aws marketplace

Akamai API Security

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Akamai API Security

Akamai API Security Recap

Akamai API Security offers robust protection against DDoS attacks and is highly valued for its efficient API throttling capabilities, allowing multiple users to manage traffic effectively. This ensures both optimal performance and enhanced security by controlling API access and utilization.

\n\n

Akamai API Security excels in safeguarding APIs with its industry-leading throttling features, allowing multiple users to prevent overload and abuse. By managing traffic efficiently, users can maintain service availability even under high demand or potential attacks. While the platform successfully combines machine learning with API throttling in its developing URL protection feature, there\'s room for improvement, especially in preventing false positives from reputable sources and precisely detecting threats from malicious hosting providers.

\n\n

What are the key features of Akamai API Security?\n
- **API Throttling**: Efficiently manage and control the flow of API requests, ensuring consistent performance and avoiding overloads.\n
- **DDoS Protection**: Robust defenses against distributed denial-of-service attacks, safeguarding the availability and reliability of services.\n
- **Machine Learning Integration**: Enhanced threat detection by distinguishing between legitimate and malicious API calls, refining security measures.\n
- **URL Protection**: Developing feature that combines machine learning and API throttling for advanced security, with a focus on refining accuracy.

\n\n

What benefits should be looked for in reviews when evaluating Akamai API Security?\n
- **Improved Performance**: Reduced risk of API overloads and maintained service availability during high traffic periods.\n
- **Enhanced Security**: Strong defenses against DDoS attacks and abuse, ensuring data integrity and safe access.\n
- **Efficient Traffic Management**: Smarter throttling mechanisms equipped to handle large volumes of requests, prioritizing legitimate usage.\n
- **Advanced Threat Detection**: Utilization of machine learning to better identify and respond to security threats.

\n\n

Implementation of Akamai API Security across industries varies. For example, e-commerce platforms benefit from its robust DDoS protection and API throttling, ensuring customer transactions remain secure and services available during peak shopping times. Financial

service companies use its machine learning capabilities to detect and block suspicious activities, preserving the integrity of client transactions while managing large volumes of API calls. Media streaming services leverage its ability to prevent overload, providing uninterrupted streaming experiences even during high demand events.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Ultimately, it has given us confidence that our data and services are well-protected."

Ron Machan
Cloud Engineer at HCL Software

- "Akamai API Security is preventing multiple issues, and the organization is doing well with Akamai API Security profits, which is good."

Alark Singh
IT Specialist at Allianz

- "Akamai API Security has been a strong and reliable solution for securing my APIs, especially in terms of visibility and behavioral-based threat detection."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

"If I had to say something positive about the product that brings me the biggest benefit, I would say visibility."

Verified user

System Engineer at a retailer with 10,001+ employees

"What I already appreciate about Akamai API Security is that initially we were struggling with how to get this configured, but after that everything went smoothly."

RaghavendraRao PV

Incident Manager at a computer software company with 1,001-5,000 employees

"Akamai API Security has positively impacted my organization by greatly improving my visibility into API exposure and risk posture, which has translated into concrete benefits as I can now proactively identify risky endpoints and apply protection policies, improving overall security and reducing response times to incidents."

Ronald Paz

Consulting Systems Engineer at Boomslang Tech

"Akamai API Security has impacted my organization positively because when a user tries to access our servers from all over the world, the traffic first hits the DNS security or Akamai edge firewall before reaching our perimeter or infrastructure."

Verified user

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

What users had to say about valuable features:

The standout features include automated API discovery, which helps us find even undocumented endpoints. The real-time behavioral analysis is valuable, as Akamai API Security detects abnormal patterns quickly. I also value schema validation to block improper requests and their bot management integration, which keeps malicious automation at bay.

It has made a significant difference in reducing risk. We have had fewer incidents of API abuse, such as scraping or suspicious traffic spikes. Our security posture is stronger because we have better visibility into all our APIs, even ones we did not initially know were exposed. Ultimately, it has given us confidence that our data and services are well-protected. ."

Ron Machan

Cloud Engineer at HCL Software

Read full review

"Akamai API Security helps comply with DORA compliance in the Europe region, preventing any compliance issues. It helps demonstrate that the ISO understands the secured side is protected by Akamai API Security, ensuring that if any DOS attack is present, it will not occur or take the side down.

"Currently, no improvements are apparent. In the last few years, there was improvement as bot attacks have been addressed, with more focus now placed on bot attacks. At that time, there was a drawback, but Akamai API Security is improving day by day. Currently, no drawbacks are evident, and the product is good. Akamai API Security is delivering the best products every year.."

