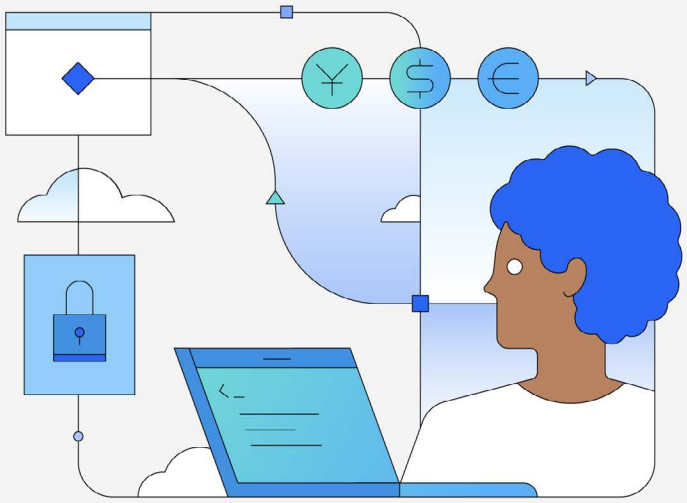
API security with IBM API Connect

Protect APIs and sensitive data from intensifying threats



APIs play a critical role in today's digital landscape because they are vital to improving business agility. But as they proliferate, unsecured APIs pose significant data security threats and simplistic security measures are no longer sufficient to protect them.

Incidents of API security breaches are on the rise. Many have resulted in substantial data loss, impacting even reputable organizations. Such vulnerabilities transcend industry and location, emphasizing the critical need for robust security strategies and tools tailored to APIs. Implementing stringent API security protocols protects the data, apps and services that API endpoints show and helps ensure their availability for legitimate users. But API security is not only about protecting the endpoints. It should also prioritize the security of network interactions like data transmission, user requests and inter-app communications across the API lifecycle.

IBM API Connect® is a market-leading full lifecycle API management solution that boasts a comprehensive set of API security capabilities. IBM API Connect brings together two complementary approaches to secure your APIs and provide a well-rounded API security strategy.

The essential API security features in IBM API Connect enable users to:

- Control access to APIs through industry standards, such as OAuth, OIDC and third-party services.
- Build and enforce policies to support API protection, mediation, transformation and more. IBM API Connect also comes with a Policy Editor, a graphical UI with a simple click and add experience and an extensive set of built-in policies.

The advanced API security capabilities available through our partnership with Noname Security use AI and machine learning to help users:

- Discover APIs across their estate to create a complete inventory of managed and unmanaged APIs.
- Improve their security posture by identifying misconfigurations and vulnerabilities in APIs.
- Detect and block API attacks in near real-time using machine learning.
- Find and fix vulnerabilities before APIs go into production by actively testing every API.

To achieve a 360-degree approach to API security, it's critical to start considering security from the design stage, while also enforcing security measures at runtime with real time detection and prevention of security threats and attacks.

Learn more →

Request a live demo →