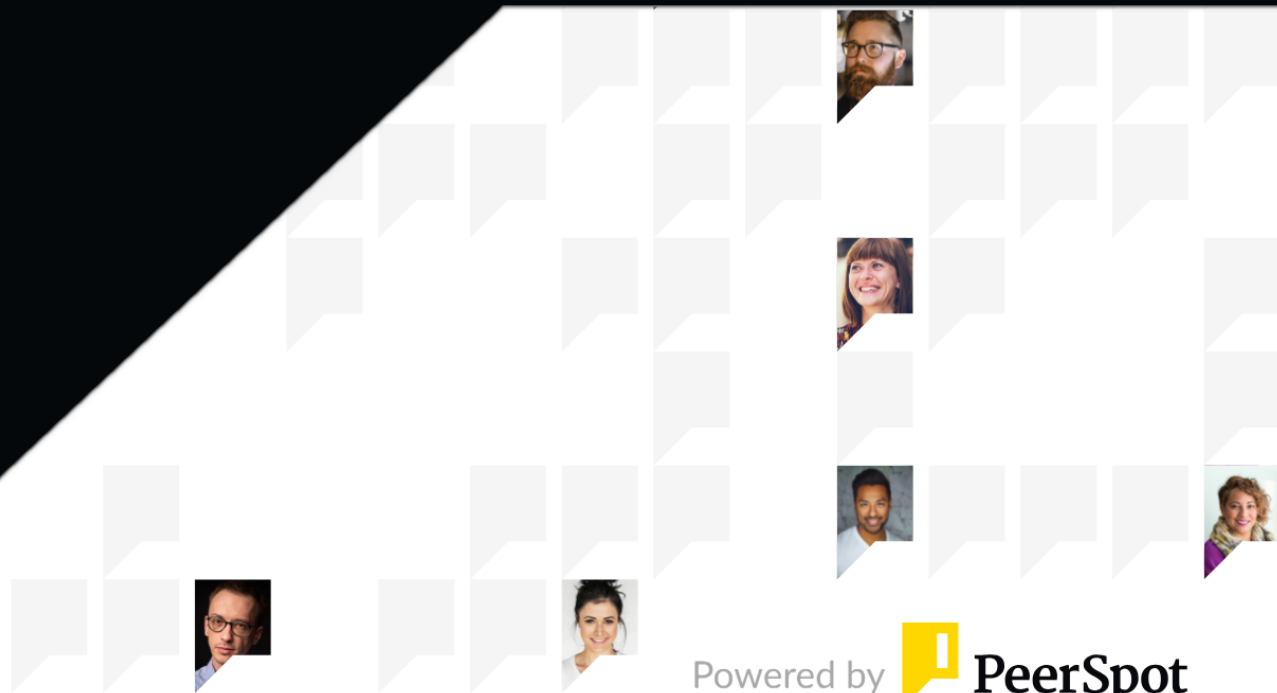


aws marketplace

Sumo Logic Security

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 17

Use Case..... 18 - 20

Setup..... 21 - 23

Customer Service and Support..... 24 - 26

Other Advice..... 27 - 31

Trends..... 32 - 33

About PeerSpot..... 34 - 35

Product Recap



Sumo Logic Security

Sumo Logic Security Recap

Sumo Logic Security offers efficient event monitoring with customizable alerts, centralized log search, and real-time threat detection. It supports multi-cloud environments and integrates with threat intelligence, reducing workload with AI-driven analytics.

Sumo Logic Security empowers organizations with advanced logging and monitoring solutions, facilitating comprehensive security event management. Its robust log search and comparison features, combined with user-friendly dashboards, enable quick event analysis. The platform's multi-cloud support and real-time threat detection are notable features, seamlessly integrating automated log correlation and AI analytics to optimize user experience. Despite needing enhancements in querying and dashboard functionalities, Sumo Logic Security remains a reliable choice for application log management, IT asset visibility, and incident alerting. Organizations utilize it for threat detection, posture monitoring, and compliance audits, in platforms like AWS, focusing on security insights and performance monitoring.

