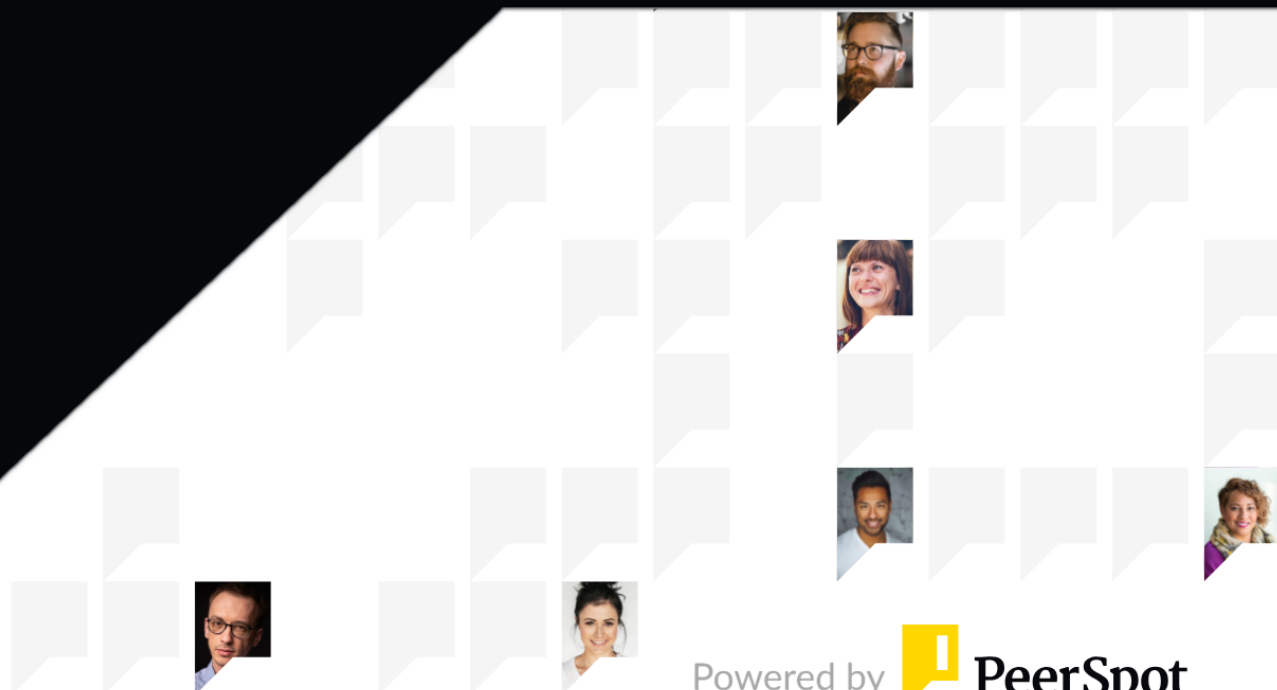




SentinelOne Singularity Endpoint

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 14

Other Solutions Considered..... 15 - 16

ROI..... 17 - 19

Use Case..... 20 - 24

Setup..... 25 - 27

Customer Service and Support..... 28 - 30

Other Advice..... 31 - 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



“I think that is where SentinelOne Singularity Endpoint stands out; they are doing quite great there, and at the same time, the Purple AI feature is much better.”



Ravishankar KumarPatel

Solution Architect Cybersecurity at Microland Limited



“For mean time to detect, it has improved by 50%, and mean time to respond is now reduced by 40%.”



Sandesh Khatal

Soc Analyst at Softcell Technologies Limited

- ✓ “SentinelOne Singularity Endpoint helps reduce alerts by approximately 40%, as it streamlines the analysis process for alerts we receive, and it helps free up about 70 to 80% of our time when managing alerts.”



SameerJadhav

SOC Analyst at Softcell Technologies Limited

- ✓ “Overall, our experience with SentinelOne Singularity Endpoint has been very positive; the combination of MDR and endpoint protection significantly strengthens our security posture, especially as we grow as a small to medium business in the energy sector and battery manufacturing.”



Viral Shaa

IT Security Analyst at Eos Energy Enterprises, Inc.

- ✓ “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

- ✓ “Regarding return on investment, from a security perspective, SentinelOne Singularity Endpoint covers your endpoint security effectively, it is very cost-effective, and while we provide services to our customers, the ROI is very great because we are getting returns from what we earn by selling the product.”



Subodh Desai

SOC Analyst at Softcell Technologies

What users had to say about valuable features:

“Storyline eliminates the single biggest bottleneck in incident response: manual event correlation. Without Storyline, investigating any EDR alert requires pulling raw logs, matching process IDs that Windows recycles, cross-referencing timestamps, and manually stringing together command line executions, registry changes, and network connections. Storyline does this automatically on the agent by assigning a unique Storyline ID to the entire execution chain in real time.

