Why Should You Prioritize API Security?

by Janet Wagner on December 18, 2023 • 9 min read

Share this post

Companies often ask API teams to juggle various priorities from API design, coding, and deployment to maintenance, monetization, and security. The prioritization of all these actions is impossible, which is why it's important to address what's critical first. Security should remain at the forefront of all organizations, especially those building API products.

In this article, we'll walk you through API security management. After a brief overview, you'll discover why it is crucial for businesses and how to implement best practices.

What is API Security Management?

APIs are the glue holding applications and systems together, and they often handle sensitive information. With an effective API security management strategy in place, developers can better protect APIs from threats.

Components of API Security Management

Managing the security and integrity of your APIs requires multiple components, including:

- **Authentication and authorization —** Implement authentication and authorization protocols, such as OAuth 2.0, JSON Web Tokens (JWTs), and OpenID Connect. Utilize role-based access control (RBAC) to manage who can access your APIs.
- **WAFs and firewalls —** Use Web Application Firewalls (WAFs) to monitor and filter HTTP and HTTPS traffic for malicious traffic. Secure backend infrastructure with network firewalls.
- **Data encryption —** Use TLS/SSL to encrypt data in motion and at rest. Encryption ensures data transmitted to and from an API is protected from unauthorized access or attacks.
- **Input validation and sanitization —** Validate and sanitize user input so API requests contain only appropriate values and data types. Taking these steps helps protect APIs from attacks like SQL injection and cross-site scripting (XSS).
- **Rate limiting —** Control the number of requests users and clients can make to an API within a set timeframe. Rate limiting prevents users from making too many requests to abuse or attack your API.

Learn More

Related posts

SmartBear • November 30, 2023

APIs Aren't Just Code. They're Business Assets.

Janet Wagner • November 14, 2023

Build Better APIs with AI-Powered Testing Tools

SmartBear • October 31, 2023

Don't Be Afraid of the Docs!

Julia Seidman • September 25, 2023

API Passwords Stink! Freshen Up Your Security Practices

Jason Harmon CTO • September 21, 2023

Security September: Essential Pillars to Ensure API Security with Dan Barahona

Take a listen to
The API Intersection.

- **Monitoring and logging —** Implement tools to continuously monitor your APIs for unusual behavior, logging any activity and API requests for analysis in the event of an incident.

These components protect your APIs from cyberattacks and safeguard sensitive data, helping you better manage their security. Here, an API gateway can come in handy as a mediator between your API and clients, allowing you to implement certain security measures. Specifically, a good API gateway will include multiple capabilities like the above-mentioned authentication and authorization, rate limiting, API monitoring, and access control.

Why is API Security Management Important?

API security management is critical to building successful API products. Consumers demand reliability and reward quality when it comes to mobile and web applications—and an effective API management strategy can ensure both. API security is especially important if you have clients in highly regulated industries like insurance, finance, and healthcare. Companies in these sectors can't afford to use dependencies that expose them to risk.

Consistency and efficiency are key business success factors bolstered by good API security. Stoplight encourages API product providers to design and build consistent APIs. This means prioritizing security before designing each API, and long before writing any code. By addressing security early on, you can avoid having to go back and fix vulnerabilities once you've already deployed your API.

Additionally, API security allows you to better protect your most important assets—people and data. APIs transmit data to and from a wide range of devices and applications. They also provide access to data stored in many places like databases, the cloud, data warehouses, and file systems. Your API program likely connects your APIs to sensitive data stored somewhere. Being on top of these considerations will boost the trustworthiness of your brand.

Finally, consider how information is increasingly exposed through microservices as companies build new data-driven applications. These innovative applications help companies compete in a modern marketplace, but only if you deploy them in a secure manner.

API Security Management Best Practices

Given the important considerations above, it’s clear that API security needs to be front and center in your API development strategy. Below, we summarize some best practices to keep your APIs safe and secure.

Build More Compelling API Products

An effective API security management strategy will include these best practices to help you build more compelling API products:

- **Embrace “API as a Product” —** API as a Product means treating every API as a valuable, standalone product throughout its lifecycle. When you think of your APIs as products, you can better understand how to secure them.
- **Practice “product thinking” —** If you want to treat your APIs as products, you’ll need a team who will practice product thinking. That team must have a product mindset when considering the bigger picture. The product team will view the API from every

angle to create an effective security management strategy.