What are the key features of Sumo Logic Security?

- **Log Search:** Facilitates centralized search and event analysis.
- **Custom Alerts:** Offers flexibility in monitoring specific security events.
- **AI-driven Analytics:** Reduces workload and speeds up response times.
- **Real-time Detection:** Ensures swift threat identification and mitigation.
- **Multi-cloud Support:** Enables integrations across cloud environments.

What benefits can users expect from Sumo Logic Security?

- **Ease of Implementation:** Quick setup and deployment processes.
- **Cost-effective Pricing:** Provides value-driven investment with supportive customer service.
- **Responsive UI:** Enhances user experience and efficiency in operations.
- **Compliance Audits:** Facilitates thorough security audits and reporting.

Organizations in industries like finance and technology implement Sumo Logic Security to maintain security and compliance, leveraging its advanced monitoring and alerting capabilities. Teams focus on application troubleshooting and forensic analysis, ensuring robust security posture and effective incident response across cloud-based environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Sumo Logic Security has positively impacted my organization by increasing engagement with different teams.”



Migell Roberts

Senior Security Analyst at City Electric Supply Company

- ✓ “As a cloud-native SIEM, it scales up very well automatically, and real-time threat detection is available, so detection time has dropped significantly from three to four hours to under 30 minutes, reducing alert fatigue by over 100 days of low-volume alerts and significantly improving our KPIs, alert efficiency, decision quality, and operational stability.”



Pavan Kashetty

Security Engineer at a tech vendor with 11-50 employees

- ✓ “My SOC analysts were crushed under Splunk, but Sumo has actually eased the workload and made it tolerable for three people.”



Frank Krieger

CISO / Founder / GRC at VINCTA BV

- ✓ “The features I find most useful in Sumo Logic Security are the ease of implementation and connectors; they have a very easy connection and many connectors to important systems, making it very easy to implement and fast to start running in production.”



Shay Chouker

CSO at Altera

- ✓ “Compared to other tools, I prefer the UI much better as it categorizes data very well for me.”



Verified user

Security Analyst at a tech vendor with 10,001+ employees

- ✓ “Sumo Logic Security offers a single dashboard and customization, which are the most valuable features.”



Wilson Aitan

Deputy Country Manager at PT Securite Asia Indonesia (ABP Securite)

- ✓ “The Log Analytics platform is the most effective. If we cannot find the data in other tools, like email security or NDR, we can fetch those logs in the Log Analytics platform of Sumo Logic.”



Vinay Patel D N

Soc Analyst at a outsourcing company with 5,001-10,000 employees

What users had to say about valuable features:

“Sumo Logic Security offers a single dashboard and customization, which are the most valuable features. Additionally, it has a cost-effective structure because it is based on data storage and the number of scans, rather than uploading data. This cost model impacts the customers positively by offering a more straightforward pricing structure..”

WilsonAitan

Deputy Country Manager at PT Securite Asia Indonesia (ABP Securite)

[Read full review](#) 

“The features I find most useful in Sumo Logic Security are the ease of implementation and connectors; they have a very easy connection and many connectors to important systems, making it very easy to implement and fast to start running in production.

“Sumo Logic's diverse log sources support very much for my digital transformation, and this is a strong side of the system. They have wide support for connectors, enabling me to implement almost any system with webhooks and connect whatever I want, so this aspect is definitely a strong side of this product..”

Shay Chouker

CSO at Altera

[Read full review](#) 

“The first thing that I like about Sumo Logic Security is the earlier UI and the latest one, which has a clean layout. Since I can track so many good things, the UI has improved from before when it was not as good. Compared to other tools, I prefer the UI much better as it categorizes data very well for me. If I were using other security tools or other SIEM tools, I would need to think a bit and find something, which would be hard and fast. However, I am so adapted to this tool, and the features that they have implemented, including filters and other things, are the best.

