

aws marketplace

SentinelOne Singularity Endpoint

Reviews, tips, and advice from real users



Powered by  PeerSpot



Contents

- Product Recap..... 3 - 5
- Valuable Features..... 6 - 15
- Other Solutions Considered..... 16 - 18
- ROI..... 19 - 21
- Use Case..... 22 - 26
- Setup..... 27 - 29
- Customer Service and Support..... 30 - 32
- Other Advice..... 33 - 36
- Trends..... 37 - 38
- About PeerSpot..... 39 - 40

Product Recap



SentinelOne Singularity Endpoint

SentinelOne Singularity Endpoint

Recap

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.



Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “All customers from us are very happy because the biggest difference is that SentinelOne Singularity Complete gives us the support team and the TAC team.”



Vaibhav Mahendra Kolhe

Soc Analyst at Softcell Technologies Limited

- ✓ “Since implementing SentinelOne Singularity Complete, our IT team has been able to respond to endpoint threats up to seventy percent faster compared to our previous manual process.”



Abhinandan Yadav

Network Security Engineer at Arrow PC Network Pvt Ltd

- ✓ “SentinelOne Singularity Complete has behavior-based AI that detects alerts that are not predefined without relying on predefined rules, detecting zero-day attacks or any behavioral changes in the baseline of the user or any suspicious anomalies through AI-based threat detection only.”



Verified user

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

- ✔ “SentinelOne Singularity Endpoint has positively impacted my organization by helping us achieve faster containment of endpoint threats, better visibility during investigations, and reducing reliance on traditional antivirus tools.”



Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

- ✔ “Stability-wise, SentinelOne Singularity Complete is very good, as it runs continuously, and if our endpoint is online, it will protect our endpoint 100 percent.”



Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

- ✔ “This feature is fantastic because it remediates issues while maintaining a clear audit trail, which is great for compliance.”



Daniel Giacomelli

Security and Compliance at a outsourcing company with 1,001-5,000 employees

- ✔ “The biggest benefit for my customers is that it is autonomous, where mostly everything is automated, and the threat detection, as well as auto-remediation rules, are set up.”



Krishna R

DGM. Technical Security at a tech services company with 10,001+ employees

What users had to say about valuable features:

“What I like the most about SentinelOne Singularity Complete is the rollback capability for Windows systems. The TAC team and VSS rollback are the two features I appreciate most about SentinelOne Singularity Complete.

“The response of the TAC team is very good. If SentinelOne Singularity Complete did not have a TAC team or support team, I would say it would be very lacking. When we get stuck anywhere, whether in any admin task or any threat hunting or investigation path, they are very helpful because there is a human voice on the other side helping us..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“SentinelOne Singularity Endpoint offers Storyline, which provides process visibility that is one of its strongest features. It helps me understand what happened before and after detection.

“The detailed process visibility and Storyline in SentinelOne Singularity Endpoint are very strong features that help in understanding what happened before and after detection, making process visibility the best feature I have noticed.

“I appreciate the autonomous response time in SentinelOne Singularity Endpoint. It can kill malicious processes, quarantine files, and isolate the system quickly. Additionally, behavior layer detection is not only signature-based, which is useful for known threats. The lightweight agent performs well on endpoints, resulting in better performance on endpoint systems..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“A favorite feature of mine about SentinelOne Singularity Endpoint is the VSS rollback feature, which is most valuable. If a laptop is infected with any malware, there is an option to rollback files and recover them from before the attack happened.

“Using SentinelOne Singularity Endpoint has helped me reduce alerts because it is integrated with FortiSIEM, one of the leading SIEM tools, and with SOAR technology. Whenever alerts come on SentinelOne Singularity Endpoint, they are directly raised to SOAR technology automatically. This is an automatic tool, so manual interaction is not required. All work is done by SentinelOne Singularity Endpoint, and I only have to take action on the analyst's verdict to determine if it is a true positive or false positive and investigate accordingly..”

Raj Borge

Mdr Analyst at Softcell Technologies

[Read full review](#) 

“SentinelOne Singularity Endpoint offers behavior AI detection, which is not just a normal signature thing, real-time threat blocking, automatic endpoint isolation, detailed process visibility, and easy-to-use dashboards.

“Using SentinelOne Singularity Endpoint has positively impacted my organization by significantly reducing malware infections, providing faster incident responses, and enhancing the state of our endpoints.

“SentinelOne Singularity Endpoint has helped reduce my organization's mean time to detect (MTTD) by 30 to 40%.

