NGINX
Part of F5

PRODUCT DATASHEET

F5 NGINX INGRESS CONTROLLER

Enterprise-Class Connectivity for Kubernetes Apps

WHY USE NGINX INGRESS CONTROLLER?

Increase Uptime
Ensure availability of business-critical apps in scalable, dynamic environments, preventing connection timeouts and errors

Improve Security
Integrate strong centralized security controls at the edge of a Kubernetes cluster to strengthen app protection

Gain Insight
Achieve better visibility into app health and performance to reduce outages and simplify troubleshooting

Increase Uptime, Improve Security, and Gain Better Insight into App Health

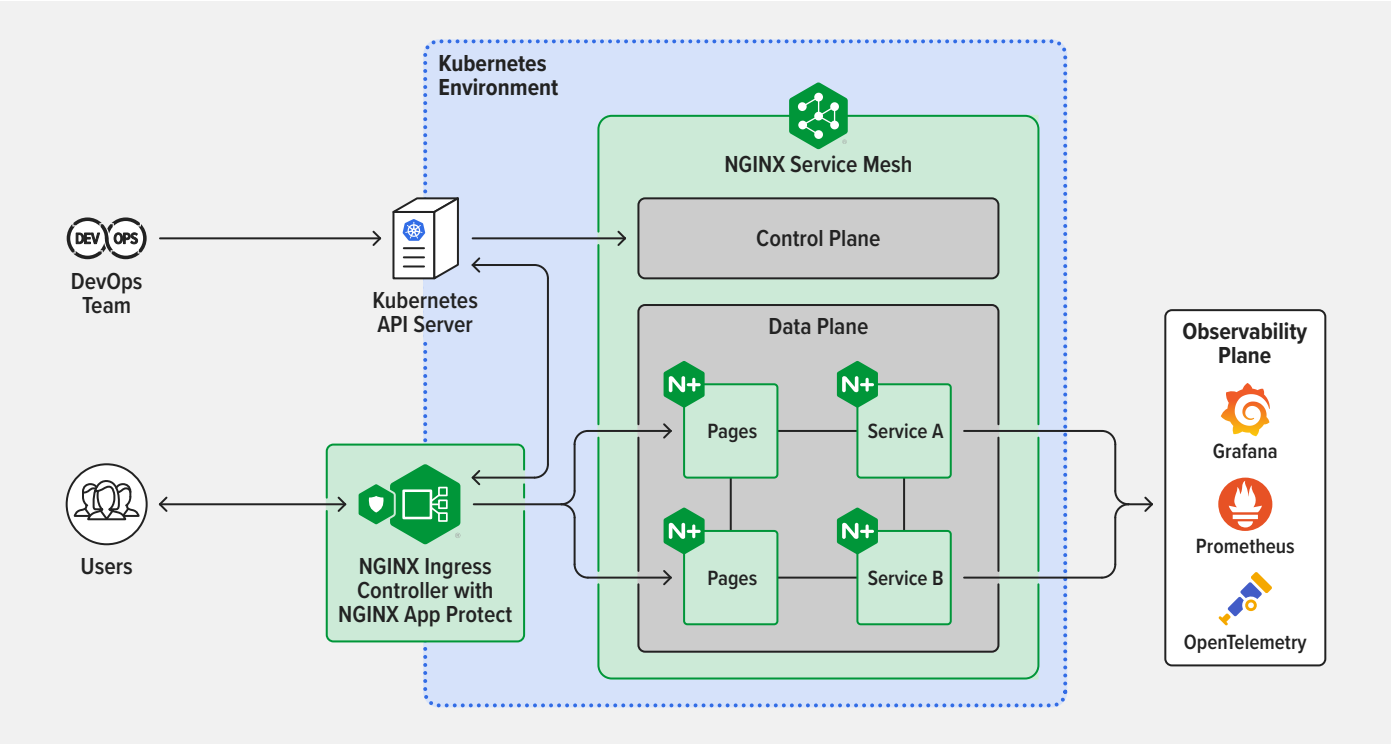
Kubernetes adoption is growing rapidly as organizations discover it's the most suitable way to deploy and run containerized microservices-based applications at scale.

However, organizations are facing challenges with security, reliability, observability, and scalability when they run Kubernetes in production:

- Connection timeouts and errors in scalable, dynamic environments lead to service interruptions
- Inadequate protection across distributed environments increases risk of exposure to cybersecurity threats
- Insufficient visibility into app health and performance causes outages and troubleshooting difficulties

NGINX Ingress Controller is a part of NGINX Connectivity Stack for Kubernetes, designed to address app connectivity challenges in production environments – including on premises, in the cloud, and at the edge – with its enterprise-class availability, security, and visibility features:

- Ensures availability of business-critical apps with advanced load balancing and connectivity patterns
- Improves protection with strong centralized security controls at the edge of the Kubernetes cluster
- Reduces outages and simplifies troubleshooting with granular real-time and historical metrics and dashboards



Benefits of NGINX Ingress Controller

Simplify and streamline app connectivity in any Kubernetes environment. Enhance capabilities of cloud provider and pre-packaged Kubernetes offerings with higher degrees of security, availability, and observability at scale.

Ensure Availability

Prevent connection timeouts and errors and avoid downtime when rolling out a new version of an app or during topology changes, extremely high request rates, or service failures.

- Advanced Layer 7 (HTTP/HTTPS, HTTP/2, gRPC, WebSocket) and Layer 4 (TCP/UDP) load balancing with active health checks
- Blue-green and canary deployments
- Rate limiting and circuit breaker connectivity patterns

Improve Visibility

Gain better insight into app health and performance with more than 200 granular real-time and historical metrics to reduce outages and simplify troubleshooting.

- Discover problems before they impact your customers
- Find the root cause of app issues quickly
- Integrate data collection and representation with ecosystem tools, including OpenTelemetry, Grafana, Prometheus, and Jaeger

Strengthen Protection

Ensure holistic app security with user and service identities, authorization, access control, encrypted communications, and Layer 7 app protection.

- HTTP basic authentication, JSON Web Tokens (JWTs), OpenID Connect (OIDC), and role-based access control (RBAC)
- End-to-end encryption (SSL/TLS passthrough, TLS termination)
- OWASP Top 10 and Layer 7 DoS defense through integration with optional NGINX App Protect modules

Automate Security for DevSecOps

Reduce complexity and tool sprawl through technology consolidation for faster and easier app delivery.

- Tight integration with NGINX Service Mesh for unified app connectivity into, out of, and within the cluster
- Data and control planes are the same across all hybrid and multi-cloud environments
- Focus on core business functionality, offloading security and other non-functional requirements to the platform layer

To learn more, visit nginx.com/k8s

NGINX
Part of F5