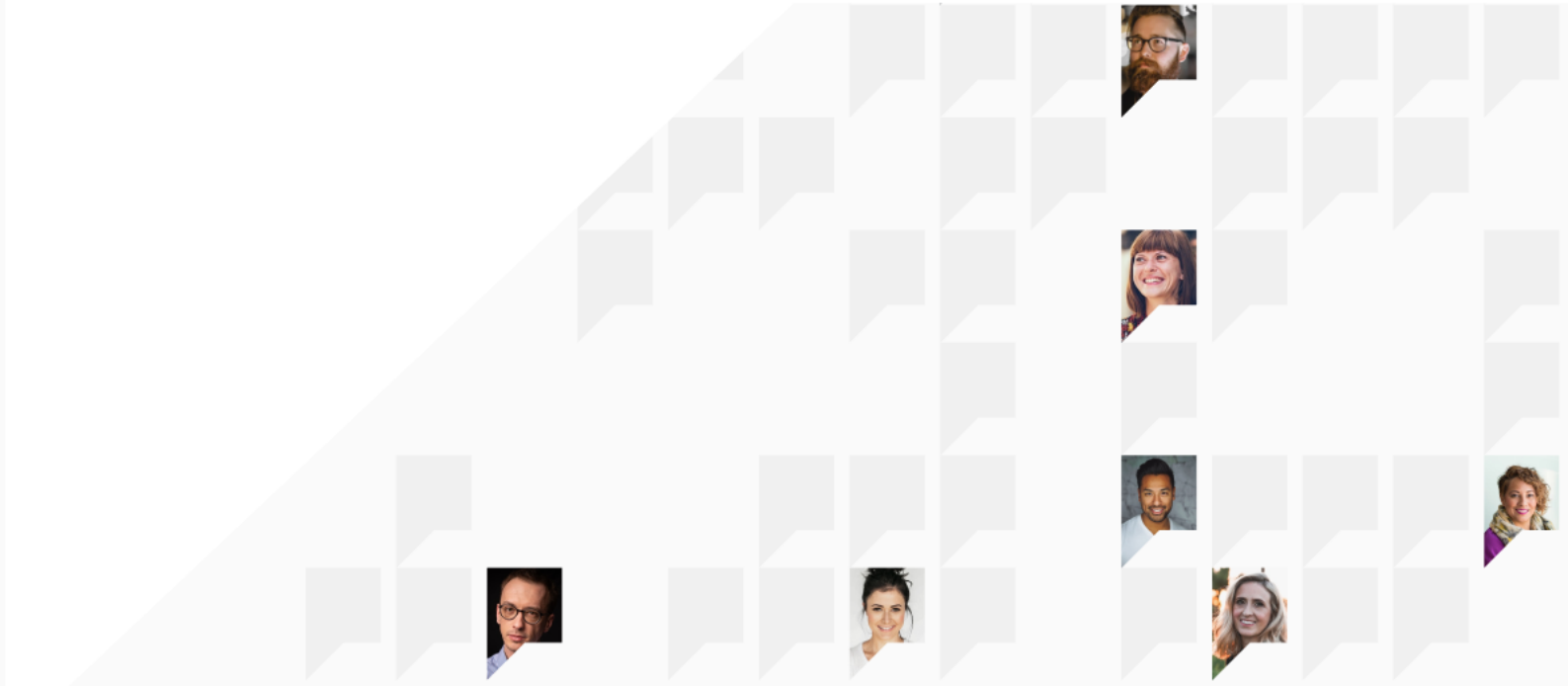
PeerSpot

AI Observability

Reviews, Tips and Advice from Real Users

August 2026



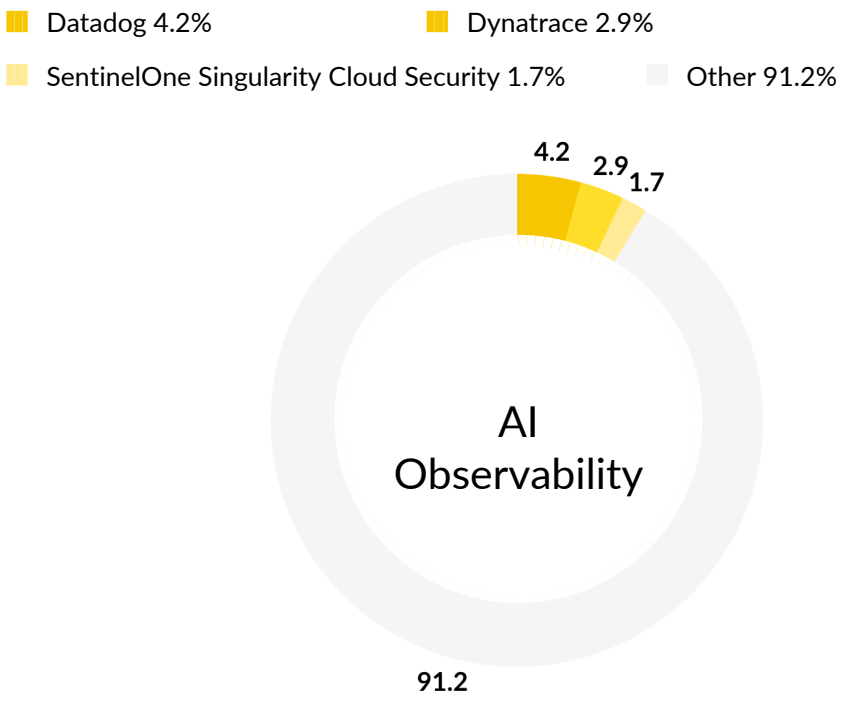
Contents

AI Observability Recap

AI Observability recap

Mindshare And Ranking

As of **August 2026**, in the AI Observability category, the mindshare of **Datadog** is **4.2%** and it decreased by 36.2% compared to the previous year. The mindshare of **Dynatrace** is **2.9%** and it decreased by 25.7% compared to the previous year.The mindshare of **SentinelOne Singularity Cloud Security** is **1.7%** and it increased by 1.4% compared to the previous year. It is calculated based on PeerSpot user engagement data.



Top Solutions

Datadog

SentinelOne Singularity Endpoint

Dynatrace

SentinelOne Singularity Cloud Security

Check Point Infinity

SentinelOne Singularity AI SIEM

Darktrace

Data Hub

View 273 more products

Focus on solutions

Datadog

Executive summary

Datadog integrates extensive monitoring solutions with features like customizable dashboards and real-time alerting, supporting efficient system management. Its seamless integration capabilities with tools like AWS and Slack make it a critical part of cloud infrastructure monitoring.

Datadog offers centralized logging and monitoring, making troubleshooting fast and efficient. It facilitates performance tracking in cloud environments such as AWS and Azure, utilizing tools like EC2 and APM for service management. Custom metrics and alerts improve the ability to respond to issues swiftly, while real-time tools enhance system responsiveness. However, users express the need for improved query performance, a more intuitive UI, and increased integration capabilities. Concerns about the pricing model's complexity have led to calls for greater transparency and control, and additional advanced customization options are sought. Datadog's implementation requires attention to these aspects, with enhanced documentation and onboarding recommended to reduce the learning curve.

What are Datadog's Key Features?

- Sharable Dashboards: Facilitate collaboration with customizable, intuitive dashboards.
- Extensive Integrations: Seamlessly connects with tools like Slack and AWS to support workflows.
- APM and RUM: Provides deep insights into application performance and user interactions.
- Real-Time Tools: Enables agile responses to system issues with real-time monitoring.
- Unified Tagging and Visualization: Eases management of complex systems with simplified visualization.

What Benefits and ROI Should Users Look For?

Efficient Troubleshooting: Centralized logging speeds up the identification and resolution of issues.
Streamlined Workflows: Integrations with popular tools enhance operational efficiency.
Improved Observability: Comprehensive monitoring improves system reliability and performance.
Resource Optimization: Efficient microservices and container management leads to better cloud resource utilization.

Responsive Alerts: Customizable alerts ensure timely identification of critical issues.

In industries like finance and technology, Datadog is implemented for its monitoring capabilities across cloud architectures. Its ability to aggregate logs and provide a unified view enhances reliability in environments demanding high performance. By leveraging real-time insights and integration with platforms like AWS and Azure, organizations in these sectors efficiently manage their cloud infrastructures, ensuring optimal performance and proactive issue resolution.

Sample customers

Adobe, Samsung, facebook, HP Cloud Services, Electronic Arts, salesforce, Stanford University, CiTRIX, Chef, zendesk, Hearst Magazines, Spotify, mercardo libre, Slashdot, Ziff Davis, PBS, MLS, The Motley Fool, Politico, Barneby's

Top comparisons

More comparisons

Dynatrace

Compared 4% of the time

Learn more

New Relic

Compared 3% of the time

Learn more

Splunk AppDynamics

Compared 2% of the time

Learn more

Reviewers - Percentages by top Industries

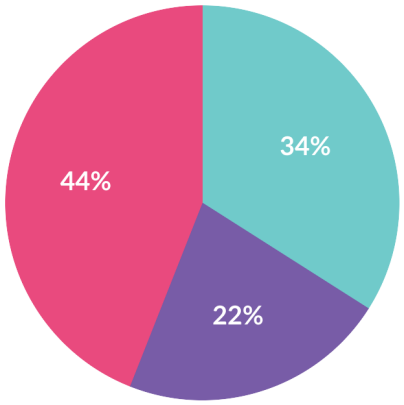
Financial Services Firm	20%
Computer Software Company	18%
Real Estate/Law Firm	6%
Retailer	6%

Visitors Reading Reviews - Percentages by Top Industries

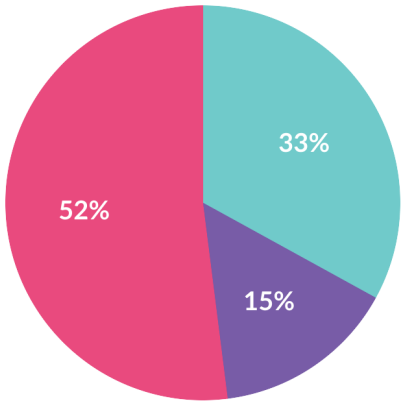
Financial Services Firm	14%
Manufacturing Company	9%
Computer Software Company	8%
Outsourcing Company	6%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "Since adopting Datadog, it has reduced the manual effort by around seven to eight hours per week, making the process completely automated."

Kavya S
Data Engineer at a outsourcing company with 201-500 employees

- "We have seen a clear return on investment with Datadog, mainly in terms of time saved and faster incident handling."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

- "Overall, it has improved operational efficiency and reduced downtime by enabling quicker responses during incidents."

SurajYadav
Network Security Consultant at NTT DATA

"Datadog has positively impacted our organization because our customers are very happy using it."

Abednego Petrus

Technical Manager, Consulting at a outsourcing company with 1,001-5,000 employees

"Datadog has positively impacted our organization, as it has eliminated many negative issues, which I call tool sprawl, by replacing four or five separate monitoring tools with one unified platform."

BasilJiji

System engineer at a retailer with 10,001+ employees

What users had to say about valuable features:

"The best features of Datadog for me are the user-friendly real-time dashboard and its ability to easily integrate with AWS, Azure, Kubernetes, Kafka, and provide a centralized log management system, which gives me excellent visibility into the microservice architecture.

"Datadog has impacted my organization by providing a centralized monitoring system so that each person can trace what is happening in the VM servers, and it has given us a centralized dashboard view.

"Since adopting Datadog, it has reduced the manual effort by around seven to eight hours per week, making the process completely automated.

"Datadog has improved the collaboration across the teams and cross-functional teams, making it very fast and allowing us to easily track what is wrong.."

Kavya S
Data Engineer at a outsourcing company with 201-500 employees

Read full review

"The best features of Datadog are the correlation capabilities and unified visibility. The most useful aspect is that I can see metrics, logs, and service-level data in one place. During troubleshooting, I do not have to switch tools; I can directly correlate spikes in latencies with log error patterns, which saves considerable time. Another feature I find very useful is the dashboards, which are flexible, and I can create views based on what I actually need to monitor daily instead of relying on default setups. The integration with cloud services makes onboarding very easy, and once integrated, most of the data starts flowing automatically without much manual effort.

"Datadog has had a positive impact, mainly by improving how quickly we detect and understand issues. Earlier, when something went wrong, considerable time went into figuring out where the problem actually was. Now, with better visibility across services and logs, we can quickly narrow down the source, whether it is application, infrastructure, or dependency-related. It has also helped in reducing the back and forth between teams because we can validate issues with the data before escalating, which has made incident handling smoother and more efficient overall.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

“One of the best features of Datadog, in my opinion, is its unified visibility across the metrics, logs, and traces in a single platform. The dashboards are very flexible and customizable, which helps a lot in creating meaningful monitoring views based on different use cases. I also find the log management quite useful because it allows quick correlation with metrics during troubleshooting. Another strong feature is its integration, especially with cloud platforms such as AWS or Azure, which makes onboarding and monitoring much easier without heavy manual work.

“Integration with cloud platforms such as Amazon Web Services or Microsoft Azure has really made daily monitoring much easier. Once the integration is set up, Datadog automatically pulls metrics from services such as virtual machines, load balancers, and databases without needing manual configuration on each resource. In one case, I was monitoring a cloud-based application where we started seeing performance issues through Datadog's Azure integrations. I could quickly view metrics from the application server and the back-end database in the same dashboard. It helped me identify that the issue was not network-related but due to the increased load on the backend services. Instead of checking multiple portals, everything was available in one place, which saved time and made troubleshooting faster.

“Datadog has had a positive impact mainly by improving visibility and reducing troubleshooting times. Earlier, we had to rely on multiple tools to check metrics and logs, which delayed root cause analysis. With Datadog, everything is centralized, so it is much faster to identify issues and take actions. It has also helped in proactive monitoring with properly tuned alerts. We are able to detect unusual behaviors such as spiking in traffic or resource usage before it turns into a major incident. Overall, it has improved operational efficiency and reduced downtime by enabling quicker responses during incidents..”

SurajYadav
Network Security Consultant at NTT DATA

Read full review

“Datadog's best feature is real user monitoring.

“I prefer Datadog's real user monitoring most because of its analytics capabilities. First, Datadog is recognized in the Gartner Digital Experience for real user monitoring. Second, the analytics capability is very powerful, enabling us to check the experience of customers first. We can also correlate with the back-end side of the performance for real user monitoring and application monitoring. Finally, the capability of metrics within real user monitoring provides many helpful insights for mobile developers to improve their mobile application performance..”

Abednego Petrus

Technical Manager, Consulting at a outsourcing company with 1,001-5,000 employees

Read full review

"Datadog is an incredibly powerful daily driver for any engineer, and the recent addition of LLM observability for AI apps and Cloud Security Management makes it feel like a platform that is truly keeping up with modern tech trends. The dashboarding and alert integrations are great features offered by Datadog, giving us all the required information on a single screen, and the alert integration performs its job in a very good manner.

Datadog has positively impacted our organization, as it has eliminated many negative issues, which I call tool sprawl, by replacing four or five separate monitoring tools with one unified platform. This has improved our MTTR and broken down silos between Dev and Ops teams.

Since Datadog has been introduced, the response time when seeing an alert has increased, so alerts have been taken care of within less time and routed to the other teams who have been taking the required actions. This has given us a very positive approach towards the entire working culture.."

BasilJiji

System engineer at a retailer with 10,001+ employees

Read full review

"The best features Datadog offers are digital user experience, troubleshooting, and remediation capabilities, which help identify what is going wrong and where. I focused on the root cause analysis of incidents and tickets, as examining the RCAs makes it easier to find remediations and helps with shifting incidents left. Datadog will positively impact my organization by allowing me to handle ticket resolutions at a much faster pace and bring productivity by reducing the number of support engineers required at the monitoring level. If I integrate Datadog with my managed environment or cloud environment, the RCAs and all the left shift will be automated, and with automation, I will be able to reduce the number of support engineers.."

Aman

Enterprise solution architect at a manufacturing company with 10,001+ employees

Read full review

Pain Points

The main pain points mentioned:

✖ "If I could change one thing about Datadog, it would be the pricing, as it has extraordinary functionality, but the pricing is somewhat expensive, and as we increase the number of servers and monitoring services, the cost increases."

Kavya S

Data Engineer at a outsourcing company with 201-500 employees

✖ "One area where Datadog can be improved is around alert quality. In the beginning, it tends to generate many alerts, and without proper tuning, many of them are not actionable."

Kallamuddin Ansari

Cyber Security Consultant at HR Software Solution

✖ "In a dynamic environment, it can generate a lot of alert noise if not tuned properly."

SurajYadav

Network Security Consultant at NTT DATA

✖ "Datadog could improve its pricing because it is very tricky, and most of our customers notice many hidden costs."

Abednego Petrus

Technical Manager, Consulting at a outsourcing company with 1,001-5,000 employees

✖ "Datadog is a platform that can be improved by making its pricing more predictable, as sometimes it is difficult to forecast exactly how much a new project will cost until after we have started ingesting the data."

BasilJiji

System engineer at a retailer with 10,001+ employees

Room for improvement:

"If I could change one thing about Datadog, it would be the pricing, as it has extraordinary functionality, but the pricing is somewhat expensive, and as we increase the number of servers and monitoring services, the cost increases. A more predictable and flexible pricing structure would be beneficial, along with additional customization options and reporting features.."