Alark Singh
IT Specialist at Allianz

Read full review

"The best features that Akamai API Security offers, which I use most frequently and consider most important, are automatic API discovery and behavior-based anomaly detection.

My experience with automatic API discovery has shown that the platform continuously maps API endpoints and detects unusual traffic patterns, helping me identify exposed APIs that are uncontrolled and detect misuse.

The discovery of APIs and detection of usage based on behavior is an additional functionality that makes Akamai API Security different from traditional tools.

Akamai API Security has positively impacted my organization by greatly improving my visibility into API exposure and risk posture.

That improvement in visibility and risk posture has translated into concrete benefits for my organization, as I can now proactively identify risky endpoints and apply protection policies, which improves overall security and reduces response times to incidents.."

Ronald Paz
Consulting Systems Engineer at Boomslang Tech

Read full review

"The best feature Akamai API Security offers is that it gives full premium protection to hostnames and all the subdomains that are hosted on the platform. There is also a feature called Bot Manager Premier, which is auto fine-tuning by Akamai platform itself. Considering all the security posture being followed worldwide, the same database will be used to implement the security posture in our current organization as well. Beyond that, there are other tools such as DDoS management and bot management, and also all kinds of security related to OWASP Top 10 security.

Bot Manager Premier feature is a premium feature or a subscription that we have to take with it. When this is enabled, it gives premium security on the configurations that we have set for it and provides advanced expert level suggestions and configurations on those settings where it is configured.

Akamai API Security has impacted my organization positively because when a user tries to access our servers from all over the world, the traffic first hits the DNS security or Akamai edge firewall before reaching our perimeter or infrastructure. Before an attack goes live, we detect it on the WAF itself, which is the outer layer of security. We detect it and block it. We also set up security features such as crypto challenges or Captcha, which gives us ultimate protection against attacks.."

Verified user

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

Read full review

"If I had to say something positive about the product that brings me the biggest benefit, I would say visibility. Akamai API Security has capabilities that stand out, including how they classify the APIs into different categories such as PII information and identity information.

The anomaly detection feature helps with identifying potential breaches in my case. Because we baseline the traffic every day, we know our business and how much traffic we receive on each API endpoint. If we start receiving a huge volume of traffic on a specific API endpoint that we don't see regularly, it's classified as an anomaly, and we look into whether it is expected or an attack or a breach that is happening on that particular endpoint.

Akamai API Security also helps to monitor API usage trends in my case. When I say the word visibility, everything comes under visibility, such as who is calling the API. This product will give all the details.

Akamai API Security has a new feature called Adaptive Security Engine, which offloads us from the manual upgrading of firewalls. This helps to comply with regulatory requirements in my case. We go through these regular audits of PCI, GDPR, and all. All these audits will go through Akamai API Security because it is the key system that takes data and payment details.

It is also effective for protection against DDoS attacks, and we have implemented custom controls depending on the nature of the traffic and the business countries that we have. Different levels of controls are implemented to protect our systems from high-volume DDoS attacks.."

Verified user

System Engineer at a retailer with 10,001+ employees

Read full review

"One of the best features of Akamai API Security is its ability to automatically discover and map APIs, which gives complete visibility into all exposed endpoints, including shadow or undocumented APIs. This is very important from a security standpoint. Another key feature that stands out is the behavior analysis. Instead of relying only on static rules, it analyzes the normal API traffic patterns and helps in detecting anomalies such as unusual request volumes or abnormal user behavior.

"I also find the integration with WAF very effective as it allows me to enforce security policies such as rate limiting, access control, and protection against OWASP API threats in a unified way. Additionally, the detailed visibility and analytics it provides for API traffic, such as request patterns, client behavior, and threat insights, are very useful for both monitoring and troubleshooting. Among these, the most valuable feature for me is the behavioral-based detection combined with API discovery because it helps me to proactively identify unknown risks and secure APIs more effectively.

"Behavioral-based detection and API discovery have been very useful in my day-to-day operations, especially for identifying unknown risks. From an API discovery perspective, it has helped me identify shadow or undocumented APIs that were exposed but not properly secured. In one case, I found an internal data API that was accessible externally, which was not part of the official API inventory. This was potentially a security risk, and I was able to take immediate action to secure it.

