aws marketplace

AttackIQ

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

AttackIQ

AttackIQ Recap

AttackIQ offers a cybersecurity platform focusing on security optimization through breach and attack simulation, enabling organizations to assess and improve their defense mechanisms effectively.

Using advanced technology, AttackIQ helps organizations evaluate security processes against real-world threat scenarios. Its platform provides continuous security assessments, which help in identifying vulnerabilities before exploitation by adversaries. It allows for the strategic allocation of resources towards enhancing security through actionable insights and reporting.

What key features make AttackIQ stand out?

- Breach and Attack Simulation: Conducts realistic attack scenarios to test defenses.
- Automated Testing: Regularly checks security protocols against evolving threats.
- Comprehensive Reporting: Offers detailed insights into security performance metrics.
- Threat Intelligence Integration: Incorporates global threat data for precise assessments.

What benefits and ROI should be evaluated?

- Improved Security Posture: Leads to a reduction in potential system breaches.
- Resource Optimization: Allows allocation of resources to high-risk areas.
- Enhanced Awareness: Increases understanding of threat landscapes within teams.
- Risk Mitigation: Identifies weaknesses before they result in data leaks.

Industries such as finance and healthcare, highly sensitive to data breaches, utilize AttackIQ for its rigorous testing capabilities. By simulating sophisticated cyber threats, organizations within these sectors can better protect critical data and maintain compliance with stringent regulatory standards.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "AttackIQ has had a positive impact on the organization, especially in the areas of continuous security validation, detection improvement, and overall defensive readiness, with highlights including improved visibility into detection gaps, stronger security controls validation, better SOC readiness, and faster detection engineering improvements, which are improvement areas we have implemented in our project using AttackIQ."

SangramGupta

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

- "AttackIQ is solving a lot of the problems that I had before or that we as an organization had before, even the security team, so it is solving all my issues."

Verified user

DevOps at a marketing services firm with 51-200 employees

- "After using AttackIQ, it has helped the team and the company improve on false positives and reduce risk, as most people are now capable of identifying how to work on detection, improving fine-tuning and all those things."

Verified user

Software Development Analyst at a tech vendor with 10,001+ employees

"Overall, I've had a good experience with the product. It's worked well for me."

NOUBOUM NOUBI BORIS HERMAN

Network Performance Management at Huawei Cameroun

What users had to say about valuable features:

"The continuous testing and continuous offensive testing are among the best features that AttackIQ offers, and being able to categorize it based on criticality such as very critical, emergency, high, medium, and low is valuable.

AttackIQ allows us to resolve issues much quicker because these issues come in categories, enabling us to prioritize them and fix the emergency issues first.

It has definitely reduced response time and improved our discoverability of these issues in the first place.."

Verified user

DevOps at a marketing services firm with 51-200 employees

Read full review

“The best features AttackIQ offers include being a cybersecurity platform specializing in breach attack simulation and AEF validation, as it tests the organization's defenses by simulating real-world attack behavior, which are aligned with the MITRE ATT&CK framework, providing a platform where I can run real-world attack scenarios and identify and mitigate them.

“AttackIQ is well-aligned with the MITRE ATT&CK framework and has strong continuous validation. The platform is built to run continuous and automation tests, which helps during point-in-time checks or reduces blind spots.

“AttackIQ positively impacts my organization as most of my colleagues and seniors have been using it to understand real-world attack scenarios and how to cope with those situations, benefiting the company, colleagues, and team.

“After using AttackIQ, it has helped the team and the company improve on false positives and reduce risk, as most people are now capable of identifying how to work on detection, improving fine-tuning and all those things. It has definitely benefited the organization in terms of faster risk identification and faster response times..”

Verified user

Software Development Analyst at a tech vendor with 10,001+ employees

Read full review

"Some of the best features I found in AttackIQ are its continuous security validation capabilities, MITRE ATT&CK alignment, and the ability to proactively test whether security controls are actually working as expected in real-world attack scenarios, representing real-world case studies and best features I have encountered in my project.

The continuous security validation capabilities of AttackIQ were one of the most valuable parts used by our team, especially since before using the platform, a lot of validation activities depended on periodic penetration testing, manual testing, or assumptions that security controls are functioning, which presented an actual challenge for the overall organization. AttackIQ helped change that, making validation more operational, repeatable, and proactive. From a usability perspective, once the initial setup and workflows are configured, the platform becomes fairly straightforward for day-to-day validation activities, with MITRE ATT&CK mapping and predefined attack scenarios making it easier for security teams to understand what was being tested and how the controls were responding.

