Unsichere Zeiten, unklare Wege – unabhängige Schutzmaßnahmen in der Cloud

Schützen Sie die Anwendungen und Daten Ihrer Behörde selbstbestimmt in Cloud-Umgebungen

Markus Pfaff

CTO and Chief Architect Federal

24. Januar 2024

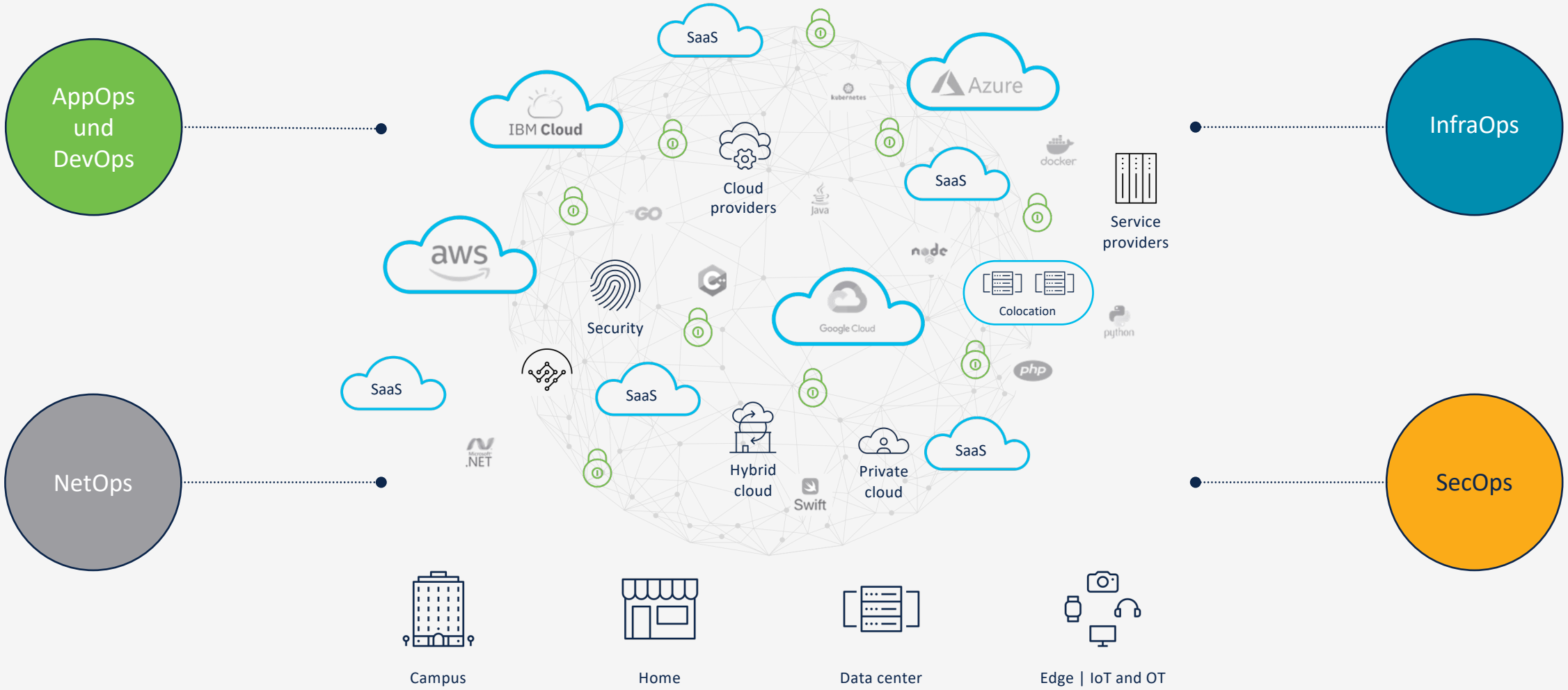
2025 Reimagine GERMANY

Problemstellung

- Digitalisierung der öffentlichen Verwaltung
- Cloud Technologie für Dienstleistungen des Staates
- Cloud wird als unsicher betrachtet

Moderne Anwendungen

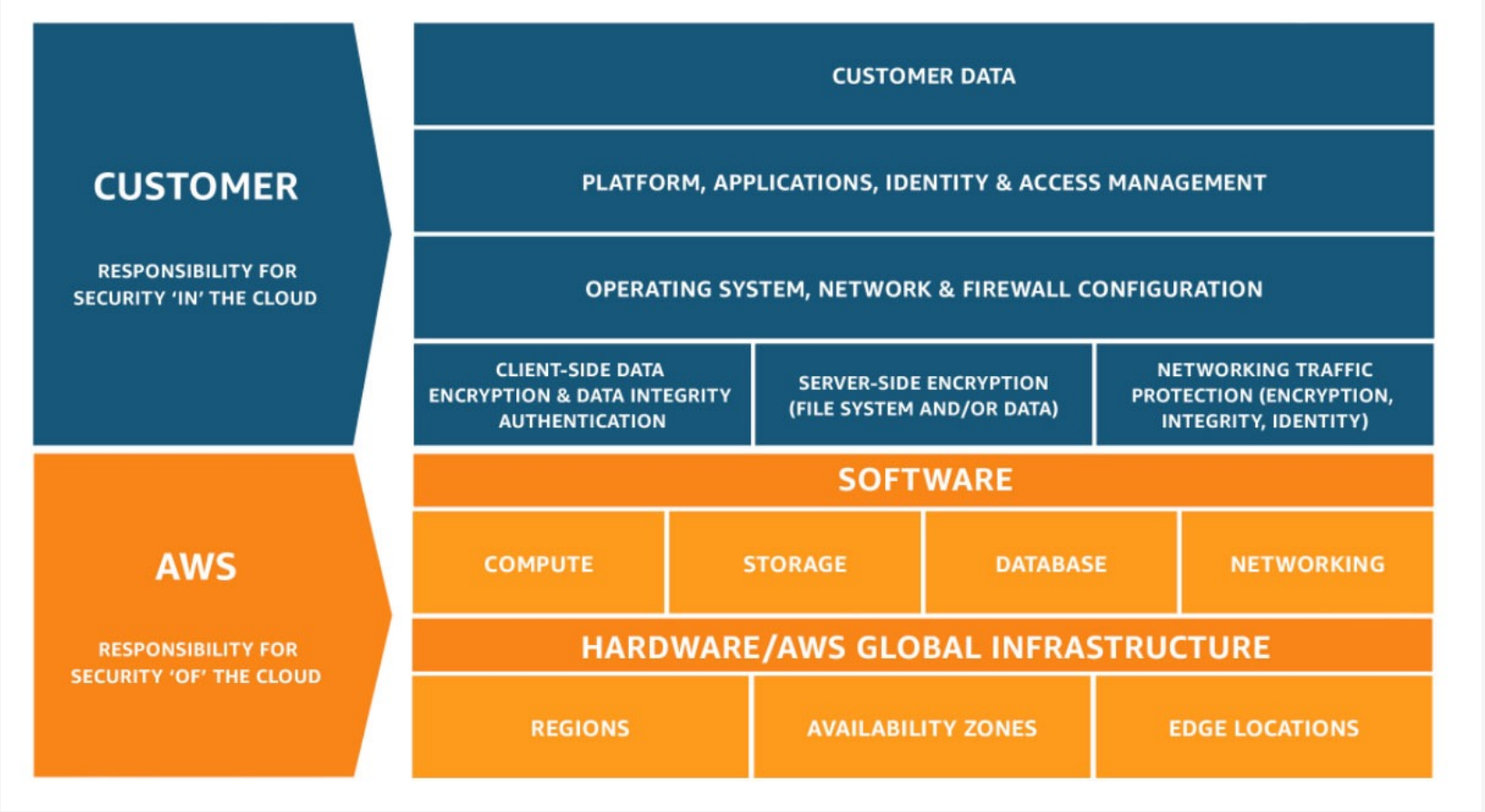
Betrieb von Anwendungen in einer komplexen Umgebung



Geteilte Verantwortung ist vorgegeben

Cloud Nutzer:
Sicherheit **in** der Cloud

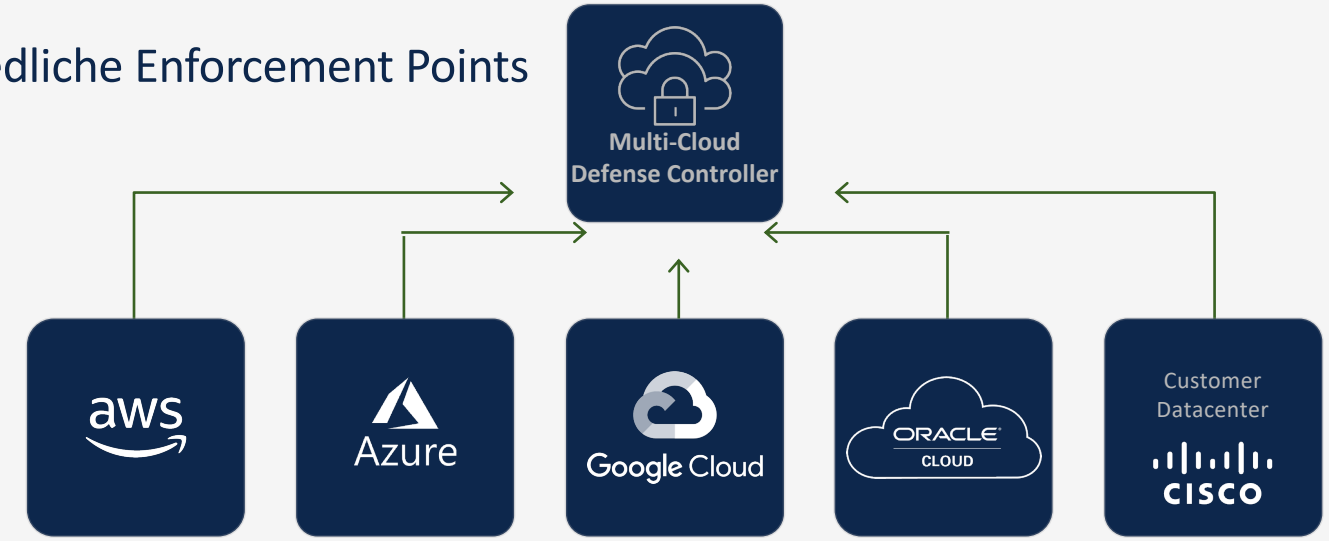
Cloud Service Provider:
Sicherheit der Cloud



https://aws.amazon.com/de/compliance/shared-responsibility-model/
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate?hl=de

Multi-Cloud World

- Cloud ist nicht vergleichbar mit einem Rechenzentrum
- Jeder CSP ist anders – zu viele Cloud native Komponenten –
- Abhängigkeiten von externen Scripts, Templates und Cloud Komponenten
- Komplexe Service Integration und komplexes Routing
- Sichtbarkeit – Kein “Single-pane-of-glass” und eingeschränkte Kontrolle
- Policy – Keine einheitliche Policy und unterschiedliche Enforcement Points



4 Insights

Centralized Policy

Observability

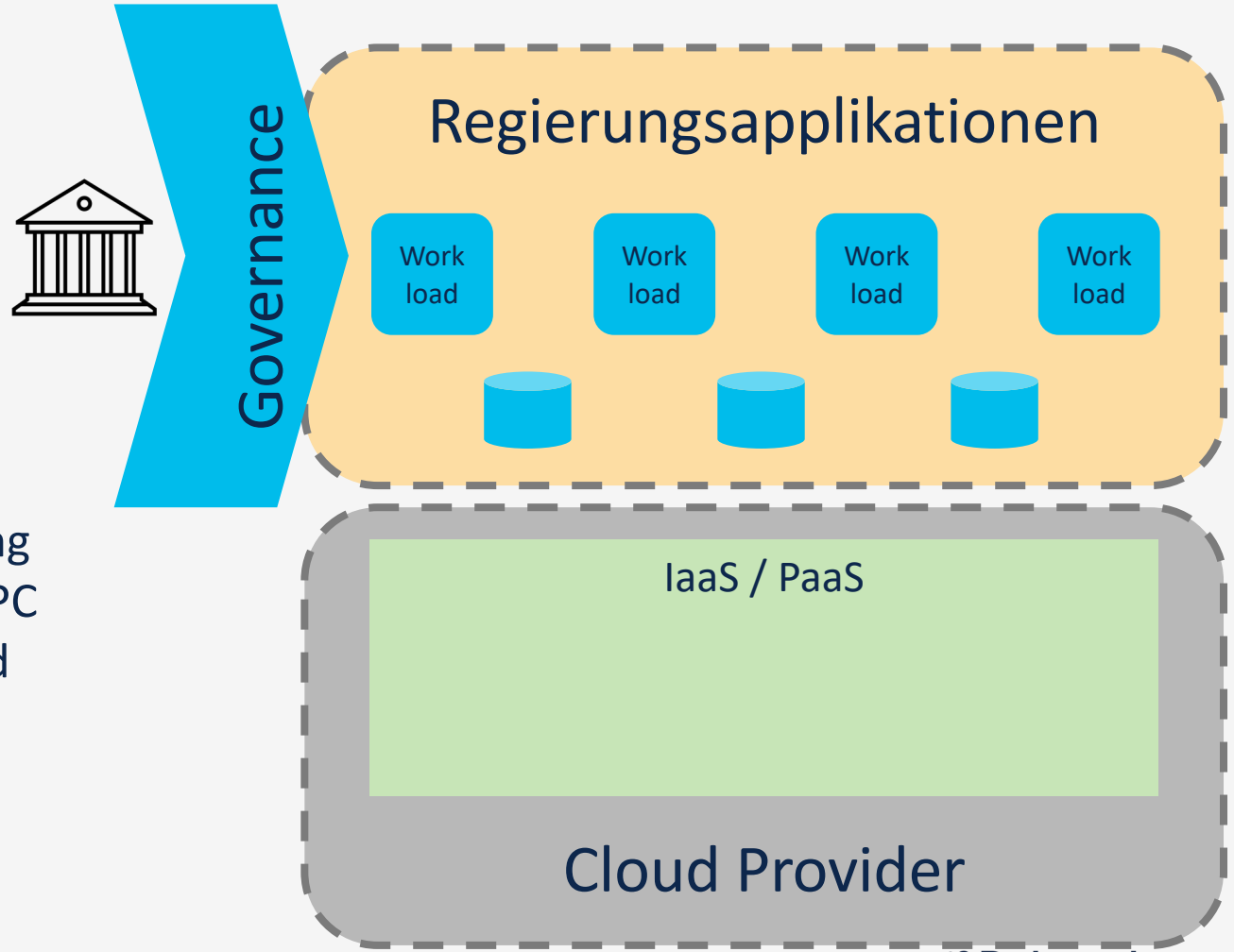
Enforcement

Collaborate

Centralized Policy

Ein Regelwerk in der Multi-Cloud - 1

- Unabhängig von der Cloud Umgebung
  - Private, sovereign, public cloud
- Sichere Verbindung in die Cloud
- Transport agnostisch
- Erweiterung des WAN in die Cloud Instanzen
- WAN Automation Teil der eigenen IT Abteilung
- Absicherung der Work-loads innerhalb der VPC
- Anpassung an dynamisches Umfeld der Cloud
- Datenhoheit behalten