“SentinelOne Singularity Endpoint has improved my organization's mean time to respond (MTTR) by 30 to 40% due to its automated detection and response capabilities..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“The best feature of Singularity Platform is that everything is unified in one platform, which would be a main unique selling point for them. The unique feature is Next-Gen AV plus EDR, which detects and blocks threats in real-time.

There is a rollback feature that rolls back to the previous state if anything goes wrong after a new feature is installed or a ransomware attack occurs. Singularity XDR extends visibility beyond the endpoints and correlates how the endpoint, cloud, identity, and network help me to see a full attack chain.

The real-time personalization feature allows for customizing the detection rules and adapting security decisions based on who is doing what and where. It tracks users with behavior-based personalization, detecting abnormalities such as a non-admin gaining admin access. It also detects credential theft by correlating identity plus endpoint data for better context.

For policy personalization in my SOC, I group devices based on alert names, agent versions, or OS types, which helps significantly. I can personalize based on alert severity and true positives or false positives, leading to automated responses. A unique feature in Singularity Platform is StoryLine technology, which connects incidents into a full storyline attack.

It explains the attack pattern in a way that follows commands executed after an incident, and I can write workflows using AI, working even offline, mainly with agent-based decisions without constant cloud dependency.

I have customized dashboards for my companies, including an overview dashboard showing alerts from endpoints. I created a unified dashboard with a network and an endpoint dashboard, consolidating SOC-related unassigned alerts and daily solved alerts. I customized that dashboard myself, and it is very easy to do, being a UI-based feature.

Real-time monitoring is very helpful, helping me stay one step ahead in cybersecurity. It allows me to see exactly what is happening at this moment, and knowing about an attack immediately is better than knowing an hour or two later.

The sooner I know, the better it is for me. Real-time monitoring helps me significantly as a SOC analyst, making it one of the best features. After an alert, analyzing what happens next is just two to three clicks away, needing only to input the timeline, the query, and the affected user or endpoint..”

Verified user

Soc Analyst at a tech consulting company with 11-50 employees

[Read full review](#) 

“The best feature of SentinelOne Singularity Complete is that the console allows us to manage endpoints across multiple locations, which is critical for our distributed environment.

“What stands out most about managing endpoints across multiple locations with SentinelOne Singularity Complete is the centralized dashboard, which gives us real-time visibility into all endpoints across every location from a single console. We can see threat alerts, device status, and policy compliance, which saves a lot of time compared to managing each location separately. Additionally, the reporting capabilities are very valuable. They allow us to generate detailed audit and compliance reports quickly, track trends, and identify recurring issues. This combination of centralized monitoring and actionable reporting makes it much easier to maintain a consistent security posture across our entire environment.

“One feature I particularly appreciate about SentinelOne Singularity Complete is the AI-powered behavior detection. It can identify suspicious activity even before it is classified as malware, which adds an extra layer of proactive protection. I also appreciate how the platform automatically prioritizes threats based on the risk level, so our IT team can focus on the most critical issues first without being overwhelmed by alerts.

“SentinelOne Singularity Complete has positively impacted my organization in several ways. Improved security regarding threats such as malware, ransomware, and suspicious behavior are detected and remediated automatically, reducing the risk of breaches. Better visibility across locations is another advantage. The centralized access console and reporting give us consistent oversight of all endpoints, helping us maintain compliance and quickly respond to alerts. Increased efficiency is evident as well; automated responses and rollback capabilities save our IT team significant time that would otherwise be spent manually investigating and resolving incidents.

“Since implementing SentinelOne Singularity Complete, our IT team has been able to respond to endpoint threats up to seventy percent faster compared to our previous manual process. Incidents that used to take hours to investigate and remediate now often get resolved within minutes, thanks to automated detection, containment, and rollback. Additionally, we have reduced endpoint downtime by

approximately sixty percent, minimizing disruption for our users..”

Abhinandan Yadav

Network Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

Other Solutions Considered

“I would give SentinelOne Singularity Complete a rating of 10 out of 10 because you can compare it with CrowdStrike, and I can say that SentinelOne Singularity Complete is top tier..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“I have previously used CrowdStrike. I can say SentinelOne Singularity Complete is better than CrowdStrike because it is more AI-capable and integrated. It gives us alerts based on behavior using the AI. In this aspect, I have only used CrowdStrike as an EDR, and I can rate SentinelOne as better than CrowdStrike..”