“Since we are using Sumo Logic Security on the security part, we need to look through all the things and maintain them since there might be some crashes in the data that we are receiving. If we do not update the data points each and every time, some data points might have failed. If the server is offline, it might not report in Sumo Logic, so we need to check at the server level why this issue is being caused. We need to update the agent for Sumo Logic Security and ensure it is up-to-date..”

Verified user

[Read full review](#) 

Security Analyst at a tech vendor with 10,001+ employees

“Sumo Logic Security offers excellent features including ease of use. I came from a competing product, Splunk, and I was able to recycle a lot of the knowledge from that tool into Sumo because the logic was very similar.

Beyond the ease of use, the consumption model of Sumo Logic Security is also easy to understand, which was helpful. The build-out with Sumo was very good, as they spent a lot of time ensuring that we were sized correctly for the product, and the follow-ups were good. Sumo Logic Security has really good customer support.

The capabilities of Sumo Logic Security in providing security visibility across multi-cloud and hybrid environments are very good, particularly because Mambu is still a multi-cloud vendor, and the product worked extremely well in that scenario.

Regarding the automated TDRI workflows in Sumo Logic Security, they are excellent. I would put them at the top because they are truly useful and actually work as advertised.

My experience with Sumo Logic Security has been good. My SOC analysts were crushed under Splunk, but Sumo has actually eased the workload and made it tolerable for three people.

The improvements or benefits I have seen from Sumo Logic Security relate to alerts. We were buried under alerts and Sumo actually helped us clean that up. The number one value is being able to action things in a proper time frame..”

Frank Krieger

CISO / Founder / GRC at VINCTA BV

[Read full review](#) 

“The best features of Sumo Logic Security are automated log and event correlation, which may come from a firewall event, and User Entity Behavior Analytics (UEBA) for detecting impossible travel and unusual access times. Threat intelligence enrichments are good, and the MITRE ATT&CK framework is beneficial. The centralized log search for investigation is better compared to multiple SIEM solutions, where I can query everything in one place. The SEC records feature, something that returns `index=sec_records`, provides all the logs from different places. Pre-built dashboards and analytics, especially threat trends and the anomalies that return compliance patterns, are valuable. The workflow, including playbooks and workflows, can be triggered when we need to quarantine an endpoint, revoke credentials, or block IPs. Most importantly, it is cloud-native and has elastic scale. As a cloud-native SIEM, it scales up very well automatically, and real-time threat detection is available.

One of the most important things is MTTD, which is faster threat detection that reduced our MTTD, and we were able to detect alerts with multiple detections that used to take hours. Now the correlated alerts surface the real threat very quickly. Detection time has dropped significantly. We used to have MTTD of three to four hours, but now it is under 30 minutes. Automatically, our mean time to response has also increased substantially. Analysts are able to quickly pivot items and make faster decisions, especially without switching between tools. We have all our EDR tools and firewalls integrated to the same platform and viewing everything there. As a SOC, which faces major problems, it reduced the alert fatigue by over 100 days of low volume alerts, which have been made into insights, and this has greatly improved our alert efficiency and decision quality, the way we are able to enrich information. Operation stability has also improved very much. It has significantly impacted our organization, and our KPIs have improved substantially with respect to this..”

Pavan Kashetty

Security Engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“The best features Sumo Logic Security offers, in my opinion, are the ones that allow you to use dashboards as enrichments. For example, we had a situation where there was a suspected compromise on a specific server, a database server to be exact, and so we linked an enrichment action in the CSE component to then point us to a Qualys dashboard. In this specific case, the suspected server was suspected as being compromised, and we were able to check any available vulnerabilities from the Qualys dashboard itself by using it as an action in Sumo Logic Security.

We are actually using both out-of-the-box and custom rules from Cloud SIEM Enterprise, and it has been really great because we have a variety of ways to create rules based on our needs, such as match rules. What I really do appreciate are the first-seen rules that we can use in a fashion to determine a baseline of normal versus unexpected behavior depending on the entity, and I really do enjoy these.