Ein Regelwerk in der Multi-Cloud - 2

Zentrale Policy umsetzen

Beobachten

Regulieren

Regierungsapplikationen

Work load

Work load

Work load

Work load

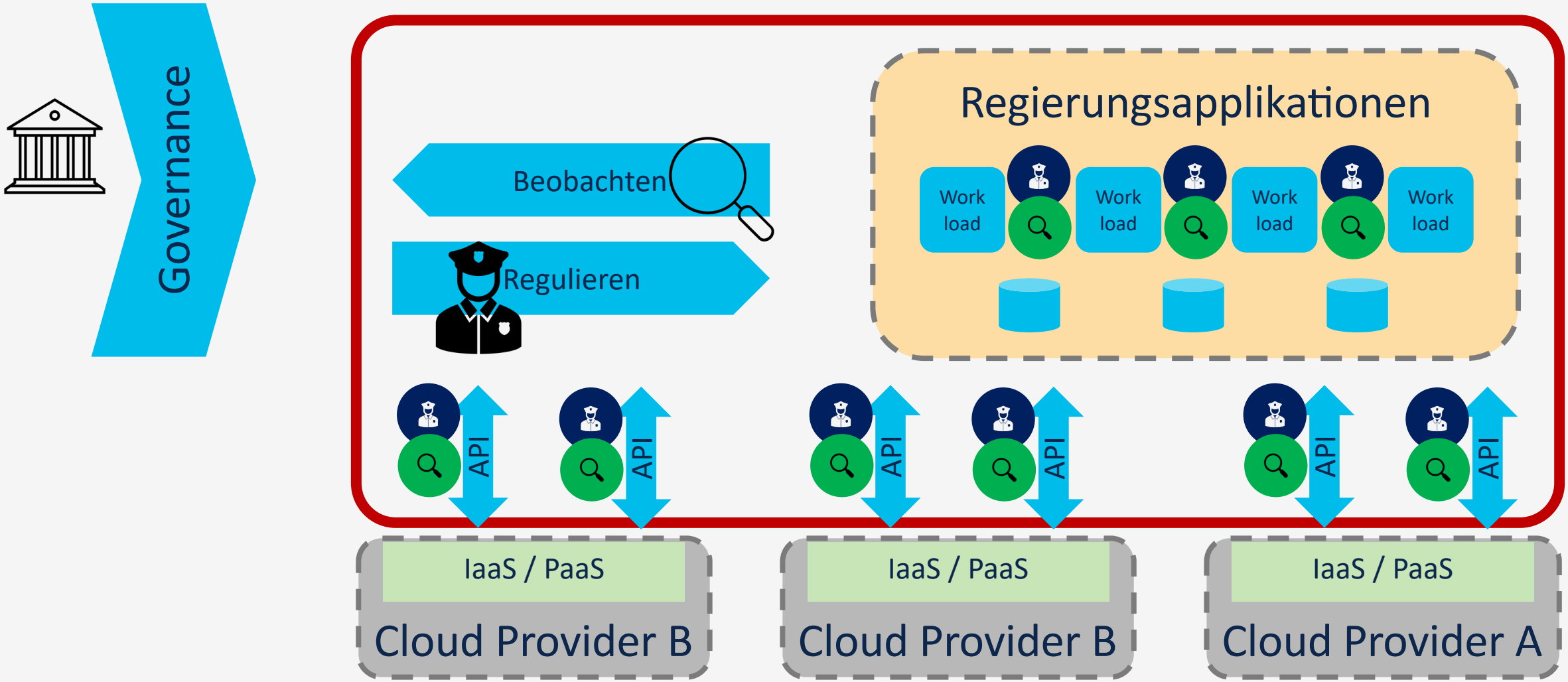
API

API

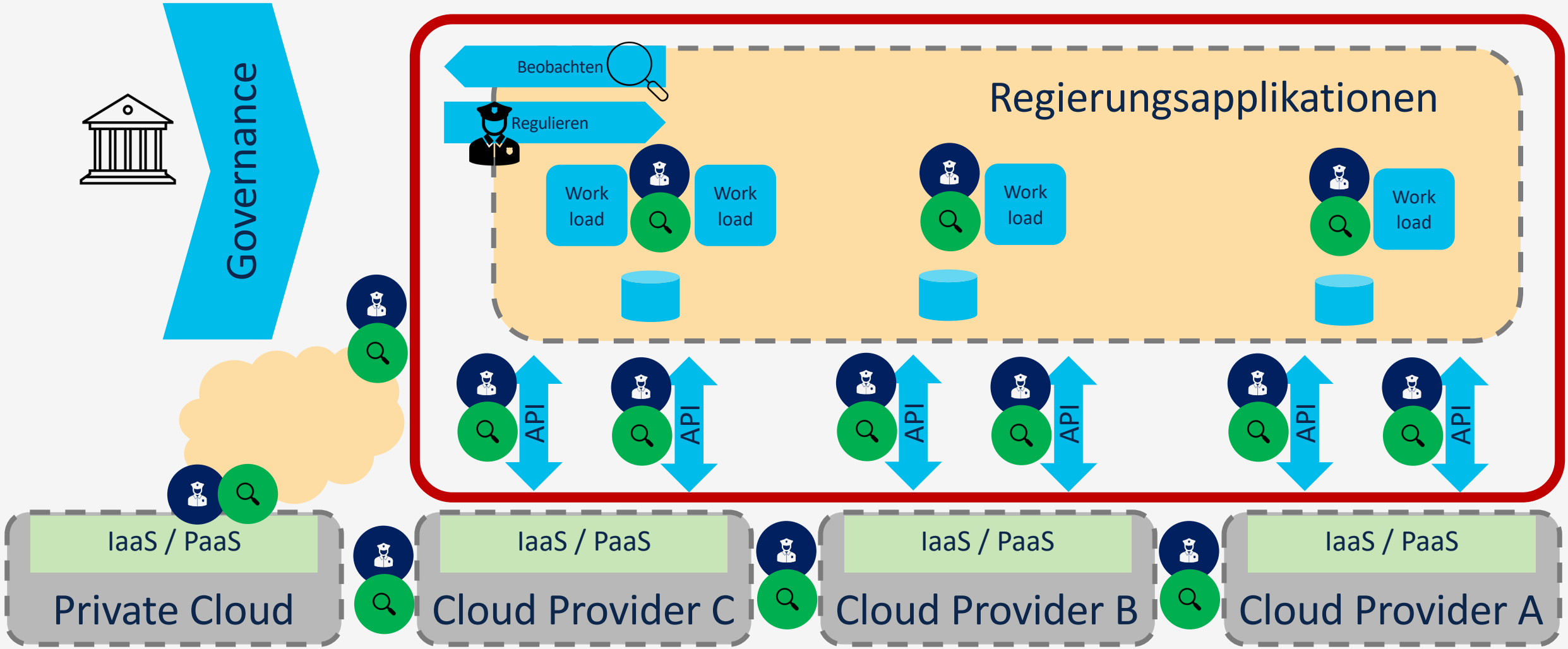
IaaS / PaaS

Cloud Provider

Ein Regelwerk in der Multi-Cloud - 3



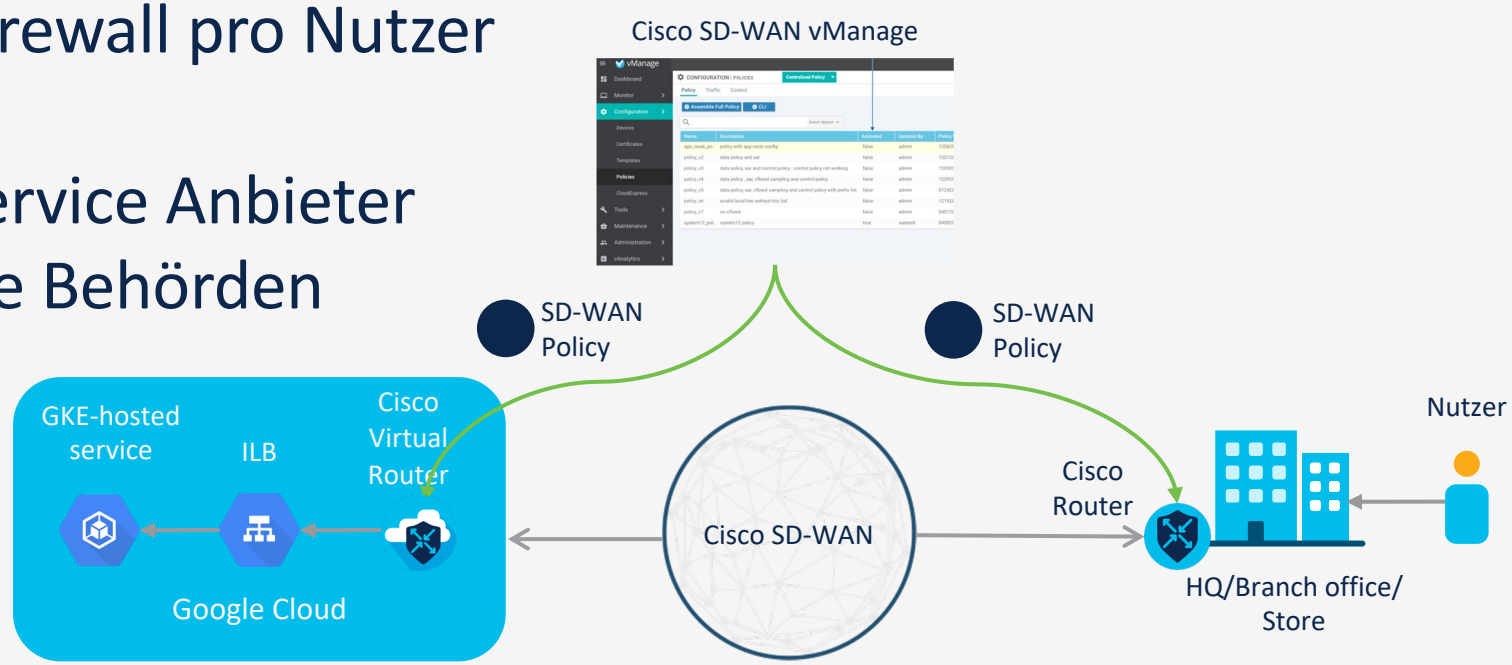
Ein Regelwerk in der Multi-Cloud - 4



Secure Connectivity

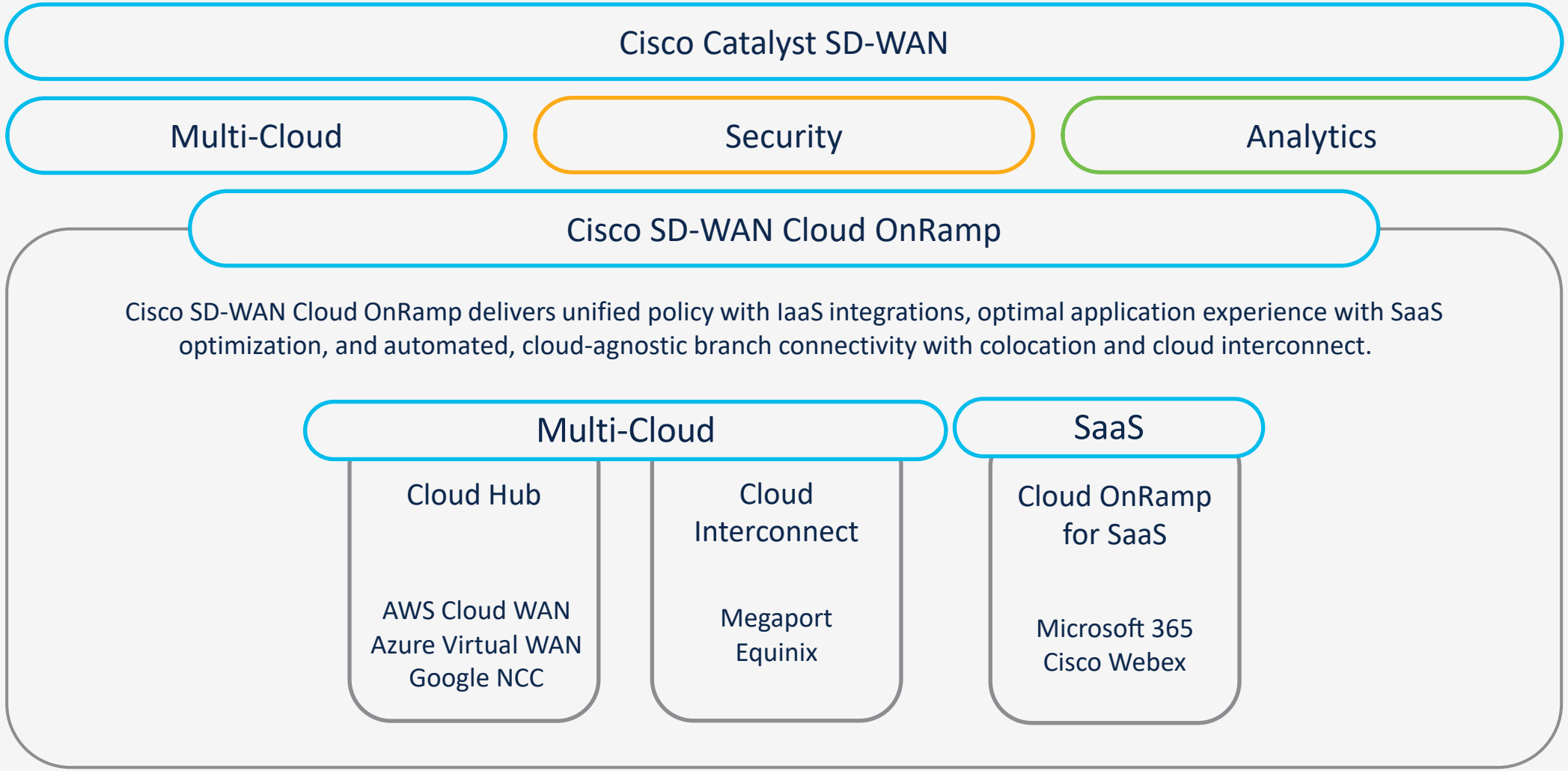
Security Komponenten Cisco SD-WAN Umsetzung

