Cisco Kubernetes WAAP (KWAAP)

Native, air-gapped application and API protection for cloud-native environments

As Kubernetes becomes the foundation for cloud-native applications, protecting them in runtime—without compromising agility—is more urgent than ever. Traditional web application firewalls (WAFs) weren't built for a microservices software development lifecycle. They live outside the cluster, struggle with API context, and break CI/CD pipelines.

Cisco® **KWAAP** (Kubernetes Web Application and API Protection) is a Kubernetes-native, CRD-managed, and **air-gapped** solution that embeds runtime application and API security directly into your Kubernetes environment—scaling with your workloads and aligned with DevOps workflows.

Securing Kubernetes without slowing it down

Today's DevOps, InfoSec, and DevSecOps teams face increasing complexity and risk:

- APIs are the #1 attack surface, but traditional WAFs lack visibility into API calls and business logic and do not provide accurate, real-time protection against HTTP distributed denial-of-service (DDoS) attacks on API-based applications.
- Most perimeter WAFs can't inspect **east-west microservice traffic** inside the cluster.
- Security is expected to **shift left**, but legacy tooling isn't built for GitOps or automation.
- Industries like finance, defense, and healthcare demand **air-gapped deployments**—yet almost all app security tools require cloud-based management or external connectivity.

The result? Gaps in protection, tool sprawl, and friction between security and velocity.

What's needed

A modern Kubernetes-native WAAP that can:

- **Deploy inside the Kubernetes cluster** (not around it)
- Be **managed declaratively via CRDs**
- Fit into **CI/CD and GitOps workflows**
- Understand **modern APIs and business logic**
- Be **operational in air-gapped environments with** no **dependency on cloud services or external calls**
- **Protect against automated bot-driven API and DDoS attacks** that go beyond the standard OWASP Top 10

How Cisco KWAAP solves these challenges

Cisco KWAAP is purpose-built for the realities of Kubernetes and DevSecOps. It secures both north–south and east–west traffic at runtime, with granular API and app-layer protections—and it can do it while entirely air-gapped.

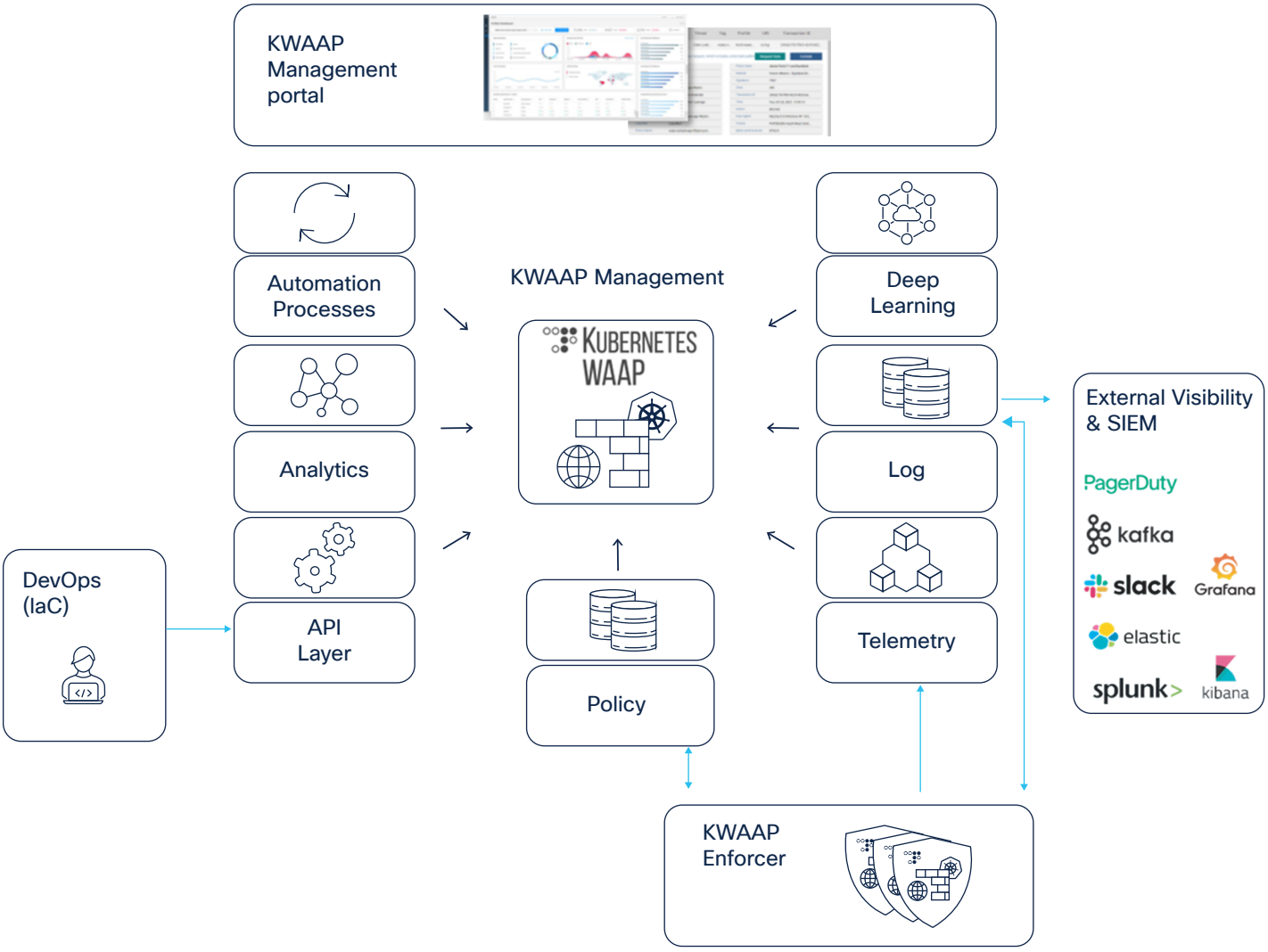
Core advantages

Security:

- **OWASP Top 10:** Complete and deep coverage with a unique model that combines negative and automated behavioral-based positive security
- **Advanced API protection:** API discovery and AI-based protection against the OWASP Top 10 API security risks
- **Web DDoS protection:** AI-powered behavior-based automated real-time protection against sophisticated and highly aggressive HTTP DDoS attacks
- **AI-based auto cross-correlation** between the WAF and API protection engines that automatically blocks malicious sources

Operational features:

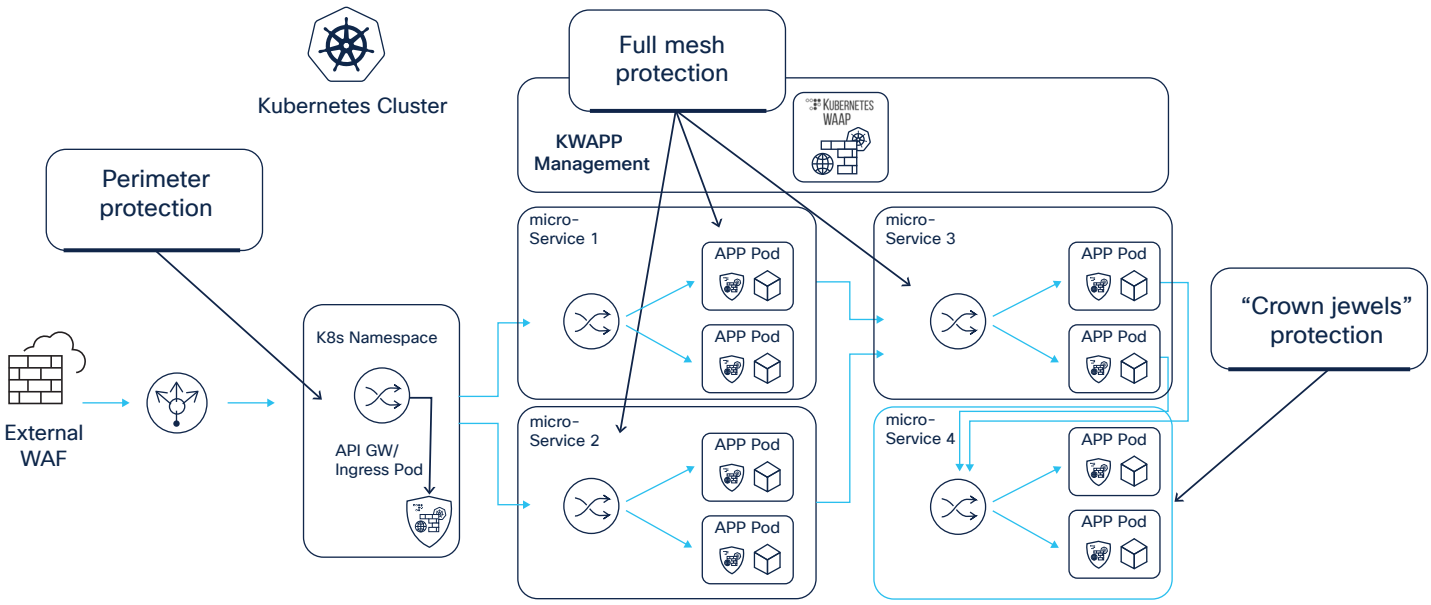
- **Runs natively entirely within your Kubernetes cluster** as a sidecar in the same pod as the microservice, and can work as a reverse proxy after either a sidecar proxy (e.g., Itsio/Envoy) or any other ingress method outside of the pod (e.g.,Nginx ingress controller)
- **Built-in observability** that integrates with Prometheus, Elastic, ELK, Datadog, and more
- **100% air-gapped: No reliance on external data flow or communication:** ideal for air-gapped, offline, or disconnected environments
- **All configurations can also be managed as Kubernetes CRDs** (no GUI dependency)
- **Detect-only, alert, or blocking enforcement modes** to support gradual rollout and safe testing
- **Integrates with third-party SIEM and SOAR solutions** for streamlined and seamless security management and orchestration



Cisco Kubernetes WAAP (KWAAP) is sold by Cisco through its global OEM partnership with Radware

Unique highlights

Feature	Why it matters
Air-gapped by design	Runs in completely disconnected environments without calling home—ideal for defense, regulated industries, and secure clouds
Kubernetes-native architecture	Deploys like any other service; no traffic redirection or external proxies
CRD-based policy management	Declarative WAF configuration via GitOps, Helm, kubectl
API protection	Automatically discovers APIs and validates OpenAPI schema at runtime—critical for modern microservices
Protects east-west traffic	Detects lateral movement and internal misuse between services
Shift-left friendly	Integrates with CI/CD pipelines, supports detect-only testing modes
Zero code changes required	Transparent deployment with no developer rework



Summary

Whether you're securing a mission-critical banking app, a healthcare platform, or a government workload in an air-gapped cluster, Cisco KWAAP empowers your DevOps and DevSecOps teams to deploy true application and API protection as a Kubernetes-native, fully self-contained solution—with no compromise on automation, agility, or security.

Cisco KWAAF is Kubernetes-native application and API protection, built to accelerate IT modernization.

Cisco Kubernetes WAAP (KWAAP) is sold by Cisco through its global OEM partnership with Radware