Kavya S

Data Engineer at a outsourcing company with 201-500 employees

Read full review

"One area where Datadog can be improved is around alert quality. In the beginning, it tends to generate many alerts, and without proper tuning, many of them are not actionable. It would help if there were more built-in guidance or smarter defaults to reduce noise. Another improvement area is cost visibility and control. As log and metric ingestion increases, it has not always been straightforward to track which data is driving the cost. More granular and real-time cost insights would make it easier to manage. Additionally, while the dashboards are flexible, navigating and organizing them at scale can become slightly difficult. Better structuring or management options would help in larger environments.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

"If you are asking for improvements, I feel some small areas where Datadog can improve. One area is alert management. In a dynamic environment, it can generate a lot of alert noise if not tuned properly. More intelligent alerting or built-in recommendations would help. Another aspect is cost visibility. As log ingestion increases, pricing can scale quickly. Having more transparent and granular cost control features would make it easier to manage usage. Also, the initial setup and configuration can feel a bit complex for new users.."

SurajYadav
Network Security Consultant at NTT DATA

Read full review

"Datadog could improve its pricing because it is very tricky, and most of our customers notice many hidden costs. Additionally, if possible, Datadog should offer deployment options not only for SaaS but also for on-premises solutions, which would benefit banking transactions.

"Regarding pricing, it remains tricky with many hidden costs. For technological enhancement, there could be an on-premises option alongside the SaaS version. I also find setting up and configuring Datadog to be very complex.."

Abednego Petrus

Technical Manager, Consulting at a outsourcing company with 1,001-5,000 employees

Read full review

"Datadog is a platform that can be improved by making its pricing more predictable, as sometimes it is difficult to forecast exactly how much a new project will cost until after we have started ingesting the data.

When it comes to the documentation, we do not have much available right now, so if Datadog can improve the documentation part, it would really help the engineers to work on this.

Datadog is the most comprehensive observability tool on the market, and it only loses two points because the pricing for log ingestion can grow quickly if we do not carefully manage our filters.."

BasilJiji

System engineer at a retailer with 10,001+ employees

Read full review

"Datadog could be improved with a simpler graphical user interface that can be extended to non-technical users, such as a CXO, if they want to review the dashboard overall for current tickets and the ticketing dashboard. It would be beneficial to have documentation auto-generated while examining remediations or integration with existing systems.."

Aman

Enterprise solution architect at a manufacturing company with 10,001+ employees

Read full review

Pricing

"The tool is open-source."

Akshay Manchalwar
Technical Support Engineer at Cybage Software

Read full review

"The solution's pricing depends on project volume."

Huu Huy TRUONG
Project senior at Moka Cloud factory

Read full review

"Licensing is based on the retention period of logs and metrics."

Verified user
Site Reliability Engineer at a financial services firm with 1-10 employees

Read full review

"The solution is fairly priced but history and log storage can get costly depending on your needs."

Enrique Bassallo
AWS Cloud Architect Consultant at a manufacturing company with 10,001+ employees

Read full review

"This solution is budget friendly."

Rawat Singhsatit
Solutions Consultant Manager at MFEC

Read full review

SentinelOne Singularity Endpoint

Executive summary

SentinelOne Singularity Complete is an advanced endpoint security platform featuring centralized management across multiple locations. It leverages AI-driven behavior detection, threat prioritization, and ransomware rollback for enhanced protection and streamlined operations.

With a focus on endpoint protection, threat detection, and automated response, SentinelOne Singularity Complete provides comprehensive security through AI-powered behavioral analysis and real-time threat detection. The centralized console simplifies management, offering seamless integration and minimal system impact. Its robust reporting capabilities facilitate compliance with audit-ready reports. Lightweight agents operate across diverse environments, improving visibility and performance while curbing manual efforts. To optimize its utility, faster console load times and improved customizability in reports and dashboards are recommended. Users may benefit from smoother integration with IT tools and enhanced policy management flexibility, as well as upgraded agent processes and simplified endpoint deployment. Expanding built-in analytics and refining alert management can further heighten platform efficacy.

What are the key features of SentinelOne Singularity Complete?

AI-Powered Detection: Utilizes advanced AI to identify potential threats based on behavior.
Automatic Remediation: Automatically rectifies detected issues, reducing response times.
Ransomware Rollback: Restores data to previous states if affected by ransomware attacks.
Centralized Dashboards: Provides real-time insights through intuitive dashboards.
Threat Prioritization: Identifies and ranks threats based on potential impact.

What benefits should users look for in reviews?

Integration: Seamlessly connects with security solutions to enhance risk management.
Minimal System Impact: Operates efficiently, preserving system performance.
Enhanced Protection: Delivers robust threat defense through AI-driven technology.
Compliance Support: Offers detailed reporting for audit readiness.
User Convenience: Combines autonomous decision-making with an intuitive interface.

In various industries, SentinelOne Singularity Complete is implemented for endpoint protection and incident management. Companies rely on it for its real-time threat detection and automated response capabilities, ensuring compliance and reduced manual intervention. Its adaptive nature supports diverse environments, enhancing operational efficiency.

Sample customers

Havas, Flex, Estee Lauder, McKesson, Norfolk Southern, JetBlue, Norwegian airlines, TGI Friday, AVX, Fim Bank

Top comparisons

More comparisons

CrowdStrike Falcon

Compared 4% of the time

Learn more

Fortinet FortiEDR

Compared 3% of the time

Learn more

Cortex XDR by Palo Alto Networks

Compared 3% of the time

Learn more

Reviewers - Percentages by top Industries

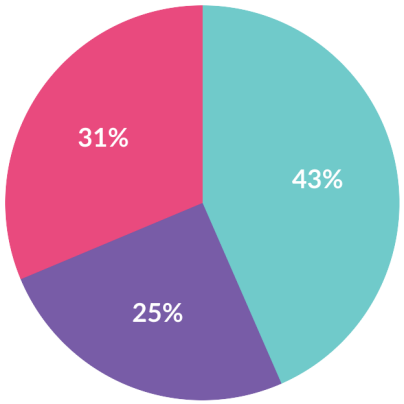
Manufacturing Company	16%
Media Company	11%
Computer Software Company	9%
Financial Services Firm	7%

Visitors Reading Reviews - Percentages by Top Industries

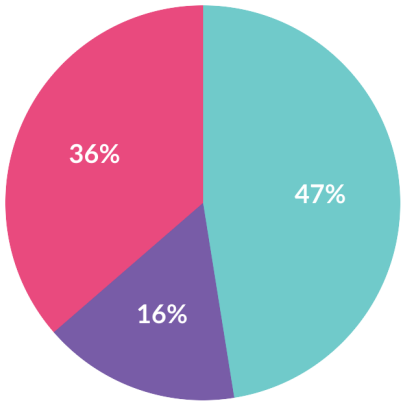
Outsourcing Company	9%
Manufacturing Company	9%
Computer Software Company	9%
Financial Services Firm	7%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "When I compare SentinelOne Singularity Endpoint with other solutions like CrowdStrike, I find that SentinelOne Singularity Endpoint is the best because the threat detection is real-time and incident response is also real-time."

Paramjeet Singh

IT Engineer at Softcell Technologies Limited

- "My advice for others looking into using SentinelOne Singularity Endpoint is to go for it, as it effectively does the EDR job."

Verified user

Technical engineer at a tech services company with 10,001+ employees

- "SentinelOne Singularity Endpoint has positively impacted my organization by improving endpoint security through faster threat detection, providing better visibility and quicker incident response features including AI, automation, endpoint isolation, and effectively containing threats while reducing the workload for the SOC team."

Tanuja Parab

Dark L2 Web Analyst at a tech services company with 11-50 employees

"Overall, SentinelOne Singularity Endpoint has been a valuable security solution for my organization, as the AI-driven detection, automatic response, and centralized management provide strong protection while reducing the time required for monitoring and incident response."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

"SentinelOne Singularity Endpoint has positively impacted our organization by strengthening our overall endpoint security and improving our ability to detect, investigate, and respond to threats."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

What users had to say about valuable features:

"Deep Visibility is the best feature because I can analyze multiple types of logs and check on any attacks that happen. Purple AI is also one of the best features because I can search for most types of queries and use it in Deep Visibility. Real-time detection in SentinelOne Singularity Endpoint is better compared to other Singularity tools.

When I compare SentinelOne Singularity Endpoint with other solutions like CrowdStrike, I find that SentinelOne Singularity Endpoint is the best because the threat detection is real-time and incident response is also real-time. The multiple types of features, particularly Purple AI, are great compared to AI features in other EDR tools, and Deep Visibility is also the best in comparison to other EDR tools.

SentinelOne Singularity Endpoint helps me ingest and correlate across security solutions by assisting in my implementation of other tools. I have integrated multiple tools, including automation tools, so when any alerts are triggered, I can automatically send them to the client side within seconds for client safety.

I have used the Ranger functionality in SentinelOne Singularity Endpoint, which belongs to asset inventory. There are multiple types of assets in my organization, such as servers and hosts, and it shows how many agents are installed, how many laptops, how many servers, and how many endpoints or PCs are available with SentinelOne Singularity Endpoint installed.

Purple AI in SentinelOne Singularity Endpoint is important for data privacy and security as an AI feature. I can ask any questions related to SentinelOne Singularity Endpoint, and it provides answers about searching logs in Deep Visibility. Purple AI can create queries that are easily copied and pasted, allowing me to see the results regarding the logs.

Purple AI helps amplify team knowledge because if any new employees join, they can ask anything related to SentinelOne Singularity Endpoint and Purple AI provides answers to their queries. It also provides use cases that help create multiple types of alerts, allowing me to fine-tune my rules for client safety.

SentinelOne Singularity Endpoint helps streamline threat investigations for

SecOps workflows because it provides multiple data points found in alerts, such as hashes and the frequency of triggering alerts, making it easier to investigate.."

Paramjeet Singh
IT Engineer at Softcell Technologies Limited

Read full review

"The best features of SentinelOne Singularity Endpoint include the endpoint level remediation and the indicators referring for an alert, giving an overall picture of the actions that need to be taken by the analyst side.

"The remediation part of SentinelOne Singularity Endpoint plays a major role in investigation because if I am unsure whether a file is genuine or malicious, SentinelOne Singularity Endpoint analyzes its behavior and automatically remediates it, facilitating easy removal of legitimate files from quarantine.

"The user accessibility in SentinelOne Singularity Endpoint console is a feature I would highlight, as it is convenient for a new analyst, enabling them to understand and migrate to the console within a week.

"SentinelOne Singularity Endpoint positively impacts my organization by effectively detecting alerts and endpoint level alerts.

"The positive impact of SentinelOne Singularity Endpoint is evident in the remediation part, as it activates remediation as soon as the alert triggers, reducing environmental impact.."

Verified user
Technical engineer at a tech services company with 10,001+ employees

Read full review

"My favorite feature of SentinelOne Singularity Endpoint is the behavioral AI detection because it identifies suspicious activity or malicious PowerShell execution, even when malware has not been seen before, helping us respond to threats much faster.

"One example of how behavioral AI detection in SentinelOne Singularity Endpoint has helped us in real scenarios is when we detected PowerShell activity on an endpoint. Instead of relying on known malware signatures, it identified abnormal behavior, allowing us to investigate the process tree, confirm the suspicious activity, isolate the endpoint, and prevent the spread, enabling containment of the incident quickly before it impacted other systems.

"The behavioral AI in SentinelOne Singularity Endpoint helped us identify suspicious activity and is a feature I truly appreciate, as it aids in our investigations promptly alongside our SOC team.

"SentinelOne Singularity Endpoint has positively impacted my organization by improving endpoint security through faster threat detection, providing better visibility and quicker incident response features including AI, automation, endpoint isolation, and effectively containing threats while reducing the workload for the SOC team.

"I do not have exact metrics to share, but I have definitely seen a reduction in the manual effort of our SOC team. For instance, whenever SentinelOne detects suspicious behavior, it automatically correlates related processes and provides a complete process tree, saving analysts' time because we do not have to manually piece together events. Features including automation remediation and endpoint isolation also help contain threats quickly and decrease required manual intervention.."

Tanuja Parab
Dark L2 Web Analyst at a tech services company with 11-50 employees

Read full review

"The best features of SentinelOne Singularity Endpoint are its AI-powered behavioral detection, automated threat response, and endpoint isolation capabilities. I also appreciate the centralized management console, which makes it easy to monitor all the endpoints and investigate incidents. The ability to automatically quarantine malicious files and provide a clear attack timeline helps me reduce investigation time and simplifies incident response.

The feature I rely on most from SentinelOne Singularity Endpoint is the automated threat detection and response. It identifies suspicious behavior in real time and can automatically quarantine malicious files or isolate the affected endpoint. This reduces the amount of manual investigation required, speeds up incident response, and allows me to focus on other IT admin tasks instead of constantly monitoring endpoints.."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Read full review

“The best features of SentinelOne Singularity Endpoint are Purple AI and the network containment option, with Purple AI being the most important feature and the network containment model being the best feature.

SentinelOne Singularity Endpoint has helped me consolidate security solutions as it is also used as a single solution.

I use the Ranger functionality, which is used for finding known and unknown devices.

The Ranger functionality provides clear network and asset visibility by showing how many endpoints are in the network and how many endpoints are not in the network.

The ability to ingest and correlate across various security solutions is used for detection, incident detection, and response, which is related to the high severity of incident detection and preventing malware and ransomware attacks.

Purple AI plays a crucial role in amplifying my team knowledge by being used for threat hunting and incident summarization on indicators of compromise like file hashes, IP addresses, and domains, helping us find the root cause of attacks.

Purple AI impacts streamlining threat investigations on my SecOps workflow by enabling faster threat detection, reducing investigation time, and improving incident response.

SentinelOne Singularity Endpoint frees up about twenty percent of my time.

It has reduced my mean time to detect and my mean time to respond to incidents within fifteen minutes..”

Vedangi Jadhav
Technical Support Engineer at Softcell Technologies

Read full review

"The best features of SentinelOne Singularity Endpoint include AI-powered threat detection and prevention, autonomous response and remediation, Storyline incident tracking, ransomware protection and rollback, and endpoint detection and response capabilities. It also has a single lightweight agent, protection across different environments, deep visibility, and investigation tools, and it offers identity and attack path context with related Singularity capabilities.

"The AI-powered detection and autonomous response capabilities have helped my team by improving our ability to identify and respond to threats quickly instead of relying only on manual investigation or signature-based detection. SentinelOne Singularity Endpoint helps to detect suspicious behaviors and emerging threats in real time while reducing the workload on my security team by automatically containing threats, stopping malicious processes, and helping prevent further impacts.

"SentinelOne Singularity Endpoint has positively impacted our organization by strengthening our overall endpoint security and improving our ability to detect, investigate, and respond to threats. Its AI-driven detection and automated response capability have reduced the time needed to identify and contain security incidents, improved visibility across endpoints, streamlined security operations, and reduced the manual efforts required for threat investigation and remediation. By automating key response actions and providing better incident context, SentinelOne Singularity Endpoint has helped my team improve efficiency, minimize risk, and maintain a stronger security posture, which has resulted in reduced team operations time.."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Read full review

Pain Points

The main pain points mentioned:

✖ "In SentinelOne Singularity Endpoint, one area that has room for improvement is the custom dashboard, which is not supported."

Paramjeet Singh

IT Engineer at Softcell Technologies Limited

✖ "SentinelOne Complete did not reduce alerts; instead, it increased noise in the environment until fine-tunings were done for customized rules."

Verified user

Technical engineer at a tech services company with 10,001+ employees

✖ "While SentinelOne Singularity Endpoint is a strong endpoint security solution, there are areas that could be improved."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

✖ "In SentinelOne Singularity Endpoint, there is room for improvement in custom rules and the dashboard for finding rules and blocking actions."

Vedangi Jadhav

Technical Support Engineer at Softcell Technologies

✖ "SentinelOne Singularity Endpoint provides strong protection and automation capabilities, but there are a few areas where it could be improved, such as enhancing the user experience with more intuitive dashboards and simplified workflows."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Room for improvement:

"In SentinelOne Singularity Endpoint, one area that has room for improvement is the custom dashboard, which is not supported. The default dashboard cannot be modified, so I suggest improvements on the operations management side.."

Paramjeet Singh

IT Engineer at Softcell Technologies Limited

Read full review

"Recently, I faced an issue with SentinelOne Singularity Endpoint while detecting rogue devices, as there is a gap when scanning initiated from the admin console, recognizing different MAC IDs depending on the connection type, which leads to conflict between managed and unmanaged assets.

"Another area needing improvement is the process graph of SentinelOne Singularity Endpoint, which could be made more user-friendly, eye-catching, and offer a better in-depth view.."

Verified user

Technical engineer at a tech services company with 10,001+ employees

Read full review

"I am satisfied with SentinelOne Singularity Endpoint overall, but if it could be improved, it would be in providing more customizable reporting, a richer dashboard, and broader integration with third-party tools. Other than that, I find it effective and reliable with no major suggestions for improvement.

"Based on my experience with SentinelOne Singularity Endpoint, I have not encountered any major issues that significantly affect our day-to-day operations. The platform has been stable, and while every product continues to evolve with new features and integrations, I do not have additional improvements to suggest at this time.."

Tanuja Parab

Dark L2 Web Analyst at a tech services company with 11-50 employees

Read full review

"While SentinelOne Singularity Endpoint is a strong endpoint security solution, there are areas that could be improved. The management console could be more intuitive for new users, and some advanced features have a learning curve. Reporting and dashboard customization could offer more flexibility, and more detailed documentation and troubleshooting guidance would help admins resolve issues.."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Read full review

"SentinelOne Singularity Endpoint provides strong protection and automation capabilities, but there are a few areas where it could be improved, such as enhancing the user experience with more intuitive dashboards and simplified workflows. These improvements would make it easier for administrators to quickly access important insights and manage threats. Additional customization options for alerts, reporting, and automation policies would also be valuable, allowing organizations to better tailor the platform to their specific security needs. Improvements in integrations with a wide range of third-party security tools would also be beneficial.."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Read full review

"Everything has been fine from my side. We are getting feedback from customers who are expecting web protection. The malware and Singularity capabilities are working fine with no problems. It can detect virus and spyware effectively. However, competitors such as Trellix and Trend Micro have features for web protection with category-based web protection for web security. This option is not available in SentinelOne Singularity Endpoint. We can block a particular URL, but we need to manually add the URL in SentinelOne Singularity Endpoint. Competitors such as Trellix and Trend Micro have category-based options such as social networking and search engines. If SentinelOne Singularity Endpoint provides this kind of feature in the future, it will be easier to approach our customers, and we can easily transition our existing customers from Trend Micro and Trellix.."

Karthick Elangovan
Technical Support Team Leader at Safezone Secure Solutions Private Limited

Read full review

Pricing

"The pricing appears to be pretty affordable."

Yasiru Perera
Lead Engineer - Systems & Security at Connex Information Technologies PVT LTD

Read full review

"The pricing was very similar in terms of its competitors, but I believe SentinelOne's capability and willingness to attract new business allowed us to save some extra money."

Verified user
Co-Founder & VP Sales and Marketing at a tech services company with 11-50 employees

Read full review

"We buy the licensing in bulk. From a pricing standpoint, because we buy in bulk, we get very good pricing. Based on its functionality and capabilities, it is well worth the price. I do not think it is at all expensive based on what you get in the solution. We use the complete up to the core. Our pricing is probably a little bit more than somebody who is on the core. In general, it is well worth what you get for the price you pay."

Marc McGrath
Chief Information Officer at a tech services company with 1-10 employees

Read full review

"SentinelOne Singularity Complete is expensive compared to Microsoft but not Sophos."

Joseph Damian
IT Director at a wholesaler/distributor with 11-50 employees

Read full review

"I find the licensing cost for SentinelOne Singularity Complete fair."

Kevin Thompson.
Director of information technology at Stuart & Branigin LLP

Read full review

Dynatrace

Executive summary

Dynatrace offers AI-driven root cause analysis, full-stack observability, and more. Its seamless integration and automated alerts enhance operational efficiency for application performance monitoring across diverse environments.

Dynatrace provides users with comprehensive tools for proactive monitoring, leveraging AI-powered insights to detect bottlenecks and monitor user behavior. It enhances system dependency visualization via Smartscape and offers deep transaction insights through PurePath. Session Replay captures real user experiences, while custom dashboards emphasize essential metrics. Integration capabilities and seamless deployment are key, though users face challenges with navigation, integration, and licensing. Enhancing third-party training tools and optimizing real-time AI diagnostics is desired, with demands for better database monitoring reports and simpler UI.

What are Dynatrace's key features?

- AI-Driven Root Cause Analysis: Identifies issues with precision.
- Full-Stack Observability: Monitors across all platforms.
- Smartscape: Visualizes system dependencies.
- PurePath: Provides transaction flow insights.
- Session Replay: Captures user interactions.
- Custom Dashboards: Focuses on essential metrics.
- Automated Alerts: Minimizes downtime.

What benefits should users consider?

- Operational Efficiency: Enhances performance management.
- Seamless Deployment: Reduces manual intervention.
- Integration Capabilities: Ensures smooth system coexistence.
- User Experience Insights: Tracks behavior and reliability.

Dynatrace is implemented in industries like finance for monitoring infrastructure and user experience. In manufacturing, it helps ensure system reliability. Its AI-driven approach is crucial for cloud deployments, supporting performance optimization and proactive monitoring.

Sample customers

Audi, Best Buy, LinkedIn, CISCO, Intuit, KRONOS, Scottrade, Wells Fargo, ULTA Beauty, Lenovo, Swarovsk, Nike, Whirlpool, American Express

Top comparisons

More comparisons

Datadog

Compared 5% of the time

Learn more

Splunk AppDynamics

Compared 4% of the time

Learn more

New Relic

Compared 4% of the time

Learn more

Reviewers - Percentages by top Industries

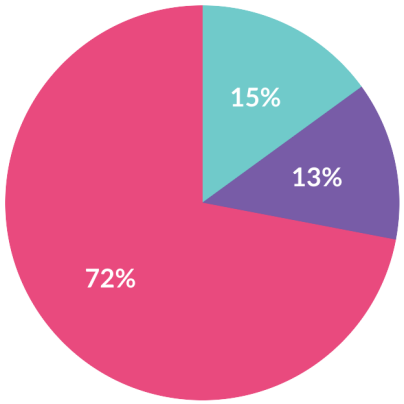
Financial Services Firm	32%
Insurance Company	10%
Computer Software Company	9%
Manufacturing Company	8%

Visitors Reading Reviews - Percentages by Top Industries

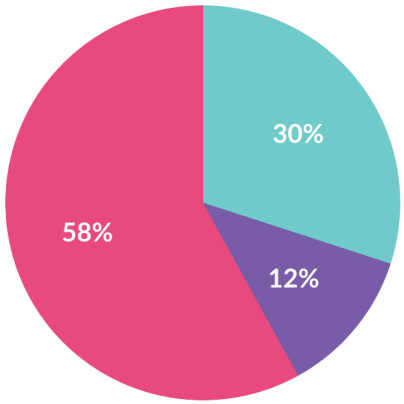
Financial Services Firm	19%
Manufacturing Company	9%
Outsourcing Company	6%
Computer Software Company	6%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "By using the APM tool for resource management and time management, we have saved a lot of time, so I would say this is a good investment that the organization has made."

Dipu Das

Senior performance tester at a outsourcing company with 10,001+ employees

- "Dynatrace has contributed to significant improvements such as reducing P1 tickets resolution time from four hours to under one hour and drastically cutting alert volumes from between two hundred to four hundred alerts per week down to approximately sixty to one hundred twenty."

Vaibhav Karad

BizOps Engineer at a tech company with 10,001+ employees

- "We have seen an average three-year return on investment of 451%, which is a huge number when it comes to the saving part."

BasilJiji

System engineer at a retailer with 10,001+ employees

"Dynatrace has positively impacted my organization by allowing us to see very quick action whenever there is an issue with production."

Vinothkumar Sugumar

Senior Software Engineer at a retailer with 10,001+ employees

"I advise anyone looking to set up a monitoring system in their project to consider Dynatrace because it will monitor their infrastructure, servers, and application performance, providing automatic service discovery and real-time metrics; it is the best option to choose or set up in their project."

Verified user

Cloud Engineer at a tech vendor with 10,001+ employees

What users had to say about valuable features:

"For me, the best feature Dynatrace offers is full-stack observability, which allows me to check my infrastructure or the containers because most of my applications are cloud-based, and with Dynatrace, I can check the database or the network path, or which are on-premises or cloud, making full-stack observability more suitable for me.

"Dynatrace is our APM tool, which provides deep code-level visibility, allowing us to check the methods or exceptions, database calls, or external services, and we can easily trace them out.

"Dynatrace has positively impacted my organization because usually when I do a load test, our API SLA is only one second, but it crosses more than three seconds or five seconds, and by using this APM tool, we can figure out what is causing it, what kind of error it is throwing, and how we can optimize it, making it very useful for my organization as well as for me while doing load testing.

"For the metrics or numbers, our error rate should be less than three percent, and achieving less than three percent, even if it is one percent, is very good, and the reduction of the error rate by using Dynatrace was quite good.."

Dipu Das

Senior performance tester at a outsourcing company with 10,001+ employees

Read full review

"The best features that Dynatrace offers include the AI-powered root cause analysis with Davis AI, which automatically identifies root causes by correlating metrics, logs, and traces, saving substantial time during incident resolution. Full-stack observability is another top feature, as it covers application, infrastructure, and network-related services while integrating with cloud environments. I appreciate the PurePath distributed tracing that provides deep dive insights into every transaction across microservices, helping us pinpoint slow database queries and external API calls. RUM allows us to track actual user sessions that impact UX, while synthetic monitoring proactively detects issues before they affect real users. OneAgents simplify infrastructure-related configurations, and I want to emphasize the importance of business analytics integration to tie technical metrics with business KPIs, as my role involves prioritizing issues based on their impact on business outcomes.

"The feature that saves me the most time is Davis AI, as it automatically analyzes all data elements, understands metrics, logs, and traces, and pinpoints exact root causes of issues. Instead of manually digging through dashboards, I receive clear explanations of problems, such as high CPU usage due to garbage collection or memory issues, which drastically reduce the mean time to resolution (MTTR). The manual investigations that used to take hours can now be solved in under a minute, eliminating guesswork and allowing me to respond quickly without needing cross-team checks. For instance, Davis AI recently flagged a slowdown in microservices that led me to a recent inefficient data query introduced during deployment, allowing me to roll back changes in only fifteen minutes.."

Vaibhav Karad

BizOps Engineer at a tech company with 10,001+ employees

Read full review

“Dynatrace is a super platform that easily manages over 10,000 hosts and is highly stable, making it the best.

“Dynatrace manages over that many hosts through an elastic grid architecture, which efficiently handles thousands of services and containers with minimal overhead.

“Dynatrace has drastically improved our MTTR and provides one monitoring tool across the entire landscape. We have achieved a massive reduction in operational costs and tool sprawl.

“We have seen an average three-year return on investment of 451%, which is a huge number when it comes to the saving part. We are seeing an increase in the efficiency for our IT and DevOps team with introducing Dynatrace, including 40% fewer Sev1 and Sev2 outages annually.

“Dynatrace is a powerful expert-level tool that transforms complexity into a business asset. The inclusion of runtime application security has become a critical feature for our modern DevSecOps workflows..”

BasilJiji

System engineer at a retailer with 10,001+ employees

Read full review

"The best features Dynatrace offers include AI-based metrics collection, which impresses me a lot because it is very helpful to quickly check all the issues that come up. The first thing is end-to-end visibility across all the services. That is one thing where we can know the infrastructures, hosts, containers, VMs, and what is happening with the application. Then this automatic discovery and mapping helps a lot. Distributed tracing, which is the PurePath thing, is a very helpful feature. For root cause analysis, the recent Davis AI is something game-changing and is helping a lot, saving a lot of time. That is the main feature right now. The remaining things are the foundational features and making access to all the features so quick. Davis AI makes use of the features that exist, and now I am using those features. So that is a good thing.

"The root cause analysis feature specifically helps my team save time or solve issues by providing detailed timings and external APIs and cache whenever the PurePath thing comes, to trace every subsequent call. We are not only working with our own microservices; we are working along with multiple vendors. Sometimes the latency is not from our system but from a vendor system. During those times, we see why this service is taking a lot of time because this service is waiting for a call. These small details on timings and the DB cache add so much value to the PurePath thing. The AI powered Davis detects anomalies and root cause issues across the stack, which is also a valuable feature. Application topology and network flows are also very helpful. These things are primarily helping us.

"Before moving on, I would appreciate the custom dashboard and visualization part of Dynatrace, where I did not talk much about those things. The real-time charts are very helpful to monitor the health of the application. Heat maps are really cool to see, and service flow maps are really required to understand the things. The key performance indicators are very good. These are the key standpoints of my application metrics. Whenever I am the on-call person in PagerDuty, these are the things I am fundamentally looking for. This is a lookup book for me to make sure this application is in good health.

"Dynatrace has positively impacted my organization by allowing us to see very quick action whenever there is an issue with production. We can quickly open the dashboard, see the error rates where it is happening, and perform a quick analysis

to find the root cause. That is a huge part. The second part is improvisation; whenever we come to a stable state and have some technical debt to take, we can check what APIs are causing latency and work on those issues, asking why it is happening. Sometimes it leads to redesigning the domain, coming from the dashboards. Every time we do not know how many services exist or why a particular service is working for this domain while we are in some centralized stage. But while coming to this Dynatrace dashboard, seeing all services in one place helps us think why this service is talking to this service. We can classify domain-level and regroup the domain. This way, it is helping us by giving a mental model and a mental map to track everything. That is a huge win for us.."

Vinothkumar Sugumar
Senior Software Engineer at a retailer with 10,001+ employees

Read full review

"The best features Dynatrace offers include configuring alerts and dashboards, such as problem notifications and custom dashboards for EC2 health, ECS service performance, error rates, and latency, along with anomaly detection and security and IAM, allowing outbound traffic to Dynatrace and using IAM roles for EC2 with no sensitive data stored locally. In my project, I use Dynatrace OneAgent on EC2 and ECS to monitor the infrastructure, containers, and application performance, providing automatic service discovery, real-time metrics, distributed tracing, and AI-based root cause analysis.."

Verified user
Cloud Engineer at a tech vendor with 10,001+ employees

Read full review

"The best feature Dynatrace offers is APM. When I mention APM, I am referring to Application Behavior Monitoring, and database monitoring is what makes that feature stand out for me.

"Database monitoring is very helpful to know the performance of query performance, meaning how much latency there is for the query once called from the application side, and if there is an error from the query, it indicates issues such as ORA errors from Oracle or other errors from PostgreSQL and MySQL or any DBMS.

"Dynatrace positively impacts our organization because it is a unified monitoring solution that centralizes the performance of infrastructure, application, and database.."

Abednego Petrus

Technical Manager, Consulting at a outsourcing company with 1,001-5,000 employees

Read full review

Pain Points

The main pain points mentioned:

✖ "Dynatrace itself is a very good platform where the UI interface is very simple and usable, but I would say if it were made even more simple, similar to our Splunk dashboard, that could help users or newer users understand it more easily, especially since sometimes I have seen when using Dynatrace, we are not able to add the time frame properly."

Dipu Das

Senior performance tester at a outsourcing company with 10,001+ employees

✖ "In terms of improvements, I believe Dynatrace could enhance cost and licensing structures, as the current pricing can be expensive for large-scale deployments."

Vaibhav Karad

BizOps Engineer at a tech company with 10,001+ employees

✖ "The platform could improve its custom visualization options, as some executive dashboards feel restrictive compared to other tools."

BasilJiji

System engineer at a retailer with 10,001+ employees

✖ "I think Dynatrace can be improved in dashboard creation, as this is the face of a product."

Vinothkumar Sugumar

Senior Software Engineer at a retailer with 10,001+ employees

✖ "Dynatrace can be improved by fine-tuning AI-based settings."

Verified user

Cloud Engineer at a tech vendor with 10,001+ employees

Room for improvement:

"Dynatrace itself is a very good platform where the UI interface is very simple and usable, but I would say if it were made even more simple, similar to our Splunk dashboard, that could help users or newer users understand it more easily, especially since sometimes I have seen when using Dynatrace, we are not able to add the time frame properly.

"If you add some more fields with simple words or simple terms instead of the complex terms used for a resource, that might be helpful.

"Dynatrace can be better and more user-friendly, and that is my advice, but overall, it is a good application and APM tool for a performance tester.."

Dipu Das

Senior performance tester at a outsourcing company with 10,001+ employees

Read full review

"Beyond the features already discussed, I would like to see improvements in auto-discovery, smart instrumentation, and a unified data model to centralize all metrics and events on a single platform. This change would minimize the need to jump between tools and manually stitch data together. Continuous improvement features tied to SLO objectives should also ensure deployments meet performance standards.

"In terms of improvements, I believe Dynatrace could enhance cost and licensing structures, as the current pricing can be expensive for large-scale deployments. More flexible and granular billing options would be beneficial, especially for ephemeral workloads. Additionally, while the initial setup is straightforward, understanding advanced features requires expertise. Improvements in user guidance, such as tutorials or workflow documentation, could help new users navigate the platform more easily, particularly with customization options and dashboard enhancements.

"Further improvements could include fostering deep native integrations with major platforms and enhancing the ease of integrating with CI/CD tools such as Jenkins or GitHub Actions. Additionally, supporting better OpenTelemetry for custom traces and metrics would simplify setups. Native integrations with BI tools would enhance our analytical capabilities, making real-time dashboard creation easier.."

Vaibhav Karad
BizOps Engineer at a tech company with 10,001+ employees

Read full review

"The platform could improve its custom visualization options, as some executive dashboards feel restrictive compared to other tools. Additionally, making raw log data more cost-effective would add significant value.."

BasilJiji
System engineer at a retailer with 10,001+ employees

Read full review

"I think Dynatrace can be improved in dashboard creation, as this is the face of a product. Although Dynatrace may have many things, new users typically do not know the whole power of the product. To onboard new people, it would be beneficial to provide template dashboards or suggested dashboards. Organizations working with microservice architecture will follow some templates, so suggesting simple, hand-picked features that are really helpful could make a difference. Quick configurable and customizable templates would be very useful. Whenever they come into the product, they can use this template and feel that their product is applied to it. Immediately, they will think everything is online and can improve easily. This base can be provided in template form. Since Dynatrace has a lot of features now, the AI integration makes it simple, but the product itself is very huge. To understand and utilize it, maybe it would be good to index the essential features.."

Vinothkumar Sugumar
Senior Software Engineer at a retailer with 10,001+ employees

Read full review

"Dynatrace can be improved from the security side because other observability products are enhancing security features, while Dynatrace has room for improvement in this area.

"For integration, Dynatrace can improve with WebMethod because it is quite common among our customers using that platform, and they want to monitor their transactions for ESB, which is middleware.

"Dynatrace could improve its recommendations, which are not only for cause analysis but also for application performance, infrastructure, and database, including database tuning for the query. I would rate Dynatrace an eight for these reasons.."

Abednego Petrus

Technical Manager, Consulting at a outsourcing company with 1,001-5,000 employees

Read full review

"I give it a nine because the one percent improvement is required in itself, since if I provide a ten, then there is no room for improvement.

"Dynatrace provides regular upgrades as a software used to provide server health checks, network monitoring, and application performance monitoring, so the team looking into Dynatrace's development provides regular updates. I don't think I can provide any improvements to Dynatrace as an end user.."

Dinesh Nikam

Network Engineer at a tech vendor with 10,001+ employees

Read full review

Pricing

"Dynatrace is an expensive solution."

Roopesh Shetty
Senior IT architect at a healthcare company with 51-200 employees

Read full review

"The solution is not cheap."

KapilK
Senior Manager, Technical Architect Performance at Duck Creek Technologies

Read full review

"We purchased a subscription for one year and it is an expensive solution for a large enterprise like ours."

Verified user
Software Systems Analyst at a manufacturing company with 10,001+ employees

Read full review

"The pricing is a bit on the higher end."

Sathis-Kumar
Senior Manager at Bank of America

Read full review

"Dynatrace is usually paid on a yearly basis."

Verified user

Solutions director at a tech services company with 51-200 employees

Read full review

SentinelOne Singularity Cloud Security

Executive summary

SentinelOne Singularity Cloud Security offers a streamlined approach to cloud security with intuitive operation and strong integration capabilities for heightened threat detection and remediation efficiency.

Singularity Cloud Security stands out for its real-time detection and response, effectively minimizing detection and remediation timelines. Its automated remediation integrates smoothly with third-party tools enhancing operational efficiency. The comprehensive console ensures visibility and support for forensic investigations. Seamless platform integration and robust support for innovation are notable advantages. Areas for development include improved search functionality, affordability, better firewall capabilities for remote users, stable agents, comprehensive reporting, and efficient third-party integrations. Clarity in the interface, responsive support, and real-time alerting need enhancement, with a call for more automation and customization. Better scalability and cost-effective integration without compromising capabilities are desired.

What are SentinelOne Singularity Cloud Security's standout features?

- Ease of Use: Intuitive operation simplifies navigation across platforms.
- Real-Time Detection: Quick identification and response to threats.
- Automated Remediation: Streamlines recovery processes with integration capabilities.
- Forensic Visibility: Aids in thorough threat analysis and prevention strategies.
- Comprehensive Console: Offers full visibility and historical data tracking.
- Platform Integration: Supports seamless operation across cloud and hybrid environments.

What benefits should users expect from SentinelOne Singularity Cloud Security?

Enhanced Efficiency: Automation and third-party integration improve threat response.
Improved Detection: Reduces mean time to detect and respond to threats.
Operational Support: Comprehensive visibility and forensic tools aid operational decisions.
Cost Efficiency: Affordable integration with scaling capabilities without high overhead.

SentinelOne Singularity Cloud Security is deployed in industries needing robust cloud security posture management, endpoint protection, and threat hunting. Utilized frequently across AWS and Azure, it assists in monitoring, threat detection, and maintaining compliance in diverse environments while providing real-time alerts and recommendations for proactive threat management.

Top comparisons

More comparisons

Wiz

Compared 7% of the time

Learn more

Prisma Cloud by Palo Alto Networks

Compared 6% of the time

Learn more

Microsoft Defender for Cloud

Compared 5% of the time

Learn more

Reviewers - Percentages by top Industries

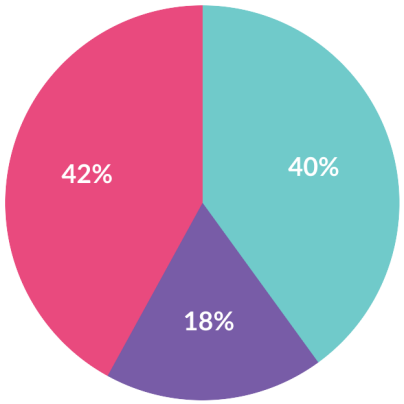
Computer Software Company	18%
Construction Company	16%
Media Company	11%
Insurance Company	7%

Visitors Reading Reviews - Percentages by Top Industries

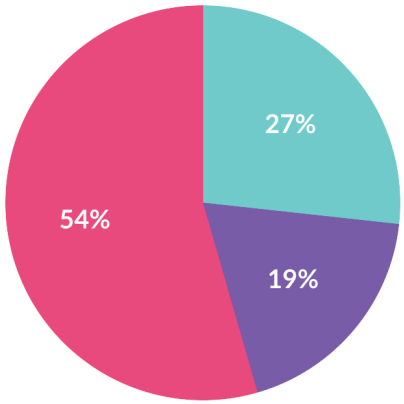
Financial Services Firm	13%
Computer Software Company	10%
Manufacturing Company	9%
Comms Service Provider	6%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "SentinelOne Singularity Cloud Security has improved our security visibility, reduced the manual effort, accelerated the remediation process, and strengthened compliance across cloud environments."

DeepPujara

Siem Engineer at a tech services company with 11-50 employees

- "SentinelOne Singularity Cloud Security has improved our organization's cloud security by giving us centralized visibility across cloud assets, workloads, identities, and configurations."

Verified user

Cyber Security Engineer at a outsourcing company with 51-200 employees

- "SentinelOne Singularity Cloud Security has improved our organization's security visibility and response capability by giving our team better insights into cloud risk and suspicious activity."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

"The quality of the product in terms of reliability and what it offers is exceptional."

Prince Joseph

Group Chief Information Officer at NeST Information Technologies Pvt Ltd

"SentinelOne Singularity Cloud Security has improved our organization's overall security posture by providing better visibility into cloud workloads and faster threat detection."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

What users had to say about valuable features:

Key features of SentinelOne Singularity Cloud Security include Cloud Security Posture Management (CSPM), cloud workload protection, risk prioritization, compliance monitoring, and unified visibility across cloud environments.

The risk prioritization feature of SentinelOne Singularity Cloud Security has definitely made a difference in our daily workflow. Compared to some other cloud security tools we have used, SentinelOne does a better job of prioritizing risk based on potential impact instead of simply listing every finding with the same level of importance. This helps us focus on the issues that require immediate attention rather than spending time triaging low-risk alerts. In practice, it has reduced the amount of manual work effort needed to review findings.

“It makes it easier to decide what should be remediated first with SentinelOne Singularity Cloud Security, especially in large cloud environments where the number of alerts can grow quickly. We still validate critical findings before making changes, but overall, it has made our remediation process more efficient and helped the team respond faster.

“SentinelOne Singularity Cloud Security has improved our security visibility, reduced the manual effort, accelerated the remediation process, and strengthened compliance across cloud environments.

“Since using SentinelOne Singularity Cloud Security, we have reduced the time spent identifying cloud misconfigurations, improved remediation efficiency, and achieved better compliance readiness through continuous monitoring. .”

DeepPujara

Siem Engineer at a tech services company with 11-50 employees

Read full review

"Standout features include Cloud Security Posture Management, Cloud Workload Protections, Attack Path Analysis, Cloud Security, Data Security, and AI-powered investigation in which I use Purple AI to automate investigation, correlate cloud, endpoint, and identity telemetry, summarize incidents, and reduce alerts. It also has a unified security platform that brings together cloud, endpoint, and identity security in a single console with a shared data model. This simplifies operations and enables faster incident response.

"The feature that has made the biggest difference is Cloud Security Posture Management. In my day-to-day work, it continuously monitors our cloud environment for security misconfigurations, such as overly permissive IAM roles, publicly exposed storage buckets, or missing security controls. Instead of manually reviewing cloud configurations, I receive prioritized alerts that highlight the most critical risks in the management console, and this helps me focus on remediating issues that could have the greatest security impact. I reduce manual effort and improve our overall cloud security posture.

"SentinelOne Singularity Cloud Security has improved our organization's cloud security by giving us centralized visibility across cloud assets, workloads, identities, and configurations. It helps us detect misconfigurations, prioritize critical risks, and monitor threats in real time. As a result, I have reduced manual security reviews, fixed threats faster, and strengthened our overall cloud security posture. The unified platform also simplifies security operations by consolidating multiple cloud security capabilities into a single console, improving both efficiency and compliance.."

Verified user

Cyber Security Engineer at a outsourcing company with 51-200 employees

Read full review

“The best features of SentinelOne Singularity Cloud Security are its threat detection capabilities, real-time visibility across cloud environments, and automated response features. The ability to identify suspicious activity, quickly provide context around risk, and help security teams to investigate and remediate threats efficiently stand out the most. The centralized visibility and integrations with the broader security operations also make it easier to manage cloud security from a single platform.

“The integration with our broader security operations helped to streamline workflows by bringing cloud security insights into our existing security tools and processes. This integration reduces the need to manually correlate data from multiple sources, speeds up investigations, and gives our team better context when responding to alerts. This saves time during incident triage and helps security analysts prioritize and address threats more efficiently.

“SentinelOne Singularity Cloud Security has improved our organization's security visibility and response capability by giving our team better insights into cloud risk and suspicious activity. A major benefit has been faster threat investigations and response. Our security teams can quickly understand the context of alerts and take action. It has also helped reduce manual efforts, improve consistency in security operations, and strengthen our overall cloud security posture.

“Since using SentinelOne Singularity Cloud Security, we have seen improvements in how quickly our team can identify, investigate, and respond to potential threats. Better visibility and automated security insights have helped reduce manual investigation time and improve the efficiency of our response process. While we do not have specific metrics to share, the overall impact has been faster triage, better prioritization of risk, and a more proactive approach to cloud security.

“Its AI capability provides valuable support for governance and security by helping teams to identify risk, prioritize threats, and make faster security decisions. The AI-driven insights improve visibility across cloud environments and help to reduce the manual efforts required for monitoring and investigations.

“Overall, the AI capability is accurate and reliable. The AI-generated insights generally help to prioritize real risks, reduce alert fatigue, and provide useful

context for investigations..”

Verified user
Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Read full review

“The quality of the product in terms of reliability and what it offers is exceptional. It actually delivers on what it says it does. I think SentinelOne Singularity Cloud Security is a leader, and the product is built with an incredible amount of robustness. The protection that it's meant to offer is what we are actually getting.

“SentinelOne Singularity Cloud Security wins out because the partner that we have and the support that we get from the SentinelOne Singularity Cloud Security team in the country makes it quite seamless for me.

“I'm using SentinelOne Singularity Cloud Security, especially on the log aggregation side, as the point where logs from my other security products and tools are flowing in. I found that pulling logs into SentinelOne Singularity Cloud Security through the established integration methods that it supports was not very complex. We were able to achieve that with the team's help fairly quickly..”

Prince Joseph
Group Chief Information Officer at NeST Information Technologies Pvt Ltd

Read full review

“The best features of SentinelOne Singularity Cloud Security are its real-time threat detection, behavioral AI-based analytics, automated response capabilities, and comprehensive visibility across cloud workloads. The centralized management console makes it easier to investigate alerts, while the detailed telemetry helps speed up incident analysis and remediation. Overall, it provides good visibility with minimal operational work.

SentinelOne Singularity Cloud Security has improved our organization's overall security posture by providing better visibility into cloud workloads and faster threat detection. It has reduced the time needed to investigate security alerts, enabled quicker incident response, and helped our security team manage cloud risk more efficiently. Overall, it has increased confidence in the security of our cloud environment while reducing manual effort..”

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Read full review

"The best feature of SentinelOne is its lightweight agent. Unlike traditional antivirus products that require frequent signature updates, SentinelOne uses behavioral AI to detect threats. Because of this, it consumes very little bandwidth and has minimal impact on system performance.

Another feature I like is its automated response. When it detects malicious activity, it can automatically stop the process, quarantine the infected files, and isolate the affected endpoint. This helps contain threats quickly without requiring immediate manual intervention.

SentinelOne also provides excellent visibility through its unified dashboard. It is easy to monitor endpoints, investigate incidents, generate reports, and perform threat hunting from a single console. The dashboard is clean and user-friendly, making daily security operations much easier.

It also has strong coverage of the MITRE ATT&CK framework. For example, it can quickly detect and block suspicious activities such as PowerShell abuse and other common attack techniques used by attackers.

Finally, the platform supports compliance with frameworks such as ISO 27001, SOC 2, and NIST, making it easier to demonstrate security controls during audits.."

Harish (Kumar)
Cybersecurity And Information Governance Head at Aeren

Read full review

Pain Points

The main pain points mentioned:

✖ "I would like to see more customizable dashboards, deeper reporting capabilities, and broader integrations with third-party cloud management platforms in SentinelOne Singularity Cloud Security."

DeepPujara

Siem Engineer at a tech services company with 11-50 employees

✖ "SentinelOne Singularity Cloud Security is a strong platform, but there are a few areas where it could improve."

Verified user

Cyber Security Engineer at a outsourcing company with 51-200 employees

✖ "SentinelOne Singularity Cloud Security is a strong platform, but there are areas where it could be improved."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

✖ "The unified platform experience with SentinelOne Singularity Cloud Security is not fully realized yet."

Prince Joseph

Group Chief Information Officer at NeST Information Technologies Pvt Ltd

✖ "SentinelOne Singularity Cloud Security could be improved by providing more customizable reporting and dashboards, reducing false positives in certain scenarios, and offering deeper investigation with third-party security and IT management tools."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Room for improvement:

I would like to see more customizable dashboards, deeper reporting capabilities, and broader integrations with third-party cloud management platforms in SentinelOne Singularity Cloud Security. Additionally, regarding the event search feature, the power query is useful, but it has a learning curve for those new to the platform, which could be improved.

DeepPujara

Siem Engineer at a tech services company with 11-50 employees

Read full review

"SentinelOne Singularity Cloud Security is a strong platform, but there are a few areas where it could improve. I would like to see more customizable dashboards and reporting so different teams can focus on the metrics most relevant to them. The initial setup and policy tuning could also be simplified, especially for organizations with complex multi-cloud environments. Additionally, expanding integrations with third-party security and DevOps tools would make it even easier to fit into existing workflows.

"A few additional improvements would further enhance the platform. The user interface could be made more intuitive, especially for first-time users, by simplifying navigation and making key findings easier to locate. The documentation is comprehensive, but more step-by-step implementation guides, best practices, and real-world deployment examples would help administrators get up to speed more quickly. From a support perspective, faster response times for complex issues and a larger library of troubleshooting articles and knowledge base content would improve the overall customer experience.."

Verified user

Cyber Security Engineer at a outsourcing company with 51-200 employees

Read full review

"SentinelOne Singularity Cloud Security is a strong platform, but there are areas where it could be improved. Adding more flexible customization options for alerts, more advanced reporting and dashboards, and deeper integration with a wider range of cloud and security tools would make the platform even more valuable.

"While there is room for improvement in areas such as customization, reporting, and integration, it has been a reliable solution that has positively impacted our cloud security.."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Read full review

"There are some other features that probably could be done quite well for SentinelOne Singularity Cloud Security. Some of the features like the AI-SIM, for example, should be promoted more and should be enhanced a little bit more, so I don't have to worry about the SOC part of the operation being done by a third party. SentinelOne Singularity Cloud Security should be able to leverage this far more easily. Those are areas where SentinelOne Singularity Cloud Security can do better. They also have features where you're able to do a lot of log retention. If I'm getting the logs to be retained for a year and if the log aggregation is going to be working very effectively, then I think they should be able to build on this data that they're collecting and there should be a lot more security offerings and analytics that they should be able to do.

"The unified platform experience with SentinelOne Singularity Cloud Security is not fully realized yet. There are still other products that I have which are sitting in here. The moment this one and the architecting behind this can come forward and guide us, I think there are still some more steps we need to take before we can achieve the unified experience. It is consolidating, but it's not reached that level yet.

"At the moment on the MTTR side with SentinelOne Singularity Cloud Security, it can actually have an impact after I get to the next level of integration and consolidation. Right now, my team is having to work through multiple products before they can make decisions.."

Prince Joseph
Group Chief Information Officer at NeST Information Technologies Pvt Ltd

Read full review

"SentinelOne Singularity Cloud Security could be improved by providing more customizable reporting and dashboards, reducing false positives in certain scenarios, and offering deeper investigation with third-party security and IT management tools. More built-in guidance for alert investigation and remediation would also help teams resolve incidents more efficiently, especially those with smaller security teams.

Overall, SentinelOne Singularity Cloud Security is a strong security platform, but continued improvement in user experience, reporting flexibility, and integration capabilities would make it even more effective. Enhancing documentation, providing more advanced customization options, and adding more automation around routine security tasks would help organizations get more value from the platform.."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Read full review

“I don't know much about how the AI works inside SentainelOne Singularity Cloud Security. The behavioral AI is the core protection of the AI engine. It may be fast to block processes and quarantine files before any threat, but as a customer, I don't know how I am using the AI.

Purple AI is the optional add-on of the generative AI assistant, and we are not using that add-on much since it is optional.

We are not going deep normally with the Offensive Security Engine, because my security team looks for only threat notifications which we remediate manually. Most of the time, it resolves automatically.

We are not using the Secret Scanning feature much.

We are not managing cloud identities, nor are we enforcing least privilege with CIEM capabilities.

One negative is that the learning curve is steep. Security analysts need training to fully utilize SentinelOne Singularity Cloud Security as there are playbooks and other resources. Another issue is that premium features such as Purple AI, cloud security, or identity protection come with additional costs. Overall, the product is more expensive than traditional antivirus or other competitive products. Additionally, there are false positives due to behavior detection, which occasionally leads to high CPU or memory usage during telemetry collection or full system scans, especially on older systems such as some of our laptops with i5 10th generation processors and 8 GB RAM. It feels heavy on those devices. Licensing is also complex due to multiple products and add-ons, which complicates straightforward licensing..”

Harish (Kumar)
Cybersecurity And Information Governance Head at Aeren

Read full review

Pricing

"As a partner, we receive a discount on the licenses."

Andrea Alberti
Security Analyst at Intersistemi Italia s.p.a.

Read full review

"It's not cheap, but it is worth the price."

Satyavijay Chavan
Information Security Engineer at DataVigilant Infotech

Read full review

"SentinelOne Singularity Cloud Security is on the costlier side."

Abuzer Khan
Network engineer at ACC Ltd

Read full review

"The pricing tends to be high."

Shahnawaz-Alam
Sr Security Engineer at a computer software company with 5,001-10,000 employees

Read full review

"It is cost-effective compared to other solutions in the market."

MOHITH PULIVENDULA
Sr security engineer at Halodoc

Read full review

Check Point Infinity

Executive summary

Check Point Infinity offers unified security management, integrating with Active Directory for a streamlined experience. It centralizes network, endpoint, and cloud security, enhancing efficiency and visibility while employing AI-driven threat prevention.

Check Point Infinity simplifies operations with its unified console, providing seamless integration across enterprise environments. With ThreatCloud AI, real-time analytics, and automation, Infinity enables proactive threat prevention and policy enforcement, strengthening security and reducing manual workloads. However, performance issues, a steep learning curve, and complex setup are challenges users may face. Its interface demands a detailed onboarding process, and while centralization improves threat prevention and policy consistency, the platform has complex licensing and costly implementation, especially for large organizations.

What are the most notable features?

- Active Directory Integration: Seamless integration that enhances identity management.
- Centralized Management: Unified console that simplifies operations and improves visibility.
- ThreatCloud AI: Real-time analytics and AI-driven threat prevention.
- Automation: Reduces manual workload, improving response times and consistency.
- Unified Security: Integrates network, endpoint, and cloud environments.

What benefits and ROI should users evaluate?

- Improved Security Posture: Strengthens defense against cyber threats.
- Cost Savings: Reduces operational expenses in complex IT environments.
- Efficiency: Centralized management enhances operational efficiency.
- Consistency: Policy enforcement is streamlined across all environments.
- Enhanced Visibility: Unified console improves threat monitoring and detection.

In industries like finance, healthcare, and telecommunications, Check Point Infinity is implemented to protect critical infrastructure from advanced cyber threats. Organizations utilize its centralized dashboard for firewall management and comprehensive threat detection, ensuring compliance and data security.

Sample customers

Edel AG

Top comparisons

More comparisons

Securonix Next-Gen SIEM

Compared 8% of the time

Learn more

Cortex XDR by Palo Alto Networks

Compared 7% of the time

Learn more

Idira Privileged Access Manager

Compared 7% of the time

Learn more

Reviewers - Percentages by top Industries

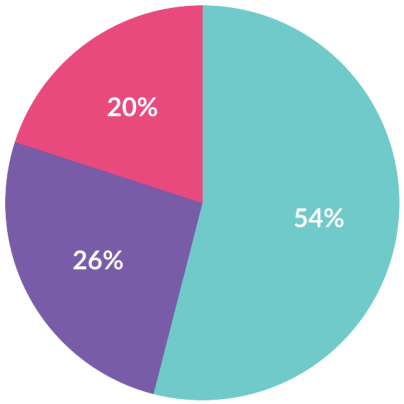
Security Firm	38%
Manufacturing Company	17%
Non Tech Company	13%
Financial Services Firm	8%

Visitors Reading Reviews - Percentages by Top Industries

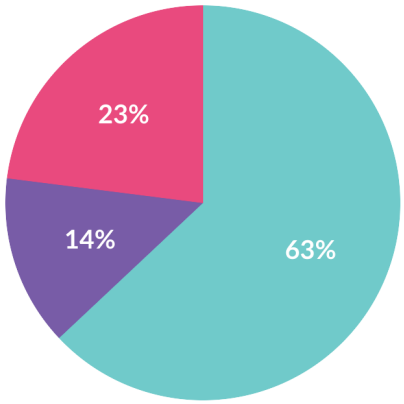
Security Firm	14%
Manufacturing Company	13%
Financial Services Firm	12%
Construction Company	9%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "The advanced threat prevention feature has significantly helped my organization; for example, Check Point Infinity flagged a suspicious file that had bypassed our email filters, and it turned out to be a zero-day malware—the threat prevention engine blocked it before it reached the user and gave us an alert instantly, saving us from a potential data breach."

Carol Berrocal

IT at a security firm with 51-200 employees

- "Since adopting Check Point Infinity, I have seen a noticeable improvement in how we manage and respond to security threats across our infrastructure."

Gerardo Rojas

Support at a security firm with 51-200 employees

- "Check Point Infinity has positively impacted the organization because it has allowed the consolidation of multiple security tools into one unified platform, which immediately reduced complexity and saved time for the team and IT department."

Alex Duarte

Security Support at a non-tech company with 201-500 employees

"Check Point Infinity has positively impacted my organization by streamlining security prevention and strengthening our overall posture."

Ruben Ruiz

Sr. VP of Creative & Development at a non-tech company with 51-200 employees

"Check Point Infinity has had a positive impact by providing a unified security framework that reduced complexity and improved visibility across all layers."

Minor Corrales

Networking Admin at a tech company with 51-200 employees

What users had to say about valuable features:

"The best features Check Point Infinity offers include advanced threat prevention, which I use with AI and driver-based threat intelligence to block zero-day attacks, phishing, ransomware, and other sophisticated threats before they cause damage.

The advanced threat prevention feature has significantly helped my organization. For example, Check Point Infinity flagged a suspicious file that had bypassed our email filters, and it turned out to be a zero-day malware. The threat prevention engine blocked it before it reached the user and gave us an alert instantly, saving us from a potential data breach.

Check Point Infinity has positively impacted my organization by improving our overall security posture and reducing manual workload. Specifically, it has reduced my manual workload by saving several hours a week. Before using Infinity, we spent hours manually investigating alerts and updating threat signatures, but now automatic threat detection and response help reduce false positives, allowing us to spend less time on non-issues.."

Carol Berrocal
IT at a security firm with 51-200 employees

Read full review

"The best features that Check Point Infinity offers include an intuitive interface that is accessible from anywhere, with the Azure Infinity portal hosting multiple security solutions under one roof.

Since adopting Check Point Infinity, I have seen a noticeable improvement in how we manage and respond to security threats across our infrastructure.

I have observed saved time by the support department.."

Gerardo Rojas
Support at a security firm with 51-200 employees

Read full review

"The automation and orchestration that Check Point Infinity brings to ease of response is invaluable. Instead of teams manually chasing down alerts across different systems, Check Point Infinity can automatically correlate events and apply prevention measures across endpoints, network, clouds, and applications at the same time.

Check Point Infinity has positively impacted the organization because it has allowed the consolidation of multiple security tools into one unified platform, which immediately reduced complexity and saved time for the team and IT department.

The team has definitely noticed a significant difference since switching to Check Point Infinity. Incident response is much faster because alerts are consolidated in one console.."

Alex Duarte
Security Support at a non-tech company with 201-500 employees

Read full review

“One of the best features for me is unified threat prevention and centralized management.

Unified threat prevention and centralized management have helped my team day-to-day by reducing the time spent switching between different tools and dashboards. For example, when I had to investigate suspicious traffic across endpoints, gateways, or events in the VPN, everything was visible in one place. We could quickly trace the issue and apply consistent policies without delays.

Check Point Infinity has positively impacted my organization by streamlining security prevention and strengthening our overall posture. With everything managed under one platform, I've noticed clear improvements in efficiency since my team no longer has to juggle multiple tools or dashboards. I've also seen cost savings by consolidating licensing and reducing the need for separate solutions. By consolidating multiple tools into one platform, my team saves several hours each week that used to be spent switching between dashboards and managing separate policies. The unified platform has also reduced troubleshooting time during incidents..”

Ruben Ruiz

Sr. VP of Creative & Development at a non-tech company with 51-200 employees

Read full review

"Check Point Infinity offers a unifying architecture, shared threat intelligence, and consistent policies enforced across network and cloud. The way it consolidates everything under one framework stands out most.

The shared threat intelligence in Check Point Infinity has helped the organization by automatically blocking threats that appear across different layers of the environment. A phishing attempt was first detected at the email gateway, and the same intelligence was instantly applied to endpoints and firewall. The attack was stopped everywhere at once. That kind of integration has improved the security posture by reducing response time and ensuring consistency.

Check Point Infinity has had a positive impact by providing a unified security framework that reduced complexity and improved visibility across all layers. A single dashboard now provides visibility to see threats across network, cloud, and endpoints in real-time. Previously, three different tools had to be checked, which often delayed response.."

Minor Corrales

Networking Admin at a tech company with 51-200 employees

Read full review

"The best feature Check Point Infinity offers for me is threat prevention, which is effective at blocking malware, ransomware, and phishing, as well as preventing zero-day attacks before they reach users or systems.

For our team, the threat prevention in Check Point Infinity works by layering multiple defenses that stop attacks before they reach users or systems, and the most effective feature for us is the specific SandBlast Zero-Day Prevention, which uses advanced sandboxing and threat emulation to detonate suspicious files in a safe environment.

Check Point Infinity has impacted my organization positively, as I have seen a reduction in security incidents and response times, with threats that used to slip through different point solutions now being blocked automatically thanks to the unified prevention layers.."

Roy Lopez
TI at a security firm with 51-200 employees

Read full review

Pain Points

The main pain points mentioned:

✖ "One area for improvement in Check Point Infinity is the user interface, as it can feel complex for new users."

Carol Berrocal

IT at a security firm with 51-200 employees

✖ "One area where Check Point Infinity could improve is in the reporting and analytics customization."

Gerardo Rojas

Support at a security firm with 51-200 employees

✖ "One area where Check Point Infinity could be improved is its user interface. It brings together a lot of powerful features, but sometimes the console feels overwhelming and requires extra time to navigate."

Alex Duarte

Security Support at a non-tech company with 201-500 employees

✖ "The addition of languages for the support could improve Check Point Infinity."

Ruben Ruiz

Sr. VP of Creative & Development at a non-tech company with 51-200 employees

✖ "Another improvement that would make our experience smoother with Check Point Infinity is simplifying the initial setup and configuration process; while powerful, it can feel overwhelming for smaller teams without dedicated security engineers, so more guides, wizards, or automatic best practice templates would be helpful."

Roy Lopez

TI at a security firm with 51-200 employees

Room for improvement:

"One area for improvement in Check Point Infinity is the user interface, as it can feel complex for new users. Streamlining navigation and making threat reports more intuitive would be beneficial.."

Carol Berrocal

IT at a security firm with 51-200 employees

Read full review

"One area where Check Point Infinity could improve is in the reporting and analytics customization.

I would definitely expand the reporting and analytics side, as while Check Point Infinity does a solid job of aggregating logs and presenting threat data, the customization options for dashboards and reports could be more flexible.."

Gerardo Rojas
Support at a security firm with 51-200 employees

Read full review

"One area where Check Point Infinity could be improved is its user interface. It brings together a lot of powerful features, but sometimes the console feels overwhelming and requires extra time to navigate.

The documentation of Check Point Infinity is not always intuitive.

Integration with third-party tools is an area that could make Check Point Infinity even stronger.."

Alex Duarte
Security Support at a non-tech company with 201-500 employees

Read full review

"The addition of languages for the support could improve Check Point Infinity. Support is currently only available in English. I suggest adding additional language support.."

Ruben Ruiz
Sr. VP of Creative & Development at a non-tech company with 51-200 employees

Read full review

"I think Check Point Infinity needs to improve the documentation for deploying it the first time, making it more intuitive and providing better facilities for searching different investigations or deployments about this product.

Another improvement that would make our experience smoother with Check Point Infinity is simplifying the initial setup and configuration process; while powerful, it can feel overwhelming for smaller teams without dedicated security engineers, so more guides, wizards, or automatic best practice templates would be helpful.."

Roy Lopez
TI at a security firm with 51-200 employees

Read full review

"I think Check Point Infinity could be improved in terms of documentation. I need more images and pictures, and the steps should be more intuitive.

"Another improvement I would like to see in Check Point Infinity is a more streamlined onboarding process for new administrators since the initial setup can feel complex. Better documentation and guided tutorials would make adoption faster and easier.."

Cristopher Z

Administrador De Redes at a financial services firm with 501-1,000 employees

Read full review

Pricing

"The solution's price is quite high, and the licensing model requires extra licenses for various features like SD-WAN."

Martin Ellmann
Chief Executive Officer at EE Solutions GmbH

Read full review

"When it comes to price, the paramount consideration is the strength of the security. If the security measures provided by the product, such as Check Point Infinity, are robust and meet our requirements, price becomes a secondary concern."

Babu Kp
Technical Support at Hitachi Systems, Ltd.

Read full review

"The flexibility in pricing is advantageous, and being a special partner allows for negotiating special rates based on the project requirements."

Nuno Faria
Managing Partner at NCSO

Read full review

"I rate the product's price a six on a scale of one to ten, where one is cheap, and ten is expensive."

Hendrik-Du Plooy
Regional Manager at Saber1

Read full review

"The product has good pricing considering the features and a global approach."

MONICA HERRRA
Systems Engineer at PGE

Read full review

SentinelOne Singularity AI SIEM

Executive summary

SentinelOne Singularity AI SIEM offers comprehensive security information and incident management designed to enhance threat detection, response, and investigation capabilities within enterprise environments.

SentinelOne Singularity AI SIEM is known for its robust capabilities in the realm of cybersecurity, providing organizations with an advanced tool to combat modern threats. The platform integrates machine learning and artificial intelligence to automate threat identification and streamline incident response processes. Its intuitive interface allows teams to manage security events efficiently, ensuring rapid reaction to potential vulnerabilities. As a scalable tool, it adapts to evolving security demands, providing valuable insights to safeguard critical business operations.

What are the important features of SentinelOne Singularity AI SIEM?

- Automated Threat Detection: Uses AI to identify threats with minimal human intervention.
- Comprehensive Data Analysis: Capable of processing extensive security-related data for informed decision-making.
- Real-time Monitoring: Continuously tracks events for immediate alerts on suspicious activities.
- Scalability: Adapts to the changing needs of enterprises, maintaining effectiveness at any scale.
- Seamless Integration: Easily connects with existing security infrastructure to enhance overall protection.

What are the key benefits or ROI from SentinelOne Singularity AI SIEM?

Improved Security Posture: Enhances the ability to detect and respond to complex threats, minimizing risks.
Operational Efficiency: Automates routine processes, allowing security teams to focus on strategic tasks.
Cost-effectiveness: Reduces the need for extensive manual analysis, cutting down operational costs.
Business Continuity: Protects critical operations from disruptions, ensuring uninterrupted service delivery.

Scalability and Flexibility: Ensures ongoing adaptability to growing and dynamic security demands.

In industries such as finance and healthcare, implementation of SentinelOne Singularity AI SIEM often means tailored solutions to protect sensitive data, meeting regulatory compliance. These sectors appreciate its capability to provide detailed insights and reduce the risk of data breaches, thus preserving stakeholder trust.

Top comparisons

More comparisons

Microsoft Sentinel	Fortinet FortiSIEM	Huntress Managed SIEM
Compared 23% of the time	Compared 17% of the time	Compared 6% of the time
Learn more	Learn more	Learn more

Reviewers - Percentages by top Industries

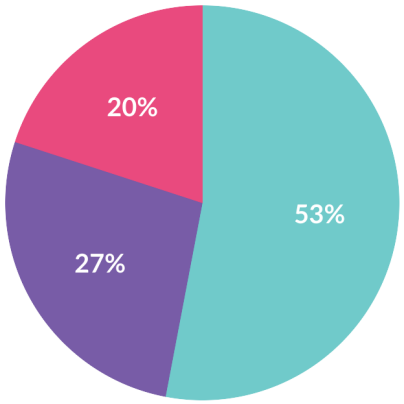
Outsourcing Company	40%
Comms Service Provider	10%
Manufacturing Company	10%
Media Company	10%

Visitors Reading Reviews - Percentages by Top Industries

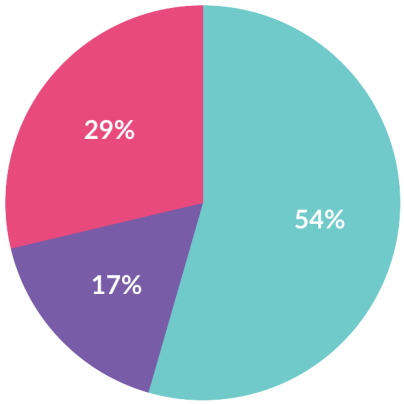
Outsourcing Company	22%
Construction Company	7%
Manufacturing Company	6%
Media Company	6%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "SentinelOne Singularity AI SIEM has improved our overall security posture and is reducing the workload on the SOC team."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

- "SentinelOne Singularity AI SIEM has impacted my organization positively because I am observing some improvement, including real-time monitoring and real-time threat detection that help secure both our and the client's organization from anything suspicious or any malicious types of alerts."

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

- "SentinelOne Singularity AI SIEM has positively impacted my organization by improving visibility, reducing investigation time, and helping the security team respond to incidents faster."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

"I have experienced no issues with SentinelOne Singularity AI SIEM; it is the best product I have ever used, very stable, handy, easy to manage, and excellent with its AI-driven capabilities."

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

"The best features of SentinelOne Singularity AI SIEM include its user-friendly interface, ease of deployment, and ease of use, and it is also easy to control the devices, as we block USB on all machines, export the configuration of machines, and have very good visibility of the instance with excellent reports."

Ayman Said

Infrastructure System's Manager at ICAPP (Americana Group)

What users had to say about valuable features:

“The best features of SentinelOne Singularity AI SIEM are AI-powered threat detections, unified security data, Purple AI assistant, automated investigations, hyper-automations, and fast threat hunting. These features include centralized log management, Purple AI for natural log investigations, automated alert correlations, and hyper-automations for incident response. These features help security teams detect threats faster, reduce manual effort, minimize false positives, and significantly improve mean time to detect and mean time to respond.

“These features significantly improved our SOC workflow. Previously, analysts had to manually collect logs from multiple tools and correlate alerts, which was time-consuming. With SentinelOne Singularity AI SIEM, alerts were automatically correlated into a single incident with an attack timeline, making investigations much faster. Purple AI helped summarize the incident and answer natural language queries, reducing the time spent searching through logs.

“SentinelOne Singularity AI SIEM has improved our overall security posture and is reducing the workload on the SOC team. Its AI-driven detection and automated response capabilities help us identify threats faster, reduce false positives, and shorten incident response times. The centralized visibility across endpoints and cloud environments also made investigations more efficient, while automation reduced repetitive manual tasks.

“It has improved SOC efficiency by reducing time analysts spend on manual alert investigations and response. Previously, analysts had to collect information from multiple sources and manually correlate events. With SentinelOne Singularity AI SIEM's AI-driven alert prioritization, automated incident correlations, and investigation timelines provide better context quickly. The team can identify the root cause faster, reduce alert fatigue, and take response actions such as isolating affected endpoints more efficiently..”

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Read full review

"SentinelOne Singularity AI SIEM offers the best features that belong to the AI. This includes automated alerts. We can also do the automated alerts on these fields. I can create multiple types of use cases. It means we will create multiple types of use cases for our requirements. For example, if we have blocked any suspicious or malicious app in the environment, we can block these. That is a best feature, and Purple AI is also a best feature in SentinelOne Singularity AI SIEM tools. Deep Visibility is also a best feature because we can check multiple types of activity, such as what it is doing, what activities it is currently performing, and what the steps are. There are multiple types of best features in there.

"I will give an example of how Deep Visibility has helped me in my investigations or daily work. If any suspicious or malicious malware types of alerts are triggered in SentinelOne Singularity AI SIEM, then I will check the source of this with the help of Deep Visibility. Deep Visibility is basically for when any alerts are triggered on any endpoint. You can see what types of activity are being done, what is being downloaded, and what types of history there are. You can check the source, the destination, and what systems are doing this activity. I will check that type of feature in Deep Visibility.

"SentinelOne Singularity AI SIEM has impacted my organization positively because I am observing some improvement. There are multiple tool alerts in our organization, but SentinelOne Singularity AI SIEM feature is real-time monitoring and real-time threat detection. With the help of our and the client's organization, it is secure. There are improvements. Those types of improvements are better for securing our organization from anything suspicious or any malicious types of alerts.

"There are faster response times available with SentinelOne Singularity AI SIEM. Also, there is the automation alert. We can set any parameter on SentinelOne Singularity AI SIEM source, and it will automatically raise an alert to the client side. We can also integrate that type of feature with SentinelOne Singularity AI SIEM. With the help of alert raising, there is the fastest way to raise an alert. That is the best feature and there is a very big improvement.."

Dev Reshwal
Technical Support Executive at Softcell Technologies Limited

Read full review

"The best features SentinelOne Singularity AI SIEM offers include centralized log management, AI-powered threat detection, Purple AI, AI Security Assistant, unified investigation timeline, and threat hunting. Hyper automation, fast search and investigation, cloud, and identity visibility are also standout features.

Out of those features, the centralized console is the one I find myself using the most, and it has made a big difference in my daily work.

SentinelOne Singularity AI SIEM has positively impacted my organization by improving visibility, reducing investigation time, and helping the security team respond to incidents faster.."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Read full review

"The best feature is that it collects and correlates logs, which is very helpful. We also use it for AI-powered investigations. The platform provides unified visibility, AI-driven alert correlations, threat hunting, automated response, and AI-driven data pipelines. These are the features I found most valuable.

"We have been using the AI-driven alert correlation feature extensively. Without AI-driven alert correlation, an employee clicking on a phishing email could exploit our entire organization. The AI automatically recognizes that all of these events are connected because they involve the same user, endpoint, and timeframe. We use it when somebody receives a phishing email or clicks a link, credentials are used from an unusual location, PowerShell is launched, connections are made to a malicious server, and persistence attempts occur. The correlation feature helps us identify and correlate these attacks, determine where the attack started, and find the threat so we can fix it.

"The platform brings together AI, automation, and unified visibility in a way that helps security teams work more efficiently. Rather than switching between multiple tools and manually correlating alerts, analysts can investigate incidents from a single console with AI-assisted context. Features such as automated alert correlation, threat hunting, and response workflows help reduce investigation time and improve overall SOC productivity.

"One of the biggest positive impacts has been improved operational efficiency for the security team. By centralizing telemetries from multiple sources and using AI to correlate related alerts, we have reduced the time spent on manual investigation. Analysts can focus on higher priority incidents. We have also noticed faster incident detection and response, better visibility across endpoints, cloud, and identity environments, as well as improved collaboration because everyone works from the same incident view.."

Vanshika
Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

Read full review

"With the help of this tool, the response time to sophisticated threats has improved significantly, and it recently cuts the MTTR time using Purple AI by 40%.

"SentinelOne Singularity AI SIEM allows us to use natural language; we do not need knowledge of scripting or querying languages to correlate threats. We can search in normal, plain, simple English. For example, if I want to check the detections regarding a particular threat in a particular attack surface, I only need to provide it in plain, simple English, and Purple AI will generate a query and summarize the results for that. It has made my job much easier, both for myself and for the SOC teams. With minimal effort, we can get the queries asked by the auditors or forensics teams.

"AI analytics reduces the manual tasks and helps us prioritize critical and immediate threats that need to be addressed. The analytical part mainly provides clarity on what we should focus on, which threats to investigate, or if we need to report it or whitelist false positives. These kinds of tasks are largely automated and taken care of.

"Knowing which threat we need to look at first based on its criticality makes it easier for us to address it. Getting to the problem is one thing, and with Purple AI, we are able to get answers without using complex queries; we just search for what we are looking for, and it generates the corresponding steps right in the console, which helps us respond to critical threats on an immediate basis.

"After implementing SentinelOne Singularity AI SIEM, we can see that we have visibility over all the applications on our endpoints, and it helps us identify which of those applications are more vulnerable or critical, whether high or medium. These kinds of visibilities are available, allowing us to proactively protect the endpoint and our infrastructure.."

GANESAN K
Senior Technical Engineer at Safezone Secure Solutions Private Limited

Read full review

"The AI features of SentinelOne Singularity AI SIEM are absolutely perfect. There are not any issues because there is a game that you play with SentinelOne. This game allows me to drive a proof of concept for customers. When I play the game, SentinelOne provides a tool called Purple AI, which allows for simple queries just like ChatGPT. This means you do not need an expert to understand what is happening around your endpoints and identify threats. I can simply write, 'What happened to my Windows endpoint in the last seventy-two hours?' and it provides all reports and logs. This functionality makes it accessible even for CEOs and decision-makers to understand their environment better, making it an excellent feature for SOC, giving visibility and clarity.."

Emmanuel-Bentil
Managing Director at iMark Consult

Read full review

Pain Points

The main pain points mentioned:

✖ "SentinelOne Singularity AI SIEM is a strong platform, but there are a few areas where it could be improved."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

✖ "SentinelOne Singularity AI SIEM is the best, but sometimes the dashboards are a little simple compared to other tools."

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

✖ "While it provides many built-in decorations and dashboards, creating highly customized decoration rules and reports can sometimes require additional efforts."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

✖ "The AI-generated investigations can occasionally require manual validation for complex incidents."

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

✖ "SentinelOne Singularity AI SIEM can improve in the area of XDR, especially in the integration between SentinelOne and other solutions and components in the network, as it was not working well with the Fortinet firewall."

Ayman Said

Infrastructure System's Manager at ICAPP (Americana Group)

Room for improvement:

"SentinelOne Singularity AI SIEM is a strong platform, but there are a few areas where it could be improved. First, the initial setup and integration with some third-party tools could be simpler. Second, more customizable dashboards and reporting would help the management team confirm their needs.."

Verified user

Cybersecurity Postsales Engineer at a outsourcing company with 51-200 employees

Read full review

"SentinelOne Singularity AI SIEM is the best, but sometimes the dashboards are a little simple compared to other tools. The custom dashboard is not available in their features. Therefore, I would suggest adding the custom dashboard for any of our requirements.

"The AI-driven analytics from SentinelOne Singularity AI SIEM has not affected our ability to reduce false positives.

"SentinelOne Singularity AI SIEM has affected my SOC's efficiency in investigating alerts and responding to incidents. If we receive any alerts, we can observe what activity is being done. We can see if it is malicious or something suspicious, or a true positive. We can analyze the path, the hash, and whether the signature is verified or not. We can see if it is an alert triggered by any engine. We can see the source of this. We will do that type of analysis and raise it to the client side. Also, if I identify anything suspicious or malicious in the alert, I will forcefully kill and quarantine it immediately.."

Dev Reshwal
Technical Support Executive at Softcell Technologies Limited

Read full review

"Overall, SentinelOne Singularity AI SIEM is a strong platform, but there are a few areas where it could be improved. One area is customization. While it provides many built-in decorations and dashboards, creating highly customized decoration rules and reports can sometimes require additional efforts. Another area is third-party integrations. Although it integrates with many security products, expanding native integration and simplifying onboarding for less common vendors would make deployment easier.

From a usability perspective, I think the platform could make advanced investigation more intuitive. New analysts can face a learning curve when building complex searches, custom detection rules, or dashboards. Improving the user experience with more guided workflow templates and contextual recommendations would help teams become productive more quickly.."

Verified user

Desktop Support Engineer at a outsourcing company with 51-200 employees

Read full review

"Overall, SentinelOne Singularity AI SIEM is a very strong platform, but there are a few areas where I would like to see improvements. The AI-generated investigations can occasionally require manual validation for complex incidents. Increasing the precision and explainability of AI recommendations would be valuable. I would also appreciate even broader out-of-the-box integrations with third-party security tools and more pre-built detections and response playbooks. Additionally, making dashboards and reporting even more customizable would help organizations tailor the platform to different teams and executive reporting needs.

"SentinelOne Singularity AI SIEM is a very strong platform, so I do not have much to suggest for improvement. Those are the main areas I would highlight. Overall, the platform is quite mature, and the improvements I would like to see are more about enhancing usability than addressing major shortcomings. Continued investigation into AI accuracy and explainability, additional native integrations with third-party tools, richer pre-built automation playbooks, and more flexible dashboards and reporting would be beneficial.."

Vanshika
Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

Read full review

"SentinelOne Singularity AI SIEM can improve in the area of XDR, especially in the integration between SentinelOne and other solutions and components in the network, as it was not working well with the Fortinet firewall. The API and the integration between each other is not working well at this time, and they are promising to work on this area, but they have not done that effectively.."

Ayman Said
Infrastructure System's Manager at ICAPP (Americana Group)

Read full review

"They could expand more integrations for other third-party products that are not currently available. Those are areas they can improve or have yet to improve.

"For example, we have firewall integrations, so if we integrate our firewalls, we will be able to have a log view of the traffic. If traffic is coming from the firewall, we can see from which side a particular threat is coming. Currently, they support only FortiNet, Cisco, and Palo Alto. However, many of our clients use SonicWall firewalls, which are not in SentinelOne Singularity AI SIEM marketplace. They could add SonicWall because it is also a global product that needs to be included.

"SentinelOne Singularity AI SIEM is pretty good compared to Charlotte AI from CrowdStrike. However, if it could provide more information on IOA, that would be beneficial. While SentinelOne Singularity AI SIEM does provide those details, leveraging that information to proactively check our systems for vulnerabilities would be better. In Charlotte AI, those functionalities are available. Therefore, the prompt can be improved, and provide more information on the attackers and attacks we are facing. Indicators of compromise are one thing, but IOA is another critical aspect that needs to be taken care of to help organizations proactively improve their cyber defenses against evolving attacks, as many attacks are happening globally. The same attacks may come to India or target our organization as well; thus improving on the IOA part would be beneficial.."

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

Read full review

Darktrace

Executive summary

Darktrace revolutionizes network security with AI-driven alerts, anomaly detection, and robust visibility across networks. It autonomously detects threats, minimizing the need for human oversight, and offers efficient IP identification with minimal false positives.

Darktrace uses advanced AI analytics to enhance network protection. Its powerful real-time threat response capabilities and self-learning enable thorough monitoring and insightful analysis of network activities. While providing scalable and reliable security, users seek improvements in false positive reduction, user-friendly interfaces, and pricing. Enhanced third-party integration, more effective dashboards, and centralized automation features remain top priorities. Users benefit greatly from its Antigena feature, offering automated responses like blocking suspicious connections for robust network defense.

What Are Darktrace's Key Features?

- AI-Driven Alerts: Provides real-time alerts for threat detection.
- Anomaly Detection: Identifies unusual network activities with precision.
- Real-Time Threat Response: Autonomously counteracts potential threats.
- Comprehensive Monitoring: Offers detailed network activity insights.
- Scalability: Adapts to expanding network environments effectively.

Which Benefits Should Users Consider in Reviews?

- Stability: Reliable performance ensures constant protection.
- Efficient Cloud Protection: Safeguards data across cloud infrastructures.
- Intuitive Interface: Facilitates easy navigation and efficient operations.
- Network Visibility: Enhances understanding of network traffic and activities.
- Automated Threat Blocking: Quick response to potential network breaches.

In industries employing Darktrace, it is pivotal in securing LAN networks, analyzing behavioral patterns, and detecting internal and external threats. Adoption alongside platforms like F5 and SAP enhances incident response, traffic analysis, and threat identification, utilizing Antigena for proactive security measures.

Sample customers

Irwin Mitchell, Open Energi, Wellcome Trust, FirstGroup plc, Virgin Trains, Drax, QUI! Group, DNK, CreaCard, Macrosynergy, Sisley, William Hill plc, Toyota Canada, Royal

British Legion, Vitol, Allianz, KKR, AIRBUS, dpd, Billabong, Mclaren Group.

Top comparisons

More comparisons

Vectra AI

Compared 4% of the time

Learn more

CrowdStrike Falcon

Compared 3% of the time

Learn more

SentinelOne Singularity Endpoint

Compared 2% of the time

Learn more

Reviewers - Percentages by top Industries

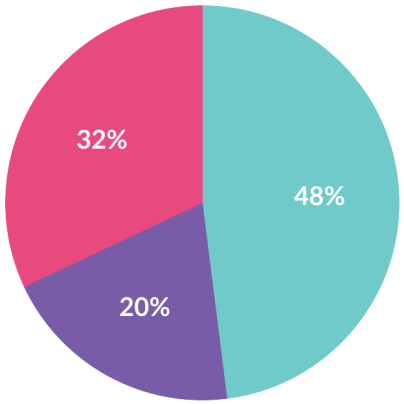
Financial Services Firm	19%
Computer Software Company	12%
Healthcare Company	7%
Manufacturing Company	7%

Visitors Reading Reviews - Percentages by Top Industries

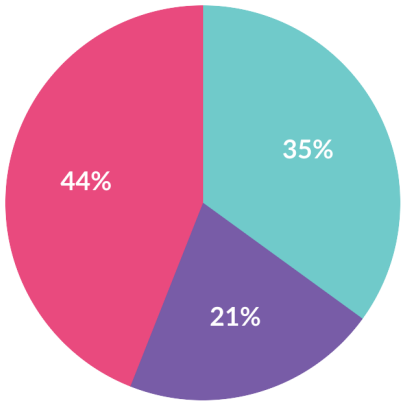
Manufacturing Company	10%
Financial Services Firm	9%
Computer Software Company	8%
Comms Service Provider	7%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- “Darktrace impacts my organization positively by providing us with a better understanding of abnormal activities detected among users.”

Pasan Jayarathna

Network Security Engineer at Cyberwell Solution

- “Regarding the autonomous response feature, I appreciate how it functions within the platform.”

Tejas Jain

Principle Cloud Architect at a tech services company with 11-50 employees

- “I can rate Darktrace's technical support as one of the best products in the world.”

Anil M

Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

"The most beneficial feature in Darktrace is identifying phishing emails with the help of the AI engine and machine learning."

Waleed Omar

Information Security Specialist at Arab Open University

"The technical support from Darktrace is very good, including support from their resellers."

Malebo Lethoba Group

Security Analyst at a healthcare company with 10,001+ employees

What users had to say about valuable features:

"In my understanding, the best feature Darktrace offers is the identification of copying files, which acts as a DLP, and it is a main concern for companies because users sometimes copy data outside without knowing, especially those without a technical background.

When I mention the DLP-like feature and file copying detection, the alerts have been very timely, as we get an alert within a couple of minutes, which is excellent. Even if some developers are working after hours and copying files, our SOC team detects this, and most of the time they call us so we can identify the users. The alerts are quite accurate and proactive.."

Pasan Jayarathna

Network Security Engineer at Cyberwell Solution

Read full review

"The features I find most effective in Darktrace include anomaly detection. The machine learning model provides accurate alerts after the learning period of 1 or 2 weeks, especially for network anomalies or something that the user is trying to access, which can include trying to visit unknown sites or botnets, and those things get detected and represented in a very good dashboard.

"Darktrace positively impacts my organization by enhancing threat hunting, particularly in east-west traffic within the same subnet. Previously, we only used traditional firewalls that cannot catch this lateral traffic. After deploying Darktrace, we gain insights into machine-to-machine communication, which adds more value to the organization and is especially beneficial for the SOC team.."

Anil M

Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

Read full review

The most beneficial feature in Darktrace is identifying phishing emails with the help of the AI engine and machine learning. In case it does not identify something, we can automatically make Darktrace learn from selections and other functionalities.

Regarding the ROI, we have experienced a significant reduction in phishing emails and have utilized our time efficiently, resulting in approximately 70% ROI. ."

Waleed Omar

Information Security Specialist at Arab Open University

Read full review

The functions I find most valuable in Darktrace are the AI analyst as well as the detection.The autonomous response capabilities of Darktrace are not crucial for me because it doesn't work in a network where there are no core switches. In a modern network, the autonomous response doesn't work, especially when sitting in a shared data center.If I'm running a traditional network where I am not in a shared data center with a layer two dedicated for my resources, then it can work for me. However, if I am in a data center where I don't have layer two, it becomes an issue because the autonomous response is reliant on sending spoofed TCP resets to my core switch to block traffic, which is a major issue.

Malebo Lethoba Group
Security Analyst at a healthcare company with 10,001+ employees

Read full review

The AI analysis and AI investigation features are incredibly effective. I do not need to manually process incidents as Darktrace provides an incident summary, potential detection paths, and other details, all exportable with just a click. The tool is very powerful and saves a lot of time. The autonomous response technology eliminates the need for human intervention by automatically handling incidents even during off hours.

Verified user
Security Information & Incident Analyst at a financial services firm with 1,001-5,000 employees

Read full review

The autonomous mode, which is the Antigena AI response, is particularly valuable. It is capable of responding to lateral movement and ransomware deployment within environments where there is data exfiltration. For example, if more than 2.5 gigabytes of data have been pulled in a few minutes, it engages by blocking for one-hour intervals, alerts, and extends the block until it goes into full isolation if the violation continues.

ChristopherMangava
Group Cybersecurity Administrator at Tharisa

Read full review

Pain Points

The main pain points mentioned:

✖ "As of now, I feel Darktrace can be improved to better detect end device activities, such as laptops or desktops, to bind it with our network."

Pasan Jayarathna

Network Security Engineer at Cyberwell Solution

✖ "If asked to rate Darktrace support on a scale from zero to ten where ten is the best, I would give them five points."

Tejas Jain

Principle Cloud Architect at a tech services company with 11-50 employees

✖ "Pricing bothers me and this is one of the major factors when choosing a solution."

Anil M

Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

✖ “I feel that Darktrace could be improved, particularly in the support aspect which is currently very poor. We need to chase Darktrace instead of them being proactive with us.”

Waleed Omar

Information Security Specialist at Arab Open University

✖ “In a shared environment, it doesn't work, and there are still some integration issues.”

Malebo Lethoba Group

Security Analyst at a healthcare company with 10,001+ employees

Room for improvement:

“In terms of improvement for Darktrace, pricing is the main concern. Pricing bothers me and this is one of the major factors when choosing a solution. When we get feedback from customers, that's the only felt need. When we factor in Darktrace, we do it only limited. We put it on where the perimeters and connections are, but still, some gray areas are left out, especially if we have multiple branches. We need Darktrace on each branch to get the data out, and I suggest having some kind of a centralized product that gets data from multiple sources to aggregate and provide the data..”

Anil M

Technical Consultant - Unix Platform Services at BITS AND BYTE IT CONSULTING PVT LTD

Read full review

I feel that Darktrace could be improved, particularly in the support aspect which is currently very poor. We need to chase Darktrace instead of them being proactive with us.

The support is the main problem, though there are some other issues as. .”

Waleed Omar
Information Security Specialist at Arab Open University

Read full review

I am uncertain what would make Darktrace better because of the autonomous response issue. In a shared environment, it doesn't work, and there are still some integration issues. They say they can integrate with most firewalls, but when we did an integration with Meraki MX firewalls, that integration didn't work and still doesn't work to this day.

Malebo Lethoba Group
Security Analyst at a healthcare company with 10,001+ employees

Read full review

Updates keep coming, which is great, but I prefer a unified UI experience. The intelligence section and the incident view should be seamlessly connected in one view to avoid jumping between pages. This integration would make incident management more intuitive.

Verified user
Security Information & Incident Analyst at a financial services firm with 1,001-5,000 employees

Read full review

I have observed a product called LinkShadow, which has more modules of integration and consolidates everything into one dashboard, such as authentication monitoring. Darktrace could improve by integrating with email security gateways like Mimecast or Ironscales. In LinkShadow, this is referred to as mesh technology. Additionally, the Darktrace dashboards are not easy to navigate until one becomes familiar with them.

ChristopherMangava
Group Cybersecurity Administrator at Tharisa

Read full review

“The presence of sales representatives in my country needs improvement. There is no dedicated salesperson in Egypt, and having one would help to improve focus on this market..”

Mohamed Eletreby
Solution Architect at a tech services company with 51-200 employees

Read full review

Pricing

"The pricing is quite high, estimated at around $350,000 per year."

Peter-Murphy
Head of Technology Operations at Pobl Group

Read full review

"The product is expensive."

Sammy Mukuna
Network Admin at Naivas Ltd

Read full review

"Darktrace is quite an expensive solution."

Themis Papaioannou
Co-Founder & Managing Director at CyberOne S.A.

Read full review

"The tool's pricing is costly."

Irwin Gibson
Chief ICT Officer at Barbados Public Workers Cooperative Credit Union Ltd

Read full review

"The pricing is reasonable."

Summa Lai
IT Manager at Calgary United Way

Read full review

Data Hub

Executive summary

Data Hub is an advanced platform designed to streamline data management processes, enhance data accessibility, and provide comprehensive analytics capabilities for informed decision-making.

Data Hub offers a unified approach to handling large-scale datasets, empowering organizations to effectively manage, analyze, and extract insights from their data infrastructure. It provides robust features for data integration, storage, and visualization, supporting diverse business needs and driving data-driven strategies.

What are the key features of Data Hub?

- Data Integration: Seamlessly combines data from multiple sources for cohesive analysis.
- Scalability: Supports growing data needs without performance degradation.
- Analytics Tools: Enables advanced data processing and insightful reporting.
- Security: Robust security protocols to ensure data compliance and protection.
- Custom Dashboards: Offers customizable interfaces for tailored analytics displays.

What benefits do users experience with Data Hub?

- Increased Efficiency: Streamlines data processes, reducing time and resource spent.
- Cost-Effectiveness: Minimizes need for multiple data management tools.
- Improved Decision Making: Provides actionable insights through data analytics.
- Enhanced Collaboration: Facilitates data sharing across departments, encouraging teamwork.

Data Hub is implemented across industries such as finance, healthcare, and retail, providing tailored solutions that meet specific demands in areas like customer data analysis, patient record management, and inventory tracking. Its ability to adapt to sector-specific requirements makes it a versatile choice for businesses seeking enhanced data capabilities.

Top comparisons

More comparisons

Alation Data Catalog

Compared 30% of the time

Learn more

Collibra Platform

Compared 30% of the time

Learn more

Informatica Intelligent Data Management Cloud (IDMC)

Compared 17% of the time

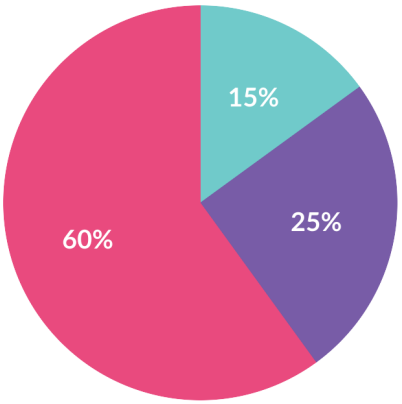
Learn more

Visitors Reading Reviews - Percentages by Top Industries

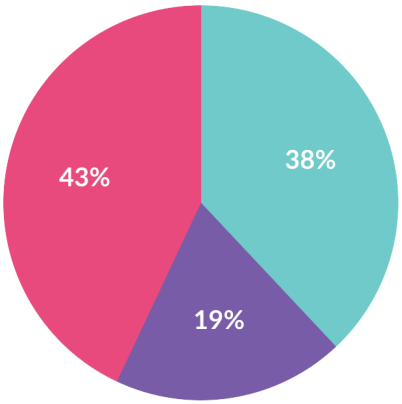
Financial Services Firm	18%
Outsourcing Company	12%
Construction Company	10%
Manufacturing Company	9%

Company size

by reviewers



by visitors reading reviews



Small Business Midsize Enterprise Large Enterprise

Valuable features

Excerpts from real customer reviews on PeerSpot:

- "Data Hub has positively impacted my organization by helping me with the data governance aspect."

  Verified user

  Associate Staff Engineer at a tech vendor with 10,001+ employees

- "Data Hub has saved approximately two million every four years, which is one of the major savings."

  Verified user

  Lead Business Analyst at a tech vendor with 10,001+ employees

- "I find Data Hub to be a very important data catalog tool for a company that values data."

  Igor Uchoa

  Senior Data Engineer at a tech services company with 1-10 employees

"We made it a place where all stakeholders in our company could log in and see which data were used for which data marts, which column values meant for which definitions, and how they were measured."

Verified user

Data Engineer at a consultancy with 11-50 employees

"Data Hub has positively impacted our organization by centralizing and co-locating all data through metadata, and we have made this our enterprise metadata catalog rather than having disorganized information across different teams."

Somashekar Venkataramaiah

Senior Technical Program Manager at a financial services firm with 10,001+ employees

What users had to say about valuable features:

"The best feature that Data Hub offers is its data catalog. The level of detail in the data catalog stands out to me, as it represents the column details, description, and tags, which are easily accessible whenever I want to access a particular column. Data Hub has positively impacted my organization by helping me with the data governance aspect. It has helped me reduce errors in data governance, save time, and improve compliance.."

Verified user

Associate Staff Engineer at a tech vendor with 10,001+ employees

Read full review

"The best features are that we do not need to use multiple tables to create our own flow. With one enriched data set that we are creating by combining the main data set with referentials, consumers can cater to their needs through one specific data set rather than having various tables at our disposal.

The second best feature is that security is built in here, whereas on Oracle, we had to manage all security-related aspects by maintaining the RDLs, restricting users based on their access levels. On Azure, security is based on the Azure RDLs that are already in place for a public Azure data lake account.

The third feature, which I consider one of the best, is OPAL, which I have already explained as Open Platform Access Library. This helps users retrieve data much faster.

The fourth advantage for the application creating this data set is that one of the new versions of OPAL, called OPAL++, helps the application audit which particular user is using this data and what kind of queries they pass throughout the day. With this, statistics can be built to see which user is utilizing the most resources and how they are utilizing them.

Data Hub has saved approximately two million every four years, which is one of the major savings. In terms of a second savings metric, more consumers have onboarded to the Azure Data Lake compared to those onboarded before, as the process is more streamlined and structured. The third savings is in terms of data on tables. Previously, tables were added as per user request, but on Azure, we have established an Enterprise Data Model. Any feeder that publishes data into Azure Data Lake must adhere to this particular model. This way we have ensured that normalization and standardization are properly taken care of.."

Verified user

Lead Business Analyst at a tech vendor with 10,001+ employees

Read full review

"I appreciate two things about Data Hub. One thing I appreciate a great deal is the ability that it has to automatically integrate with some of your tools and work as a receptor for receiving data information from your pipeline. For example, if the pipeline starts reading this table and writing these other tables, all this lineage information is sent to Data Hub automatically for some sources, while others only allow a pull-based approach. In those cases, the software needs to push the metrics from time to time to Data Hub, but it allows us to stream all these metrics to Data Hub, which is excellent and is almost seamlessly integrated with some tools that we had.

The second one is the lineage itself, because Data Hub offers a tremendous amount of data lineage capabilities, even column-level lineage, which was very useful for us and is still very useful.

I find Data Hub to be a very important data catalog tool for a company that values data.."

Igor Uchoa
Senior Data Engineer at a tech services company with 1-10 employees

Read full review

"The data injection feature was valuable to me. If comments were inserted in the tables, the data would automatically gather and enter all necessary data into Data Hub. Additionally, the data lineage graphs were really helpful in showing how data flowed to data marts and which columns were used for creating other columns. Those were helpful but somewhat hard to manage features.."

Verified user

Data Engineer at a consultancy with 11-50 employees

Read full review

"The best features that Data Hub offers include metadata propagation and lineage propagation.

These features have specifically helped my team and our workflows by enabling people to find the right data. We have different sets of data that include business data and application data. People who are new, including data analysts, machine learning scientists, or data scientists, can easily find the specific data they are looking for because it is all centralized in one place.

Data Hub has positively impacted our organization by centralizing and co-locating all data through metadata, and we have made this our enterprise metadata catalog rather than having disorganized information across different teams. It has saved time for many data analysts and data scientists to find the right data.."

Somashekar Venkataramaiah

Senior Technical Program Manager at a financial services firm with 10,001+ employees

Read full review

The best features that Data Hub offers and stand out to me are its ability to invest in metadata from a variety of databases including Oracle, MySQL, AWS database, and MongoDB. Data Hub can also work with files, embedding dataset structures. It is easy to comprehend and facilitates our teams, such as BI, EI, and data governance, to understand data and IT structures. Using Data Hub, we can build and maintain a live data dictionary, providing company-wide clarity on data.

Anhnq Ho

Finance Feedback Committee at MB Shinsei Finance Limited Liability Company

Read full review

Pain Points

The main pain points mentioned:

✖ "Data Hub can be improved with easy accessibility. I think integration with other environments is needed to enhance accessibility."

Verified user

Associate Staff Engineer at a tech vendor with 10,001+ employees

✖ "Sometimes when it goes out of memory due to multiple jobs in progress, some records are dropped because the executor is dropped without completing the entire process."

Verified user

Lead Business Analyst at a tech vendor with 10,001+ employees

✖ "Regarding what I dislike about Data Hub, I think the UI is minimalistic, and I found myself lost sometimes when looking for a specific dataset."

Igor Uchoa

Senior Data Engineer at a tech services company with 1-10 employees

✖ "From our understanding, we could not really enjoy the scalability of the data."

Verified user

Data Engineer at a consultancy with 11-50 employees

✖ "Data Hub can be improved since the version we have in our company does not support profiling for the table side."

Anhnq Ho

Finance Feedback Committee at MB Shinsei Finance Limited Liability Company

Room for improvement:

"In my day-to-day work, most consumers raise concerns with respect to the enrichment that we perform on top of the main data set provided by the respective feeding application. This is where most of the work lies for us because consumers come with multiple data-related concerns regarding data quality issues, data mapping issues, or completely missing data during the enrichment process. It is my day-to-day responsibility to ensure that no records are dropped after the main data set is enriched with referentials. On Azure, we use an architecture on Spark that builds this particular enrichment using executors and driver memory. Sometimes when it goes out of memory due to multiple jobs in progress, some records are dropped because the executor is dropped without completing the entire process. A final solution is being built to address this particular use case.

On Oracle database, when you needed to create a new attribute or when a specific user needed a particular value available for their reporting use case, whether for regulatory reporting, compliance, audit, or any kind of requirements, we would determine which would be the most appropriate table and try to add this attribute to that particular flow. In this scenario, only the application creating these tables and the user are involved. To ensure that the table does not become bulky and the data inside it is not overloading, such cases are not ensured at all and there is no normalization.

When it comes to the Enterprise Data Model, version one was created looking at all the users who currently require this particular data set. Later, when one or multiple users request the addition of a new attribute or addition of a new block of information altogether, a team called the Data Management Office becomes involved. They take care of adding this attribute to the given model, publish a new version, and ensure that the new version created is backward compatible so that downstream impacts are minimized.

Data Hub would achieve a perfect rating once all consumers migrate to the Azure database and we address the majority of concerns they have.

Since a public data lake is being used on Azure, resources are coming from Azure itself. As a result, we cannot publish any confidential information onto the Azure

Data Lake; private spaces have been created for this purpose. Once the public data lake is resilient enough to any online threats or issues, I believe Data Hub using the public data lake will become one of the major use cases where the majority of consumers can adopt it for going forward, instead of using a private lake or the Oracle database, which is entirely private and not hosted on any public platform.."

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

Read full review

"Regarding what I dislike about Data Hub, I think the UI is minimalistic, and I found myself lost sometimes when looking for a specific dataset. I could find it in the search bar, but multiple things appeared with the same name, making it hard to differentiate if it was a pipeline, a table, or a schema. This UI aspect could use improvement. Additionally, there was another issue regarding configuration; back when I used it, we had to manually input a JSON with all the configurations for a given source, which caused some issues with no visibility on those issues. Mostly the UI is something they could improve.."

Igor Uchoa
Senior Data Engineer at a tech services company with 1-10 employees

Read full review

"I am not familiar with how people use Data Hub as a knowledge system for developing LLM models or RAG, so I am uncertain what improvements could be made in that sense. However, the way we used it, the data was quite heavy because it consisted of multiple components such as graph DBs, Elasticsearch, Kafka for data injection, and MySQL for metadata storage. This made it somewhat bulky on our server when we deployed Data Hub, and we had difficulty managing the memory constraints and disk usage.

When we used Data Hub, we attempted to provide different servers for different components, but we could not find good manuals on how to use it in a more productive server manner. Having guidelines or manuals on this could be helpful.."

Verified user
Data Engineer at a consultancy with 11-50 employees

Read full review

Data Hub can be improved since the version we have in our company does not support profiling for the table side. It lacks functionality for checking the database and table side in production. Despite its robust support, the absence of table-profile support remains puzzling. An enhancement could include a customized Oracle Adapt connection for better handling data tables, especially for Oracle.

Anhnq Ho
Finance Feedback Committee at MB Shinsei Finance Limited Liability Company

Read full review

One aspect that could be improved is the ability to have more specific KPIs regarding the enrichment, completeness, and accuracy of the information.

Data Hub can be improved in several ways, primarily by enhancing the data quality evaluation capabilities. Additionally, I would suggest improving the hierarchy of business glossary terms, as understanding the characteristics of each business data object can be challenging within the current structure of business glossary terms in Data Hub. ."

Chakib Bekhouche
Consultant at jems groupe

Read full review

"We are using the free version of Data Hub with Docker Compose, so it is somewhat difficult to find out the lineage. If we are using Data Hub free version, then we can only figure out the tables' lineage, but we cannot search the column lineage, which is why I would like to add the columns-level lineage.

"I need the lineage function for more column-level lineage and I think more example documents that are essential for our company would be very useful because there are many glossary terms and features in Data Hub, but I did not know which are more essential for us.

"Additionally, I also have one more concern regarding using Docker Compose for Data Hub; the memory issues come up sometimes and consume a lot of memory resources, so I need a more efficient way to use Data Hub without these issues.."

Jueun Moon
Data Engineer at a pharma/biotech company with 501-1,000 employees

Read full review

Vendor Directory

The Vendors	The Products
2616 Design	2616 Design Risdac AI Redaction Platform for Enterprise LLM Security
A2Z	A2Z AccessiDoc
AG Ledger	AG Ledger AGLedger
AIceberg	AIceberg
AIvilo Cloud Technologies	AIvilo Cloud Technologies Aivilo Lens
	AIvilo Cloud Technologies Aivilo Lens AI-driven Strategy Assessmnet
API7.ai	API7.ai API7 Cloud
	API7.ai AISIX Cloud
ATH Infosystems	Zammad on Ubuntu 26.04 with maintenance support by ATH Infosystems
Accenture	Accenture GenWizard EventOps
Actian	Actian Data Intelligence Platform
AgenticFlowPro	AgenticFlowPro HelixCloudOps: Autonomous AI Cloud Operations and SRE Platform
AlertAI	AlertAI: AI Security, Governance & FinOps

AlertD	AlertD AI for DevOps and SREs
Algen.AI	Traccia.ai
Alice (Formerly ActiveFence)	WonderFence
	WonderCheck
Amnic	Amnic - Cloud Cost Observability Platform
	Amnic: AI Token Management
Anomalo	Anomalo Data Quality
Aokumo	Aokumo AI
AppFactor	MCP Bridge by AppFactor
Applisafe	Applisafe
Arato.ai	Arato AI
Arize AI	Arize AI
Arthur	Arthur AI
Articul8 AI	Articul8 AI Articul8 LLM-IQ Agent
	Articul8 AI Articul8 Network Topology Agent

Ataccama	Ataccama ONE Platform
Atos	Atos AgentX
Auditty	Auditty Real Time Log Intelligence
Autonoma	Autonoma BUILD
	Autonoma PLATFORM
BMC	BMC Helix
Band	Band: Communication layer for Multi-Agent Systems
Base14	base14 Scout
BizoneAi	BizoneAi Bizone
Blue Peak	Blue Peak De-ID Studio: Document De-Identification for AI and Analytics Pipelines
BonData	BonData AI Data Engineer For Everyone
Boomi	Boomi iPaaS
	Boomi One Platform Digital Edition
Braintrust Data	Braintrust
Bright Data	Bright Data MCP

BugZero	BugZero ServiceNow Integration
CTX	CTX Reflector v2 for BGP Control Plane
CYLLiX	Cyllix Observability Node on AL2023
Cambridge Technology	Cambridge Technology NanoOrch
Causely	Causely AI
	Causely Mediator
Check Point Software Technologies	Check Point Infinity
Chkk	Chkk
Ciroos	Ciroos AI SRE Teammate
CleanStart Security	CleanStart Security CleanStart: Secure Software Supply Chain and Hardened Container Images
Cloud SOE	Cloud SOE Squid Proxy Server on AWS
Cloudfu	Debian 13 x86_64 minimal with support by Cloudfu
	CentOS Stream 9 x86_64 latest with support by Cloudfu
CloudiDR	CloudiDR LLM Ops
Cloudology	Cloudology Clu Ops Agent

Code Creator	SigNoz All in One Observability Server by Code Creator
	Private AI Document Search by Code Creator
Codenotary	Codenotary AgentMon AI Agent Runtime Security & Oversight
CoffeeBean Technology	CoffeeBean Technology MCP Server
Comet	Comet
Coralogix	Coralogix
Coxwave	Coxwave Align
CrewAI	CrewAI
Cribl	Cribl MCP Server
CtrlB: Redefining Observability	CtrlB: Redefining Observability CtrlB: The Fastest Data Lake for Observability and Security
Cyera	Cyera DataPort
	Cyera Data Security Posture Management for Security Hub Extended
DD Vand	DD Vand DriftLock: Schema Drift Monitoring for VPC Data Pipelines
DINAMO Networks	DINAMO Networks Appdome Platform
Dagger	Dagger Enterprise Essentials

Darktrace	Darktrace
Dash Security	Dash Security Dash AI Agent Security Platform
DataFlint	DataFlint
DataHub	Data Hub
DataRobot	DataRobot
	DataRobot 11
Datadog	Datadog
Deeploy	Deeploy Core
DevRev	Computer by DevRev
Devco Services	Devco Services AI readyness Check
Diagrid	Diagrid Catalyst Enterprise
	Diagrid Catalyst
DinoCloud	DinoCloud Rex Copilot
Dynamiq	Dynamiq Gen AI platform
Dynatrace	Dynatrace

Eden AI	Eden AI
Elementary Data	Elementary Data Elementary
Emdrtc	Emdrtc Aegis Data Shield
Evoke Security	Evoke Security Evoke Agentic Security Platform
F5	F5 AI Red Team
	F5 AI Guardrails
Fabrix.ai	Fabrix.ai Fabrix AI Agents for Operational and Business Intelligence
Faros AI	Faros AI Faros Platform
Ferrum Health	Ferrum Health AI Governance Suite
Finops Control	Finops Control Infra-Observability-at-a-glance
Fission Labs	Fission Labs FloTorch Enterprise
Flexera	Flexera Cloud Cost Optimization
Fortinet	Fortinet FortiSIEM
Fyrii.ai	Fyrii.ai Observability
Gainsight	Staircase AI by Gainsight

Galileo	Galileo
Gathid Software	Gathid Software Gathid Identity Observability Platform
Geordie	Geordie Agentic Security Platform
H3 Labs	Maxim AI
HCLSoftware	HCL iControl
HITRUST	HITRUST
HackerOne	HackerOne
Honeycomb.io	Honeycomb Enterprise
Hud	Hud: Runtime Code Sensor
IBM	IBM Instana Observability
	IBM Instana Observability Self-Hosted
	IBM Instana Observability MCP Server
	IBM watsonx.data integration as a Service
ICTBIT	ICTBIT Aladdin FinOps & Cloud Governance Platform
Incisio AI	Incisio AI

Info Inlet	Info Inlet VM monitoring using prometheus and grafana
Info Services	Info Services ClairAI
Iverse	Iverse
JEFFE.ai	JEFFE.ai
Jaxon AI	Jaxon AI DSAIL
JetStream Security	JetStream Security JetStream Enterprise AI Visibility & Governance Platform
KSP IT TECH	KSP IT TECH Finops-cloud-cost-ami
Kanu AI	Kanu AI Cloud Engineer Containers
Kaya	Kaya
Keysight Technologies	Keysight CloudLens Collector
	Keysight CloudLens Manager
	Keysight CloudLens Virtual Packet Broker
	Keysight Vision Orchestrator
KloudMate	KloudMate
Kong	Kong Konnect

	Kong Konnect Enterprise
KubeSense	KubeSense AI
LangChain	LangChain LangSmith
	LangChain LangSmith Agent Engineering Platform
LaunchDarkly	LaunchDarkly
Letta	Letta
Limy AI	Limy AI
Linx Security	Linx Security MCP Server
LogiRoot AI	LogiRoot AI LogiRoot: Runtime AI Governance & Verifiable Audit Evidence
LogicMonitor	LogicMonitor Edwin AI
Logz.io	Logz.io OrionIQ Autonomous AI Agents for Observability and IT Operations
MONITORAPP	MONITORAPP AISWG-VE for AWS
Madarson IT	Madarson IT SUSE Linux Enterprise Server 15
Magure	Magure MagOneAI
Manage Stacks	Manage Stacks Fully Managed, and Optimized Grafana with Prometheus

	Manage Stacks Fully Managed, and Optimized Prometheus with Docker
	Manage Stacks Fully Managed, and Optimized Grafana
	Manage Stacks Fully Managed, Secured, and Optimized Wazuh
MasterDatabase	MasterDatabase AtomikHub: Multi-Cloud Monitoring, FinOps & AI Observability
Merge	Merge Agent Handler
Meyi Cloud	Meyi Cloud Meyi Connect
Meyi Cloud US	Meyi Cloud US Prometheus, Grafana & Loki on Ubuntu with support by Meyi Cloud
Microsoft	Azure AI Metrics Advisor
Mindflow	Mindflow
Mint Security	Mint Security Platform
Miri Infotech	Sonarqube pre-configured by Miri Infotech Inc. on Ubuntu
NOFire AI	NOFire AI
NetPrompt AI	NetPrompt AI
Netskope	Netskope Data Security Posture Management
Observe, Inc.	Observe

Oodle AI	Oodle AI
OpenLM	OpenLM Platform
Openlayer	Openlayer
Operant AI	Operant AI Gatekeeper
Operata	Operata
	Operata CX Observability for Amazon Connect, Low Volume
OpsTree Global	OpsTree Global Buildpiper
PHTN.ai	PHTN.ai
Palo Alto Networks	Palo Alto Networks Prisma AIRS API
Pebble	PebbleAI
Pelanor	Pelanor
Plurai	Plurai Simulation
Plural	Plural Kubernetes Management
Port0	Port0 CloudRoute Visualize Your AWS Network in Minutes
PostHog	PostHog

Prezelfy	Loki on AL2023 Hardened by Prezelfy
Propagate	Propagate Nextcloud
Pydantic	Pydantic Logfire
Qualifire	Qualifire Platform
Quantixa	Quantixa Ablefield
Rad AI	Rad AI
Rapid7	Rapid7 InsightCloudSec
	Rapid7 InsightAppSec
Redwood Software	Redwood Software RunMyJobs
Reejig	Reejig: Boldly and responsibly reinvent work for the AI era
Resolve AI	Resolve AI
RubixKube	RubixKube
Runlayer	Runlayer
Saviynt	Saviynt MCP Server
Sedai	Sedai

Selector	Selector AIOps
Sensedia	Sensedia AI Gateway
SentinelOne	SentinelOne Singularity Endpoint
	SentinelOne Singularity Cloud Security
	SentinelOne Singularity AI SIEM
	SentinelOne Observo AI
Sentrilite	Sentrilite Observability and Audit Agent
Sherlocks.ai	Sherlocks.ai
Singulr AI	Singulr AI Governance and Security Platform
SmileShark	SmileShark SharkMon
SoftBank Corp.	SoftBank Corp. AGENTIC STAR
SolidCore.ai	SolidCore.ai SolidCore
Solo.io	Solo.io agentgateway
Span	Span
Splunk	Splunk MCP Server

Spot - A Flexera company	CloudCheckr
	Spot.io Contract
StackAI	StackAI Customer Hosted
	StackAI Hosted
StackGen	StackGen StackHealer Agent
Status.io	Status.io
Straiker	Straiker AI
	Defend AI
SuperAnnotate	SuperAnnotate
Sweep	Sweep
Synadia	Synadia Managed Platform
Sysdig	Sysdig Secure
Tata Elxsi	Tata Elxsi NEURON Autonomous Network Platform
TeamForm	TeamForm
Tech 42	Tech 42 AI Agent Starter Pack built with AgentCore

TeraOps	TeraOps AI and Cloud ROI Engine
ThinkCloud	ThinkCloud NovaGuard Cloud Security Platform- CNAPP
	NovaGuard Cloud Security Platform by ThinkCloud
Tigera	Calico Cloud
TomorrowX	TomorrowX
Traccia	Traccia AI
Traversal	Traversal
Trustwise	Trustwise AI Control Tower
Turiya AI	Turiya AI
UST	UST PACE FinOps
VNGRS	Kumru LLM API
VeloDB	VeloDB Cloud
Vercom LogLens	Vercom LogLens AlertBridge
Verified Images	Grafana on Ubuntu 26.04 by Verified Images
Vertesia	Vertesia Platform

Vibranium Labs	Vibranium Labs Vibe AI
Webrix	Webrix MCP Security Platform
Weights & Biases	Weights & Biases
Xenium Cloud Technologies B.V.	Xenium Cloud Technologies B.V. XePlatform: Managed, Private and Hybrid AI Inside Your

	AWS Account
XperiencOps	XperiencOps XOPS Knowledge Graph Platform
Xtremax Pte	Xtremax Pte Chocolate Factory AI
Zeabur	Zeabur Nuphos
Zenity	Zenity
	Zenity AI Security & Governance Platform for Security Hub Extended
ZvitSev	Zvitsev API Shield
aizome	Aizome Platform
bCloud	bCloud Hatch
	bCloud Valkey Cluster
	bCloud Photoview server
	Jetty on Ubuntu 26.04 With maintenance support by bCloud

	EspoCRM 9.3.7 on Ubuntu 26.04 with Maintenance Support by bCloud
blaZop	blaZop AIOps Platform
digitate	ignio AIOps Platform
	digitate ignio AIOps Platform <India>
eCloudvalley HK	eCloudvalley HK MAIAH Governance
eg Innovations	eg Innovations eG Universal Agent Operator
	eg Innovations eG Enterprise Express Cloud
groundcover	Groundcover Observability Platform
	Groundcover. The observability platform for engineers and agents
highflame	Highflame: Secure AI Fabric
kCloudHubs	Symfony Framework on Ubuntu 24.04 with maintenance support by kCloudHubs
	Victoria Metrics Ubuntu 24.04 with maintenance support by kCloudHubs
	Safety Gym on Ubuntu 24.04 with maintenance support by kCloudHubs
	Typemill on Ubuntu 24.04 with maintenance support by kCloudHubs
	KooBoo on Ubuntu 24.04 with maintenance support by kCloudHubs

	Theano on Ubuntu 24.04 with maintenance support by kCloudHubs
	Glances Ubuntu 26.04 with maintenance support by kCloudHubs
	Typemill Ubuntu 26.04 with maintenance support by kCloudHubs
	Safety Gym on Ubuntu 26.04 with Maintenance Support by kCloudHubs
lreceive	lreceive: LLM Compliance Audit Proxy for PII/PHI Redaction & SOC 2
nudgebee	NudgeBee
pCloudHosting	pCloudHosting LlamaIndex
	pCloudHosting Singledispatch AI
	pCloudHosting PyGPT
	pCloudHosting Gencore AI for Oracle Object Storage
	pCloudHosting Qodo Embed
	pCloudHosting Gencore AI for GoogleCloud Storage
	PrestoDB on Ubuntu 24.04 with maintenance support by pCloudHosting
	Whereabouts on Ubuntu 24.04 with maintenance support by pCloudHosting
	ORAS on Ubuntu 24.04 with maintenance support by pCloudHosting

	Flatpress on Ubuntu 24.04 with support by PCloudHosting
	Munin on Ubuntu 26.04 with support by PCloudHosting
	SQLalchemy on Ubuntu 26.04 with support by PCloudHosting
perfware.cloud	perfware.cloud Log Processor

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