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

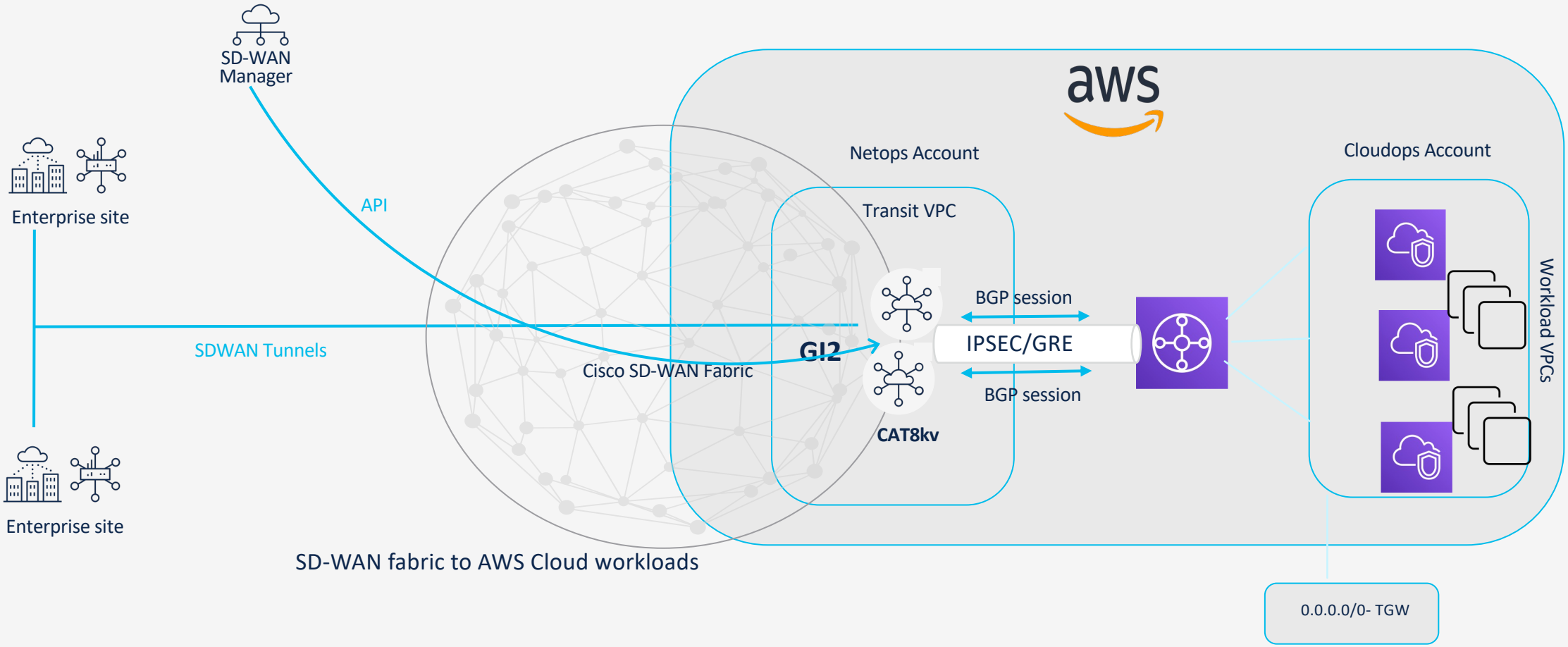


https://www.cisco.com/c/de_de/solutions/enterprise-networks/sd-wan/sd-wan-security.html

SD-WAN Cloud Networking



AWS - Site-to-Cloud



SD-WAN fabric to AWS Cloud workloads

Simple

Automated

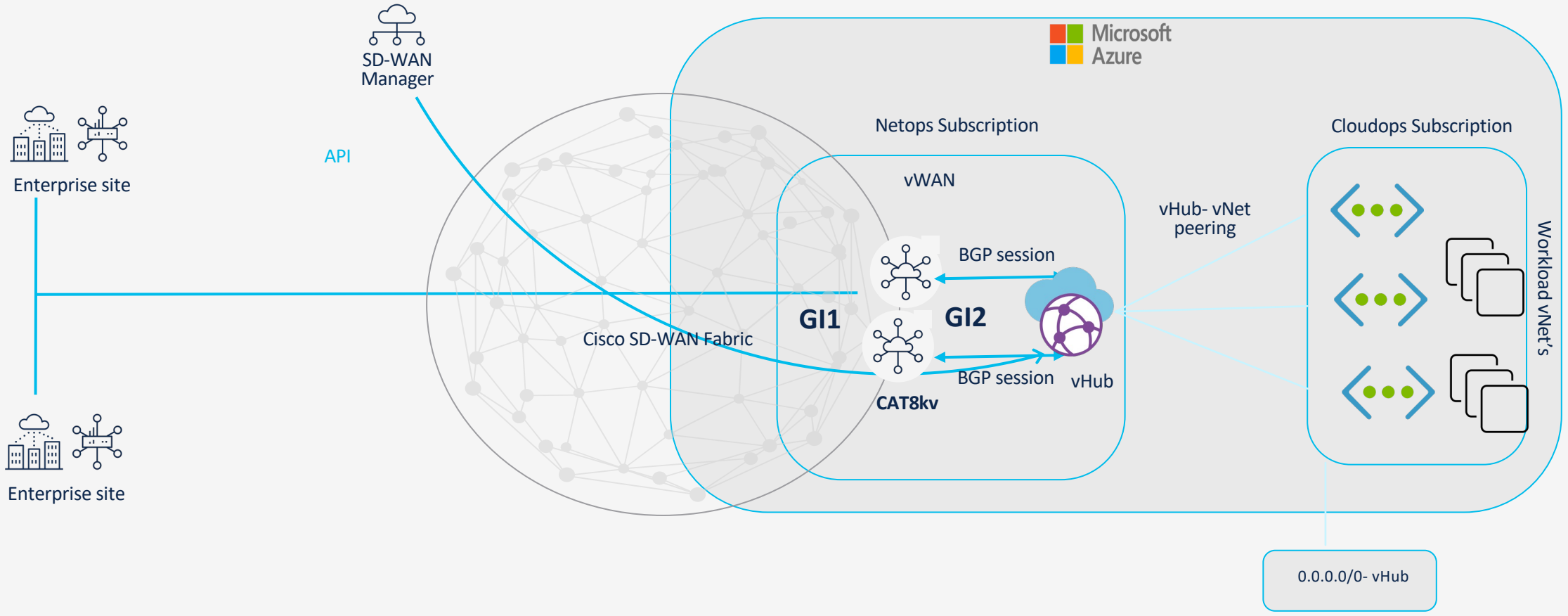
Secure

Azure - Site-to-Cloud

Microsoft Azure

Azure Government

SD-WAN fabric to Azure Cloud workloads



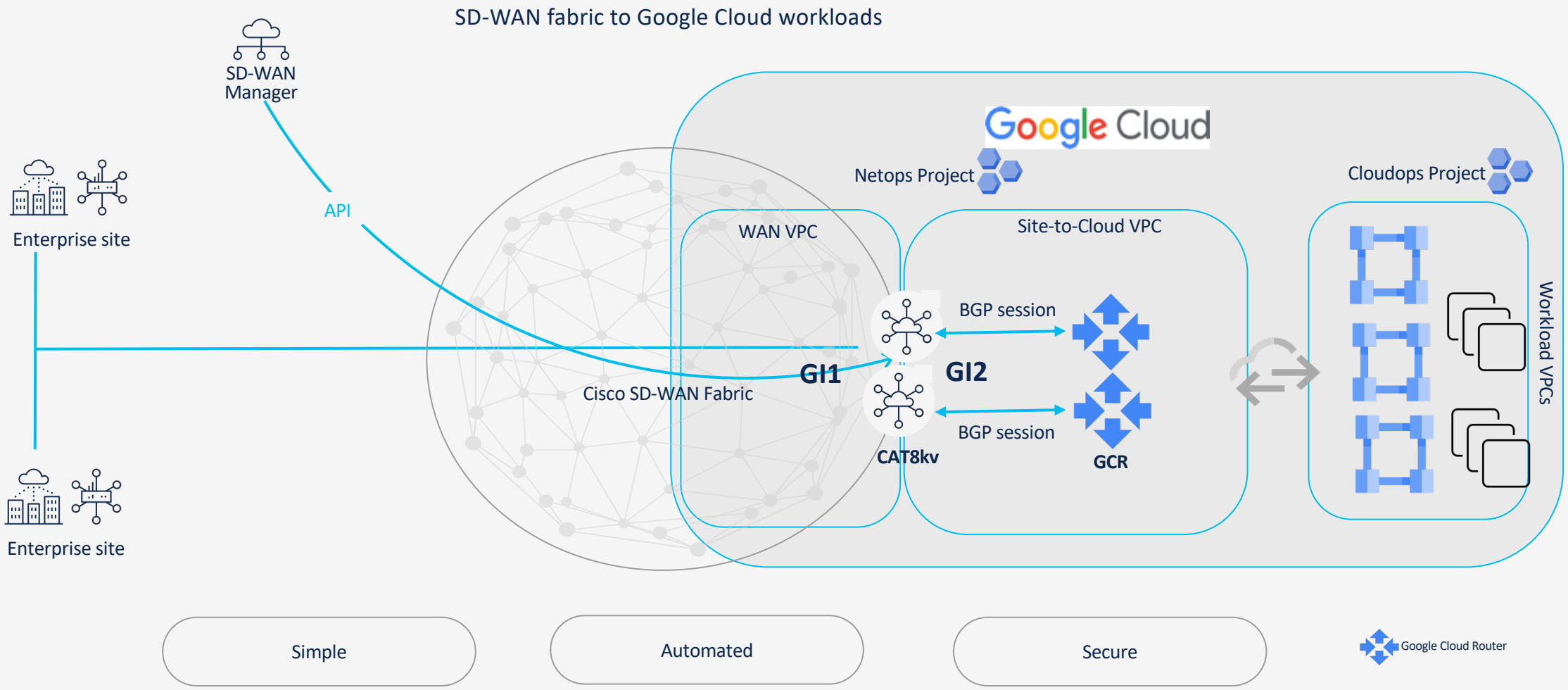
Simple

Automated

Secure

2025 Reimagine GERMANY

Google Cloud - Site-to-Cloud



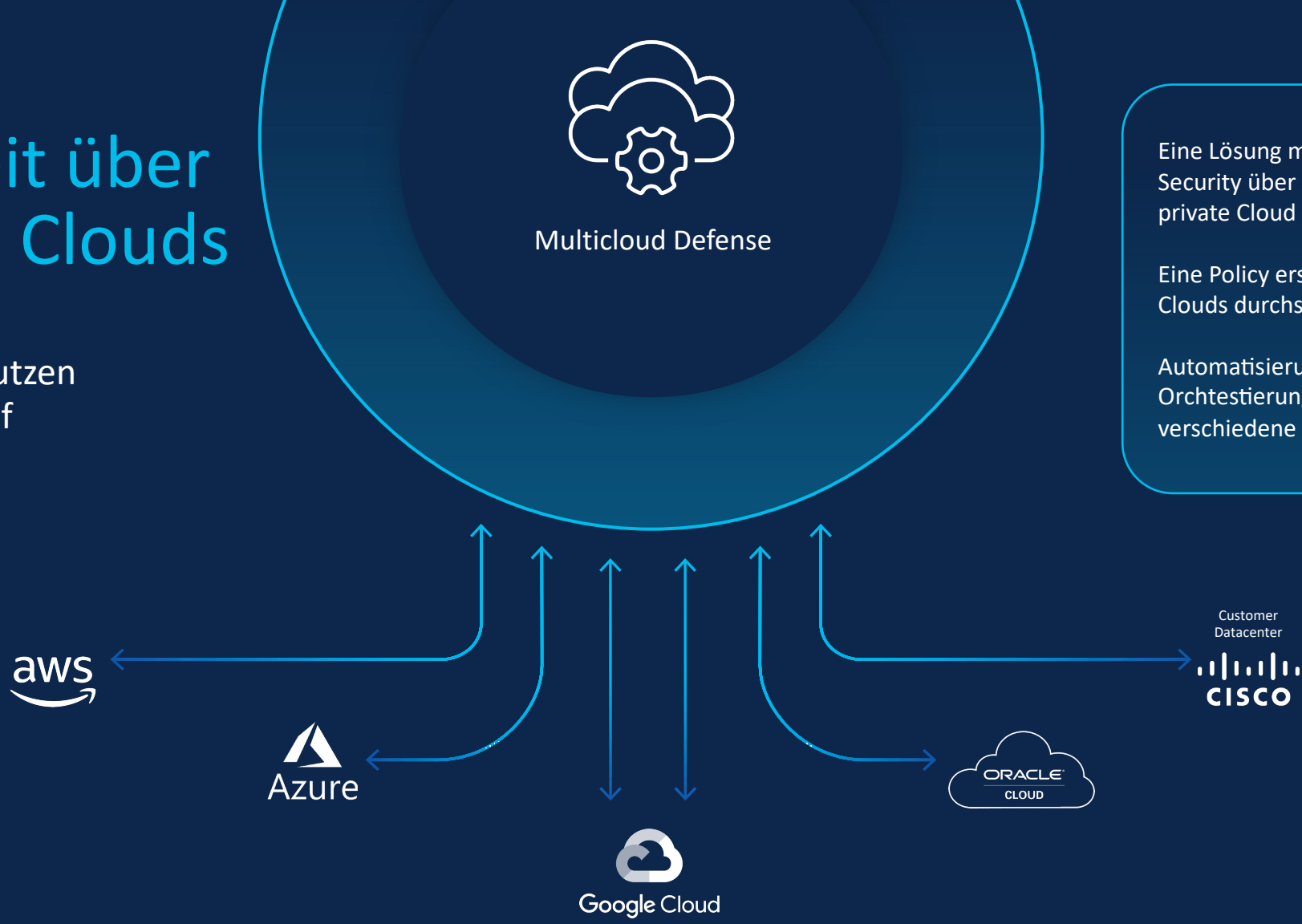
Cloud Native Advanced Network Security

Cloud Security Positioning

	 Multi-Cloud Defense	 Cloud Application Security	 Secure Workload
Suite Positioning	**Cloud-based network security**	**Multi-cloud cloud-native application protection platform**	**Hybrid-cloud Zero-Trust workload security**
Why Critical?	Consistent, automated, advanced security implementation across multi-cloud	Provides CNAPP protection to multi-cloud workloads using graph-based context	Zero-trust protection for hybrid-cloud workloads utilizing machine-driven policy lifecycle automation
Market Drivers	• Single-policy across cloud providers • Avoids CSP tool sprawl • Advanced in-line security controls • SaaS delivered controller • PaaS delivered security	• Agentless • Context-based prioritization • Dynamic Remediation • Build to runtime protection	• Zero Trust / Least Privilege • SaaS delivered • Automated Policy Discovery • Workload & container security • Enforcement and Compliance
Security Features	✓ WAF ✓ IDS / IPS ✓ Geo IP ✓ Malicious IP ✓ Antivirus ✓ FQDN Filtering ✓ URL Filtering ✓ DLP ✓ Cloud-native Identity	✓ Attack Paths ✓ CSPM ✓ CWP ✓ API Security ✓ CI/CD Security ✓ Serverless Protection	✓ Dynamic Policy ✓ CVE Identification ✓ Policy Simulation ✓ Threat Intelligence ✓ Flow and telemetry visibility ✓ Agent or Agentless

