



F5 NGINX APP PROTECT WAF

# Secure, Automate, and Scale Modern Apps and APIs

## WHY USE NGINX APP PROTECT WAF?



### Improve Security

Surpass basic OWASP Top 10 protection with over 7,500 advanced signatures, bot signatures, and threat campaign protection



### Accelerate DevOps

Release apps faster with security automation that integrates seamlessly into CI/CD pipelines



### Simplify Management

Gain centralized visibility with easy security policy management for total control of your WAF fleet

## Improve Security, Accelerate DevOps, and Simplify Management with NGINX

Most organizations today manage between 200 and 1,000 applications in hybrid and multi-cloud environments, with over 75% exposing their apps to the Internet via APIs. Transitioning to microservices, containers, and clouds is critical to achieve better efficiency but adds complexity and makes consistent application security particularly challenging.

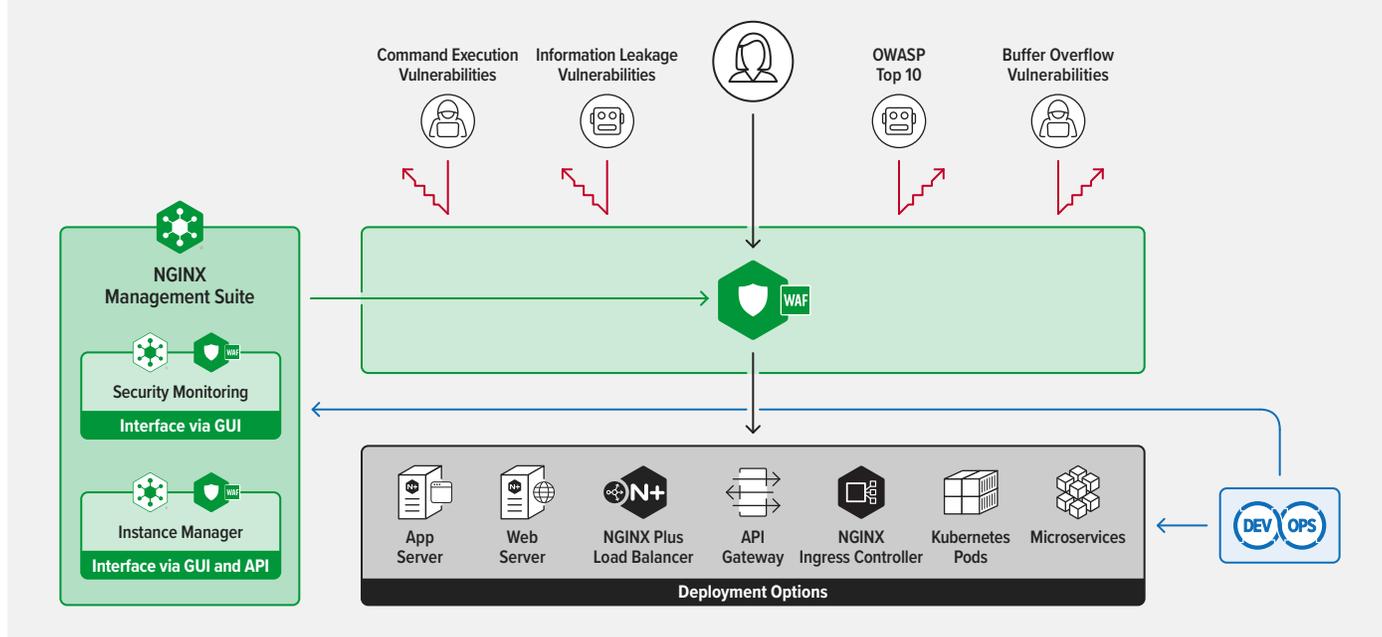
How can you secure your applications and APIs at scale with consistent security policies across distributed architectures and environments?

NGINX makes it easy to protect your apps and APIs with NGINX App Protect WAF, a platform-agnostic security solution based on F5's trusted and field-proven advanced WAF technology. It delivers consistent performance and protection against even the most sophisticated Layer 7 attacks.

With NGINX App Protect WAF you can:

- Reduce the cost of breaches by up to 80% with declarative policies integrated as security-as-code into CI/CD pipelines for easy security automation supporting DevSecOps
- Build more reliable and secure applications with robust protection that yields fewer false positives and provides your customers with better user experiences
- Easily scale your app security in Kubernetes clusters and the cloud while significantly reducing compute costs with a lightweight, high-performance, low-latency WAF
- Give security and DevOps teams flexible control over app security workflows and policies with multiple deployment options, ranging from edge load balancers to API gateways and Ingress controllers to per-service or per-pod proxies in a Kubernetes cluster
- Achieve centralized visibility and total security policy control over your entire WAF fleet

## NGINX App Protect WAF Blocks Layer 7 App and API Attacks at Scale



### Enforce Robust Security

Mitigate sophisticated Layer 7 threats and attacks:

- Enhance app security beyond the OWASP Top 10 with over 7,500 advanced signatures, bot signatures, and threat campaign protection
- Protect traditional HTTP/S and HTTP/2 applications as well as gRPC bi-directional streaming
- Mask personal identifiable information (PII) with the built-in Data Guard feature
- Surpass PCI DSS requirements and avoid regulatory non-compliance

### Integrate Security at Scale

Integrate WAF security with NGINX data and management planes and across public cloud:

- Centralize WAF visibility and configuration management at scale using NGINX Management Suite
- Embed WAF on NGINX Plus API gateways for API security
- Integrate at the edge or within the cluster using NGINX Ingress Controller for Kubernetes app security
- Deploy in hybrid and multi-cloud environments including AWS, Azure, and Google Cloud

To learn more, visit [nginx.com/waf](https://nginx.com/waf)

### Deploy Platform-Agnostic Security

Leverage a single WAF security solution across distributed architectures and environments:

- Deploy NGINX App Protect WAF as an embedded solution across all topologies from load balancer to per-pod proxy
- Achieve high performance and throughput with 10x lower latency than AWS WAF for lower compute costs
- Enable security teams to easily build one config file and push to multiple clouds
- Streamline technology integration using the NGINX portfolio for vendor consolidation and reduced tool sprawl

### Automate Security for DevSecOps

Incorporate WAF security into every stage of the software development lifecycle (SDLC):

- Apply consistent app security with declarative policies created by SecOps and deployed by DevOps
- Automate security-as-code seamlessly into CI/CD pipelines, reducing the cost of breaches by up to 80%
- Save time and money by resolving vulnerabilities before apps are released into production
- Leverage easy security policy integration via the Kubernetes API to keep developers agile

