UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

USP CORE WAAP

Applikationssicherheit in modernen IT-Landschaften

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

Applikationssicherheit in modernen IT-Landschaften

Core WAAP ist die moderne Antwort auf die Sicherheitsanforderungen digitaler Unternehmen. Die cloud-native Lösung schützt Applikationen und APIs in dynamischen IT-Landschaften effizient, integriert sich flexibel in bestehende Prozesse und sorgt für Agilität, Skalierbarkeit und nachhaltige Compliance.

EINLEITUNG

Die digitale Transformation verändert nicht nur Geschäftsmodelle, sondern auch die Anforderungen an Sicherheit und Effizienz. Unternehmen müssen gleichzeitig Agilität, Skalierbarkeit und Compliance sicherstellen.

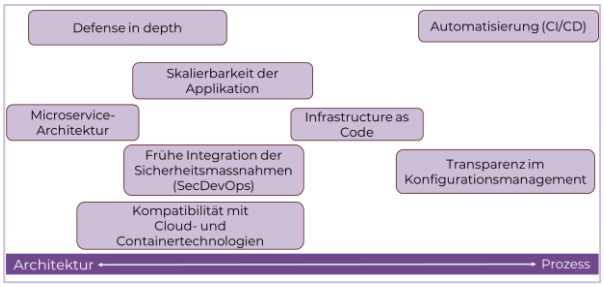

Abbildung 1: IT-Anforderungen im Wandel

WARUM HERKÖMMLICHE ANSÄTZE NICHT MEHR AUSREICHEN

Webanwendungen und APIs gehören zu den häufigsten Zielen von Cyberangriffen. Jährlich erleben über 85% der Unternehmen Angriffe auf der Anwendungsebene, die versuchen ihre WAF umgehen[1] insbesondere dort, wo klassische Schutzmechanismen an ihre Grenzen stossen[2].

Mit der Verlagerung von Anwendungen in die Cloud, dem Einsatz von Microservices und immer schnelleren Entwicklungszyklen steigt die Komplexität in IT-Landschaften laufend.

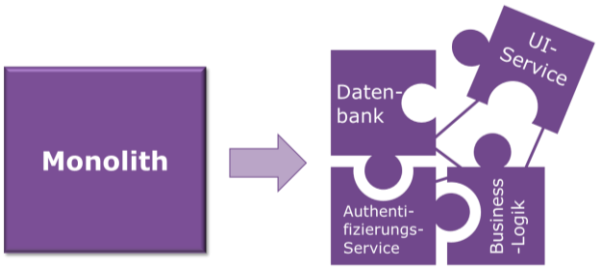

Abbildung 2: Wandel von Monolith zu Microservices

Traditionelle WAFs wurden für monolithische Umgebungen und klar abgegrenzte Perimeter entwickelt. Sie bieten jedoch nur begrenzte Sichtbarkeit und sind nicht dafür gemacht, interne Kommunikationswege (Ost-West-Traffic) und moderne DevOps-Prozesse effektiv abzusichern.

Gerade in agilen Projekten und modernen CI/CD-Pipelines sind klassische Ansätze zu starr: Die Trennung von Entwicklung, Deployment und nachgelagerter Sicherheitsprüfung verzögert Iterationen und erhöht das Risiko, dass Schwachstellen zu spät erkannt werden.

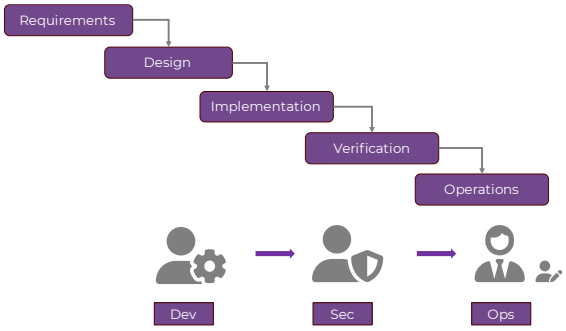

Abbildung 3: Traditioneller Entwicklungsprozess

Dadurch steigt auch der Personalaufwand erheblich: Viele Sicherheitsmassnahmen müssen manuell gepflegt, abgestimmt und aktualisiert werden, was Ressourcen bindet und das IT-Team zusätzlich belastet.