In terms of threat intelligence, I was able to integrate, as an example, AlienVault, and using their actions, automated integrated actions into playbooks to enrich certain entities such as IPs, domains, URLs, and hashes. It has been very paramount to how we operate due to the fact we can all stay in the same single platform of Sumo Logic Security without having to reach out to different third-party sources, opening up different browsers, essentially saving time on trying to respond to an incident or review an incident. It has been really good in terms of integrating and using the threat intelligence features.

I find Sumo Logic Security's AI-driven analytics effective in reducing analyst workload and response times, and I have seen a difference since using those features. For example, we are using the anomaly-based AI detections in Sumo monitors, and I would say that it has been good, but the reason I say it could be better is the fact that we are seeing a bit of some false positives when it comes to understanding what is typical normal behavior and relying on AI to understand what normal behavior is versus what is unexpected. I found that when using this type of monitor, I do have to do quite a bit of tuning, which I would hope the AI would be a little bit more robust and essentially leave me hands-off when it comes to this.

We also use the dashboard enrichment feature in Sumo Logic Security when alerts pertain to specific entities, and we use it a lot. For example, we will get insights for server entities, and it is easy for us to pivot over to a dashboard when it comes to an enrichment perspective to determine if there are any actual vulnerabilities related to it. Another example is if we have an AWS related entity, we can pivot over using an enrichment action to navigate to one of the AWS dashboards to get some quick information pertaining to the specific entity involved in the insight.

Sumo Logic Security has positively impacted my organization by increasing engagement with different teams. For example, we have the database team being onboarded to Sumo Logic Security regarding their database logs, where they use it to monitor their database when it comes to informational all the way up to critical types of events, and they use it for alerting as well. This is due to the fact that they were not able to find any solution that can provide this type of functionality for them, and they have pivoted to Sumo Logic Security for their needs.

From this increased engagement, we are able to respond faster to incidents. For example, if they are seeing a type of activity that involves a user or an admin that is not supposed to be logging in at a specific time, they do get alerts on that. In addition to that, we are able to save time on fewer alerts because we are able to perform tuning on the logs to be able to only get relevant security-related incidents..”

Migell Roberts

Senior Security Analyst at City Electric Supply Company

[Read full review](#) 

Other Solutions Considered

“We have not typically evaluated other solutions as alternatives. As I mentioned, we used Splunk, Azure Sentinel, and Devo. We directly switched to Sumo Logic Security as per our organization's needs. We had used different SIEM platforms as well..”

Pavan Kashetty

Security Engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“I believe that we did look at another cloud-based solution, but I wasn't at the company during the evaluation process.

I would recommend to look at Sumo Logic, but also look at Datadog and Loggly. Look at some of the competitors who are also in this space..”

Verified user

VP of DevOps Engineering at a manufacturing company with 11-50 employees

[Read full review](#) 

“When comparing Sumo Logic Security with other tools such as Splunk, I see advantages such as its easier implementation, especially for companies that lack cybersecurity know-how; Sumo Logic Security can be beneficial for quick setup. However, while it is good for average tasks without needing three engineers, Splunk allows for more configuration to meet specific organizational needs, although it requires more expertise and time..”

Shay Chouker

CSO at Altera

[Read full review](#) 

“I have tried using Azure Sentinel in our organization.

“With the length of data transfer that we are having day in and day out, I do not find Azure Sentinel to be much feasible compared to Sumo Logic Security that we are currently using. It all depends on the data transfer credits that we are using day in and day out..”

Verified user

Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“I came from a competing product, Splunk, and I was able to recycle a lot of the knowledge from that tool into Sumo because the logic was very similar.

When comparing Sumo Logic Security to Splunk or other vendors, the models are vastly different. Sumo's consumption model is easier to understand, while Splunk's is much more complex. Additionally, the Splunk service was not really fit for the size of our organization, which was about 1,000 people as it was a much more robust solution for something larger..”

