aws marketplace

Anvilogic

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

©2026 PeerSpot, All Rights Reserved

Product Recap

Anvilogic

Anvilogic Recap

Anvilogic offers a no-code platform that enhances SOC efficiency by leveraging AI capabilities, providing detection coverage and industry-specific insights while integrating seamlessly with platforms like Snowflake.

Providing advanced visibility into detection coverage, Anvilogic delivers industry-specific insights through a powerful AI-driven, no-code environment. Users benefit from features like log normalization, the Armory for pre-built detections, and integration flexibility with platforms such as Snowflake. The platform significantly enhances SOC efficiency by reducing false positives and delivering quick insights. With integration into the MITRE framework and customizable alerts, Anvilogic improves detection logic and facilitates effective threat management, ensuring efficient detection across diverse environments.

What Are Anvilogic's Key Features?

- **Visibility into Detection Coverage:** Offers a clear view of detection capabilities across environments.
- **AI Capabilities:** Utilizes AI for advanced threat detection and alert generation.
- **No-code Environment:** Simplifies operations with user-friendly interfaces.
- **Integration Flexibility:** Connects smoothly with platforms like Snowflake.
- **Log Normalization:** Standardizes log data for enhanced clarity and analysis.
- **MITRE Framework Integration:** Aligns with industry standards for effective threat identification.

What Benefits Should Users Look For?

- **Improved SOC Efficiency:** Streamlines operations and reduces false positives.
- **Quick Insights:** Provides rapid detection insights for proactive threat management.
- **Cost-effectiveness:** Delivers value through enhanced capabilities at an effective price point.
- **Customizable Alerts:** Allows tailored threat notifications for better focus.
- **Enhanced Threat Management:** Empowers teams to manage threats efficiently across environments.

Anvilogic specializes in detection engineering for SOC teams, integrating data from tools like SentinelOne and Splunk. Its AI-driven capabilities streamline detection processes, reduce false positives, and extend to log ingestion, detection logic versioning, and threat prioritization. Industries use Anvilogic to enhance security operations through advanced detection scenarios and coordinated alert efforts, enabling efficient detection of behavioral patterns and management of security incidents.

©2026 PeerSpot, All Rights Reserved

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- “Anvilogic plus Snowflake has vastly improved our total cost of ownership for the SIM platform; we went from a pretty expensive platform in Splunk that was not vertically scalable due to budget limitations to a platform now that is far more efficient per terabyte of data ingested and processed per day.”

Verified user

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

- “They teach you and give you insights every morning or every week, saying, 'Hey, this is not working, so what do you want. You're getting one or two of these alerts per day. Do you want to squash them from error to warning?' They're always giving you tips on how to improve the efficiency of the system itself.”

Jason Murphy

Vice President, Information & Cyber Security at St. George's University

©2026 PeerSpot, All Rights Reserved

"I view Anvilogic as an easy button for detection engineering—you're talking about replacing multiple headcount and a lot of process and oversight with the technology."

Brandon Bryant

Director, Cybersecurity Operations at Labcorp

"Anvilogic allows me to extract a plethora of information, including mapping TTPs assigned for detection logic, which effectively helps in setting quarterly coverage agendas, thus illustrating its vital role in detection strategy and management presentations."

Verified user

Threat Researcher 2 at a tech vendor with 1,001-5,000 employees

"Among those features, the one that has made the biggest difference for our team is the AI capability; we have seen a significant shift in our SOC operations."

Verified user

Security Data engineer at a tech vendor with 5,001-10,000 employees

©2026 PeerSpot, All Rights Reserved

"Anvilogic has impacted my organization positively because it is native for cloud-type infrastructures and they have a significant proactive approach to cost licensing."

Kevin Hernandez

Manager, Threat Intel & Detection Operations at Zendesk

"Before Anvilogic, we had no visibility into our detection coverage. The ability to break it down by industry verticals, such as attackers and adversaries, is valuable."

Ajish John

Head of Information Security at a tech vendor with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

What users had to say about valuable features:

"In my opinion, the best features Anvilogic offers are the AVLs and the logics, which are pretty user-friendly. It has extensive mapping with MITRE frameworks and various other capabilities.