"From a behavioral detection standpoint, it helped me understand what normal API traffic looks like, such as typical request rate, user behavior, and access patterns. Based on this baseline, I was able to quickly detect anomalies. For example, I observed a sudden increase in requests to specific API endpoints from a small set of IPs, which was not part of the normal behavior. Even though it was not triggering the traditional WAF rules, behavioral analysis flagged it as suspicious. Based on this, I implemented rate-limiting and access controls, which helped prevent potential abuse and ensured that the API remains stable. Overall, these features helped me to move beyond static rule-based security and enabled a more proactive and intelligent approach to API protection.

"Akamai API Security has had a very positive impact on my organization, especially in improving visibility and control over API traffic. One of the key

outcomes I noticed was a significant reduction in malicious API traffic, particularly bot-driven attacks such as credential stuffing and automated abuse. This helped improve the overall security posture of my application.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Other Solutions Considered

We previously used a cloud provider's native WAF and API gateway. We switched to Akamai API Security because we needed more advanced, API-specific protection, especially for detecting unknown or undocumented APIs that our previous tool did not handle as effectively.

Ron Machan
Cloud Engineer at HCL Software

Read full review

"I have worked with security tools for a total of seven years. Previously, I worked with GardiCore, and now I work with Akamai API Security. Regarding AlgoSec, I have used it in the past, but not in the current company. It was used a couple of years ago.."

Alark Singh
IT Specialist at Allianz

Read full review

"Other vendors are known, such as F5, Fortinet, Imperva, and Barracuda. These vendors are not currently being worked with, but F5 is being looked at, and another solution is in the POC phase, with feedback available upon completion of the POC. Currently, I primarily work with two products for these purposes: Akamai API Security and Illumio.."

Alark Singh
IT Specialist at Allianz

Read full review

We evaluated other options, including Cloudflare's API security offerings, as well as AWS's native WAF combined with API Gateway. Ultimately, we chose Akamai API Security because its API discovery, schema validation, and global edge network offered deeper and more tailored API protection for our hybrid environment.

Ron Machan
Cloud Engineer at HCL Software

Read full review

"I chose a rating of seven instead of a higher or lower rating because there are other technologies and solutions in the market such as Cloudflare, Radware, and F5 that also come under the API security category. Considering those solutions, they have other features which might be more convenient for users and administrators than what Akamai offers. The same applies on both sides. There is no tool that combines all of the features from all kinds of solutions provided together. Akamai API Security also has some missing features that might be more convenient for users, features that are present in other WAF technology solutions.."

Verified user

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

Read full review

ROI

Real user quotes about their ROI:

We have definitely seen ROI. For example, by preventing API-related incidents, we estimate saving tens of thousands in potential breach costs. We have also reduced incident response time by approximately 30 percent, freeing up our security team to focus on other tasks. While it is an investment, the savings in risk mitigation and efficiency make it worthwhile.

Ron Machan
Cloud Engineer at HCL Software

Read full review

"I have seen a return on investment with the platform in visibility, gaining 40 to 50 percent across my entire environment compared to what I had before, and the time reduction for incident investigation has dropped significantly.."

Ronald Paz
Consulting Systems Engineer at Boomslang Tech

Read full review

"I observed some savings from Akamai API Security, including time savings or money savings. We calculated the availability because if the website is down, we won't be able to trade.."

Verified user
System Engineer at a retailer with 10,001+ employees

Read full review

"There are good savings because if the site goes down, financial losses will occur. Akamai API Security is preventing multiple issues, and the organization is doing well with Akamai API Security profits, which is good.

"In percentage terms, from last year, more than 30 to 40% is being saved, and it is ongoing. Time-saving is significant at 30 to 40%, and it is growing year by year at a rate of about 10% to 15%, demonstrating growth.."

Alark Singh
IT Specialist at Allianz

Read full review

"I can identify all of these benefits after the implementation of Akamai API Security. Identifying and following up with the team was previously very challenging. Teams are reluctant to provide information, some managers ask us to look at their Confluence page, our time is wasted, and everyone's time is wasted. We have to follow up with the developers, they are on leave, and everything was a mess. Getting everything from one single portal without anyone's interference saved us a lot of money, time, and frustration.."

RaghavendraRao PV

Incident Manager at a computer software company with 1,001-5,000 employees

Read full review

Use Case

“My major use case is that we consume Akamai API Security. We use it to protect our API endpoints, as all our applications are microservices and APIs are the core communication endpoints, and we use API Protector to protect those endpoints..”

