

Code to Runtime Security with Akamai and Apiiro




APIs power modern applications, driving innovation and enabling seamless digital experiences. However, they also present a growing attack vector, exposing organizations to significant risks if not properly secured. Akamai and Apiiro have joined forces to address this challenge by integrating Akamai API Security with Apiiro's application security posture management (ASPM) platform. This joint solution empowers organizations to protect APIs from code to runtime, reducing risk, simplifying remediation, and accelerating the pace of innovation without compromising security.

Visibility is essential to managing API-based risks effectively. Identifying and responding to vulnerabilities quickly is critical — once an issue is detected, security teams must work with developers to remediate high-risk vulnerabilities as soon as possible. Yet most solutions fail to connect identified risks with their source in code, forcing security and developer teams to scramble. The Akamai–Apiiro integration solves this disconnection by providing end-to-end visibility and context.

Akamai API Security discovers APIs in traffic, and analyzes APIs for misconfigurations and vulnerabilities that can lead to an attack. For each vulnerability, it provides developers with detailed insights, including a description of what happened, why it poses a risk, and how to replicate the issue. This actionable information is passed to the Apiiro platform, which maintains a comprehensive inventory of APIs discovered using deep analysis of the code. Apiiro's platform automatically matches the APIs and vulnerabilities identified by Akamai with its existing API library, mapping each vulnerability to the relevant repository, specific line of code, and the responsible code owner.

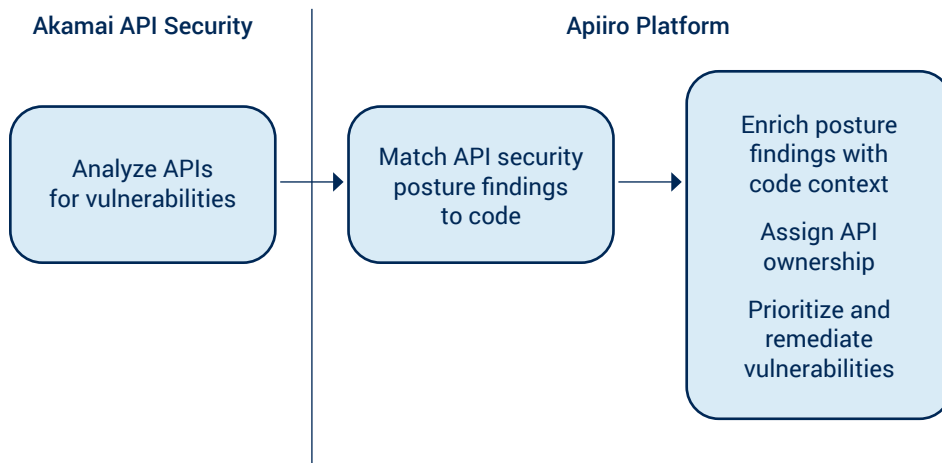
This seamless integration ensures that API risks detected by Akamai API Security are dynamically traced back to their root causes. Developers are equipped with all the necessary information to remediate vulnerabilities quickly, enhancing both the speed and effectiveness of the resolution process. Furthermore, this approach fosters better communication and collaboration between security and development teams, bridging a critical gap in API security workflows.

Benefits for your business

-  **Increased visibility**
Enhance code analysis with API vulnerability context.
-  **Accelerated time to remediation**
Automatically map API vulnerabilities to source code and assign development team owners.
-  **Reduced risk profile**
Streamline vulnerability investigation by correlating API traffic to code and prioritize vulnerabilities based on potential impact.



How it works



Key use cases

- Automated risk assessment: Continuously and comprehensively analyze APIs and related code to identify risk.
- Accelerated risk mitigation: Prioritize API vulnerabilities, map them to source code, and assign owners to reduce mean time to resolution (MTTR).
- Preproduction guardrails: Integrate security measures into development workflows to monitor and manage API changes proactively.

Conclusion

The Akamai–Apiiro offering provides a unique approach to API security by delivering end-to-end visibility and actionable insights. With this integration, Apiiro customers can extend protection beyond code to runtime, ensuring comprehensive API security. At the same time, Akamai customers can enhance remediation efficiency by tracing API risks to their origin in code and assigning them to the appropriate teams. Together, Akamai and Apiiro empower businesses to innovate securely and confidently in an increasingly complex API landscape.

