aws marketplace

SentinelOne Singularity AI SIEM

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

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:

- "AI-driven capabilities will give me real-time detection and will protect my autonomous AI interruption."

Mohan Janarthanan

Associate Vice President at Novac Technology Solutions

- "SentinelOne Singularity AI SIEM's AI-powered analytics does affect our SOC's ability to reduce false positives; that is one of the biggest advantages because the manpower that I have is limited."

Prince Joseph

Group Chief Information Officer at NeST Information Technologies Pvt Ltd

- "After using SentinelOne Singularity AI SIEM, it has reduced our incident response time by forty to fifty percent compared to other tools."

Verified user

IT Security Analyst at a tech consulting company with 11-50 employees

"Overall, I would assess the overall security posture after implementing SentinelOne Singularity AI SIEM as significantly better."

Fabian Brandt

IT Security Consultant at Systemhaus for you GmbH

"When they face attacks such as ransomware and are dissatisfied with their existing solutions, they switch to SentinelOne Singularity AI SIEM, which is quite good in detecting unknown threats, cleaning the system, and handling ransomware."

Verified user

Cyber Security Engineer at a retailer with 201-500 employees

What users had to say about valuable features:

"AI-driven capabilities will give me real-time detection and will protect my autonomous AI interruption. We are using NLP language where my prompt engineer will upload some sensitive data. This can be detected and can protect my sensitive data from exfiltration. The AI-driven threat detection capabilities improve our overall security posture. By enabling the power of these capabilities, I can allocate my engineers or analysts in a more effective manner instead of allocating them on a day-to-day basis, which plays the major role.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

"The best features in SentinelOne Singularity AI SIEM include AI capabilities; they have two types of AI. First, AI is on the dashboard, which you can interact with, such as asking for logs of the last ten days, and it will provide them to you. This is one type of AI, similar to a chatbot. The other AI operates in the back end to find malware. It employs a combination of AI and ML to check for viruses or any other malicious processes, including fileless attacks.

The impression I have of the AI-driven threat detection capabilities of SentinelOne Singularity AI SIEM is that it is good and working fine, and I have never found any complaints from any customer. The dashboard is also quite simple.."

Verified user
Cyber Security Engineer at a retailer with 201-500 employees

Read full review

"I particularly appreciate a feature called Purple AI, which is an AI-based tool that allows us to fetch logs and investigate through a single prompt. It is useful for providing a brief summary of what has happened without needing to review logs in detail. Through this AI capability, we can understand exactly what has been occurring.

There is significant automation we can implement through a feature called hyper-automation. We can automate workflows easily using a drag and drop interface, rather than writing scripts. This makes automation in SentinelOne very straightforward.

I would say the quality is top-notch. It provides perfect summaries, has reduced our response time, and helps us reduce false positives. We receive mostly true positive alerts and do not need to write additional detection rules. SentinelOne Singularity AI SIEM can detect new sophisticated threats and zero-day attacks on its own without requiring rules from us. This automated detection capability is something I truly appreciate.."

Verified user

IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

"The best features of SentinelOne Singularity AI SIEM are 100% Purple AI.

In addition to that, though somewhat tedious, the implementation of any data you want is a feature of SentinelOne Singularity AI SIEM, and also the option to analyze that via Purple AI to some degree. Additionally, the existence of a large catalog of native integrations is valuable.

Overall, I would assess the overall security posture after implementing SentinelOne Singularity AI SIEM as significantly improved. We finally have visibility into things that were never visible before. When talking to new customers and onboarding them, it is always apparent that there are so many things in their environment that they never even really knew about and had no visibility into. They previously needed to go through obscure, hard-to-use, and weird tooling to potentially access this information. Having all of that in SentinelOne Singularity AI SIEM makes it so much easier.."

Fabian Brandt
IT Security Consultant at Systemhaus for you GmbH

Read full review

"SentinelOne Singularity AI SIEM improves my response time to sophisticated threats in two ways: it helps me to identify which ones I need to act on, which means I am not wasting time on the things I do not need to worry about or can be a lower priority. In that respect, it helps me to prioritize and act on what needs to be acted on first, so it brings it to the surface faster.