Frank Krieger

CISO / Founder / GRC at VINCTA BV

[Read full review](#) 

“We used Devo and Splunk before Sumo Logic Security. Due to our organization's budget platforms and other factors, we switched to Sumo Logic to have our SIEM. We used to face challenges before, such as storage clusters and scaling issues, and the detection part was very much worse in other SIEMs. I may not give specific details, but Sumo Logic insights are playing a major role today in our investigation and reporting parts. I have used Splunk, Devo, and even ArcSight..”

Pavan Kashetty

Security Engineer at a tech vendor with 11-50 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“We have seen ROI. The product saves time. Because of it, we don't have to provide credentials for everybody to look at individual systems to find their logs..”

Jeffery Statham

Software Architect at Solink

[Read full review](#) 

“The return on investment I have seen with Sumo Logic Security in the past year and a half is tough to quantify, but I would estimate it has hit the milestones we set internally for return on investment, as we have not looked at the product and said it is not paying for itself..”

Frank Krieger

CISO / Founder / GRC at VINCTA BV

[Read full review](#) 

“We look at ROI constantly. We put the amortized cost of Sumo Logic and New Relic right in the console that our service teams can look at. The ROI is good enough for us not to move away from Sumo Logic..”

Verified user

[Read full review](#) 

VP of DevOps Engineering at a manufacturing company with 11-50 employees

“The troubleshooting part of Sumo Logic has solved a lot, e.g., if there is any downtime on the website. So, we have reduce our downtime by a lot with Sumo Logic because we can easily troubleshoot issues..”

Tejprakash Sharma

[Read full review](#) 

DevOps Engineer at TO THE NEW

“As I mentioned, we have 100% return on investment very well. I have experienced that we used to have over 100 alerts where we needed eight analysts, but now we are able to operate with five analysts because the time drop in investigation has been from 20 to 40 minutes. We have saved 64 hours of our time overall. Before we used to have eight analysts, now we have at least five analysts and we are able to do the work completely. We have a good return on investment in terms of even the log retention part as well..”

Pavan Kashetty

[Read full review](#) 

Security Engineer at a tech vendor with 11-50 employees

Use Case

“My clients use Sumo Logic Security depending on their needs. Some of my clients are looking for network visibility and observability, while others focus on the security aspects, utilizing the Sumo Logic SIEMs..”

Wilson Aitan

Deputy Country Manager at PT Securite Asia Indonesia (ABP Securite)

[Read full review](#) 

“My main use cases with Sumo Logic Security are the same as Splunk; it is not log management, but rather security events and information, a security information system like SIEM..”

Shay Chouker

CSO at Altera

[Read full review](#) 

“We primarily use Sumo Logic as a SIEM, Security information and event management tool. It serves as a Cloud SIEM and is utilized for alert monitoring, insight monitoring, and as a continuous intelligence platform..”

Vinay Patel D N

[Read full review](#) 

Soc Analyst at a outsourcing company with 5,001-10,000 employees

“The product is a log aggregator of all the logs from all our environments, including AWS. Our infrastructure is deployed on AWS. We ship all logs to Sumo Logic. Based on the logs, we create alerts. These alerts are sent to an email ID, which creates tickets..”

Sourabh Pardhi

[Read full review](#) 

Senior Information Security Analyst at Everbridge

“The main use case for Sumo Logic Security is as a SIEM platform where our customers prefer it to gather logs from multiple places and have good detections, especially Sumo Logic insights, which is helping us a great deal to detect and correlate logs from different platforms and consolidate them into one insight. It helps for investigation and analysis. The major part is threat detection and threat analysis..”

Pavan Kashetty

[Read full review](#) 

Security Engineer at a tech vendor with 11-50 employees

“My main use case for Sumo Logic Security is relying on it for security insights when it comes to security alerts. This is heavily used by people who are on a weekly on-call rotation to ensure that security incidents from Sumo insights are actioned on and remediated.

