aws marketplace

Rapid7 InsightIDR

Reviews, tips, and advice from real users

Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 10

Other Solutions Considered . . . . . 11 - 12

ROI 13

Use Case . . . . . 14 - 17

Setup . . . . . 18 - 21

Customer Service and Support . . . . . 22 - 23

Other Advice . . . . . 24 - 28

Trends . . . . . 29 - 30

About PeerSpot . . . . . 31 - 32

©2026 PeerSpot, All Rights Reserved

Product Recap

Rapid7 InsightIDR

Rapid7 InsightIDR Recap

Rapid7 InsightIDR is a cloud-based security information and event management solution known for its user behavior analytics, offering rapid detection and response capabilities while facilitating seamless integration across systems.

Rapid7 InsightIDR is designed to enhance threat detection and investigation through its efficient user behavior analytics and advanced threat intelligence framework. The platform's cloud-based deployment ensures rapid setup and comprehensive event monitoring across diverse IT environments, including endpoints and Office 365. Its intuitive interface supports seamless data collection, honing in on threat detection through honeypot utilization and intelligent alerting. However, it is noted for lacking some customization features and better integration, especially with Microsoft and ITSMs.

What are the key features of Rapid7 InsightIDR?

- User Behavior Analytics: Detects threats by analyzing patterns and anomalies.
- Cloud Deployment: Enables quick setup and scalability.
- Comprehensive Monitoring: Monitors events across systems and platforms like Office 365.
- Honeypots and Alerting: Utilizes honeypots to reduce false positives and alert fatigue.
- Threat Intelligence Framework: Supports effective threat hunting and remediation.

What benefits should users consider in reviews when evaluating Rapid7 InsightIDR?

- Enhanced Detection: Improves threat detection with user behavior analysis.
- Easy Integration: Integrates across systems for a streamlined security approach.
- Rapid Response: Facilitates quick action against identified threats.
- Operational Efficiency: Offers a cohesive view of security operations.

Rapid7 InsightIDR is prominently used in security operation centers to manage events, detect threats, and respond effectively. Industries apply it for network behavior monitoring, compliance, and vulnerability management. Companies integrate it with security tools to boost threat investigation, ensuring full SIEM functionalities and robust log management capacities. Its application spans behavioral and intrusion analytics, aiding in monitoring and addressing malicious activities.

©2026 PeerSpot, All Rights Reserved

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Rapid7 InsightIDR has positively impacted my organization by capturing most logs and every minute detail, including endpoint logs, network logs, and any email-related logs if a malicious link has been clicked."

Prajwal Chougale

SOC L2 Analyst at a tech services company 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."

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

©2026 PeerSpot, All Rights Reserved

"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

"The solution provides satisfying native integration features"

Validated user

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

"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."

Vikas Dusa

Cyber Security Trainer and Programmer at Freelancer

©2026 PeerSpot, All Rights Reserved

What users had to say about valuable features:

"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

©2026 PeerSpot, All Rights Reserved

"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

©2026 PeerSpot, All Rights Reserved

"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

©2026 PeerSpot, All Rights Reserved

"The best features that Rapid7 InsightIDR offers include its log display, which is easy to understand for any SOC analyst. In hunting, if there is any red team activity or a true positive incident and an analyst wants to hunt or review logs, Rapid7 has simple logic and features such as legacy log search and normal log search using KQL, Kusto Query Language, which allows for fetching and analyzing logs in detail. The way everything is arranged and easy to understand, along with insights into network sensors or devices configured with Rapid7, helps us understand where logs are being ingested and where traffic is moving.

"Out of all the features, log search is what I find myself using the most. Compared to Microsoft Sentinel, Rapid7 InsightIDR's SIEM tool makes log search very easy. The log display is simple, and the investigation part is very intuitive using Rapid7. Logs are segregated into different categories, such as ingress logs, web traffic logs, Active Directory logs, and cloud security logs, making it seamless to present everything on their dashboard, which has been immensely helpful for my investigative work.

"Rapid7 InsightIDR has positively impacted my organization by capturing most logs and every minute detail, including endpoint logs, network logs, and any email-related logs if a malicious link has been clicked. All logs are integrated and ingested into Rapid7 InsightIDR, which is useful for hunting or checking for any true positive incidents that trigger. A notable feature is that if an investigation opens on a single entity and any alerts are observed around that time, they are tagged under a single incident with all activity logged under one template or interface. This allows an analyst to make quick and easy decisions and analyze all investigation artifacts. Recently, when one of our users clicked a malicious URL that Microsoft Defender could not track immediately, Rapid7 notified us that a malicious email was found, helping us take action before Microsoft could respond.

"Rapid7 InsightIDR provides very crisp, detailed, and on-point alerts whenever there is suspicious activity, which has led to very few false positives for the clients using Rapid7 InsightIDR. It has saved us a lot of time by reducing noisy alerts, and the dashboard is effortlessly managed and neatly organized, allowing us to create allow lists or block lists for any kind of activity.."

Prajwal Chougale

Read full review

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

©2026 PeerSpot, All Rights Reserved

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.."

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

Read full review

"For this client, we have exclusively used Rapid7 InsightIDR since the beginning as there were no other solutions in place. However, I can say that we used Microsoft Sentinel for other clients, and in comparison, Rapid7 InsightIDR has proven to be a more efficient and time-saving tool.."

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

Read full review

©2026 PeerSpot, All Rights Reserved

"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 a consultancy with 51-200 employees

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

©2026 PeerSpot, All Rights Reserved

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

"I have seen a return on investment; all employees, particularly the SOC analysts, are satisfied as they easily got trained and adapted to this tool. The logs are delivered in a crisp and direct manner, simplifying analysis of the alerts significantly.."