The user-friendly AVLs and mappings help in my day-to-day work because the AVLs are readable and understandable rather than appearing as disorganized code that is difficult to comprehend. I can use macros to assist myself. Allow listing is also user-friendly because it has its own process where I choose a field first and then allow list something in that field.

Anvilogic has positively impacted my organization because I started working with this organization after they implemented Anvilogic. I would say it is much easier to create all the use cases and detection engineering tasks with Anvilogic integrated with Splunk. They are implementing some AI features that I would like to test out and am still waiting to try. The fact that it is easier to create use cases and engineering tasks has made my daily work more efficient with all the filtering capabilities that Anvilogic provides.."

Ángel García Favieres
CyberSecurity Specialist at Aiuken

Read full review

©2026 PeerSpot, All Rights Reserved

“I currently utilize multiple of Anvilogic's AI features, both for fine-tuning and developing new content, as well as the threat intelligence feeds that it provides.

In my opinion, the best features Anvilogic offers are the AI features, which are great, and their common language rule tuning and modeling is much simpler than those other vendors that require query building skills.

The common language rule tuning and modeling have made things easier for my team because it is broken down into multiple smaller chunks rather than one large chunk of code. Multiple smaller, pre-processed data points are basically visible and editable in those smaller chunks without having to actually code at all.

Anvilogic has impacted my organization positively because it is native for cloud-type infrastructures and they have a significant proactive approach to cost licensing. Rather than having to import all data, it actually sits on top of Snowflake, which reduces overall cost for data storage itself. Since implementing Anvilogic, our overall costs have been reduced. .”

Kevin Hernandez
Manager, Threat Intel & Detection Operations at Zendesk

Read full review

©2026 PeerSpot, All Rights Reserved

“The best features that Anvilogic offers include its independence from a particular solution, allowing us to have Snowflake as a data repository now and the flexibility to move to other platforms such as Databricks or Splunk while keeping our detections intact. Another valuable feature is the AI capability, which not only assists in detection but also helps us to write queries, completing multiple tasks efficiently. Additionally, Anvilogic is a no-code platform, so the base search is already ready for us, and we just have to tweak it according to our use cases. Anvilogic's new features enable us to improve SOC efficiency and filter out a lot of false positive alerts. Additionally, it has an attached MITRE framework, automatically detecting it so we do not have to manually add the MITRE framework IDs as we did in Splunk.

Among those features, the one that has made the biggest difference for our team is the AI capability; we have seen a significant shift in our SOC operations. Many false positives are handled by the AI, allowing the team more time to discuss and investigate the actual use cases. Each use case also includes a description of what it is trying to detect, which helps engineers understand the use case's purpose without needing to reach out to seniors for clarification..”

Verified user

Security Data engineer at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The best features Anvilogic offers are consistent recording and tracking of detection engine detection rules as they adapt over time to adversary's behaviors, and the ability to operate in multiple security SIEM environments.

"Anvilogic works for my team by providing a single point of contact to put detection engineering rules that then get distributed to all of the various event management engines, as we have multiple SIEM environments in our company, including Microsoft Defender, Splunk, Elastic, and others.

"Anvilogic has changed how my team thinks about detection by allowing us to no longer apply the same configurations and correlation rules in multiple Splunk environments and can transparently search across multiple SIEMS platforms.

"What surprised me the most about Anvilogic once I started using it is the ease of creating and maintaining custom threat intel and threat scenarios.."

Joe Moore
Cybersecurity Architect at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Anvilogic's best features are detection, SIEM support that is logged into the SIEM, AI detection in the SOC workflow, as well as threat detection and correlation of that particular software.

"Anvilogic's AI detection in the SOC workflow stands out compared to other solutions I've tried because the accuracy of the AI makes it the best software for my organization. The AI agent assists with detection and threat creation, analyzes behaviors, and triggers alerts if any suspicious behavior occurs, along with investigation and MITRE ATT&CK mapping, which helps me significantly.

"Anvilogic has positively impacted my organization by helping with both known and unknown threats already present in the current threat landscape, detecting SIEM tools such as Splunk, Microsoft Sentinel, Snowflake, and Databricks, optimizing those tools, and strengthening my organization in the cybersecurity realm.

"I have seen a reduction in response time as a specific outcome. Due to SIEM modernization and SOC automation, it has helped me significantly by reducing false-positive reports and alerts.."

