aws marketplace

Rapid7 MDR

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 10

Other Solutions Considered 11

ROI 12

Use Case . . . . . 13 - 14

Setup . . . . . 15 - 16

Customer Service and Support 17

Other Advice . . . . . 18 - 19

Trends . . . . . 20 - 21

About PeerSpot . . . . . 22 - 23

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

- "The features of Rapid7 MDR that I find most effective for threat detection are the threat intelligence capabilities because it already collects many vulnerabilities and exploitations, as well as the configuration of network devices."

Hiroshi Watanabe

Marketing Expert at J's communication

- "The enrichment that Rapid7 MDR generates for the client is greater than with other tools, and this has had a big impact."

Verified user

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

"We've filled in crucial gaps we had with our previous solution. This was a key factor in choosing Rapid7 during the selection process. The ROI is already starting to show, too."

Oluwaseun Sonaike

Head, Networks and Security at First City Monument Bank Limited

"The product allows us to customize our alerts."

RussellBurrows

Senior IT Security Specialist at KNIPPERX INC.

What users had to say about valuable features:

"The integrations are a big plus. We can easily onboard log sources and transition from our previous MSSP without any hassle. We don't have any major issues and it has good ease of use for resource onboarding a breeze.."

Oluwaseun Sonaike

Head, Networks and Security at First City Monument Bank Limited

Read full review

“Rapid7's MDR service offers several strong points. Firstly, it excels in incident response. Rapid7 focuses not only on incident detection but also on response, aiming to minimize false positives effectively. This capability is crucial for reducing unnecessary alerts and ensuring that responses are targeted and efficient.

Additionally, Rapid7's MDR service extends beyond just incident response. It includes features for vulnerability assessment and vulnerability management, which are essential for proactive security measures. These features help in identifying and managing potential risks before they can be exploited..”

Nuki Agustino Wono
Senior Security Consultant at ITSEC Asia

Read full review

“It is a good solution. It's not a black box. Our security operations center has similar access to the console that we have access to. It's very open. The product has automation workflows. It has around 5000 detections in it. I trust the solution.

The product is continuously developing. Whenever something new comes out, the product is upgraded. We can also bring in community threat feeds. The product allows us to customize our alerts. Log query searching has come a long way. It doesn’t require us to code anymore. We can just type in what we are looking for.

We can also deploy our agents. The good thing about agents is that we can use the automation workflow to disable user accounts. We can also make it disable and quarantine an asset. These features are provided right out of the box. The workflows do not cost us more money..”

RussellBurrows
Senior IT Security Specialist at KNIPPERX INC.

Read full review

"Being able to list the vulnerabilities of the machines, being able to correlate alerts with the respective users who managed them, and having the artificial intelligence for creating query searches in the logs is crucial. The artificial intelligence for creating queries in the logs with Rapid7 MDR has been a great help because normally we use another platform called CrowdStrike, and the queries there are very different. This ultimately helps us create queries faster and more efficiently.

Rapid7 MDR has had a big impact when handling tickets by enriching them with information for the client. The client has been very pleased when handling tickets with Rapid7 MDR, unlike with other platforms, and this has had a positive impact.

It has helped with the ease and speed of detections and event correlations. Rapid7 MDR is very transparent. Investigations and detections are always identified normally, and they enrich the tickets.."

Verified user

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

Read full review

“The features of Rapid7 MDR that I find most effective for threat detection are the threat intelligence capabilities because it already collects many vulnerabilities and exploitations, as well as the configuration of network devices. They integrate everything into one solution. The other solutions such as CrowdStrike or SentinelOne don't collect all the vulnerabilities or threat intelligence except within their product itself, making Rapid7 MDR very strong in this aspect.

“I have seen an ROI from this solution in terms of time savings. Because it includes everything, including SIEM, EDR, and vulnerability control, other solutions require integration of every module and vendor. It is easier to implement once they start, as the modules of the EDR can be challenging to implement and may require consulting..”