Verified user
System Engineer at a retailer with 10,001+ employees

Read full review

Our primary use case is protecting public-facing APIs that handle sensitive customer data. Day-to-day, we use Akamai API Security to monitor API traffic for anomalies. If we see unusual request patterns, such as a spike in calls from one IP, we can immediately enforce rate limits or block suspicious actors, ensuring only legitimate access is allowed.

We also leverage Akamai API Security for API schema validation. We ensure incoming requests match the expected structure. If anything deviates, whether it is malformed or unexpected, Akamai API Security blocks it, which protects us from abuse and accidental errors. .”

Ron Machan
Cloud Engineer at HCL Software

Read full review

"My main use case for Akamai API Security would be providing security to the hostnames and to the API URLs and paths that have been hosted on the Akamai platform. On a daily basis, there will be multiple traffic instances and false positive traffic that comes into our alerts such as unwanted bots and non-legitimate users hitting our retail market website, forcing it to crash or causing the server to be down with multiple 403 errors, which prevents users from accessing the website. For that, we set multiple alerts. If there is 5,000 hits per minute, then the alert will be generated and using that, we perform analysis and fine-tune our rules so that the illegitimate and unwanted traffic are blocked.."

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

Read full review

"Akamai API Security serves as our primary tool for API discovery, risk evaluation, and behavior-based threat detection. The platform provides us with visibility into all active APIs, including endpoints, and helps us reduce our attack surface.

Akamai API Security identifies undocumented APIs, commonly known as shadow APIs, and analyzes traffic to detect anomalies such as credential abuse, excessive requests, or suspicious patterns of data access.

When anomalous behavior is detected, the system alerts our SOC team and allows security policies to be applied before the traffic reaches our backend systems.."

Ronald Paz
Consulting Systems Engineer at Boomslang Tech

Read full review

"Akamai API Security is used for bot attacks, API attacks, and DOS attacks across multiple web layers, with a primary focus on DOS and bot attacks. Akamai API Security is a good solution for DOS and bot attacks because it provides exact details and helps prevent DOS attacks while protecting applications.

"The anomaly detection feature is valuable as it identifies unknown IPs and provides detailed insights. This is a good feature of Akamai API Security. The policy can be adjusted and provisioned, which is also a beneficial aspect of Akamai API Security.

"Regarding APIs, Akamai API Security is helpful for taking the API and preventing multiple web attacks. Recently, an attack was detected from an iPhone, and since iPhones are now very powerful, the attacker conducted a DOS attack. Upon reviewing the traffic and extracting the report in Akamai API Security, it was discovered that the attack was executed through API, with one certain IP hitting multiple times, reaching 30 to 40 times in a single second from a single IP. This frequency is impossible for legitimate connections, so the traffic flow was analyzed.."

Alark Singh
IT Specialist at Allianz

Read full review

“Akamai API Security's main use case in my environment is to protect critical APIs that are exposed to the internet, especially for banking and financial applications. I primarily use it to secure APIs handling sensitive operations such as user authentication, account access, payment processing, and data retrieval. These APIs are high risk because they directly interact with sensitive customer data. From a protection standpoint, I use Akamai API Security to detect and mitigate threats like bot abuse, credential stuffing, injection attacks, and unauthorized access attempts.

“I also enforce controls such as rate limiting and access validation to prevent misuse of the API.

“From a monitoring perspective, I continuously analyze API traffic patterns to identify anomalies such as unusual spikes in requests, abnormal behavior from specific IPs, or any deviations from the normal API usage. Additionally, I focus on identifying OWASP API security risks such as broken authentication or excessive data exposure and ensure the appropriate policies are in place to mitigate those risks. Overall, the goal is to ensure that all external-facing APIs are secure, resistant, and protected against both automated and targeted attacks.

“One recent example I worked on was securing a login and authentication API for a banking application. This API was being heavily targeted by automated bot traffic, mainly for credential stuffing attempts. I observed a high volume of login requests coming from a limited set of IP ranges with abnormal request patterns. Using Akamai API Security, I analyzed the traffic behavior and identified that these were non-human requests with repetitive patterns.

“Based on this, I implemented rate-limiting controls and stricter access policies to restrict excessive login attempts. Additionally, I tuned the security rules to detect anomalies such as unusual request frequency and abnormal headers. This helped me to effectively block malicious traffic while allowing legitimate users. After implementing these controls, I saw a significant reduction in unauthorized login attempts and improved overall stability of the API. This was a key use case where I used Akamai API Security for both detection and prevention of bot-driven attacks.