The most important thing about SentinelOne Singularity Endpoint is the behavioral AI engine, both static and dynamic, along with Storyline technology. During a security incident, raw events and logs from Windows and/or Linux quickly cause analyst fatigue. SentinelOne automatically correlates all execution trees, registry, network sockets, and file writes under a single deterministic Storyline ID. We do not have to spend more time manually linking event IDs together. Clicking a Storyline visually outlines the entire attack chain from initial drop to execution attempt..”

Gokhany Gokhany

Cyber Security Consultant at Bkl Bilişim Teknolojileri Yazılım Danışmanlık Eğitim Tic Ltd Şti

[Read full review](#)

“The best features SentinelOne Singularity Endpoint offers include the ability to remotely scan computers with the current latest and greatest holistic software without downloading the newest agent to scan the system. I can scan a system remotely against the most recent signature database and updated definitions with holistic analysis of the application in a pinch. I can also remotely deploy and remotely update agents as needed, which is a really good feature to have.

“I find myself using the remote scan and update feature constantly. When I work in IT, we get calls all the time from end users about clicking on suspicious links or emails, and being able to simply execute a remote scan on demand is extremely helpful.

“SentinelOne Singularity Endpoint has helped reduce my organization's mean time to detect. Overall, it protects you instantly based on a user doing something they probably should not be doing and opening an application they should not have, and it usually gets stopped right then and there..”

C Benson

Infrastructure And Systems Administrator

[Read full review](#) 

“The recent feature is the Prompt AI. Using that Prompt AI feature, we can get queries to build a quick summary. We can build a query using natural language processing, which means plain English text, and it gives the query accordingly, and it is going to be useful for us to threat hunt and actively identify threats. That is a good feature. The other additional feature is retrieving the files from the computer even though the machine is isolated through the shell. These are pretty good features that I have found useful.

“It actively monitors the endpoints for any threats. There is no such EDR that could actively block any kind of threat in the world.

“It consolidates the vulnerability management side by actively identifying the risk applications that have been running in the endpoints. We can do the threat hunting through the log collections from the endpoints and then actively write a query to identify the threat that has been running in the environment. It also does the network scanning and also a bit of the VSS management. We can manage the VSS backups as well, handling the VSS snapshot backups through that. It has been a pretty good product, and it could have more capabilities or additional capabilities as well..”

Verified user

[Read full review](#) 

Network Security Administrator at a energy/utilities company with 51-200 employees

“My main use of SentinelOne Singularity Endpoint in my organization is to protect all of our endpoints, including our Kubernetes pods, our users' workstations, our Windows and Linux servers.

“The tool offers Star Custom Rules. These rules actually allow you to customize detections based on the information system.

“In my opinion, the best features that SentinelOne Singularity Endpoint offers my organization are, first, the Star Custom Rule component, which allows you to customize things based on the IS and the endpoints targeted by attacks. There is also the remediation component, which allows you to roll back based on the malicious actions that have been carried out on a workstation.

“Another particularly useful aspect of SentinelOne Singularity Endpoint is the Deep Visibility component, which logs all system actions on the machines. This allows you to do forensics if needed or to really understand what happened on the endpoint..”

Verified user

[Read full review](#) 

ingénieur systèmes et sécurité at a financial services firm with 201-500 employees

“The best features that SentinelOne Singularity Endpoint offers include the EDR visibility. It helps me understand which kind of operation Picus has done on the system, the timeline, the process tree, and which kind of command has been executed. Thanks to that, we can write the proper exclusions or write the proper security tightening rules. The visibility provided by SentinelOne Singularity Endpoint is the best part.

“On the integration side, we integrate SentinelOne Singularity Endpoint with Picus to collect the logs from the host where SentinelOne Singularity Endpoint is installed. We can collect the logs and the alerts related to the specific machines. In different products, we can see some delay on the ingestion time. After a couple of attacks, sometimes we lose some of the logs because the security solution only logs a couple of the attacks but not all of them. However, we did not encounter this issue on SentinelOne Singularity Endpoint. Each time we can access all the logs created by Picus itself, which means SentinelOne Singularity Endpoint does not miss the logs. We also did not encounter any ingestion time delay issues on SentinelOne Singularity Endpoint. In some other products, we can encounter logs that have been created after the attacks have been finished, long after the fact. We did not encounter this issue on SentinelOne Singularity Endpoint. I can conclude that SentinelOne Singularity Endpoint is good at logging and alerting.

“SentinelOne Singularity Endpoint has positively impacted our organization in that we do not use SentinelOne Singularity Endpoint in the whole company. We are only using SentinelOne Singularity Endpoint on the lab environments to validate the Picus attacks. Based on our experience, SentinelOne Singularity Endpoint's score is high when I compare it with well-known EDR solutions. I can say that SentinelOne Singularity Endpoint is one of the good products..”