Hiroshi Watanabe
Marketing Expert at J's communication

Read full review

"The best features in Rapid7 MDR are their team, which is made up of professionals. I interact with them whenever we face issues, even though we are running our own SOC, but we sometimes rely on Rapid7. It is having a human eye on everything. The MDR AI platform they recently transformed into is very helpful for defining use cases, real-time detections from a dashboard, and the reporting mechanism they have created within Rapid7 MDR.

Even the orchestrator platform they introduced for playbook creation is very helpful, as I create playbooks on Rapid7 using their predefined orchestrator platform.

Having a dedicated cybersecurity advisor through Rapid7 MDR significantly impacts aligning our security program with business needs because it approaches MDR better for big organizations such as mine. My first organization, Afiniti, was a significant AI-based company where I introduced Rapid7 MDR. The MDR is beneficial for both small and large organizations, unlike Splunk, which has more conditional formatting in their product.

Rapid7 MDR has positively impacted my organization by providing us with very effective management tools. 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. The management tool from Rapid7 allows us to access a variety of vulnerabilities in real time to fix them effectively. How we tackle that specific MDR is indicative of its market quality. We analyzed the tool during our POC before purchasing.

We deployed endpoints on a specific server and attacked that machine using different methods, such as Metasploit, conducting DDoS attempts, and generating alerts for every anomaly from Rapid7. While a competitor's solution failed to detect many attacks, Rapid7 identified them in real time, which effectively pushed my management towards choosing Rapid7 MDR. ."

Ehsan Khaleel
Manager SOC at PTCL

Read full review

Other Solutions Considered

"I decided to switch from those products because, while Qualys is a good vulnerability scanner, it is not very user-friendly. When scanning two machines, one with Rapid7 having an agent deployed for a level three scan and another with Qualys, the results were different. Rapid7 MDR indicated more vulnerabilities that were accurate upon verification, whereas Qualys missed many of them. This highlighted that IVM, Rapid7 MDR, and MDR stand out as top products in the market, especially for our financial sector.."

Ehsan Khaleel
Manager SOC at PTCL

Read full review

ROI

Real user quotes about their ROI:

"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 Sonaike
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

Use Case

"The typical use case for Rapid7 MDR is that it is highly valued. It is not so bad, but competition with EDR is tough. Rapid7 MDR does not position itself as EDR or XDR, so it is rather a SIEM type solution, which makes it different from CrowdStrike, SentinelOne, or Microsoft. They are not in the competition listing of EDR products.."

Hiroshi Watanabe
Marketing Expert at J's communication

Read full review

"Rapid7 MDR serves as our endpoint security solution. When we receive an alert from Rapid7 MDR, we check the logs of the endpoints that are managed on the client side, which provides us with richer information for the tickets. The enrichment that Rapid7 MDR generates for the client is greater than with other tools, and this has had a big impact.

Everything works very well with Rapid7 MDR. One day we had an incident related to an attack where Rapid7 MDR detected social engineering in a Teams chat, for which we received a notification by email. By correlating the events in Rapid7 MDR, we identified that it was a call from an unauthorized tenant within the organization.."

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

Read full review

“I can describe many use cases for Rapid7 MDR, as there are multiple times when a person's PC gets compromised. There is an attacker behavior analysis, ABA, which is already part of the specific Rapid7 MDR XDR solution. We define a specific set of built-in rules in the MDR services and remap those rules according to our infrastructure for specific use cases.

We also deal with multiple phishing emails that we receive, and Rapid7 MDR is effective in identifying those specific use cases. In the Fintech sector, we encounter many anomalies from different servers that are publicly exposed on the internet, and Rapid7 MDR provides very beneficial use cases that eliminate the need to write custom use cases. We can define the logic in predefined use cases such as Attacker Behavior Analysis and User Behavior Analytics.

Additionally, when onboarding any log sources, there is a RegEx parser designed for parsing every log source on the built-in platform, making it quite user-friendly. .”

Ehsan Khaleel
Manager SOC at PTCL

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.

"I rate the ease of setup a seven out of ten. It is not bad. It takes a little bit more time. It will probably take three weeks to get the product up and running, especially by the time we deploy all the agents.."

RussellBurrows

Senior IT Security Specialist at KNIPPERX INC.

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

"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

"The support is quite responsive. We often jump on calls for onboarding assets and custom configurations like log forwarding. We haven't needed much beyond that.."

