

Workload Protection as a Service

State-of-the-Art Security für Ihre
Container- und Multi-Cloud-Umgebung



Ihre Herausforderung

Mit der Digitalisierung von Geschäftsprozessen steigt auch die Angriffsfläche für Cyberkriminelle. Gerade in Container- und Multi-Cloud-Umgebungen mit einer Vielzahl an Komponenten können IT-Verantwortliche schnell den Überblick verlieren. Sie stehen vor der Herausforderung, Konfigurationsprobleme aufzudecken, Verbindungen transparent zu machen und zu überwachen, auffälliges Verhalten in ihrer Infrastruktur frühzeitig zu entdecken und rechtzeitig zu reagieren. Zudem möchten sie Security in ihre DevOps-Prozesse einbinden (DevSecOps) und auf diese Weise Fehler im Quellcode von vornherein unterbinden.

Unsere Lösung

Mit dem Produkt Workload Protection as a Service bieten wir IT-Entscheider:innen eine einfach zu implementierende Lösung, welche diese Challenges adressiert. Dabei profitieren Unternehmen vom Betrieb der Plattform durch plusserver inkl. deutschsprachigem 24/7 Support, um schnell und einfach ihre Infrastrukturen abzusichern. Zusätzlich gehört ein persönliches Onboarding durch das plusserver Security Team zum Gesamtpaket, sodass auch ohne eigene Spezialist:innen State-of-the-Art Security im Unternehmen zur Verfügung steht.

Abrechnung nach Verbrauch (monatlich)

Asset: 9,49 €

Onboarding: 1.320,00 € (einmalige Kosten)

Gerne führen wir mit Ihnen eine begleitete Live-Demo auf Anfrage durch.

[› Jetzt anfragen](#)

Ihre Vorteile im Überblick:

- + Ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen
- + Automatisierte Inventarisierung von Cloud-Ressourcen
- + Erkennen und Blockieren von Angriffen auf Container, Web-Applikationen oder Hyper-scaler-Ressourcen
- + Benchmarks nach Industrie-Standards (CIS, NIST, PCI DSS etc.)
- + Risikomanagement zur Priorisierung von Bedrohungen
- + Netzwerksicherheit durch Einsicht in Datenflüsse über Container- und Cloud-Umgebungen inkl. Einstellen von Firewallregeln (herstellerunabhängig)
- + Meldung von sicherheitsrelevanten Ereignissen über diverse Schnittstellen (E-Mail, SMS, Syslog, SIEM)
- + Plattformbetrieb und Onboarding durch plusserver
- + Deutschsprachiger 24/7 Support
- + Integration in ein SOC möglich (plusserver oder eigenes)
- + Anwendbar z. B. auf der pluscloud open, plusserver Kubernetes Engine (PSKE), AWS, Azure

Workload Protection as a Service unterstützt Sie bei vier großen Security-Herausforderungen:

Transparenz

- + Dashboards
- + Inventarisierung von Cloud-Ressourcen
- + Risikomanagement zur Priorisierung von Bedrohungen
- + Compliance

Container-Sicherheit

- + Images & Container (Schwachstellenüberwachung)
- + Runtime Protection (XDR, File-Überwachung etc.)

Applikationssicherheit/DevSecOps

- + Source Codes Scans (DevSecOps)
- + IAC Scans (Infrastructure as a Code Scanning)
- + Compliance

Multi-Cloud-Sicherheit

- + Platform Protection (z. B. AWS, Azure und GCP)
- + Serverless-Funktionen
- + File Storage (z. B. S3)

Übersichtliches Dashboard

Nach unserem Onboarding sind Sie in der Lage, selbstständig mit dem Produkt zu arbeiten. Auf dem Dashboard sehen Sie zum Beispiel auf einen Blick, wie viele Schwachstellen gefunden wurden und wie schwerwiegend diese sind.



plusserver

Eine souveräne, zukunftsfähige und sichere Cloud

Wir bieten deutschen Unternehmen eine datensouveräne und anbieterunabhängige Basis für ihre digitalen Geschäftsprozesse. Auf unseren sicheren, skalierbaren Cloud-Plattformen realisieren Kunden zukunftsfähige und kosteneffiziente digitale Anwendungen. Wir beraten unsere Kunden zu Cloud-Architekturen sowie zur Integration bestehender IT-Umgebungen. Dabei agieren wir schnell, dynamisch und stets persönlich.

**Sie haben Fragen? Kontaktieren Sie uns.
Wir helfen gerne weiter.
Schnell und unkompliziert.**

+49 2203 1045 3500
beratung@plusserver.com

