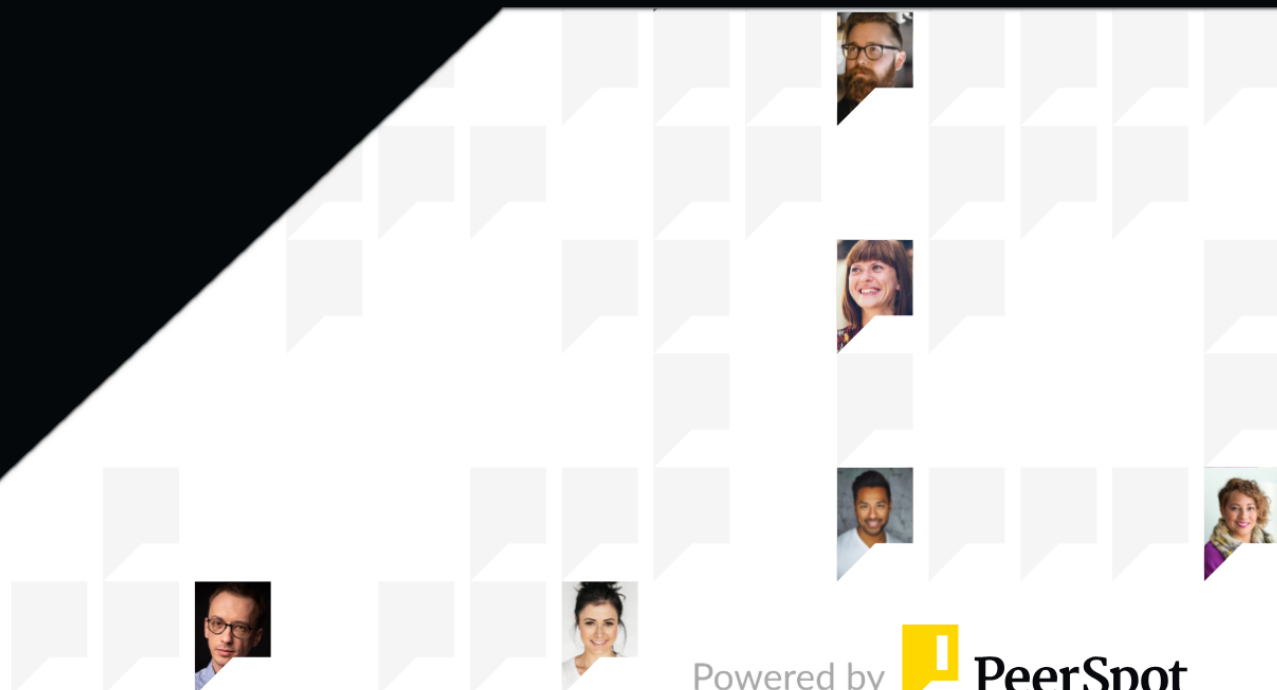




SentinelOne Singularity AI SIEM

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 18

Use Case..... 19 - 23

Setup..... 24 - 26

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

Other Advice..... 30 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

Product Recap



SentinelOne Singularity AI SIEM

SentinelOne Singularity AI SIEM Recap

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.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“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



“Overall, this affects my security posture positively because it improves it since it helps us in real-time monitoring, and it gives us automated investigation and also the auto-investigate tab, so it is pretty good.”



Likhith Varma

Senior Security Analyst at Areté Associates, Inc.



“I assess the overall security posture of our organization after implementing SentinelOne Singularity AI SIEM as significantly improved.”



Mohsinoddin Mohammed

Information Security Principal at a venture capital & private equity firm with 1,001-5,000 employees

- ✓ “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%.”



GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

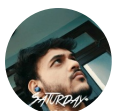
- ✓ “The beauty of the integration is that it integrates very smoothly with third-party tools, so we do not need to think about the parsers, coding, depending on the codes, or the software developers.”



Sanjay Kaushal

Vice President Cyber Security Practice Head at orbit techsol w pvt.ltd

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



Md Rafique

it support 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

What users had to say about valuable features:

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

“SentinelOne Singularity AI SIEM has impacted my organization positively and it was a very good solution..”

Ayman Said

Infrastructure System's Manager at ICAPP (Americana Group)

[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..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“The best features of SentinelOne Singularity AI SIEM include its ability to give you a brief description of what the alert is about. When an alert is triggered with AI SIEM, we have a basic analysis of what the alert is about, and it will give you the understanding of what the alert is.

