APImetrics
API INTELLIGENCE

API Security Tips To Implement

APIs allow enterprises to connect applications and platforms with databases that store sensitive user information. A compromised API can quickly lead to attacks on connected applications and, more importantly, the loss or theft of user data.

LIMIT DATA SHARING

The risk exposure increases as the amount of data shared between nodes increases. By reducing the data being shared between platforms to an authorization key rather than a user's credentials, OAuth works well against security threats.

Identify points of vulnerability in the data shared between apps, APIs, and users and secure them by limiting the data shared.

CONSISTENTLY AUDIT THE API BUILD

In the world of technology, there is always room for improvement. The API build should be audited regularly as part of an audit cycle. Ensure that there are no vulnerabilities, errors, or other build issues that attackers can exploit. Keep track of version updates and bug fixes by maintaining audit logs.

SCAN EVERY API REQUEST

Requests for APIs are vulnerable to phishing attacks and tampering. Parameters within the request URL, for example, can be manipulated to trick the API into providing sensitive information.

By scanning every API request for anomalies, we can mitigate this threat. There are solutions available that monitor API requests and provide actionable information.

SANITIZE INPUT

By sanitizing input data, you are checking, cleaning, and filtering unwanted characters and strings from the API data. The API server is thus protected from malicious code injection by bad actors.

ENFORCE A ZERO-TRUST POLICY

Conventional verification models trust some connections based on predefined protocols, for example, connections made from within the company network or by users who have accessed the API previously. In order to access data, connections from outside this predefined perimeter must authenticate and verify themselves.

Zero-trust models require all connections (with no exceptions) to authenticate before accessing resources. As a result, security risks are greatly reduced.

Source: IndusFace