"Regarding AI-driven threat detection capabilities, I have a positive impression; when it is working very well, I do not really know if it is working, but when it does not work and if I have been hit by something, then I know it did not work. My SOC team seems to be utilizing it fully, and we have been kept secure and without any breach, which I think is probably the only proof we can give. The number of events and logs that it detects is numerous and very high, so it is doing its job. Fingers crossed, we do not have anything to report where we find that we have been broken into.

"SentinelOne Singularity AI SIEM's AI-powered analytics does affect our SOC's ability to reduce false positives; that is one of the biggest advantages because the manpower that I have is limited. The tool should be able to do a lot more of the first-level analysis, and what is flagged up for the man in the middle or the man to act on should be things that really need validation, meaning it has been correlated properly and brought up for visibility and action. In this manner, it is actually helping us to protect our security operations very effectively.

"It does affect my efficiency in investigating alerts and responding to incidents; we have gone to the point of using SentinelOne Singularity AI SIEM now, and our SOC is mainly dependent on SentinelOne Singularity AI SIEM. That is becoming the foundation on which all these activities and tasks are being run, and when it is all coming together, we are seeing that it is far more effective. I hope it stays that way.."

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

Read full review

Other Solutions Considered

"All other products are having the same limitations. After every quarter or every release, they are also evolving. It is not only with SentinelOne. I have also checked with Fortinet and other products from Cisco.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

"Compared to other tools we have used, such as Sumo Logic, Splunk, and CrowdStrike, those solutions do not have as much AI capability. After using SentinelOne Singularity AI SIEM, it has reduced our incident response time by forty to fifty percent compared to other tools.."

Verified user
IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

"Apart from the Harmony, I work with various CloudGuard Check Point products, and I also have a certification for SOCRADAR. I work with SOCRADAR and still have hands-on experience doing POCs and demos with SOCRADAR. I have recently done POCs or demos with SOCRADAR. We are working with an alternate solution for that, and it is a new solution.."

Verified user
Cyber Security Engineer at a retailer with 201-500 employees

Read full review

"The benefits of SentinelOne Singularity AI SIEM include that most of the customers who use it upgrade from their existing endpoint solutions. Many are using Trend Micro endpoints, Check Point endpoints, or others, and they are unhappy, especially with solutions such as Kaspersky. When they face attacks such as ransomware and are dissatisfied with their existing solutions, they switch to SentinelOne Singularity AI SIEM, which is quite good in detecting unknown threats, cleaning the system, and handling ransomware.."

Verified user
Cyber Security Engineer at a retailer with 201-500 employees

Read full review

"I can appreciate SentinelOne Singularity AI SIEM primarily for its AI capability. For this reason, we switched to SentinelOne Singularity AI SIEM. It has behavioral AI plus machine learning that has been integrated. We chose SentinelOne Singularity AI SIEM mainly because of its AI capability. It is a unified platform that provides a unified view of security alerts without requiring us to look at other data sources or switch between different tools. This has reduced the time required for faster detection and response.."

Verified user
IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

"We have looked at other XDR products, but the strength of SentinelOne Singularity AI SIEM's SIEM, their logs, the event log capture part, which can also take in logs from other non-SentinelOne entities, stands out as quite unique. The automation that is possible on the AI platform adds to that as well. When your footprint is all on SentinelOne Singularity AI SIEM in terms of VDR, then adding to that the same from the same suite is going to be helpful. At the moment, I see them as leading in their spaces.."

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

Read full review

ROI

Real user quotes about their ROI:

"SentinelOne Singularity AI SIEM has reduced our response time to true positive alerts by approximately forty percent through automation. For false positive reduction, it has decreased our false positive rate by fifty percent.."

