Akamai

WHITE PAPER

13 Questions to Ask Your API Security Vendor

Introduction

The network of business-to-business APIs is growing exponentially. And an expanding universe of Internet of Things devices is providing new opportunities for developers to bring real-world data into applications through APIs.

But while APIs unlock many new opportunities for innovation and growth, they also introduce a new set of security challenges, including:

- Stolen API credentials
- Undetected API reconnaissance
- Misconfigured authentication and authorization
- Unprotected shadow and zombie APIs
- Remote code execution, injection, local file inclusion, and other attack techniques
- Data leakage or exfiltration
- API scraping
- Business logic abuse

Security vendors offer many options for detecting and mitigating these and other API threats, but those options are not all equally effective or easy to use.

The following 13 questions will help you frame your discussions with API security vendors and assess how effectively their products will address your organization's API security needs.

1 Is your API security product capable of performing enterprise-wide API discovery?

One of the biggest problems that security teams face is that they don't have a complete and accurate inventory of all the APIs that their organization exposes. Many of the undocumented shadow APIs that security teams miss are not part of the formal API management and security framework. It's also common that zombie APIs — those that the organization thought were retired — are still accessible. And even among sanctioned and documented APIs, there may be undocumented API parameters that can be exploited. Discovery of all north-south, east-west, and outbound APIs is imperative. The only way to ensure complete, enterprise-wide API visibility is by examining existing API activity data from a wide array of technologies and cloud platforms.

2 Does your product discover APIs continuously and, if so, how manual is this process?

APIs appear and disappear regularly because of fast-moving DevOps processes. Therefore, point-in-time inventories of APIs are insufficient. Your API security product must perform continuous discovery, which ensures that new documented APIs are inventoried, analyzed, and protected. It should also detect any future instances of shadow or zombie APIs. Additionally, products that place an ongoing burden on your team to interpret and act on findings will not be sustainable over the long term. In contrast, products that apply automation and machine learning to both discovery and assessment of APIs will keep your business running smoothly, instead of adding more manual tasks to your team's daily to-do list.

3 How does your product help my API documentation tools and processes?

Integrating your documentation approach with your API security platform has many benefits, so you should verify that your vendor has this capability. For example, automatically uploading existing Swagger documentation to your API security platform as part of your continuous integration/continuous delivery (CI/CD) process improves the accuracy of shadow API detection and shadow parameter identification (if the vendor has the ability to compare discovered API parameters with already documented parameters). Your security platform should also be able to create custom Swagger files at the click of a button for any APIs that are lacking documentation, which will help your developers begin and improve their documentation processes.

4 How much time and effort will it take to deploy your product in my environment?

The fastest and most effective way to get started is by using a security as a service (SaaS)–based API security product that can nonintrusively ingest and analyze API activity data from your existing systems. A well-designed SaaS architecture for API security can be integrated into your environment in minutes, which can accelerate your time to value by orders of magnitude and eliminate the ongoing costs and risks associated with system updates. To be even more agile, find a vendor that offers both web application and API protection (WAAP) and API detection and response so that API traffic data flows seamlessly between the solution that is protecting your incoming traffic and the solution that is protecting all API traffic within your organization.

5 How will your product help identify and prioritize the discovered APIs that are risky?

Seeing a comprehensive API inventory for the first time can be both empowering and overwhelming. Many security teams suffer from information overload and struggle to identify the areas on which to target API security efforts. The best way to avoid this is by selecting an API security product that does much of this work for you, including:

- Highlighting the presence of APIs that make sensitive data accessible
- Automatically labeling sensitive data by type (e.g., personally identifiable information, email addresses, credit card data, etc.)

Your API security platform should also allow you to create custom labeling categories so your API and security teams are speaking a common language that aligns with your business objectives and security concerns.

6 Does your product use behavioral analytics to determine a baseline of expected behavior and find anomalies?

Many types of attacks can be detected by using attack signatures to block at the WAAP level. However, many attack types found on the Open Web Application Security Project (OWASP) 2023 API Security Top 10 list, like broken object level authorization, cannot be discovered that way. These types of attacks are more passive and focused on business abuse, so they are more difficult to detect. The only way to effectively defend against all API threat vectors is by using behavioral analytics and machine learning. True behavioral analytics requires large datasets, machine learning algorithms that learn the specifics of your environment, and the flexibility and agility to automatically update and adapt on the basis of global information. A SaaS model is the only practical way to perform these activities at scale.

7 Can you capture and analyze datasets that are meaningful enough to effectively determine a baseline of normal behavior and detect anomalies?

Many API security products focus on monitoring individual API calls or, at best, short-term session activity. This is insufficient since many legitimate business processes — and many attacks — occur over a much longer period. API usage must be analyzed over a sliding time window (30 days at a minimum). This provides a more complete and accurate baseline of expected behavior, including any business processes that only occur once per month (e.g., invoicing). It also makes it possible to detect attacks that are executed slowly, across multiple days or weeks and numerous API sessions.

