UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

USP CORE WAAP

App-Centric for Kubernetes

Technisches Whitepaper

Datum: August 2025
Version: 1.2

United Security Providers AG
Telefon +41 31 959 02 02
info@united-security-providers.ch
www.united-security-providers.ch

Besuchsadresse:
Hauptsitz
Stauffacherstrasse 65/15, 3014 Bern
Zürich
Baslerpark, Baslerstrasse 60, 8048 Zürich

UNITED SECURITY PROVIDERS

USP Core WAAP
App-Centric for Kubernetes

Core WAAP – cloud-native und ressourcenschonende Sicherheit für Webapplikationen und APIs, flexibel und nahtlos integrierbar in Ihre CI/CD-Prozesse.

KONTEXT

Cloud-native Umgebungen bieten maximale Agilität, Skalierbarkeit und Automatisierung. Die steigende Verbreitung von Microservices und APIs führt jedoch zu neuen Sicherheitsherausforderungen. Manuelle Prozesse und zentrale Engpässe bremsen die Bereitstellung und erhöhen das Risiko für Schwachstellen.

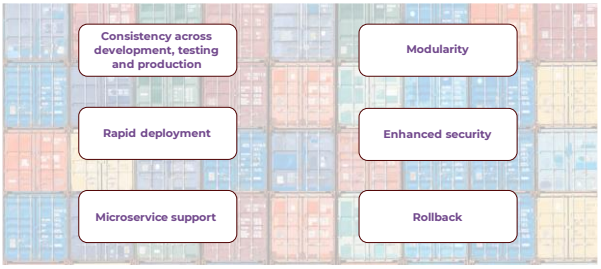

Abbildung 1: Mehrwert der Containerisierung

Moderne DevOps-Teams benötigen daher eine Sicherheitslösung, die sich nahtlos in CI/CD-Pipelines integrieren lässt und Security-as-Code sowie Automatisierung unterstützt.

TECHNISCHE ARCHITEKTUR

Core WAAP App-Centric für Kubernetes nutzt einen Kubernetes Operator, um alle benötigten Ressourcen als Infrastructure as Code bereitzustellen und zu verwalten. So lassen sich Sicherheitsrichtlinien nahtlos in Ihre CI/CD-Pipeline integrieren. Teams können dadurch Schutz sowie Richtliniendurchsetzung direkt auf Applikationsebene einbinden.

SCHLÜSSELELEMENTE

Kubernetes Operator

Der Operator überwacht kontinuierlich applikationsspezifische Core WAAP Custom Resources (CRs) und steuert automatisch Rollout und Skalierung aller Core WAAP-Komponenten im Cluster.

Core WAAP Custom Resource

Sicherheitsrichtlinien – wie OWASP Top 10, API-Schema-Validierung, Allow-/Deny-Listen und virtuelles Patching – werden als Code in der Custom Resource definiert. So sind Versionierung, Peer Review und vollständige CI/CD-Automatisierung möglich.

Core WAAP Pod

Überprüft und filtert HTTP(S)- und API-Traffic auf Layer 7 und setzt Sicherheitsrichtlinien durch, bevor der Traffic die Applikationspods erreicht.

WIE ES FUNKTIONIERT

Policy as Code: Sicherheitskonfigurationen werden versioniert, geprüft und automatisiert via GitOps oder CI/CD.

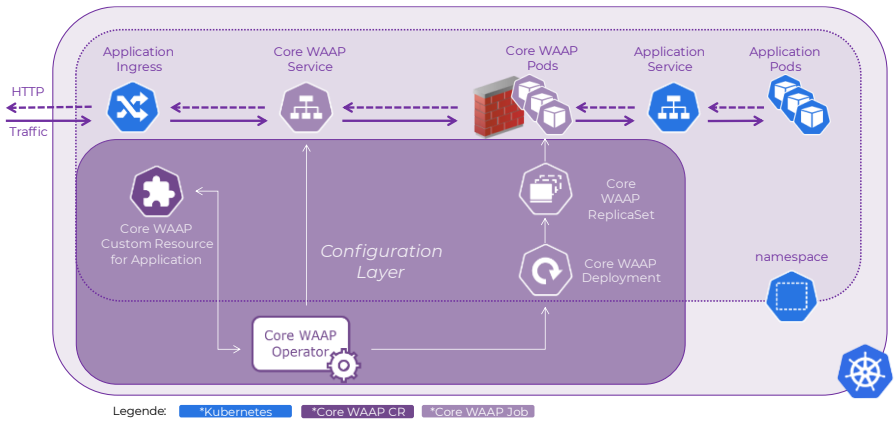

Abbildung 2: Application-Centric Architektur

Copyright © United Security Providers AG

USP Core WAAP
App-Centric for Kubernetes

Automatisierte Bereitstellung: Der Operator setzt Policy-Änderungen in Echtzeit um, stellt neue WAAP-Services bereit oder aktualisiert Policies clusterweit.

Echtzeitschutz: Sämtlicher eingehender und Ost-West-Traffic wird auf Layer 7 inspiziert, Richtlinien werden angewendet, bevor Anfragen die Applikation erreichen.