Onur Pınargözü

Expert TAC Engineer at a tech vendor with 201-500 employees

[Read full review](#) 

“I have had multiple cases where end users fell victim to phishing emails or visited the wrong link. The EDR solution from SentinelOne was able to mitigate the potential threat, which protected not only the end user but also the company. This has also happened on servers. I have seen servers exposed to the Internet that had advanced threat actors trying to get into our networks, and SentinelOne's EDR solution has been able to mitigate such attacks and in some cases perform rollbacks. We also receive notifications via email and in some cases messages, which helps us stay on top of things and makes troubleshooting much easier. SentinelOne performs the mitigation on its own, which allows me to have peace of mind. Security is not absolute, and something else will happen, but from my experience, I am able to rely on the solution and know that it is going to do what it is supposed to do. Beyond protecting the endpoint, the autonomous response capability allows remediation of threats at machine speed without my intervention. The solution just does it on its own.

“Today, I use SentinelOne for EDR, but we also use it for XDR. We are able to do assessments against our on-premise Active Directory as well as Azure, Microsoft Defender, and Exchange. We are collecting logs from our Azure enter ID, which gives me visibility that is sometimes difficult to find in the Microsoft 365 suite of tools. Being able to go into the SentinelOne Singularity Endpoint console and narrow down to the main events happening across the different platforms that we use makes things much easier, allowing me to be aware of what is happening and to triage items when needed. Having the complete SentinelOne Singularity Endpoint solution, not just with endpoint security but also with identity protection, makes my job much easier. If I had to do this manually, it would take a long time. Having the thermal response, behavioral AI, identity assessment, and the ability to stop potential lateral movements is a significant help.

“SentinelOne Singularity Endpoint offers many features. I really appreciate what EDR is able to do, not only on the antivirus side. Having a single agent on an endpoint gives me the ability to handle multiple potential threat vectors. Instead of having multiple agents doing different things, SentinelOne Singularity Endpoint agent handles the antivirus side, endpoint protection, and with the behavioral side using AI, it is able to learn, see suspicious activities, track them, and isolate potential compromised devices automatically. When looking at our

Active Directory, it has been able to do assessments and provide what the threat is using things such as MITRE, along with solutions on how to fix it. There is not one feature in particular; it is looking at it holistically and seeing how we can protect our premises not just from the endpoint but also from an identity perspective. Both complement one another.

“On the behavioral AI, it is learning about our platforms and how they behave. We have multiple systems, some of which are exposed to the Internet because that is where our website is or where platforms multiple users use that are public facing. The behavioral AI is able to learn what a system is supposed to do, and if it notices something different, it tells us about it. Simple things such as if I remotely access a device and begin using PowerShell, in some cases it will alert me and say this activity does not look normal. The behavioral AI is able to see potential activity that is just not normal, create a baseline, and act upon it..”

Adan Mendoza

Cybersecurity Analyst at a non-profit with 10,001+ employees

[Read full review](#) 

Other Solutions Considered

“Before choosing SentinelOne Singularity Endpoint, it was the main one we evaluated; we also looked at HarfangLab, but the cost was significantly higher for minimal gains..”

Verified user

ingénieur systèmes et sécurité at a financial services firm with 201-500 employees

[Read full review](#) 

“Before choosing SentinelOne Singularity Endpoint, we evaluated SentinelOne and CrowdStrike, but it really depends on the customer's needs; overall, SentinelOne Singularity Endpoint is our go-to..”

Shaun Washington

SOC Analyst II at a computer software company with 51-200 employees

[Read full review](#) 

“I did not previously switch from a different solution. We just added it for some clients, depending on what they wanted, but I was using CrowdStrike and Microsoft XDR as well..”

Verified user

2nd Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“I can use CrowdStrike Falcon because CrowdStrike relies heavily on cloud processing for advanced behavior detection and lacks an equivalent to SentinelOne's native on-device Volume Shadow Copy rollback. SentinelOne's ability to defend offline machines autonomously and restore encrypted files locally was a key differentiator..”

Gokhany Gokhany

Cyber Security Consultant at Bkl Bilişim Teknolojileri Yazılım Danışmanlık Eğitim Tic Ltd Şti

[Read full review](#) 

“I was working at a company that was already using CrowdStrike Falcon, so it was not that we switched or that I stopped using SentinelOne. It is just that CrowdStrike Falcon was what was given to me, and that is what I had to use..”

C Benson

Infrastructure And Systems Administrator

[Read full review](#) 

“For the current company I am working with, they had no EDR solutions. My recommendation was to deploy SentinelOne Singularity Endpoint as the EDR solution. At my previous company, we replaced CarbonBlack. I made a recommendation to replace CarbonBlack with SentinelOne Singularity Endpoint because of the functionality, being able to have antivirus and protect the endpoint using EDR as well as the AI side of things, including identity..”