AttackIQ has had a positive impact on the organization, especially in the areas of continuous security validation, detection improvement, and overall defensive readiness, with highlights including improved visibility into detection gaps, stronger security controls validation, better SOC readiness, and faster detection engineering improvements, which are improvement areas we have implemented in our project using AttackIQ.

The overall detection has actually improved with AttackIQ, as the SOC improved, which reduced a lot of false positives and increased the detection rate and accuracy. Previously, a lot of time was consumed to detect something or to conduct false positive investigations, but after implementing AttackIQ, there is now a reduction of almost 40 to 50% in the overall time and effort, making it an impactful area.."

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

Read full review

AttackIQ helped me significantly. From those tests, we found that some attack behaviors were detected correctly by the EDR, especially around suspicious authentication activity and remote execution attempts. However, we also identified a few gaps. Some events were logged but not properly correlated in the SIEM, so they do not generate high-priority alerts. In a few cases, alert severity tuning needed improvement because potential risky behavior was marked as low severity.

One thing I found particularly useful about AttackIQ is how it helps continuously validate defenses instead of relying only on periodic penetration tests. An interesting takeaway was that having security tools deployed does not always mean they are effectively detecting attack behavior. During simulations, we noticed that some controls were generating logs but were not properly configured for actionable alerting. I also appreciated how the platform maps results directly to the MITRE ATT&CK framework because it makes it easier to understand coverage gaps and prioritize improvements for the blue team and SOC.

“One of the best features of AttackIQ is its MITRE ATT&CK-based attack simulation capability. It makes security validation much more structured and measurable. Another valuable feature is continuous security validation because teams can regularly test whether EDR, SIEM, and other security controls are still detecting threats properly after configuration changes or updates. I also think the automated reporting and coverage mapping are very useful. They help identify detection gaps quickly and make it easier to communicate findings to SOC teams and management. What stands out most to me is that AttackIQ focuses not just on finding vulnerabilities but on validating real defensive effectiveness against realistic attack techniques.

“The automated reporting and coverage mapping features are very useful because they simplify how we analyze and communicate security validation results. After running simulations in AttackIQ, the platform automatically generates detailed reports showing which attack techniques were detected, blocked, or missed. This saves time compared to manually reviewing logs across multiple tools. The MITRE ATT&CK coverage mapping is especially valuable because it gives a clear visual understanding of which tactics and techniques are well covered and where detection gaps exist. In day-to-day operations, this helps the SOC and security

engineering teams prioritize rule tuning, improve SIEM correlation logic, and validate whether recent security changes have impacted detection capability. It also helps during audits and management reporting because the results are structured and easy to explain.

“An additional feature I appreciate in AttackIQ is the ability to safely emulate real-world adversary behavior in a controlled environment without causing operational disruption. I also appreciate the repeatability of the simulations. Teams can run the same scenarios again after making security changes to verify whether detections have improved. That makes it very useful for continuous improvement and purple team exercises. Another strong point is how it helps different teams—SOC analysts, blue teams, and security engineers—work together using the same validation data and attack-based reporting. .”

Akash Das Barman
Cyber Security Trainee at DataSpace Academy

Read full review

Other Solutions Considered

During the evaluation phase, platforms such as SafeBreach and Cymulate were considered because they operated in the breach and attack simulation space. The decision to move forward with AttackIQ was mainly influenced by its strong MITRE ATT&CK alignment, detailed security validation workflows, and the flexibility it provided for continuous testing and purple team activities.

Akash Das Barman
Cyber Security Trainee at DataSpace Academy

Read full review

ROI

Real user quotes about their ROI:

"It's hard to say about money saved because it has only been four and a half months with AttackIQ, but definitely a lot of time has been saved. I would say approximately 15% of our time.."