Verified user

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

[Read full review](#) 

“We are using CrowdStrike, and in CrowdStrike, we are using Charlotte AI. If we raise a ticket on the community portal, within one or two hours, we get a reply from the team, and they are very helpful and can also come to the call. However, with CrowdStrike, I do not prefer it from my perspective as compared to SentinelOne Singularity Complete..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“Before choosing SentinelOne Singularity Endpoint, I evaluated other options like Microsoft Defender for Endpoint and CrowdStrike Falcon. However, I selected SentinelOne mainly because of its strong behavioral AI-based detection and automated response..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“I would choose SentinelOne Singularity Endpoint. In Symantec AV, there is only signature-based and behavior-based threat detection, whereas SentinelOne Singularity Endpoint has advanced behavior AI and pre-static AI. In Symantec AV, alerts must be manually raised and actions taken on the endpoint, but SentinelOne Singularity Endpoint has fully automated AI. The use cases are moderate in Symantec AV, but SentinelOne Singularity Endpoint is very easy with a modern UI. I prefer SentinelOne Singularity Endpoint because I have worked with both..”

Raj Borge

Mdr Analyst at Softcell Technologies

[Read full review](#) 

“Before choosing SentinelOne Singularity Complete, we evaluated multiple options such as CrowdStrike Falcon, Microsoft Defender for Endpoint, and other EDR solutions. We conducted a proof of concept phase to see which aligned best with our security requirements and operational workflow before committing to SentinelOne Singularity Complete..”

Abhinandan Yadav

Network Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen a return on investment with SentinelOne Singularity Endpoint, as it reduces incident impact, leads to faster responses and detections, reduces less manual remediation, and improves analyst productivity..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“I can say that when an alert comes, we already have the protect policy and protect mode. After applying the protect policy, everything is taken care of by SentinelOne Singularity Complete..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“Singularity Platform does bring a good return on investment. First, proofs of concept are shown for the two EDRs, comparing what they offer. Large enterprises that can afford it often choose SentinelOne for its ease of management compared to other platforms..”

Kandregula Sathvik

Security Engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“I have seen a return on investment with SentinelOne Singularity Complete solution, as it is very easy to understand and functions through one unified agent managing the cloud, SIEM, and EDR solutions..”

Divya More

Technical Support at Softcell Technologies Limited

[Read full review](#) 

“SentinelOne Singularity Endpoint reduces the time of SOC employees, providing a return on investment.

“SentinelOne Singularity Endpoint has freed up my staff for other projects and tasks, reducing their workload by about 40 to 60% due to its main detection and investigation capabilities..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“I have seen a return on investment with SentinelOne Singularity Complete. Automatically detecting, remediating, and rolling back threats has reduced manual investigation by approximately sixty to seventy percent, allowing IT teams to reduce mean time to respond and mean time to detect, with mean time to detect improved by sixty to seventy percent. Resource efficiency is also enhanced; the platform's automation has enabled a smaller team to manage a larger number of endpoints without compromising security. Downtime is reduced by sixty percent. Overall, the solution delivers seamless operation, improved threat management, and cost-effective security, making a strong investment in our organization..”

Abhinandan Yadav

Network Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

Use Case

“My main use case for SentinelOne Singularity Endpoint is to work in our environment mainly for endpoint protection, threat detection, response, monitoring and suspicious process, and investigating the alerts..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“SentinelOne Singularity Endpoint is used for endpoint security to detect, prevent, and respond to cyber threats in real time. Using AI-based behavior analysis, it helps the SOC team to investigate incidents, automate responses and actions, and protect systems from malware and ransomware. SentinelOne Singularity Endpoint includes EDR, XDR, and NGAV..”

Raj Borge

Mdr Analyst at Softcell Technologies


[Read full review](#) 

“My main use case for SentinelOne Singularity Endpoint is endpoint protection, threat detection, incident response, and visibility across user systems and servers. I primarily use it for malware and ransomware detection, suspicious process monitoring, automated remediations, endpoint isolations, threat hunting, and root cause analysis using Storyline. SentinelOne Singularity Endpoint has AI-powered EPP and EDR with autonomous responses, making these the best use cases that I have used day-to-day for the past two years.

“The endpoint isolation and threat hunting capabilities of SentinelOne Singularity Endpoint stand out as the most valuable for my team because we rely on them the most on a daily basis..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“I use Singularity Platform as a SIEM across many infrastructures, including cloud and on-premises environments, to detect attacks on endpoints, cloud workloads, identities such as Active Directory, and network signals.

