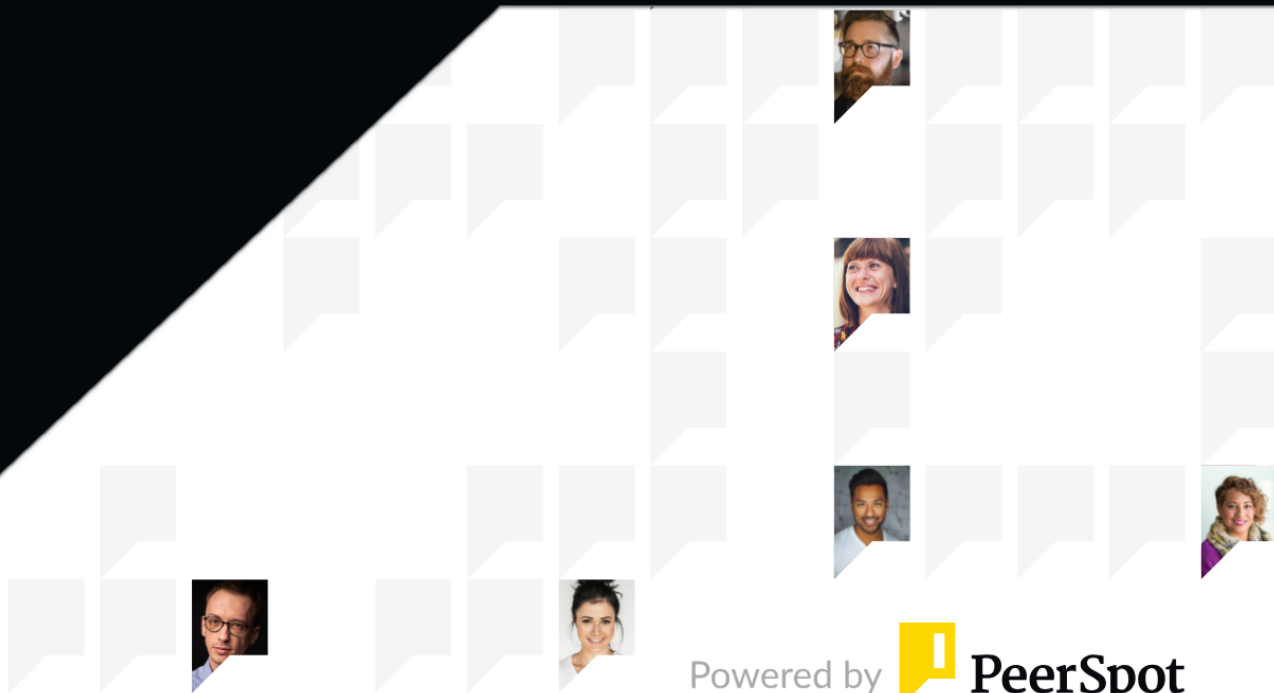




Rapid7 MDR

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 14

ROI..... 15 - 17

Use Case..... 18 - 23

Setup..... 24 - 26

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

Other Advice..... 30 - 37

Trends..... 38 - 39

About PeerSpot..... 40 - 41

Product Recap



Rapid7 MDR

Rapid7 MDR Recap

Security teams today need more than reactive detection and response. They need a preemptive approach that helps them understand where attackers are most likely to succeed and act before incidents escalate.

Rapid7 MDR delivers preemptive, AI-assisted detection and response across endpoint, identity, cloud, and email, combining native and third-party telemetry to provide full ecosystem visibility. By uniting vulnerability intelligence, asset context, and environment insight, Rapid7 helps organizations identify high-impact exposures and focus on the risks that matter most.

Through a transparent partnership model, Rapid7 works as an extension of your team, using AI to accelerate triage and investigation so experts can validate threats, contain attacks, and guide recovery with speed and precision. Beyond response, every investigation strengthens your defenses, creating a continuous cycle that reduces risk and improves resilience over time.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Once we introduced Rapid7 MDR along with their vulnerability assessment tool, IVM, we transitioned from using Qualys and Tenable, which are top-tier tools in the market, because the management tool from Rapid7 allows us to access a variety of vulnerabilities in real time to fix them effectively.”



Ehsan Khaleel

Manager SOC at PTCL



“In my opinion, the best features Rapid7 MDR offers are the 24/7 coverage with unlimited incident response and also the latest AI-driven alerts, which is one of the best features I have seen recently.”



Arun Arun

Application Security Engineer



“Despite the pricing being a consideration, I always recommend Rapid7 MDR first.”



Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET



“Rapid7 MDR has slashed our mean time to respond from several hours down to minutes and gives us enterprise-grade 24/7 SOC coverage without the massive overhead of hiring and staffing internally.”



Prateek Rao

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees



“Overall, Rapid7 MDR helps us to strengthen our security operations by providing continuous monitoring, high quality threat detection, and expert analysis support.”



Verified user

Soc Analyst at a manufacturing company with 10,001+ employees



“Instead of dedicating resources for around-the-clock monitoring, Rapid7 MDR acts as an extension of our security team, saving man-hours each month while improving detection and response capabilities.”



Venkata Kalla

Information & Security Engineer at Infosys



“Rapid7 MDR has positively impacted our organization by ensuring that alerts can come at any point in time, and we do not have to worry because someone is there to fix it proactively.”



Aritro Bhattacharjee

Product Specialist at Frontier Business Systems

What users had to say about valuable features:

“The best features for me in Rapid7 MDR are the fact that it automates network traffic with users and the attacker behavior analytics, known as ABA, rather than UBA. The user behavior analytics and the attacker behavior analytics are important because it is a network-focused sensor that measures real-life patterns of users and attackers, which many other products do not provide. Rapid7 MDR has that real-life metrics, and I have gone through their platform, which also allows customers to correlate the newest attack patterns and methods they are using. They update their database periodically and integrate it with their MDR, which is why I appreciate their ABA and UBA so much.

“The visibility of Rapid7 MDR is very accurate, and the transparency is commendable. If I am not too sure about its performance, I can correlate it with their cloud platform, which always has an updated dashboard about attacks. I also have access to the government database for correlation, and that shows they are doing real-time updates on these attacks, which is pre-built into the MDR. The accuracy and transparency for tracking are commendable..”

Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET

[Read full review](#)

“The best features that Rapid7 MDR offers are 24x7 alert monitoring, expert threat hunting, and high quality alert validation, which significantly reduces false positive alerts. I also appreciate the detailed incident investigations, actionable remediations and recommendations, and the ability to correlate the data from network and cloud environments. The service integrates all the security tools, and Rapid7 MDR analysts provide timely communication and valuable expertise that helps us to respond to attacks more efficiently.

“I think the best feature is reducing the false positive alerts so we, instead of reviewing many alerts ourselves, Rapid7 MDR analysts validate the incidents with the relevant context before escalating them. This significantly reduces the alerts and false positives, allowing the SOC team to work on only high priority alerts.

“Rapid7 MDR provides capabilities such as robust alert monitoring and investigation, and the Rapid7 MDR analysts already prioritize alerts and help the security analysts focus on high priority alerts only. Because of this, it improved our overall security posture and reduced the workload of the SOC analysts. With continuous monitoring, faster threat detection, and expert analyst support, we have been identifying security issues more quickly. Overall, it has ensured critical security events are detected and handled promptly..”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“The standout feature is their Insight Agent with Active Response, which lets their SOC isolate compromised endpoints immediately and without needing any manual intervention from us. Active Response stopped a potential ransomware outbreak over a long weekend by instantly isolating the endpoint.

“I also value the Attacker Model and endpoint visibility for strategic posture and guidance rather than just reactive alerts. Their AI governance is solid because they maintain a strict human-in-the-loop model, using AI for pattern recognition while keeping the expert analyst at the center.

“The accuracy and reliability have been excellent over the past few years. The AI triages quite dependably, classifying noise and correlating multi-vector events. I would rate the accuracy and reliability an eight out of ten. The AI triage is quite dependable at classifying noise and correlating multi-vector events, but it still requires human analyst validation, which ensures we avoid catastrophic false positives or missed threats.

“Their transparency is excellent because we share the exact same InsightIDR platform that their SOC uses to triage alerts. This means there is zero black box mystery. For example, when they isolated the endpoint for suspicious PowerShell activity, the investigation timeline laid out the precise command flags, the triggering user account, and the SOC analyst's commentary within minutes..”

Prateek Rao

[Read full review](#) 

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees

“The best features Rapid7 MDR offers include the ability to configure alerts, log ingestion, monitoring capability, and threat detection that correlates telemetry from multiple security tools to detect advanced attacks, with every high priority incident validated by Rapid7 analysts initially, significantly reducing false positives.

“I find myself relying most on the threat detection and investigation quality, as well as the threat intelligence, which has made a significant difference in the effectiveness of my incident response team.

“Rapid7 MDR is an excellent choice for organizations that want enterprise-grade threat detection and response without building a 24/7 in-house SOC team, combining expert analysis, high fidelity detections, broad integration support, and actionable incident response.