Sicherheit über mehrere Clouds

Cloud Vorteile nutzen ohne Verzicht auf Sicherheit



Eine Lösung managed die Security über alle Public und private Cloud

Eine Policy erstellen und in allen Clouds durchsetzen

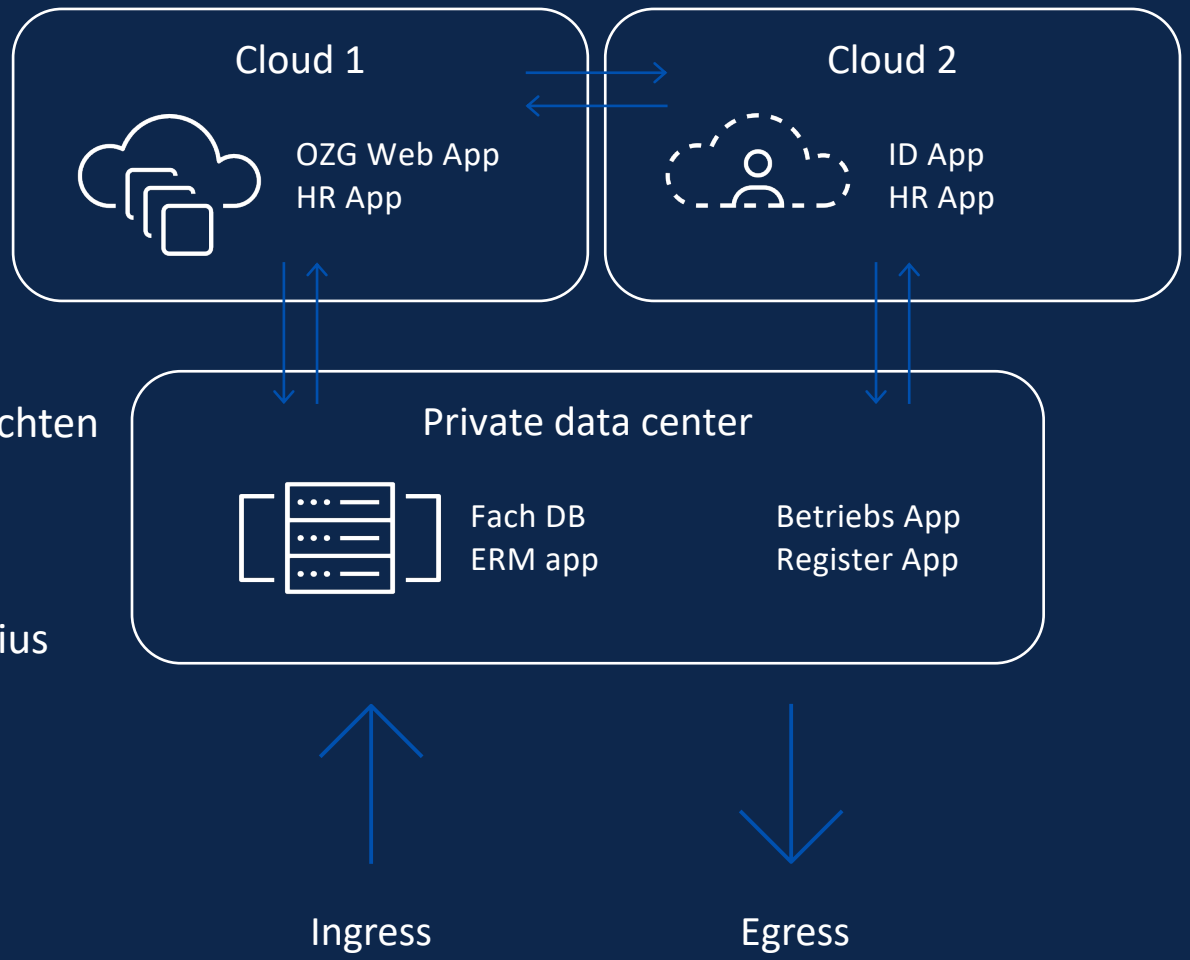
Automatisierung und Orchtestierung über verschiedene Clouds nutzen

Kompletter multi-direktionaler Schutz

Ingress security: Stopt inbound Angriffe auf Web und non-web Applikationen.

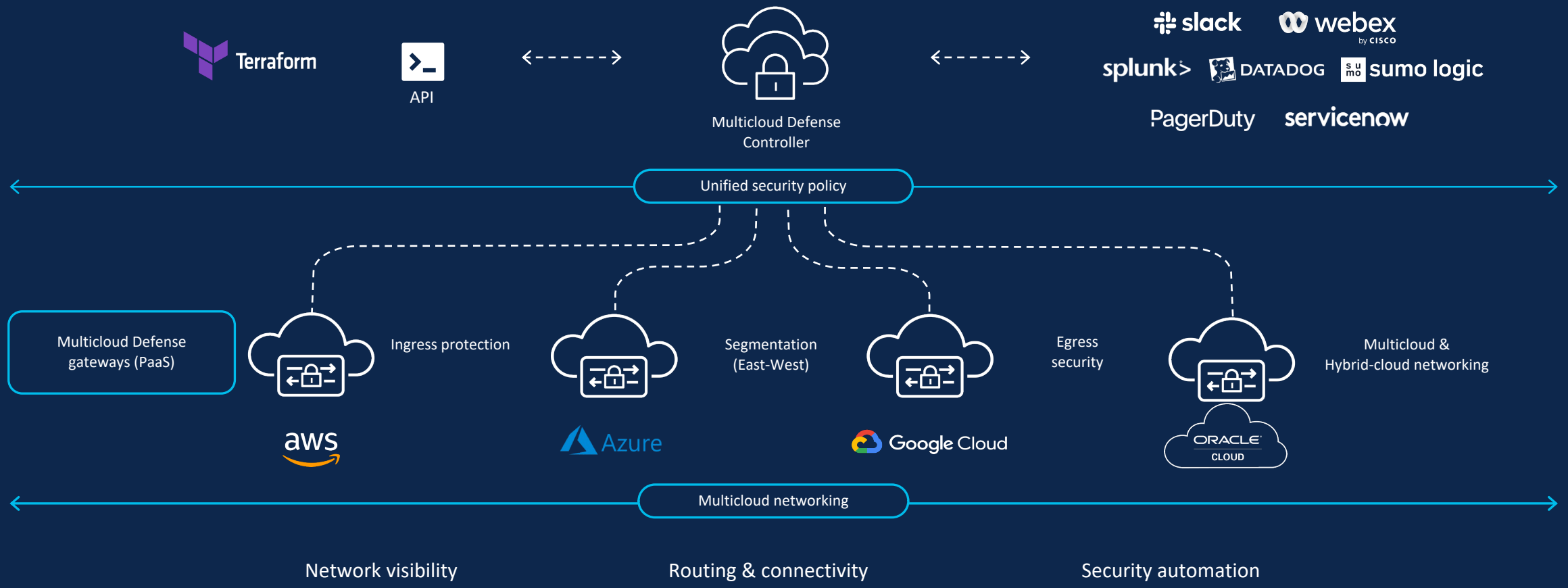
Egress security: Erkennt und blockiert Command & Control, Botnets, und ungewünschten Datenabfluss.

East-west security: Reduziert Verbreitungsradius und schützt gegen Ransomware durch Einschränkung von Quer Bewegungen.

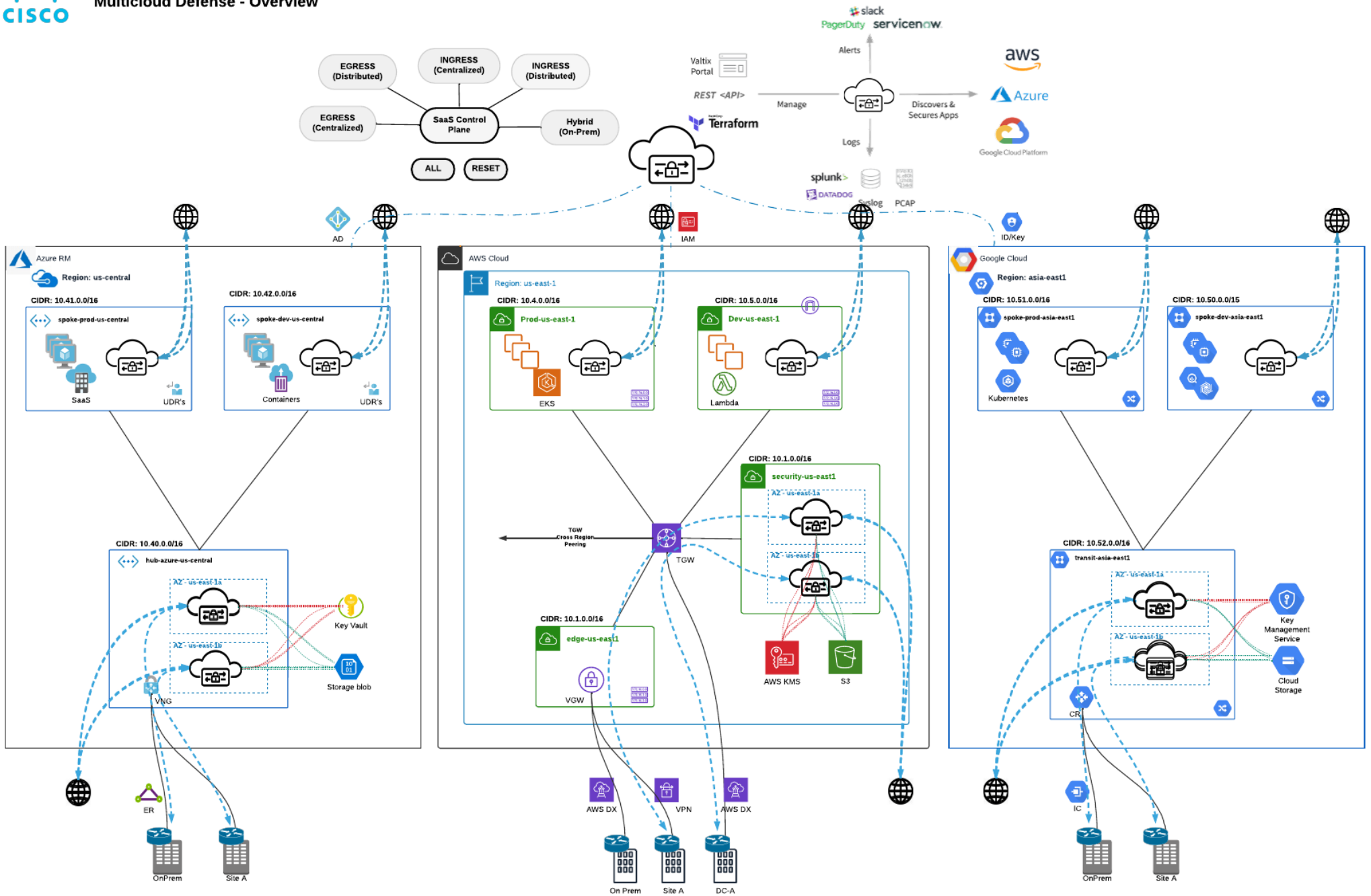


Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud native network security



Multicloud Defense - Overview



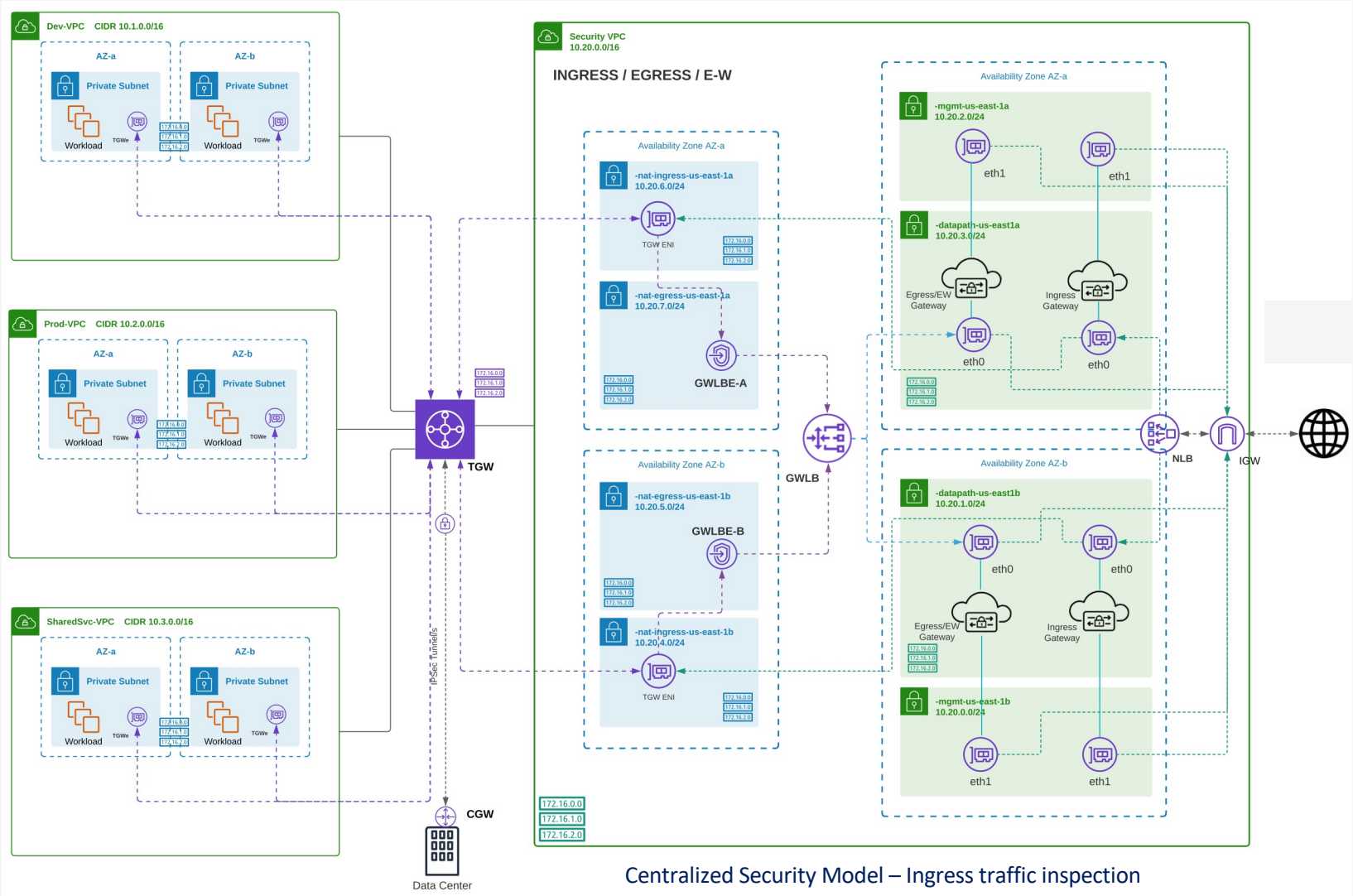
AWS Centralized Security Model - Ingress

Overview

- Security VPC
- AWS Transit Gateway (TGW)
- Network Load Balancer (NLB) for ingress traffic forwarding
- Ingress Gateways for traffic inspection

Orchestration

- Security VPC
- Network Load Balancer
- Multicloud Defense Gateways
  - Deployment
  - Insertion
  - Autoscaling
- Transit Gateway
  - New or existing TGW
  - TGW attachment
  - Traffic engineering (routing)
- VPC subnet route to TGW