“Apart from the primary use case of protecting authentication APIs, I have also

seen significant value in using Akamai API Security for detecting and controlling abnormal API usage patterns. One key scenario was identifying excessive data access through a certain API where clients were making unusually high-frequency requests to retrieve the data. While this was not a direct attack, it had the potential to impact application performance and expose sensitive data patterns.

“Using Akamai API Security, I was able to baseline the normal API behavior and quickly identify these anomalies. Based on that, I implemented rate limiting and access restrictions to control such usage. Another area where it made a difference was in reducing the false positives. By analyzing the API traffic behavior more intelligently, I was able to fine-tune policies so that legitimate users were not impacted while still maintaining strong security controls. Overall, Akamai API Security helped me to move from reactive security to a more proactive and behavior-based approach, thus improving both security and user experience..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

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.

"Akamai API Security is very easy to install. It is agentless, and one of the best aspects is that no agent has to be deployed on the server, making it very easy to deploy any Akamai API Security solution.."

Alark Singh

IT Specialist at Allianz

Read full review

"My experience with the cost, initial setup, and licensing of Akamai API Security is that the price is aligned with any security tool at an enterprise level. It may seem high, but it justifies the investment because of all the mapping of the APIs, and I did not encounter any problems with the implementation.."

Ronald Paz

Consulting Systems Engineer at Boomslang Tech

Read full review

"This a SaaS platform and majority of our clients prefer integration with Noname on the cloud. It is pretty fast in terms of the implementation, coming from the POV and the actual production. It took us about 90 days. That included the project management, preparation and POV. ."

Patrick Geronimo

Technology Director at IPV Network

Read full review

"Because Akamai API Security was a new tool, we definitely needed support from the vendor directly. We were working only using Postman and Bruno. We had to directly move from installable tools to Akamai, which is a cloud platform. We definitely wanted some tool knowledge from the vendor, and once that was provided, things went very smooth. The tool started identifying the endpoints all by itself, and we ourselves do not have any visibility.

The main challenges we had with Akamai API Security were how to set it up on the AWS cloud environment and how to access this portal. We had to handle the major and basic configuration, and given that our organization had a lot of internal APIs which are not exposed to the outside environment, public APIs, and intermediary APIs, all these had to be interconnected. The vendor also had to understand our current environment and then recommend how to specifically access our internal APIs. All those network-related issues required us to bring in the NOC team and ask them to open certain ports specific to our APIs, and then everything went smoothly. The major heavy lift was done by the network team and the vendor side.."

RaghavendraRao PV

Incident Manager at a computer software company with 1,001-5,000 employees

Read full review

Customer Service and Support

The customer support has been responsive and knowledgeable. Whenever we had questions or needed help fine-tuning, their team was quick to assist. Overall, we felt well-supported throughout.

I would rate their customer support a solid 9. They have been proactive and effective. The only reason it is not a 10 is that on very complex issues, it sometimes took a bit longer, but overall, they have been excellent. .”

Ron Machan
Cloud Engineer at HCL Software

Read full review

“Regarding customer support, I have interacted with Akamai support a few times, mainly during the initial onboarding and for policy tuning. The support experience has been very positive. The team was responsive and technically knowledgeable. They helped me fine-tune the configuration and resolve issues effectively. Overall, both in terms of scalability and support, my experience with Akamai has been reliable and smooth..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"Akamai API Security technical support has been engaged, and they support technically well. However, there is one drawback regarding technical support. Akamai API Security makes back-end changes because a SaaS solution is being used. Sometimes they inform about changes, and sometimes they do not, which impacts clients as a P1 or P2 incident. This has happened multiple times, but when tickets are raised, they support instantly and resolve the issues. The experience with support would be rated as a nine.."

Alark Singh
IT Specialist at Allianz

Read full review

Other Advice

"My main recommendation for organizations considering implementing Akamai API Security would be to complete a checklist before implementing it by first performing a complete inventory of APIs to understand which shadow APIs will be found and to consider how to integrate with different monitoring systems.."

Ronald Paz
Consulting Systems Engineer at Boomslang Tech

Read full review

"I chose Akamai API Security because it's a strategy, and the product was better in line with existing operational capabilities. My general experience in security is around fifteen years, which is longer than the three years I have been working with Akamai API Security. I would give Akamai API Security a rating of nine because there will always be some scope for improvement here and there. My overall review rating for this product is eight.."

