Sicherer Informationsverbund

Skalierbare und sichere Netzwerkplattform zur Verbindung der Behörden mit Cloud Service Anbietern

2025 Reimagine GERMANY

Markus Pfaff mpfaff@cisco.com
CTO Cisco Public Sector Federal Germany
23. Mai 2023

Deutsche Verwaltungscloud


Souveränität
HL
HL

Anhängigkeiten aller Beteiligter

Problemstellung

- Digitalisierung der öffentlichen Verwaltung
- Cloud Technologie für Dienstleistungen des Staates
- Keine Betrachtung des Netzwerks
- Richtlinien IT Sicherheit passen nicht mehr
- Infrastruktur- und Security- Fähigkeiten sind komplex
- Anwendungsentwickler bestimmen den Security-by-Design Ansatz

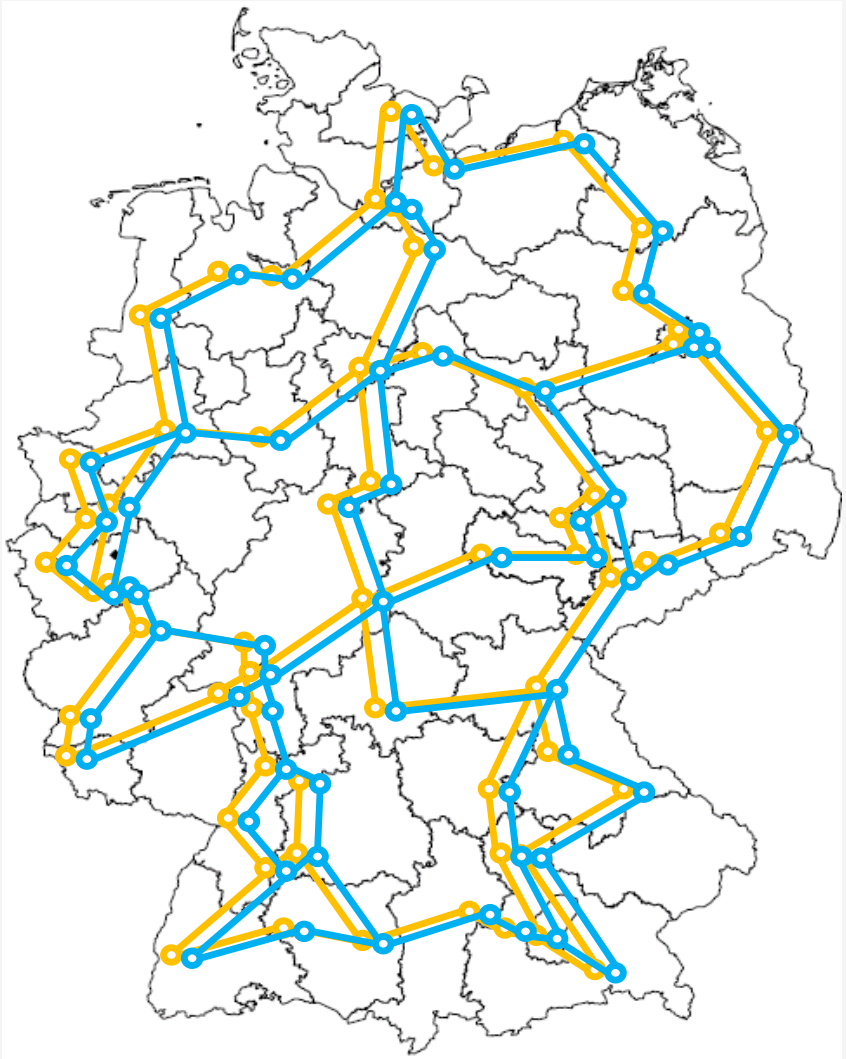
4 Insights

- Robuste Netzwerke mit Infrastruktur als Code (IaC)
- Security Plattform
- DevOps Modell um diese Fähigkeiten zu nutzen
- Managen von Veränderungen

Robustes Netzwerk und Infrastruktur als Code
IaC

Robuste Netzwerk Topologie

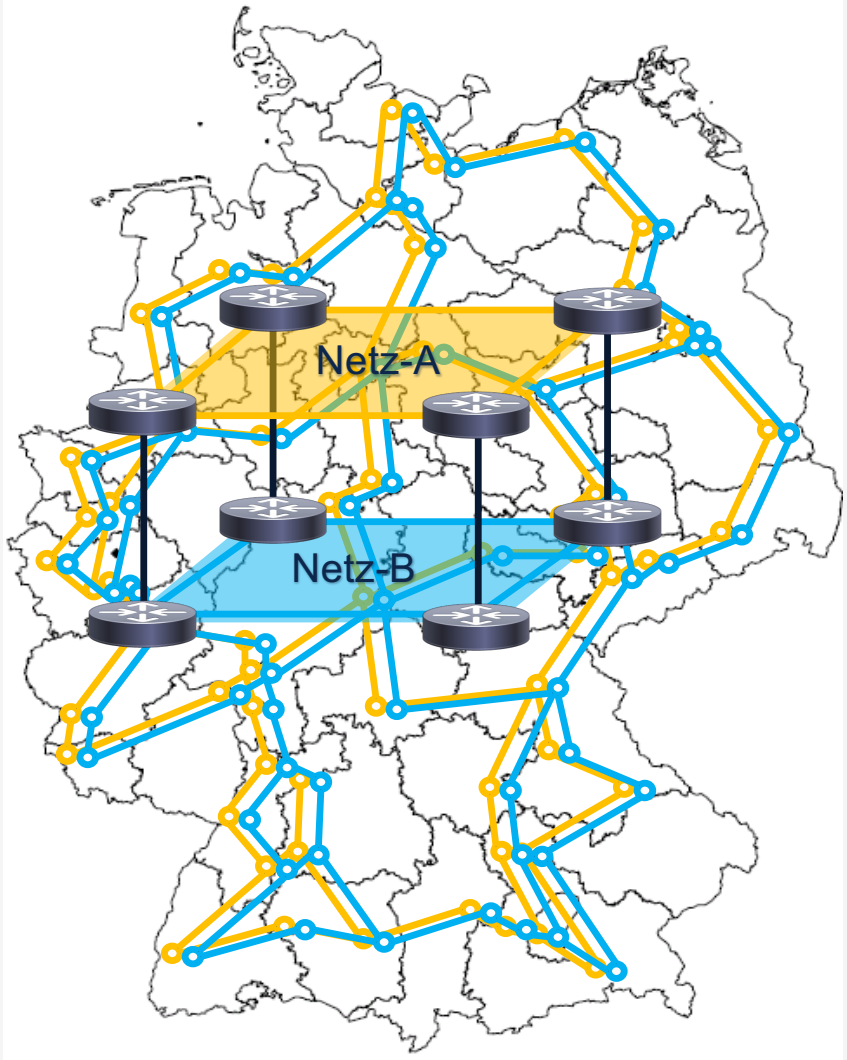
Netz-A
Netz-B



Glasfaser Infrastruktur

- Dual-Plane Design
- Separate Glasfaser Infrastruktur pro Plane
- Vermeiden eines Shared-Risk-Path
- Physikalische Sicherung der Standorte

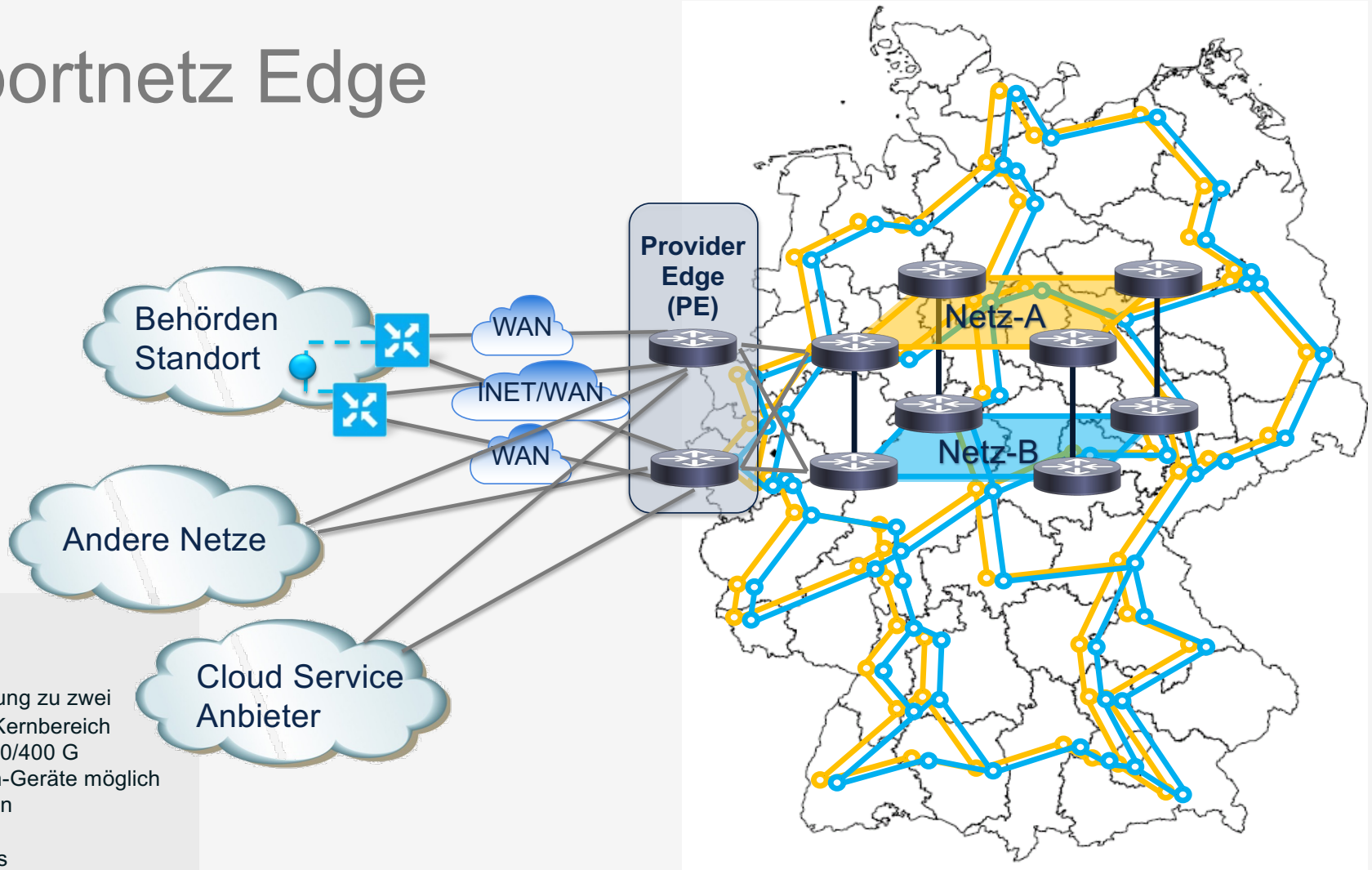
IP Transportnetz Core



Provider Router (P)

- Dual-Plane Design
- Hochverfügbare Service Provider Geräte
- Segment Routing Protokoll
- Link-Geschwindigkeiten: 100G / 400G
- Integration der optischen Netze (Routed Optical Network, RON)
- Einfache Queuing-Fähigkeiten und kleine Routing- und Forwarding-Tabellen

IP Transportnetz Edge



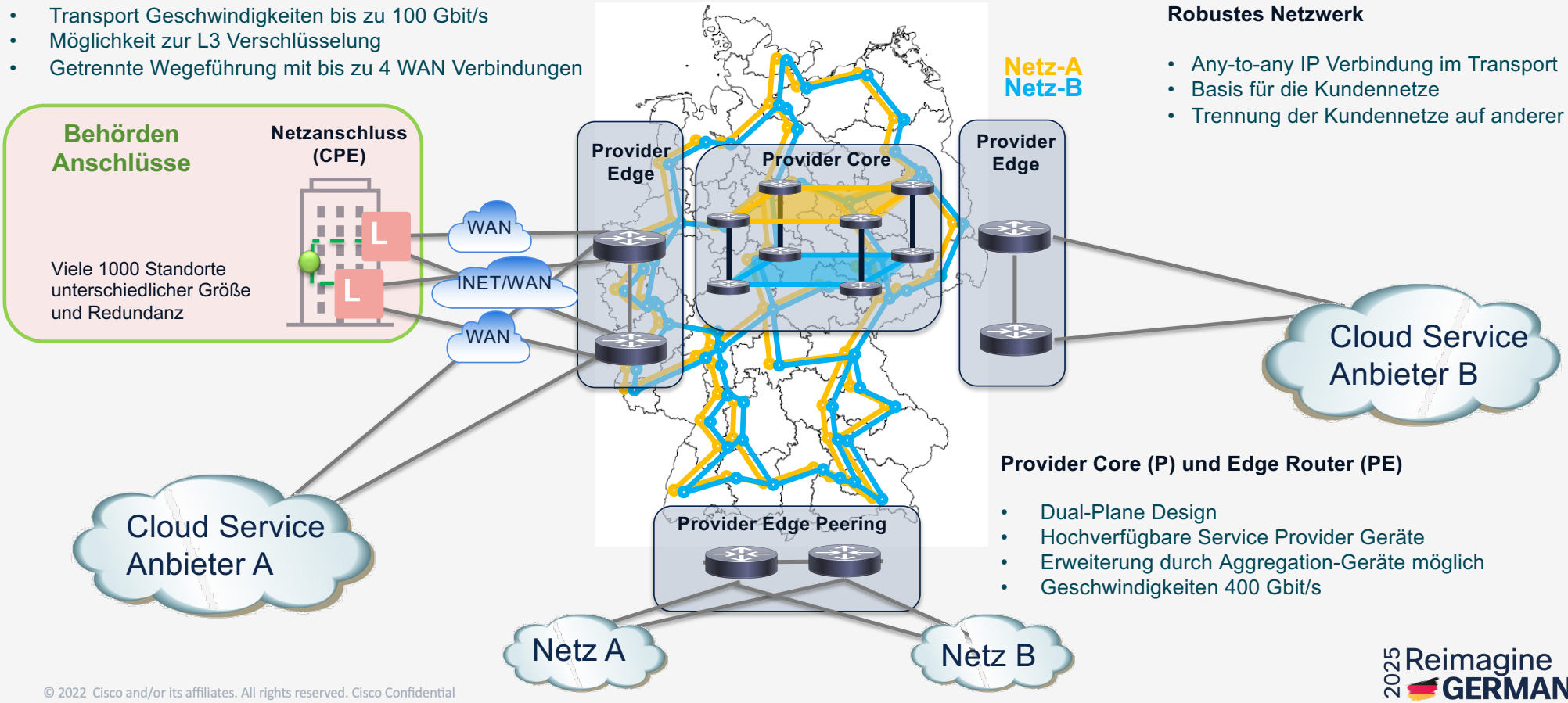
Provider Edge Router (PE)

- Hochverfügbare Geräte
- Diverse / Redundante Verbindung zu zwei unterschiedlichen Routern im Kernbereich
- Link-Geschwindigkeiten: 40/100/400 G
- Erweiterung durch Aggregation-Geräte möglich
- Erweiterte QoS-Funktionalitäten
- Größere Routing-Tabellen
- Durchsetzung von Nutzer SLAs

Zusammenfassung IP Transportnetz

Customer Premises Equipment (CPE)

- Transport Geschwindigkeiten bis zu 100 Gbit/s
- Möglichkeit zur L3 Verschlüsselung
- Getrennte Wegeführung mit bis zu 4 WAN Verbindungen



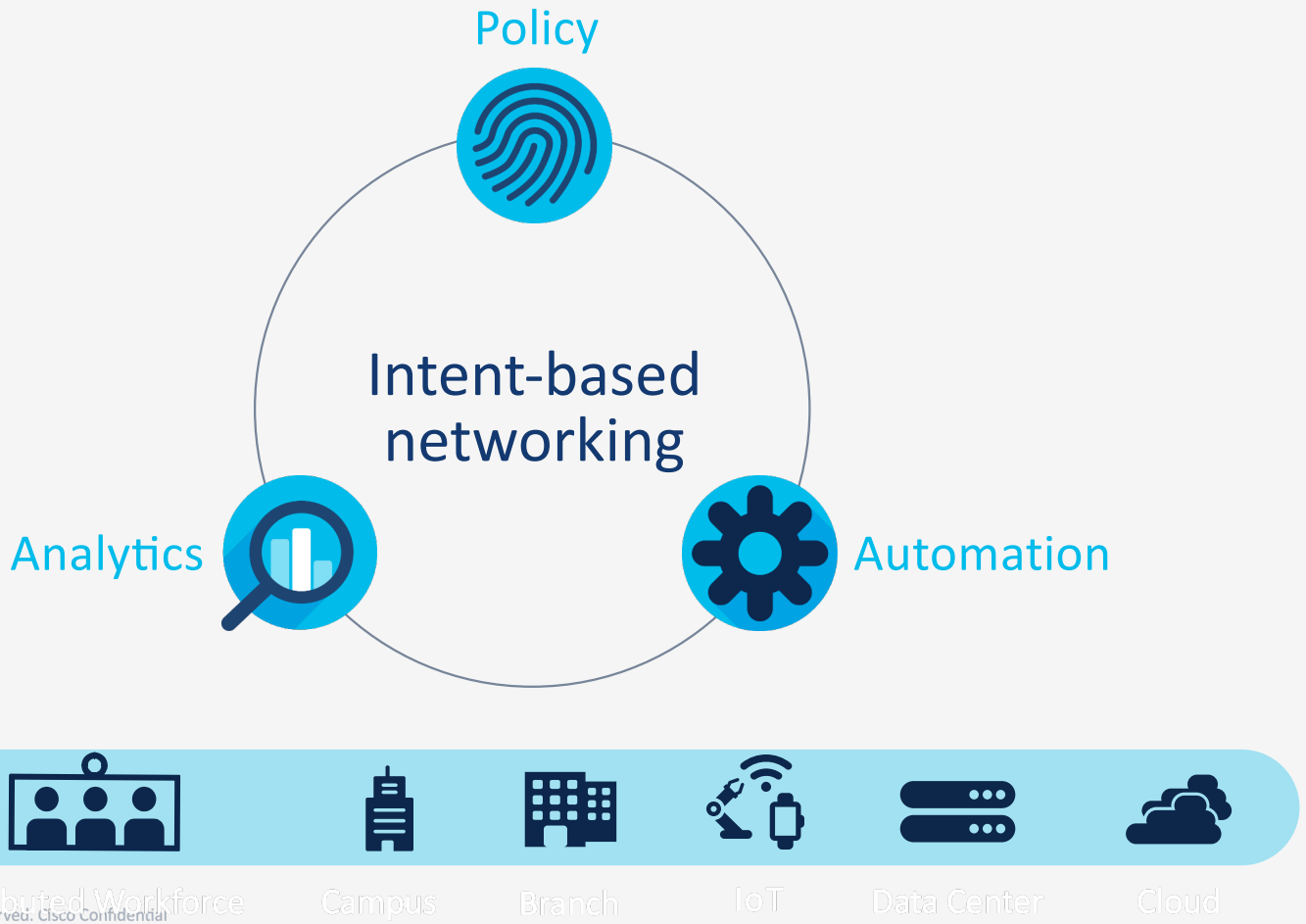
Robustes Netzwerk

- Any-to-any IP Verbindung im Transport
- Basis für die Kundennetze
- Trennung der Kundennetze auf anderer Ebene

Provider Core (P) und Edge Router (PE)

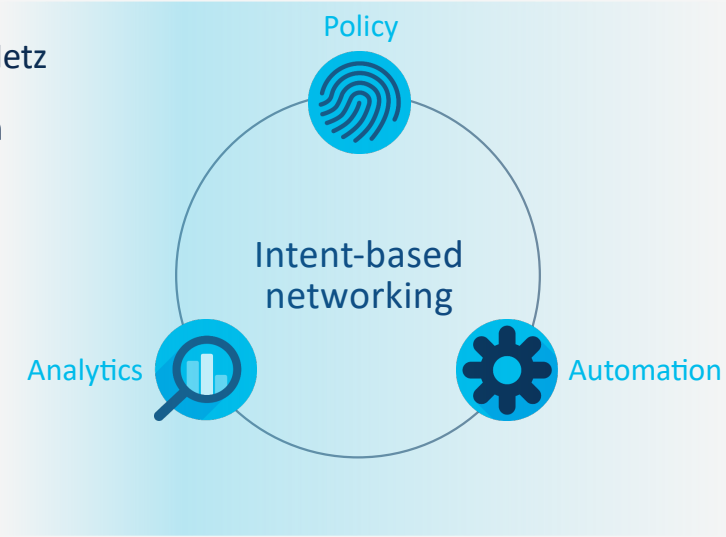
- Dual-Plane Design
- Hochverfügbare Service Provider Geräte
- Erweiterung durch Aggregation-Geräte möglich
- Geschwindigkeiten 400 Gbit/s

Software Definiertes Netzwerk



Software Definiertes Netzwerk

- Kommunikationsabsicht im Netz
- Automatisiertes Bereitstellen
- Kontinuierliches Beobachten
- Kontinuierliches Optimieren



- Trennung von Data und Control Plane
- Kontroller-basierte Control Plane
- Weiterentwicklung Segment Routing SRv6
- Virtualisierung der Netzwerk Funktionen

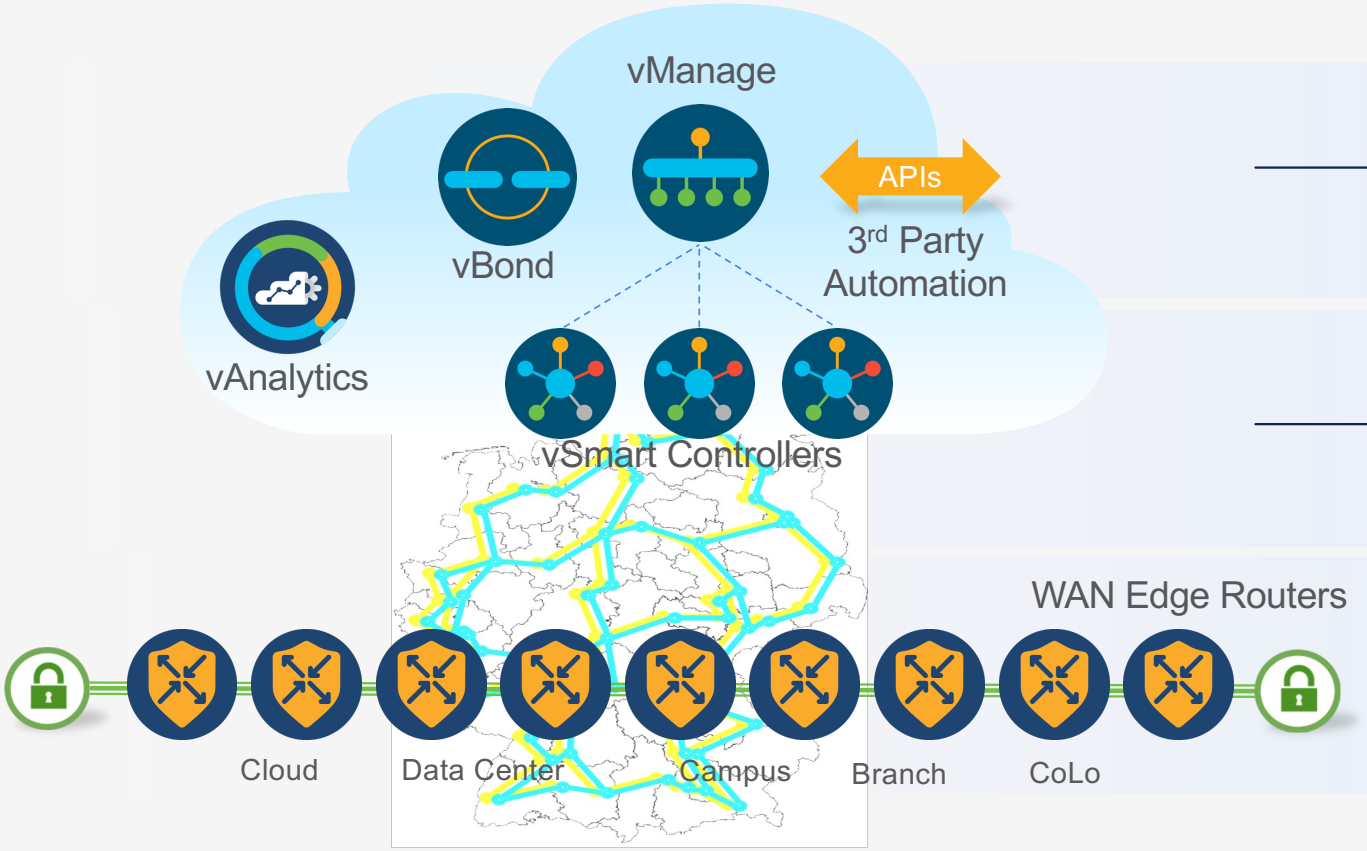
- Zentrales Management aller Netz Funktionen
- Dynamische Veränderung des Netzwerk Verhaltens
- Hohe Visibilität des Netzverkehrs
- Flow-basierte Überprüfung und Zuordnung des Netzverkehrs

- Bereitstellung aller Funktionen über API des Kontrollers
- Virtuelle Netzwerke
- Integration von Security Funktionen

Cisco SD-WAN Solution Overview

MEF 3.0 SD WAN konform

Anwenden der SDN Prinzipien auf das Wide Area Network



Management und Orchestration Plane

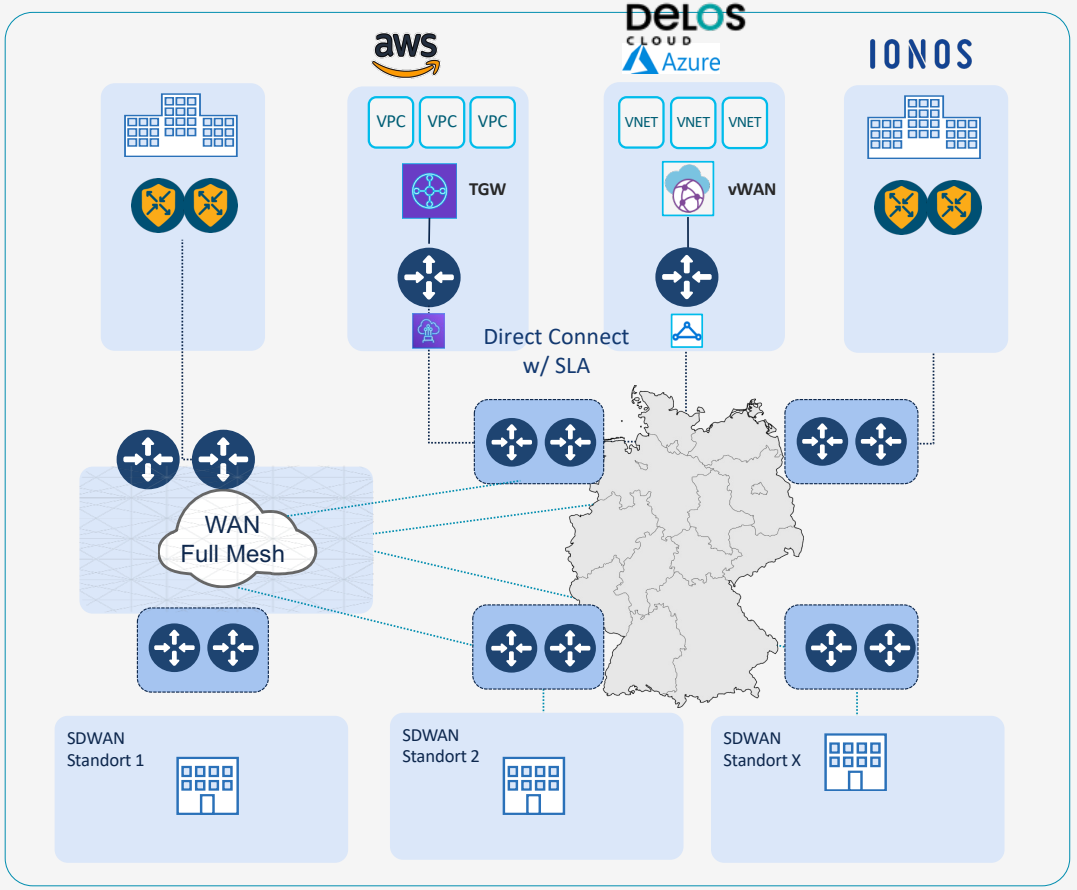
SD WAN Control Plane

Data Plane

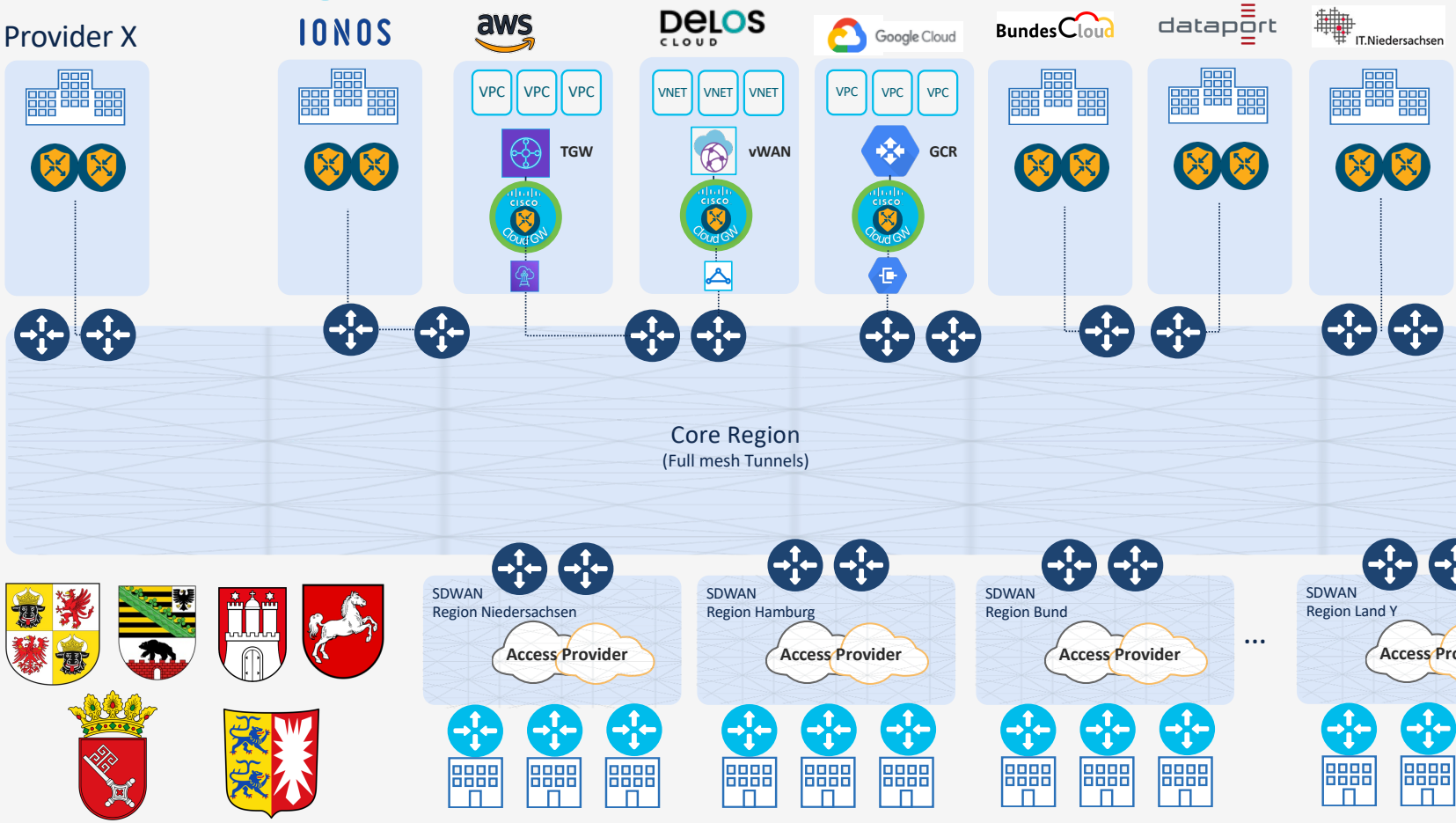
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html

SD WAN Sichtweise für eine Behörde

- SD-WAN Region
- Eine Netzwerk Policy
- Zentrales Management
- Anschluss aller Standorte
- Virtuelles Full Mesh
- SD WAN Edge in die Cloud Provider
- Sicherer Zugriff auf Public Clouds über Netze der ÖV
- 7500 CPE und 150 Tenants
- Maximal bis zu 10.000 CPE



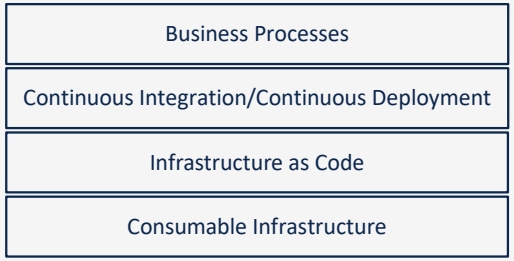
Multi-Region SD WAN Fabric

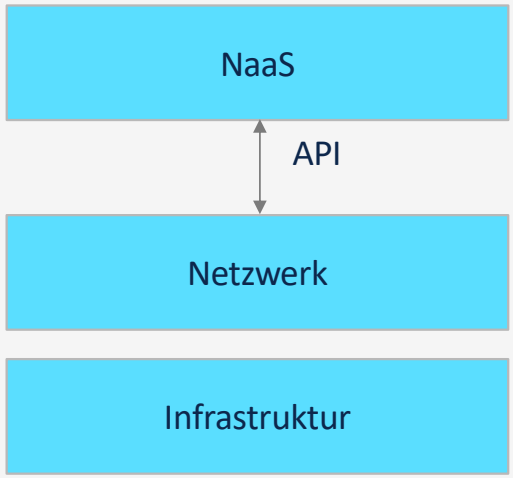


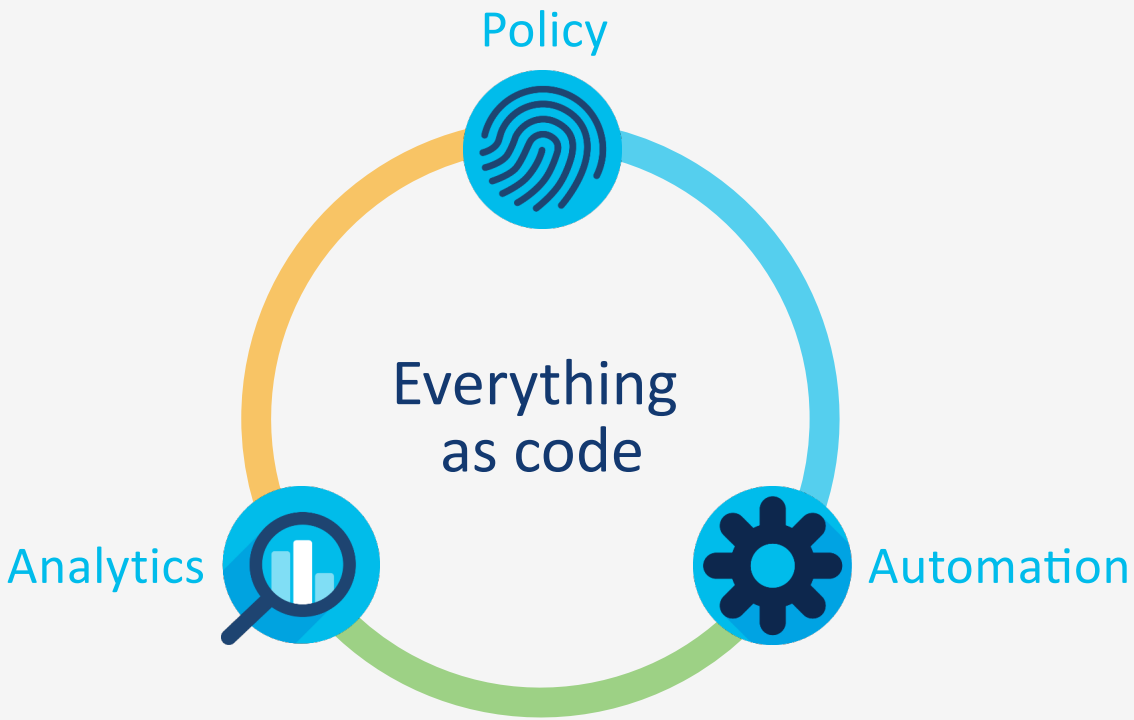
- Reduzierte Komplexität
- Trennung von Regionen / Kunden
- Trennung Inter Region Traffic
- Anschluss von zentralen Cloud Services

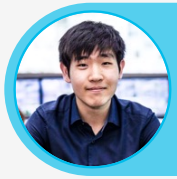
Everything-as-Code

- Umsetzung einer Plattform
- Automatisierungsgrundlage
- Alle Funktionen als API darstellen
- API ansprechbar aus Prozess Automatisierung
- Definierte Service Parameter
- Variablen werden verlangt
- Datenmodell basierend
- Verwendung von Single-Source-of-Truth
- Ermöglicht Verkettung von Services
- Kommunikation zwischen Beteiligten am Code (Daten und Fakten)
- Service (Konfiguration) maschinenlesbar und überprüfbar