Singularity Platform is used to detect, investigate, and respond to threats all in one platform, which is why it is called Singularity Platform, because it has EDR, XDR, and cloud security all unified in one system.

I use fraud detection while working with financial companies and many fintech companies. Although SentinelOne is not known for fraud detection, it does detect stolen credentials, accounts that have been misused, or privilege abuse. I use it to a certain extent, but I cannot provide a deep-dive analysis on it today as I am fatigued from working through the night.

In my organization, I have around ten clients, of which six use SentinelOne as a SIEM, mainly financial companies, with one being a shopping-based company. I cannot provide all client details, but that is the general overview..”

Verified user

[Read full review](#) 

Soc Analyst at a tech consulting company with 11-50 employees

“My main use case for SentinelOne Singularity Complete is for endpoint protection, threat detection, and automated response across all our corporate devices. Day-to-day, it is used to monitor endpoints in real time for malware, ransomware, and other threats. Automatically remediating detected threats and performing rollbacks when necessary allows us to maintain visibility into security events through the management console. Additionally, it supports our IT team with alerts and actionable reports for faster incident response.

“A recent incident illustrates how we use it in our environment. Recently, one of our endpoints was targeted by a ransomware variant. SentinelOne Singularity Complete immediately detected the suspicious behavior, quarantined the affected files, and automatically rolled back the changes to restore the system to its previous state. This prevented any data loss and allowed the user to continue working without downtime. The alert also provided our IT team with detailed insights, helping us quickly understand the scope of the incident and ensure no other devices were affected.

“We rely on SentinelOne Singularity Complete not only for malware and ransomware protection, but also for behavior-based threat detection, which can catch unusual activity that traditional antivirus might miss. It helps us maintain compliance by generating audit-ready security reports for management..”

Abhinandan Yadav

Network Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“My use cases for SentinelOne Singularity Complete are mainly for endpoint security to detect, prevent, and respond to cyber threats in real time. SentinelOne Singularity Complete serves as the first use case for endpoint security.

“Our organization does not have the Ranger functionality because our customer does not require it.

“We have integrated SentinelOne Singularity Complete with Shuffle SOAR technology, which is a most powerful tool.

“Our organization is an MSSP provider with 10+ customers for whom we are providing security. We have 8,000 endpoints installed for our customers, and we are a 24/7 team providing security to our clients.

“We have applied the protect policy and take basic analysis, which takes a couple of minutes before we raise the alert.

“Regarding Purple AI, we are using it to identify the IOC. We have limited access to Purple AI, but we are using it for threat hunting purposes to find the IOCs..”

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.

“For the initial deployment of SentinelOne Singularity Complete, I can say that it is very easy. We just need to create one tenant for the SentinelOne Singularity Complete platform. SentinelOne Singularity Complete setup is very easy..”

Dev Reshwal

[Read full review](#) 

Technical Support Executive at Softcell Technologies Limited

“Deployment of SentinelOne Singularity Complete is easy. Installing agents is straightforward. We can do it using Active Directory and group policies. It is easy to install agents in endpoints..”

Verified user

[Read full review](#) 

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

“The deployment of SentinelOne Singularity Complete was straightforward and easy. It took approximately one day to implement SentinelOne Singularity Complete, based on the number of clients we had..”

Verified user

[Read full review](#) 

Technical Account Manager at a computer software company with 11-50 employees

“The initial setup process for Singularity Platform is straightforward across all three platforms—Mac, Linux, and Windows—and doesn't require any prerequisites. It is a very lightweight agent, and the setup is easy to handle..”

Kandregula Sathvik

[Read full review](#) 

Security Engineer at a tech vendor with 11-50 employees

“The initial deployment of SentinelOne Singularity Endpoint is easy and very straightforward. All that is needed is to set up a tenant and create a package file. Once installed, it automatically connects to the management console, and the entire system can be set up in one or two hours..”

Raj Borge

[Read full review](#) 

Mdr Analyst at Softcell Technologies

“Regarding the initial setup, I can say it is very easy to set up. We just need to create one tenant from my customer name and send and install the packets for Mac OS, Windows, and Linux servers. We take remote access, and within 5 to 10 minutes, one endpoint will be installed, although it takes some time to connect to the dashboard. The setup is very straightforward, and we have installed over 500 agents in one day. That is a very fast process we have accomplished..”