Verified user
System Engineer at a retailer with 10,001+ employees

Read full review

"Using Akamai API Security, we have set certain alerts and are continually doing multiple fine-tuning activities. We are doing fine-tuning and improvements from time to time. Because of this, our false positive alerts have reduced significantly because we have cleaned up our configurations and made many changes. For this reason, it has become much better.

Organizations can go ahead with using Akamai API Security in their infrastructure. However, this solution is quite costly as it comes with the content delivery network, providing both content delivery and security. Considering this solution, it is quite expensive.

Akamai API Security is a great technology and many innovations are coming through for this solution. It is getting better day by day with tuning. This is the most practical WAF solution that is in the market. Administrators who use this will get a great understanding about how live threats and attacks are happening. This gives total transparency to people about what kind of cyber threats are occurring. I rate this solution a seven out of ten.."

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

Read full review

Since implementation, we have seen approximately a 40 percent reduction in suspicious API traffic incidents. Additionally, response times for anomaly detection and mitigation improved by around 25 percent, thanks to Akamai API Security's real-time analysis and edge presence.

I would advise others to start with a clear map of their APIs, documented or not, because Akamai API Security will discover them. Be prepared to fine-tune policies early on to reduce false positives, and make sure to align the cost model with your traffic growth. Ultimately, the protection is worth the upfront planning.

“Akamai API Security's edge network gives it a performance advantage over some other solutions. We have used cloud WAF or API gateways that add latency, but Akamai API Security's distributed presence keeps protection fast. The global reach and low latency really stand out in comparison. I would rate this solution an 8 overall. .”

Ron Machan
Cloud Engineer at HCL Software

Read full review

"Akamai API Security is for web pages or online use, while Illumio is for cloud and on-premise use. Akamai API Security is agentless, while Illumio is agent-based. Both are working with different methods.

"Jira is used for tracking project deadlines and implementing projects, as well as for multiple POCs and project management. Confluence is also used for tracking troubleshooting, offerings, and details on the Confluence page.

"The overall experience and satisfaction with Akamai API Security would be rated as a nine out of ten.."

Alark Singh
IT Specialist at Allianz

Read full review

"My advice would be to first have a clear understanding of your API landscape, including all exposed endpoints and their criticality before implementing Akamai API Security. I would also recommend starting with proper API discovery and monitoring in learning mode, so you can baseline the normal traffic behavior before enforcing strict security policies. This helps reduce false positives. It is important to gradually implement controls such as rate limiting and access validation rather than applying aggressive policies from the beginning.

"Additionally, teams should invest time in understanding the behavioral insights provided by the platform, as that is where the real value lies in detecting advanced threats. I would suggest working closely with Akamai support during the initial setup and tuning phase to get better results. Overall, with the right approach and tuning, it can be a very powerful solution for securing APIs.

"Akamai API Security has been a strong and reliable solution for securing my APIs, especially in terms of visibility and behavioral-based threat detection. With proper tuning and understanding of API traffic, it provides more effective protection for enterprise environments. I believe it is a valuable solution for any organization looking to move from traditional security to more advanced API-focused protection. I would rate this solution an 8 out of 10.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

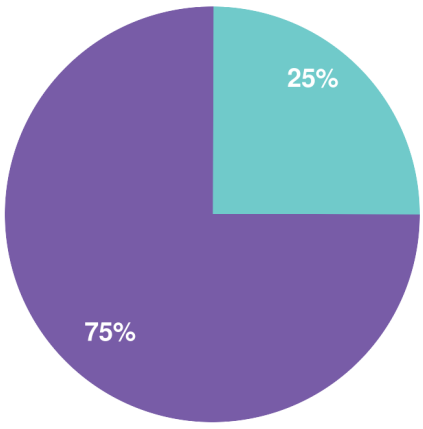
Top Industries

by visitors reading reviews

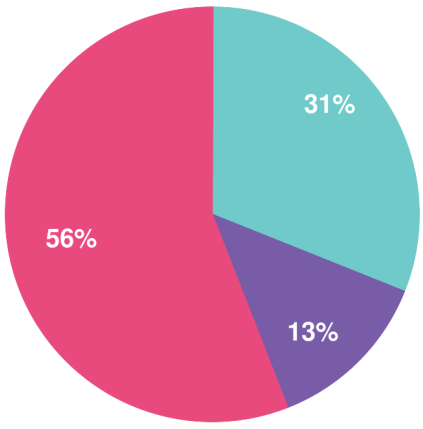
Financial Services Firm	21%
Computer Software Company	12%
Manufacturing Company	8%
Retailer	5%

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