges or complexities with the implementation of Unified Vulnerability Management because I have not deployed it.

"I suspect that Unified Vulnerability Management can generate customizable reports, but since I have not implemented it, I do not know.

"From my perspective, I use an antivirus solution and a vulnerability management solution. I also have a CMDB, so I already have those. Unified Vulnerability Management could potentially be my CMDB, but I do not know.

"My understanding is that Unified Vulnerability Management integrates with a number of known vendors that are in the marketplace, popular and common vendors. Therefore, I am guessing that the integration will work, but not having deployed it, I do not know.

"I cannot rate Unified Vulnerability Management in general from one to ten because I have not implemented the product. Conceptually, I think Unified Vulnerability Management is a great idea, but I do not know if it delivers. I can only tell the marketing information and not the real-life information.

"My overall review rating for Unified Vulnerability Management is five.."

Verified user
Cyber Security Architect at a manufacturing company with 1,001-5,000 employees

Read full review

"For a review, I can provide solutions such as Unified Vulnerability Management, Fortigate, Palo Alto firewall, and based on Gartner, I can see that Forescout is also a notable mention.

"We do use Unified Vulnerability Management.

"We have used the remediation workflow tools, but we do not fully trust auto-remediation. First, we manually validate whether it is truly a vulnerability or just a false positive alert because sometimes the version indicates a vulnerability, yet there is an available patch for that version. In those cases, we can exclude it manually, so there is no necessity to upgrade certain applications or servers. These false positive vulnerability logs do arise, and we manually filter those before applying changes to avoid potential outages. For instance, this week we focus on critical vulnerabilities, while in the next fifteen days, we will address high vulnerabilities, then move on to medium and low vulnerabilities, which we will prioritize only after more than ninety days.

"The integration capabilities notably influence our security strategy, as we have it integrated with Microsoft Defender, a scanner that provides critical input. We also utilize a DLP solution and a CASB solution, using ChatGPT and Copilot, with the current integration being mainly with Windows Defender.

"Risk-based prioritization is vital for resource allocation; for instance, we treat a CVE of ten as critical, and anything from nine point eight down to eight is considered critical. Between eight and seven is high, while below that becomes medium and low. Vulnerabilities rated six or seven are not acted upon urgently, while we respond immediately to vulnerabilities rated at ten and nine, aiming to fix them within the next fifteen days. During our quarterly scans, if we find three or four vulnerabilities across twenty to twenty-four different assets, we allocate tasks to the respective owners, providing them with the remediation steps and necessary patch details for formal change requests.

"Regarding the pricing for Unified Vulnerability Management, it is definitely not cheap; when compared to Qualys, it is more reasonable. It ranks high among the best software available, nearly matching the price of the Gartner number one product, which is Qualys. Rapid7 is also present, and it is lesser in cost than Unified Vulnerability Management.

"We have deployed Unified Vulnerability Management in both cloud and on-premises environments.

"I have been working with Unified Vulnerability Management products for a total of ten years, and specifically, we have been using the Unified Vulnerability Management scanning product for about four years. We initially checked it in two thousand nineteen and purchased it for five years back then, marking our experience with the product from its first stage.

"My overall rating for this product is nine out of ten.."

Utpal Sinha
Sr Manager at HCL Tech

Read full review

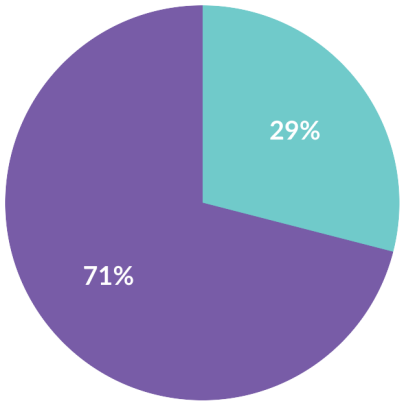
Top Industries

by visitors reading reviews

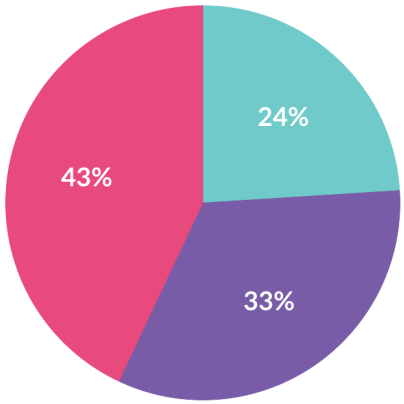
Construction Company	23%
Manufacturing Company	8%
Financial Services Firm	7%
Comms Service Provider	6%

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