Centralized Security Model – Ingress traffic inspection

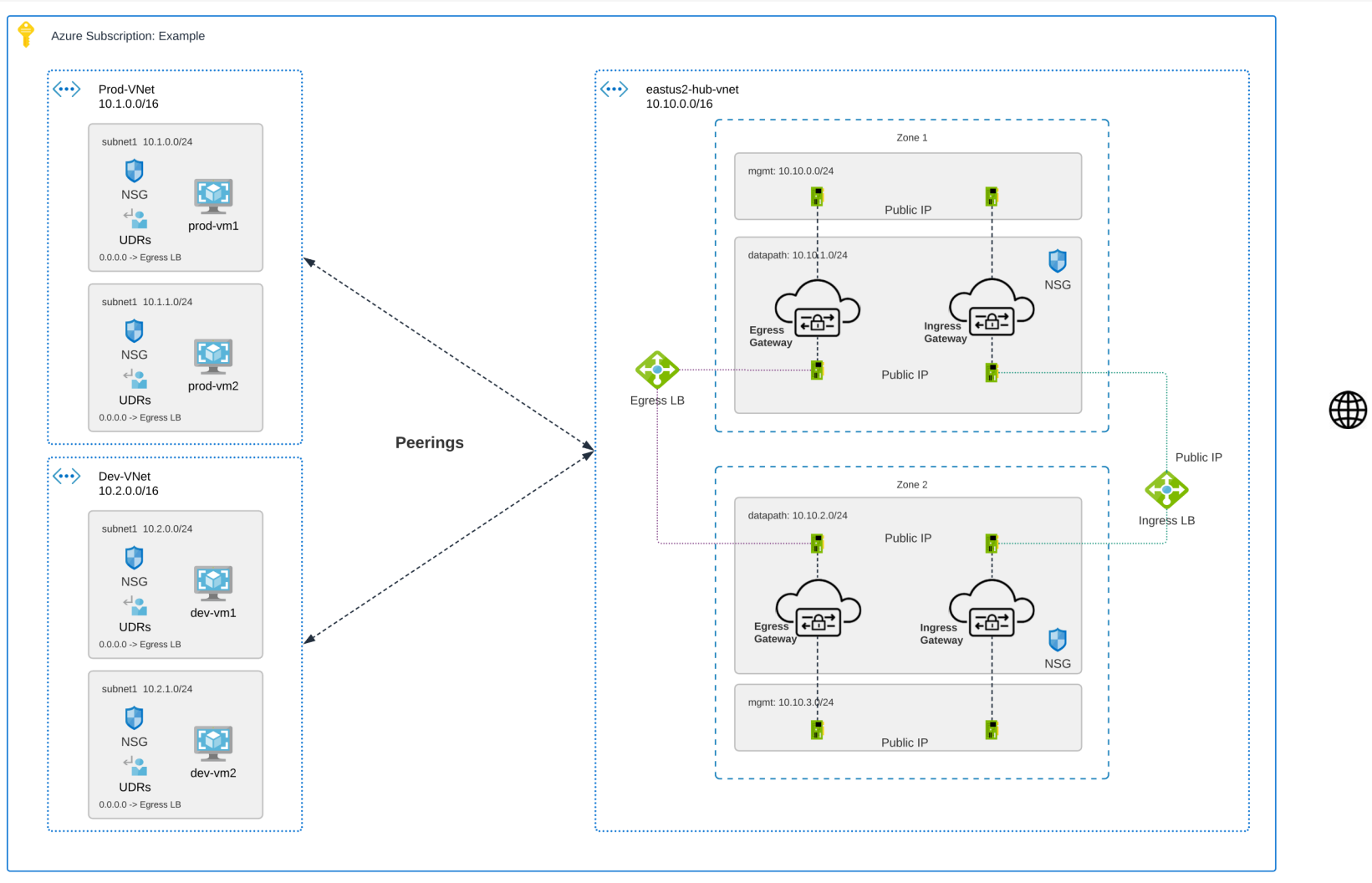
Azure Centralized - Ingress & Egress

Overview

- Security vNET
- Ingress Gateway
- Egress Gateway
- Internal Load Balancer
- External Load Balancer
- vNET Peering

Orchestration

- Security vNET
- Network Load Balancers
- Multicloud Defense Gateways
  - Ingress & Egress GW
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



Azure Centralized – Ingress & Egress traffic inspection

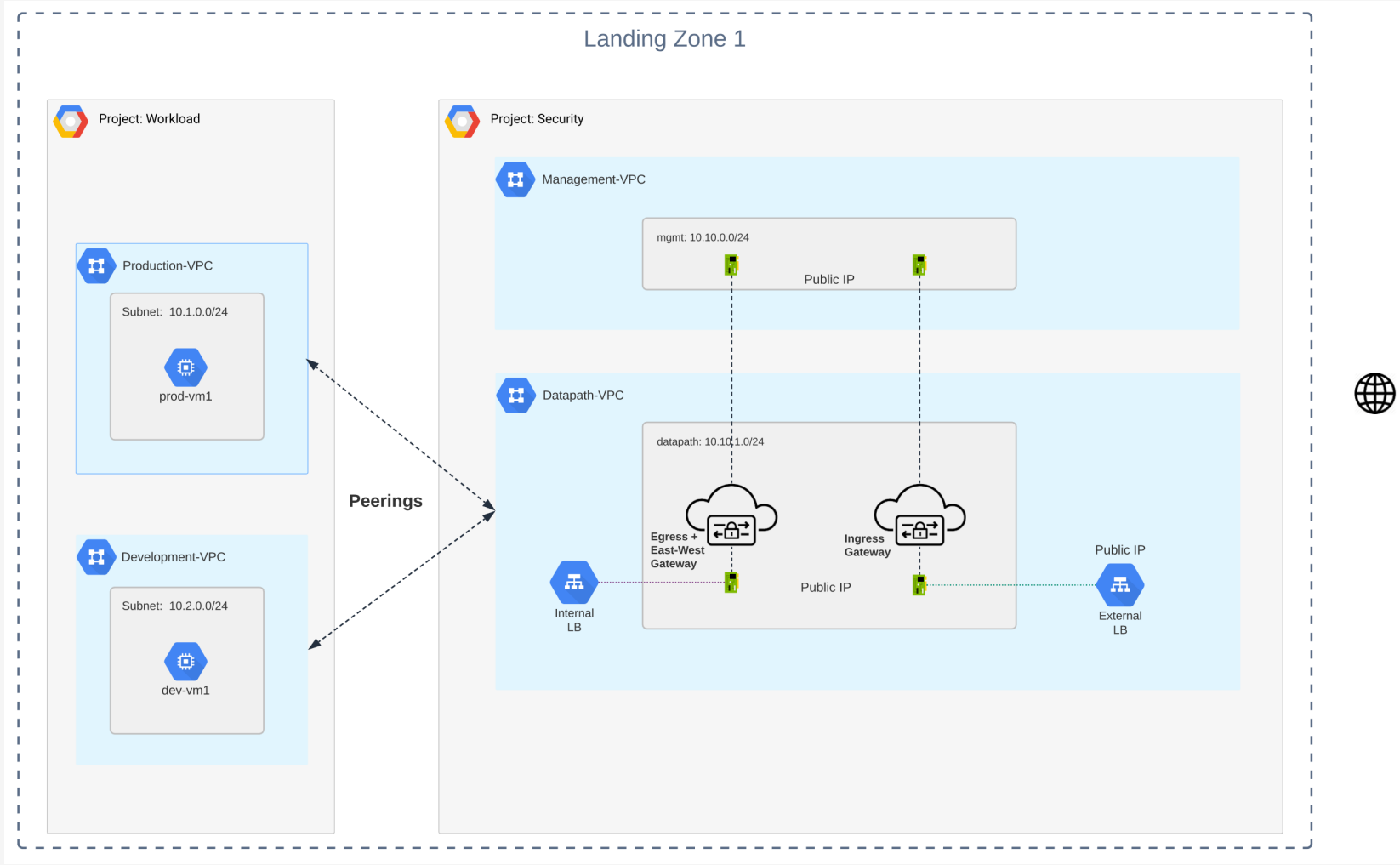
GCP Centralized - Ingress, Egress & East/West

Overview

- Security VPC
- Egress Gateway
- Internal Load Balancer
- VPC peering

Orchestration

- Security VPC
- Network Load Balancers
  - Internal & External
- Multicloud Defense Gateways
  - Egress GW
  - Ingress GW
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



GCP Centralized – Ingress, Egress & East/West traffic inspection

Cloud Native Application Protection

Sicherheits Anforderungen der Cloud-Native Applikationen von der Entwicklung bis in die Produktion mit Panoptica

Code + Build Security

Prioriseren und abhelfen:

- Gesamten Entwicklungszyklus
- Governance Policies
- Infrastructure-as-Code

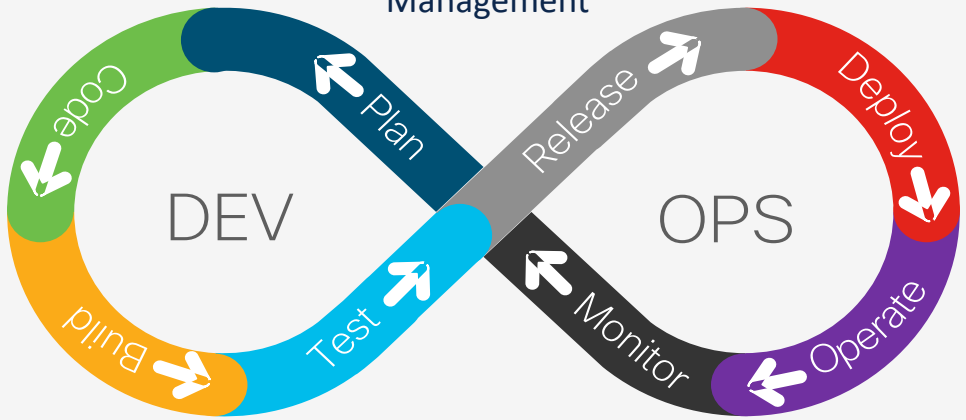
Cloud Security Posture Management

Automatisieren und vereinfachen:

- Compliance Monitoring
- Resource Management

Identity & Access Management

Artifact Scanning



Runtime Protection

Cloud Configuration

Attack Path Analysis

Priorisieren mit Präzision.
Risiko mindern wo es am nötigsten ist—zuerst.

App + API Security

Assess und Monitor:

- Interne und Externe APIs
- API Tokens

Cloud Workload Protection

Kontinuierliches Risk Management:

- Virtual Machines
- Containers
- Serverless

Observability

OpenTelemetry

Was ist OpenTelemetry?

Was ist OpenTelemetry?

> Ein Observability Framework für cloud-native Software.
>
> **- opentelemetry.io**

Applikation

API

Code Instrumente um Telemetrie Daten zu erzeugen

SDK

Sammeln der Telemetrie un weiterleiten in Verarbeitungs kette

Processing

Verarbeitung der Telemetry Daten: Sampling, filtern, anreichern

Exporter

Konvertieren und kommunizieren

Kollektor

Daten filtern, zusammenbringen abarbeiten und kommunizieren

Telemetry / Observability / Monitoring Back-end

OpenTelemetry

OpenTelemetry Daten Quellen

1

Metric

A measurement about a service, collected at runtime

2

Trace

End-to-End progression of a request, across services

Span

A unit of work within a Trace

3

Log

A time stamped text record, often attached to Spans

Events are a specific type of log

4

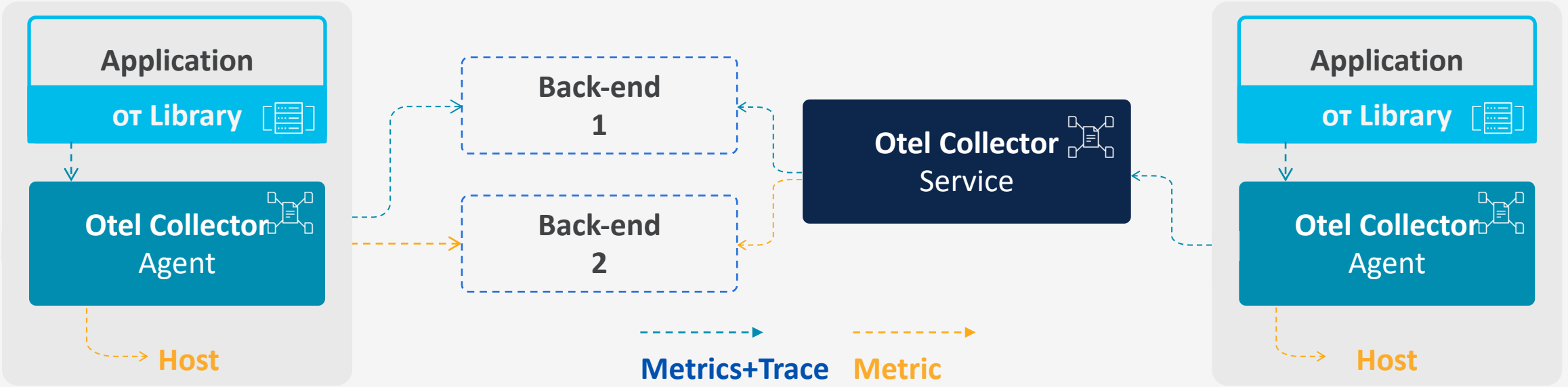
Baggage

Mechanism for propagating name/value pairs.

To establish a causal relationship between events from different services.

OpenTelemetry

Open Telemetry Referenz Architektur



OpenTelemetry Instrumentierungs-Libraries sollten zu jeder Anwendung (manuell) hinzugefügt werden oder der OT Agent sollte genutzt (automatisch)

Der OpenTelemetry Kollektor kann als Agent auf jedem Host in der Umgebung installiert und konfiguriert werden, um die Telemetrie Daten an die jeweiligen Back-ends der Nutzer gesendet zu werden.

Optional, können Gateway Kollektoren mit Load Balancing provisioniert werden.
Die agent-mode Kollectoren sprechendann zum Gateway Kollektor, das wiederum mit den Back-Ends spricht

Backends können open-source oder kommerzielle Anwendungen sein.

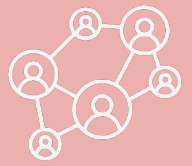
Source: https://opentelemetry.io/docs/

OpenTelemetry

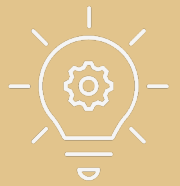
Cisco Observability Platform (COP)

Bringt missions-kritische Daten der Organisation zusammen und zeigt sie in einer einzigen Echtzeit-Ansicht

Korreliert Telemetrie aus verschiedenen Bereichen, die besonderen Einfluss auf den Erfolg der Organisation haben

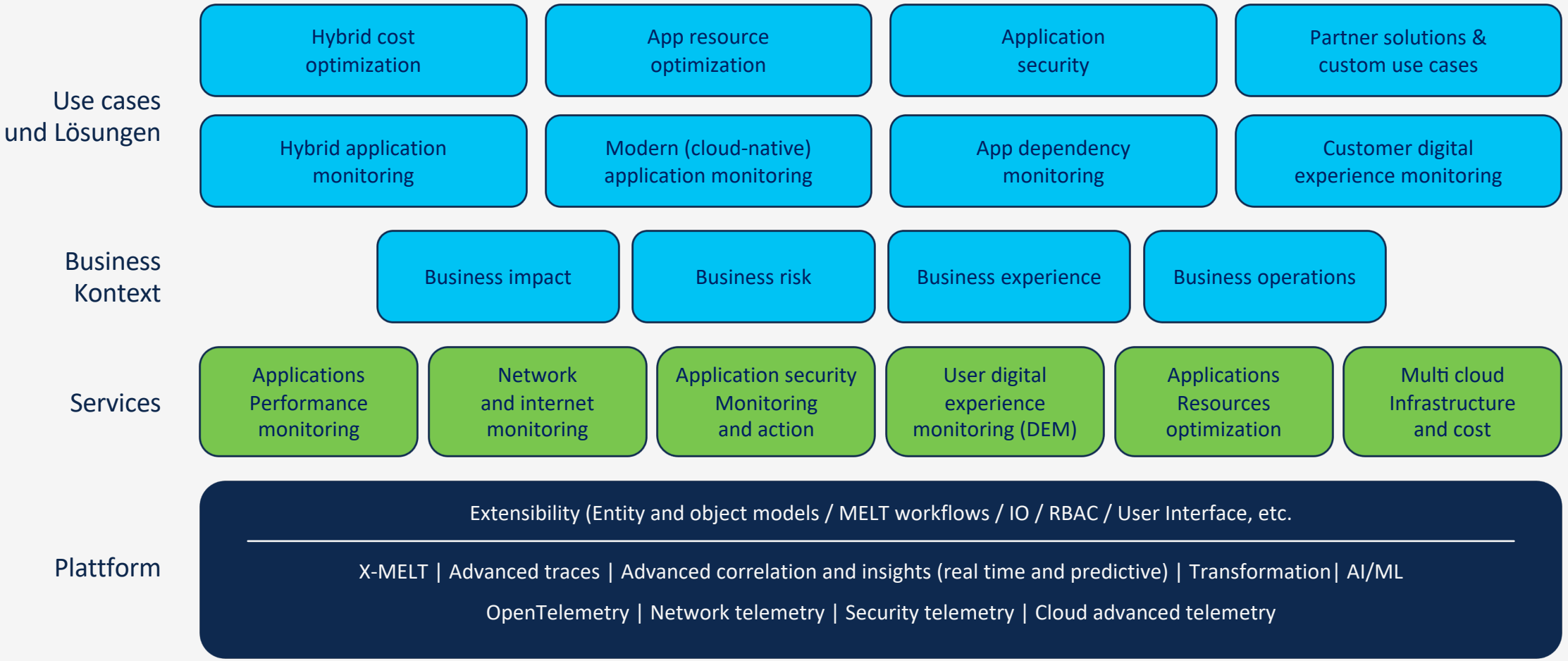


Verbindet Menschen und Tools über die gesamte Organisation, um komplexe Probleme schnell zu identifizieren und zu lösen



Nutzt spezielle Applikationen oder erweitert existierende, um die besonderen Bedarfe der Organisation zu adressieren

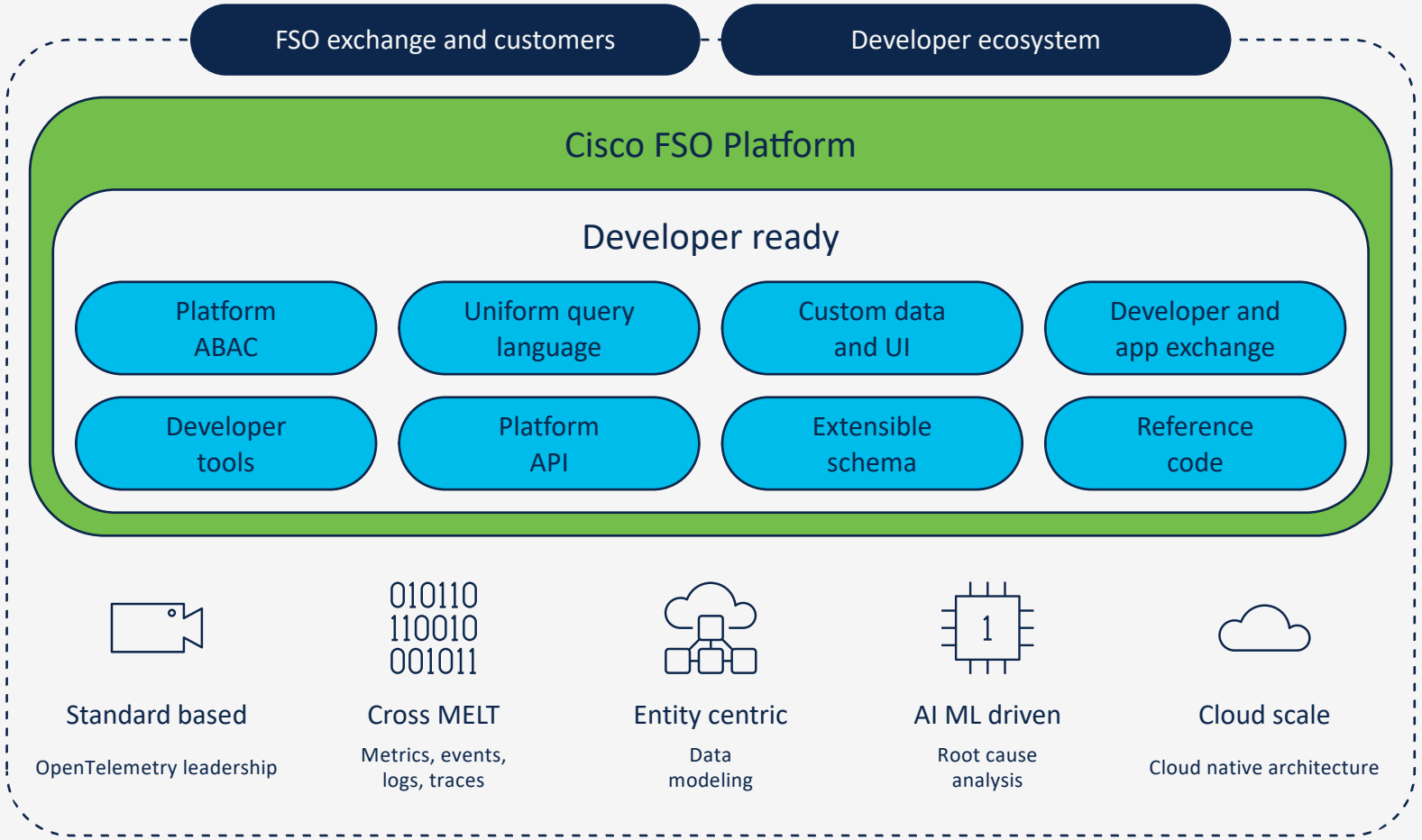
Cisco Full-Stack Observability Architektur



Cisco FSO Platform

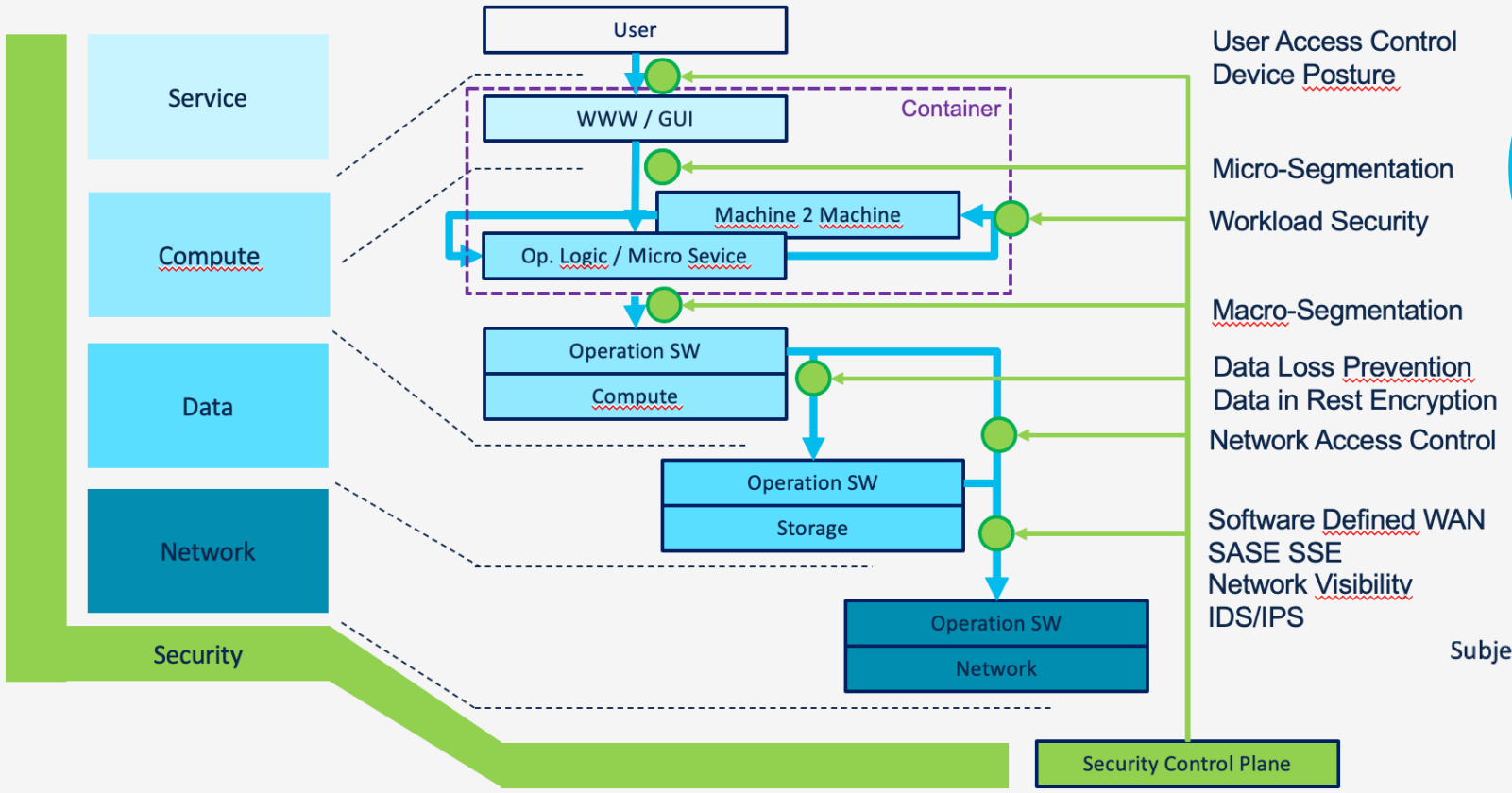
Ermöglicht neue Observability Öko-Systeme

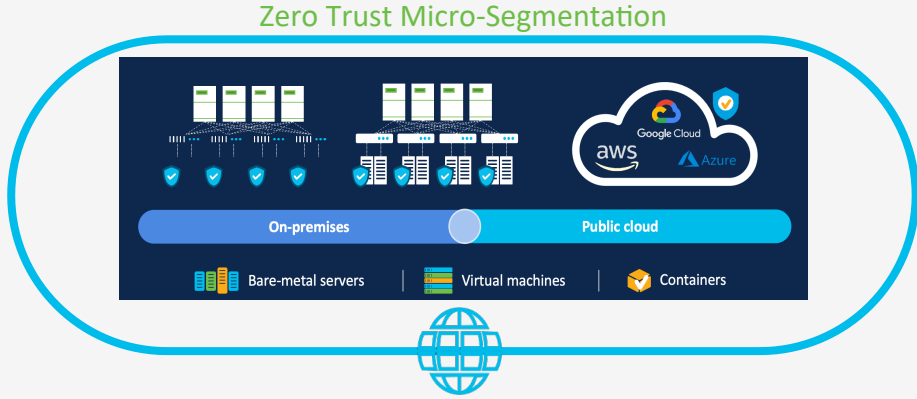
- Voll erweiterbar
- Native Unterstützung von OpenTelemetry
- Basiert auf MELT
- Bietet Unified Query Language (UQL)

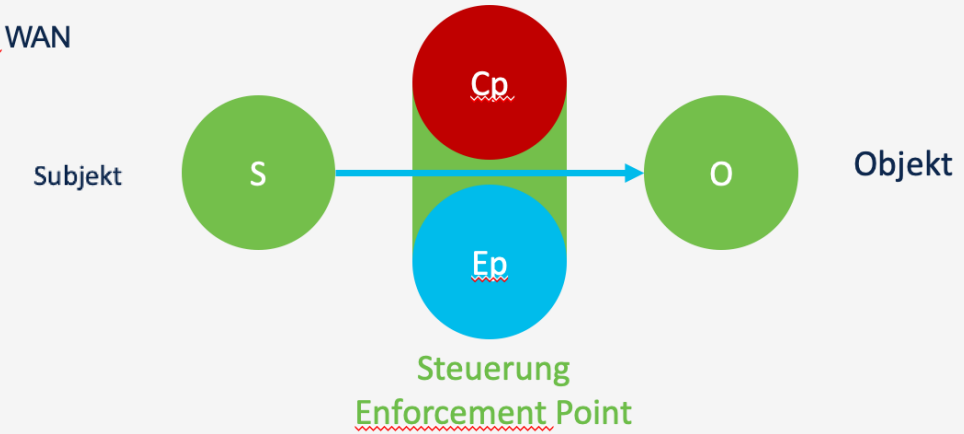


Enforcement

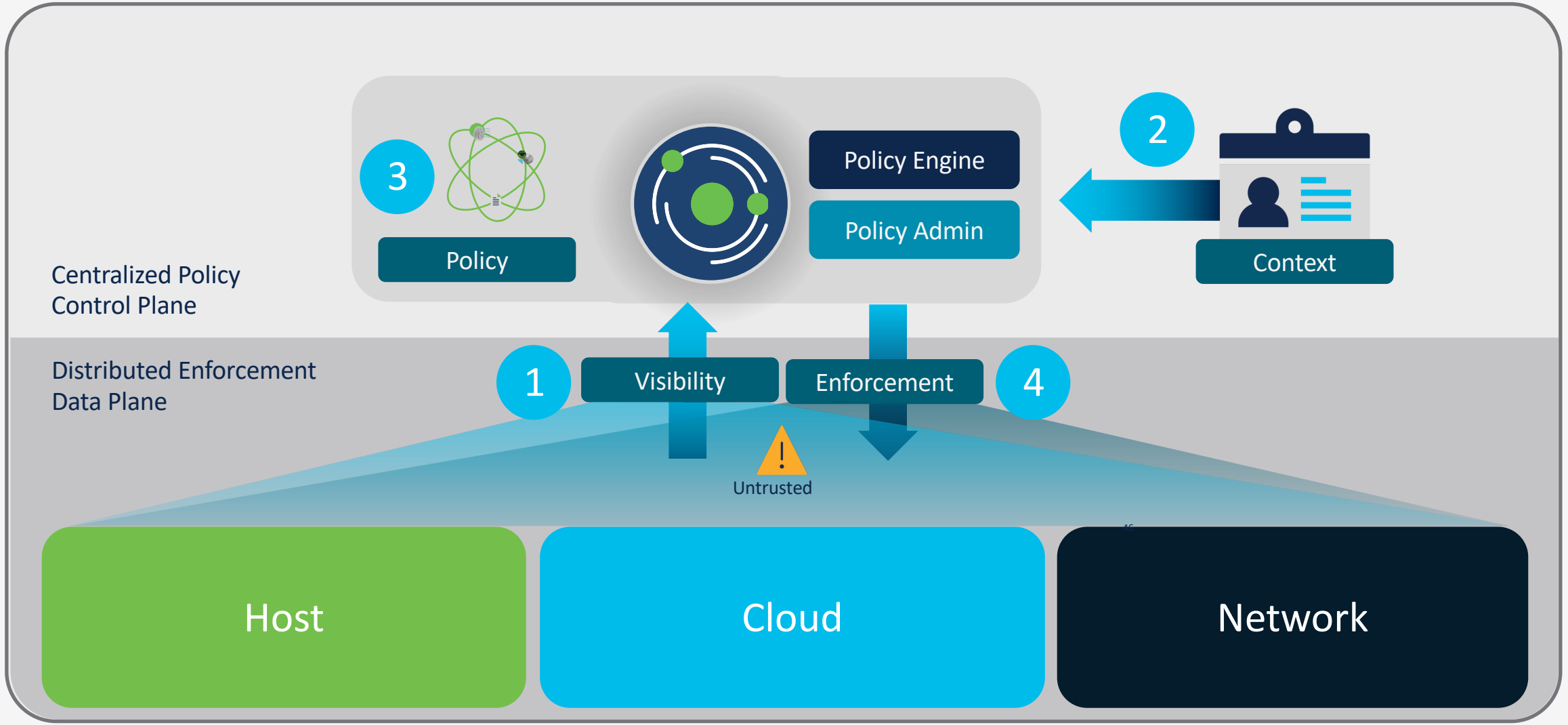
Durchsetzung der Regeln in allen Systemen