DevOps

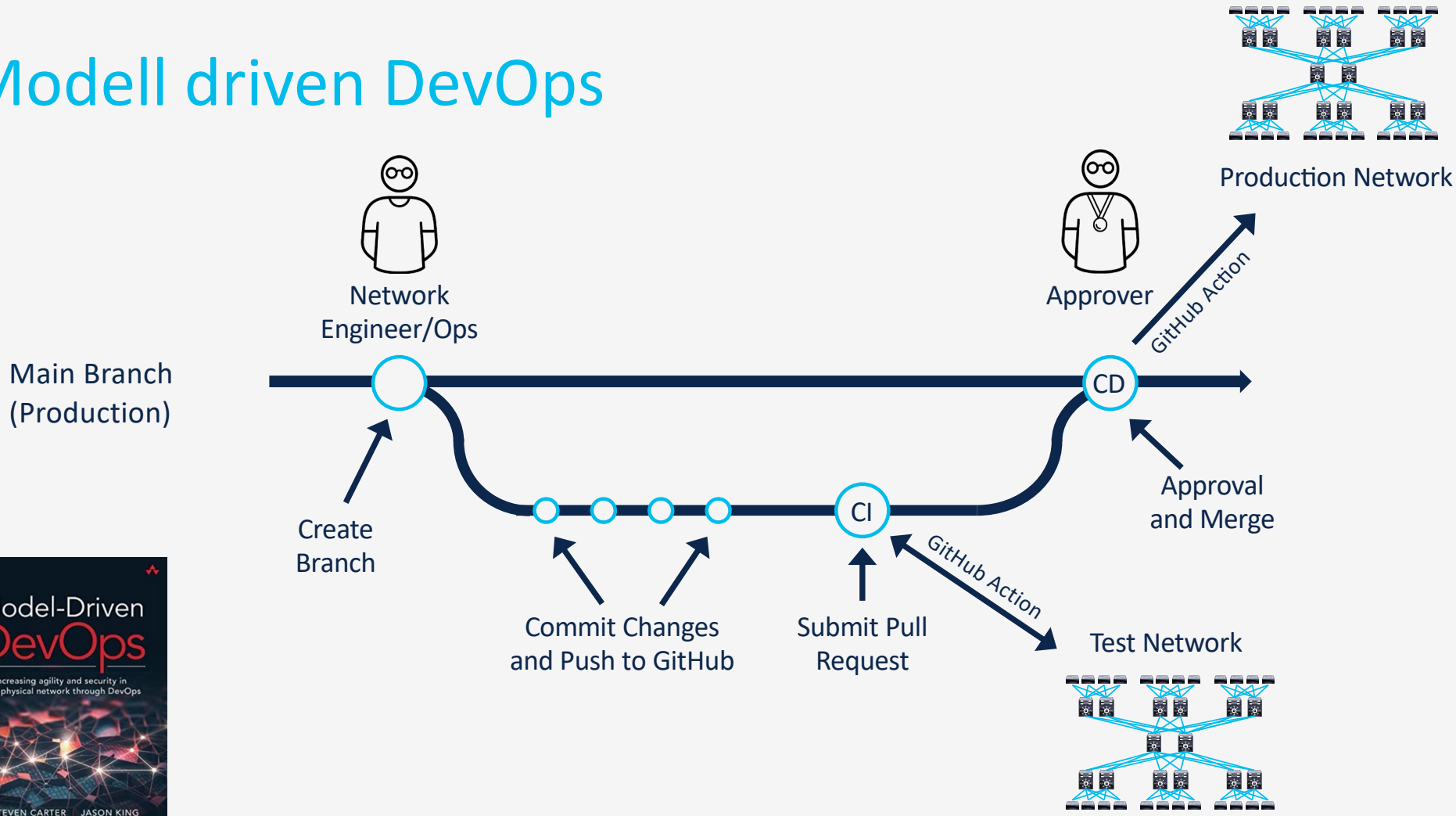

SecOps


App developers


NetOps

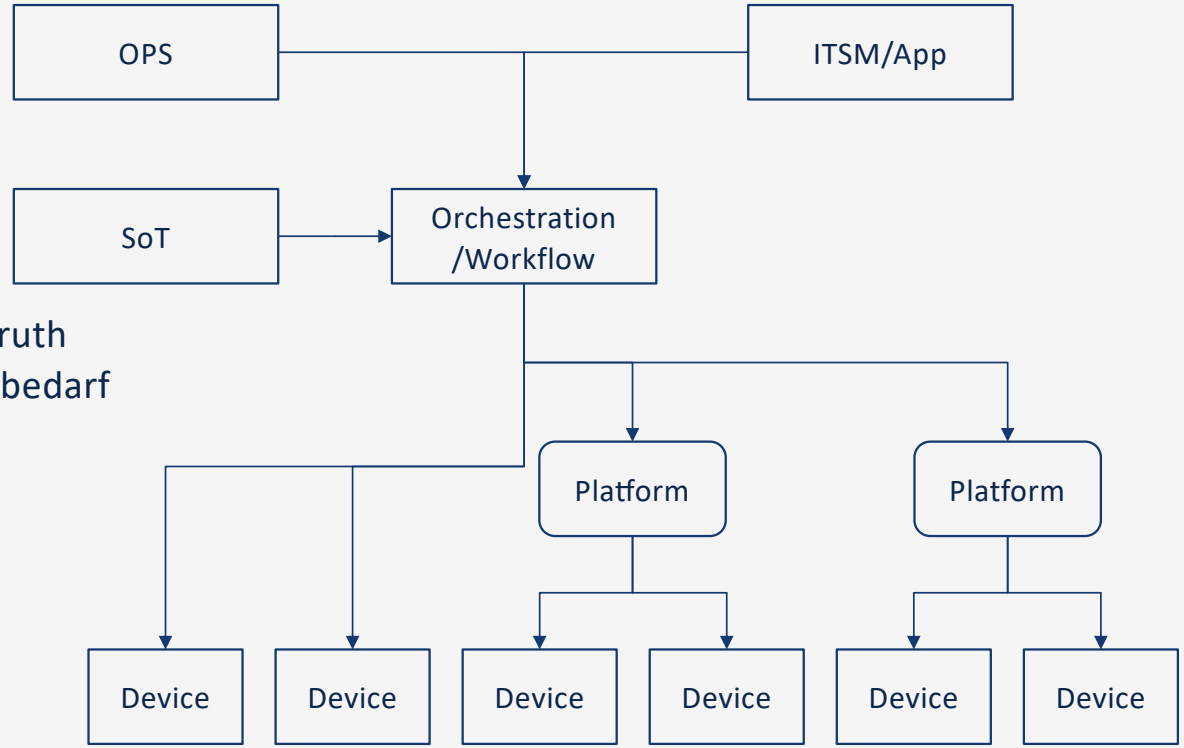

CloudOps

Modell driven DevOps



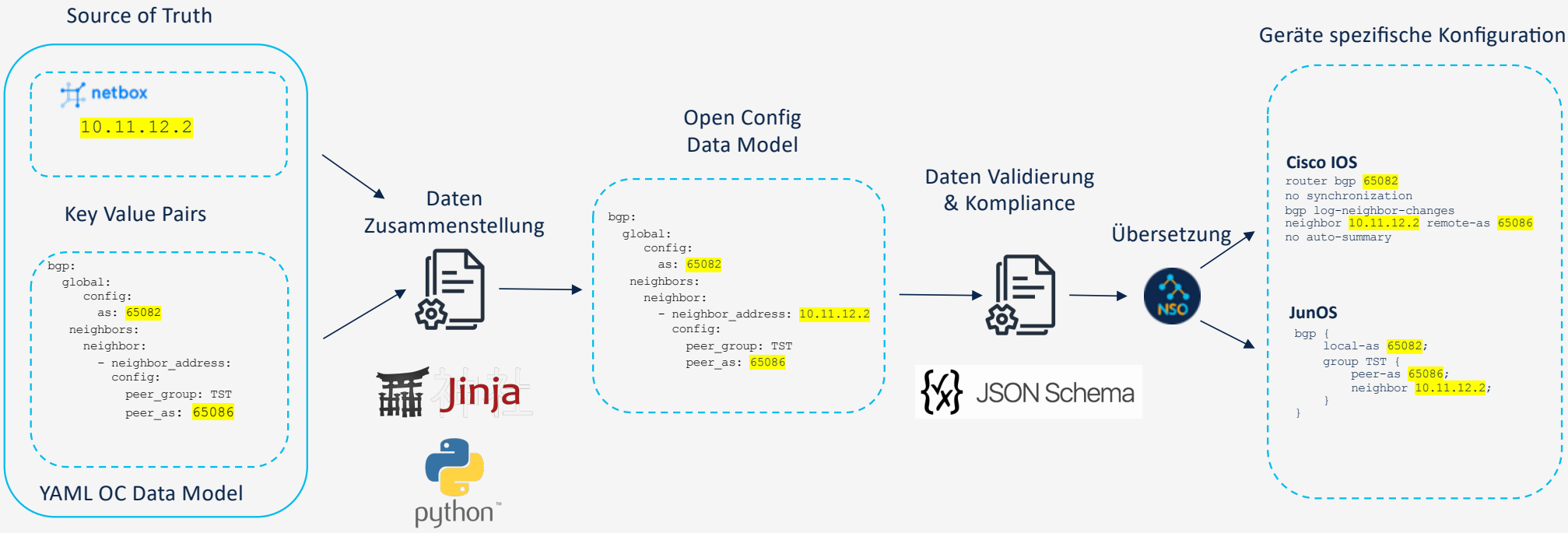
https://www.amazon.com/Model-driven-Devops-Increasing-Security-Physical/dp/0137644671

Modell-Driven DevOps Framework



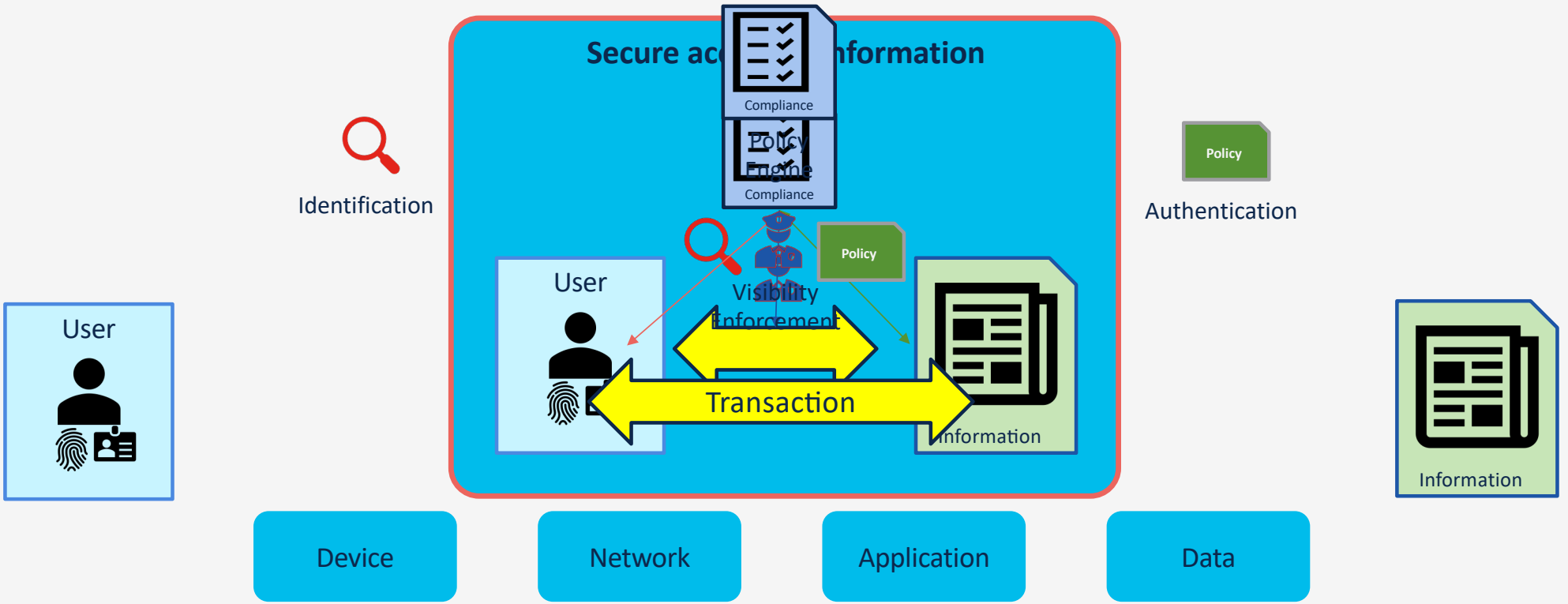
Single Source of Truth
Hoher Sicherheitsbedarf

Implementierung Überblick

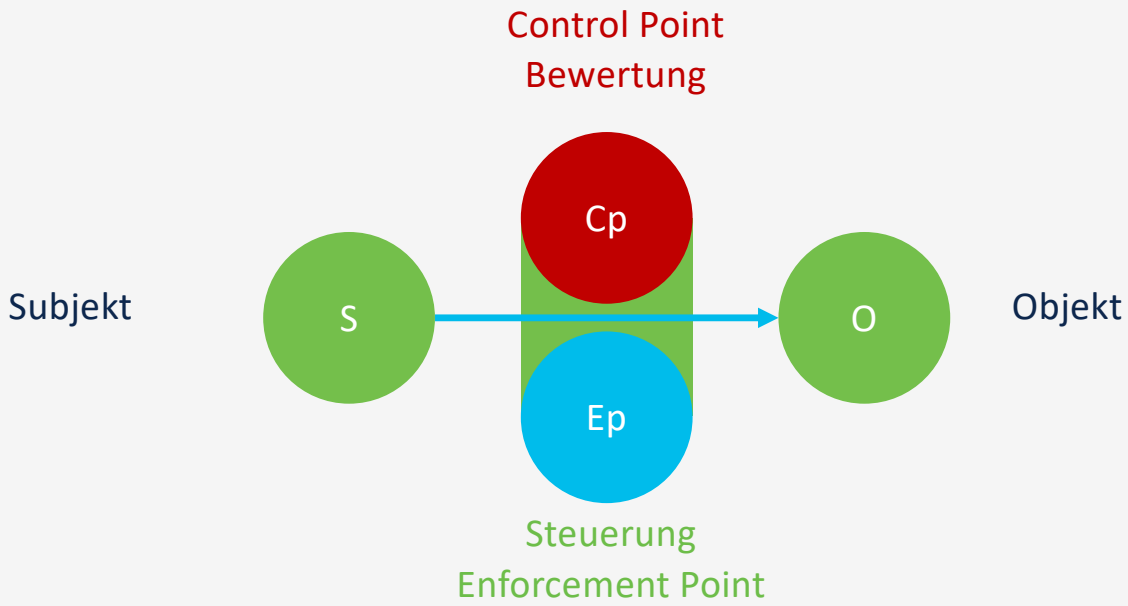


Security Plattform

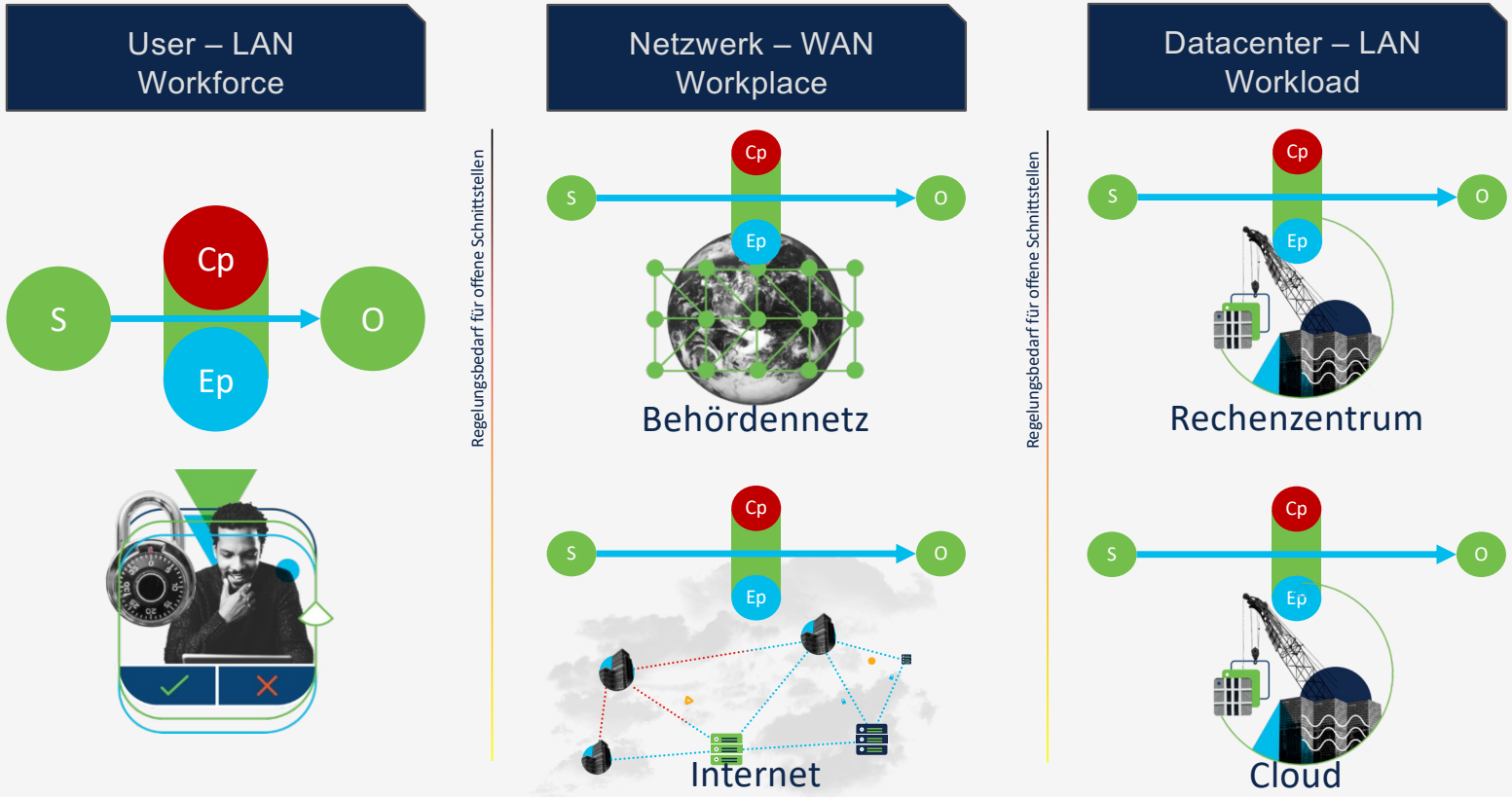
Notwendigkeit einer multi-domain Architektur



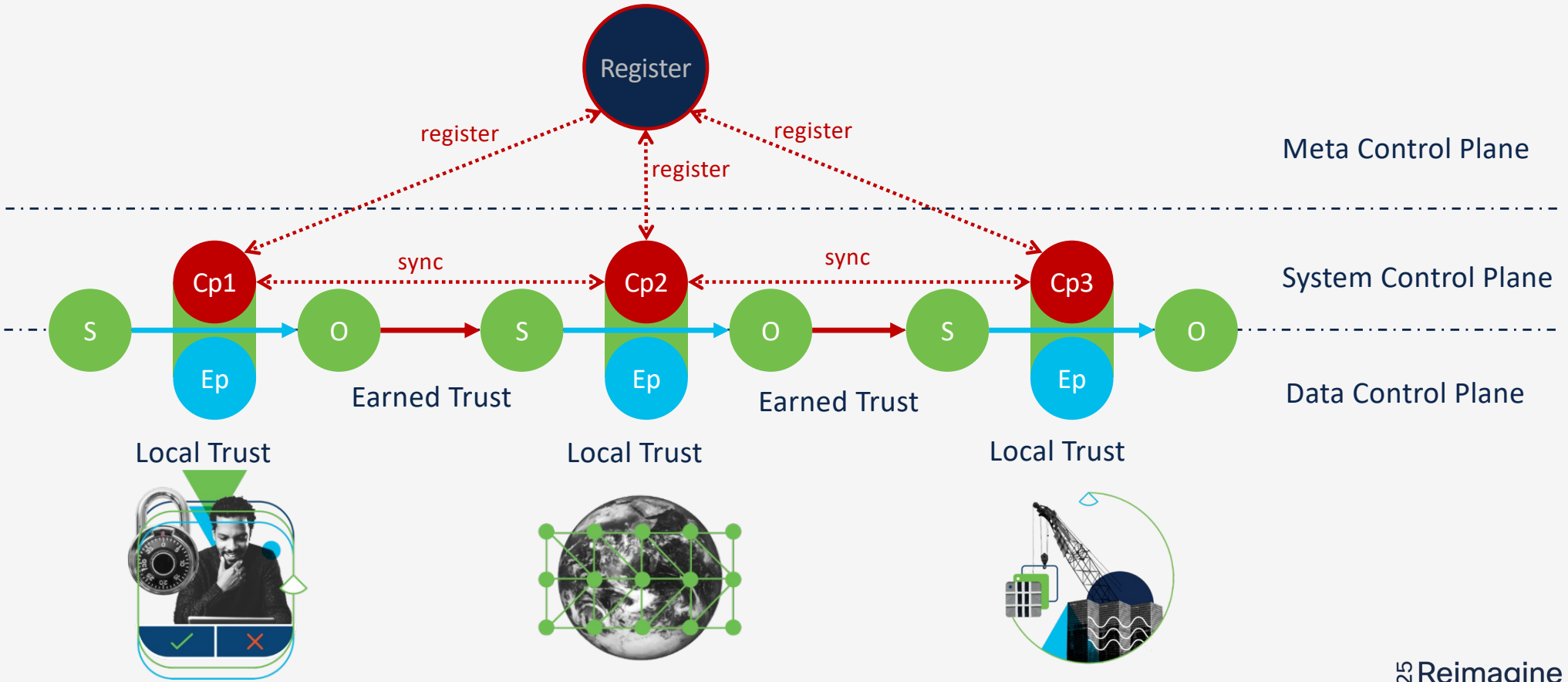
Zero Trust Logisches Modell der Least Privileg Steuerung



Föderale Verwaltung



Zero Trust: Föderale Verwaltung



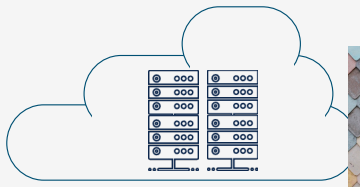
Multi-Fabric Security Plattform

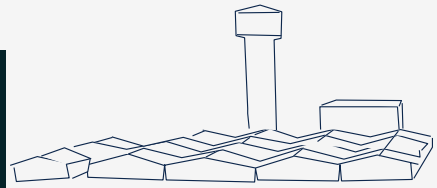
Presentation	Service	Anwendungen
Operation	Compute	Blade, Embedded, SW-Container
Information	Data	Distributed Filesystem
Communication	Network	MANET, LAN, SD-WAN
Security	Security	SASE, Zero Trust, XDR

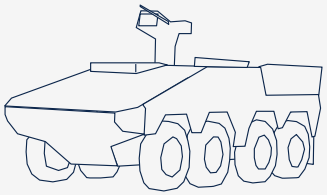
Joint Situational Awareness

Joint Logistic Support

Andere Ideen



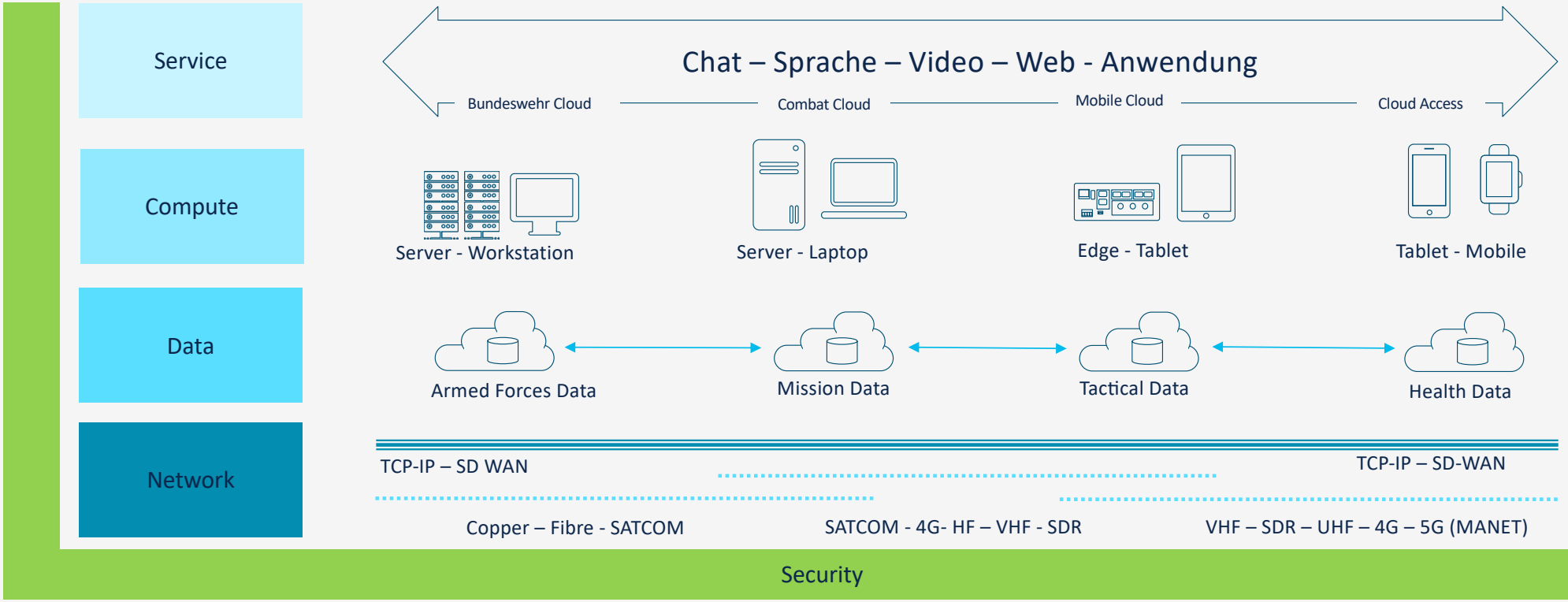




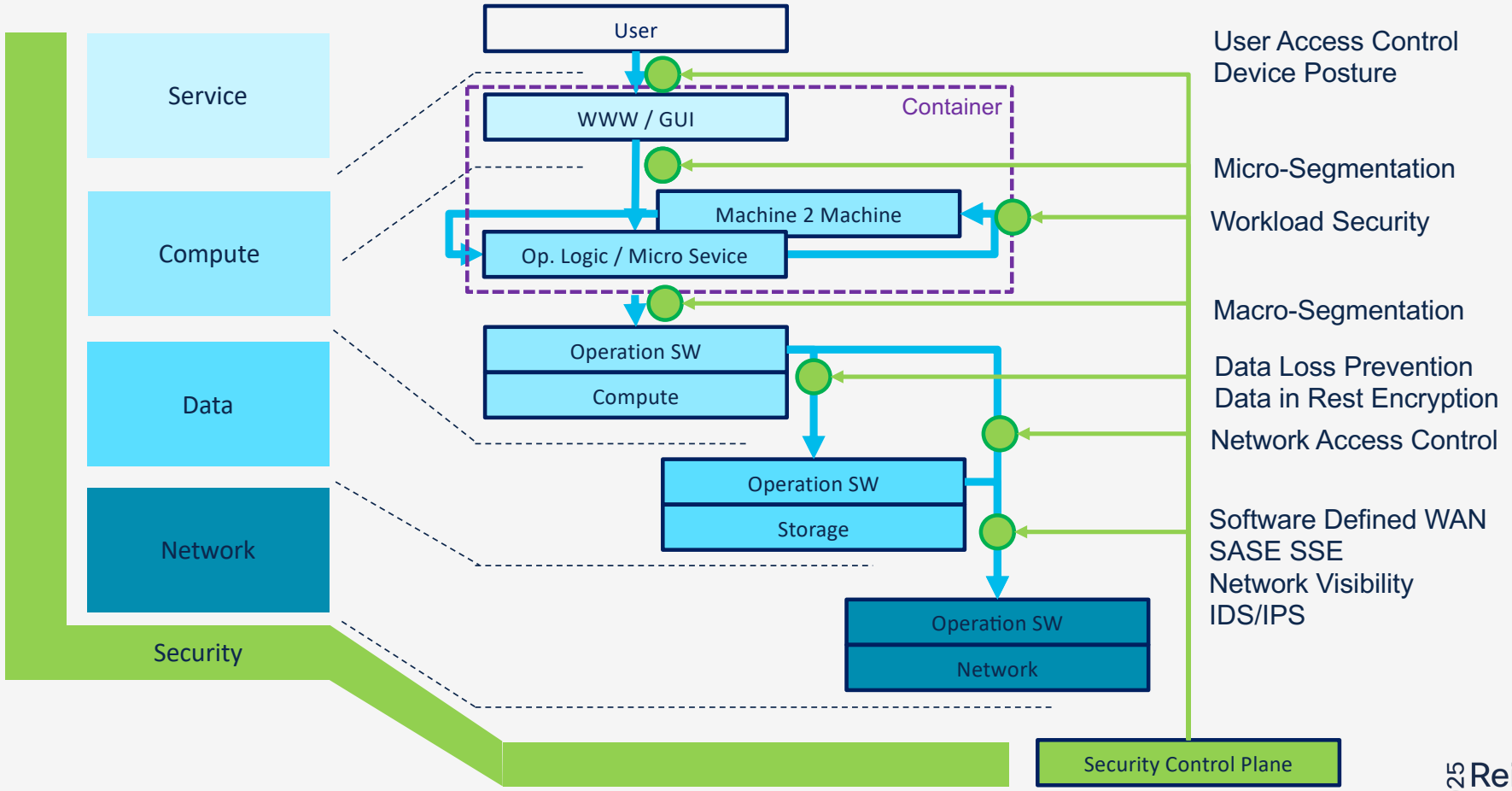
Ideenpapier BITKOM: IT-Sicherheit in einer Multi-Fabric Service- Architektur
Verteilung auf Anfrage

2025 Reimagine GERMANY

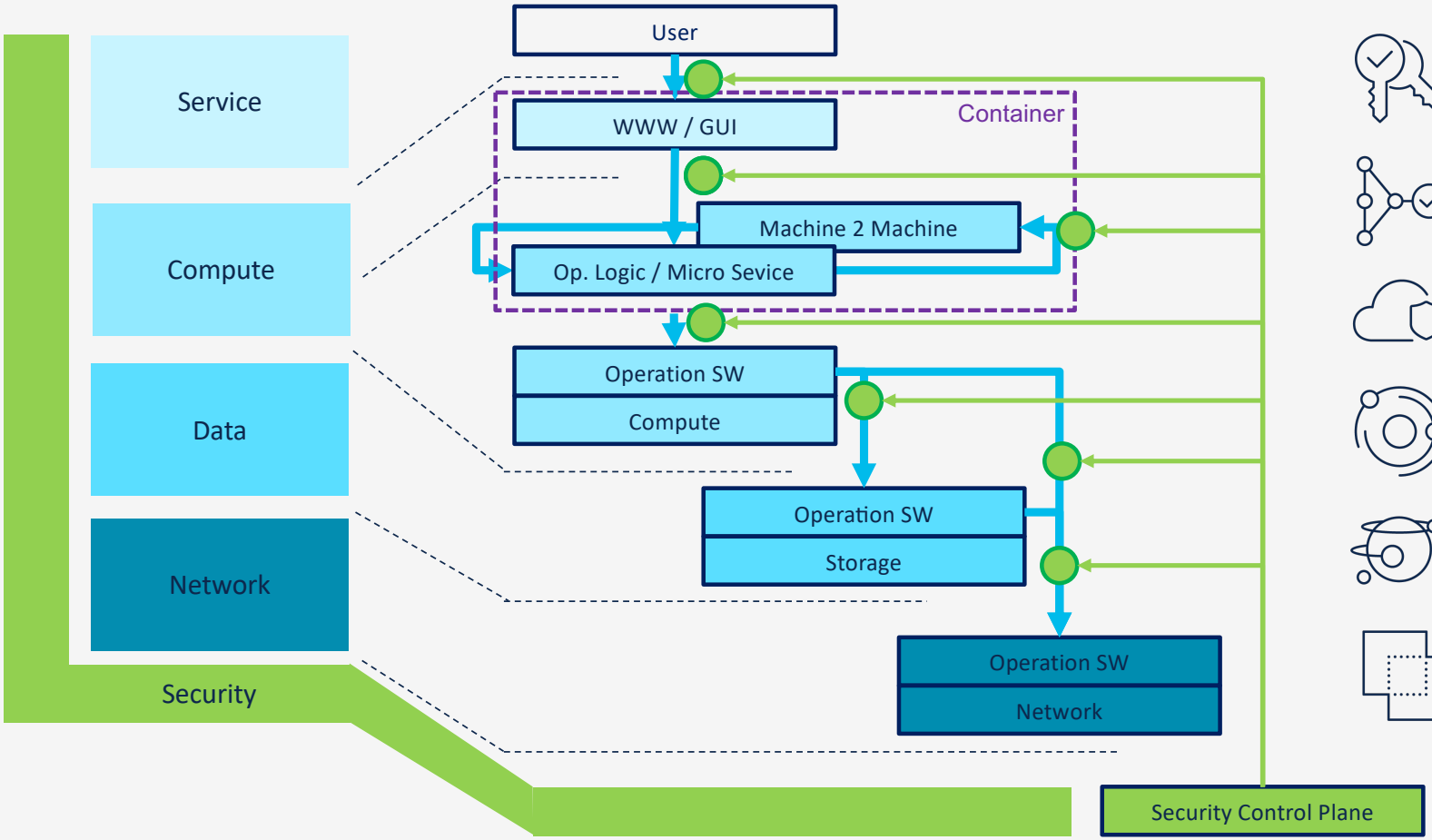
Gesamtbild Security Plattform



Security Plattform



Cisco Lösungen für die Security Plattform

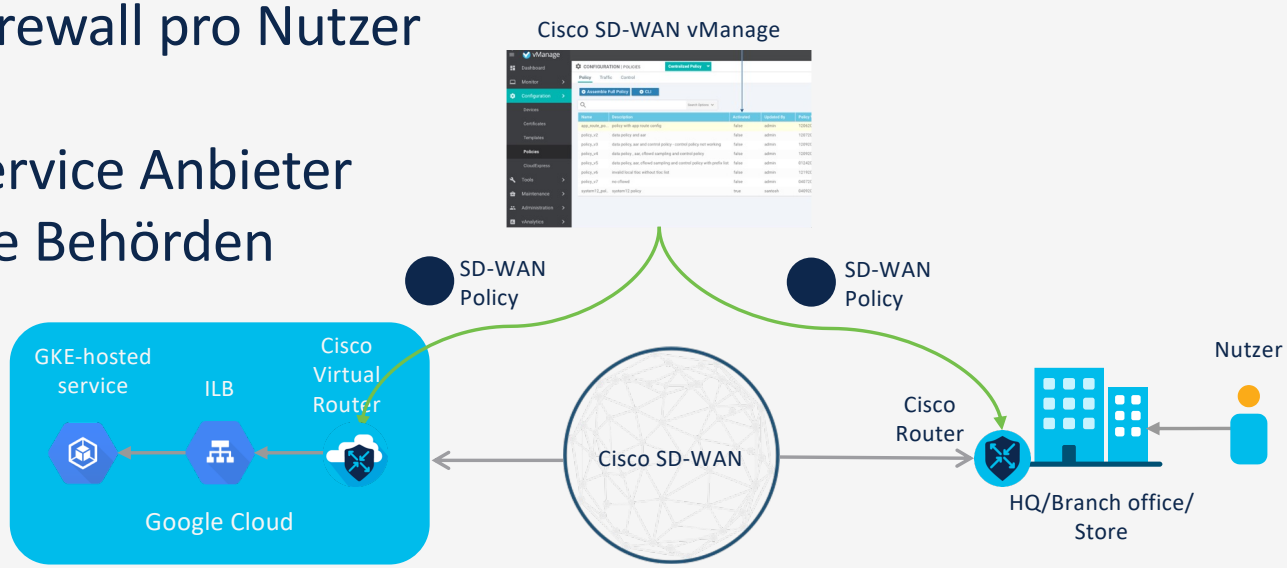


- Secure Access
- Secure Endpoint
- Umbrella
- Secure Workload
- Secure Network Analytics
- Secure Firewall

https://www.cisco.com/c/en_ae/products/security/portfolio.html

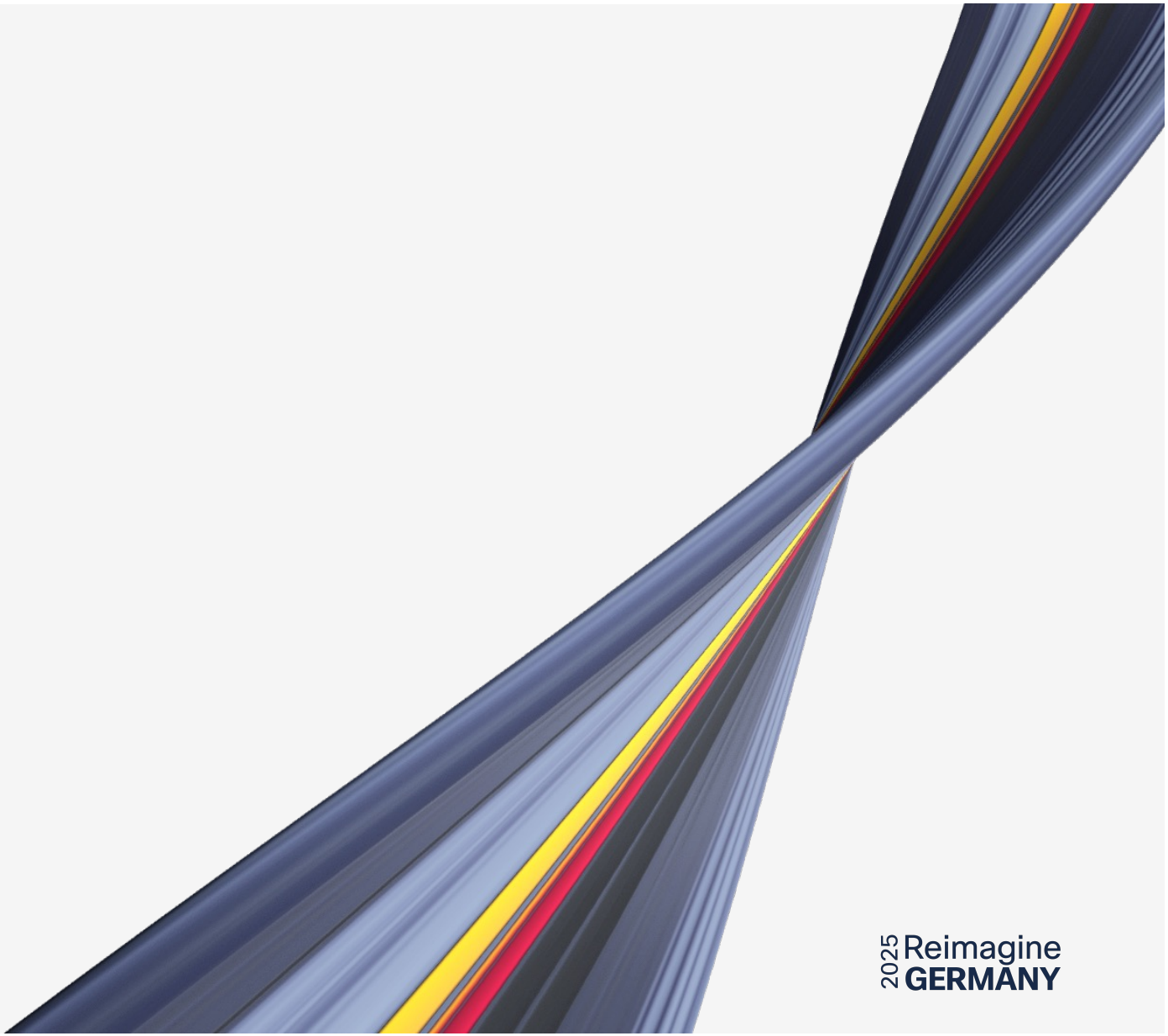
Security Komponenten Cisco SD-WAN Umsetzung

- Hohe Visibilität der Datenströme
- Zertifikat basiertes CPE Roll-Out
- IPSec Encryption
- Policy based routing
- Dynamische 5-tuple Firewall pro Nutzer
- IDS / IPS
- Integration in Cloud Service Anbieter
- Skalierbar für tausende Behörden



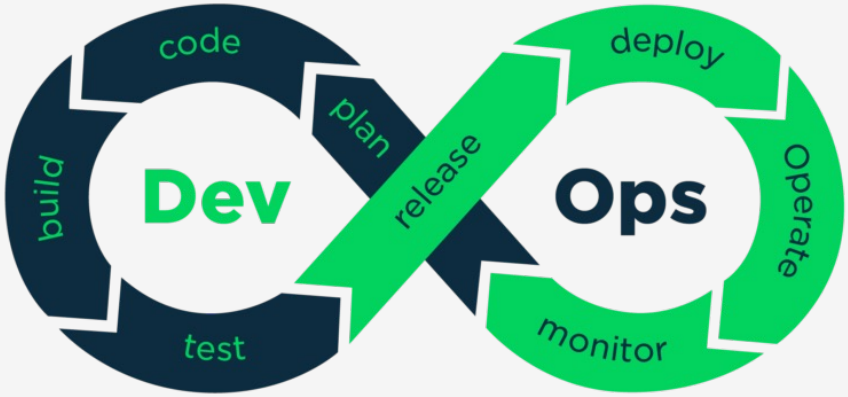
https://www.cisco.com/c/de_de/solutions/enterprise-networks/sd-wan/sd-wan-security.html

DevOps

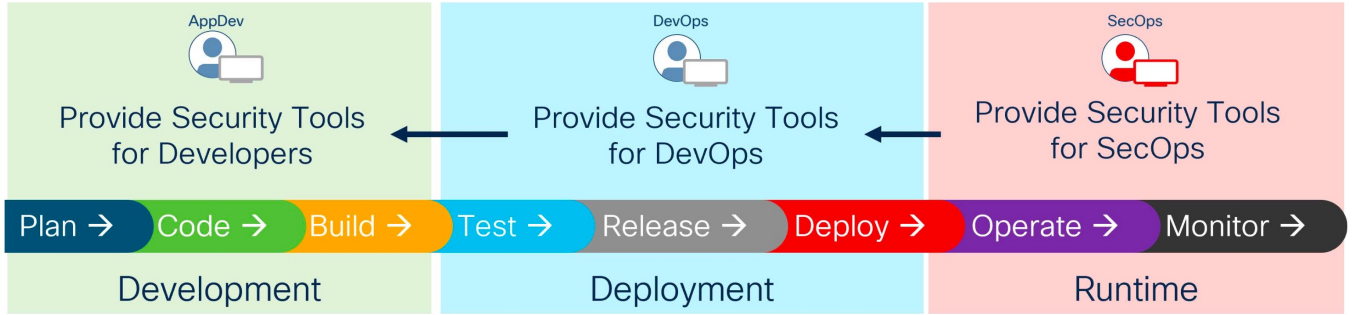


Sichere CI / CD Pipeline

- Security by Design
- Move Security to the left
- Integriertes Security Assessment
- Automatisierte Policy Durchsetzung im Code
- Entwickler nutzen Security Komponenten
- Credentials Management
- Software Komponenten Überwachung
- Cloud Native Security Komponenten
- API Monitoring und Spezifikationsanalyse
- Konformitätsprüfungen vor dem Deployment



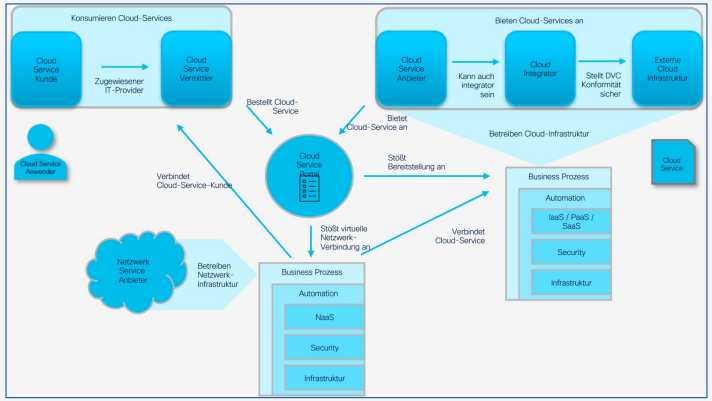
Panoptica

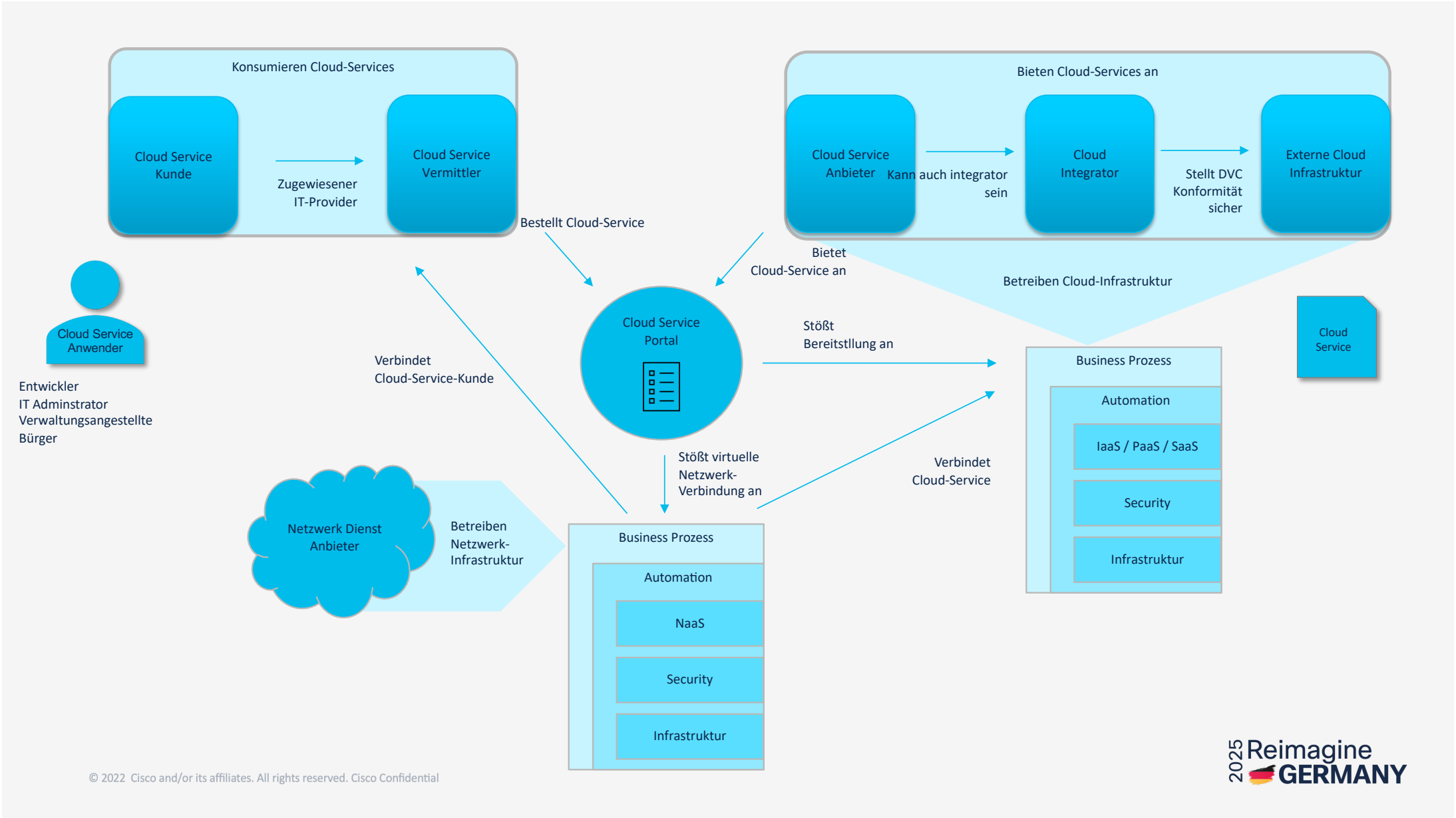


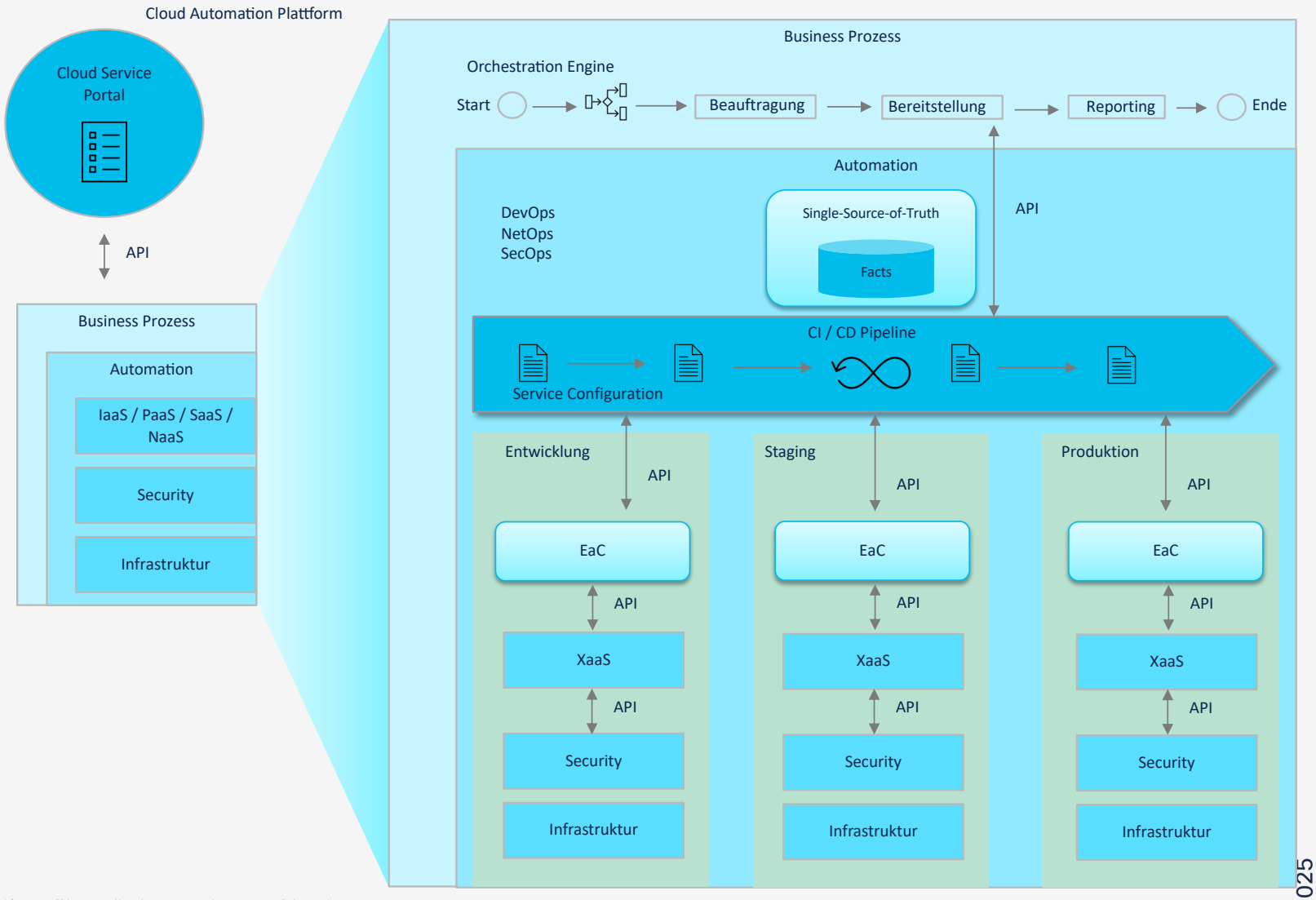
https://eti.cisco.com/blog/panoptica-launch

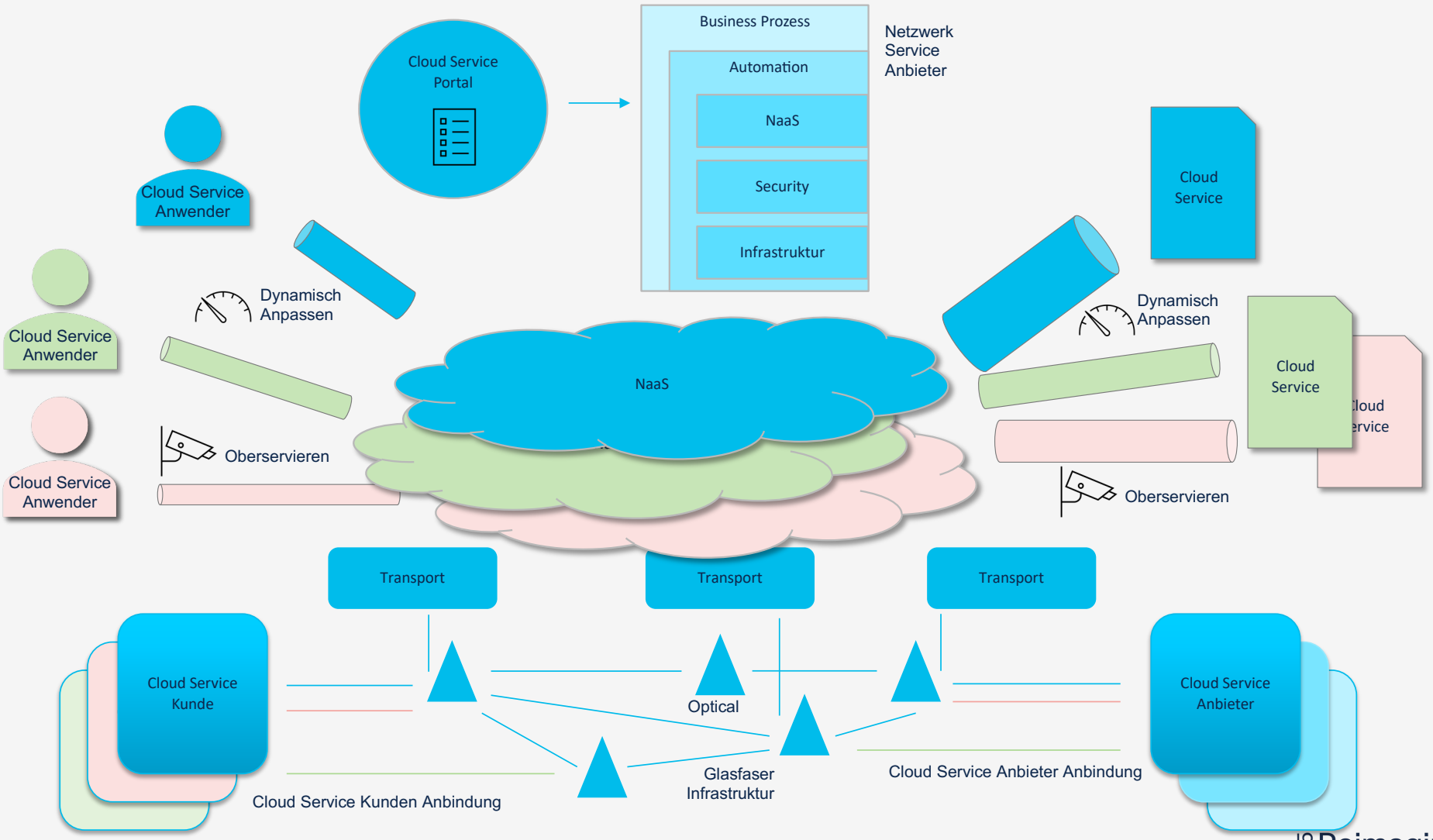
Design Automation

- Vom Service zum automatisierten Betrieb
- Architektur notwendig für Automation
- Software Definierte Netzwerke
- Security Plattform
- Gemeinsame und verteilte Verantwortung



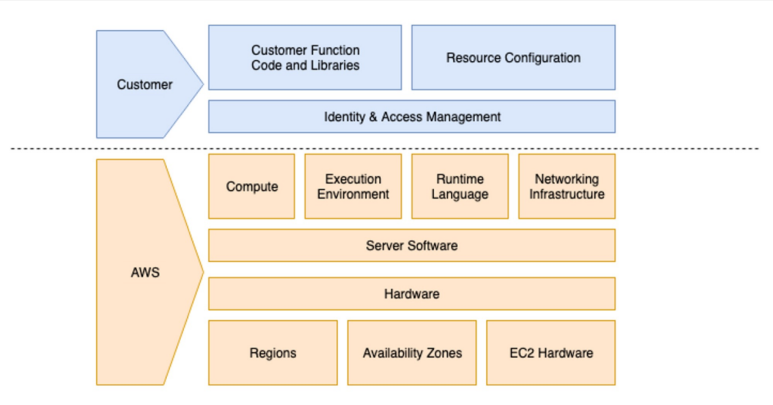






Gemeinsame und verteilte Verantwortung

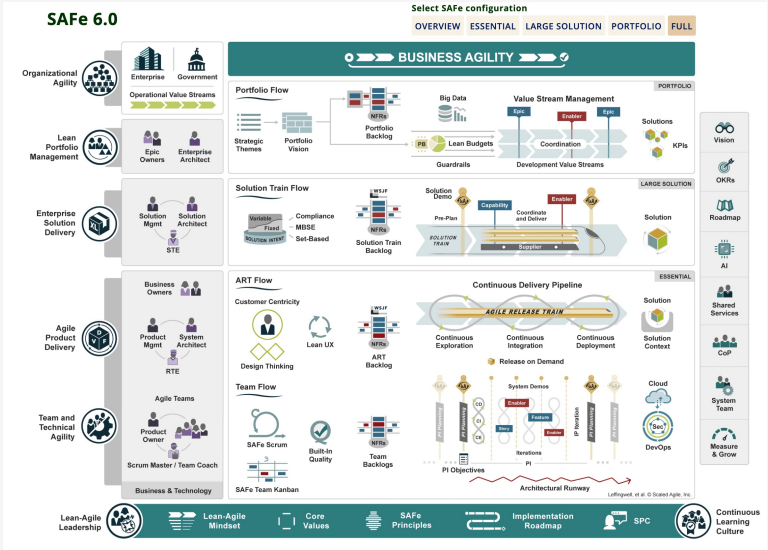
- Cloud Modell Shared Responsibility
- ZT Modell Multi-Domain Architektur
- DevOps verteilte Betriebsverantwortung
- Verantwortung verteilt auf Politik, Regulierung, Dienstleister und Industrie



https://aws.amazon.com/compliance/shared-responsibility-model/

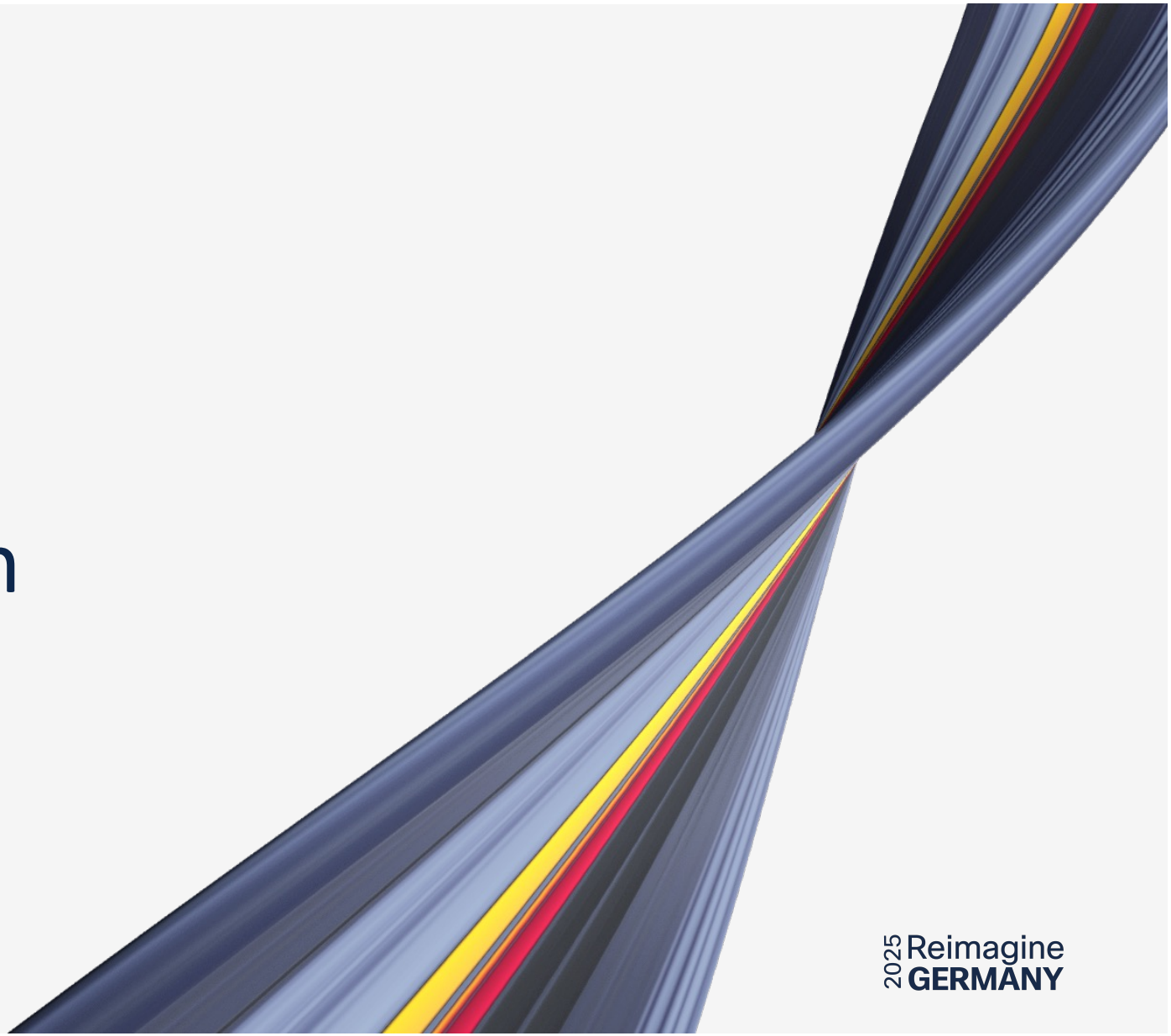
Agile gemeinsame Lösungsentwicklung

- Skalierbares Agiles Framework für Enterprise und Government (SAFe)
- Lernende Arbeits-Kultur
- Schnelle Rückmeldung der Service Konsumenten
- Minimum Viable Produkts
- Budgetierung
- Lebenszyklus der Lösung (TCO Betrachtung)
- Betreibbarkeit
- Verwenden von Trusted Source Software



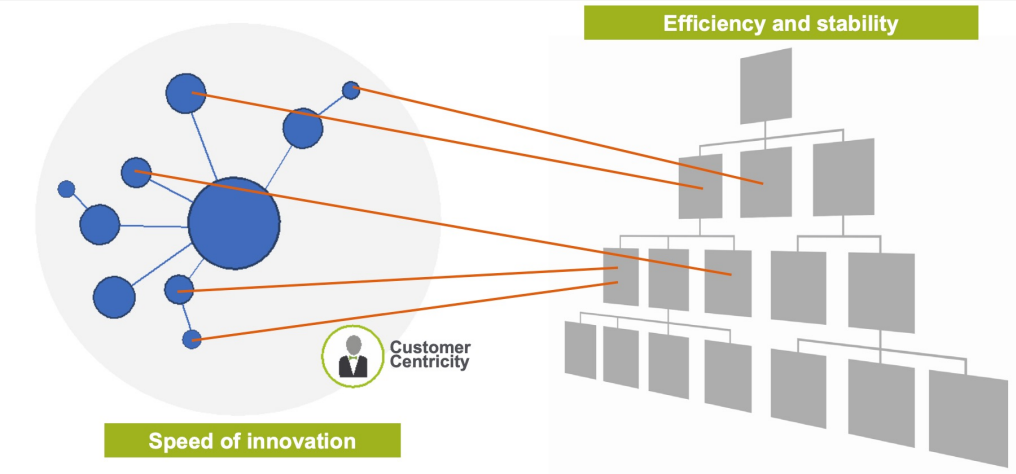
https://scaledagileframework.com/

Managen von Veränderungen



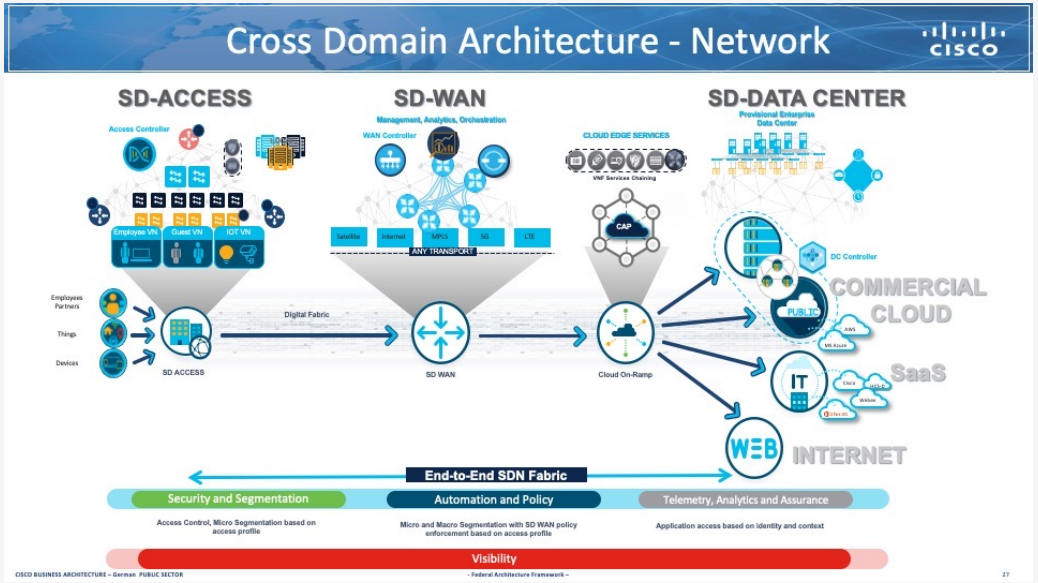
Änderung in der Organisation der Zusammenarbeit

- Einbeziehung aller Interessenten
- Transparente Kommunikation
- Zusammenarbeit zw. Konsumenten, Entwicklern, Betreibern, Herstellern
- Echtes agiles Vorgehen vom Budget bis zum Betrieb



Architektur und Governance

- Modulare Referenz Architektur
- Klare Verantwortlickkeiten für
  - Konzeption
  - Finanzierung
  - Föderal
  - Technisch
  - Betrieblich
  - Sicherheit



- ✓ Technologische Fähigkeiten vorhanden
- ✓ Neue Modelle der Zusammenarbeit
- ✓ Den Wandel managen

Bauen sie einen sicheren Informationsverbund mit den aktuellen Fähigkeiten und Standards

Future ***Ready***

2025 Reimagine GERMANY