Vaibhav Mahendra Kolhe

Soc Analyst at Softcell Technologies Limited

[Read full review](#) 

Customer Service and Support

“Technical support is good. I would rate it 8 out of 10 because there is a feature of AI support. If we require any help with documentation, we receive it immediately. With a single prompt, we receive help with documentation, and those documentations are very clear..”

Verified user

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

[Read full review](#) 

“I evaluate the customer service and technical support of SentinelOne Singularity Complete as very supportive, with fast response times.

I have seen improvements in meantime to detect and respond, with detection times being very good, less than 15 minutes or even less than 10 minutes. .”

Divya More

Technical Support at Softcell Technologies Limited

[Read full review](#) 

“Regarding the technical support and customer service teams, I rate them 10 out of 10 on a scale of 1 to 10. The TAC team, which is available 24/7, is the reason for this rating. We are now in India, but if we get stuck at midnight, any other TAC team will be in GMT or Europe or America, and they will assign our support engineer and suddenly schedule a call for us and resolve the issue. The TAC team plays a major role and is very important for us..”

Vaibhav Mahendra Kolhe

Soc Analyst at Softcell Technologies Limited

[Read full review](#) 

“I have contacted the technical support or customer support, and this is the most significant reason we are using SentinelOne Singularity Complete. They are very helpful because there is a human voice on the other side helping us.

“If you compare with CrowdStrike, our organization has shifted to SentinelOne Singularity Complete only because of that TAC team or support team..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“Experience with customer service and technical support has been primarily with tech support because, during the initial configuration time, there were many doubts. Tech support was mostly used, while customer service has not needed to be contacted. Direct contacts for technical support were available.

On a scale of one to ten, the technical support of SentinelOne would be rated as an 8.5..”

Kandregula Sathvik

Security Engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“Whenever I get stuck on any alert with SentinelOne Singularity Endpoint and do not understand it, or when I face any admin task challenges, I manually open a ticket with the customer team. Every time they help regarding the case. Each day, if I get stuck anywhere in SentinelOne Singularity Endpoint, whether with any admin task or threat hunting, the tech team or support team will surely help.

“For the support team of SentinelOne Singularity Endpoint, I would rate them nine out of ten because there is a human voice there, so they are listening and responsive..”

Raj Borge

Mdr Analyst at Softcell Technologies

[Read full review](#) 

Other Advice

“We are managing 7,000 to 8,000 endpoints for clients, and the setup is very easy. I have given SentinelOne Singularity Complete an overall review rating of 10 out of 10..”

Dev Reshwal

Technical Support Executive at Softcell Technologies Limited

[Read full review](#) 

“The mean time to detect with SentinelOne Singularity Endpoint is very low. The mean time to respond for SentinelOne Singularity Endpoint is approximately two to three minutes since it is integrated with SOAR, and alerts are raised within that timeframe. From endpoint to console, alerts are received in real time with no lagging. SentinelOne Singularity Endpoint requires no maintenance. Since we have a partnership with the SentinelOne Singularity Endpoint team and are an [MSSP](#) provider, no maintenance is required. My overall rating for this review is eight out of ten..”

Raj Borge

Mdr Analyst at Softcell Technologies

[Read full review](#) 

“Singularity Platform requires maintenance, which is typically done on weekends. Although there was a maintenance window recently, it is almost acceptable, but technical issues can cause lag or latency, which is common in upgrades. They can improve by utilizing a backup or other measures.

I recommend Singularity Platform because of features such as the StoryLine model, [Purple AI](#), and automating workflows with hyper-automation capabilities. I would hesitate to recommend it solely due to reliability issues..”

Verified user

Soc Analyst at a tech consulting company with 11-50 employees

[Read full review](#) 

“I rate the customer support for SentinelOne Singularity Endpoint a perfect 10 out of 10.

“If any organization is battling with strong endpoint security and seeking faster detection and response, SentinelOne is a very good choice.

“SentinelOne Singularity Endpoint sometimes generates false positives, which they can work on. Additionally, the user interface can be improved, and more detailed reports could help further.

“My overall review rating for SentinelOne Singularity Endpoint is 8.5 out of 10..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“SentinelOne Singularity Endpoint Complete has helped me consolidate my security solutions.

“SentinelOne Singularity Endpoint Complete has helped free up my staff for other projects and tasks, saving around 25 to 40 percent of their time.

“It has also helped reduce my organization's Mean Time to Respond by about 25 to 30 percent.

