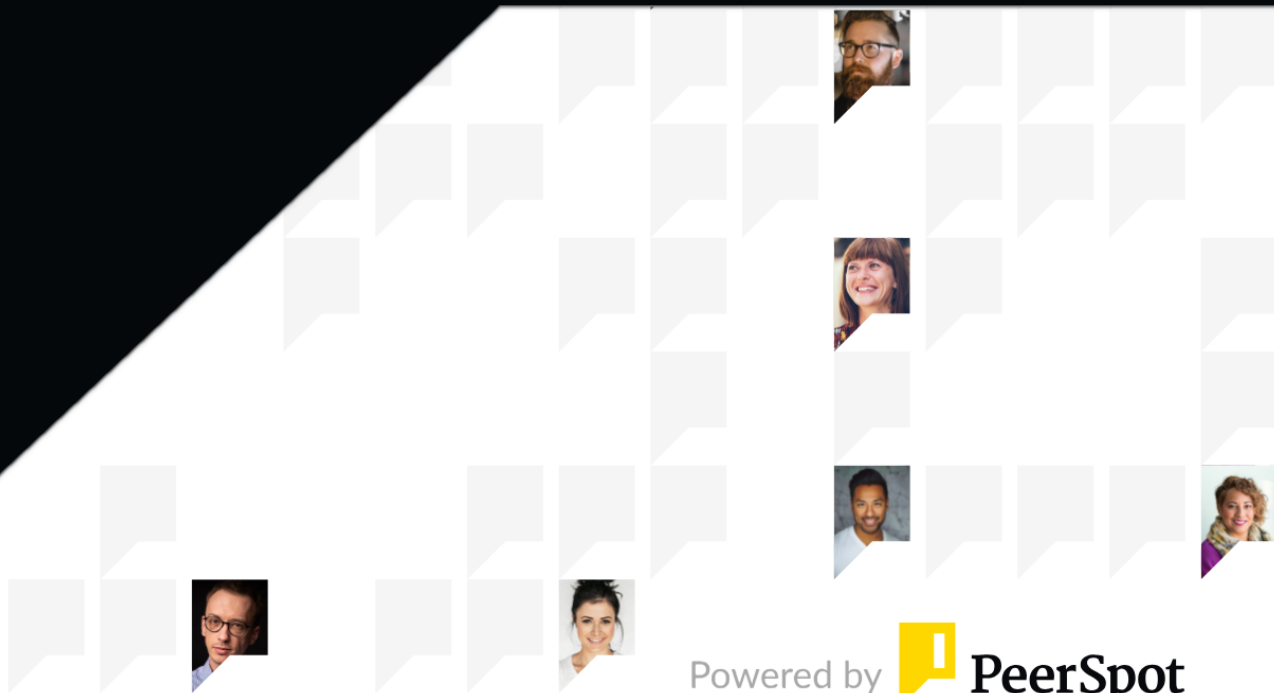


aws marketplace

Anomali

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 14

ROI..... 15 - 16

Use Case..... 17 - 22

Setup..... 23 - 24

Customer Service and Support..... 25 - 26

Other Advice..... 27 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

Product Recap



Anomali

Anomali Recap

Anomali delivers user-friendly cyber threat intelligence, offering concise insights with robust capabilities for evolving scenarios.

Anomali offers a powerful platform for cyber threat intelligence, allowing organizations to efficiently stream and analyze threat feeds. It excels in threat modeling, prioritizing intelligence, and supporting large-scale automation through its API, fostering a proactive security approach.

What are Anomali's Key Features?

- **Threat Intelligence:** Provides concise and user-friendly intelligence.
- **Threat Modeling:** Enables prioritization and efficient organization of intelligence.
- **Credential Monitoring:** Performs quickly with efficient dataset handling.
- **API Automation:** Supports large-scale automation for robust intelligence management.
- **Adaptability:** Offers capabilities to grow beyond initial use cases.

Which Benefits or ROI Should Users Consider?

- **Efficient Intelligence Collection:** Quickly gathers and organizes data for use.
- **Enhanced Threat Analysis:** Correlates data effectively for proactive security.
- **Automation Support:** Saves time with extensive API capabilities.
- **Scalability:** Adapts and scales with emerging security needs.

Anomali serves as a crucial tool for threat intelligence in industries ranging from finance to healthcare. Organizations stream threat feeds into Anomali to correlate and aggregate data, enhancing security measures and facilitating thorough threat investigations. Its adaptability makes it suitable across different sectors.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Anomali has positively impacted my organization and my clients by helping them improve threat visibility, accelerate incident response, and make better use of their resources.”



TarunKumar11

Global Leadership Council at a tech company with 10,001+ employees

- ✓ “Anomali has positively impacted our organization with many improvements since we started using it, as we receive many block hits from them, and we can say that our coverage has been extended to 90% because we do MITRE mapping.”



Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

- ✓ “I think it's one of the awesome tools I've worked with to date.”



Verified user

Lead Cyber Threat Intelligence Incident Response Engineer & Security Engineer at a retailer with 10,001+ employees

- ✓ “With Anomali, we benefit by obtaining threat information prior to incidents, making our threat hunts proactive and having incident response plans ready, which saves almost 40% of the time from the traditional model.”



SangramGupta

Security Consultant at Deloitte

- ✓ “I have seen a return on investment with Anomali, as it improves analyst investigation time, enhances threat visibility, and supports fast incident responses.”



R Nandasana

Senior Information Technology Security Consultant at Mideast Data Systems

- ✓ “Anomali is a very versatile platform, quite effective, and very fast when it comes to downloading and maintaining the information of the indicators of compromise.”



Verified user

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



“Anomali has positively impacted my organization because earlier we were not using any TIP format and were just dependent on open source, which gave us tons of irrelevant alerts, but with Anomali, we now get very specific and targeted alerts, allowing us to navigate through a handful of alerts that are applicable to us and saving a ton of working hours.”



Rajat Sawant

Sr. Threat Intelligence Analyst at a tech vendor with 10,001+ employees

What users had to say about valuable features:

“The best features Anomali offers, in my opinion, are the dynamic dashboards that we can easily create and Anomali Query Language, which is very fundamental and very useful for us.

The dynamic dashboards and Anomali Query Language are so valuable for my work because when we talk about data, the tough part is how to represent it. Anomali eases out that highly important task for us because we cannot go to leadership and tell them in numbers. The widgets and dashboards make it more attractive and make it easier to represent and help others understand. Anomali adds a bonus to it because it makes it really easy for us to do that..”

Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#)

“The best features Anomali offers are that it shows all the information on the particular dashboard, whether something is malicious or not and what the reputation status is.

Anomali has impacted my organization positively because our SOC team, which is actively monitoring all the tools—either SIM, SOAR, or threat intelligence platform—operates in multiple shifts. It has impacted our organization in a positive way by showing whether malicious activities or APTs are present. Whatever attackers are there, it shows on the dashboard and we can perform our analysis and execute remediation effectively.

Anomali has improved our MTTR and MTDD..”

Verified user

Security Analyst L2 at a financial services firm with 10,001+ employees

[Read full review](#) 

“In my opinion, the best features Anomali offers include the ability for other organizations to score the intel according to their analysis, which helps us to grab more details about that alert and get more depth on that alert. Scoring the intel has helped my team significantly; for a particular incident, we were unsure whether it was impactful or not, but considering other organizations rated it high, we thought it was an important alert that should be investigated. Otherwise, it would have been overlooked as a benign event.

Anomali has positively impacted my organization because earlier we were not using any TIP format and were just dependent on open source, which gave us tons of irrelevant alerts. Segregating those alerts was a big task, but with Anomali, we now get very specific and targeted alerts, allowing us to navigate through a handful of alerts that are applicable to us. It has saved a ton of working hours..”

Rajat Sawant

[Read full review](#) 

Sr. Threat Intelligence Analyst at a tech vendor with 10,001+ employees

“One of the best features that Anomali offers is its excellent integration with Splunk, SOAR, and various EDR tools. Anomali can also be used with many firewall solutions. I appreciate this feature because if any attacker enters our environment, they likely go through our firewall or bypass it. Anomali's threat intelligence feed saves a lot of my time and has flexible deployment options, which I also value.

The user interface of Anomali is somewhat complex for new users. If you are a security professional familiar with hardware and have a background in cybersecurity, it is manageable. However, it can be complex for IT personnel or developers who may not be as experienced in cybersecurity.

Anomali has positively impacted my organization by improving dashboard experiences and reporting capabilities. It simplifies many workflows for analysts, allowing them to save time and acquire accurate information. .”

R Nandasana

Senior Information Technology Security Consultant at Mideast Data Systems

[Read full review](#) 

“Anomali's best features include its mature threat intelligence platform with a large intelligence repository, which is a major strength. It has strong feed aggregation, aggregating feeds from over 200 sources. It offers fairly reasonable automation capabilities that make it easy to operationalize threat intelligence.

“Among these features, threat intelligence operationalization stands out as making the biggest difference for organizations. It aggregates intelligence from hundreds of sources, automatically de-duplicates, applies risk scoring, applies context, and reduces much manual effort. Threat intelligence operationalization represents Anomali's best feature—its ability to turn raw threat intelligence into actionable security outcomes.

“Threat intelligence operationalization, combined with a comprehensive threat intelligence platform, aggregation through various feeds, automation, integration, and strong correlation with MITRE, is what organizations should primarily use Anomali for. Organizations need to use these capabilities much more coherently.

“Anomali has positively impacted my organization and my clients by helping them improve threat visibility, accelerate incident response, and make better use of their resources. Anomali has reduced incident response times by providing context around threats and indicators. It has significantly reduced analyst workload through automation and reduced the effort required for correlations. Additionally, it provides better vulnerability prioritization and much stronger visibility into cyber risk and emerging trends..”

TarunKumar11

Global Leadership Council at a tech company with 10,001+ employees

[Read full review](#) 

“The best features I have used in Anomali include threat intelligence management. It provides a comprehensive and centralized threat intelligence feed for us. Based on a specific industry, we can gather all the threat IOCs with this tool. Those threat reports can be easily passed to the vulnerability management team, the threat hunting team, and the SOC team. Those threats are helpful for them to hunt a threat in a proactive way.

Reporting is another valuable feature we have used. It provides comprehensive threat reports based on IOC enrichment and correlations. Those reports are helpful whenever we provide that data to the SIEM team or SOC team.

Anomali has positively impacted my organization by improving efficiency and reducing risks. I can provide a practical example involving monitoring indicators associated with ransomware campaigns. Anomali helps us correlate the threat intelligence with internet security technology, allowing the overall team to identify potentially relevant indicators. Without a threat intelligence tool, the SOC team would require more time to investigate or act upon the incident management plan for that threat actor. With Anomali, we benefit by obtaining threat information prior to incidents, making our threat hunts proactive and having incident response plans ready, which saves almost 40% of the time from the traditional model.

The 40% time savings have significantly impacted my team and business. In the traditional process, the SOC team relied only on the SIEM solution and the logs it gathered. Whenever it detected any potential threat or risks, they needed to manually check and hunt for the threat, consuming significant time. With Anomali, the SOC team is already aware of the nature of the threat, the threat actor, and the IOCs. This allows us to easily develop an incident response plan or proactively hunt for that threat or vulnerability, utilizing all the data from Anomali. This reduces the time for incident response by 40 to 50% overall compared to the traditional approach..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

Other Solutions Considered

Before using Anomali, I used ThreatConnect. I decided to switch from ThreatConnect to Anomali really for commercial reasons. ThreatConnect is also a quite complete platform.

Verified user

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

[Read full review](#) 

“We have not used any other TIP solution before Anomali, although we have done proofs of concept of multiple clients' solutions, but we have not opted for any of them over Anomali..”

Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

“Before choosing Anomali, we evaluated other options such as Google Threat Intel platform, Palo Alto Threat Intel platform, and ThreatConnect, and we found them not to be as mature as Anomali..”

Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

“I did not previously use a different solution before Anomali. This was a solution that was not present in most of our clients' environments. My clients had point solutions, but they did not have a comprehensive solution that could correlate, and therefore no platform like this existed..”

TarunKumar11

Global Leadership Council at a tech company with 10,001+ employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I do not have specific ROI numbers, but we have saved a lot of time. Previously, we needed to sift through extensive data via SIEM solutions to achieve visibility and prepare dashboards manually, but now we can identify metrics quicker..”

Aditya Yadav_

[Read full review](#) 

Associate Consultant at a tech vendor with 1,001-5,000 employees

“I have seen a return on investment with Anomali, as it improves analyst investigation time, enhances threat visibility, and supports fast incident responses. The time taken for analysts to identify and resolve issues has significantly decreased since we started using this product..”

R Nandasana

[Read full review](#) 

Senior Information Technology Security Consultant at Mideast Data Systems

“We have seen a return on investment, as we saved a lot of time because performing our threat intelligence manually is a very tedious task that we cannot handle. Anomali provides us with a very cost-effective value compared to the market, and I would rate it ten out of ten for return on investment metrics..”

Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

“I have seen return on investment with Anomali, with relevant metrics including money saved, fewer employees needed, and time saved. Many clients have reported SOC efficiencies in terms of reduction in mean time to detect and mean time to respond. Analyst productivity has improved significantly, with hours saved because of automation and AI-driven work that Anomali performs. Risk reduction matrices are also available, including the number of incidents prevented or detected in time.

“Specific metrics related to these improvements include a thirty to fifty percent reduction in manual threat analysis effort and a twenty to forty percent reduction in investigation time. Anomali also improves mean time to detect and mean time to respond by enhancing analyst activity..”

TarunKumar11

Global Leadership Council at a tech company with 10,001+ employees

[Read full review](#) 

Use Case

“My main use case for Anomali is that we use it as a TIP. As a TIP in my day-to-day work, we have specific rules configured for our organization. The client we work for is an FMCG client, and we have built alert cases around that, including supply chain attacks, vendors, and the technologies we use in that client. Anything triggered around those use cases will be notified to us, and then we investigate the alerts.

Apart from this main workflow for our team, we use the Sandbox of Anomali. Specifically, our SOC team uses that, and we have integrated Anomali with our security tools including Defender and CrowdStrike in order to block the IOCs..”

Rajat Sawant

Sr. Threat Intelligence Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“My main use case for Anomali is for threat intelligence. We have a threat stream and threat practice on that. We are checking overall and verifying malicious websites, malicious hashes, and malicious URLs that are coming to the internal organization.

I can give a quick specific example of how I use Anomali in my workflow. I have used Anomali to check which malicious URLs and websites are attacking our internal organization. We check the threat intelligence portal like VirusTotal and other sources, and if the reputation of that URL is malicious, we block it in Anomali..”

Verified user

[Read full review](#) 

Security Analyst L2 at a financial services firm with 10,001+ employees

“I was using Anomali primarily for threat intelligence operations, security monitoring, and threat detection initiatives. I was part of the SOC team, and my role and responsibilities involved working with threat intelligence feeds and providing comprehensive threat reports on a weekly basis to the SOC team.

The primary use case was threat intelligence. Before using any threat intelligence tool, the SOC team must rely on the logs they receive from their SIEM solutions. If we integrate threat intelligence into the overall practices with Anomali, it helps us gather all the threat information beforehand so that the SIEM engineers can schedule or create rules based on those threats or the nature of threats, making the threat hunt easier for the SIEM solutions or the SOC team. This approach is impactful for using the tool..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“My main use case for Anomali is to use the Threat Intelligence platform to enrich our incidents. We have our own SIEM, so we use Anomali to enrich and segregate some of our threat rules, which is the main purpose for using it. Additionally, we receive threat IOCs from Anomali that we use to secure our environment.

A specific example of how we use Anomali is when we ingest threat intelligence feeds for many security alerts we are running. For instance, we discovered some anonymous IPs and certain files in our system. Based on these detected files, we get IOCs from Anomali, which prioritize our incidents if they identify critical files or hacker activities, thereby helping us hunt these threats effectively.

Regarding my main use case for Anomali, I do not have many additional use cases. Anomali is primarily a platform that adds more detailed information to our ServiceNow incidents created via SIEM, which we use in conjunction with Splunk and EDR. This integration significantly reduces false positives by providing context, enabling us to identify wrong files or IPs more efficiently. .”

R Nandasana

Senior Information Technology Security Consultant at Mideast Data Systems

[Read full review](#) 

“My main use case for Anomali is as a TIP platform, and the multiple services that I use include Security Analytics, Anomali SaaS platform, and Anomali Integrator.

A specific example of how I use Anomali in my daily work is that we have integrated all of the security controls present in our environment with Anomali. Anomali collects all the intelligence throughout the globe, and we distribute it further to our different security controls. We have a Security Analytics platform from Anomali, and with that, we have integrated our SIM and TIP platform together. With that, we can easily flag which IOCs are interacting with our environment and at what pace and what action is occurring. For example, if an action is allowed, blocked, dropped, or denied, we can easily flag the IOCs interacting with our environment and take quick action against them.

With Anomali, we create many dashboards that are very useful to present in leadership meetings so that leadership can easily understand the data, which IOCs are interacting with our environment, what are the top malwares within our industry, what are the top ransomwares, and what is the nature of the IOCs interacting within our environment. We create beautiful widgets and dashboards with the Security Analytics platform and present them to leadership..”

Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

“I have had exposure to Anomali for over five years and have been advising many clients regarding a cyber threat intelligence platform they could use. I have recommended Anomali to many of my clients throughout this period.

“My main use case for Anomali is rooted in the fact that there are many use cases within cyber threat intelligence, which is what Anomali stands for. This helps organizations aggregate, enrich, prioritize, and operationalize threat intelligence across its security operations. Primary use cases include security operations, threat hunting, incident response, threat intelligence, and automated blocking.

“I can provide a specific example of how I have seen Anomali used for threat hunting or incident response. A scenario I have advised on involves Anomali's use of artificial intelligence, which has made it analytical driven. It performs threat correlation, intelligence enrichment, and provides better pattern recognition through risk scoring. This makes it quite trustworthy and helps organizations prioritize intelligence through enrichment. I have seen Anomali provide strong results to businesses at large.

“Anomali helps achieve faster threat detection and faster incident response through improved productivity of analysts who would otherwise perform many tasks manually. Automation helps significantly in enrichment and correlation of indicators of compromise. This allows organizations to make better decisions with respect to threats and enhances regulatory and executive reporting..”

TarunKumar11

[Read full review](#) 

Global Leadership Council at a tech company with 10,001+ employees

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.

“I would describe the initial setup process of this solution as similar to the regular features of boarding. At first, the second part of onboarding was to integrate the systems that need to be treated by an anomaly and that require a bit of technical knowledge and architectural knowledge and that lasts long and is an ongoing process. There are 10 people involved in the deployment of this solution. The vendor is tasked with the maintenance of this solution..”

Peter Pamuk

Managing Member at a tech vendor with self employed

[Read full review](#) 

“Anomali follows a subscription-based model for pricing, setup cost, and licensing. Their licensing is typically a combination of the number of modules you would use. It is based on the number of analysts using Anomali, the number of intelligence feeds, and whether deployment is on-premise or SaaS. For a global enterprise, costs can range from two hundred fifty thousand to five hundred thousand dollars, and mid-size organizations might spend seventy-five thousand to one hundred thousand dollars. SaaS deployment usually costs less. Mostly it is an annual platform subscription, and multi-year deals for three to five years can provide good discounts..”

TarunKumar11

[Read full review](#) 

Global Leadership Council at a tech company with 10,001+ employees

Customer Service and Support

My experience with Anomali's customer support has not gone so well for us. Not because they are bad at support, but because the tool being limited means the support people fall short.

Verified user

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

[Read full review](#) 

“Regarding the technical support, we have contacted them for the automation part that we are running through compatibility problems and they were slow to solve our problems..”

Peter Pamuk

Managing Member at a tech vendor with self employed

[Read full review](#) 

Support in the past has been top-notch, but recent trends indicate that it has taken a back seat, as we often don't get answers for days. We'll receive excuses such as "I was out of the office" or "I forgot to follow up on this, I apologize." While they apologize, it doesn't seem very professional how they're handling support anymore.

ChrisCollins

Enterprise Security Architect V at FirstEnergy

[Read full review](#) 

“The customer support provided by Anomali is the best in the market.

My advice to others looking into using Anomali is to go all out for Anomali. Trust their customer service as it is the best in the market. They will provide you with the best support, listen to your challenges, work at the back-end for your challenges, and come up with a solution as soon as possible..”

Dichandna Shandana

[Read full review](#) 

Solution Delivery Advisor at a tech vendor with 10,001+ employees

“Anomali customer support is known for being absolutely very good for enterprise customers. I would rate Anomali customer support as very good with very responsive support for critical issues. They have strong onboarding and deployment assistance, provide a dedicated technical account manager for large customers, and engage in regular product updates and customer interaction. Resolution times can vary depending on the issue, and this is an area where they can further improve. Smaller customers may not receive the same level of attention as large customers do.

“I would rate Anomali customer support on a scale of one to ten as approximately an eight point five. For responsiveness, technical expertise, and implementation support, I would rate it a nine out of ten, as my experience has been quite solid..”

TarunKumar11

[Read full review](#) 

Global Leadership Council at a tech company with 10,001+ employees

Other Advice

“My advice to others looking into using Anomali is that it is a good platform to start with if you do not have any TIP solution in your organization. I would rate this review eight out of ten..”

Rajat Sawant

Sr. Threat Intelligence Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“My advice for others looking into using Anomali is to identify clear intelligence use cases before deployment. Defining specific use cases is essential, especially when focusing on threat intelligence in SOC workflows. Anomali may not help with every issue that occurs in the SOC..”

R Nandasana

Senior Information Technology Security Consultant at Mideast Data Systems

[Read full review](#) 

“I have used Anomali for the past four months in my previous organization.

There is nothing else I would like to add about the features.

On a scale of one to ten, I would rate Anomali an eight to nine. I would give Anomali that score because we see Anomali as a threat intelligence platform and we can work with it and improve the MTTR. I rate this product eight out of ten overall..”

Verified user

Security Analyst L2 at a financial services firm with 10,001+ employees

[Read full review](#) 

“Regarding Anomali's accuracy and reliability of output, I think it is important to have someone from the security engineering side validate all the outputs from the tool. Once the output has been validated, it should be passed to the incident response team.

If you are involved in cybersecurity practices, specifically in defensive security, responsible for threat hunting, threat intelligence, and vulnerability management or SOC operations, you can implement this tool in your system or environment. It can proactively provide you the threat feed, threat actor details, and IOCs, helping you create a better incident response plan and hunt threats proactively..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“I would clearly recommend Anomali to organizations, as I have done in the past.

Anomali is appropriate for clients who have a mature security operating center consuming multiple threat intelligence sources and want to operationalize their threat intelligence across their security ecosystem. It is not suitable for small organizations with limited security maturity but rather for large, enterprise-level grade setups. New customers should define their threat intelligence objectives, start integrating and ingesting everything in a platform like Anomali to maximize value, and regularly fine-tune and review to reduce noise from intelligence sources and feeds. Treat Anomali as a strategic intelligence platform rather than simply a feed repository. I would rate this review overall as an eight out of ten..”

TarunKumar11

[Read full review](#) 

Global Leadership Council at a tech company with 10,001+ employees

“Anomali integrates with other security tools or platforms in our environment using on-premises integrators.

We manage threat intelligence feeds within Anomali by having both automated and manual processes. We integrate open-source feeds, paid source feeds, and trusted circle groups that we have particularly joined. We perform a monthly activity to check how many false positives we get from the feeds that we have integrated using the feed optimizer option. This is how we manage our feeds and keep a check on whether we are getting many false positives, how they are interacting with our environment, and if we are receiving daily updates from the feeds or if we are getting feeds at their certain refresh interval.

We handle false positives in Anomali by following a process for reviewing those IOCs that are of our business needs but are flagged by different sources. We follow tagging procedures. For example, certain IOCs are marked malicious from one feed, but they are not highly malicious or they are for our business needs. We label them as false positive tags, and within our rules created for sharing intelligence with our integrators, we exclude that data with that particular false positive tag.

To ensure compliance or regulatory requirements are met using Anomali, we follow a quarterly review activity in which all patch updates and all the vulnerability assessments are performed for the servers that Anomali utilizes. We conduct a complete application-level assessment on a quarterly basis. After that, we get a list of vulnerabilities found within the servers involved with Anomali, and we take actions to fix those vulnerabilities or the assessments found.

User access and permissions within Anomali are role-based.

We maintain and update Anomali's threat intelligence sources by manually reviewing the sources.

The learning curve for new users on Anomali is very easy. Anomali University portal provides very good learning insights, making it easy and user-interactive. I would rate this product a nine out of ten overall..”

Dichandna Shandana

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

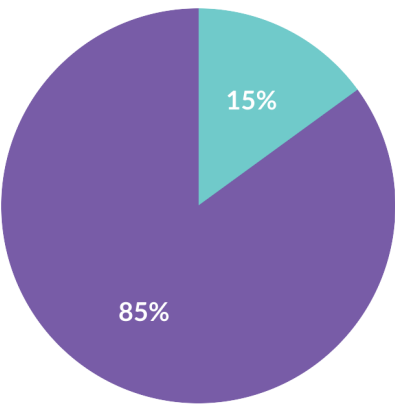
Top Industries

by visitors reading reviews

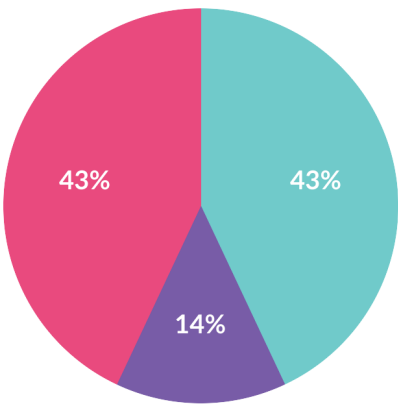


Company Size

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