Secure Workload Ansatz für Zero Trust



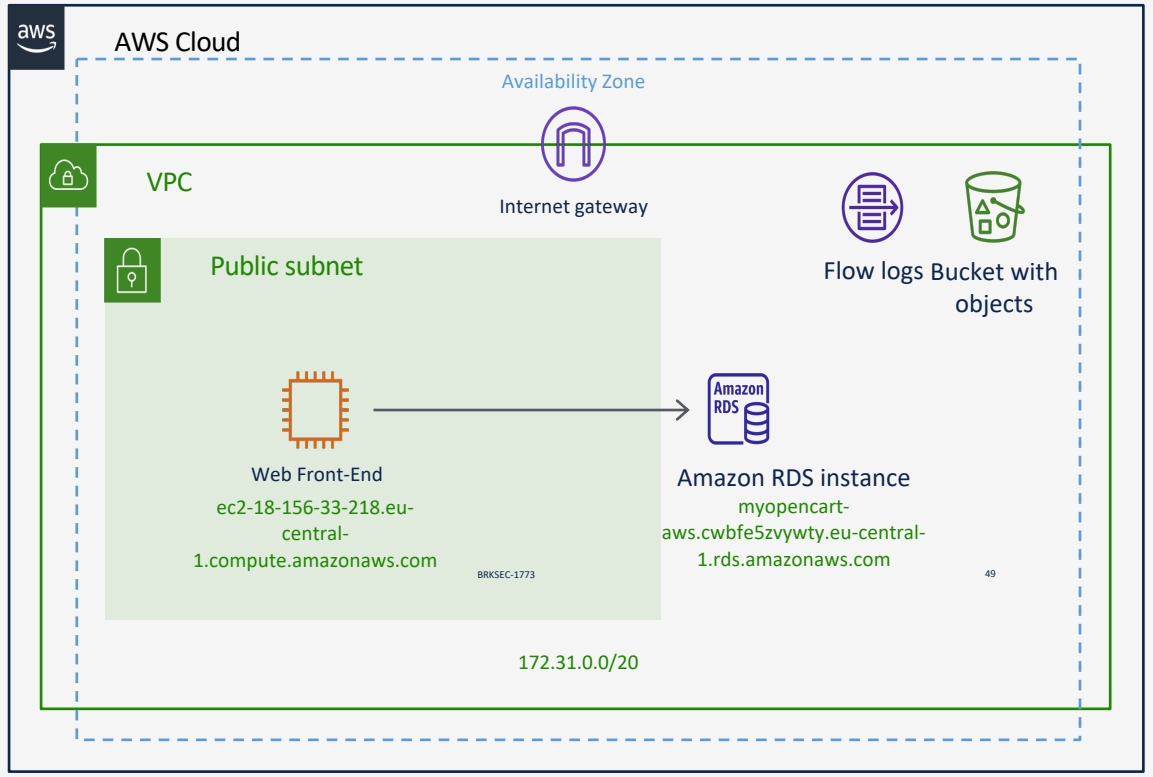
Wie nutzen Kunden Cisco Secure Workload?

Secure Workload

Applikations Visibilität	**Visibilität** in jede Workload Kommunikation der Applikation, sowohl bezogen auf den Kontext, das Verhalten der Anwendung und die Interaktion mit Nutzern und Geräten.
Zero trust Micro-Segmentierung	**Verhindert laterale Bewegung** setzt eine verteilte Firewall Policy oder “micro-perimeter” an jedem Workload durch und wendet das “least-privilege-access” Prinzip auf jeden an.
Kompliance	**Hierarchical policy model** ensures overall policy compliance while enabling teams to implement policies based on their roles, and data hygiene efforts pave the way for external compliance mandates.
Cloud Migration	**Darstellung der Applikations Abhängigkeiten (ADM)** und speichert den Lebenszyklen der Polic- Automatisierung, die komplette Historie der Applikation und zugeordneten Policy, die für die sichere Migration der Applikation in die Cloud notwendig sind

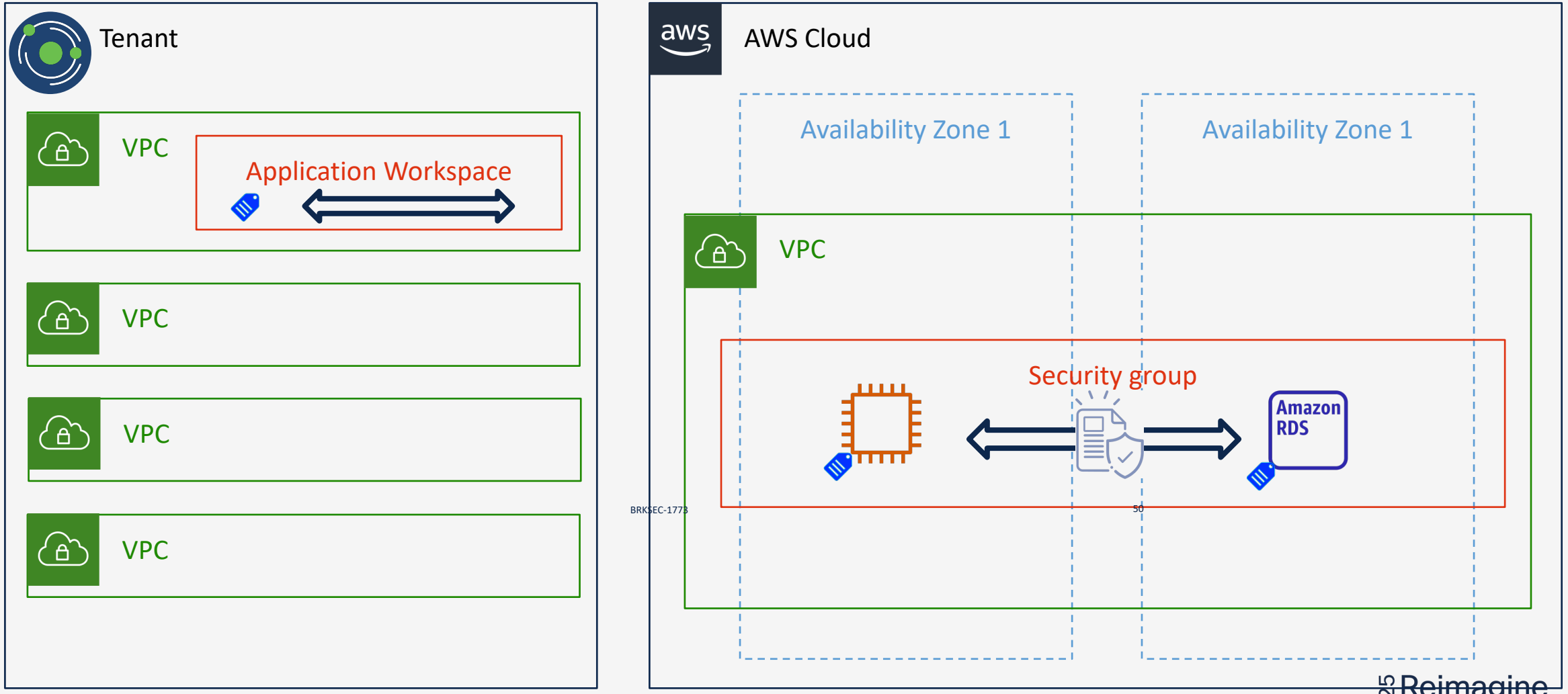
Workload Segmentierung

- Software Agenten im Workload
- Unterstützt Bare Metal, Virtual Machines, Container
- Nutzt Tags in der Cloud für Policy Zuordnung
- Überwachung über Flow-Logs
- Mikro-Segmentierung durch Security Elemente der Cloud-Service-Anbieter
- Policy Sichtberkeit für DevOps, SecOps und Netops

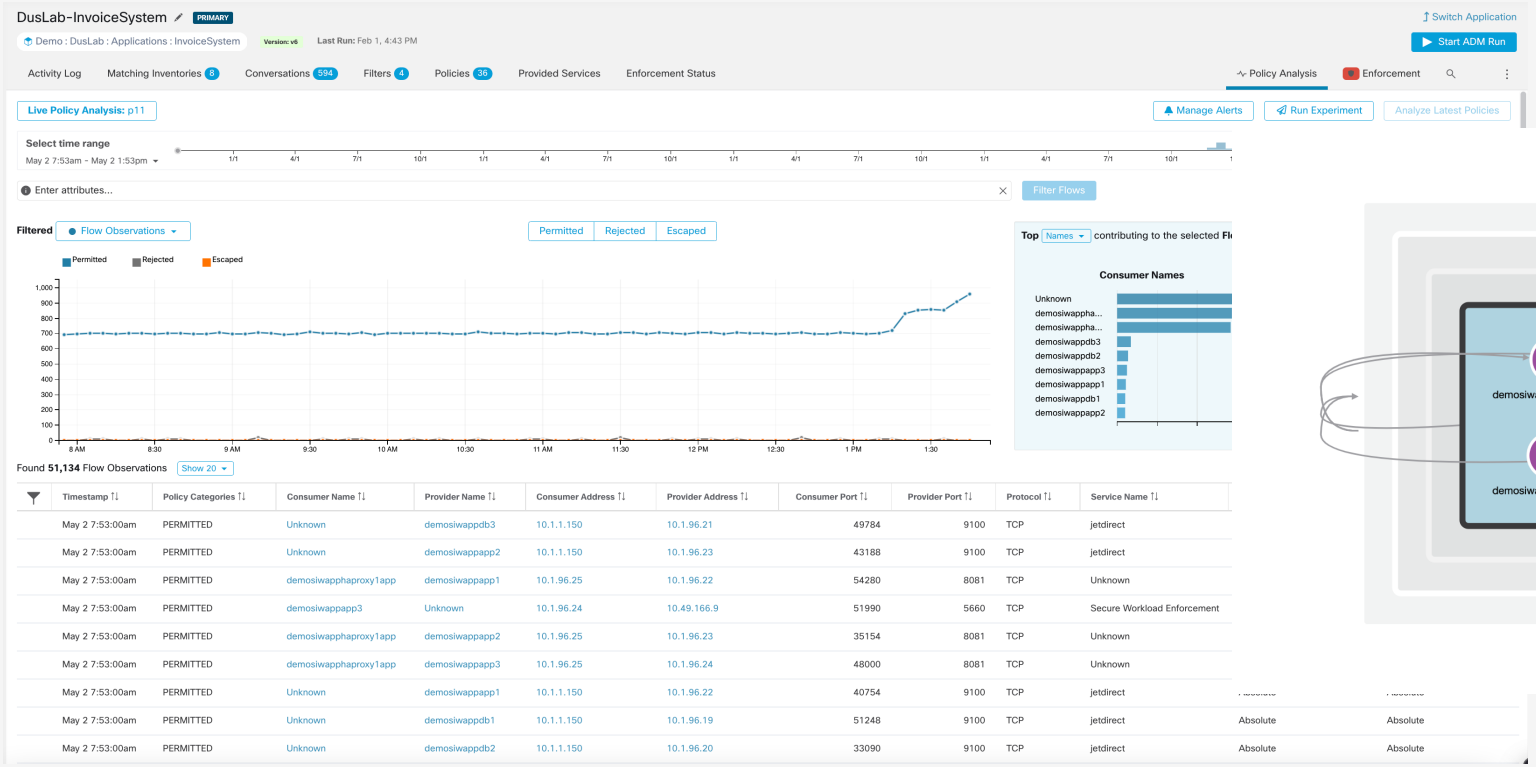


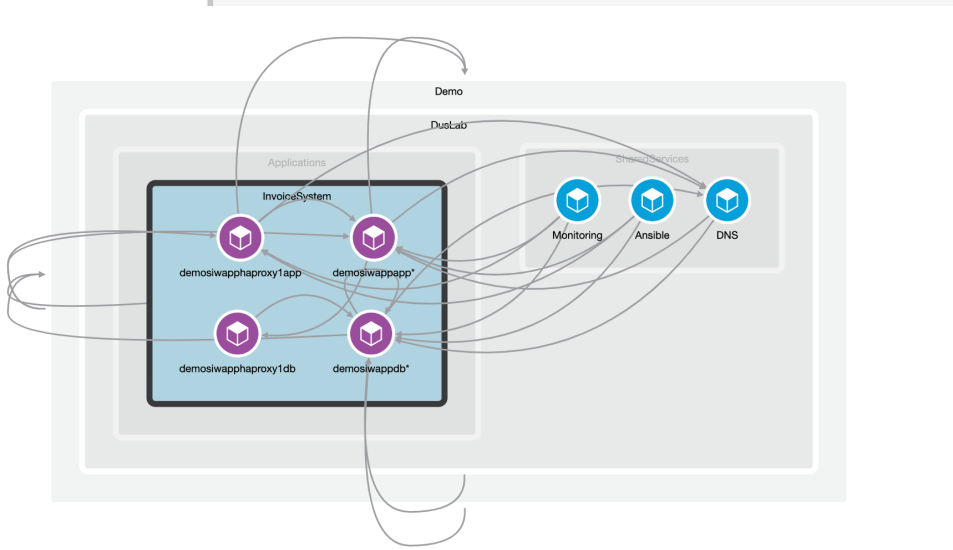
For your info & reference

Policy mapping AWS



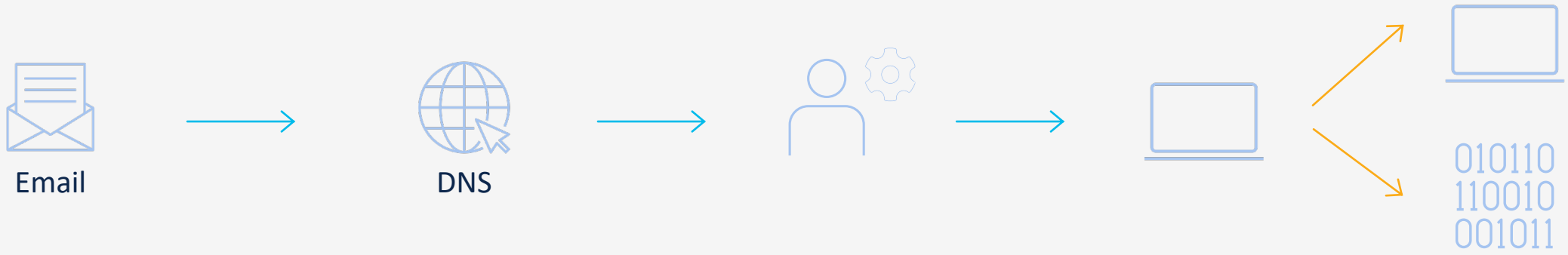
Policy Analyse und Kontrolle





Vielfalt in der Bekämpfung von Ransomware Angriffen

Most attacks use a sequence like this…



A well-tailored and personalized email causes a user to click…

Which goes to a questionable web site…

Which leads to a strange process being created locally on the user's device…

That process will connect to another machine or directly to their data

T1566: Spear phishing

T1055: Process Injection

T1189: Drive-by Compromise

T1087: Account Discovery: Domain Account

T1570: Lateral Tool Transfer

T1048: System Network Connections Discovery

Vendor A	Vendor C	Vendor E	Vendor G	Vendor D

Das XDR Versprechen

Sammlung der Telemetrie von vielen Security Tools

Anwendung von Analysen auf die gesammelten und homogenisierten Daten, um eine Schädigung zu erkennen

Reaktion und Beseitigung dieser Bösartigkeit

Building Blocks einer idealen XDR Solution?