“Rapid7 MDR has positively impacted my organization by containing most of the false positives, as its in-house 24/7 team continuously monitors customer environments, enabling organizations to detect and respond to threats much faster.

“Measurable improvements include seeing a reduced number of false positives compared to other tools because Rapid7's in-house team handles most of them, and the faster threat detection reduces the mean time to detect from hours or days to minutes due to continuous monitoring..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“In my opinion, the best features Rapid7 MDR offers are the 24/7 coverage with unlimited incident response and also the latest AI-driven alerts, which is one of the best features I have seen recently. The integration models they have across different endpoints is also valuable.

“After the AI-driven alert triage was used, our time spent on identifying false positive alerts was reduced drastically because a large portion of our time was previously spent on identifying false positives and segregating them. After the AI-driven alert triage was implemented, this was directly reduced, which helped us identify actual alerts and work on them quickly. The AI enrichment also provides assets and vulnerability context even before a cybersecurity analyst gets into the picture.

“In terms of how Rapid7 MDR has impacted my organization positively, it has reduced our false positives after the AI feature was implemented. This reduction in false positive alerts gave us 24/7 coverage without having an in-house SOC team. It also helps us connect various endpoints to identify, detect, and monitor various endpoints across multi-cloud environments. It has helped us maintain our security posture on a day-to-day basis to keep our systems safe and secure, monitor our user usage, and identify vulnerabilities and asset criticalities.

“Previously, the need for multiple analysts and multiple security personnel was reduced after the AI implementation. It gave us detailed response information, detailed incidents, and reduced false positives. It also provided us with the reports we needed for further analysis and gave us the gist of what the incident would look like and what would possibly be going wrong. It has reduced the number of billable hours and also gave us time to work on other improvement factors, which has actually reduced our overall human billing..”

Arun Arun

Application Security Engineer

[Read full review](#) 

“The best features Rapid7 MDR offers include proactive threat hunting, as simply reacting to alerts will not work in today's sophisticated security landscape.

“There are many instances where proactive threat hunting has helped our organization catch threats that could have been missed; people take their laptops home, and we have zero visibility, but with this MDR solution, we have peace of mind.

“Regarding Rapid7 MDR's AI capabilities, I find it very positive and it provides a lot of help in audits and has a robust pre-authorized framework with strict controls.

“Speaking about Rapid7 MDR's accuracy and reliability of output, I have to give it a ninety-nine percent rating, as there are very low false positive rates with accurate vulnerability scoring.

“The transparency of Rapid7 MDR regarding gaining visibility into detections and investigations is outstanding, with the dashboard being the best in its class and centralizing telemetry data effectively.

“The inclusion of digital forensics and incident response within the MDR service significantly improves our incident recovery process by providing historical timelines and root cause analysis.

“The risk-aware detection features in Rapid7 MDR are unique, as they eliminate guesswork by cross-referencing alerts and helping to prioritize realistic attack paths.

“We have used the multi-vector telemetry feature in Rapid7 MDR, and it greatly improves the accuracy of our investigations through true correlated visibility across platforms.

“Having a dedicated cybersecurity advisor through Rapid7 MDR impacts our security program by aligning it with business needs thanks to their industry expertise and knowledge on mitigating attacks..”

Aritro Bhattacharjee

Product Specialist at Frontier Business Systems

[Read full review](#) 

Other Solutions Considered

“We evaluated many other solutions for various situations, but ultimately we chose Rapid7 MDR because of the price and the service, which were perfect for us..”

Verified user

Security Engineer at a retailer with 201-500 employees

[Read full review](#) 

“We have Rapid7 IVM and SIEM, and we are still using them. We have now added Rapid7 MDR as a service, which reflects our previous positive experience with Rapid7 solutions..”

Verified user

Security Engineer at a retailer with 201-500 employees

[Read full review](#) 

“The key differences between Rapid7 MDR and competitors such as ManageEngine or Sophos technologies are minimal as both OEMs have different approaches to implementation but aim for the same goal. Rapid7 MDR excels in accuracy over Sophos, especially concerning real-life monitoring, which is a significant differentiator for me..”

Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET

[Read full review](#) 

“The main competitor for Rapid7 MDR would be CrowdStrike, in my opinion.

“I have not looked into CrowdStrike; I do not know the specifics of what they call it, but they have the big offerings as well..”

JensWolf

Systems Administrator at a consultancy with 51-200 employees

[Read full review](#) 

“We previously managed an on-premises SIEM using Splunk with fragmented endpoint tools. We switched because the operational overhead of tuning custom correlation rules, constant log ingestion cost spikes, and staffing were becoming quite unsustainable for our team..”

