NGINX App Protect®
Denial of Service

Modern Defense Against Application Attacks

Prevent Layer 7 Attacks with Adaptive Learning and Automated Protection

With an ever-increasing proportion of consumer and business activity moving online, malicious attacks on digital infrastructures have grown exceedingly common – and the complex nature of modern applications makes security complex. Layer 7 attacks on applications and APIs have spiked by 20% in recent years while the scale and severity of impact has risen by nearly 200%. These attacks abuse applications in a variety of ways and can result in performance degradation, outages, abandoned revenue, and damage to customer loyalty and brand. To protect complex and adaptive applications, you need a dynamic solution that removes the burden from security teams while supporting rapid application development and competitive advantage.

To combat Layer 7 attacks on modern applications, security and development teams need to:

- Integrate flexible "security as code" protections into development processes such as CI/CD workflows to mitigate application abuse
- Mitigate Layer 7 attacks automatically by detecting anomalies in client behavior and server health status
- Ensure consistent security by seamlessly integrating protections into modern app infrastructures

NGINX App Protect Denial of Service (DoS) is a modern application security solution specifically designed to protect your most critical assets – applications. Running natively on NGINX Plus, and built on F5's market-leading WAF and behavioral protection, NGINX App Protect DoS incorporates consistent and adaptive DoS protection across clouds and architectures.

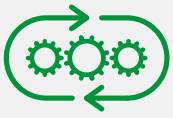
Why NGINX App Protect DoS?

Strong App Security

Protect your business from revenue-impacting denial of service by defending against Layer 7 attacks which can evade traditional network defenses

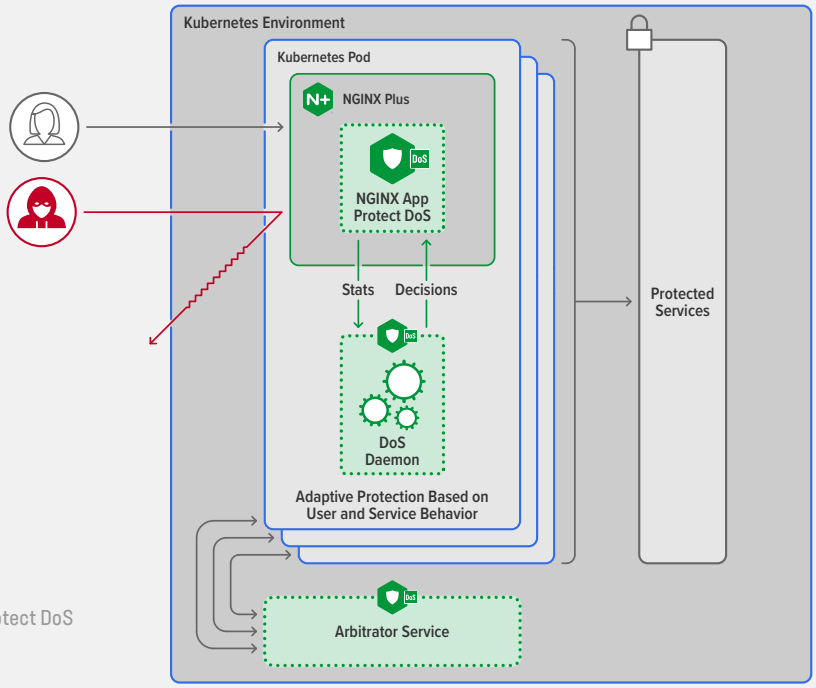
Built for Modern App Architectures

Enable consistent app security for web applications, microservices, cloud-native apps, and APIs, with delivery on NGINX providing advanced security, performance, and scale



CI/CD Friendly

Enable security to keep pace with development with centralized management and automation of security policy to remove workflow bottlenecks and support "shift left" Dev initiatives



Architecture for NGINX App Protect DoS in a Kubernetes Environment

Seamless Integration with NGINX, the #1 Web Application Platform

- Enables strong security controls to integrate seamlessly into modern infrastructure architectures – wherever NGINX Plus is deployed
- Minimizes costs, reduces latency, accelerates performance, and improves the user experience
- Reduces the complexity, manual oversight, and tool sprawl needed to deliver modern apps from code to customer

Security as Agile as Your Apps

- Natively integrates security policy and facilitates “security as code” integration with DevOps tools
- Deploys rapidly as a lightweight software package
- Automates protection through a continuous feedback loop that measures mitigations and their effectiveness

Dynamic and Adaptive Statistical Model

- Learns and baselines normal traffic patterns using statistical models and analysis of client behavior and application/API health
- Constructs and deploys dynamic signatures to mitigate attacks automatically
- Continuously measures mitigation effectiveness and adapts to changing behavior or health conditions

Speed Time to Market at Reduced Cost

- Takes the burden off developers so they can focus on delivering new capabilities that lead to competitive advantage
- Gives emerging DevSecOps teams a way to integrate security into automated app delivery
- Enables cost-effective protection at NGINX scale with no-touch configuration

Supported Environments

Cloud

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- VMware

Containers

- Docker
- Kubernetes
- OpenShift

CPUs

- x86 (64 bit)

Operating Systems

- CentOS
- Debian
- Ubuntu

To discover how NGINX can help you, visit nginx.com.

NGINX
Part of F5