8 Can your product identify every entity, relationship, and activity within raw API data to provide business context?

The best way to make API activity data actionable is by enriching it with context about the business implications of API usage. The following identification and labeling capabilities are essential for your API security platform to assess and profile the relationships among the different entities:

- Representations of API users (user entities), such as IP addresses, API keys, access tokens, userID, partnerID, merchantID, supplierID, etc.
- Representations of business processes (business process entities), such as reservations, payments, invoicing, account balance, etc.

Granular analysis at this level is the only way to turn the vast amount of data generated by APIs into a meaningful and understandable baseline of expected behavior.

9 Can your product plot every activity by every entity in your APIs on a timeline to show behavior changes over time?

While understanding and monitoring API activity and threats at a macro level is critical, the ability to narrow the focus of your analysis to specific entities is equally important. For example, if anomalistic behavior is identified for a specific business partner, the ability to view all the activity for that entity on a timeline is invaluable. The same is true for business process entities. Seeing the full story of what happened, and when, on a timeline for every entity within your APIs is a powerful visualization that makes the story of normal use and business abuse obvious. The ability to rewind the activity to see what happened before and after an alert is a powerful tool to help you understand business logic abuse.

10 How can I integrate your product with existing tools, processes, and workflows?

Sending alerts to your security information and event management (SIEM) product is helpful, but it is just a starting point. Increasingly, security teams are using more sophisticated security orchestration, automation, and response (SOAR) tools to initiate predefined workflows when security threats and incidents are detected. And since many API security issues require action by developers outside of the security team, your API security platform also needs to integrate with the development team's issue tracking and workflow management tools. If your security tool is analyzing API traffic, it makes sense that it should also use APIs to help orchestrate responses in your CDN, web application firewall, or API gateway and allow you to create your own playbooks.

11 Can I query your product's API and activity data for proactive threat hunting and risk mitigation?

Security and development tool integrations can't just be black boxes that send one-way alerts to your tools. Your security and API teams need the ability to tap into the source data behind an alert or issue. Look for API security platforms that allow users to query API details directly through a built-in web interface or via APIs that enable integration of the API security platform with other preferred tools and interfaces. This will empower your security team to conduct proactive threat hunting efficiently and effectively. It will also help your developers and other nonsecurity stakeholders understand how APIs are targeted by attackers while being used legitimately.

12 What steps do you take to ensure that the sensitive data you collect about my business is protected?

The advanced behavioral analytics required to secure APIs against today's threat landscape are only possible with the scale of the cloud. Given the size and sensitivity of your API dataset, it's important to challenge your security vendor to ensure that your data will be protected. Verifying the practices that your vendor uses to secure its cloud infrastructure is important, but it's only the starting point. Require your API security vendor to use techniques such as tokenization; that is, replace sensitive data with anonymized tokens before it's transmitted to the cloud. This ensures data privacy even if the vendor — or their upstream cloud provider — experiences a security incident.

13 Does the solution provide granular access to API activity data?

Data is a crucial strategic element for everything from compliance to context for attack prevention. Many vendors offer their own version of storage for API data over time, but be sure to dig deeper to understand what is really being offered. Alerts-only solutions miss the full story, because compromised API activity can occur slowly over time, not just once an alert takes place. Alternatively, a comprehensive vendor will remove blind spots by recording all API activity and will provide the tooling to review that activity in detail instead of losing it in a vague machine learning model. It's important to have this granular access to your data because then you can proactively monitor for threats instead of retroactively reacting after there's been an attack alert.

13 questions to ask your API security vendor

1. Is your API security product capable of performing enterprise-wide API discovery?
2. Does your product discover APIs continuously and, if so, how manual is this process?
3. How does your product help my API documentation tools and processes?
4. How much time and effort will it take to deploy your product in my environment?
5. How will your product help identify and prioritize the discovered APIs that are risky?
6. Does your product use behavioral analytics to determine a baseline of expected behavior and find anomalies?
7. Can you capture and analyze datasets that are meaningful enough to effectively determine a baseline of normal behavior and detect anomalies?
8. Can your product identify every entity, relationship, and activity within raw API data to provide business context?
9. Can your product plot every activity by every entity in your APIs on a timeline to show behavior changes over time?
10. How can I integrate your product with existing tools, processes, and workflows?
11. Can I query your product's API and activity data for proactive threat hunting and risk mitigation?
12. What steps do you take to ensure that the sensitive data you collect about my business is protected?
13. Does the solution provide granular access to API activity data?

As you may have already guessed, Akamai API Security can effectively offer the protections recommended by this list. Explore our solution.