Prateek Rao

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

“We were using an in-house SIEM before with different use cases and analytics. It did not give us more insight into the logs that we were fetching. The benefits that came with Rapid7 MDR is the analysis we are getting now, which is quite useful..”

AbhijeetSharma

Senior Project Engineer at CDACINDIA

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen a return on investment; the productivity metric shows that the same teams who used to handle alerts manually can now focus on proactive work because this is taken care of by someone else..”

Aritro Bhattacharjee

Product Specialist at Frontier Business Systems

[Read full review](#) 

“Rapid7 MDR has provided a clear return on investment by significantly reducing the time my internal security team spends on alert triage through validated investigations and actionable recommendations..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“We saw an ROI. We saw specific cost reductions. We used to pay extra for external user insight and vulnerability management in our old setup. Now, that's all included in Rapid7, which saves us money and simplifies vulnerability management..”

Oluwaseun Sonaïke

Head, Networks And Security at First City Monument Bank Limited

[Read full review](#) 

“I have seen a positive return on investment concerning Rapid7 MDR, as we have invested wisely, yielding results in detection mechanisms. I can confidently say that investing in Rapid7 MDR has been worthwhile, despite acknowledging that every tool has its flaws. Overall, the category is very good..”

Ehsan Khaleel

Manager SOC at PTCL

[Read full review](#) 

“We have seen definitive ROI across key metrics. Head-count avoidance as a primary metric has saved us three to four SOC analysts, which equates to roughly \$400,000 to \$500,000 in salaries and overhead. Engineering hours saved amount to almost 25 to 30 hours per week. Speed to resolution has increased quite dramatically, with MTTR down from several hours to just minutes..”

Prateek Rao

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

“I would not be the right person to talk about the money saved, but I could say there has been lots of time saved since we have onboarded Rapid7 MDR. The need for cybersecurity personnel has also been reduced.

“We were directly using Rapid7 MDR as the first solution.

“The inclusion of digital forensics and incident response within Rapid7 MDR service has positively impacted my incident recovery process, both operationally and financially. During an incident, creating a separate retainer or negotiating scopes and often waiting for external responders to onboard before meaningful work could begin could actually delay our recovery time. However, with Rapid7 MDR, DFIR is fully included in the services, which means there is no hourly fee, no caps, or engagement limit. This means our forensics begins immediately, which gives us an upper hand. In terms of financials, we do not pay additional fees for investigators or separate tools to onboard or for negotiations on retainers..”

Arun Arun

Application Security Engineer

[Read full review](#) 

Use Case

“My main use case for Rapid7 MDR is providing protection where manual intervention from the company side is almost zero, which is essential for maintaining effective security.

“The main point is knowing that someone is managing, not only selling, the complete solution we deployed and are fond of, and that is the backbone of our use case..”

Aritro Bhattacharjee

Product Specialist at Frontier Business Systems

[Read full review](#) 

“Network detection and response is basically what I use Rapid7 MDR for, and it is a very good solution for that. I am using Rapid7 MDR for Microsoft environments, confirming its utility within those systems. I take advantage of the expanded ecosystem telemetry support offered by Rapid7 MDR. I have used InsightIDR, which is a SIEM for Rapid7, and InsightVM for vulnerability management. I appreciate their approach to detecting threats, and I consider it one of the best OEMs for threat detection and response, whether dealing with network issues, mobile devices, or user behaviors. Despite the pricing being a consideration, I always recommend Rapid7 MDR first..”

Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET

[Read full review](#) 

“My main use case for Rapid7 MDR is to monitor incidents and ensure our applications are secured. I also want to make sure we are proactive in identifying threats.

“I use Rapid7 MDR daily as part of our security process. My workflow starts on a day-to-day basis by checking the dashboard for overnight alerts to see if there are any incidents and to investigate them. If there is any incident that needs to be escalated to my SOC team, I handle that accordingly. It is mainly to monitor the applications 24/7 for any incidents or alerts. We also use Rapid7 MDR to investigate user activities.

“We also use Rapid7 MDR for threat hunting with custom queries and for reports on a weekly and monthly basis to find how many incidents have occurred and to get all those details..”

Arun Arun

Application Security Engineer

[Read full review](#) 

“My primary use case of Rapid7 MDR is to do 24/7 threat monitoring and managed detection and response. We use it to identify suspicious activity across endpoint, network, and cloud environments and investigate the alerts and reduce false positive alerts through analysis.

