aws marketplace

Rapid7 InsightIDR

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Rapid7 InsightIDR

Rapid7 InsightIDR Recap

Parsing hundreds of trivial alerts. Managing a mountain of data. Manually forwarding info from your endpoints. Forget that. InsightIDR instantly arms you with the insight you need to make better decisions across the incident detection and response lifecycle, faster.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Rapid7 InsightIDR is budget-friendly and has a good market position because not everybody can afford to go for LogRhythm or Splunk or QRadar."

SohailHyder
Head Of Cyber Security at Super Secure

- "The platform offers unlimited storage and agent-based solutions."

Asim Naeem
Principal IT Security & Compliance at IBEX Holdings Ltd

- "The solution provides satisfying native integration features"

Verified user
Director of Solutions and Alliances at a tech services company with 1-10 employees

- "Scalability-wise, I rate the solution a ten out of ten. As a cloud tool, the product is highly scalable."

Prasanth Prasad
Chief Technology Officer at a tech vendor with 51-200 employees

"I have seen that Rapid7 InsightIDR provides security to the networks and endpoints in the company."

Agustinus DWIJOKO

Network & Security Engineer at PT. Centrin Online Prima

"I like that it's a cloud-based solution."

Khizar Butt

Country Sales Lead at securic systems

"I like the tool's user analysis feature."

Gerard Konan

Founder & CEO at AGILLY

What users had to say about valuable features:

"The most valuable feature of the solution is the single pane of glass that allows me to see all the information in one spot. I can see at one spot to see all the information from all the logs and everything.."

JensWolf
Systems Administrator at Gernandt & Danielsson Advokatbyrå KB

Read full review

"The platform offers unlimited storage and agent-based solutions. I have user behavior analytics (UBA) and MITRE ATT&CK as well. The user behavior analytics feature helps in enhancing the security posture by helping to identify user behaviors and engineering alerts based on them.."

Asim Naeem
Principal IT Security & Compliance at IBEX Holdings Ltd

Read full review

"It's a great tool. The solution helps us a lot in threat detection. It's one of the most updated tools. The UI is very good. We can easily start using the tool and explore it. It also provides features like legacy UBA that other products do not provide. We can customize the rules from the default template in InsightIDR. UBA is a great feature.

When a new user is created in Active Directory, an investigation is created. We can use the default features to create an investigation. The solution has many advanced features and default templates that help protect from attacks without a user's intervention. It is quite impressive.."

Awais Sajid
Security Engineer at Secure Networks

Read full review

"UEBA is an important element these days, but usually the requirement is for threat detection, investigation, and response. This is what Rapid7 InsightIDR provides.

"Banks typically go for threat detection, investigation, and response capabilities. End-user entity and behavior analysis, or UEBA, is certainly an important addition if we provide the solution along with UEBA. It provides that and this is something that the customer cannot ignore because they want to have a 360-degree coverage of their emails or for their users and what they are doing. This is definitely their requirement.."

SohailHyder
Head Of Cyber Security at Super Secure

Read full review

“The most valuable feature of the product for managing security events stems from the fact that the product's intelligence part is very good since it offers its own threat intelligence and vulnerability management platform. The tool also has its own cloud security posture management platform. The tool also is a dynamic application security testing platform. The aforementioned tools fall under Rapid7 InsightIDR's kitty. The intelligence and the data that Rapid7 gathers from customers across the globe enrich the quality of its detection capabilities. All other tools in the market depend on third-party solutions for intelligence. Rapid7 InsightIDr has the intelligence part natively available within the product, giving it a good edge over other vendors.

.”

Prasanth Prasad
Chief Technology Officer at a tech vendor with 51-200 employees

Read full review

"During simulations or demonstrations, the tool generates alerts, providing details such as the specific application, its origin, and potential threats. For instance, it can identify if an application belongs to a known ransomware group. The system rates the threat, offering a clear detection ratio, such as 97 out of 100. It not only identifies threats but also illustrates the associated behaviors, helping us understand the potential risk to a particular endpoint.

