NGINX
Part of F5

PRODUCT DATASHEET

F5 NGINX MANAGEMENT SUITE
API CONNECTIVITY MANAGER

Manage and Govern APIs Across Any Environment

WHY USE API CONNECTIVITY MANAGER?

Empower Developers
Enable developers to seamlessly deploy, manage, and secure APIs for their applications

Simplify Governance
Operate, monitor, and govern API gateways and developer portals from a single pane of glass

Improve Security
Easily apply global security policies and enforce consistent API security without sacrificing performance

Empower Developers, Simplify Governance, and Improve Security with NGINX

APIs are the connective tissue of modern applications, linking together data and services to deliver customer experiences. Today API calls make up over 80% of global Internet traffic, and the number of APIs is increasing exponentially.

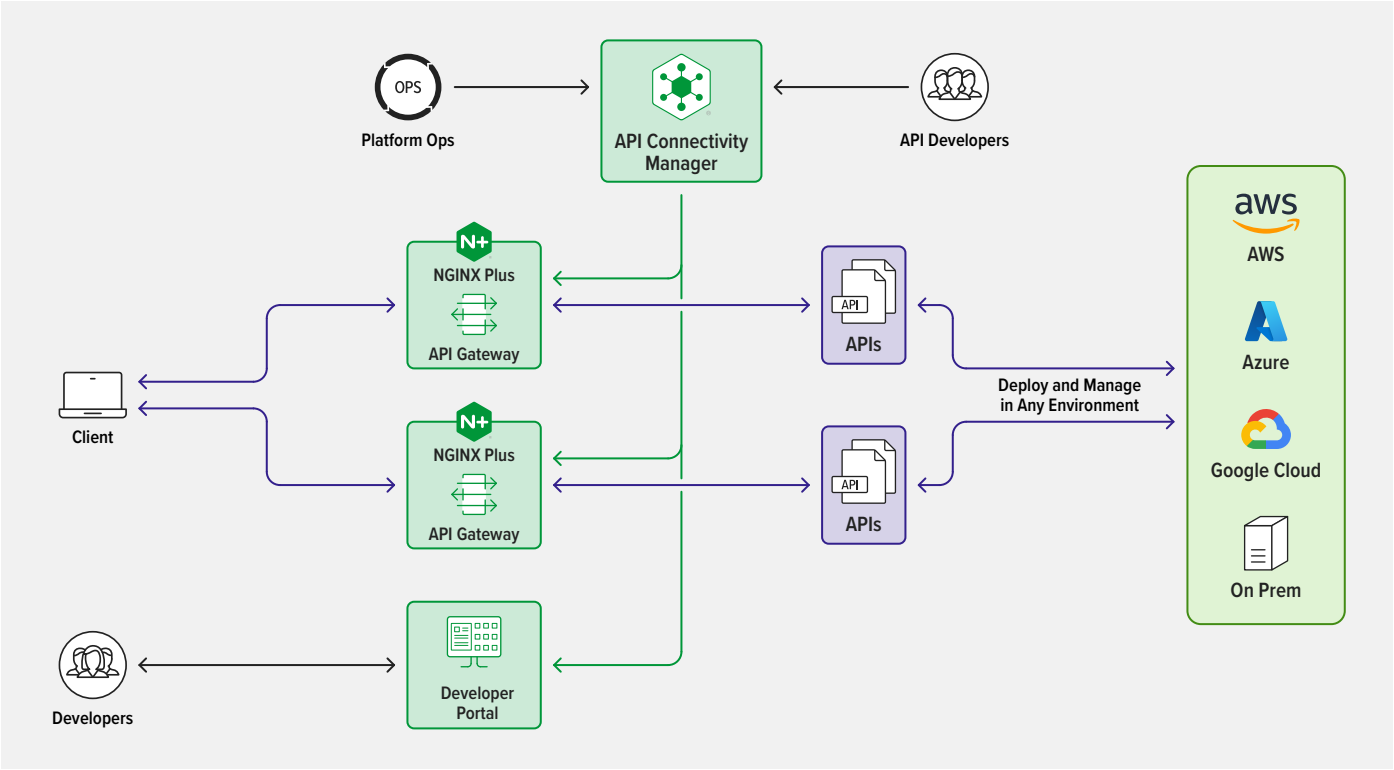
But the proliferation of APIs has created new risks.

As the number of APIs and complexity of cloud-native apps increase, it becomes very hard to discover and monitor where APIs are deployed. Unsecured APIs are easy targets for attack, and even minor misconfigurations can lead to severe outages.

NGINX helps ensure the connectivity, reliability, and security of your APIs, wherever they are deployed.

With API Connectivity Manager you can:

- Provide a frictionless experience for developers to deploy and operate APIs with optimal security and performance
- Create a single source of truth so developers can rapidly discover, onboard, and use your APIs in their applications
- Govern and secure APIs with visibility and control across any environment



Benefits of API Connectivity Manager

Accelerate Time to Market

Automate the configuration and deployment of API gateways so developers can bring new capabilities to market faster:

- Deliver your APIs with near-zero latency using lightweight, industry-leading NGINX Plus API gateways
- Deploy as many API gateways as you need, wherever you need them – in the cloud, on-premises, or at the edge
- Integrate into CI/CD pipelines and DevOps workflows to automate API operations with a fully declarative REST API

Create a Developer Platform

Create a single source of truth for your APIs so developers can rapidly discover, onboard, and use APIs in their projects:

- Publish and onboard new APIs with proper documentation using the OpenAPI Specification
- Enable self-service workflows so developers can register, generate API credentials, and immediately begin using APIs
- Help developers move from onboarding to “hello world” in minutes by testing API calls on the developer portal

Simplify API Governance

Provide uniform oversight for platforms, environments, certificates, and configurations from a single pane of glass:

- Create and scale policies across the enterprise to simplify administration and reduce risks from configuration errors
- Apply workspace isolation for service and infrastructure teams by giving developers dedicated spaces to deploy API proxies
- Empower developers to manage API-level policies with fine-grained controls for rate limiting, authentication, and more

Enforce Consistent Security

Protect your APIs with a suite of tools to manage authentication, authorization, and access to your APIs and microservices:

- Secure access to APIs by authenticating API requests with JSON Web Tokens (JWTs), API Keys, or OAuth/OIDC
- Protect backend services from attacks that can overwhelm API endpoints by applying rate limits at the API gateway
- Identify security threats with a unified view of API traffic – or integrate with your existing monitoring solution

To learn more, visit nginx.com/API

NGINX
Part of F5