“One of the examples was we used Rapid7 MDR to detect a suspicious malware activity or PowerShell activity on a user's device. Rapid7 MDR can correlate that endpoint element with network authentication and identification, and it finds if it has suspicious activity and then escalates it with details. The alert had already been validated and with context, we were able to isolate the affected endpoint, investigate the user's activity, and confirm the incident. At the same point, Rapid7 MDR filtered several benign administrative activities such as PowerShell execution, which significantly allowed us to focus on genuine threats.

“Overall, Rapid7 MDR helps us to strengthen our security operations by providing continuous monitoring, high quality threat detection, and expert analysis support. The contextual investigation and actionable recommendations have improved our SOC response and allowed the SOC team to focus on high priority activities rather than spending time on false positive alerts..”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“Rapid7 MDR has been our primary 24/7 managed detection and response solution software throughout the two and a half years we have been using it.

“Recently, Rapid7 MDR flagged and automatically contained a suspicious PowerShell execution on an endpoint device. Once Rapid7 MDR contained the endpoint, the team provided a full forensics summary showing the malicious script that was attempted, which was basically a credential harvesting attack. Our internal team removed the compromised user tokens and re-imaged the machine, then pushed the updated detection rules that resulted in zero lateral data movement or data loss.

“Beyond the standard endpoint detection, Rapid7 MDR acts as a true extension of our lean security team and is integrated directly into our SIEM and Slack for instant escalation.

“We primarily run on AWS alongside some Microsoft Azure workloads integrated with our on-premises data centers. Rapid7 MDR ingests CloudTrail logs and monitors identity and activity across all those environments..”

Prateek Rao

[Read full review](#) 

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees

“My main use case for Rapid7 MDR is to manage detection and response, SIEM, and other threat management solutions from Rapid7, including the vulnerability part.

“I use Rapid7 MDR in parallel to Rapid7 SIEM, where all the logs are ingested and where I carry out investigations and incident response activities.

“The transparency of Rapid7 MDR detection is high, with detailed insights into each incident, including analyst notes, supporting evidence, attack timelines, and recommendations for remediation.

“The risk-aware detection features in Rapid7 MDR are effective, as they help me focus on significant threats by correlating telemetry to identify realistic attack paths and prioritize incidents based on actual risk.

“Having digital forensics and incident response included in Rapid7 MDR has greatly improved my incident recovery process by helping me determine root causes and the extent of compromises.

“I utilize the integrated MDR for Microsoft environments, experiencing great visibility and effective incident response through this enhancement..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[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 setup process for Rapid7 MDR is always easy and straightforward. All their products are quite easy to implement; I do not need to overthink it. Reading the datasheet to understand it shows that it is not difficult at all..”

Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET

[Read full review](#) 

“I cannot speak to how the initial setup was because we had Rapid7 IVM and SIEM before, and that setup occurred before my time. The setup for Rapid7 MDR was very simple because we already had half of the infrastructure in place..”

Verified user

Security Engineer at a retailer with 201-500 employees

[Read full review](#) 

“The deployment setup process for Rapid7 MDR is straightforward. I have deployed both the cloud environment and on-premises Nexpose service. Their services, whether on-premises or cloud-based, are easy to deploy, and the endpoints are lightweight and compatible with other tools in our environment..”

Ehsan Khaleel

Manager SOC at PTCL

[Read full review](#) 

“Based on my experience, it is really easy to start working with Rapid7 MDR; you are up and running in a day or two.

“The initial setup process for Rapid7 MDR is really easy; it was really easy for us..”

JensWolf

Systems Administrator at a consultancy with 51-200 employees

[Read full review](#) 

“The initial setup is straightforward. To install the Rapid7, sensor and pull off kit, we only need less than a day.

I rate the initial setup an eight or nine out of ten, where one is difficult, and ten is easy..”

Nuki Agustino Wono

Senior Security Consultant at ITSEC Asia

[Read full review](#) 

“The initial setup of Rapid7 MDR is relatively easy because it integrates everything. However, the complete setup process is challenging due to the numerous modules involved. This includes cloud deployment, on-premises implementation of network devices, data collection, and agent installation. Implementation is manageable for existing Rapid7 customers, but it can be very challenging for new customers..”

Hiroshi Watanabe

Marketing Expert at J's communication

[Read full review](#) 

Customer Service and Support

“I would rate Rapid7 technical support as definitely a 10, because whenever we have had any problems, it is really fast and sensitive to our knowledge. I get the help I really need, and it is fast, so it is really good..”

JensWolf

Systems Administrator at a consultancy with 51-200 employees

[Read full review](#) 

“Customer support and the SOC are both top-notch and quite responsive. They respond within minutes, especially for critical escalations, and are backed by a dedicated customer success manager for regular check-ins. I would give the customer support a nine out of ten..”

Prateek Rao

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

“If we talk about different vendors, there is competition, but the user interface of Rapid7 MDR is quite useful for us. The support is also good. There are different vendors which have more experienced staff. However, Rapid7 MDR has been the best in zero-day attacks and the vulnerabilities that come into picture. We prefer that..”

AbhijeetSharma

Senior Project Engineer at CDACINDIA

[Read full review](#) 

“Regarding Rapid7's support team, I must say that their response time is not as quick as I would prefer. While they do respond, it can take a few days or even a week to get on a call.

“On a scale of one to ten for tech support, I would rate them a seven. The support is good overall, but I believe the pace of response could improve..”

Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET

[Read full review](#) 

“Customer support is excellent, and they promptly connect whenever I raise a request, which I would rate more than nine.

“I chose 9.5 because of their excellent customer support, efficient integration processes, and active communication during high incidents, helping my internal security team effectively handle critical situations..”

Prajwal Chougale

[Read full review](#) 

SOC L2 Analyst at a tech services company with 51-200 employees

“Getting responses from any service industry is challenging. We have an SLA, especially those SLAs from which we really need support based on our customer expectations, particularly for our developers. Every machine has Rapid7 MDR installed. We have our own IT department that is enabled with all training. The thing is that we do not directly rely on Rapid7 MDR for support, but we have built up our own competency with Rapid7 MDR. Only for very urgent issues do we get support from Rapid7 MDR, but that also depends upon the contract. We do not have extensive experience where we frequently interact with Rapid7 MDR, but wherever there is a setting, configuration management, or something similar, we are getting support from their technical or non-technical staff. It is about how you build your relationship with them. We are training our employees and providing them with training, and once they are trained, we believe this is a common shared responsibility..”

Shrikrishna Kashid

[Read full review](#) 

Senior Technical Service Engineer Expert at a tech vendor with 10,001+ employees

Other Advice

“Ensure that you negotiate pre-authorized containment thresholds clearly during onboarding and use marketplace commits like CTP to simplify procurement. I would rate Rapid7 MDR overall an eight out of ten..”

Prateek Rao

PARTNER & MANAGING DIRECTOR at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

“My advice to others is to choose Rapid7 MDR if you want a cost-effective SIEM solution backed by a great security support team.

“I benefit from using AI-assisted risk-aware investigation workflows, which streamline investigations by correlating all relevant alerts and details into a single workflow, reducing manual effort in triaging incidents.

“I gave this product a rating of 9.5 out of 10..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“Rapid7 MDR provides valuable visibility into security events, vulnerabilities, and risks, which relates to governance and security. The reporting and logging capabilities support all our readiness, help demonstrate security controls, and efficiently manage processes in our organization. The combination of AI-driven insights and expert analyst validation provides a well-balanced approach where automation improves speed while human expertise ensures accuracy. I particularly

appreciate the Rapid7 analyst detections and investigations, which reduce alert fatigue, improve threat visibility, and speed up our security operations. Rapid7 MDR is a primary detection response service that makes it safer to say that our organization is well-protected.

For compliance support, Rapid7 MDR provides good visibility into vulnerabilities, threats, and security. When suspicious login activity is detected by Rapid7 MDR, the MDR team provides detailed information, including the affected user account, source IP address, and timeline of events, which helps us validate the event. The transparency is very good for Rapid7 MDR.

Rapid7 MDR follows a structured risk detection process that combines automated analysis and threat intelligence. It collects data, logs, and telemetry from endpoints, servers, and cloud environments, then enriches the data against multiple data sources and analyst validation.

The multi-vector feature is one of the best features, as it analyzes and correlates data across multiple attack vectors such as endpoints, identity, cloud environments, network, email systems, and other security tools. For example, an attacker may compromise a user account through phishing email, log in from an unusual location, and then try to access sensitive cloud resources. Individually, these events might appear harmless, but Rapid7 MDR correlates and analyzes data from email, identity, and cloud environments to recognize this attack chain and generate a high-fidelity alert. The benefits of multi-vector detection include better visibility across the attack, detection of complex attack chains, reduction of blind spots, improved threat detection accuracy, faster incident investigation, and providing better context for analysts.

The ecosystem is supported through endpoint telemetry, processing, and file activity, which has a significant positive impact on our security program. Rapid7 MDR is integrated with Microsoft and our other security tools. We are using AI-assisted risk workflows, including data ingestion, AI-based analysis, risk scoring and prioritization, analyst validation, investigation, and containment. The ecosystem supports endpoint telemetry, processing, file activity, and user behavior.

