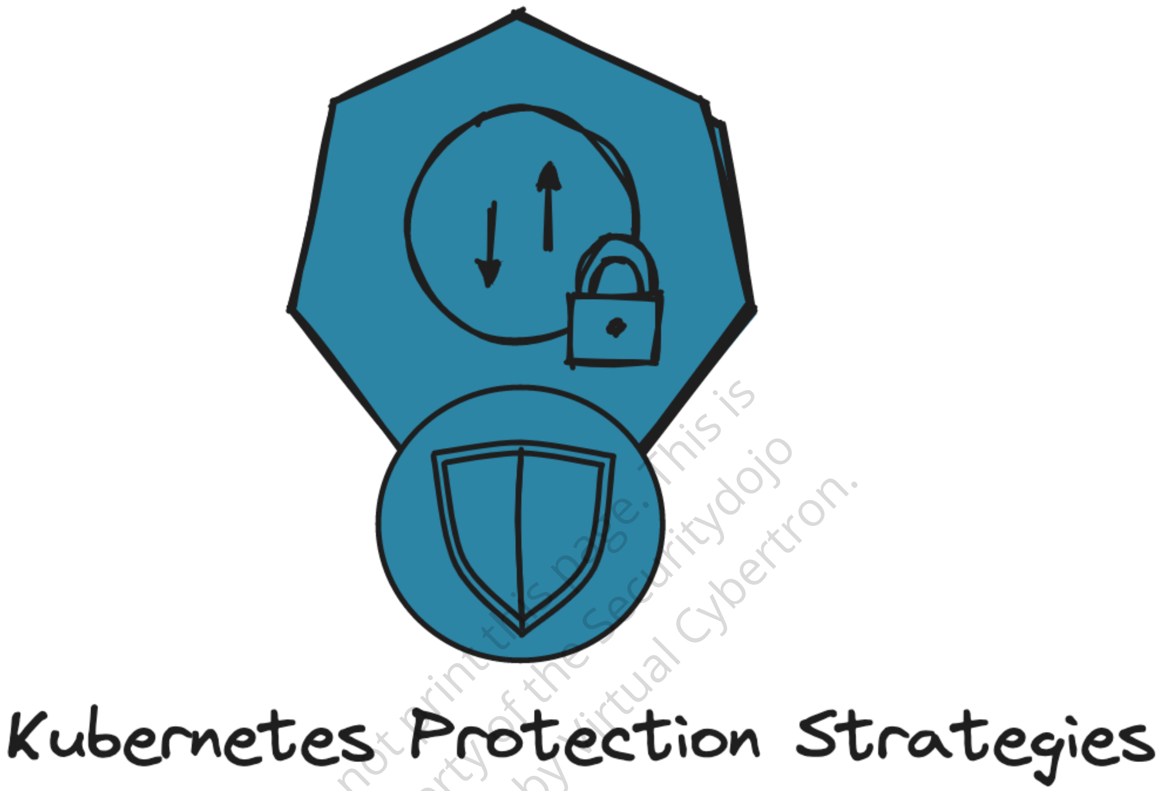
Protection Strategies



Protection strategies are practices implemented to enhance the security and protection of Kubernetes clusters and applications running within them.

These strategies aim to mitigate potential risks and vulnerabilities by employing various security mechanisms and tools.

The mentioned protection strategies include:

- Network Policies: Network policies give a Kubernetes cluster fine-grained control over network traffic. They specify guidelines for network inbound and outbound traffic.
- RBAC (Role-Based Access Control): RBAC gives Kubernetes access control and authorization tools.
- Secret Management: In Kubernetes, secrets are used to store sensitive data including API keys, certificates, and passwords.

- Admission Controller (such as Kyverno): Admission controllers are parts of the Kubernetes API server that intercept and verify requests. They uphold particular laws and regulations, such as upholding security laws, validating pod configurations, and guaranteeing adherence to organizational standards.
- Cilium: For Kubernetes, Cilium is a networking and security plugin. Access control lists (ACLs), network layer visibility, and inter-pod communication encryption are among the advanced network security features it offers.
- AppArmor: A Linux security module called AppArmor makes it possible to implement fine-grained application-level security restrictions. It restricts the capabilities and actions of containers within a Kubernetes cluster.
- Istio Service Mesh: Istio is a service mesh solution. By integrating functions like mutual TLS (Transport Layer Security), granular access control, traffic routing, and telemetry, it improves network security.

image generated via adobe ai