Verified user
DevOps at a marketing services firm with 51-200 employees

Read full review

We did see operational value and positive return from using AttackIQ, mainly through time saving and improved security validation efficiency. Before using BAS-driven validation, a lot of testing and verification work required more manual effort from security teams. One clear improvement was faster identification of detection gaps. Instead of discovering issues only during incidents or periodic assessments, we could proactively validate defenses on a regular basis. That helped reduce troubleshooting time for the SOC team and improved confidence in alert quality. We also saw efficiency gains during purple team exercises because the simulations and reporting were standardized, which reduced coordination overhead between red team and blue team activities. I do not have exact financial metrics, but operationally, the platform helped save analyst time, improve detection tuning cycles, and reduce the effort required for repeated manual validation testing.

We measured improvements mainly through repeated simulations and comparing detection results before and after tuning changes. For example, during the initial credential access simulations in AttackIQ, a few attack techniques were only generating low-confidence events and were not triggering SOC escalation. After updating SIEM correlation rules and refining EDR policies, we reran the same simulations and saw a noticeable improvement in alert quality and detection consistency. In one case, missed or poorly correlated detections for lateral movement scenarios were reduced significantly after tuning. We also observed that analysts could identify simulated attack chains faster because the alerts became more contextual and actionable. We mainly tracked the improvements using attack coverage reports, alert fidelity, and validation scores from repeated AttackIQ assessments. The key benefit was having measurable evidence that defensive visibility improved over time rather than relying only on assumptions.
."

Akash Das Barman
Cyber Security Trainee at DataSpace Academy

Read full review

Use Case

“My main use case for AttackIQ is conducting breach and attack simulation or any kind of new ransomware simulation, basically for executing particular real-world attack scenarios.

“Regarding my main use case, I have used AttackIQ Ready, Flex, and Enterprise, which are the main three product types I have utilized most..”

Verified user
Software Development Analyst at a tech vendor with 10,001+ employees

Read full review

“We use AttackIQ for automated, continuous testing and offensive testing. We use their scaled offensive testing module in AttackIQ, which continuously validates your environment and cloud environment, then identifies exposures that we take and try to fix them.

I'm the security person on the team, so AttackIQ has become really useful for us to automate this continuous testing because before we would only have point-in-time testing. We would only be able to get a scan at a single point in time, but now it's useful because it provides continuous monitoring.

We use public cloud for AttackIQ..”

Verified user
DevOps at a marketing services firm with 51-200 employees

Read full review

My main use case for AttackIQ has been validating security controls and testing detection coverage against MITRE ATT&CK techniques. Recently, I used it in a lab setup to simulate credential access and lateral movement techniques to verify whether our security controls were functioning as expected.

In my case, the primary cloud platform in our hybrid environment was Amazon Web Services with some integrations connected to on-premises infrastructure. We used that setup to validate security controls across both cloud workloads and internal systems, especially for monitoring logging and attack simulation visibility. I used the platform on Amazon Web Services. .”

Akash Das Barman
Cyber Security Trainee at DataSpace Academy

Read full review

"I use AttackIQ primarily as part of security validation and threat exposure assessment within our cybersecurity operation, where the platform is mainly used to simulate attack techniques and validate whether the existing security controls are effectively detecting and responding to the threats.

We conducted a purple team exercise where we used AttackIQ to simulate attack behaviors mapped to MITRE ATT&CK techniques with the control testing environment, with the main goal being to validate whether the SIEM detection was triggering correctly and to check if the endpoint security controls are responding as expected, and if the SOC monitoring workflows were functioning properly. That exercise helped identify a few detection gaps where certain behaviors were either not generating alerts consistently or lacked sufficient contextual visibility, and based on the findings, the security team refined the SIEM correlation rules, improved the alert prioritization, and enhanced monitoring coverage for specific attack techniques.."

SangramGupta
Security Consultant at a tech vendor 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.

"One area for improvement is the initial configuration complexity, which is very complex in the initial stage to configure the whole thing and integrate with the SOC, presenting a learning curve for organizations that are new to adversary emulation or continuous security validation.."

SangramGupta

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

Read full review

"The initial setup was difficult. It was not straightforward. I struggled at the outset to get everything up and running.

The deployment itself took a long time to execute on.

The product does require regular maintenance as well.."

NOUBOUM NOUBI BORIS HERMAN

Network Performance Management at Huawei Cameroun

Read full review

In our environment, AttackIQ was mainly used in a hybrid setup. Some security infrastructure and monitoring components were hosted in the cloud, while certain internal systems and validation targets remained on-premises. The setup allowed us to validate detections across both cloud-connected and internal enterprise environments, which was important for testing lateral movement visibility and overall security coverage across different segments of the infrastructure.