It provides user entity behavior analysis and a threat intelligence framework, combining SIEM and EDR for automation. My experience with user behavior analytics is positive and wonderful. It allows fetching logs, managing users, and overseeing endpoints. The capability to conduct investigations and import applications, along with configuring endpoints by collecting data, adds to its functionality. The platform offers a variety of features, including a dashboard for new alerts. This dashboard provides a quick overview of the number of users, endpoints, and noticeable behaviors. ."

Vikas Dusa
Cyber Security Trainer and Programmer at Freelancer

Read full review

Other Solutions Considered

"I have used IBM QRadar, Splunk, and Sentinel. We use Splunk in our offices, too. Compared to other products, Rapid7 InsightIDR's UI is very good. It is very easy to handle. We are working with the tool currently and are quite satisfied with it.."

Awais Sajid
Security Engineer at Secure Networks

Read full review

"We had a list of three products. We tried them all, and in the end, we went for Rapid7 because it was easy to deploy, and it required little or no maintenance. The price was another reason.."

Verified user
Security Solution Engineer II at a security firm with 501-1,000 employees

Read full review

"In the past, my company used Unomaly, a tool from Sweden. My company switched from Unomaly to Rapid7 InsightIDR after seeing that the former could only checked syslogs, while we wanted something that checked our overall systems.."

JensWolf
Systems Administrator at Gernandt & Danielsson Advokatbyrå KB

Read full review

"Currently, I am not working with the LogRhythm solution. I have another SIEM solution in place. Previously, three years back, I was working with LogRhythm, however, now I do not.."

Asim Naeem
Principal IT Security & Compliance at IBEX Holdings Ltd

Read full review

"Enterprise-level customers have better options, such as LogRhythm, QRadar, and Splunk. These products are core SIEM-based companies that are old players in this market. Rapid7 is a relatively new entrant in the SIEM market. However, it has strong capabilities, and customers trust big names, big companies they've known from the beginning, who have been working on SIEM solutions since inception.."

Khizar Butt
Country Sales Lead at securic systems

Read full review

"We used to use QRadar in my previous company. The first difference is in the deployment architecture. QRadar comes with cloud and on-prem options. In countries like Pakistan, where I am from, there are very strict regulations for using cloud solutions, especially in the banking sector. Rapid7 only offers a SaaS-based SIEM.

The second difference between the two is in their licensing. Rapid7 InsightIDR license is applied based on the number of nodes and devices. QRadar, on the other hand, does licenses the events per second.

The third difference is in the threat intelligence QRadar provides, and there's a huge difference between the two in this domain. QRadar is an IBM product that is very old in the SIEM market and provides relatively better threat intelligence than players like Rapid7.."

Khizar Butt
Country Sales Lead at securic systems

Read full review

ROI

Real user quotes about their ROI:

"The incident response time is good, and I can easily find or search any incident. I easily build the queries in Rapid7 and search my relevant logs or relevant investigation logs.."

Asim Naeem
Principal IT Security & Compliance at IBEX Holdings Ltd

Read full review

Use Case

"The main use case for InsightIDR is to investigate threat activity that can compromise the internal customer environment. We can track a threat from the first attempt or breach. Then we can investigate the threat from start to finish. ."

KimeangSuon
Pre-Sale Consultant at Yip In Tsoi Co., LTD.

Read full review

"I am using Rapid7 InsightIDR as an InsightIDR solution. This tool is integrated with other solutions like endpoint and NDR, and it correlates alerts, giving me a comprehensive picture of the alerts.."

Asim Naeem
Principal IT Security & Compliance at IBEX Holdings Ltd

Read full review

"Our company is a system integrator for Rapid7 InsightIDR. We use the latest SaaS version of the product. Rapid7 InsightIDR works as the foundation of the security operation center in our company. The solution is used in our organization for data ingesting for multiple security devices and solutions. Rapid7 InsightIDR provides insights and stability on the security aspects of the company. ."

Verified user

Director of Solutions and Alliances at a tech services company with 1-10 employees

Read full review

"I used it in my previous company. We were the integrator of the solution, and also a partner of Rapid7 at the time.

We used it for security monitoring and also for analytics. We used it for our own company, and like an MSSP, we sold this to our customers. So, we did security monitoring for our customers and interim response for them.

It was cloud-based, and I was using its latest version.."