Adan Mendoza

Cybersecurity Analyst at a non-profit with 10,001+ employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I believe I have seen a return on investment from using SentinelOne Singularity Endpoint, though I am not sure and was not involved in prices. I guess it helps..”

Verified user

2nd Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“In the sense that we have not experienced any major incidents of infection, this demonstrates a return on investment for SentinelOne Singularity Endpoint..”

Michael Streaker

Senior Engineer - Cybersecurity at a comms service provider with 11-50 employees

[Read full review](#) 

“The biggest benefit that SentinelOne would provide in this case is simply reputation. Because of how well SentinelOne is as a product, if a company or an MSP rolls out with it, you know you are secure and can feel confident in that. That is to me the biggest benefit that SentinelOne can offer..”

C Benson

Infrastructure And Systems Administrator

[Read full review](#) 

“SentinelOne Singularity Endpoint really reduced the number of threats. SentinelOne Singularity Endpoint reduced our MTTD by roughly forty percent. It reduced our MTTR by roughly thirty percent, depending on which business unit you are dealing with because some business units do not even have any cyber expert, making the alerts more complex to handle..”

Verified user

[Read full review](#) 

Responsible Programme Cybersécurité at a retailer with 10,001+ employees

“I do not have metrics as to how much time the solution has saved me, but I can give an example from my experience. I go to work in the morning and take a look at the platform for ten to fifteen minutes, then maybe during lunch and before I clock out. I do not have to spend a lot of time on the platform. If something happens, I get a notification or an alert about the incident. For the most part, we are not spending a lot of time looking at things. We know that if something happens, we are going to be notified..”

Adan Mendoza

[Read full review](#) 

Cybersecurity Analyst at a non-profit with 10,001+ employees

“In an enterprise retail and distribution environment, the measurable impact of SentinelOne Singularity Endpoint comes down to four operational metrics. I observed a seventy to eighty percent reduction in mean time to respond, a ninety percent decrease in physical on-site IT dispatches, a sixty percent reduction in alert fatigue, and zero dwell time gap for offline store operations.

With traditional EDR, we spent approximately forty-five minutes on mean time to respond. Since implementing SentinelOne Singularity Endpoint, we accomplish this in five minutes. Traditional EDR vendors spend three or four hours on recovery time, but with SentinelOne, rollback is very quick..”

Gokhany Gokhany

Cyber Security Consultant at Bkl Bilişim Teknolojileri Yazılım Danışmanlık Eğitim Tic Ltd Şti

[Read full review](#) 

Use Case

“My main use case for SentinelOne Singularity Endpoint is whitelisting applications. I use whitelisting for different domains, file paths, executables, and disabling snapshots..”

C Benson

Infrastructure And Systems Administrator

[Read full review](#) 

“My main use case is to protect the endpoints. Back in 2020, I conducted multiple proofs of value for different vendors, including SentinelOne. At the end of my evaluation, SentinelOne was the solution that provided a better fit for what we needed to do, and it was one of the best solutions, not just in terms of doing what it was supposed to do, but also in terms of cost. The end goal was to protect the endpoints, including Windows, Linux, and MacOS systems, as well as Windows servers and cell phones..”

Adan Mendoza

Cybersecurity Analyst at a non-profit with 10,001+ employees

[Read full review](#) 

“My main use case for SentinelOne Singularity Endpoint is running the Picos Breach and Attack Simulation tool in our lab environment. After performing attacks on specific EDR tools, we understand which tools require which kind of exclusions to complete the attacks properly. We also determine how we can tighten the security policy, what kind of rules we can add, or which options we can tighten. After the prevention section, we can integrate with the API endpoint on SentinelOne Singularity Endpoint, and thanks to that, we can also fetch some logs and validate the operation in the detection side..”

Onur Pınargözü

Expert TAC Engineer at a tech vendor with 201-500 employees

[Read full review](#) 

“My main use of SentinelOne Singularity Endpoint in my organization is to protect all of our endpoints, including our Kubernetes pods, our users' workstations, our Windows and Linux servers.

“A concrete example of how I use SentinelOne Singularity Endpoint in my daily work is that the main tasks are to clear doubts on alerts related to threats. The majority of the time, approximately 90% of alerts turn out to be false positives, but the AI model learns relatively quickly and after two years, we no longer have to clear that many false positives.

“Regarding rule customization and the remediation feature, these aspects concretely make my security management easier on a daily basis. The custom rules can allow you to reach a level similar to AppLocker. We use them to monitor everything that happens in certain user folders and to enable detection of unauthorized applications..”

Verified user

ingénieur systèmes et sécurité at a financial services firm with 201-500 employees

[Read full review](#) 

“SentinelOne Singularity Endpoint actively monitors endpoints continuously whenever there is activity, and then correlates the events accordingly, and flags threats using a storyline.