Evans Vasavan
Security Engineer at GlobeSecure Technologies Pvt Ltd

Read full review

©2026 PeerSpot, All Rights Reserved

"One of the best features Anvilogic offers is the Armory, which is full of various different pre-built detections; that was a huge improvement from any kind of pre-built detections we had in Splunk and saved a lot of time to really increase our coverage capability. I also appreciate the normalization process for log sources, normalizing them to a consistent schema where those alerts automatically apply is a nice feature and gives us a very clear-cut way to handle lots of different log sources in a centralized manner, ensuring that we are doing threat detection on those log sources.

The normalization process has enhanced our log monitoring maturity; previously in Splunk, we had SIEM mapping set up for log sources, but it did not translate necessarily to immediate security value because there were not pre-built detections that leveraged that SIEM mapping. The ability for Anvilogic to have built-in curated detection logic that automatically applies once we normalize logs creates immediate maturity and value every time we normalize a log source. It gives us a target to identify if a log source should be normalized. If it should, we know the value and output from Anvilogic; if it should not, we can identify custom use cases and build custom logic in Anvilogic or hold onto those logs in our data lake without any detections running on them if it is more for compliance or incident response.

Anvilogic plus Snowflake has vastly improved our total cost of ownership for the SIEM platform; we went from a pretty expensive platform in Splunk that was not vertically scalable due to budget limitations to a platform now that is far more efficient per terabyte of data ingested and processed per day. The savings per terabyte of data being ingested and monitored for security threats was a pretty significant percentage, which was a huge advantage. We now have budgetary space to scale up our solution as needed as the business grows.

We have had to make difficult decisions to not ingest certain logs in the past due to budgetary restrictions, but now we can take a more liberal approach in accepting most requests and ingesting those logs into our SIEM because the cost to do so is not a problem for the company and for our internal budgets, which is huge.."

Verified user

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Other Solutions Considered

"We were previously using Splunk and decided to switch due to its lack of AI capabilities related to the SIEM product. We also evaluated other options before settling on Anvilogic.."

Verified user
Security Data engineer at a tech vendor with 5,001-10,000 employees

Read full review

"I previously used top tier SIEM's. I switched to Anvilogic because it looked overall better and proved to be a better fit for our type of architecture.."

Kevin Hernandez
Manager, Threat Intel & Detection Operations at Zendesk

Read full review

"We did not previously use any different solution and directly switched to Anvilogic. Before choosing Anvilogic, we did not evaluate other options and directly purchased it from a vendor who offered it to improve our organization's capabilities. After trying it for two years, it has been working well.."

Evans Vasavan
Security Engineer at GlobeSecure Technologies Pvt Ltd

Read full review

©2026 PeerSpot, All Rights Reserved

"We evaluated various options before choosing Anvilogic, including Gurucul, Panther Security, and Splunk Cloud, among others. Ultimately, we found Anvilogic to be the best fit for our needs.."

Verified user

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

"Based on the context of the environment, I find Anvilogic is highly beneficial for smaller cybersecurity teams needing an efficient detection tool. Larger organizations may explore alternatives, but for small to intermediate teams, Anvilogic fits well in their detection processes.."

Verified user

Threat Researcher 2 at a tech vendor with 1,001-5,000 employees

Read full review

"We previously used Splunk and switched to Anvilogic + Snowflake.

The moment we realized we needed something better was triggered by the lack of detection coverage and the overhead required to improve detection in Splunk, along with the non-scalable cost of operating it. We constantly dropped logs from monitoring, which is not the focus of a security organization; we wanted better coverage and monitoring, and that is what Anvilogic and Snowflake enabled us to achieve.."

Verified user

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

ROI

Real user quotes about their ROI:

"I have seen a return on my investment with Anvilogic. We rolled out approximately 1,500 Armory alerts in three months, which would not have been possible with Splunk, and they were all fixed and modified as needed.."

Jason Murphy
Vice President, Information & Cyber Security at St. George's University

Read full review

"We started our journey with Anvilogic. I do not have the metrics to show in our current organization that could justify that, but the capability that we have on Anvilogic is unmatched to any other platform.."

Roger Allen
Senior Director | Detection Response at a tech vendor with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I have seen a return on investment in that Anvilogic has been more of a fundamental enablement technology than a return on investment, but it has definitely allowed us to move more quickly with integrating our corporate acquisitions as well as with our corporate colleagues who use other SIEM technologies.."

Joe Moore
Cybersecurity Architect at a tech vendor with 10,001+ employees

Read full review

"I have seen ROI with Anvilogic. We're taking these things that executives see on the news, cyber threats falling from the sky, and we're taking the timeline that would take weeks or sometimes even months to address, depending on what's required for the detection, and bringing that timeline down to hours and days.."

Brandon Bryant
Director, Cybersecurity Operations at Labcorp

Read full review

©2026 PeerSpot, All Rights Reserved

"While I do not have specific metrics, we have certainly seen a return on investment, mainly in time taken to improve detection coverage and the ability to detect threats on our logs. The Armory has greatly increased our coverage while reducing the time that would have been needed to develop detections ourselves in Splunk. However, the volume of alerts generated is shifting the cost to the operations side, requiring us to ensure that detections are tuned and alerts are efficiently firing to prevent noise that could increase costs for operations personnel and risk missing incidents.."

Verified user

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

"Anvilogic has saved us about 25% percent of what a detection engineering platform would be. It is difficult to put quantitative aspects like better operations and structure quality, but I would say efficiency increased by about 50%.

Anvilogic has not helped reduce our overall SOC or IR operations costs because we use the time we saved to do more. If we were not doing more and did not have Anvilogic, we would need one dedicated person to do this detection engineering. That cost has significantly been reduced.."

Ajish John

Head of Information Security at a tech vendor with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Use Case

"My main use case for Anvilogic is security incident event management. A quick specific example of how I use Anvilogic for security incident event management is triaging or correlation of security events from multiple security platforms and log sources.."

Kevin Hernandez
Manager, Threat Intel & Detection Operations at Zendesk

Read full review

"My main use case for Anvilogic is coordinating and tracking indicators of compromise and detection rules. I use Anvilogic for coordinating and tracking indicators of compromise or detection rules by feeding detection rules into Splunk, our Splunk environment, and these are turned into actionable alerts for our security operations center.."

Joe Moore
Cybersecurity Architect at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"My main use case for Anvilogic is for detection engineering, and I manage all of my use cases and alerts in the AVLs through Anvilogic.

A specific example of how I use Anvilogic for detection engineering and managing alerts is that we use it with Splunk, and through the Splunk logs that we send and store there, we create logics for user logins when they shouldn't have access, brute force cases, and other detection scenarios.

I also use Anvilogic for allow listing. As much as I use it for logics, I also allow list with the tool. It has some capabilities for researching my infrastructure and identifying which use cases I would need or which defenses I have covered insufficiently.."

Ángel García Favieres
CyberSecurity Specialist at Aiuken

Read full review

©2026 PeerSpot, All Rights Reserved

"Anvilogic serves as our main SIEM and detection engineering platform. We use Anvilogic to create alerts based on our data, and the AI capability to detect alerts based on whatever data we are feeding into it is a feature that our team at Kroll particularly values.

We have SentinelOne data, which is our EDR, and we have EDR data directly set up through Anvilogic input without using any third-party tool to get that data. Anvilogic has integrations directly in place, and we are using the SentinelOne input through Anvilogic. Since we uploaded or ingested that data, Anvilogic has started to give us suggestions about what alerts could be fired through that data. Anvilogic has flagged the threat identifiers through which we can build some use cases or modify them for our use. Anvilogic has also helped us understand what is a false positive and what could be a promising use case for our company in particular, providing valuable support.

Regarding how Anvilogic supports our detection engineering, the uniqueness is about AI, which we did not have in Splunk earlier. This helps us not only to close the false positives but also features AI to write our queries. This capability lifts a lot of burden from the SOC team as they do not have to focus on how to write a query but can concentrate on investigating an alert or a use case, which has really caught my eye, and I am glad we have onboarded that feature.."

Verified user

Security Data engineer at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Anvilogic serves as our security analytics tool on top of our security data lake.

In my day-to-day work, we perform detection engineering on Anvilogic, and we also use the Armory to provide us with strong coverage from a MITRE perspective and security coverage over our logs to ensure that we can detect threats and respond to those threats efficiently and effectively.

We pursued Anvilogic as a piece of the puzzle to replace Splunk, our legacy SIEM platform, and it was a big part of being able to decouple the detection capabilities that Anvilogic offers from the data storage capabilities of a data lake, which is a big use case as well.

Our data lake is run on top of AWS using Snowflake.."

Verified user

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

“Anvilogic serves as my cybersecurity company's platform that provides detection, SIEM support, and SOC investigation, along with the implemented MITRE ATT&CK framework.

“A specific example of how I use Anvilogic in my daily work is that it provides threat detection, reports, detailed reports, detection engineering, and threat hunting, which is quite good.

“Anvilogic's threat hunting feature has made my work easier because it supports advanced threats and attack scenarios, analyzing across platforms to detect both known and unknown threats, which proves very useful for my organization.

“Anvilogic has changed how my team thinks about detection by improving detection engineering, reducing false-positive alerts, and integrating hybrid SIEM and data lake architectures, and so far, it has been beneficial.

“What surprised me the most about Anvilogic once I started using it is the automation capability, which automatically detects and investigates threats such as malware and provides us with reports, making the automation aspect very strong in this software.

“Since onboarding, my usage has evolved. During the first 90 days, the software wasn't configured properly, and we were just understanding its basics. As use cases increased daily, we altered and modified some policies and rules to reduce false-positive reports..”

Evans Vasavan
Security Engineer at GlobeSecure Technologies Pvt Ltd

Read full review

©2026 PeerSpot, All Rights Reserved

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.

"Before choosing Anvilogic, we did not evaluate other options and directly purchased it from a vendor who offered it to improve our organization's capabilities. After trying it for two years, it has been working well.."

Evans Vasavan

Security Engineer at GlobeSecure Technologies Pvt Ltd

Read full review

"My experience with the pricing, setup costs, and licensing of Anvilogic has been positive. I actually really appreciate the pricing that we came into because I viewed Anvilogic as a one-for-one with enterprise security.."

Brandon Bryant

Director, Cybersecurity Operations at Labcorp

Read full review

©2026 PeerSpot, All Rights Reserved

"Since onboarding, we started with rough, quick migrations of log sources and detections from Splunk to Anvilogic, but we have since cleaned up a lot of our normalization tasks and ensured things are correctly categorized, steadily deploying more Armory detections onto our existing data sets for better coverage.."

Verified user

Read full review

Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

"We are pure cloud based, and we run on top of Snowflake. The deployment was very simple. We were in the early phase for Snowflake, so there were a couple early implementation hiccups, but we partnered with Anvilogic on those, and that was kind of part of us being that early implementation partner. We paved the way for future Snowflake customers.."

Roger Allen

Read full review

Senior Director | Detection Response at a tech vendor with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

"Since Anvilogic was a new concept and product, we needed to invest a lot of time in training our team to adopt it. Fortunately, during the evaluation phase, we established clear success criteria, one of which was training on Anvilogic. The Anvilogic team has been with us from the very beginning of this process and continues to support us today.

We have detections in multiple places. Most of our detections are on-prem, but there are some that are in the cloud. We use their integration pipelines to bring all of them together.."

Verified user

Read full review

Director, Cybersecurity at a financial services firm with 10,001+ employees

"The initial setup was quite easy for us. There was a bit of a learning curve, which involved just understanding how the platform worked, taking about a month, but integrating with our existing platforms was a piece of cake. They have APIs for most things and standard off-the-shelf solutions such as SIEMs, endpoints, firewalls, and identity providers. It was very easy to integrate. The technical integration was very easy. It took about a month of learning from my team to get comfortable with the product and how to use it. It is one of the easiest security tools to learn.

The platform does not require any maintenance on our end, but once we start building out the detections, it requires some maintenance on our side to see that everything is running properly. That is more like an operational aspect.."

Ajish John

Read full review

Head of Information Security at a tech vendor with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

Customer Service and Support

"Customer support is generally good, though we sometimes have to wait longer for answers, which can be a bit frustrating, but overall the support is satisfactory.."

Verified user
Security Data engineer at a tech vendor with 5,001-10,000 employees

Read full review

"I think that they've been extremely helpful. We've been in a pretty thick deployment with them, so we've had regular engagement from the engineering team working with us.."

Brandon Bryant
Director, Cybersecurity Operations at Labcorp

Read full review

"The customer support is excellent. We have communicated with customer support frequently, and they always try to help and actively reach out to us. I would rate the customer support a ten.."

Ángel García Favieres
CyberSecurity Specialist at Aiuken

Read full review

©2026 PeerSpot, All Rights Reserved

"I would evaluate their customer and technical support as fantastic. Their support is excellent since they answer my questions. When I try to create new solutions within the scope, they work with me effectively.."

Jason Murphy
Vice President, Information & Cyber Security at St. George's University

Read full review

"The rating for the technical support of Anvilogic would depend on factors like who handles the request, but on a scale of 1 to 10, I would rate it around 6.5 to 7. Requests are typically addressed within 45 to 60 days, which I consider a reasonable timeframe given the number of customers.."

Verified user
Threat Researcher 2 at a tech vendor with 1,001-5,000 employees

Read full review

"Customer support is great, particularly from our immediate contact, Brad, who is very engaged and responds quickly, dedicating time to answer questions and onboard us effectively. However, outside of him, the process can get vague, with requests sometimes disappearing and lacking a clear tracking system, but overall, the experience is generally positive with some expected challenges from a smaller team.."

Verified user
Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Other Advice

"My advice to others looking into using Anvilogic is to absolutely go for it and feel free to test with the tool because it is very good and I appreciate it greatly. Anvilogic is a very good tool that I like to use because it is intuitive, user-friendly, and it helps significantly with detection engineering tasks. I rated this review an eight overall.."

Ángel García Favieres
CyberSecurity Specialist at Aiuken

Read full review

"When other teams ask about Anvilogic, I tell them it makes detection engineering into a process rather than a one-time operation.

"I convinced my leadership to adopt Anvilogic by comparing it to the manual operations and the overhead of repeated detection engineering processes.

"My advice for others looking into using Anvilogic is to start with the configurations and detection rules that come prepackaged, and then reach out and create your own to expand your capabilities; once you start using this system, it becomes much easier and more efficient than manually maintaining detection rules.

"I provide this review with a rating of 10.."

Joe Moore
Cybersecurity Architect at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

“The AI capabilities mentioned on Anvilogic's website are indeed good and promising; however, there are areas that require work, particularly concerning data ingestion. Users may encounter roadblocks while integrating inputs, as we faced significant delays due to data input inconsistencies.

Initially, the triage piece was not integrated into Anvilogic's UI, but since its integration, it has helped the team to easily check the triage dashboard and assess current use cases, encouraging us to continue seeking new ways to use it more efficiently.

The moment we realized we needed something better was triggered by Splunk's lack of AI integration, which prompted my manager to consider Anvilogic due to its promising AI features. Since onboarding, we have evolved to remove false positives effectively, which was a challenge with Splunk, allowing for fewer alerts due to Anvilogic's capabilities. Additionally, we no longer need to be dependent on a particular data repository, benefiting from the flexibility that Anvilogic provides.

I rate Anvilogic a six out of ten. I chose a six out of ten for Anvilogic because, despite the impressive detection capabilities and intriguing features, I still see a need for improvement with the data ingestion process. If the data is not ingested properly, the detections could be compromised. While it excels at detection and offers good use cases, my personal experiences with certain problems influenced the decision to rate it just above average..”

Verified user
Security Data engineer at a tech vendor with 5,001-10,000 employees

Read full review

“Anvilogic has changed how my team thinks about detection and data usage because it makes it easier to follow than other tool sets. Since a lot of the content is dynamic, you can follow the trail in the threat hunt perspective compared to other tools where you have to manually recreate a new query to investigate the action

©2026 PeerSpot, All Rights Reserved

further.

The moment that led me to choose Anvilogic was triggered because we normally evaluate vendors every so often to make sure we have a proper solution in place.

My usage of Anvilogic has evolved since onboarding and it is a bit more mature now, which certainly does help.

When other teams ask about Anvilogic, I tell them that it is fairly good.

There has not been anything that has become easier to justify or explain to leadership since adopting Anvilogic.

My advice to others looking into using Anvilogic is to conduct a test or proof of concept based on your actual future stance so that you feel the proper controls and everything is adequate to where you want to go.

I am looking forward to seeing how the tool will evolve and grow, especially with the AI features. I would rate this product overall as a 9 out of 10.."

Kevin Hernandez
Manager, Threat Intel & Detection Operations at Zendesk

Read full review

"My advice to others looking into using Anvilogic is that they should try it at least once by conducting a proof of concept, and if their use cases are met, they can proceed with confidence.

"When other teams ask about Anvilogic, I tell them it has helped significantly and has reduced work in reporting and investigation within my organization since adoption.

"I have not considered what would break first if Anvilogic disappeared, but I would

©2026 PeerSpot, All Rights Reserved

say the automation capability and reporting would negatively impact my organization.

“Looking 12 months ahead, I see Anvilogic playing a bigger role as features evolve rapidly. Any improvements in false-positive reports or new features would definitely enhance its role in my organization.

“The need for something better was triggered by the various threats present in the world, which needed to be improved and detected. For that reason, we chose to purchase this software, and having worked on it for the past two years, it satisfies our organizational use cases.

“I rate this review a nine overall..”

Evans Vasavan
Security Engineer at GlobeSecure Technologies Pvt Ltd

Read full review

“Another feature we are excited about, but we have not seen the value in yet, is the AI capabilities for detection engineering; it is, in theory, going to be very powerful and really reduce our time to develop new detections. There are more agentic features coming on the roadmap that have not been released yet, and we have not been able to see the full picture of value of that aspect of the product yet, but in theory, those should be extremely beneficial and really magnifying the amount of detection engineering work our team can do.

What surprised me the most about Anvilogic was the modern solution it offered to solving a SIEM business problem, which was different from other vendors. Anvilogic being a detection engineering tool makes sense and allows us to run it on any data lake background, which is unique. This decoupling of security detection from security data storage enabled us to pursue this path.

If Anvilogic disappeared tomorrow, we would lose our detection capability, which

©2026 PeerSpot, All Rights Reserved

would be significant and necessitate finding another vendor's solution.

I rate Anvilogic about a seven on a scale of 1 to 10.

I chose a seven because the platform is a huge improvement from our legacy SIEM platform in Splunk, especially from a detection perspective. However, there are certainly opportunities to improve the user experience and capabilities, as well as to mature the platform. These three aspects make a difference in execution and can improve competitive edge significantly.

I convinced our leadership to adopt Anvilogic by emphasizing the cost benefits of increased capabilities at a lower cost. The Anvilogic-Snowflake combination presented a centralized source, which is advantageous for reusing security data across other non-SIEM use cases, making it an easy sell.

My advice for others considering Anvilogic is that depending on your company's detection engineering needs and maturity with your legacy SIEM platform, Anvilogic can provide a swift, significant value add. If you have a dedicated SIEM team with many custom use cases built on a platform such as Splunk, Anvilogic may not be the correct fit. We were a small team managing a complex old system and were not getting the full value from Splunk. Anvilogic provided a more dynamic, low-overhead solution, making it a great fit for us, but for larger teams with custom detection needs, it might be less flexible.."

Verified user
Senior Manager, Threat Prevention Engineering at a tech vendor with 5,001-10,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

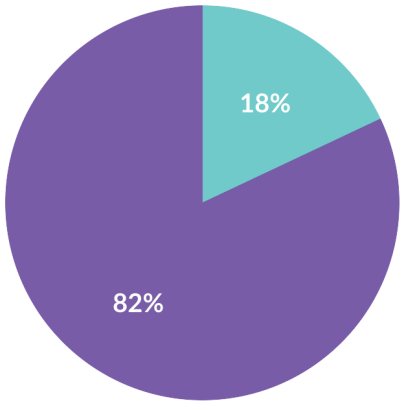
Top Industries

by visitors reading reviews

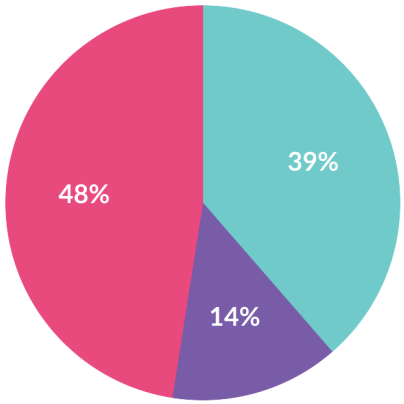
Financial Services Firm	14%
Outsourcing Company	11%
Comms Service Provider	8%
Healthcare Company	8%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved