controlware

CLOUD

ROADSHOW 2025

Der Controlware Kubernetes Checkup

Fabian Hart

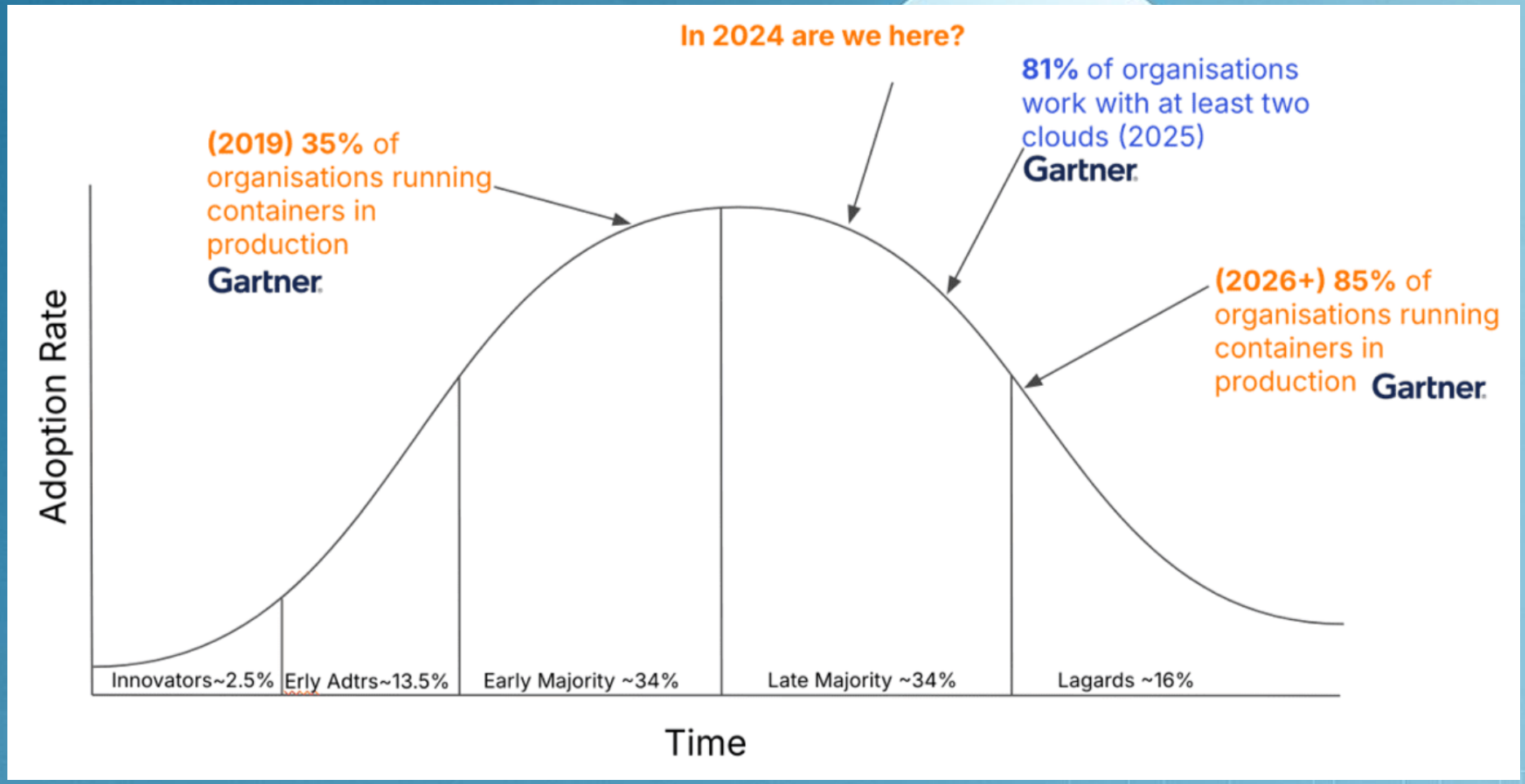
Cloud Solution Architect

© 2025 Controlware GmbH

©2025 Copyright Controlware.de

controlware

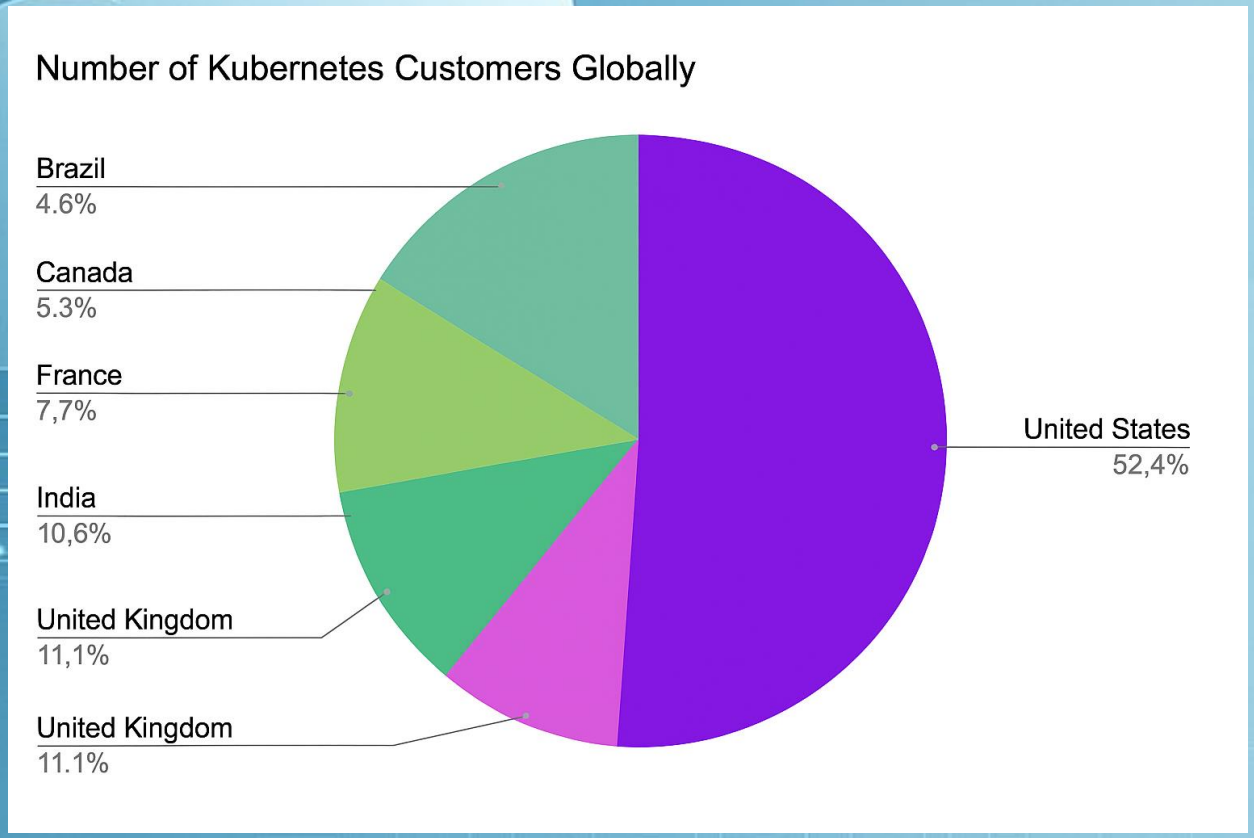
Adoption Rate



© 2025 Controlware GmbH

Marktanteile zu Kubernetes & Container

- *Der Kubernetes-Markt hat im Jahr 2022 einen Wert von $1,195 Mrd. und eine Prognose auf $9,69 Mrd. im Jahr 2031*
- *Deutsche Kunden befinden sich unter den Top 5 Nutzern*
- *Containerisierung wird sowohl on-Prem als auch in der Public Cloud betrieben.*
- *Im Jahr 2023 nutzen 66% aller Unternehmen Container in einer Produktionsumgebung. Weitere 18% befinden sich in einer Evaluierung*



© 2025 Controlware GmbH

Source: Kubernetes adoption, security, and market trends report 2024 by Red Head

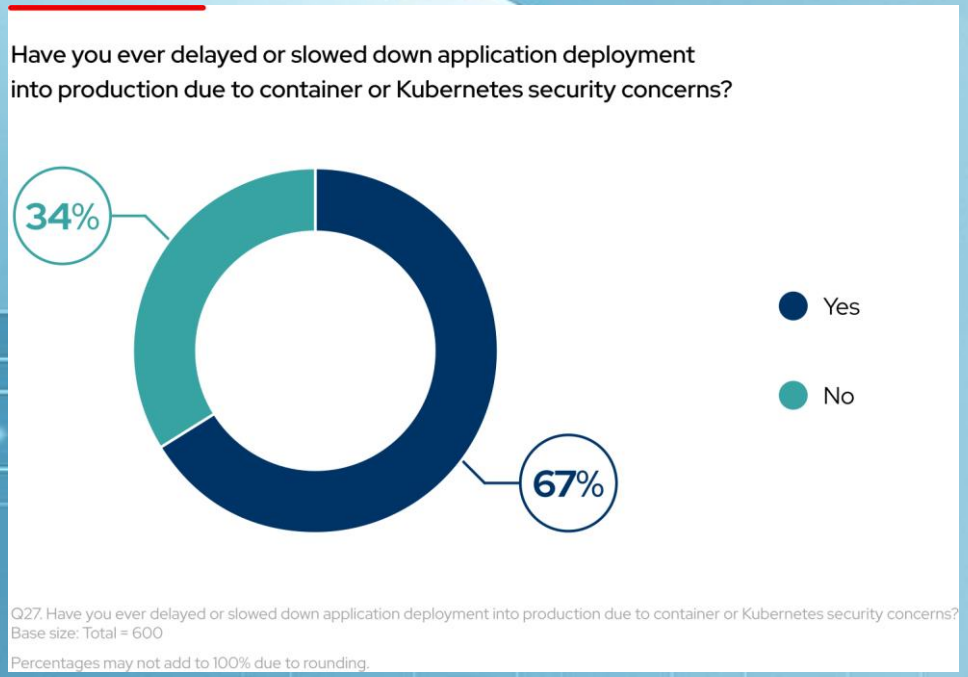
controlware

Kubernetes Security....warum sprechen wir darüber

- *Kubernetes ist extrem Beliebt*
- *Immer mehr Cloud-native Architekturen*
- *Kubernetes ist Komplex*
- *Schnelllebig*
- *Oft nicht klar wer macht was*

© 2025 Controlware GmbH

Damit sind wir nicht allein....



© 2025 Controlware GmbH

Source: Kubernetes adoption, security, and market trends report 2024 by Red Head

controlware

Warum Kubernetes Security herausfordernd ist

- Dynamische Infrastruktur
- Viele Komponenten
- Standardkonfiguration oft unsicher
- Komplexe Rechteverwaltung
- Multi-Tenancy
- Geringe Sichtbarkeit
- Tool-Wildwuchs
- Dev vs. Ops vs. Security

© 2025 Controlware GmbH

controlware

Typische Angriffsflächen & Bedrohungen

Kubernetes API-Service: ein Angriff hier kann alle Steuerungsfunktionen kompromittieren.

Multi-Tenancy: Verschiedene Teams teilen sich denselben Cluster → saubere Isolierung nötig

etcd (Key-Value Store):ungeschützter Zugriff kann zu vollständiger Kompromittierung führen.

Kubelet: Lokaler Agent auf jedem Node – Ziel für Privilege Escalation

Container Images: Unsichere oder manipulierte Images → Supply Chain Angriffe

Netzwerkkommunikation: Ohne Network Policies können Pods frei untereinander kommunizieren → Risiko von lateraler Bewegung

Unsichere Standardkonfigurationen: Z. B. Container mit Root-Rechten oder fehlender Isolation

© 2025 Controlware GmbH

controlware

Kubernetes Sicherheitsmaßnahmen

- **RBAC**

  Zugriffssteuerung für APIs & Ressourcen
- **Namespaces**

  Trennung von Workloads & Teams
- **Network Policies**

  Datenverkehr zwischen Pods kontrollieren
- **Pod Security Admission**

  Richtlinien wie kein Root-Zugriff durchsetzen
- **SecurityContext**

  Container-Hardening (z. B. keine Privilegien)
- **API Server**

  Zugriff absichern, TLS, Authentifizierung

© 2025 Controlware GmbH

controlware

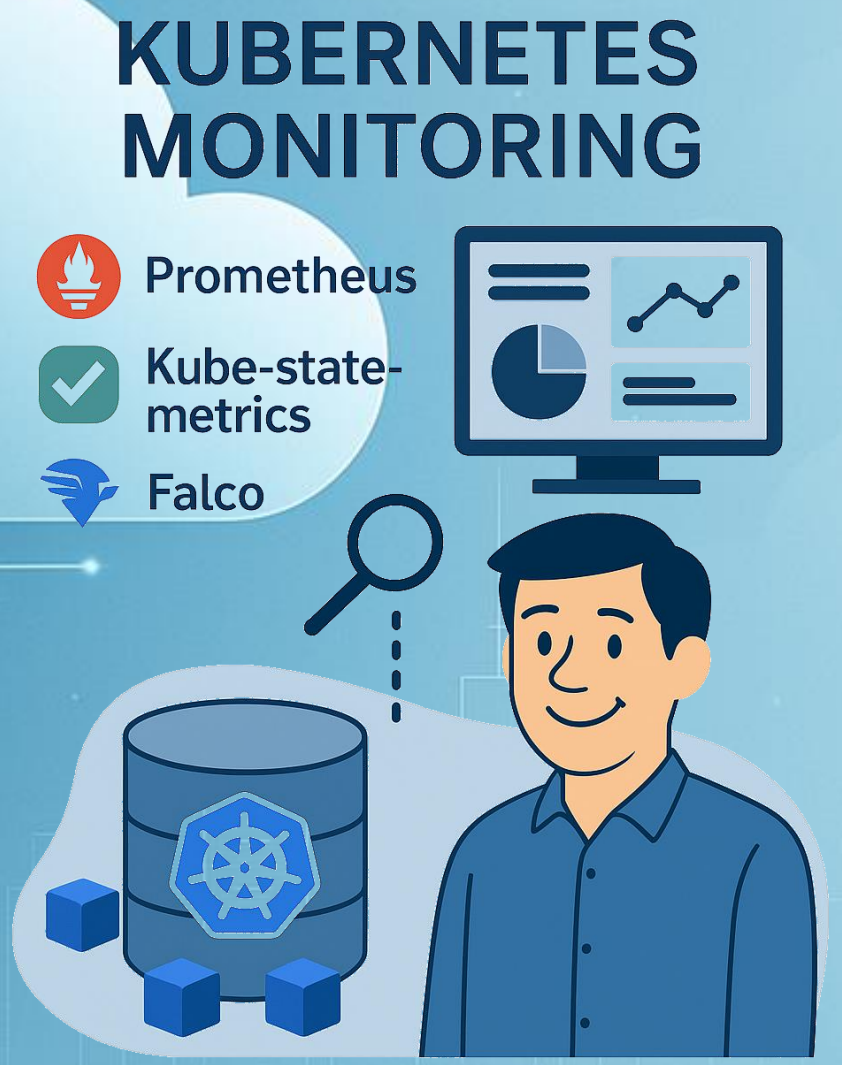
Security in der Supplychain

- *Frühe Security-Checks*
- *Image/Dependency-Scans*
- *Secrets Detection*
- *Policy Enforcement*
- *Nur geprüfte Deployments*
- *CI/CD = Prod-Code*

© 2025 Controlware GmbH

Observability, Auditing & Incident Response

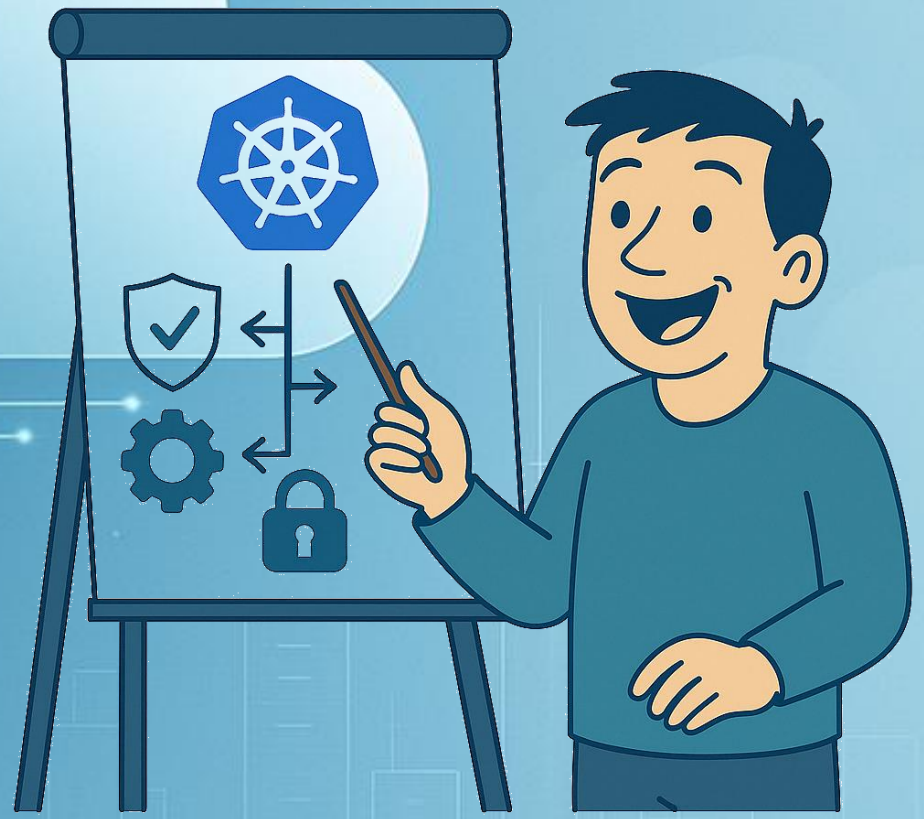
- *Kontinuierliche Überwachung des Clusterzustands*
- *Verhaltensbasierte Detektion*
- *Kontextbasierte Alarmierung*
- *Zentrale Log- & Event-Korrelation Transparente Sicht auf alle Komponenten,*
- *Monitoring als Grundlage für Incident Response-Prozesse*



© 2025 Controlware GmbH

Fazit

- *Kubernetes ist Komplex*
- *Sicherheit ganzheitlich denken*
- *Tools ≠ Sicherheit ohne klare Prozesse*
- *Shift Left spart Nachbesserungen*
- *Security ist ein Dauerprozess*
- *Regelmäßige Prüfungen & Updates*
- *Container-Nutzung stets hinterfragen*



© 2025 Controlware GmbH

Unser Angebot

Der Kubernetes Checkup

- Komplette Sichtung der Cluster
- Checkliste + Bewertung
- Empfehlungen + Best Practices

Weitere Betreuung

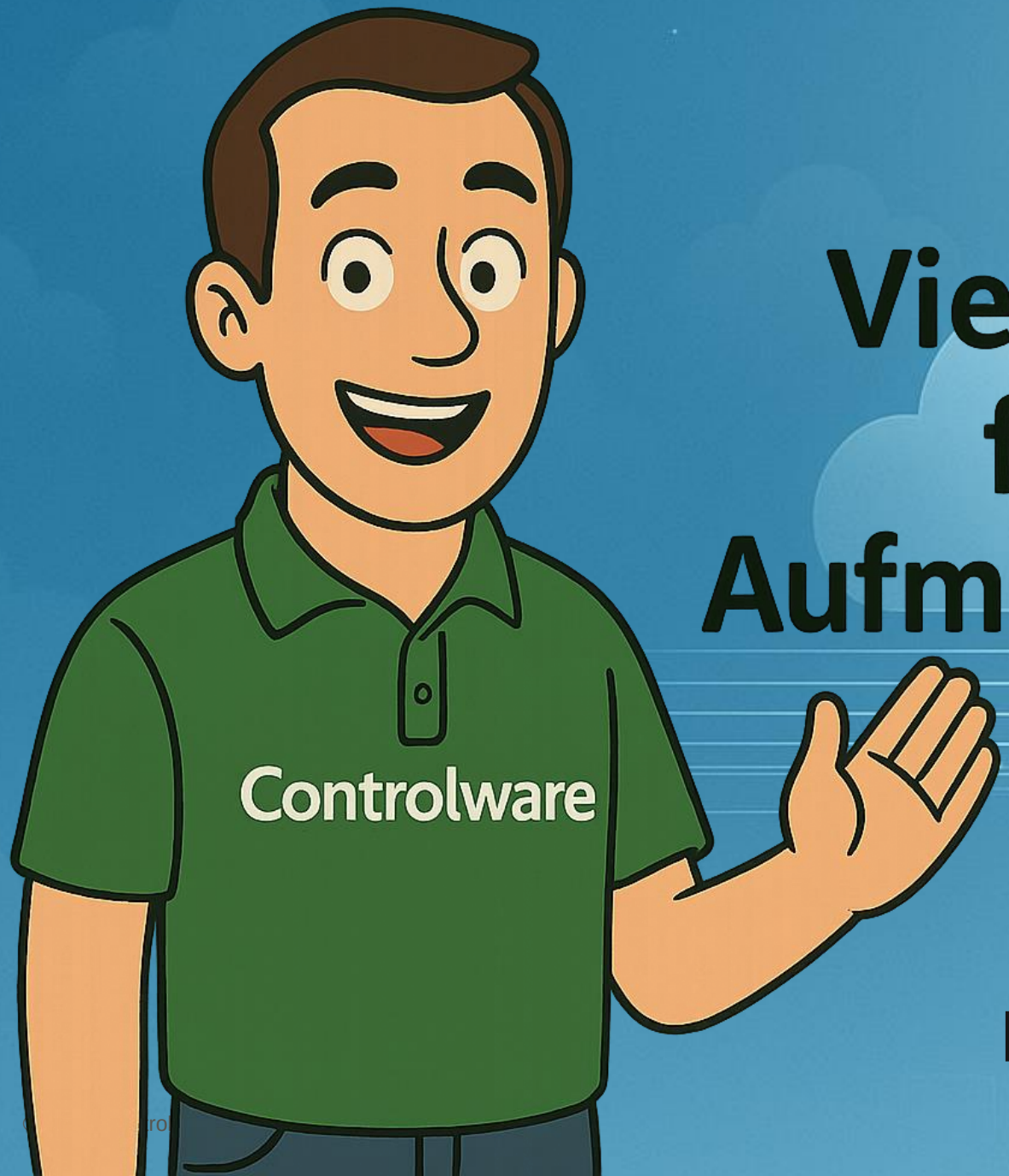
- Planung und Aufbau
- Aufbau der Security
- Komplette Betreuung
- Umbau von Clusterinfrastruktur
- Monitoring Alerting
- Backup & Recovery
- Manage Service

© 2025 Controlware GmbH

controlware

FAQ

© 2025 Controlware GmbH



Vielen Dank für Ihre Aufmerksamkeit!

Kontaktdaten:
Fabian.Hart@controlware.de
Mark.Hoehl@controlware.de