VORTEILE DURCH CONTAINER UND ORCHESTRIERUNG

Unternehmen setzen auf Container und Orchestrierungs-Systeme wie Kubernetes, um die Flexibilität, Automatisierung und Effizienz ihrer IT-Betriebsmodelle zu steigern. Container sorgen für Plattformunabhängigkeit, optimale Ressourcennutzung und ermöglichen es DevOps-Teams, Releases schneller und mit höherer Qualität umzusetzen, und bieten entscheidende Vorteile: Anwendungen lassen sich einfach zwischen verschiedenen Cloud- und On-Premises-Umgebun-

[1] Ponemon Institute, The State of Web Application Firewalls

[2] Verizon 2025 Data Breach Investigations Report

Copyright © United Security Providers AG

gen verschieben, ohne aufwändige Codeanpassungen. Das senkt Ausfallzeiten und Kosten nachhaltig.

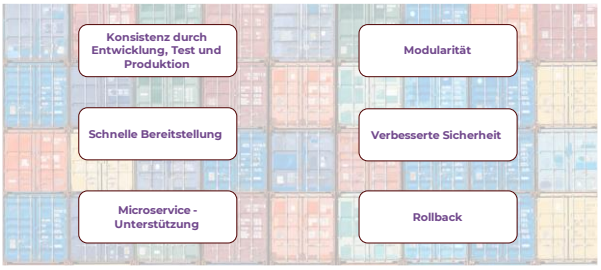

Abbildung 4: Mehrwert der Containerisierung

Mit der Integration von Security in den DevOps-Lebenszyklus (SecDevOps) setzen moderne Unternehmen auf das Prinzip „Security by Design“: Sicherheit wird von Anfang an automatisiert in alle Phasen integriert – von der Planung über die Entwicklung und das Testing bis hin zum Betrieb.

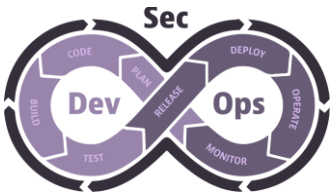

Abbildung 5: SecDevOps

Dank dem Shift-Left-Ansatz werden Security-Checks und Richtlinien frühzeitig und kontinuierlich umgesetzt. Risiken lassen sich so schon im Entstehungsprozess erkennen und beheben, sodass Innovation nicht gebremst, sondern gezielt und sicher gefördert wird.

WAS CORE WAAP ANDERS MACHT

Core WAAP ist cloud- und container-native und wurde speziell für moderne und microservice-basierte IT-Landschaften entwickelt.

Anders als viele Lösungen, die als separates Sidecar pro Applikation laufen (Microgateway-Prinzip) oder Cloud-basiert als Proxy fungieren, lässt sich Core WAAP direkt in die Anwendungsumgebung integrieren. Dies reduziert Ressourcen und ermöglicht eine flexiblere Einbettung.

Im Unterschied zu traditionellen Sicherheitslösungen bietet Core WAAP einen ganzheitlichen Schutz: Neben dem externen Datenverkehr (Nord-Süd) kann Ost-West-Traffic (Service-zu-Service) im Cluster ebenfalls überwacht und geschützt werden, womit Zero Trust-Prinzipien sichergestellt werden. So bleiben Anwendungen und APIs sowohl in der Cloud als auch im eigenen Rechenzentrum oder in hybriden Umgebungen jederzeit geschützt.

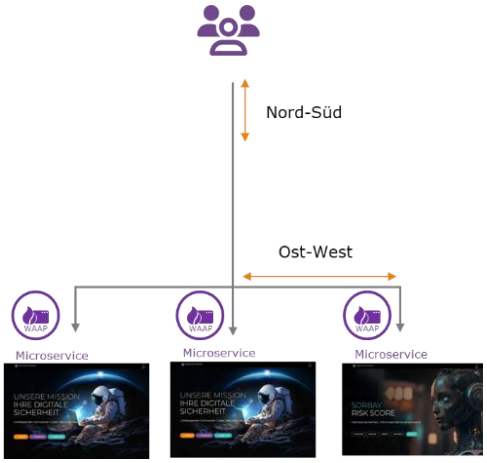

Abbildung 6: Ost-West und Nord-Süd

Durch die nahtlose Integration in bestehende CI/CD-, Deployment- und Test-Umgebungen automatisiert Core WAAP Sicherheitsprozesse, ermöglicht eine schnelle Bereitstellung und sorgt für effizientes Richtlinienmanagement.