“SentinelOne Singularity Endpoint Complete has helped reduce alerts by around 20 to 25 percent.

“One real case I handled involved a suspicious PowerShell execution on a user endpoint. SentinelOne Singularity Endpoint generated a behavior alert because the script tried to download content and spawn an additional response. I checked the process tree, parent-child relationship, command line activity, and network behavior using the console. I isolated the machine immediately after removing the threat, and what I appreciated was how quickly the investigation proceeded because the most required details were already available in one place.

“Based on my experience, SentinelOne Singularity Endpoint Complete easily reduces alert fatigue by reducing alerts by around 20 to 25 percent. I would rate this product at 8.5 out of 10..”

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

[Read full review](#) 

“In our environment, we do use [Purple AI](#) as part of SentinelOne Singularity Complete to help with threat analysis, investigation workflows, and speeding up the incident triage. [Purple AI](#) acts as an AI-powered security analyst, helping translate complex data into actionable insights and enabling faster threat hunting and investigation across our endpoint security data.

“Purple AI plays a critical role in amplifying our team knowledge by helping us interpret alerts, investigate threats, and identify patterns across endpoints quickly. It essentially amplifies our team's knowledge by providing contextual insights, suggesting remediation steps, and correlating between security events that might otherwise be missed.

“SentinelOne Singularity Complete has significantly reduced the number of alerts our IT team has to handle manually. By leveraging AI-driven behavior analysis and automated threat automation, low-risk or duplicate alerts are filtered out,

allowing the team to focus on the most critical incidents. In our experience, the platform has reduced actionable alerts by fifty to sixty percent.

“SentinelOne Singularity Complete has significantly reduced our organization's mean time to detect. With real-time AI-driven detection, automatic alerts, and behavioral analysis, threats are identified almost immediately upon occurrence. In our environment, we have observed that mean time to detect has improved by approximately sixty to seventy percent, meaning our IT team can detect and respond to incidents much faster than before. The rapid detection has been critical in preventing escalation and minimizing potential impact on end-user systems.

“SentinelOne Singularity Complete has significantly reduced our organization's mean time to respond, thanks to automated remediation, rollback capabilities, and prioritized alerts. Our IT team can respond to incidents almost immediately. Mean time to respond has been reduced by approximately sixty-two percent, allowing threats to be contained and resolved in minutes rather than hours.

“For others looking into using SentinelOne Singularity Complete, I advise utilizing the Purple AI summarization. The alert without much manual investigation allows us to determine if it is a true positive or not by seeing the Purple AI alert summarization, what happened, what process, activity, and what the underlying behavior is. Overall, SentinelOne Singularity Complete is highly effective, but organizations get the most value when they combine automation, AI, incident, and proactive management. Regularly reviewing the report with audit features is valuable for complete tracking of trends. Utilize the AI-driven insight to amplify your team knowledge and reduce alert fatigue. Planning for deployment across sites if you have multiple locations is essential, as is planning your policy and endpoint coverage for centralized management. I rate this solution a nine out of ten..”

Abhinandan Yadav

Network Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

Top Industries

by visitors reading reviews

Computer Software Company

11%

Manufacturing Company

8%

Financial Services Firm

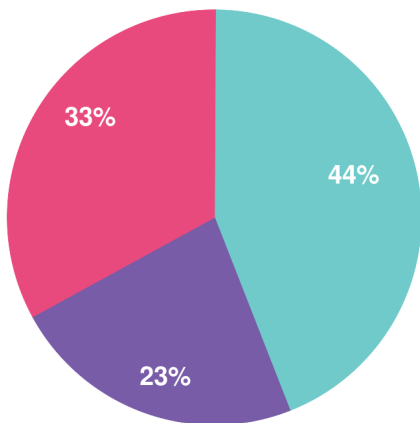
8%

Government

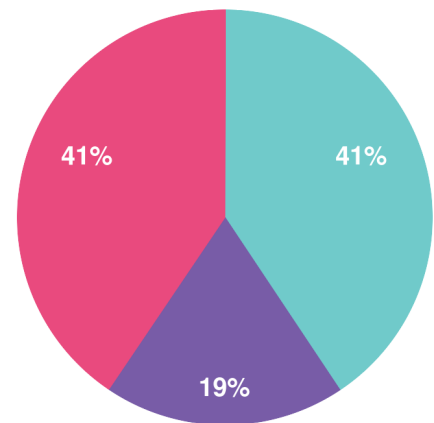
6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise

Midsize Enterprise

Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944