“It actively detects and monitors if anything suspicious happens on the endpoint, and then actively blocks it and raises an incident alert for the security team to review.

“There was a recent incident where there was a modification of a VSS backup on a server endpoint. SentinelOne Singularity Endpoint actively detected that modification and raised an alert with us, and we quickly reviewed it. Although it was a false positive, it was a legitimate application that was trying to modify the VSS backup and delete and take a fresh backup from scratch. However, SentinelOne Singularity Endpoint actively monitored it and flagged it as suspicious activity. Though it was a false positive, the underlying activity was detected correctly.

“Whenever it detects threats, it helps us respond to threats quickly because the EDR actively monitors the threat and blocks it. When there was suspicious activity at three o'clock in the night, SentinelOne Singularity Endpoint does not require active monitoring of the alert by the team. In that scenario, there could be a lot happening by the time when we see the alert, and the latent moment might have occurred since the start of the attack. SentinelOne Singularity Endpoint actively monitors the threat and then blocks the threat if any other suspicious attributes are being shown as part of the attack. This is the feature that I appreciate about SentinelOne Singularity Endpoint; it actively blocks the threat and once it blocks the thread, we can review it later on and look for more details, and we can unquarantine the thread if we feel it is a false positive, or we can take action accordingly. It actively blocks the threat from moving laterally..”

Verified user[Read full review](#) 

Network Security Administrator at a energy/utilities company with 51-200 employees

“A user in finance opens a macro enabled Word document disguised as a vendor invoice. No traditional malware executable .exe is saved to disk, so standard virus scans pass without a hit. In this case, the Word macro launches PowerShell with a base64-encoded command designed to download the secondary payload directly into system memory. SentinelOne does not wait for a known signature. Its agent recognizes anomalous process lineage. Before the scripts can establish a command and control connection to exfiltrate data or pull down ransomware, the local SentinelOne agent immediately terminates the execution tree.

Storyline eliminates the single biggest bottleneck in incident response: manual event correlation. Without Storyline, investigating any EDR alert requires pulling raw logs, matching process IDs that Windows recycles, cross-referencing timestamps, and manually stringing together command line executions, registry changes, and network connections. Storyline does this automatically on the agent by assigning a unique Storyline ID to the entire execution chain in real time.

The most important thing about SentinelOne Singularity Endpoint is the behavioral AI engine, both static and dynamic, along with Storyline technology. During a security incident, raw events and logs from Windows and/or Linux quickly cause analyst fatigue. SentinelOne automatically correlates all execution trees, registry, network sockets, and file writes under a single deterministic Storyline ID. We do not have to spend more time manually linking event IDs together. Clicking a Storyline visually outlines the entire attack chain from initial drop to execution attempt.

In large scale retail environments, endpoint POS or back-office system downtime directly translates to customer friction and lost revenue. SentinelOne impacts traditional antivirus solutions that often trigger heavy disk scans that degrade POS performance or generate false positives that lock down systems. SentinelOne's lightweight local agent operates with minimal overhead without impacting cashier or store operations. The business outcome is that threats are localized and contained at the operating system level without locking down the device, ensuring uninterrupted store sales..”

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 deployment of SentinelOne Singularity Endpoint is very easy, and freshers can implement and deploy these services without issues. Installing the agents takes less than five to ten minutes, making it convenient..”

Paramjeet Singh

IT Engineer at Softcell Technologies Limited

[Read full review](#) 

“The advice I would give to other professionals who are considering using SentinelOne Singularity Endpoint is that during implementation, do not put it directly into blocking mode but allow an adaptation period for the solution in detect mode in order to clear as many false positives as possible..”

Verified user

ingénieur systèmes et sécurité at a financial services firm with 201-500 employees

[Read full review](#) 

“When I first deployed SentinelOne Singularity Endpoint, we had multiple solutions handling orchestration for our cybersecurity program, which meant having multiple agents doing different things and collecting telemetry. In the past, I had CarbonBlack and other solutions and was missing out on things. Being able to have a single console to look at multiple metrics from different endpoints, including servers both Windows and Linux, as well as identity, has made performance and productivity much better..”

Adan Mendoza

[Read full review](#) 

Cybersecurity Analyst at a non-profit with 10,001+ employees

“We use part of the out-of-the-box integrations, so Microsoft Azure and Office 365, and they were included in our license. We did not need to purchase any additional module. It was straightforward to implement. There is good documentation available from SentinelOne, so it was really simple and it works really well..”

Robert Wojcik

[Read full review](#) 

Senior IT Administrator at a financial services firm with 201-500 employees

“We had the opportunity to interconnect SentinelOne Singularity Endpoint with our current SOC and SIEM tool, and the interconnection was really great and easy. SentinelOne Singularity Endpoint can offer some direct connectors, and we used one of them to ensure that everything can be configured quickly and easily, so we were really satisfied with this part..”

