wallarm

# A Buyer's Guide to API Security

API SECURITY GUIDE

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107

# A Buyer’s Guide to API Security

API security protects your APIs against unauthorized access, malicious attacks, and data leaks. The more APIs you use and the more complex your API architecture, the harder you’ll need to work to ensure that security issues with APIs don’t undercut the value that APIs bring to your applications and infrastructure. Issues such as weak API authentication, injection attacks against API endpoints, and API sprawl are just some of the challenges that can turn APIs into the weakest link in your security strategy if you don’t address these risks effectively. Securing your APIs becomes even more critical in the modern development world, which follows the “API-first” model and approach.

In this guide, we will explore key elements of API security to help organizations understand the new types of security risks that arise from the use of APIs and how to respond effectively against those threats. Finally, we will share some best practices for security practitioners to address API security risks. But first, let's look at why security and product leaders should care about API security.

- Why should security and product leaders care about API security?
- What are the key considerations for API security?
- What are some of the key challenges facing security teams responsible for API security?
- What are the benefits of implementing effective API security?

## API Security Dominates Cybersecurity

2024 cemented APIs as the most critical attack surface in modern cybersecurity. Their ubiquity across industries and their essential role in enabling digital transformation made them a primary target for adversaries.

APIs were the dominant cybersecurity risk in 2024. Among the attacks, 33.5% targeted modern APIs like RESTful and GraphQL, while 18.9% involved legacy APIs including AJAX backends and URL parameter-based systems.

The impact of API exploits was felt across industries. As per the Wallarm 2025 ThreatStats$^{TM}$ Report, high-profile breaches like Dell's API abuse incident exposed 49M records, and Twilio Authy's breach compromised 33.4M linked phone numbers. These incidents demonstrated how attackers are exploiting insecure APIs.

# APIs are at the heart of modern applications

Modern applications fundamentally rely on APIs to connect data and infrastructure. APIs are critical gatekeepers, managing data flow between applications, databases, and infrastructure. This reliance is even more prominent when considering AI systems.As is revolutionizing enterprise operations, it has also introduced a new era of API security challenges. Securing AI-powered APIs must be at the forefront of every organization's security strategy. CISOs and CIOs who take immediate, proactive steps will mitigate risks, protect sensitive data, and ensure their AI initiatives drive innovation - without compromising security.

Without APIs, products would lack the connectivity and integration across different systems that drive their usability. APIs are also a favored attack vector for cybercriminals, common API threats - like unauthorized access, data breaches, and injection attacks - can have enormous consequences. For example, an attack on Deutsche Telekom, as detailed in Wallarm's Q3 2024 ThreatStatsTM Report, exposed the personal data of more than 250 million people in July 2024. As development teams are hard-pressed to move faster and innovate, this can amplify the risks associated with API security. Organizations face the challenge of securing an ever-expanding attack surface while maintaining application performance and user experience.

# Staying ahead of the security challenge

There are a few common challenges that you might come across when implementing an API security solution. Here's what they are and how to overcome them:

## API sprawl

Identifying all the APIs your team uses may be challenging, particularly if you're a large organization or have many simultaneous development projects. One of the most critical tasks for enterprise security teams is to get an accurate and complete inventory of all APIs, including internal and external ones.

## Protect your business logic

Organizations face a growing challenge in securing APIs, particularly sensitive endpoints critical to core business processes like authentication, payment, AI, and user management. Without a clear path to securing APIs, security teams struggle to address vulnerabilities before they are exploited.

### Prevention vs. detection

Performance degradation is the biggest risk when introducing new security capabilities within an organization. Security teams have to work closely with application owners to enable the right security policies without impacting application performance.

### Evolving threat landscape

APIs have become modern cybersecurity's most critical attack surface. Their ubiquity and essential role make them ideal targets for adversaries. Wallarm’s analysis of CISAs 2024, known as exploited vulnerabilities, revealed that over 50% of exploits were API-related, up from 20% in 2023.

### Adoption of Gen AI

AI is fundamentally reshaping how enterprises use technology. APIs are enabling this growth, acting as the critical interface between AI models and the applications they power. AI has amplified traditional risks and created new ones for security teams, like vulnerabilities in AI tools.

## You Cannot protect what you cannot see

One of the most fundamental challenges in securing APIs is the first step around visibility. Most organizations have a static view on the number of APIs in their environment and how they interact with other systems. Often these are owned and maintained by the development teams. Quite often, the security team is responsible for securing these APIs. These teams need visibility into all the APIs that are in use, whether they are exposing any sensitive business data/logic, and how they are protected against the latest cyberattacks. Security teams need to evaluate:

- Orphan APIs
- Rogue APIs
- Shadow APIs
- Zombie APIs

# Key Characteristics of an ideal API security solution

## API Discovery and Posture Management

APIs present a large attack surface as each action requires its endpoint. Ensuring all endpoints are identified and fully documented allows for potential attack vectors to be recognized, mitigated, or monitored.

## Real-time Blocking

Security teams are overwhelmed by alerts from tools that do little to stop attackers. The primary purpose of the API security solution should be to stop API attacks before they impact customers' APIs, AI applications, and businesses.

## Automated Remediation

API owners and security teams today spend a lot of time manually identifying APIs and then reacting to attacks. This is primarily due to lack of proactive detection and remediation capabilities within the current set of tools. Security teams need an automated platform that proactively blocks incoming attacks with minimal manual intervention.

## Scalability

With the explosive growth of AI to deliver business transformation. It has become essential for application owners and security teams to ensure that their API security infrastructure supports the new requirements.

