Secure Distributed Apps and Microservices at Scale Without Adding Complexity and Overhead

The ever-increasing number of cybersecurity attacks on web apps creates significant risk of exposure to both external and internal threats in on-premises, hybrid, and multi-cloud Kubernetes environments.

Organizations face security challenges because:

• The number and sophistication of cyberattacks is growing exponentially and consequences of a security breach can be irreparable
• Complex environments with disaggregated technologies and tool sprawl are harder to secure, operate, manage, and troubleshoot
• Failure to comply with governmental and industry regulations for protection of sensitive data can be very costly
• Strict security controls are seen by developers as a barrier to agility

F5 NGINX helps protect Kubernetes apps from edge to cloud without adding complexity and overhead:

• Prevent unauthorized activity through constant authentication, identity validation, and detection of behavioral anomalies
• Minimize the attack surface through least-privilege policies, fine-grained access control, and end-to-end encryption
• Simplify delivery of apps securely from code to customer with an integrated WAF and app-level DoS defense
• Streamline self-service app releases across multi-tenant development teams without compromising security
Benefits of Zero Trust Security for Kubernetes Apps

Using Kubernetes-native technologies, including Ingress controller and WAF/DoS protection, NGINX helps your organization implement comprehensive Zero Trust security for your Kubernetes apps.

Authentication and Authorization
Manage user, app, and service identities and authorize them to perform actions across the Kubernetes cluster with HTTP Basic authentication, JSON Web Tokens (JWTs), and OpenID Connect through integrations with identity providers (IdPs) such as Okta and Azure Active Directory (AD).

Data Encryption and Integrity
Secure communications regardless of location with authentication and encryption to ensure validity, confidentiality, and integrity of data through TLS passthrough, SSL/TLS termination, and mTLS.

Access Control and Access Policy
Easily align with your organization’s security needs and enable self-service and governance across multi-tenant teams through role-based access control (RBAC) and custom resource definitions (CRDs).

Monitoring and Observability
Gain actionable insights into the security posture of your apps, APIs, and infrastructure through prebuilt integrations with your favorite tools, including OpenTelemetry, Grafana, Prometheus, and Jaeger.

WAF and DoS Protection
Protect apps from the OWASP Top 10 and Layer 7 DoS attacks without slowing down release velocity and performance.

To learn more, visit nginx.com/zt