NGINX
Part of F5

Zero Trust Security for Kubernetes Apps

Holisitic App Protection from Edge to Cloud

Secure Your Distributed Apps, Microservices, and APIs at Scale

The sophistication and number of cybersecurity attacks is growing exponentially, which creates significant risk of exposure to both external and internal threats in on-premises, hybrid, and multi-cloud Kubernetes environments.

Security incidents are costly in many ways: they can disrupt your organization's productivity, damage your reputation, violate regulatory compliance, and result in theft of confidential data.

Traditional security models place a perimeter around your infrastructure and assume that users and activity inside it are trustworthy. For today's distributed environments, however, location can no longer be the basis for trust – traffic that seems to be "internal" can still be a threat.

Adopting a Zero Trust security model for your Kubernetes infrastructure can help improve your security posture. Zero Trust is an identity-based security model that helps protect users, applications, data, and devices regardless of their location – inside or outside of the organization's boundaries, remote, on-premises, or in the cloud. It is based on three core principles – never trust, always verify, and continuously monitor.

F5 NGINX offers centralized Zero Trust security policy enforcement in Kubernetes at the edge of the cluster with NGINX Ingress Controller and within the cluster with NGINX Service Mesh.
In addition, with NGINX App Protect you can deploy advanced WAF and DoS protection against sophisticated cyberattacks at the cluster, service, or pod level. This frees developers from the burden of building, maintaining, and replicating security logic across their apps – instead they can easily leverage security technologies at the platform level.

Why Use NGINX for Zero Trust in Kubernetes?

Secure Kubernetes apps from edge to cloud without adding complexity and overhead.

Actionable Insights

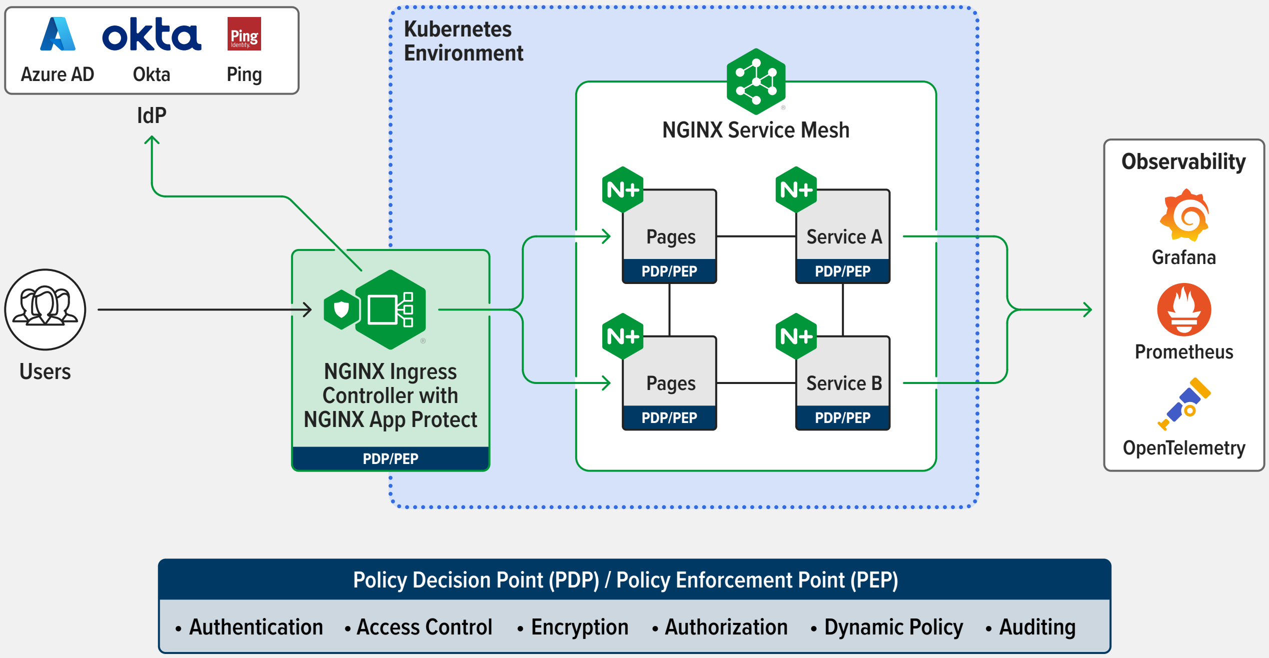
Detect and mitigate cybersecurity threats before they cause damage to your organization and customers

Deployment Flexibility

Streamline and unify protection of your apps and APIs no matter where you run Kubernetes

Protection at Scale

Improve customer experiences under peak workloads without compromising security



Authentication and Authorization

Zero Trust mandates authentication and authorization of every device, user, service, and request. With NGINX you have several options for authentication and authorization services, including HTTP Basic authentication, JWT authentication, and OIDC authentication through integration with identity providers such as Okta and Azure AD. Use NGINX to issue secure identity certificates for authenticating services and authorizing them to perform actions across the Kubernetes cluster.

Data Encryption and Integrity

Zero Trust demands that all communication be secured regardless of location, which requires both authentication of all parties, and encryption to ensure the confidentiality and integrity of data. For user-to-service communication, NGINX supports both TLS Passthrough and TLS termination. For service-to-service communication, NGINX uses mTLS for authentication and encryption, and ensures that only specific services are allowed to talk to each other.

Access Control and Access Policy

Access control is another critical element in a Zero Trust architecture. NGINX supports role-based access control (RBAC) for easy alignment with your organization's security needs. With RBAC in place, users get gated access to the functionality they need to do their jobs without having to file a ticket and wait for the IT team to fulfill it. You get fine-grained access management capabilities that enable self-service and governance across multiple teams.

Observability

Auditing, monitoring, logging, tracing, and reporting are key to successfully establishing Zero Trust and improving your security posture. NGINX generates granular real-time and historical metrics, and integrates with popular tools including OpenTelemetry, Grafana, and Prometheus. Deep traces reveal how requests are processed end to end, the kind of information you need for actionable insights into the health and performance of your apps, APIs, and infrastructure.

WAF and DoS Protection

To further strengthen the security of your distributed applications and protect them from OWASP Top 10 and Layer 7 DoS attacks, leverage NGINX App Protect's WAF and DoS modules. Built on F5's industry-leading security expertise, NGINX App Protect provides agile, app-centric protection from the most advanced threats without compromising release velocity and performance. It can also easily forward telemetry to third-party analytics and visibility solutions.

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