Verified user

Security Solution Engineer II at a security firm with 501-1,000 employees

Read full review

"We use the tool for deployment, incorporating both EDR and SIP management. It serves the purpose of event management, including log retrieval from endpoints, malware detection, and providing about system health. This includes assessing vulnerabilities and determining the level of risk the system is exposed to at specific points in time. Its dashboard is wonderful.

We use Rapid InsightIDR for security operations, threat response, and DFIR. It also provides lab practices to individuals. ."

Vikas Dusa
Cyber Security Trainer and Programmer at Freelancer

Read full review

"I am working with Rapid7 InsightOps and Rapid7 InsightIDR because the requirement is as such from the customer side, particularly the banks. Whatever the requirement is, these are the products that we are working with.

"I usually recommend Rapid7 InsightIDR for banks because that is the bigger chunk here who do business in cybersecurity or whose requirement is that compliance requirements need to be filled by certain products, which Rapid7 InsightIDR is one of them.."

SohailHyder
Head Of Cyber Security at Super Secure

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.

“Due to the product's complexity, the initial setup can be challenging. Additionally, setting up the product and training the customer can be quite demanding. Deploying the appliance or sensor on-premises can take up to twelve months..”

Hiroshi Watanabe

Marketing Expert at J's communication

Read full review

“The initial setup is easy. It involves tasks such as data collection, onboarding, and downloading, making the process straightforward for clients. You can deploy it on mobile devices as well. It offers deployment options for iPhone users and Windows. .”

Vikas Dusa

Cyber Security Trainer and Programmer at Freelancer

Read full review

“The initial setup is easy. The deployment took only half an hour. It's just a cloud platform. You just have to deploy a connector like Select Pro, and it will set the data from the on-premise. It will send it to the cloud platform, and you can have it installed in five to ten minutes..”

Verified user

Read full review

Network Support Engineer at a tech services company with 51-200 employees

“The time required to complete the product's installation phase depends on the number of endpoints that a user has in their environment. Insight Agent can be deployed in a couple of minutes.

Five engineers in my company take care of the deployment phase of Rapid7 InsightIDR.

The solution is deployed on the public cloud services offered by AWS..”

Agustinus DWIJOKO

Read full review

Network & Security Engineer at PT. Centrin Online Prima

“I rate the initial setup a ten out of ten.

The solution's initial setup was very straightforward.

The solution is deployed on an on-premises and cloud model. The cloud services are provided by Rapid7.

The solution can be deployed in half a day or four hours in a small environment.

I was the only person involved in the product's deployment phase..”

JensWolf

Systems Administrator at Gernandt & Danielsson Advokatbyrå KB

Read full review

“I would rate the initial setup a nine out of ten. It's quite straightforward to put the solution to work. Once Rapid7 InsightIDR activates the tenant, the deployment process becomes straightforward. In our company, we just download the agents and install them in the customers' virtual machines. Following the aforementioned step, some integration with Azure Entra ID authentication services or on-prem authentication is required. Thus, some base integration is required for login data. For the final stage of deployment, as part of the company, we configure a couple of customizations for the detection rules to start ingesting data; the niche customizations can be performed easily for the use cases. In our company we have an engineering deployment team who are highly skilled in setup processes. For client companies with less than 500 devices, usually one full-time engineer is enough for the deployment. For clients with 500 devices, when we at our company use automation to deploy the agents, it takes only a couple of days to finish the deployment process. .”

Verified user

Director of Solutions and Alliances at a tech services company with 1-10 employees

Read full review

Customer Service and Support

"Rapid7's customer support is awful. They didn't respond at all. Tenable's support is always available. I didn't have to visit the customer every time they wanted to perform a scan.."

SamiAyyash

Threat Intelligence Engineer at a tech services company with 11-50 employees

Read full review

"Our company mostly receives fast and suitable support from Rapid7 InsightIDR, but sometimes the response arrives quite slow. I would rate the technical support a seven out of ten. ."

Verified user

Director of Solutions and Alliances at a tech services company with 1-10 employees

Read full review

"Rapid7 InsightIDR's technical support is reactive and supportive. However, they only speak English. Our native language is French and it would be better if they can have some French speaking agents. ."