Verified user

[Read full review](#) 

Responsable Programme Cybersécurité at a retailer with 10,001+ employees

“Do not just test the platform on clean IT machines. Run a POC across a diverse cross section of your environment, including servers, POS terminals, laptops, workstations, and remote laptops. While deployment via cloud software as a solution is fast, plan for a two to four week baseline period. SentinelOne's one-click Volume Shadow Copy rollback is one of the strongest capabilities. Test this feature in a non-production environment using safe browser, software simulation, or test frameworks. Experiencing how fast encrypted files revert gives your SOC team complete confidence during live incidents. Do not treat EDR as isolated tools. Connect SentinelOne Singularity Endpoint immediately into your central SIEM data lake and then to firewalls. Automate response playbooks from day one to maximize reduction in mean time to respond and lower overall alert fatigue..”

Gokhany Gokhany

[Read full review](#) 

Cyber Security Consultant at Bkl Bilişim Teknolojileri Yazılım Danışmanlık Eğitim Tic Ltd Şti

Customer Service and Support

“The customer support is good, especially with easy tasks. The response was very faster in the easy tasks and more lower in the more complex issues. But overall, I am satisfied with the quality of support. I can say eight out of ten..”

Marco Spagnoletti

Shift Lead SOC Analyst at CYBEROO

[Read full review](#) 

“I would rate the technical support of SentinelOne Singularity Endpoint at ten out of ten because when I raise alerts, I receive responses within ten to fifteen minutes. The support team assists me with any troubleshooting, providing excellent response times..”

Paramjeet Singh

IT Engineer at Softcell Technologies Limited

[Read full review](#) 

“I had experience with customer support in Rosemont. I rate customer support an eight. I rate it this way because their managed detection and response team provides fast expert triage during critical security incidents. However, time to resolution for non-critical complex cases can sometimes be slow or too tier two and three..”

Gokhany Gokhany

Cyber Security Consultant at Bkl Bilişim Teknolojileri Yazılım Danışmanlık Eğitim Tic Ltd Şti

[Read full review](#) 

“I can understand that since there is a shortage of staff in SentinelOne, sometimes when we raise a case, it takes some time to respond. However, since we have the Prompt AI, things have been pretty easy for us to handle by ourselves instead of relying on tech support or customer support. The tech support does a great job whenever we raise a ticket..”

Verified user

Network Security Administrator at a energy/utilities company with 51-200 employees

[Read full review](#) 

“I rate the customer support provided for SentinelOne Singularity Endpoint based on my experience as we do not have direct support with SentinelOne; our MSSP is responsible for contacting customer support. We have had incidents with fairly high levels of criticality, and SentinelOne responded very quickly..”

Verified user

[Read full review](#) 

ingénieur systèmes et sécurité at a financial services firm with 201-500 employees

“Customer support for SentinelOne Singularity Endpoint is amazing. I have only had to use customer support once, which was to whitelist an application where the new UI of Singularity made whitelisting the file path difficult because it changed the order of operations on how whitelisting happens. My documentation was set up for the old portal through the old process of how you whitelist an application, and once the new view came out, it changed how that process worked. I had to go back through and update my documentation on it.

“Licensing for SentinelOne Singularity Endpoint was great, as it was quick and easy to get users added and removed from the system. Outside of that, I have not had to do anything else with SentinelOne..”

C Benson

[Read full review](#) 

Infrastructure And Systems Administrator

Other Advice

“I give SentinelOne Singularity Endpoint a rating of 8 out of 10. I chose 8 out of 10 because it is a very good score that comes close to perfection, but since there are always improvements to be made to a product, I did not want to give the maximum score..”

Verified user

ingénieur systèmes et sécurité at a financial services firm with 201-500 employees

[Read full review](#) 

“I do trust its alerts, and I do think that it is catching things. It is simple and straightforward. Looking at the marketplace, I am able to do the integrations as long as they follow the instructions, and it is pretty straightforward. I do not know that it has helped reduce alerts, but over time, users are aware that these platforms are installed on the endpoints and understand that if something happens, they are going to see the alerts come up and see the mitigation take place. They have seen that in the past. From an admin point of view, it is much easier to take a look at a single pane versus multiple platforms. Users are beginning to see that there is something installed on their computer whose whole job is to protect the endpoint. Do your homework and make sure that what you are getting out of SentinelOne Singularity Endpoint aligns with the goal of the business. [Understand](#) what the business is that you work with, conduct an assessment, and see if SentinelOne Singularity Endpoint aligns well with the company's goals. I would rate this solution a 9 out of 10..”