Vollständige Beobachtbarkeit: Alle Logs und Metriken werden für zentrale Analyse und Alarmierung exportiert.

Skalierbarkeit & High Availability: Architektur unterstützt horizontale Skalierung, Self-Healing, hohe Verfügbarkeit.

Self-Service: Teams können selbstständig Policies anpassen und testen, ohne auf zentrale Security-Teams angewiesen zu sein.

INTEGRATION IN DAS KUBERNETES-ÖKOSYSTEM

TRAFFIC FLOW

- Externer HTTP(S)-Traffic wird über den Standard Kubernetes Application Ingress oder Gateway geleitet.
- Der Core WAAP Service fängt alle eingehenden Anfragen ab und prüft diese, bevor sie an Applikation, beziehungsweise API - typischerweise ein Service - weitergeleitet werden.
- Core WAAP kann pro Namespace oder pro Applikation konfiguriert werden und ermöglicht so flexible und granulare Sicherheitssegmentierung.
- Ost-West-Traffic (Service-zu-Service) im Cluster kann ebenfalls überwacht und geschützt werden, womit Zero Trust-Prinzipien sichergestellt werden.

POLICY FLOW

- Policies werden im Git-Repository versioniert und durchlaufen Review-Prozesse.
- Die CI/CD-Pipeline validiert und spielt die Policies ins Cluster ein.
- Core WAAP Operator synchronisiert die Konfiguration und setzt diese zur Laufzeit durch.
- „Hot Reload“ und „Graceful Restart“ ermöglichen Policy-Updates ohne Downtime.
- ML-gestütztes Autolearning reduziert False Positives und verbessert Security-Korrektheit im Betrieb.

SECURITY FEATURES & BETRIEBSOPTIMIERUNG

Schutzmechanismen: Layer 7 Inspection, OWASP Top 10 Schutz, API Security, Virtual Patching.

Hybrides Security Modell: Vereint die Vorteile vom positiven und negativen Security Modell. Dies ermöglicht eine enorme Flexibilität, um einen optimalen Applikationsschutz zu gewährleisten.

Zero Trust & Microsegmentation: Pro Namespace/Applikation steuerbar.

Betriebsoptimierung: Automatisierung reduziert manuellen Betriebsaufwand um bis zu 30 % (Praxiswerte)

Schnellere Reaktion auf Schwachstellen dank **Virtual Patching**

Vereinfachtes Management durch **zentrale Policy-Verwaltung** und Log-Integration.

ICAP-Integration für Content Scanning: Direkte Anbindung externer Security-Scanner, z. B. Antivirus für Datei-Uploads.

Identity & Access Integration: Umfassende OAuth2/OIDC-Unterstützung inkl. PKCE und OIDC Relying-Party-Funktionalität.

PERFORMANCE, SKALIERUNG, BETRIEB

Performance: Nachweisbare Durchsatzraten, niedrige Latenz

Skalierung: Clusterweit und/oder pro Namespace

Reduzierter Betriebs- und Wartungsaufwand (Praxiswerte: bis zu 30 %)

Erweiterbarkeit durch Skripting: Flexibles Anpassen der Policy-Logik via eingebetteter Lua-Engine – ohne externe Komponenten.

Betrieb: Updates ohne Downtime, Rolling Updates unterstützt

Copyright © United Security Providers AG

USP Core WAAP
App-Centric for Kubernetes

HIGHLIGHTS

Core WAAP App-Centric ist von Ingenieuren für Ingenieure entwickelt:

- ✓ **Echte App-zentrische Architektur:** Direkte Einbettung in die Applikationsumgebung statt separater Sidecars oder rein Cloud-basierter Proxys.
- ✓ **Sichtbare Sicherheit:** Entwickler, Plattform- und Security Engineers erhalten direkte Sichtbarkeit und Kontrolle – weniger Abhängigkeit von zentralen Firewall-Teams.
- ✓ **Automation-first:** Alle Operationen (Bereitstellung, Skalierung, Updates, Auditing) über Kubernetes-native APIs und Operator-Workflows automatisiert.
- ✓ **Feingranulare Kontrolle:** Policies können so granular oder generisch wie nötig definiert werden – pro Applikation, pro Namespace, pro Umgebung für volle Flexibilität.
- ✓ **Schnelle Reaktion:** Virtuelles Patching und Konfigurationsupdates werden sofort im Cluster ausgerollt. Sicherheits- und Konfigurationsupdates in Echtzeit, ohne Downtime.
- ✓ **Transparenz und Nachvollziehbarkeit:** Jede Änderung ist versioniert, überprüfbar und auditierbar – für Audit & Compliance.
- ✓ **Kein Lock-in:** Offene APIs, native Kubernetes-Standards – portierbar über Cloud-Anbieter und On-Prem-Plattformen.

TRY SCENARIOS

Erfahren Sie mehr über Core WAAP und wie Ihre Organisation von moderner Applikations- und API-Sicherheit profitieren kann. Kontaktieren Sie uns für eine individuelle Beratung oder Live-Demo. Oder klicken Sie auf «Try Scenarios», um Core WAAP in Aktion zu erleben.

UNITED SECURITY PROVIDERS
ZERO TRUST UNIVERSE

Copyright © United Security Providers AG