My overall review rating for Rapid7 MDR is 7 out of 10..”

Venkata Kalla
Information & Security Engineer at Infosys

[Read full review](#) 

“We have not used the multi-vector telemetry feature in Rapid7 MDR.

“We have not used the integrated MDR for Microsoft environments feature.

“We use the AI-assisted risk-aware investigation in Rapid7 MDR and it has impacted our triage by providing detailed context. It gives us detailed impact analysis and also does a deep analysis on what the threat could be and what the potential causes are. It also does a root analysis and gives us the impact event, impact asset, and also what a possible solution could be. This has made the security alert solving easier and faster to resolve.

“We have not used the expanded ecosystem telemetry support.

“I do not have anything else to add about the features.

“I do not have any other improvements needed for Rapid7 MDR that we have not discussed yet.

“I would need some time to think about the transparency of Rapid7 MDR in terms of gaining visibility into detections and investigations.

“Rapid7 MDR's risk-aware detection features have created a very meaningful positive impact. The integration between the detection and exposure management within Rapid7 MDR unified platform means that the team can actually work on threats that impact the business rather than other threats. Vulnerability data, assets, critical user identity context, and attack path information all feed directly into the detections. When an alert actually fires, it evaluates the isolation and gives us the ability to focus on what needs to be fixed.

“It has reduced 60 to 65 percent of false positives, which is actually very helpful and is good because it is almost near to accurate. The reasoning is also almost correct. I would say it is learning day by day but it is actually performing well.

“In terms of Rapid7 MDR's AI governance and security, it is more transparent because with the AI capabilities, it has made a transparent approach to governance and security. This means it gives us the ability to see how alerts are triggered and on what actions, and also provides a list of details on the transparency of what AI takes action on and what decisions it has made. Every AI-driven triage decision is

auditable and gives us a flow of what has been taken. Because auditing is one of the major factors in compliance, we are able to see what all decisions and when and what factors have made that decision. We can see the reasoning, the evidence considered, and the outcome. From the governance standpoint, the human analyst is still in the loop across the triage cycle.

“My overall review rating for Rapid7 MDR is seven out of ten..”

Arun Arun

Application Security Engineer

[Read full review](#) 

“We are utilizing the AI-assisted risk-aware investigation workflows in Rapid7 MDR. They help us improve our alert triage and prioritization by providing context around the alerts, identifying the risk factors, and helping analysts to focus on more critical security events. Instead of treating every alert with the same priority, the workflow considers factors such as asset criticality, behavior, threat intelligence, and attack patterns to determine the potential impact. This has helped in reducing false positive alerts and overall alert fatigue, and in speeding up the investigation of the real threats.

“Rapid7 MDR AI capabilities are good for improving threat detection and alert prioritization and also in the investigation. From the governance and security perspective, I think they have strong controls around data handling, access management, and transparency, which helps in improving data security. Also, the combination of AI-driven analysis and Rapid7 MDR analysts provides a good balance where AI can help identify attack patterns quickly, while human experts validate findings and make the response decisions.

“Rapid7 MDR is quite good and I appreciate the responses. I use it on a daily basis. I think it is really reliable as compared to the other platforms which I use, and it helps in reducing the investigation time by providing additional context and highlighting the important points.

“The inclusion of the forensics and incident response capabilities has improved our investigations by providing deeper analysis and helping us to understand the scope of the threat and the impact of that on the environment. The forensic analysis also helps us identify the root cause, the affected systems, attackers' activities, and required remediation steps.

“Rapid7 MDR has a few features that I think are very valuable because it goes beyond simple alert generation and focuses on the actual risk and potential impact of that risk in our organization. By considering factors such as important assets and user behavior, threat indicators, and the context of the attack, we can better assess our security posture.

“I have used the multi-vector telemetry capabilities in Rapid7 MDR. It has helped me in improving investigation accuracy by correlating the data across different endpoints, user activity, and network activity. Having visibility across different telemetry sources provides better context for the alerts and helps us differentiate between legitimate and potential threats.

“Cybersecurity advisor helps us make decisions by providing expert guidance and helping us focus on the risks and threats that matter the most to our business. They help us understand our security gaps, identify additional improvements, and also align our security strategy with the business requirements. This also ensures that our resources are used effectively and that security supports the organization's overall goals.

“Currently, we are not using the integrated Rapid7 MDR for Microsoft environments feature. I think our team will be enabling that in the upcoming time.