Adan Mendoza

Cybersecurity Analyst at a non-profit with 10,001+ employees

[Read full review](#) 

“I notice that integration is faster with SentinelOne Singularity Endpoint. It is also a kind of product that is easier to use. In some products, I do not want to mention the names of them, but some of them are hard to use, whereas SentinelOne Singularity Endpoint is easy to use. I did not use SentinelOne Singularity Endpoint before starting at Picus. Even though I did not use it before starting at Picus, I easily got used to it because the UI is easy to use and everything seems clear. I only use SentinelOne Singularity Endpoint in the lab environment. We did not use it in the whole company. However, if we had been using it, we would have benefited from it. I can say SentinelOne Singularity Endpoint offers faster detection.

“I looked at the console and I see some numbers related to the different EDR vendors for both simulation speed and also the result itself. SentinelOne Singularity Endpoint's score is demonstrated as the third highest score in the system. It is also the third speediest one. This means that overall, SentinelOne Singularity Endpoint has demonstrated good performance. I provided a rating of eight out of ten for SentinelOne Singularity Endpoint..”

Onur Pınargözü

Expert TAC Engineer at a tech vendor with 201-500 employees

[Read full review](#) 

“The impressions are pretty great. It has been actively blocking the threat and also correlates all the events using storyline, which has been pretty great.

“It is going to be really helpful because earlier, I used to go through the documentation, and it used to take a lot of time for me to actively find the relative answer to the question. With the Prompt AI, I can just query my question to the Prompt AI, and then it actually returns the results in a better way. If I have any queries, I can reach out to Prompt AI instead of raising a tech support case. It saves a lot of time.

“My suggestion would be to look at whether, based on the range of the products that we use, SentinelOne Singularity Endpoint supports those products or not, and then accordingly, we can purchase SentinelOne Singularity Endpoint and also evaluate how well it integrates with other security solutions inside our environment. I gave this review a rating of eight out of ten..”

Verified user

Network Security Administrator at a energy/utilities company with 51-200 employees

[Read full review](#) 

“I have been using SentinelOne Singularity Endpoint on and off for a while now. I am used to the older portal, but since the transition to the newer one, I have only used it for maybe five to six months.

“When you are working with an MSP that deploys SentinelOne Singularity Endpoint and has experience with it, you get a boost in reputation for just having that. To me, that would be the expected antivirus software or security software that should be standard with MSPs and organizations as a whole. SentinelOne sets the bar for security mitigation.

“There was a specific section where I discussed governance, and I would actually include it here. If I could use SentinelOne as a way to audit my governance for specifically NIST 873 or FIPS 140-3 or CMMC2, that would be amazing.

“If I was seeking a product for security and mitigation, I would start with SentinelOne and end with SentinelOne. I would put more trust in that application than any other on the market, one because I have a lot of experience with it, but two, it is trusted by most MSPs that I have worked with.

“I have used SentinelOne Singularity Endpoint's Ranger functionality before, but only one time, and I cannot recall everything I did with it. It was with network enumeration, and that was kind of the limit of what I used it for.

“I never got to choose between different security systems because the companies that I worked for either already had SentinelOne set up or they did not.

“My advice for others looking into using SentinelOne Singularity Endpoint is to do it, as you have nothing to lose, and it is the best there is. I would probably shorten the name SentinelOne Singularity Endpoint, as it is kind of long and a mouthful. Just keeping it as SentinelOne sounds better, as it sounds SentinelOne has a new product called [Singularity](#) when you say it that way. I gave this review a rating of ten out of ten..”

C Benson

Infrastructure And Systems Administrator

[Read full review](#) 

“SentinelOne Singularity Endpoint reduces alerts between sixty and eighty percent.

It is feasible to significantly increase team capacity. On average, enterprise SOC teams report saving fifty to seventy percent of the operational time previously spent on endpoint triage, investigation, and remediation. Time is saved because automated Storyline correlation, automated remediation, and drastic noise reduction with routine EDR overhead reduced, enabling security personnel to redirect their freed-up time toward proactive threat hunting across broader telemetry feeds, security architecture and hardening, vulnerability management

and patching cycles, and automation engineering such as building custom cloud playbooks.

SentinelOne Singularity Endpoint has reduced our organization's mean time to detect. Real world enterprise deployments see a seventy to ninety percent drop in mean time to detect, taking detection times from industry averages of hours or days down to seconds or minutes. Mean time to detect drops sharply because detection happens locally on the agent at machine speed during execution without reliance on cloud round trips or manual analyst log queries. Instead of waiting for a known hash or static signature hit, the engine flags suspicious behavioral patterns instantly upon process start. It immediately groups related execution events into a single visual context, eliminating the need for analysts to spend time searching and stitching raw logs together to confirm an active threat.

When evaluating the governance and security of SentinelOne's AI capabilities, specifically [Purple AI](#) and on-agent behavioral AI models, SentinelOne performs exceptionally well compared to broader enterprise AI implementations. Security vendors are held to strict compliance standards, and their AI architecture is built around data isolation and zero-retention principles. Data privacy, retention architectures, and role-based access control with prompt governance maintain high data privacy, access control, and explainability. No customer data trains shared LLMs, tenant isolation is strictly enforced, and console AI queries strictly inherit existing console role-based access permissions.