A specific example of a security incident where Sumo Logic Security played a key role is when, about a couple of weeks ago, we had an incident where a user was a victim of a click-fix attack. Sumo Logic Security was able to determine that this user had performed some risky activity and also correlated the fact that the URL was associated with that incident. We were able to determine the involved entities, which included the user's device, and we were able to quickly action on it and perform a reset of the user's account in order to begin the remediation process.

In addition to the previous points, I use Sumo Logic Security for a lot of the enrichments when it comes to insights as well. An example of this is when we receive insights regarding a user entity, we are able to use Sumo enrichment automation to get user details including their manager. This is definitely beneficial in an example such as the one I provided earlier where a user was compromised, where we can at least know who the proper chain of command is if that needed to be used in that specific incident..”

Migell Roberts

Senior Security Analyst at City Electric Supply Company

[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.

“It is easy to deploy Sumo Logic Security, since we are always on call with the support team, and there was a specific SME deployed for us from Sumo Logic Security who helps us whenever we get stuck in some part or cannot proceed. They help us in that part..”

Verified user

[Read full review](#) 

Security Analyst at a tech vendor with 10,001+ employees

“The implementation process of the solution was good and not very difficult. You can easily integrate Sumo Logic Security with AWS or Kubernetes. Even new users who are aware of AWS can follow the documentation and easily deploy the solution..”

Moole Muralidhara Reddy

[Read full review](#) 

DevOps and Solution Architect at a recruiting/HR firm with 10,001+ employees

“The initial deployment of Sumo Logic Security was complex, but working with Sumo made it very easy.

It took three months to deploy Sumo Logic Security..”

Frank Krieger

[Read full review](#) 

CISO / Founder / GRC at VINCTA BV

“The initial setup is very easy.

In terms of the initial deployment, it's just a matter of installing the solution. It's sort-of similar to onboarding a server..”

Verified user

[Read full review](#) 

Associate Director - Database & DevOps at Medlife

“The setup of Sumo Logic Security is easy.

The time it takes for the deployment depends on how many logs and the sources there are.

I rate the initial setup of Sumo Logic Security a seven out of ten..”

DipeshBhawsar

[Read full review](#) 

Architect at a financial services firm with 1,001-5,000 employees

“The integration and configuration in our AWS environment is automated. We automated it so every AMI comes ready with Sumo Logic and New Relic. Therefore, we have no issues.

We integrated with New Relic. Thus, we get alerts sometimes from Sumo Logic's logs as opposed to just native alerts when they are from CloudWatch or New Relic..”

Verified user

[Read full review](#) 

VP of DevOps Engineering at a manufacturing company with 11-50 employees

Customer Service and Support

“The support team is very cooperative. As soon as the team receives our tickets, a support person is assigned to us. They reach out to us and try to solve the problem..”

Sourabh Pardhi

Senior Information Security Analyst at Everbridge

[Read full review](#) 

“We have two options for technical support. If we take the enterprise support, we get a reply within one or two hours. If you don't have enterprise support, you will get a reply in around one day or 12 hours, based on their availability..”

Moole Muralidhara Reddy

DevOps and Solution Architect at a recruiting/HR firm with 10,001+ employees

[Read full review](#) 

“I would rate the support from Sumo Logic Security as about a seven. It depends on the person providing support, but in general, they usually provide continuous support post-implementation, being in touch and trying to help, which makes their after-sale process better than Splunk..”

Shay Chouker

CSO at Altera

[Read full review](#) 

“We have a weekly meeting with the technical team for all our queries since it is included in our package.

“I would rate the quality and speed of Sumo Logic Security support seven out of ten since the meetings are close to other vendors only, but they can improve on that part..”

Verified user

[Read full review](#) 

Security Analyst at a tech vendor with 10,001+ employees

“The build-out with Sumo was very good, as they spent a lot of time ensuring that we were sized correctly for the product, and the follow-ups were good. Sumo Logic Security has really good customer support.

The interactions have been extremely good, and the account team is great, so I never feel as though they just forgot us.

I rate the technical support for Sumo Logic Security a nine..”