# Key Characteristics of an ideal API security solution

## Integration

Application owners and security teams constantly battle with increased complexity in modern infrastructure,resulting in a siloed approach.The API security solution should easily integrate with existing development tools and augment existing security tools to enhance security effectiveness.

## Ease of Use

One of the most prevalent challenges in adoption of security products is their usability. Security teams, often tasked with maintaining security across the entire organization, have to rely on multiple disparate tools each with its own learning curve. This increases the complexity and impacts adoption. API security solutions should be easy to deploy, use, and manage for the security teams.

## AI and Machine Learning

The threat landscape keeps evolving at a rapid pace. So it's imperative that the tools also need to evolve to effectively detect and remediate the new threats. The same applies to API security as well, security teams need to consider solutions that incorporate these latest technologies to improve their effectiveness.

# Benefits of API security

There are four main reasons for implementing an API security tool:

### Protect sensitive data

APIs today have become the conduit to share all kinds of data internally and externally with different applications. As more and more APIs communicate with each other, organizations need to protect this sensitive data without impacting critical business applications.

### Ensure business continuity

Lots of business-critical applications require APIs to communicate with one another. With API security, you can minimize the impact on your applications, helping ensure business continuity for your customers if your API is targeted.

### Enhance security posture

Mature security teams prescribe defense-in-depth security strategies. These strategies ensure that they use all the tools in their arsenal, including API Gateways, WAFs, and API security, to minimize the risk of a potential breach.

### Regulatory Compliance

Numerous regulations globally require organizations to protect sensitive data, such as personally identifiable information and financial information. Implementing a robust API security solution can help you comply with these standards.

## Block API attacks, don’t just detect them

Security teams constantly struggle with the proactive prevention vs. detection paradigm shift in the ever-changing threat landscape. Many market solutions claim to have detection and protection capabilities when it comes to API Security. Security teams must understand each of these capabilities in detail relative to their organization's security posture. Some of the key questions they need to address during the evaluation phase include:

- How do I track and remediate risky API endpoints, especially those handling sensitive and PII data?
- How can I protect against OWASP Top-10 and 0-day exploits leveraging known and unknown vulnerabilities?
- How can I automatically apply real-time mitigations without relying on 3rd party tools or manual intervention?

In addressing these key challenges, security teams must consider the constraints:

- Will there be an adverse effect on the performance of my applications
- Only legitimate API traffic is allowed through the application

# Summary

APIs are what make digital transformation a reality, but they are not without security risks and vulnerabilities. With the increased reliance on APIs, it becomes more and more important to protect and secure your APIs. Understanding the risks associated with APIs is a business imperative. API attacks can be costly. Obvious financial impacts like legal fines, stolen finances, and incident response budgets can run into the hundreds of millions. However, other hidden costs often compound the issue, especially if you're not expecting them.

Many of the costs associated with an API breach come as a surprise to organizations and put a significant strain on finances, but they don't have to. At this point, API security is an absolute business necessity. It can be costly up front, but it's either pay a fixed cost now or watch financial losses spiral later.

# API Security Assessment

## 1. API Security Prioritization Assessment

The objective is to connect security risks to business outcomes, and understanding if API security a priority for both technical and executive stakeholders.

While API security is a critical component of cybersecurity, it isn't always a top priority for all organizations. Consider these questions to understand how important API security is for your company. The more items on the list below that are relevant to you, the more important API security will be for your organization.

- ✓ **APIs generate revenue at your organization**
- ✓ **APIs handle sensitive business data**
- ✓ **Building applications that leverage modern architectures like microservices and kubernetes**
- ✓ **Migrating legacy applications to modern cloud infrastructure**
- ✓ **Utilize a WAF or a WAAP or API Gateway for application security**
- ✓ **Cybersecurity a board-level discussion**
- ✓ **Build your own APIs and applications**
- ✓ **Development teams maintain a CI/CD pipeline**
- ✓ **Investing in new emerging technologies like agentic AI or building Gen AI applications**

## 2. Company Preparedness Assessment

The objective is to identify pain points related to API visibility, security gaps, compliance, and operational complexity.

As many organizations look to implement API security programs, often the biggest challenge is determining how organized and prepared the company is to create an effective API security initiative. Understanding your organization’s strengths and weaknesses helps you understand where to invest and focus your resources more efficiently.

The more items on the list below that are part of your organization's current security architecture, indicates a higher degree of maturity in API security.

- ✓ **Dedicated Application Security team**
- ✓ **Maintain an inventory of your entire API estate**
- ✓ **People and processes to address API security issues like API misconfigurations, API leaks and block API attacks**
- ✓ **OWASP Top 10 Coverage**
- ✓ **OWASP Top 10 API Coverage**
- ✓ **Compliance requirements like NIST- SP 800-53, PCI-DSS, GDPR, DORA**
- ✓ **Mitigate and respond to API abuse(bots, credential stuffing, Account takeover)**

## 3. Vendor Assessment Criteria

The objective is here to help recognize gaps in their current security model and understand the need for a modern API security approach and the requirements needed to support the ideal solution.

You're now ready to choose an API security vendor to help support your API security program. API security platforms have a broad range of features and capabilities. Ensure that the vendor you choose aligns closest to the needs of your organization.

- ✓ **Solution supports multi-cloud environment**
- ✓ **Solution supports on-premises and hybrid deployment**
- ✓ **Blocks active API threats in real-time**
- ✓ **Detect API responses that leak sensitive data like PII, PHI or PCI**
- ✓ **Prevents abuse from legitimate users who bypass static rate limits**
- ✓ **Easy to deploy and manage for the security team**
- ✓ **Scales across applications and users without impacting performance for security effectiveness**
- ✓ **Leverages a privacy-first architecture to protect customer data**

wallarm

BOOK A DEMO

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107