Evaluating the accuracy and reliability of SentinelOne Singularity Endpoint AI capabilities requires splitting the platform into its two distinct AI components: on-device behavioral AI engine and generative AI analysis, which is [Purple AI](#). Overall, SentinelOne is considered one of the most reliable and accurate platforms in the EDR space, though each AI engine operates under different reliability profiles and trade-offs. Strengths include independent third-party validation through industry benchmarks such as the MITRE ATT&CK evaluations, where SentinelOne consistently achieves one hundred percent detection coverage with zero detection delays. Limitations include false positive sensitivity on custom applications. When deployed in complex enterprise environments with heavily

customized non-standard internal applications or aggressive admin scripts, it can flag benign activity as malicious and requires initial policy baseline tuning. The behavioral engine's primary role in stopping fileless, zero day, and ransomware threats warrants a rating of nine. The Storyline correlation engine also receives a rating of nine.

Vulnerability scanning and threat hunting have improved. I give this review an overall rating of eight out of ten..”

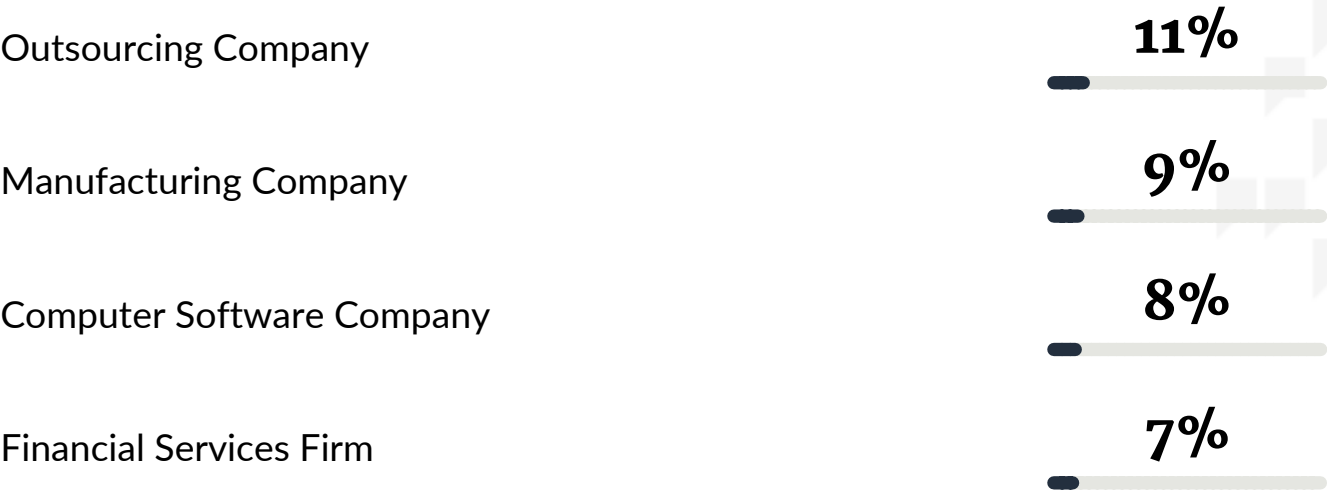
Gokhany Gokhany

Cyber Security Consultant at Bkl Bilişim Teknolojileri Yazılım Danışmanlık Eğitim Tic Ltd Şti

[Read full review](#) 

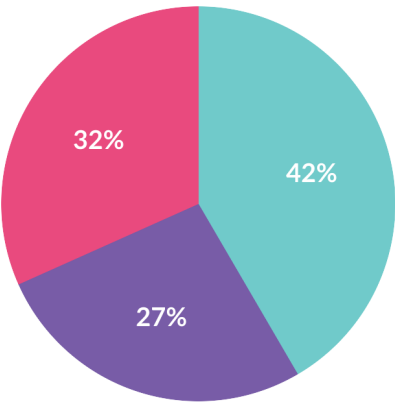
Top Industries

by visitors reading reviews



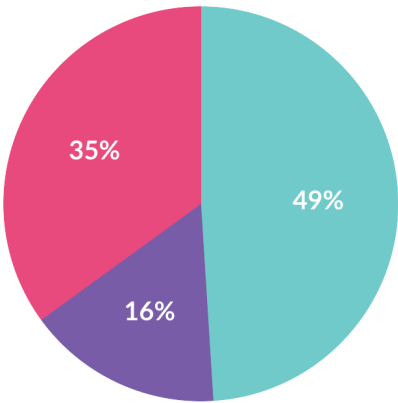
Company Size

by reviewers



Company Size

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