“I especially value that analysis feature. If you get an alert in SentinelOne Singularity AI SIEM, we have an auto-investigate tab as well. If you click on that auto-investigate tab, it will correlate with all the products and data sources it has, and it will give you a deep analysis of what the alert is and what is happening, so everything is covered.

“The real-time monitoring is pretty good. It correlates between all the different data sources that have been integrated with SentinelOne Singularity AI SIEM. It will correlate everything and give you a pretty good storyline of what the alert is about.

“Overall, this affects my security posture positively because it improves it since it helps us in real-time monitoring, and it gives us automated investigation and also the auto-investigate tab, so it is pretty good..”

Likhith Varma

Senior Security Analyst at Areté Associates, Inc.

[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](#) 

“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

[Read full review](#) 

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

“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](#) 

Other Solutions Considered

“I have only worked with SentinelOne Singularity AI SIEM because I have recently started working. I have seven to eight months of experience, so I have never used any different solution..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“I previously used another SIM solution. The main reason for moving to SentinelOne was to improve centralized visibility, simplify security options, and take advantage of AI-driven event correlations. With the previous solution, investigation often required switching between multiple tools and manually correlating events..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“Before choosing SentinelOne Singularity AI SIEM, I did not evaluate other options because SentinelOne Singularity AI SIEM is the best according to me. We have used other tools, but SentinelOne Singularity AI SIEM has multiple types of features and it is an easy-to-understand tool. That is why I am choosing SentinelOne Singularity AI SIEM..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“I considered other enterprise SIEM platforms such as Sentinel, Splunk, Enterprise Security, IBM, and Google Security Operations. I evaluated them based on integration with my existing environment, AI-assisted threat detection, scalability, ease of investigation, automation capabilities, and total cost of ownership. SentinelOne stood out because of its strong integration between EDR and AI SIEM, centralized visibility, and AI-driven event correlations..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“I was not directly involved in the product evaluation or selection process, so I cannot accurately state which vendors were formally evaluated. In general, organizations looking at AI-powered SIEM solutions consider options such as Microsoft Sentinel, Google Security Operations, IBM, Falcon Next-Gen SIEM, and Microsoft Defender. However, I have not worked on those solutions, so I only have knowledge of SentinelOne Singularity AI SIEM..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“In our organization, we previously used the CrowdStrike solution.

“We switched from CrowdStrike to SentinelOne Singularity AI SIEM because our organization is an MSSP organization. That means I provide services to the client. We had twenty to thirty clients in our organization that we managed. Twenty-seven or twenty-eight clients were using SentinelOne Singularity AI SIEM, but only one or two clients were on CrowdStrike. Their client also switched to SentinelOne Singularity AI SIEM. That is why, at this time, we are only managing SentinelOne Singularity AI SIEM..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

ROI

Real user quotes about their ROI:

“SentinelOne Singularity AI SIEM has impacted my operational costs positively, and I think we made a good deal with them because we are a big group and have a big account, so we got a good deal with SentinelOne..”

Ayman Said

Infrastructure System's Manager at ICAPP (Americana Group)

[Read full review](#) 

“I cannot provide verified metrics because I was not directly involved in measuring ROI, so I would not want to speculate. My experience is that the value comes from improved analyst productivity, faster investigations, and reduced operational overhead rather than a specific percentage of cost savings..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“When we took the service from SentinelOne, they provided an onboarding process with a dedicated engineer who helped us with all aspects of the implementation. A dedicated engineer from SentinelOne regularly contacts us, assists with configuration, and works with us on implementation details..”

Mohsinoddin Mohammed

[Read full review](#) 

Information Security Principal at a venture capital & private equity firm with 1,001-5,000 employees

“I have seen a positive return on investment primarily through operational efficiency rather than reducing headcount. The biggest measurable benefit has been the reduction in investigation time. Before using SentinelOne Singularity AI SIEM, investigating a moderately complex alert took around thirty to sixty minutes because analysts had to collect logs from multiple security tools. With centralized log management and AI-driven correlation, I can often understand the scope of an incident in about ten to fifteen minutes..”