Verified user
IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

"I have checked with Check Point and CrowdStrike when comparing competitors. This particular new AI era is new, and people are more focused on the AI part, but the outcome discussions are what matter. Because it is new technology, I do not have that much clarity on the costing front. However, this is not too expensive and it is not a white elephant. It is somewhere in the middle. If I take this trio of Check Point, SentinelOne, and CrowdStrike, SentinelOne is the most expensive among them.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

"In terms of ROI, it is hard to justify; the good thing is if there is a cost to an incident, I think we are protected. If we are not having any incidents, then it is doing its job, but I am not able to convince people about it. Overall, my perspective should be about my security budget in this space, how it benchmarks, and from that perspective, how the metrics are showing. If I am spending more compared to my peers in this space and the value that I am getting is the same as what they are getting, then I am probably overpaying. However, if I am in the middle of the park kind of range, then it is probably optimally priced. At the moment, I feel the pricing is a little bit on the higher side, but the tool is positioned in a place where risk is very high, and we do not want to take chances, so we are prepared to pay the premium.."

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

Read full review

Use Case

"For us, the use case is primarily to analyze security events that are coming in and also events that are kept over a period of time, to track and use it for investigation and maybe analysis, sometimes even forensics.."

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

Read full review

"I use SentinelOne Singularity AI SIEM for endpoint security, including EDR and SIEM-based monitoring, as well as for XDR. I monitor endpoints for security reasons and receive alerts when suspicious or malicious activity is detected. When I find anything suspicious or malicious, I investigate it further.."

Verified user
IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

"The main use cases for SentinelOne Singularity AI SIEM are endpoint protection and EDRs. When you compare the EDRs with Trend Micro and others, you will find many false positives, but SentinelOne gives you the best protection. It uses its AI to scan and find new malware, how new attackers are behaving, and addresses zero-day attacks as well. It is quite good, but the only downside is that it is costly.."

Verified user
Cyber Security Engineer at a retailer with 201-500 employees

Read full review

"I am using SentinelOne Singularity AI SIEM as a customer only, and I have taken it very recently. I am using it to get visibility of investigating my alerts based on the alert events received from my endpoints. For AI-driven applications, I want to have end-to-end visibility, which is where the observability piece comes in. I am using it primarily for the AI part, as this product will cover my real-time data detections. I am planning on implementing it for my AI-driven applications.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

"Our use case with SentinelOne Singularity AI SIEM is primarily AI observability for a large part. We are using it for SIEM purposes as well. Prior to the inclusion of Purple AI, it was exclusively SIEM.."

Fabian Brandt
IT Security Consultant at Systemhaus for you GmbH

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.

"Regarding the initial setup of SentinelOne Singularity AI SIEM, I can walk you through the deployment process: you can sync your AD, and the agent installation can also be automated. You can push it directly from your Microsoft Active Directory using GPO, which makes it easy. The agent installation can be automated, so I do not think it takes much time. However, since it is an endpoint tool, you have to consider policies for different departments, including allow lists and block lists, so deploying any endpoint does take some time.."

Verified user

Cyber Security Engineer at a retailer with 201-500 employees

Read full review

"As for maintenance required with SentinelOne Singularity AI SIEM, I would say it is even easier than the base product because you do not really onboard new data sources that often. If I put it into times a year, I would say it might be twice a year-ish that you need to do maintenance work essentially. Of course, if you want to add new detections or anything, that can be whenever, but I would not really consider that maintenance.

For others looking to implement SentinelOne Singularity AI SIEM, I would recommend starting with a proof of concept. Of course, with a SIEM that is a bit more effort to fully onboard, you might want to get an in-depth demonstration first and see if it meets your needs. Even before the demonstration, ask yourself what you even expect of a SIEM and what points you want from the solution. Once you are in the presentation, you will realize that those can very easily be met and completed with SentinelOne.."

Fabian Brandt

IT Security Consultant at Systemhaus for you GmbH

Read full review

Customer Service and Support

"As of now, I have not faced many issues with technical support from SentinelOne. They are good. I would give eight out of ten for technical support because I am not sure how other solutions work, so I will take some time to fully evaluate.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

"I would rate the technical support at eight out of ten. SentinelOne Singularity AI SIEM has AI-based technical support available. When we have questions or require documentation, we receive it promptly. The support is good.."

Verified user
IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

"My thoughts on the tech support of SentinelOne Singularity AI SIEM are that it is good and AI-based, and the documentation is also good compared to other solutions I have seen.."