“My advice is that Rapid7 MDR is a good fit for organizations that want to use it for 24/7 security monitoring and expert investigation support. It also helps in reducing the workload of the internal SOC teams. With the help of this, SOC teams can mostly focus on the high priority alerts instead of wasting time on the false positives. I think this is a really good tool to have. I would give Rapid7 MDR a rating of eight out of ten because of its 24x7 monitoring capability and valuable analyst expertise that improves our security operations..”

Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“Having a dedicated security advisor through Rapid7 MDR positively impacts my alignment of security programs with business needs. As a security personnel using this for most of my customers, I can tell that the database is well updated. It gives me the most updated software for security regarding attacks and user behavior, which is crucial for business.

“The key benefit of Rapid7 MDR is the way it automatically deploys on a port for me. I look at how to strengthen my customer's environment, ensuring that every IP address internally is accurate. Rapid7 MDR helps eliminate phishing IP addresses on the network, identifying and immediately rectifying them. It also deals with alert fatigue by preventing flooding of the dashboard with raw network anomalies and attacker behaviors. Their incident response is very quick; whenever there is a detection, they respond immediately. Some detections go to the administrator for approval, but with Rapid7 MDR, I can cancel and ask questions later, making it highly recommendable for real-time resolution, reducing alert fatigue, and addressing IP guessing.

“With respect to risk-aware detection features, Rapid7 MDR provides full visibility into blind spots. I think I know my network, but I do not; Rapid7 MDR gives me full-time visibility and accurate data about things I am not seeing or paying attention to. Their third-party dashboard allows tracking of specific devices, which is essential in an enterprise environment where I cannot check each endpoint individually. Rapid7 MDR streamlines the information down to the exact affected endpoint and explains why it has been quarantined or removed from the network.

“I have utilized the AI assistant for AI-assisted investigation workflow in Rapid7 MDR, and while I think it is a new feature for them, I find it similar to functions in other products. What makes their AI different is that it allows me to design and implement solutions. If there is an issue with the platform, AI can help pinpoint the source of the problem, even if it is a configuration issue. I have not fully used it yet, but I intend to explore its functionality within Rapid7 MDR infrastructure.

“I have not actually used the multi-vector telemetry feature in Rapid7 MDR yet, although I have seen it.

“My experience with Rapid7 MDR's detection and response capabilities for

Microsoft-centric environments has been very smooth. I have not encountered any issues so far, and I believe that Rapid7 MDR and Microsoft have a good synchronization or handshake between their services, which contributes to this smooth operation.

“The inclusion of digital forensics and incident response within Rapid7 MDR service impacts my incident recovery process by providing a dashboard that offers insightful reports on incident responses. They have a vast database that is continuously updated, which they incorporate into Rapid7 MDR for threat detection and response capabilities.

“When it comes to pricing, Rapid7 MDR is known to have higher costs. However, the value is significant, and I believe that pricing should not be a problem if I recognize the worth of what I am paying for. Overall, I feel the value justifies the cost, though I see a need for a pricing reevaluation for some medium-class businesses.

“I have seen cost-effectiveness with Rapid7 MDR solutions, comparing it to other options such as ManageEngine and Sophos.

“My overall review rating for Rapid7 MDR is 8.5 out of 10..”

Emmanuel Dasho

Cyber Security Engineer | Network/Security at GCET

[Read full review](#) 

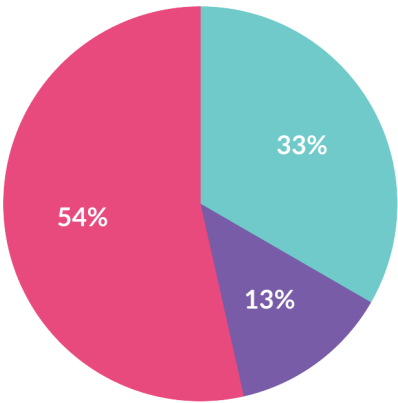
Top Industries

by visitors reading reviews

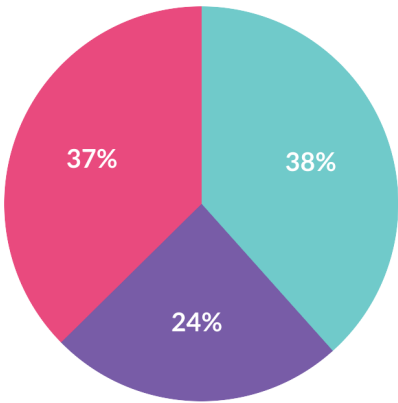


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944