- **Take an API design-first approach —** An API design-first approach involves describing every API design in an iterative way both humans and computers can understand—before you write any code. This approach enables you to create highly secure APIs by involving cybersecurity experts early in the design process. They can help you ensure your APIs have no vulnerabilities hackers could exploit, or that any design changes won't create security issues.
- **Shift security left! —** In terms of API security, shift left means you integrate security practices as early as possible, preferably early in the API design phases. Don't treat security as an afterthought—involve security teams from the beginning.
- **Cultivate teamwork —** Building highly secure APIs requires teamwork. This usually requires coordination between the API development and security teams. Each team will likely have its own goals and deadlines. Implementing an API design and management platform like Stoplight can enhance collaboration between these teams.

When consumers can trust the API products you provide, you boost customer loyalty which means more revenue for your business.

Drive Efficiency and Consistency within Your API Program

Consider following these best practices to ensure consistent security practices across all your APIs:

- **Leverage OpenAPI —** OpenAPI is a specification language for HTTP APIs offering features to help you strengthen security across your APIs. For example, OpenAPI version 3.1 supports security schemes, such as OAuth2, Mutual TLS, and OpenID Connect Discovery. With its built-in, well-tested security patterns, you can control how and when you address API security.

- **Design security with style (guides!) —** Many teams already use an API style guide to ensure the consistency of APIs across the organization. Adding enforceable security rules to your style guide will help prevent vulnerabilities and potential exploits in your designs. The OWASP Top 10 API Security Risks can be a handy reference for your API style guide.
- **Craft a strong governance program —** When it comes to securing your APIs, good governance is a must! Establish a robust governance program where you define standards and best practices for designing, coding, deploying, securing, and managing APIs. Your governance program should enable you to enforce security practices consistently throughout the entire API lifecycle.
- **Create solid API documentation —** Comprehensive documentation that includes well-tested security protocols and best practices will help developers using your APIs build secure applications. Your API documentation can steer your developers away from creating vulnerabilities and exploits in their applications because they'll have security guidelines to follow.
- **Utilize component libraries —** Component libraries allow API teams to reuse components across projects. Most APIs require authentication and authorization models, which can be great additions to your component library. Consider including common methods like API keys, OAuth tokens, or JSON Web Tokens (JWTs) to

ensure developers implement security measures consistently for each API.

- **Automate security features —** One of the best ways to build highly secure APIs is to automate security processes where appropriate. For example, you could use an automated linting tool like Spectral to ensure your API definitions conform to security standards set by your organization and enforced via OpenAPI. Automation can also boost the speed and accuracy of security processes.

All these tools increase consistency and efficiency within your API program, which can help you better secure all your APIs.

Ensure the Protection of Your Core Information Assets

These best practices can help you build great API products while protecting core information assets:

- **Adopt safer password management practices —** Passwords have been around for years, and today, we have many methods to make them more secure, like password managers and two-factor authentication. However, hackers constantly find ways to breach password security measures and access users' sensitive data. Consider updating your password management practices *by not using password*s. Try using browser-based passwordless authentication or an authenticator app like Microsoft Authenticator instead.
- **Plan an effective authentication strategy —** The best authentication strategy will look different for every company. Work collaboratively in your organization to decide which authentication approach works best for your use case. For example, some companies may need to use OAuth2 for

consumer-facing APIs while others might require SAML-based SSO for high-trust, large-scale environments. Consider all the pros and cons before implementing authentication.

- **Implement SecOps —** Security Operations (SecOps) is a methodology that combines security and operations, creating a centralized team that uses various tools and techniques to minimize security risks across the business. It's a proactive approach to security that can help you build highly secure APIs, applications, and systems. It also helps prevent vulnerabilities that could lead to data breaches.
- **Strengthen testing with AI —** You can strengthen API testing with AI in various ways. For example, AI systems can detect SQL injection or XSS attacks by analyzing API requests and response data for suspicious patterns or behaviors. You could use a large language model (LLM) to provide examples of real-world scenarios that serve as the basis for API penetration tests and then use AI to create the tests automatically.
- **Encourage a security-first culture —** Fast-moving business environments can make it hard to stay on top of every new source of risk. By implementing sound security practices and a culture of security, you don't have to anticipate every risk ahead of time. Create a security-first culture where teams have candid conversations about risks and create pathways for surfacing and tracking vulnerabilities in your APIs.

Protecting the data your APIs connect to and transmit is paramount, as a data breach can adversely impact your customers and your business in terms of money and reputation.

Prioritizing Security = Better API Products

Prioritizing security to build more compelling API products is essential to drive consistency and efficiency within your API program and to protect your core information assets. Focus on security from the beginning and your API products will benefit greatly. Choose tools to help you implement security management strategies throughout the API lifecycle.

Stoplight's collaborative cloud tools help developers design quality APIs quickly and efficiently, enabling companies to build scalable API programs. With our tools, your teams can apply effective security management strategies and best practices across your entire API program. Contact Stoplight's sales team to learn more.