Gerard Konan

Founder & CEO at AGILLY

Read full review

"The technical support could be improved. We've had times when our requests get stuck with the engineering team and we sometimes don't get a response. That's a problem for us. ."

Verified user
Security Consultant at a comms service provider with 51-200 employees

Read full review

"I have contacted Rapid7 support but not for InsightIDR. It is with for another product of theirs. I think their support is good. The support team helped us run diagnostic tests and walked us through everything until the case was resolved.."

KimeangSuon
Pre-Sale Consultant at Yip In Tsoi Co., LTD.

Read full review

"The speed of response from the technical support team may vary since I purchased it from a reseller in Sweden and not from Rapid7 directly.

I rate the technical support a seven out of ten.."

JensWolf
Systems Administrator at Gernandt & Danielsson Advokatbyrå KB

Read full review

Other Advice

“I definitely recommend Rapid7 InsightIDR. It is becoming better, with improvements being continuously made to the product.

Right now, I do not have any advice about Rapid7 for other users because every organization or user has different criteria or multiple use cases, so I refrain from commenting on that. I rate the overall solution seven out of ten..”

Asim Naeem
Principal IT Security & Compliance at IBEX Holdings Ltd

Read full review

“At our company, along with Rapid7 InsightIDR we use multiple cloud providers like Azure, Google, Oracle and AWS infrastructure to ingest data.

I would advise others to select a reliable system integrator to implement Rapid7 InsightIDR for the correct use cases or business needs. The solution is satisfying, but there are multiple other solutions in the market, and having a partner can help a customer explore all the options before adopting one. Overall, I would rate Rapid7 InsightIDR an eight out of ten. .”

Verified user
Director of Solutions and Alliances at a tech services company with 1-10 employees

Read full review

“InsightIDR automates everything through InsightConnect in a seven-day cycle.

The product has improved significantly since its inception. However, based on feedback I've received from other products in the market, aside from InsightIDR.

It improved because several sensors are deployed within the on-premise environment. It can be very efficient if the customer implements and operates it effectively.

If you combine it with InsightIDR, then it may become more compact. Maybe IBM was a bit larger. So, having MDR is the main key point for this product.

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

Hiroshi Watanabe
Marketing Expert at J's communication

Read full review

“In one instance, we faced a threat from the DarkSide ransomware, known for its ability to execute without requiring administration privileges, including a privilege escalation part. This particular ransomware was embedded in an Excel file, and it didn't need any administrative privileges for execution. The hackers cleverly concealed the DarkSide ransomware within an Excel file. When an unsuspecting team member tried to open the file, an alert indicated the malicious nature of the Excel file.

The employee was unaware that the Excel file contained a ransomware threat. As security personnel monitoring the endpoint received an alert, they immediately contacted the individual, notifying them about the presence of the DarkSide ransomware. The security team advised against opening the file and guiding the user to delete it.

I cannot compare Rapid7 InsightIDR with other tools directly because it has integrated both EDR and SIM. It combines these functionalities into an XDR platform, operating at a different level compared to other services. Additionally, the network analysis provided is wonderful.

The product is easy to use and easy to understand. It is lightweight. I rate it a nine out of ten.

I recommend it for easy deployment, enabling swift detection from endpoints to the cloud. This accelerates security orchestration across various environments and endpoints, aiding in risk mitigation within hybrid environments. The system is valuable for discovering new threats and offers exposure management to enhance understanding of the entire security operation..”

Vikas Dusa
Cyber Security Trainer and Programmer at Freelancer

Read full review

"The tool has improved the efficiency of security incident detection and response in our company as it works fairly well. It is possible to enhance the capabilities of the platform since the solution offers a whole stack or suite of tools. When dealing with Rapid7 InsightIDR, you will see the integration capabilities offered are extremely seamless. Rapid7 InsightIDR offers its own set of features that enrich the capabilities of the vulnerability management tool. In general, the product's features increase the solution's overall capabilities in terms of reporting and detection of vulnerabilities.

I can't remember a scenario where the product was effective in threat hunting or investigation. Rapid7 InsightIDR is a very acceptable product for people who want a cloud-based solution. The product is not available on an on-premises version. The product can be useful for industries ranging from SMBs to large-sized companies where there is a need for a tool that can be very easily rolled out at a very effective and attractive price point that gives them very good coverage from a cybersecurity perspective.