Frank Krieger

[Read full review](#) 

CISO / Founder / GRC at VINCTA BV

“Support for Sumo Logic Security is good. We have had a couple of issues, especially with the technical support team troubleshooting problems, particularly around API integration issues, but they had a faster response time. I would score them around 9 out of 10. Direct support includes documentations, tutorials, and training access along with community forums, which helps us resolve many questions independently without reaching out to them. Where we have faced some challenges, I would say it may be because of region-specific support in India or Europe, as some support times were slower. Some tickets even took two weeks when we were finding issues with email-related matters. Everything else is good because their documentation is very helpful and querying is also very good. They have a limited direct call option for support, but the response is good, and technically they will explain everything we need to do. Premium support is also available. The customer support is very good with them, and the documentation is helping us to fix issues today..”

Pavan Kashetty

[Read full review](#) 

Security Engineer at a tech vendor with 11-50 employees

Other Advice

“During this evaluation, I considered multiple criteria for the Sumo Logic Security solution. Based on these criteria, I rate the solution as an eight out of ten due to its effective features and pricing..”

WilsonAitan

Deputy Country Manager at PT Securite Asia Indonesia (ABP Securite)

[Read full review](#) 

“The compliance reporting tool in Sumo Logic Security is pretty acceptable; nothing special, but it is okay in helping meet regulatory requirements for my organization.

“Overall, I think Sumo Logic Security is acceptable; it is a pretty slick, nice product, with no significant additional features that I feel need to be added or improved.

“For those considering using Sumo Logic Security, I would recommend checking it out.

“I do not rate it a ten because I find some aspects of how the system works overall to be strange. My review rating for Sumo Logic Security is seven..”

Shay Chouker

CSO at Altera

[Read full review](#) 

“My advice to others looking into using Sumo Logic Security is to look at the customer service side of things. The product can be great, but if the customer

service side of things fails, I think pretty much the rest follows. I would also advise them to look at the automation features, for which Sumo Logic Security has been pretty great in expanding that realm. I think those are going to be the two main things as we are moving a lot more towards being hands-off with automation and also being able to utilize support and getting timely answers. Those would be the two key factors of looking at or giving advice when it comes to Sumo Logic Security.

I have additional thoughts about Sumo Logic Security in that I do appreciate the product. It can be as vague as you want to or as detailed as you want to when it comes to getting telemetry information from the product itself. That is what I appreciate about Sumo Logic Security. Overall, I am happy with the product, just a few hiccups here and there. I provided a rating of eight out of ten for this review..”

Migell Roberts

Senior Security Analyst at City Electric Supply Company

[Read full review](#) 

“I would say to define especially what problems they have, particularly the threat detection part, incident response part, reporting part, cloud security monitoring, or insider threat analytics. They need to plan their log strategy about how much quality versus quantity they require and send only meaningful logs while filtering out debug and low-level information that makes noise. Categorizing the logs by priority is one of the most important things. Using something with very much tiered retention periods is helpful because Sumo Logic Security provides pre-built dashboards, correlation rules, analytics, and threat intelligence feeds. That is going to be helping. I would recommend investing in training, as good training helps the team write more effective queries, build custom correlation rules, alert tuning, and perform threat hunting. These are things to focus on, which especially help the organization. Measure metrics as well, such as MTTD, MTTR, false positive rate, analyst hours worked, and threat signals escalated, as these are outstanding for Sumo Logic Security.

Regarding additional thoughts about Sumo Logic Security before wrapping up, I would mention improvement in the detection part with AI integration regarding log summarization and advanced analytics, which should be part of the roadmap. Also, how Sumo Logic Security is going to handle scalability, such as onboarding different data sources or tuning alerts. The major direction I am interested in seeing is how Sumo Logic Security will move forward with AI-based SOC capabilities, as that is the next era of SIEM tools. I would give Sumo Logic Security an overall rating of 8 out of 10..”