Kriterium	Klassische WAF	Core WAAP
Architektur	Perimeter-zentriert	App-zentriert oder Gateway, cloud-native
Schutz intern/extern	Meist nur extern	Vollständig (auch Ost-West)
Automatisierung	Manuell, eingeschränkt	Automatisiert, Policy as Code
Integration in CI/CD	Nachgelagert, wenig flexibel	Nahtlos integriert, SecDevOps-ready
Betriebsaufwand	Hoch, personalintensiv	Bis zu 30 % weniger Aufwand
Skalierbarkeit	Eingeschränkt, selten Multi-Cloud	Multi-Cloud, flexibel, elastisch
Compliance & Audit	Zusatzaufwand, nachträglich	By Design, auditierbar

Tabelle 1: Klassische WAF vs. Core WAAP

Core WAAP unterstützt Zero-Trust-Strategien mit identitätsbasierter Mikrosegmentierung und schützt zuverlässig vor gängigen Bedrohungen wie SQL-Injection und Cross-Site Scripting.

Copyright © United Security Providers AG

USP Core WAAP
Applikationssicherheit in modernen IT-Landschaften

NUTZEN AUF EINEN BLICK

Core WAAP bewährt sich in verschiedensten Branchen– überall dort, wo sensible Daten oder Geschäftsprozesse geschützt werden müssen: Ob im E-Commerce, Applikationsentwicklung, Industrie oder öffentlicher Verwaltung.

Mit Core WAAP automatisieren Unternehmen ihre Applikations- und API-Sicherheit, reduzieren Betriebs- und Wartungsaufwand um bis zu 30 % und erhöhen gleichzeitig die Agilität.

Durch konsolidierte Entwickler-Tools und weniger manuelle Tasks stehen mehr Ressourcen für Innovation und Wachstum zur Verfügung – und Risiken wie Ausfallzeiten oder Compliance-Verstösse werden nachhaltig minimiert.

HIGHLIGHTS

- ✓ **Schnelle Einführung, hohe Flexibilität:** Lässt sich schnell in bestehende CI/CD- und DevOps-Prozesse einbinden – für sofort mehr Sicherheit. Auch in komplexen Multi-Cloud- und Hybrid-Umgebungen.
- ✓ **Ganzheitlicher Schutz:** Schützt nicht nur den externen Datenverkehr, sondern auch interne Kommunikation zwischen Microservices und Anwendungen – Angriffe werden früh erkannt und gestoppt.
- ✓ **Automatisiertes Lernen und Virtual Patching:** Die Lösung passt sich durch maschinelles Lernen und Virtual Patching dynamisch an neue Bedrohungen an – mit minimalem manuellem Aufwand.
- ✓ **Zero Trust und feingranulare Kontrolle:** Identitätsbasierte Mikrosegmentierung ermöglicht flexible Zugriffskontrollen – ein Schlüssel für eine zukunftssichere, Zero-Trust-orientierte Sicherheitsarchitektur.
- ✓ **Hybrides Security Modell:** Vereint die Vorteile vom positiven und negativen Security Modell. Dies ermöglicht eine enorme Flexibilität, um einen optimalen Applikationsschutz zu gewährleisten.
- ✓ **Compliance by Design:** Erfüllt aktuelle Datenschutz- und Compliance-Anforderungen und erleichtert den Nachweis gegenüber Behörden, Kunden und Partnern.

TRY SCENARIOS

Erleben Sie, wie Ihre Organisation mit Core WAAP profitieren kann – kontaktieren Sie uns für eine individuelle Beratung oder Live-Demo. Oder testen Sie Core WAAP direkt mit unseren „Try Scenarios“ online.

UNITED SECURITY PROVIDERS
ZERO TRUST UNIVERSE

Copyright © United Security Providers AG