I was not directly involved in the procurement process, so I cannot confidently confirm whether AttackIQ was purchased through the AWS Marketplace or through a direct enterprise agreement. My involvement was mainly on the technical and operational side of using the platform for security validation and testing. ."

Akash Das Barman

Cyber Security Trainee at DataSpace Academy

Read full review

Customer Service and Support

“Overall, my experience with the customer support of AttackIQ has been positive, with the support team generally responsive, technically knowledgeable, and helpful during both onboarding and operational phases..”

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

Read full review

“I haven't had any issues with the product just yet. Therefore, I haven't reached out to technical support before. Having not spoken to them, it's hard for me to gauge their level of knowledge or responsiveness. I wouldn't be able to really comment..”

NOUBOUM NOUBI BORIS HERMAN
Network Performance Management at Huawei Cameroun

Read full review

From my experience, the customer support for AttackIQ was generally responsive and knowledgeable, especially on technical topics related to BAS workflows and MITRE ATT&CK–based validation. The support team seemed to understand enterprise security environments well, which was helpful during setup discussions and when clarifying simulations or integration-related questions. Documentation and training resources were also useful for understanding platform capabilities and best practices. Overall, the support experience was positive and aligned with what you would expect from an enterprise cybersecurity vendor.

Akash Das Barman
Cyber Security Trainee at DataSpace Academy

Read full review

Other Advice

AttackIQ is very strong in continuous security validation, MITRE ATT&CK alignment, and realistic attack simulation. The main reasons I would not give it a full perfect score are the learning curve for new users and some opportunities for improvement in reporting, customization, and remediation guidance. I would rate AttackIQ an eight out of ten overall.

Akash Das Barman
Cyber Security Trainee at DataSpace Academy

Read full review

"I would rate AttackIQ a 10 out of 10 because so far I have no issues with it. AttackIQ is solving a lot of the problems that I had before or that we as an organization had before, even the security team, so it's solving all my issues. I would say definitely make sure you know your use case before you purchase AttackIQ. I give this product a rating of 10 out of 10.."

Verified user
DevOps at a marketing services firm with 51-200 employees

Read full review

"One additional point I would like to add is that we will improve continuous security validation. Traditionally, many organizations rely heavily on periodic penetration tests or isolated assessments to evaluate security effectiveness, while AttackIQ helped us achieve a more continuous and operational approach to security controls, detections, and monitoring workflows, actually working as intended over time. We are the customer. I would rate this product a 7 out of 10.."

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

Read full review

"I'm just a customer and I personally use the product. I don't have a business relationship with the company.

I use both cloud and on-premises deployments.

Overall, I would rate the solution seven out of ten. I haven't worked with it that long, and I only really use it personally. I would need to take some time to really judge its effectiveness and to see if there is anything in terms of features that are lacking.."

NOUBOUM NOUBI BORIS HERMAN
Network Performance Management at Huawei Cameroun

Read full review

"In my current organization, we are not using AttackIQ; in my previous organization, I have used AttackIQ, and it was more of hands-on training rather than being deployed as a typical tool for improvement or knowledge enhancement.

"In my previous experience with AttackIQ, it was all on-premises and training; we

have not used any private cloud vendor.

“My advice for others considering using AttackIQ is that people can utilize it since it offers free training on purple teaming and pre-simulation, which are useful for professional growth and skills development, even for those with limited industry certifications. I would rate this review an eight out of ten..”

Verified user
Software Development Analyst at a tech vendor with 10,001+ employees

Read full review

Top Industries

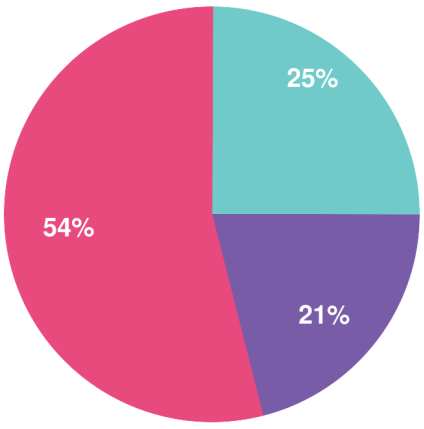
by visitors reading reviews

Financial Services Firm	16%
Manufacturing Company	12%
Construction Company	7%
Retailer	7%

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