Md Rafique

[Read full review](#) 

it support at a outsourcing company with 51-200 employees

“For instance, if you are getting attacked and you use a brand other than SentinelOne Singularity AI SIEM, you will need to contact the OEM for recovery, which takes time. In contrast, with SentinelOne Singularity AI SIEM, we have a rollback option with just an automated click. If the data gets encrypted, it automatically rolls back. This functionality minimizes downtime and the impact of the attack. Looking at that perspective—post-attack damage control—the ROI is better. Using SentinelOne Singularity AI SIEM, data retrieval happens at a much faster rate, allowing production to continue without impact..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“I have seen a return on investment with SentinelOne Singularity AI SIEM. The tool also saves our money and time. The pricing is very medium, and time is also saved because there are automation features available. That is why multiple alerts are raised by the automated process. In those times, manual alerts are less frequent compared to other tools. It is helpful. Sometimes, in our organization, two people are working on these AI-driven features in SentinelOne Singularity AI SIEM. But when the automation features are started, one person can also manage the console. It is money saved, and the automation and those types of activities are doing the automated alerts. One person is only managing and checking if the alerts are going properly. That is why it is also money-saving. It is a money-saving tool, and the pricing is also low. Any small or startup organization can also buy it easily..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

Use Case

“SentinelOne Singularity AI SIEM is a tool that we use to support our clients. Our organization is a service-based organization, so we use SIEM to provide services to software-based clients. We are a partner with SentinelOne..”

Likhith Varma

Senior Security Analyst at Areté Associates, Inc.

[Read full review](#) 

“My main use case for SentinelOne Singularity AI SIEM is centralized log management, threat detection and correlation for incident investigation, automated response, cloud security monitoring, and endpoint plus SIM correlations.

My primary use case for SentinelOne Singularity AI SIEM is centralized security monitoring and incident investigation. I ingest logs from Microsoft Entra ID, Active Directory, Microsoft 365, firewall, VPNs, and SentinelOne EDR into the AI SIEM. Instead of checking each platform individually, I use SIEM to correlate events, identify suspicious activity, and investigate incidents from a single console..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“SentinelOne Singularity AI SIEM's main use case is to enhance cybersecurity by using AI to detect, investigate, and automatically respond across endpoints, cloud, and identities. It helps security teams reduce manual efforts, accelerate incident response, and improve overall security operations.

“In my previous role, I used SentinelOne Singularity AI SIEM to investigate endpoint security alerts. Instead of manually using logs from multiple systems, I used the AI-powered investigation features to quickly identify the root cause of suspicious activities. SentinelOne Singularity AI SIEM automatically correlated related events and highlighted the affected endpoints while recommending response actions. We isolated the endpoints with a single click after verifying it was a malicious script, and we remediated the issue much faster than the previous manual process..”

Verified user

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

[Read full review](#) 

“SentinelOne Singularity AI SIEM serves as our centralized platform for security data across our environments, enabling real-time threat detection and accelerated incident response. I use it to collect and analyze logs from endpoints, cloud workloads, identity providers, firewalls, and SaaS applications.

“We initially used SentinelOne Singularity AI SIEM to identify and investigate a potential account compromise. The platform correlated unusual login activities from our identity provider, multiple authentication attempts, and suspicious PowerShell execution on an endpoint. Rather than having analysts manually check logs from different tools, the AI SIEM automatically connected these events into a single incident. This allowed our SOC team to quickly determine that the credentials were compromised and isolate the affected endpoint.

“Our primary use case focuses on improving SOC efficiency by centralizing security telemetry and using AI to correlate alerts from endpoints, cloud identity, and network sources. Instead of investigating isolated alerts, analysts receive prioritized incidents with the full attack timeline. This helps reduce alert fatigue, speed up investigations, and enable faster response to threats such as phishing, credential compromise, and lateral movement..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“Clients can use SentinelOne Singularity AI SIEM for endpoint security solutions, and apart from that, we currently have something called prompt security where it is helping us to enhance control over the AI prompts given by end-users. Some end-users tend to feed sensitive data to AI tools like Claude, Gemini, and ChatGPT. We have not implemented it yet, but we have provided a POC for agnostic prompt security.

“AI-driven Threat Detection capability is crucial because attackers have started conducting attacks using AI patterns. They analyze the patterns of defending solutions, and based on the defense architecture, they generate the payload according to the environment. To detect those kinds of payloads, we need AI-based threat detection to sense whether they come from a single source or distinct sources, where these kinds of prompts and malicious payloads are being generated.

“Real-time monitoring is a must-have functionality for any product, and SentinelOne Singularity AI SIEM has the same response. We can create rules for peculiar situations we encounter, and if those rules get triggered, the system can automatically help isolate or contain that system while providing us alerts at the same time. This way, if a particular user reports not being able to reach anything, we can quickly understand that SentinelOne Singularity AI SIEM has isolated their system..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“In my daily work, the main use case for SentinelOne Singularity AI SIEM is creating rules, fine-tuning, source recording, rule creations, and when any alerts are triggered. We can raise them to the client side, continuously monitoring any alerts. We can raise them to the client side for early resolution, also creating the dashboards, checking the logs, and agents installation. Those are the day-to-day tasks in our SIEM tool.