Pavan Kashetty

Security Engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“We are mainly concentrating on networking. We use VPC products and application logs to monitor the genuineness of users who have logged in. We also store and monitor GuardDuty logs to see if someone is trying to access the same

server multiple times. We are storing and monitoring WAF logs and GuardDuty logs. If someone faces any issues, we'll receive an email and take action based on it.

If someone tries to access one of the applications from a different country, we can search in Google and identify the location of that particular IP address. Sumo Logic Security identifies whether a particular IP address is low, medium, or high risk without the help of Google.

We can store logs in CloudWatch, but it is very difficult to search them in CloudWatch. We should know the query in order to do that. Searching for logs with Sumo Logic Security is very easy compared to CloudWatch. We have been using the solution for more than two years and haven't faced any issues with the solution's availability. I would recommend the solution to other users.

I would recommend Sumo Logic Security instead of AWS, CloudWatch, or CloudTrail. With Sumo Logic Security, you can capture and see all the logs in a single place. If some issues occur, you can log into the solution and verify all the logs. At an organizational level, we have multiple AWS accounts for different environments. Instead of logging in to all the AWS accounts, you can log in to Sumo Logic Security and verify everything.

Overall, I rate the solution a nine out of ten..”

Moole Muralidhara Reddy

DevOps and Solution Architect at a recruiting/HR firm with 10,001+ employees

[Read full review](#) 

“Regarding the effectiveness of AI-driven analytics in reducing the workload and response times, it is too early to tell, as it is something that recently came out and we have not consumed it yet.

My impressions on the built-in threat intelligence feature are not bad. I would give them four out of five stars. They tend to be very good, but very specific to certain

situations.

The impact of Sumo Logic Security in prioritizing alerts has been hard to quantify at this stage, as we are still trying to determine the value of that.

I could not tell you if the knowledge agent has helped improve onboarding efficiency because we do not utilize that function.

When it comes to how much time Sumo Logic Security saves, I would not say it is a time saver. It is an FTE saver. It did not really make my analysts work less in a day. They still have to work, but it avoided the need to procure more analysts to do the work.

Sumo Logic Security has probably saved us three FTEs.

Approximately 15 users utilize Sumo Logic Security.

Sumo Logic Security does not require any maintenance as it is a SaaS-based solution. We do not have to patch it, maintain it, or host it.

Sumo Logic Security was purchased through an engagement that was done pre-Marketplace, but it was purchased through Marketplace.

My advice for others looking to implement Sumo Logic Security would be three things: first, do a proof of concept because these solutions are very expensive. Second, definitely keep involved with Sumo through the entire process, making them a partner throughout the process. Third, and this is the most critical one, definitely take time to size your environments correctly because once you sign those contracts, that is the size.

I rate this review an overall eight..”

Frank Krieger

CISO / Founder / GRC at VINCTA BV

[Read full review](#) 

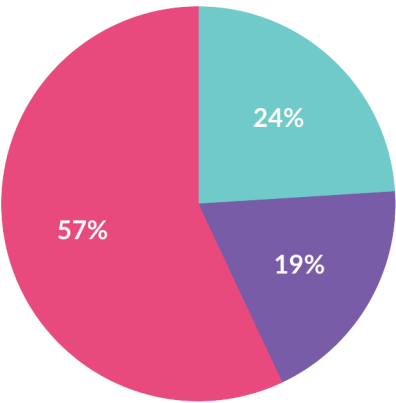
Top Industries

by visitors reading reviews

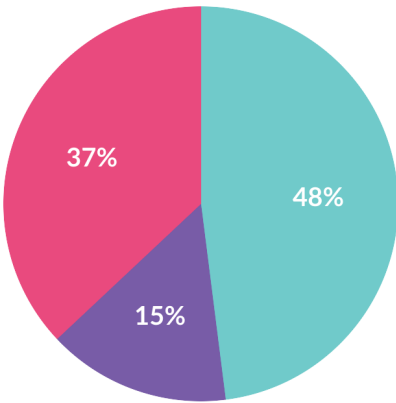


Company Size

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