PING + NGINX
Protect Your APIs Against Sophisticated Cyber Threats
ENHANCE YOUR API SECURITY

Organizations are adopting API strategies to more efficiently provide access to data, applications and services. While APIs are creating powerful ways for businesses to streamline partnerships and stimulate growth, they are also introducing a growing number of vulnerabilities that are being abused by bad actors. These security gaps are leading to costly breaches and disruptions, negatively affecting the bottom line and reputations of impacted organizations all over the globe.

To protect themselves, businesses need to extend their security practices to focus on attacks specific to APIs, including:

• Attacks that attempt to defeat login systems
• API DoS and DDoS attacks that disrupt API services and flow below rate limits
• Attacks that target data and systems

Defending against these threats requires an API security strategy that leverages standards-based access control to provide secure connections to APIs, deep visibility into API traffic to better understand API behavior, and threat detection to automatically block attacks.

To protect organizations from the latest wave of cyberattacks aimed at the unique vulnerabilities of individual APIs, Ping Identity and NGINX have partnered to provide an integrated API security solution.

HOW PING AND NGINX WORK TOGETHER

The combination of the Ping Intelligent Identity™ platform and NGINX Plus provides a complete solution to secure an organization’s APIs across on-premises, private or public clouds, and hybrid IT environments.

• NGINX Plus is an all-in-one software-based load balancer, content cache, API gateway, web server and reverse proxy. Lightweight, flexible and portable, NGINX Plus can be deployed across a multi-cloud or hybrid cloud platform. When deployed as an API gateway, NGINX Plus efficiently and securely routes API calls without sacrificing performance. NGINX Controller provides full API lifecycle management, enabling Infrastructure & Operations as well as DevOps teams to define, publish, secure and monitor APIs.

• The Ping Intelligent Identity platform provides an additional layer of API security that uses artificial intelligence (AI) to automatically detect and block threats to APIs, discover newly added APIs, provide deep API traffic visibility and reporting, and leverage deception (honeypot) capabilities to immediately block known threats to APIs.

Essentially, NGINX Plus can be deployed as an API gateway—a critical component of API infrastructure—while the Ping Intelligent Identity platform extends NGINX Plus with an additional layer of AI-powered security to protect APIs from advanced attacks and under-the-radar misuse and abuse.
WHAT ARE THE BENEFITS?

Ping Identity integrates with NGINX Plus to protect against unique API vulnerabilities by giving organizations:

- **Complete visibility into API traffic.** Complement business analytics with insight into API traffic to generate reports for compliance or forensic purposes.

- **API discovery.** Ensure awareness of APIs that may be inadvertently exposed, unknown or forgotten.

- **AI-powered protection from API attacks.** Detect anomalous behavior and automatically block threats from bad actors.

- **API deception for attack detection and blocking.** Use deception to identify and quarantine potential hackers before they access production APIs.

- **Seamless integration without API infrastructure changes.** Add a policy to NGINX Plus for integration with PingIntelligence for AI-powered cybersecurity.

Together, Ping and NGINX enable organizations to be confident in their digital transformation initiatives with a solution that provides robust API attack protection.
PING IDENTITY

Ping Identity envisions a digital world powered by intelligent identity. We help enterprises achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The Ping Intelligent Identity Platform provides customers, employees and partners with access to cloud, mobile, SaaS and on-premises applications and APIs, while also managing identity and profile data at scale. Over half of the Fortune 100 choose us for our identity expertise, open standards leadership, and partnership with companies including Microsoft, Amazon and Google. We provide flexible options to extend hybrid IT environments and accelerate digital business initiatives with multi-factor authentication, single sign-on, access management, intelligent API security, directory and data governance capabilities.


NGINX

NGINX, now part of F5 Networks, is the company behind the popular opensource project. We offer a suite of technologies for developing and delivering modern applications. Together with F5, our combined solution bridges the gap between NetOps and DevOps, with multi-cloud application services that span from code to customer.