Defend, adapt, and mitigate against layer 7 DoS attacks with F5 DoS for NGINX®

Protect your apps and APIs across hybrid, multicloud environments from hard-to-detect, application-layer DDoS attacks.

Key benefits

Accelerate attack mitigation
Stop DoS/DDoS attacks before they start with a multi-layered defense strategy leveraging eBPF technology.

Enhance security
Go beyond tracking client traffic patterns with combined service health checks to enable superior DoS/DDoS attack detection.

Automate defenses
Greatly reduce operating costs and enjoy adaptive learning for no-touch policy configuration through machine learning.

The ever-increasing risk of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

Every year, DDoS attacks continue to grow seemingly exponentially across every metric—in number, frequency, bandwidth, and complexity. Layer 7 attacks are more than keeping pace, as they have quickly become a favorite attack of cybercriminals. Threat actors use multi-vector attacks that target the application layer to maximize organizational pain and damage. They know that even a short service interruption can bring about significant revenue losses and severely damage corporate reputations, not to mention drive lawsuits against your company and cost executives their jobs. Plus, these attacks also leave your applications and environments exposed to other types of parasitic attacks, further damaging bottom lines and reputations. How can an organization today keep from becoming the latest, tragic attack headline?

Powerful, streamlined, application-layer DoS and DDoS protection

The F5® Application Delivery and Security Platform (ADSP) delivers security for any app and API anywhere, reducing the complexity associated with today's hybrid multicloud operations by consolidating your critical app services across deployments.

A key component of F5 ADSP, F5 NGINX simplifies protection against layer 7 DoS and DDoS attacks and their aftermath with F5 DoS for NGINX. F5 DoS for NGINX offers lightweight, high-performance, low-latency DoS and DDoS attack mitigation that is platform-agnostic and easily integrated across hybrid multicloud environments. Deploy DoS protection on NGINX Ingress Controller or per-pod or per-service proxies. F5 DoS for NGINX enables a comprehensive attack mitigation strategy that is configurable, robust, and multi-layered. This solution delivers adaptive, consistent protection from application-layer DoS and DDoS attacks across your distributed architectures and environments.

DoS attacks at the application layer have quickly become a favorite tool of cybercriminals to maximize organizational pain and damage.

Key features

Enable flexible, comprehensive protections

Deploy dynamic signatures to automatically mitigate attacks while measuring mitigation effectiveness and adapting to changing threat behaviors or application health conditions.

Mitigate multiple DoS attack types

Defend applications and APIs against flood attacks, low and slow attacks, challenger attacks, and targeted SSL/TLS attacks.

Automate security-as-code

Apply consistent protection by integrating declarative security policies seamlessly into CI/CD pipelines.

Reduce operating costs and false positives

Detect anomalies and block malicious traffic without affecting legitimate traffic by using machine-learning-based algorithms that observe normal traffic patterns and establish a baseline.

F5 DoS for NGINX offers lightweight, high-performance, low-latency DoS and DDoS attack mitigation that is platform-agnostic and easily integrated across hybrid multicloud environments.

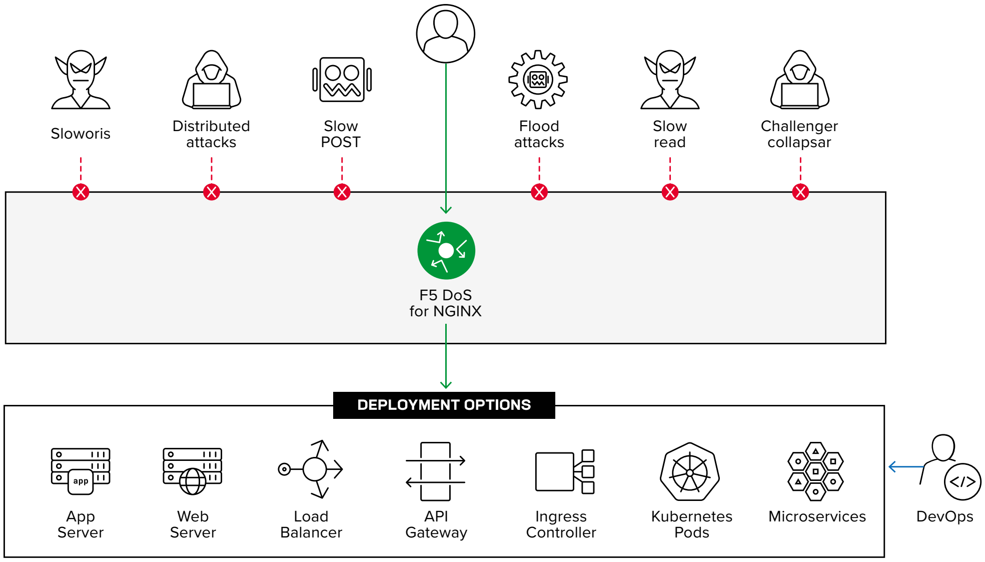

Figure 1: F5 DoS for NGINX delivers comprehensive protection against DoS and DDoS attacks for apps and APIs anywhere.

Implement a multi-layered DoS/DDoS defense strategy

F5 DoS for NGINX blocks known bad IP addresses and bad requests with attack signatures, while enforcing global rate limiting as necessary. It significantly reduces operating costs and false positives through machine-learning-based algorithms, which observe normal traffic patterns—tracking hundreds of metrics of user and application behavior—and establish a baseline, allowing the platform to then detect anomalies and block malicious traffic without affecting legitimate traffic. Dynamic signatures may be deployed automatically to mitigate detected attacks. F5 DoS for NGINX measures the effectiveness of mitigation efforts, adapting to changes in user behaviors or application health conditions.

Prevent bad actors from consuming critical resources

F5 DoS for NGINX mitigates application attacks by protecting gRPC, WebSocket, and other HTTP/S and HTTP/2 apps against multiple types of sophisticated DoS attacks including:

- GET and POST flood attacks, which overwhelm servers with a high volume of requests
- Slowloris, Slow Read, and Slow POST low and slow attacks that tie up resources
- Challenger Collapsar, which aims to exhaust targeted server resources and degrade application availability
- Targeted SSL/TLS attacks

F5 DoS for NGINX also ensures application uptime using signature mechanisms for mitigation based on the CLIENT HELLO message.

Get dynamic DDoS mitigation designed for CI/CD

F5 DoS for NGINX continuously measures mitigation effectiveness with adaptive learning. With no-touch policy configuration, F5 DoS for NGINX enables cost-effective DoS and DDoS protection at scale. You can apply consistent protection with declarative security policies via the Kubernetes API. F5 DoS for NGINX seamlessly integrates security-posture configuration changes into your CI/CD pipeline, enabling layer 7 DoS defense as security-as-code.

Lightweight, high-performance, low-latency attack mitigation

Easily integrate platform-agnostic protection with NGINX Ingress Controller and F5 DoS for NGINX across your hybrid-multicloud Kubernetes environments. Reduce complexity and tool sprawl with single-vendor DoS mitigation that automates security-as-code seamlessly into your software development lifecycle (SDLC), so security can be tested and released within your applications at production. This solution delivers cost-effective DoS and DDoS protection at scale and with no-touch configuration.

Automate your defenses, enhance your security, and stop DoS and DDoS attacks before they start with a multi-layered defense strategy by deploying F5 DoS for NGINX.

Next steps

See how F5 DoS for NGINX works with a free trial.

Contact us to find out how F5 products and solutions can enable you to achieve your goals.