Speaking about how the product has enhanced the security posture in our company, I would say that I am not really sure about the capabilities of the UABA part of the solution since I haven't seen many use cases around it.

Rapid7 InsightIDR mean time-to-detect and mean time-to-respond are fairly good because Rapid7's support team does pick up a ticket whenever it is raised from the users' end, but its mean time-to-resolve has some concerns since some of the tools under Rapid7 are available on an on-premises model. In specific to InsightIDR, I think that everything is very good, including areas like detection, MTTD, and MTTR, which are very good in InsightIDR specifically. The product can improve a bit in the area of MTTD and MTTR.

Rapid7 InsightIDR's integration capabilities with other tools are not an area I have experience with since the product is completely available on the cloud. I believe that whatever integrations users want from the product would work since it is a solution that is available on the cloud. I don't have personal experience with the integration part.

I rate the overall tool a seven out of ten.."

Prasanth Prasad
Chief Technology Officer at a tech vendor with 51-200 employees

"Rapid7 InsightIDR is budget-friendly and has a good market position because not everybody can afford to go for LogRhythm or Splunk or QRadar. It is good for a middle-tier organization. In that market, there is competition now.

"I do not recommend Rapid7 InsightIDR for bigger companies because they trust these big brands such as QRadar or LogRhythm. The general perception is that these are the solutions for big organizations having hundreds of branches or more. Rapid7 InsightIDR fits in the middle tier.

"The integration of Rapid7 InsightIDR with the security stack works fine because the systems in this part of the world are not so much cloud-driven. They have something around 20% or 30% of services running from the cloud. The rest are usually on-premises. Office 365 is one service that they get from the cloud. Networking typically includes Cisco and Fortinet in their networks. For endpoints, the operating system is usually Windows or Linux, not Mac in an enterprise environment. Windows and Linux can be easily integrated with this solution.

"The dashboard functionalities of Rapid7 InsightIDR are usually about customer-friendliness. Customers want to have some rich enrichment of the analysis or the ticket alerts or the events that come out with some processing behind the scenes. They feel that it is a more rapid or more intense process at Splunk or LogRhythm or QRadar compared to Rapid7 InsightIDR.

"For automated threat intelligence features, customers usually go for a full SOAR solution. They want to have playbooks and everything to run. Although Rapid7 InsightIDR does claim that it has integrated SOAR, called InsightConnect, this is not as advanced as a dedicated SOAR solution. LogRhythm solutions or Splunk solution or Sumo Logic solution are doing business here as well. These are considered more rich in features compared to Rapid7 InsightIDR.

"I rate Rapid7 InsightIDR between a six and seven out of ten.."

SohailHyder
Head Of Cyber Security at Super Secure

Read full review

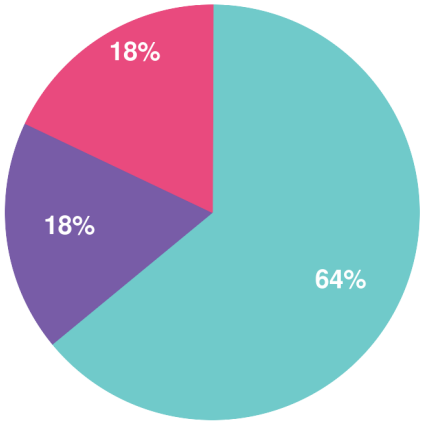
Top Industries

by visitors reading reviews

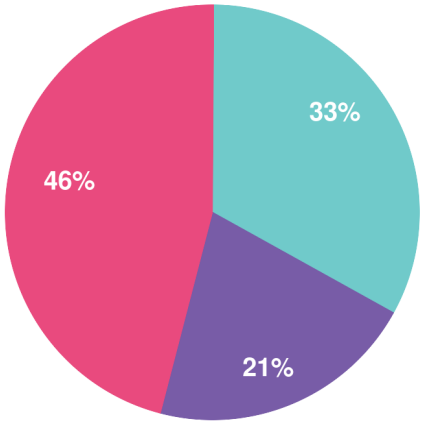
Financial Services Firm	9%
Computer Software Company	9%
Manufacturing Company	9%
Government	7%

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