Verified user
Cyber Security Engineer at a retailer with 201-500 employees

Read full review

Other Advice

"I assess the overall security posture of the company after implementation as positive; I see a big impact on that. I would rate this review as an overall eight.."

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

Read full review

"SentinelOne Singularity AI SIEM has many features, and my recommendation is to utilize all of them, but people often do not use them all. It would be helpful to automate it or use playbooks to take full advantage of the features. I rate this product a nine out of ten.."

Verified user
Cyber Security Engineer at a retailer with 201-500 employees

Read full review

"My impression of the AI-driven threat detection capabilities of SentinelOne Singularity AI SIEM is great. I am really looking forward to the upcoming feature with agentic incident investigation. If that is actually capable of autonomously investigating incidents across multiple data sources, for example, not just from SentinelOne, it will be transformative. The example I heard recently was an employee of the company opening a normal ticket just stating that their VPN connection is not working. That ticket is also made available to SentinelOne and it will then investigate what is going on with that. In the end, it turned out that this was actually an attack and that employee's VPN connection was hijacked. I am really looking forward to that feature, though it is not here yet, but even right now,

it is great.

In terms of assessing the efficiency of SentinelOne Singularity AI SIEM in improving response time to sophisticated threats, you very quickly get an overview of all data and data related to the incident. Even if there is no active incident, you can very quickly get all related information due to the Storylines and Purple AI.

SentinelOne's AI-driven analytics have affected our SOC abilities to reduce false positives, and I would say roughly about 80%.

I would rate this solution a 10 overall.."

Fabian Brandt
IT Security Consultant at Systemhaus for you GmbH

Read full review

"I would recommend SentinelOne Singularity AI SIEM to other users. Most tools do not have the same level of AI capability. SentinelOne Singularity AI SIEM has Purple AI and hyper-automation features that I can suggest to other users based on these capabilities.

SentinelOne Singularity AI SIEM has improved our SOC's efficiency in investigating alerts and responding to incidents through its AI capability. It provides us a unified view of entire alerts. We do not need to go to other data sources to understand what happened. It connects all the dots and gives us a unified alert view without requiring us to navigate to other tabs. We can see what happened from start to end. Cybersecurity and hacker tactics are constantly evolving, and we are seeing many sophisticated attacks nowadays. SentinelOne Singularity AI SIEM detects these attacks by itself without needing predefined rules, using machine learning and behavioral baselines to detect anomalies and trigger alerts. Additionally, Purple AI automatically provides a summary of incidents explaining what has happened in simple terms without requiring deep

investigation into alerts or logs. This explanation of what was abused helps us make faster decisions about whether an incident is truly a threat or a false positive alert.

SentinelOne Singularity AI SIEM has significantly impacted our security tasks and reduced manual effort. We have requirements from clients we provide services for regarding particular alerts or unreported data. We can automate notifications to the customer when these conditions occur without manually creating a ticket. SentinelOne Singularity AI SIEM can automatically notify the user. We also use it for responding to alerts. In some cases, we need to disconnect an endpoint from the network to prevent malicious activity from spreading. We use hyper-automation to automatically disconnect endpoints or remove malicious files if they are present on an endpoint.

I give this product an overall rating of eight out of ten.."

Verified user
IT Security Analyst at a tech consulting company with 11-50 employees

Read full review

Top Industries

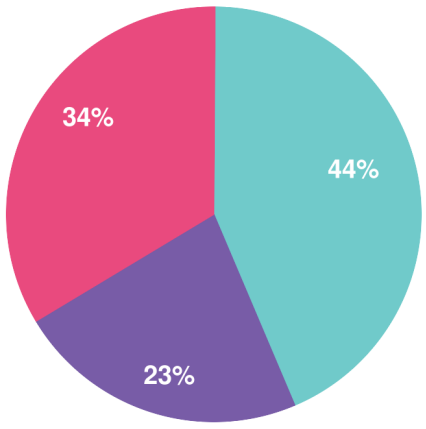
by visitors reading reviews

Construction Company	9%
Healthcare Company	8%
Comms Service Provider	8%
Financial Services Firm	7%

Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

About PeerSpot

PeerSpot is the leading review site for 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