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

Read full review

©2026 PeerSpot, All Rights Reserved

Use Case

"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. ."

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

Read full review

©2026 PeerSpot, All Rights Reserved

"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.."

Validated 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

©2026 PeerSpot, All Rights Reserved

"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

©2026 PeerSpot, All Rights Reserved

"Rapid7 InsightIDR serves as our SIEM solution where all kinds of activity, including network logs, endpoint logs, user activity, user behavior analytics, and threat hunting, are tracked. Additionally, we use it to store logs and provide them for SOC analysts, and we utilize it completely as a SIEM tool. We also have used some of their other solutions, including Rapid7 Insight Vulnerability Management and Rapid7 Threat Command.

"In our day-to-day operations, Rapid7 InsightIDR is useful for tracking everything happening at the cloud level, at Entra ID, or on-premises. All logs, including network logs and traffic between domains or inside the domain or between on-premises servers and endpoints, are collected in one place. Using various analytical rules, we get alerts, and we configure the alerts required for our organizational needs. There are many more use cases for this solution.

"When it comes to threat hunting, we analyze dark web activity and track various activities related to users. We provide all user data to the agent, which searches the dark web for alerts based on our multiple domains. We actively monitor for any leaks detected with users or any spoofed domains and set up Rapid7 InsightIDR alerts to track these activities closely.."

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

Read full review

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved

"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

Network & Security Engineer at PT. Centrin Online Prima

Read full review

"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 a consultancy with 51-200 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The learning curve for new users of Rapid7 InsightIDR is very easy. Throughout my 2.5 years of experience, I have successfully onboarded three batches of users, totaling more than 10 users, and they adapted easily to this tool. The only challenging part was the log search, but once users got into it, it became very easy to use. Compared to the KQL of Microsoft Sentinel, Rapid7 InsightIDR has been much easier for users to learn.

"My experience with pricing, setup costs, and licensing has been very positive; it is cost-effective and offers great value for the money. We bought the licensing through an agent, and the setup was straightforward thanks to the assistance from their team.."

Prajwal Chougale

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

Read full review

©2026 PeerSpot, All Rights Reserved

"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. ."

Validated user

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

Read full review

©2026 PeerSpot, All Rights Reserved

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. ."

Validated 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

©2026 PeerSpot, All Rights Reserved

"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. ."

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

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 a consultancy with 51-200 employees

Read full review

"The customer support at Rapid7 is really good. Over my 2.5 years of experience, I have submitted many support cases related to InsightIDR alerts, analytical rules, and even Insight Vulnerability Management, and they have been consistently supportive. I would rate the customer support a perfect 10 out of 10.."

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

Read full review

©2026 PeerSpot, All Rights Reserved

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. ."

Validated 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.

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved

"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

©2026 PeerSpot, All Rights Reserved

"I have completed my insights about my main use case and how we use Rapid7 InsightIDR day-to-day. All the improvements and features I have discussed are sufficient.

"I am very satisfied with the speed and performance of Rapid7 InsightIDR when handling large volumes of data, giving it a rating of 9.5 out of 10. It can handle any volume of data for any organization, making it very cost-effective, which distinguishes it as a standout SIEM tool in the market. It is straightforward, time-efficient, and easy to use.

"My advice for others considering using Rapid7 InsightIDR is to go for it if you are looking for a value-for-money and straightforward tool that suits any kind of analyst.

"Rapid7 InsightIDR is deployed in my organization through AWS public cloud. The deployment model we use most is public cloud through AWS. We use Amazon Web Services, AWS, as our cloud provider.

"Rapid7 InsightIDR integrates with other security tools or platforms in our environment, including CrowdStrike, Netskope, and email security through Defender.

"I chose eight out of ten because of the analytical rules; they lack dynamic rules, and also due to the dashboard and reporting part.

"Rapid7 InsightIDR's AI capabilities are very helpful; the simulations or the SIEM injections they provide are useful for gaining alerts or insights about the organization, and it is very secure with no downtimes that affect client security. We have weekly meetings with support to discuss licenses or any new features added, which is really helpful in getting along with the tool.

"Most of the AI capabilities are still in progress, with various features being introduced. In Rapid7 InsightIDR, it is not heavily related to AI capabilities because the focus is primarily on the SIEM aspects, including logs from your environment and the size of your setup. My overall review rating for Rapid7 InsightIDR is 8 out of 10.."

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

Read full review

©2026 PeerSpot, All Rights Reserved

"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

©2026 PeerSpot, All Rights Reserved

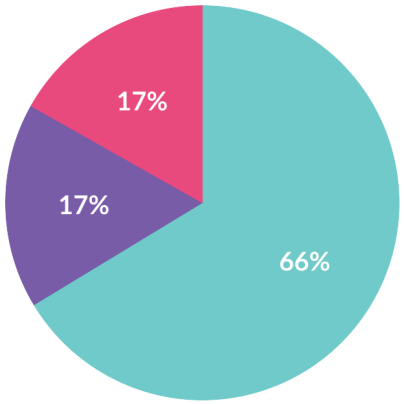
Top Industries

by visitors reading reviews

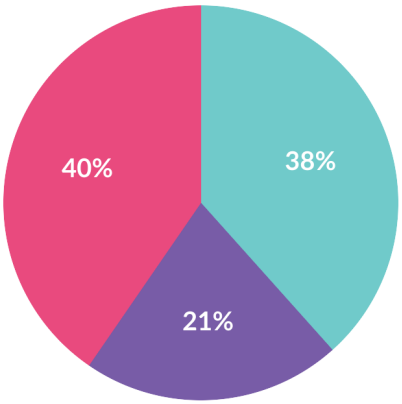
Financial Services Firm	10%
Manufacturing Company	10%
Comms Service Provider	8%
Outsourcing Company	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved