aws marketplace

Anomali

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

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:

- "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

- "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

- "We now have a very robust collection of threat intelligence based on the capabilities that Anomali provides."

ChrisCollins

Enterprise Security Architect V at FirstEnergy

"Anomali positively impacts our organization, notably improving our vulnerability management program under reducing attack surface management."

Aditya Yadav_

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

"The most valuable aspect of Anomali is the threat modeling capability."

Sai Puneeth Gundamraju

Senior Cyber Threat Hunter at a financial services firm with 10,001+ employees

"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."

Verified user

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

"The feature I have found most valuable is credential monitoring. This feature is easy and quick."

Peter Pamuk

Managing Member at a tech vendor with self employed

What users had to say about valuable features:

The most valuable aspect of Anomali is the threat modeling capability. It collects threat intel documents and IOCs and allows us to tailor it to our needs and prioritize intelligence requirements (PIRs). This enables us to receive prioritized threat intelligence.

Sai Puneeth Gundamraju
Senior Cyber Threat Hunter at a financial services firm with 10,001+ employees

Read full review

The API is our most important feature. We are very much into automation, so being able to handle things programmatically at scale has been immensely powerful for us. We've evolved beyond just the two use cases I mentioned. One of the things we decided to do is utilize the Anomali API to push everything into that platform after sorting and normalizing everything. We now have a very robust collection of threat intelligence based on the capabilities that Anomali provides. It's very adaptable; you can do a lot with it, making it a very powerful tool.

ChrisCollins
Enterprise Security Architect V at FirstEnergy

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

I consider the best features offered by Anomali to be its versatility, good information, various integrations, and feeds that are free. There are also others that are integrated and paid, but its capacity is large. It really has a high storage of indicators of compromise and its reliability is quite accurate.

Anomali has positively impacted my organization significantly; it has been a great help. 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. Additionally, it has a large amount of information about those indicators of compromise, such as their score and evaluation, and it also brings where they come from and tries to attach vectors to those indicators, which makes threat intelligence and security bulletins much easier. All the information that it provides makes it much easier to analyze and generate valuable information. .”

Verified user

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

Read full review

"The best features Anomali offers are that it acts as an application that pulls data from different solutions. As I mentioned earlier, we utilize Mandiant, Flashpoint, and other CTI solutions. Using Anomali, I push all the results into it, providing a single UI to see what Flashpoint and Google Mandiant are providing rather than jumping into different platforms, which can be time-consuming. Anomali helps us stay on a single platform and provides the required results.

"The user interface in Anomali is very good. I have worked in Anomali for five years and think they have a great UI for writing queries and finding specific results much more efficiently than in other solutions where you need to scroll down through different widgets. Anomali has a query-based language, similar to SQL, that helps us dig out specific results, whether vulnerability-related or concerning threat actors and TTPs. We can also perform string-based searches. I think it's an awesome feature. Furthermore, regarding integration, Anomali has capabilities to integrate with different downstream applications such as Palo Alto, allowing us to create playbooks to block domains, URLs, or IPs directly within the firewall.

"Anomali has positively impacted my organization by reducing the time required to find intel specific to our needs. We can create our own queries specific to our organization and pull out results related to any posts within the dark web or any activities from threat actors targeting us. This capability enables us to create saved searches that provide exact results. I estimate that Anomali has saved me about 30% of my time.."

Verified user

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

Read full review

"The best features Anomali offers include the TIP platform and Anomali Analytics, previously called Anomali Match, which provides a perspective to identify our attack surface. Correlating IOCs with the telemetry data we are ingesting from our data sources allows us to pull monthly reports identifying how many assets and users interacted with malicious content, giving insight into whether communications failed or users accessed restricted content, providing complete visibility of the IOCs traveling throughout our environment.

Anomali Analytics, or Anomali Match, helped us identify scenarios where we were getting a lot of alerts on our SIEM solution for TOR activities. Some alerts were missed, but we identified through Anomali Analytics how many interactions were happening with malicious IOCs and TOR IPs associated with vulnerabilities. We were able to identify vulnerable systems that were not patched and were interacting with those threat IPs linked to the threat actor Skinny Hunter, targeting financial sector organizations.

We identified the IOCs within our environment, observed attack patterns for that threat actor, mapped those patterns to identify vulnerable assets, and recommended to the vulnerability management team to patch on priority.

Anomali's dashboarding stands out; they introduced Anomali Query Language, allowing us to create dashboards identifying specific data sources and logs we push to security controls. We had Palo Alto and Check Point firewalls where we tracked data to identify how many IOCs we pushed and how many passed through or were blocked, providing deeper insights from each integrated security control due to the correlation of the TIP platform and Anomali Security Analytics.."

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

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

"I have used many security solutions previously, such as ThreatConnect, Command, and Recorded Future. What I find is they all have different features, even though they work in a similar domain.."

Verified user
IT Cyber Security Senior Analyst at a consultancy with 10,001+ employees

Read full review

"Currently, we are not using any other solution for this use case, but previously we used MISP, which is an open-source project that requires a lot of effort to make work. That way, it required a lot of attention from our system administrator, and we had to sanitize the data very frequently because the peers we had. Sometimes they flooded our systems with chunk data and that needs to be handled and we decided to go with a paid solution instead.."

Peter Pamuk
Managing Member at a tech vendor with self employed

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

Read full review

Use Case

I use Anomali for threat hunting, threat collection, operationalization of intelligence, such as indicators of compromise (IOCs), and dissemination of reports for report writing and documentation.

Sai Puneeth Gundamraju
Senior Cyber Threat Hunter at a financial services firm with 10,001+ employees

Read full review

We use Anomali as our threat intelligence platform for a variety of threat intelligence feeds that we subscribe to, needing a more central place to store everything so we can correlate which feeds have seen this indicator before and which haven't. This was the biggest use case for us to solve, which is why we went after it. It is definitely more than just a threat intel platform where we store all these indicators; it's almost very much a threat hunting tool that allows analysts to do investigations on those indicators and make connections, looking for other related things that we didn't necessarily see. It allows us to take a more proactive kind of approach.

ChrisCollins
Enterprise Security Architect V at FirstEnergy

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

Read full review

My main use case for Anomali in my organization is threat intelligence. We use threat intelligence with Anomali in my day-to-day work to query feeds.

What we do is query those feeds looking for all kinds of indicators of compromise: IP, URL, and other indicators of compromise. They are evaluated according to the score given by Anomali, and we also do other processing for those indicators, validations for those indicators. After that analysis, they are integrated with the different security controls: firewalls, IPS, proxy, and among others.

"We also use it for hunting topics and security bulletins. ."

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

Read full review

"My main use case for Anomali was a proactive approach to integrate Anomali Threat Intel, the TIP platform, with different security controls. The customer had two use cases: one related to the proactive approach of ingesting the IOCs into different security controls such as their IPS, IDS, email security gateways, proxy, and endpoint systems so that any malicious activity or traffic coming into their environment would be proactively blocked on all their security controls.

We also had another use case where we wanted to get specific vulnerabilities whenever published for the specific products used within the customer's environment. Apart from that, we created some custom policies to detect any malicious activity based on the telemetry data Anomali Analytics was providing, triggering alerts and notifying us.

I utilized Anomali security analytics to understand our attack surface so we could know how many anomalies or malicious traffic was running into our environment. That helped in running threat hunting activities and identifying users and machines interacting with malicious IPs, hashes, or any IOCs exposed over the internet. It helped us to identify machines containing some vulnerabilities; if there is a vulnerability exposed that bad actors utilize, we focus on and prioritize those assets for patching.

We identified based on threat actors' activities if any threat actor is tightly associated with our organization type. Supporting a financial sector organization, we targeted and identified threat actors targeting financial and insurance sector organizations, helping us to proactively mitigate and secure the environment based on IOCs or attack patterns available for the specific threat actors.."

Aditya Yadav_

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

Read full review

"My main use case for Anomali is that it helps me with intelligence gathering and dark web monitoring. It has good functionality of integration with other solutions like Google Mandiant and Flashpoint, which are other CTI solutions. It also integrates with other SIEM solutions such as Splunk, allowing us to push all the indicators of compromise and IOCs to the SIEM solution. We can customize based on the confidence score of this indicator; for instance, if the confidence score is over 75, we push it to Splunk for real-time sightings within the network. I think it's one of the awesome tools I've worked with to date.

"A specific example of how I've used Anomali for intelligence gathering or integration with Splunk is that Anomali captures all the latest intel from various sources, whether forums, open sources, articles published on social media, or researchers posting their findings in their blogs. It collects all the TTPs, IOCs, and captures them to publish within Anomali. We push those indicators to Splunk via an API-based integration for real-time checks within the network if there are any sightings or hits.

"Regarding my main use case with Anomali, while much of it is confidential, one unique capability is Anomali's TAXII/STIX based integration with different platforms. For instance, we recently integrated with the CISA platform run by the US government, which provides us with the latest advisories. They push all the results into Anomali, creating a single UI that helps us avoid jumping into various sources to find intel, which I think is a unique feature of Anomali.."

Verified user

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

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.

"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

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

Other Advice

For new users, I recommend taking the training provided by Anomali as it is very well articulated. I advise reading the user manual and taking the instructor-led training sessions from the customer support success manager. This will effectively kickstart the journey. I rate the Anomali solution a solid nine out of ten.

Sai Puneeth Gundamraju
Senior Cyber Threat Hunter at a financial services firm with 10,001+ employees

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

"When it comes to other people trying to use this solution, I'd say, first of all, if they are planning to go with Anomali, the very first step they need to go through is to standardize the threat inter-ingestion processes they have. Without that, they can't use anomaly. This is because it builds on the processes you have. If you don't have these processes, you can't use that solution at all.

Overall, I would rate this solution a seven, on a scale from one to 10, with one being the worst and 10 being the best.."

Peter Pamuk
Managing Member at a tech vendor with self employed

Read full review

I think the platform is fine as it is for now. In terms of costs, Anomali is not the cheapest, but it has helped on the operational side in reducing the efficiency burden on staff. Not the reduction of staff as such, but in the efficiency of the staff on other tasks with the reduction of the administration of this platform. My advice to other people who are considering implementing Anomali is that they validate their infrastructure. If they have too many controls that will need Anomali to disseminate, they have to take into account that they are going to deploy many integrators, which translates into on-premise infrastructure, which raises costs and increases the administrative burden. Other than that, Anomali is a very good platform in terms of dissemination of indicators of compromise and all the benefits it has at the threat intelligence level. I give this review an overall rating of 8.

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

Read full review

"My advice for others considering Anomali is to go for it, depending on your organization. Whether it is retail, finance, or service-based, decide on your PIRs and use cases to evaluate if Anomali covers those adequately.

"Any new customers looking for a solution should consider Anomali as a great option. However, it depends on the organization; whether retail, finance, product-based, or service-based, you should evaluate the use cases for yourself, conduct a POC, and see if it meets all your needs. I would rate this solution an 8 out of 10.."

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

Read full review

You have to have at least a threat intelligence background or a SOC analyst background to use it, as that's the information you'll dig around with in there. If you don't have that kind of knowledge, it probably can be a little hard to use, but they do provide training. They offer training not only for how to use the platform but also some basic threat intelligence training to explain what these things are and what these terms mean.

My company is a customer of Anomali.

I would recommend it to other people.

I would advise making sure you don't pick it without testing other products and have your use cases well thought out and documented before testing, so you know it will solve the problems you're trying to address. Keep an open mind with it and realize that whatever you can dream of, you can probably do with the platform.

Overall, I would rate Anomali an eight out of ten. ."

ChrisCollins
Enterprise Security Architect V at FirstEnergy

Read full review

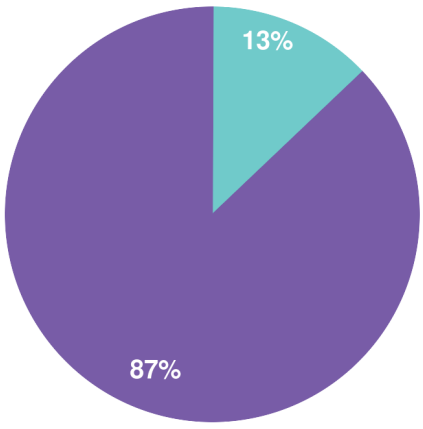
Top Industries

by visitors reading reviews

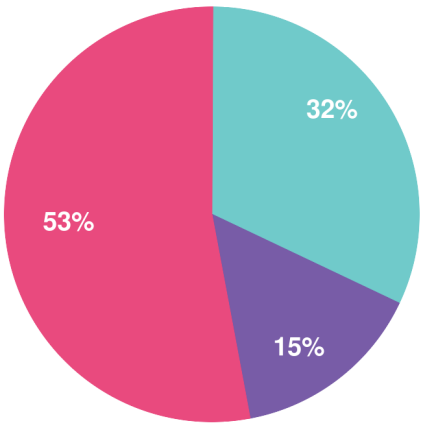
Financial Services Firm	14%
Construction Company	7%
Manufacturing Company	7%
Computer Software Company	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

About PeerSpot

PeerSpot is the leading review site for 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