“Alert fighting is a specific example of a recent situation where I used SentinelOne Singularity AI SIEM for one of these tasks. Sometimes multiple alerts are triggered in the SIEM. At that time, we analyze what type of alert it is, whether it is a true positive or false positive. That is challenging for me.

“Our day-to-day tasks include alert raising, continuous monitoring, raising the alerts, dashboard managing, creating the dashboard, rule creating, and decoder creating. If there is any requirement from the client side, we will also do these types of activities, creating any new rule.

“When I have those multiple alerts and I need to figure out if they are true positives or false positives, I usually check in Deep Visibility if it belongs to any suspicious fields or anything malicious, or if it is a true positive belonging to our organization. I also check if it belongs to any suspicious sites, IPs, or IOCs such as malicious IPs or malicious hashes, or if it belongs to any malicious paths. I will check the source, the destination, and what it is doing. We can check if the path belongs to a genuine path or a suspicious path. We will do that type of analysis and then I will specify if it belongs to a true positive or a false positive. We can follow those types of steps..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The integration part for SentinelOne Singularity AI SIEM is very easy. Any fresher can easily do this. The agent installation is also so easy. Within one to two minutes, we can install SentinelOne Singularity AI SIEM agents in the environment or client environment network. It is the best, fastest installation..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“My advice would be to plan the deployment carefully, integrate all relevant security data sources, and invest time in tuning detection and automation. SentinelOne Singularity AI SIEM delivers the most value when AI supports experienced analysts by reducing manual work and improving investigation speed rather than operating without human oversight..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“The deployment process with SentinelOne Singularity AI SIEM is somewhat complicated. Until some versions, we had scenarios where we needed to reboot machines, impacting deployment. However, with upgraded versions, we can now install the agent without any reboot, showing that they have improved that aspect..”

GANESAN K

[Read full review](#) 

Senior Technical Engineer at Safezone Secure Solutions Private Limited

“Overall, my experience with pricing, setup cost, and licensing has been positive. While SentinelOne Singularity AI SIEM is an enterprise-grade platform and not the lowest cost option, I think the pricing is reasonable considering the capabilities it provides. Features such as centralized log management, AI-driven analytics, automated workflow, and integrated security options can reduce operational overhead and improve SOC efficiency, which helps justify the investment..”

Md Rafique

[Read full review](#) 

it support at a outsourcing company with 51-200 employees

“The AI integration was pretty straightforward. I did not face any problem. We created some policies and based on those policies, we were able to identify how to integrate it via this. I do not remember the exact steps. I have a document written on it somewhere that I need to pull out. It was a pretty standard thing. You just have to go to some consoles and integrate it based on this. You have to provide the endpoint details and it got integrated very smoothly..”

Hardik Murdia

Technical Lead at a tech vendor with 51-200 employees

[Read full review](#) 

“We do participate in the initial setup of SentinelOne Singularity AI SIEM.

“The usual setup process involves the log collectors and the cloud-based device. We create the VPN tunnel from the customer locations, and then we analyze the logs, create the alert, identify the incident, exposure management, and event search. It also works as a data lake, which is very good in SentinelOne Singularity AI SIEM. We have very good vulnerability management, which shows the beauty of the product.

“There are no challenges with the initial setup because we have done multiple successful deployments..”

Sanjay Kaushal

Vice President Cyber Security Practice Head at orbit techsol w pvt.ltd

[Read full review](#) 

Customer Service and Support

“My experience with the support has been very responsive and knowledgeable, particularly for technical issues and troubleshooting. I would rate the customer support eight out of ten..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“I have not reached out to customer support yet and have not experienced it directly. However, I have heard from my organization that their customer support is very good. Several of my colleagues have spoken with customer support, and their experience was great..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“Customer support could be better. Customer support could be better because it is frequently transferred to various agents. This is just one particular case, and I do not want to elaborate further..”

GANESAN K

[Read full review](#) 

Senior Technical Engineer at Safezone Secure Solutions Private Limited

“In rating the technical support for SentinelOne, it depends on whether we are discussing EDR or SentinelOne Singularity AI SIEM. I would not rate the entire company uniformly. For the EDR, I might rate it around eight out of ten; for SentinelOne Singularity AI SIEM, I would give it five out of ten or two out of five..”

Emmanuel-Bentil

[Read full review](#) 

Managing Director at iMark Consult

“I would rate the technical support around five.

“I rate it five because even if you raise a case with SentinelOne support, you will not get that fast of a response. Even if you raise a P1 or P2, you have to engage back-end support in order to get a response from them. That has been a major drawback in the tool. Also, even if you get a response, it will be a generic response..”

Likhith Varma

[Read full review](#) 

Senior Security Analyst at Areté Associates, Inc.

“The customer support for SentinelOne Singularity AI SIEM is also the best because we have raised tickets to the support center multiple times. The support team gives an immediate answer, within ten to fifteen minutes. They also schedule calls and troubleshoot the alerts and solve the issue. The support team is very best.

“I rate the customer support for SentinelOne Singularity AI SIEM a ten out of ten..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

Other Advice

“My advice would be to spend time planning the deployment and identifying the log resources that provide the most value. SentinelOne Singularity AI SIEM is most effective when it is integrated with key systems such as Entra ID, 365, VPN, and endpoints. I would rate this product eight out of ten overall..”

Md Rafique

it support at a outsourcing company with 51-200 employees

[Read full review](#) 

“My impression of SentinelOne Singularity AI SIEM's AI-driven threat detection capability is very positive. It uses behavioral analysis and machine learning to identify suspicious activity that may not be detected by traditional signature-based methods.

“I used SentinelOne Singularity AI SIEM's automated workflow capability to reduce repetitive security tasks. For example, when a high-risk alert was detected, automated workflows helped with actions such as endpoint isolation, alert enrichment, and triggering response processes without requiring manual intervention at every step. This reduced the time analysts spent on routine tasks and has improved consistency in incident handling.

“My advice would be to clearly define your security goals and use cases before deploying SentinelOne Singularity AI SIEM. Start with proper endpoint coverage, integrate with your existing security tools, and spend time tuning policies to reduce unnecessary alerts. I would also recommend training the SOC team on the AI investigations and automation features so they can fully benefit from the platform. Finally, continuously review detection results and response processes to ensure the platform is meeting the organization's security needs. I would rate this solution an eight out of ten..”

Verified user

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

[Read full review](#) 

“The accuracy and reliability of output from SentinelOne Singularity AI SIEM are very high. SentinelOne Singularity AI SIEM is very accurate. It is also very reliable. We have not found any glitching. It is faster, and it also has real-time threat hunting and real-time detection. That is the capability in there.

“The real-time monitoring feature of SentinelOne Singularity AI SIEM helps with Deep Visibility. If any malicious or suspicious alerts are triggered, I will check the alert. We can analyze this alert with the help of Deep Visibility. We can see its

source, its destination, what it is trying to do, and if the path is genuine or not. We receive the alerts and we can do this type of investigation. Then, if anything malicious happens, we can raise it to the client side for notification purposes. We can say we observed this type of alert at this time, and it is this type of malicious activity.

“My impression of the AI-driven threat detection capabilities of SentinelOne Singularity AI SIEM is that it is the best feature because multiple alerts can be happening, but the AI-driven features immediately block them. Any alerts are blocked before they happen. And it gives the action, such as killing and quarantining the threat.

“I give SentinelOne Singularity AI SIEM an overall rating of ten out of ten..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“For the implementation and deployment of SentinelOne Singularity AI SIEM for the whole solution, it takes about months as we made a migration from EDR to another for 3,000 users across Egypt and GCC, so it takes a lot of efforts.

“I assess the efficiency of SentinelOne Singularity AI SIEM in improving my response time to sophisticated threats as very fast and very good.

“For false positive incidents, SentinelOne Singularity AI SIEM manages these situations very well, and when we are facing someone uploading a false positive file, we can deal with these situations very well. You can easily go into the interface and mark this as a false positive, and I can recover the deleted or false positive files or anything like that.

“AI-driven analytics of SentinelOne Singularity AI SIEM helped me to reduce false positives.

“I assess the real-time monitoring feature of SentinelOne Singularity AI SIEM as very good and very responsive. Monitoring is working well, and it has a fast response to any threat; it does not take more than a few seconds to detect any threat and send a request for action. So it is very good.

“For the automated workflow feature of SentinelOne Singularity AI SIEM, we did not try it.

“I rate this product an 8 out of 10..”

Ayman Said

Infrastructure System's Manager at ICAPP (Americana Group)

[Read full review](#) 

“In my organization, approximately eighty people work with SentinelOne Singularity AI SIEM.

“Our clients vary in size; we have small businesses, medium enterprises, and large enterprises as well.

“SentinelOne Singularity AI SIEM does require maintenance in that we manage the integration and everything, but the tool UI and everything is updated by the SentinelOne team itself. We do not upgrade anything.

“Doing updates for SentinelOne Singularity AI SIEM is easy.

“I evaluate the efficiency in investigating alerts and responding to various incidents as pretty good; they have a pretty good collection of events. You will have all the events that you need to do an investigation, and I would say it is pretty good. Once you start working with the tool, you will have pretty good responses in the event search to investigate.

“We are using the automated workflow feature in order to reduce the number of false positives. With that, benign threats and all will be there, so we are just closing them out. It is reducing the volume of alerts for now.

“The advice I would give others looking to implement SentinelOne Singularity AI SIEM is that it has its pros and cons. If you are looking for a decent tool for investigation, it is good. But if you are a large enterprise and if you have loads of logs that are being ingested, I would say just think about it because we are having issues while handling large clients and pulling a larger number of logs. I would rate this product an eight out of ten..”

Likhith Varma

Senior Security Analyst at Areté Associates, Inc.

[Read full review](#) 

“AI-driven analytics can reduce false positives by providing better context and correlating related alerts into meaningful incidents. This helps analysts spend less time investigating false activity and more time responding to genuine threats.

“My impression is that the AI-driven threat detection capabilities are one of the platform's key strengths. Overall, I have a positive impression. The AI-driven threat detection helps identify suspicious behavior, correlate related events into

meaningful insights, and prioritize higher-risk threats. This enables analysts to investigate and respond more quickly while reducing alert fatigue. Human validation is still important, but the AI provides valuable decision support.

“From my perspective, SentinelOne Singularity AI SIEM appears very suited for organizations with growing data volumes and increasingly complex IT environments. The visibility to ingest and correlate telemetry from endpoints, cloud workloads, identity systems, and third-party security tools provides a centralized view as the environment expands. Real-time monitoring impacts our threat identification process significantly.

“Based on its capability, SentinelOne Singularity AI SIEM can improve SOC efficiency by correlating alerts, summarizing incidents, and helping analysts prioritize genuine threats. This reduces manual investigation and enables faster incident response while analysts still validate the AI's recommendations for critical decisions.

“I think SentinelOne has taken a strong approach to AI governance and security. The platform uses AI to assist analysts with tasks such as alert correlation, investigations, and incident summarization while still allowing human analysts to validate findings before taking actions. From a governance perspective, having role-based access control, audit logs, and centralized visibility helps organizations maintain oversight. It is important to have clear governance policies, regularly review AI-generated recommendations, and ensure automated response workflows are appropriately validated.

“Overall, I would rate the accuracy and reliability of the AI capabilities as good. The AI is effective at correlating related alerts, summarizing incidents, and helping analysts prioritize investigations, which can significantly reduce manual effort. However, AI outputs should not be treated as infallible, and for higher impact security decisions, it is still important for analysts to validate the AI findings and recommendations. I would rate this review as an eight out of ten overall..”

Vanshika

Cybersecurity Engineer at Gigabit Technologies Pvt Ltd

[Read full review](#) 

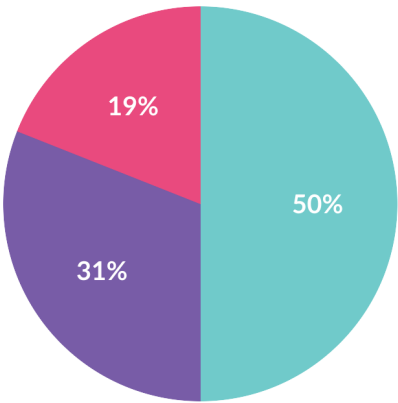
Top Industries

by visitors reading reviews

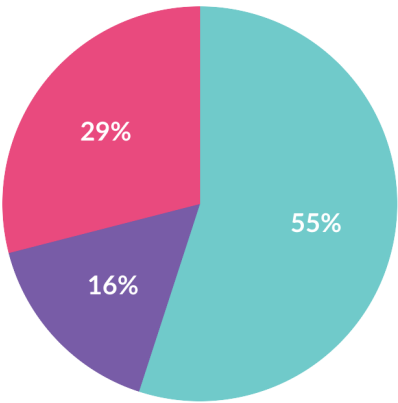


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944