	“Inputs”	XDR Portal / Platform	“Outputs”	Customer Consumption
Data Repository	Native and 3rd Party Telemetry Sources	Analytics & Correlation Engine	Incident Management	Customer Managed
	Threat Intelligence	Response Actions and Workflow Automation	Incident Response	
	Asset Context (device, user)	Case Management	Threat Hunting	Managed Detection & Response

Cisco XDR Lösung

Cisco Ansatz für XDR

Mehr erkennen, schneller agieren, Produktivität erhöhen, Wiederstandsfähigkeit aufbauen

Detect the most sophisticated threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments

Act on what truly matters, faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

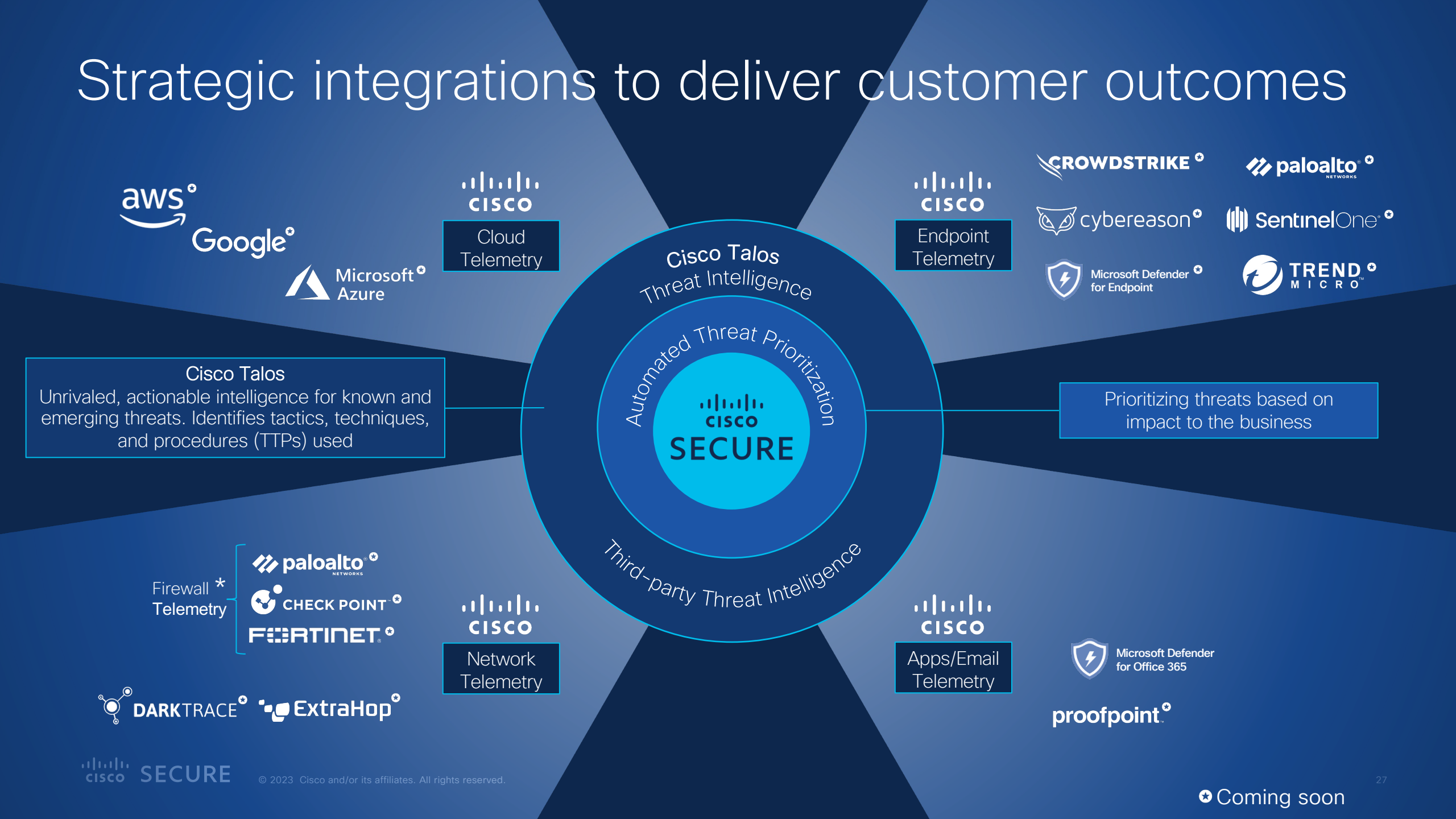
Elevate productivity

- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

Build resilience

- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

Strategic integrations to deliver customer outcomes



✪ Coming soon

Collaboration

Co-Development von Lösungen im GovTech Campus

- Win-Win für alle
- Know-How Aufbau
- Schnelle Umsetzung der Use-Cases
- Industrie Standards nutzten
- Standardisierung anstossen
- Open-Source setzt Industrie-Standards ergänzend zu IETF-IEEE
- Plattformen nutzen
- Erweitern, bereichern, spezifische Use-cases entwickeln

GovTech Campus Deutschland

Zusammenarbeit mit Cisco Open-Source Program Office

Security

- APIClarity, KubeClarity, OpenClarity
- GitBOM
- Bank-Vaults
- Dex
- API Insights

Connectivity

- Network Service Mesh
- Media Service Mesh
- FD.io
- Cloud native Operators

Data

- MindMeld
- BitBroker
- Flame

Contributions

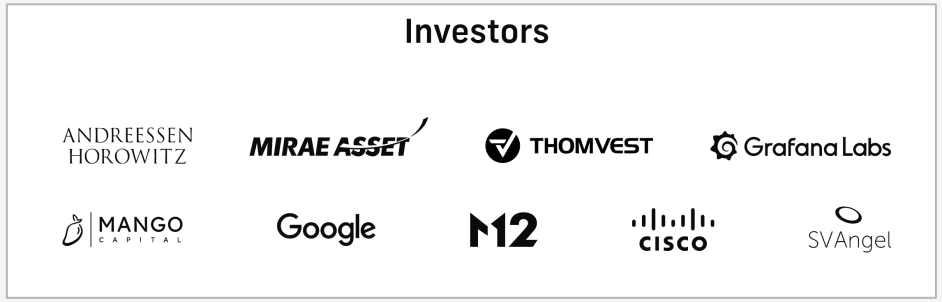
- OpenTelemetry
- KubeFlow
- Istio

Mitarbeit in Open-Source Projekten

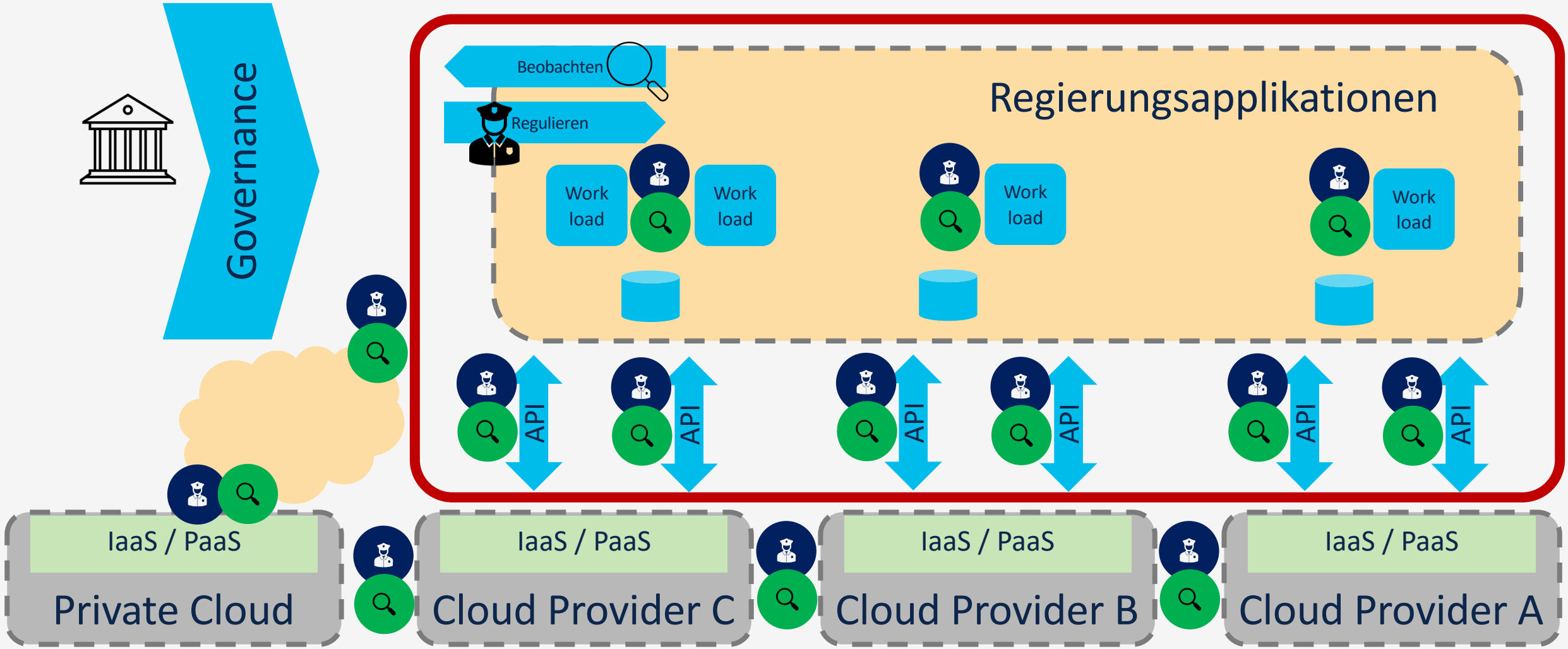
Jüngste Cisco Acquisition Isovalent

ISOVALENT

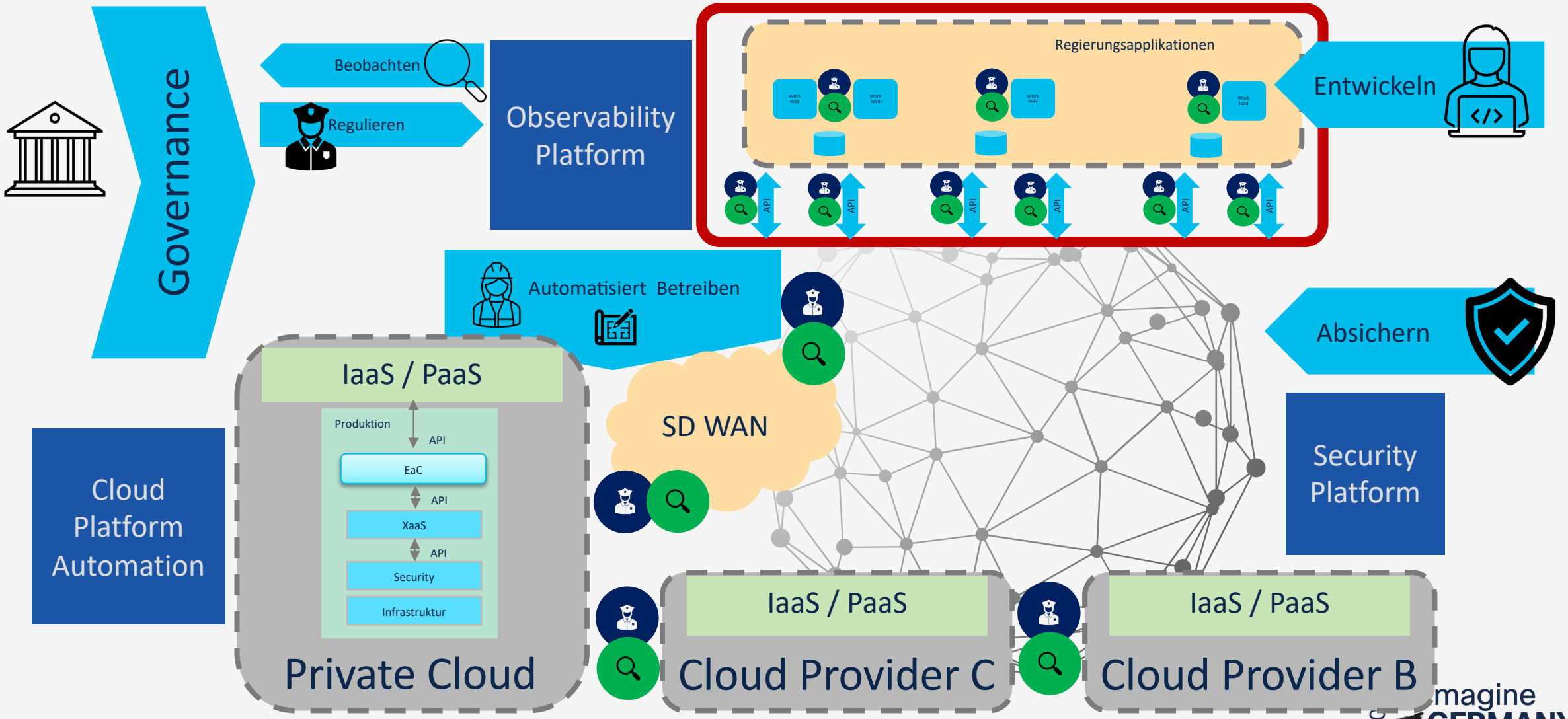
"As initial talks with Cisco sparked, we didn't have to ask what a potential acquisition would mean for Cilium, Tetragon, and our other projects. It was clear from the beginning that Cisco came to the table with a clear vision to double down on our products and our open-source strategy with a strong commitment to our open-source projects. Open source has become the way to standardize technology and cloud native infrastructure is no exception."
https://isovalent.com/blog/post/cisco-acquires-isovalent/



Ein Regelwerk in der Multi-Cloud - 4



Zielbild Multi-Cloud



https://www.cisco.com/c/de_de/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-dvc-germany.html

Future ***Ready***

2025 Reimagine GERMANY