Oluwaseun Sonaike
Head, Networks and Security at First City Monument Bank Limited

Read full review

"The technical support from Rapid7 MDR is adequate, rating approximately six out of ten. The lower tier support is not very good. Additionally, Japanese customers require Japanese representatives as the support is primarily in English.."

Hiroshi Watanabe
Marketing Expert at J's communication

Read full review

"Evaluating the customer service and technical support teams of Rapid7 MDR, I would rate them a six out of ten. I have previous experience with IBM support, which was excellent and proactive. In contrast, Rapid7 MDR support often takes longer to respond to issues. Despite their large customer base, this highlights a need for enhancement in their support team.."

Ehsan Khaleel
Manager SOC at PTCL

Read full review

Other Advice

“Rapid7 works well for us and meets our current needs. It's a solid eight out of ten. However, it depends on your organization's cybersecurity roadmap.

For example, if your long-term plan is to have an on-premise security team, then Rapid7 might not be the best fit.

We don't have on-premise capabilities and rely solely on the cloud, so it works for us. But other organizations might need that on-premise option. So, it really depends on their cybersecurity roadmap..”

Oluwaseun Sonaike
Head, Networks and Security at First City Monument Bank Limited

Read full review

“I have knowledge of CrowdStrike solutions as a competitor, though not direct experience.

“I would recommend Rapid7 MDR to others, but this market is changing quickly due to artificial intelligence. I cannot say it is the best solution for customers as the market is evolving, with new solutions emerging and existing vendors improving their offerings in the near future.

“Overall, I would rate Rapid7 MDR a seven out of ten. Once customers can implement it, it becomes a good solution for them, though implementation remains a significant consideration..”

Hiroshi Watanabe
Marketing Expert at J's communication

Read full review

"I am taking advantage of the expanded ecosystem telemetry support in Rapid7 MDR. We have enhanced the logging mechanism within Rapid7 MDR, allowing us to assign projects to different teams with visibility only of their specific assets. This approach supports various vulnerability assessments and compliance achievements. My management is overall pleased as we have managed to meet compliance standards such as ISO 27001 and NIST due to features provided by Rapid7 MDR.

I utilize AI-assisted Risk-Aware Investigation workflows, integrating both our on-prem and cloud infrastructure. By using APIs in our environment, we gain enhanced visibility, giving us detailed insights that greatly assist in real-time monitoring.

This approach impacts my alert triage and prioritization processes since Active Directory is a crucial element in our industry. Rapid7 MDR improves the alerting mechanism for Active Directories and all connected user activities. Previously used SIEM solutions did not adequately capture anomalies on ADs. With Rapid7 MDR, any anomaly triggers escalated alerts in real time.

I am using the Integrated MDR for Microsoft Environments feature, having integrated Microsoft 365 with our MDR and endpoints from Microsoft Active Directory and Azure. This integration provides us with comprehensive visibility into our infrastructure.

Regarding transparency in detection and investigations with Rapid7 MDR, we receive metrics such as MTTR and MTTD (Mean Time to Detect and Mean Time to Respond). We monitor how quickly the tool detects anomalies and how long it takes to respond, which shows improvement due to the specific MDR product. My overall review rating for Rapid7 MDR is 8.5 out of 10. ."

Ehsan Khaleel
Manager SOC at PTCL

Read full review

Top Industries

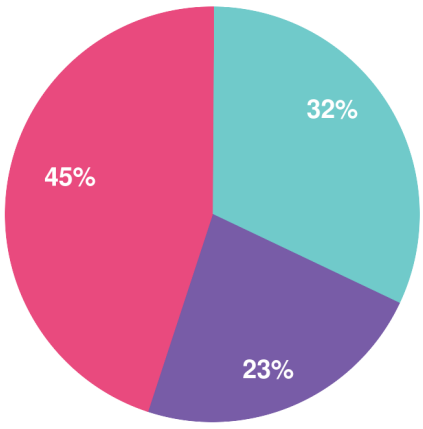
by visitors reading reviews

Educational Organization	10%
Manufacturing Company	8%
Financial Services Firm	8%
Outsourcing Company	7%

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