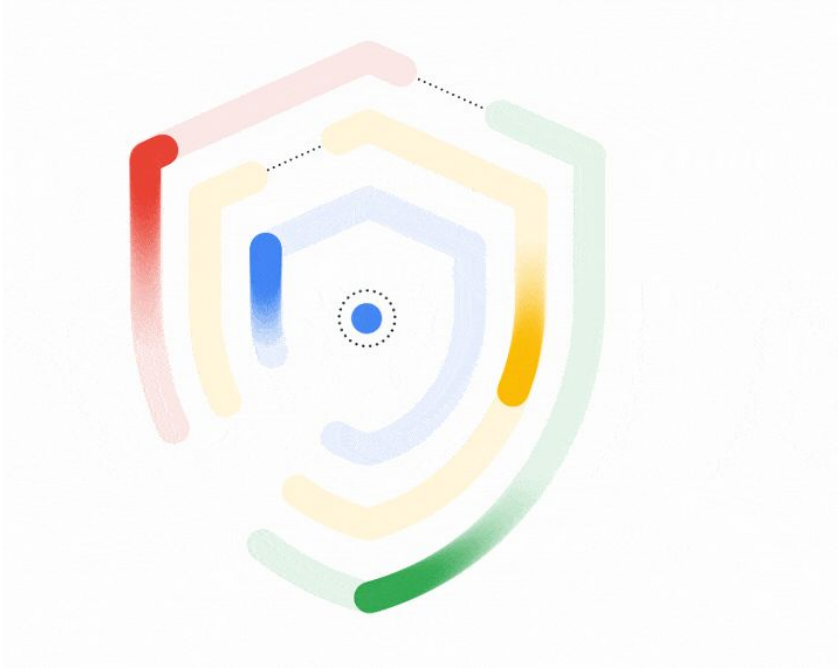
Google Cloud

Digitale Souveränität nach deutschen Maßstäben

DOK Forum 2023



September 2023

Agenda

1. Die Grundsäulen digitaler Souveränität aus Sicht eines globalen Hyperscalers
2. “Quadratur des Kreises” - regulatorische Konformität vs. Innovationsfähigkeit, ein Widerspruch?
3. Souveräne hybride Clouds - Das Google Lösungsportfolio für souveräne Cloud Transformation

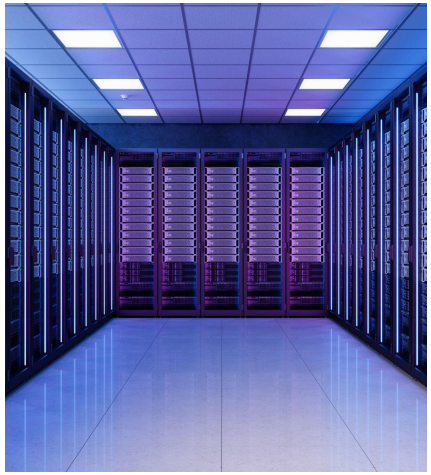
Die Entwicklung der Cloud von der Virtualisierung zur digitalen Transformation

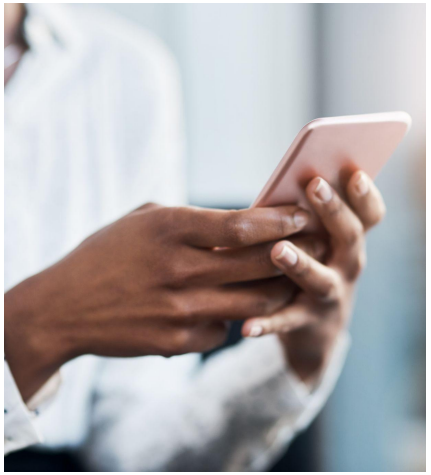
Transformation Cloud Ära
Transformation im gesamten Unternehmen

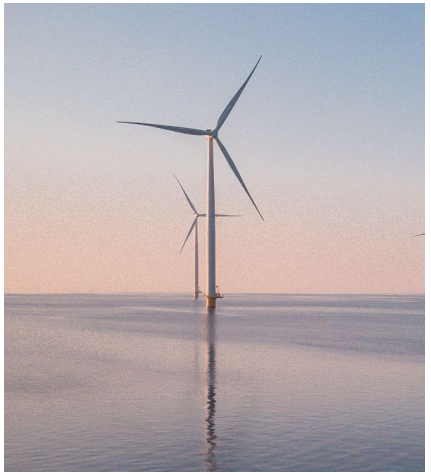
Infrastruktur Cloud Ära
Applikationsinfrastruktur aus der Cloud

VM cloud Ära
Start in die Cloud durch Virtualisierung von Rechenleistung

Public clouds ermöglichen und beschleunigen die digitale Transformation







Skalierbarkeit

Sicherheit

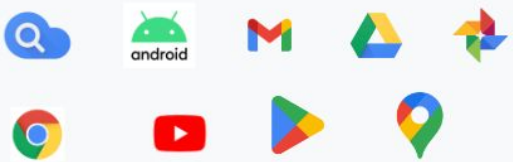
Innovation

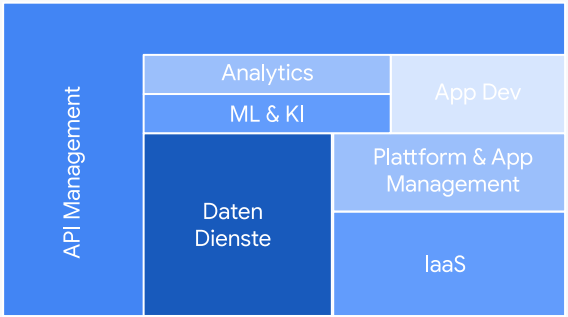
Nachhaltigkeit

Google Cloud

Google Cloud bringt das Beste von Google zu Unternehmen

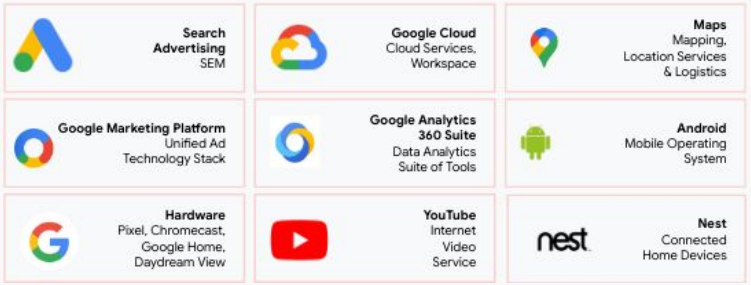
Anwendungen mit Milliarden von Nutzern





Hochleistungs-Hyperscaler für Unternehmen...

...mit nativer Integration in:



Google Cloud

Oder anders gesagt - “Alles super in der Cloud!”

Alle wollen in die Cloud ...

… oder doch nicht alle?

Vertrauen ist die Basis für die Nutzung von Cloud-Diensten

Das Bedürfnis nach Souveränität geht über den reinen Datenschutz hinaus

Sicherheit & Kontrolle

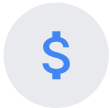
Kann ich mehr Kontrolle über meine Daten und Abläufe haben?

Wie setze ich ergänzende Datenschutzmaßnahmen ein, wie sie in den Schrems-Urteilen empfohlen werden?

Ökonomisch

Kann ich in einem Ökosystem mit gemeinsamen Werten arbeiten, dem ich vertraue?

Muss ich ein Lock-in- und Konzentrationsrisiko durch ausländische Anbieter befürchten?

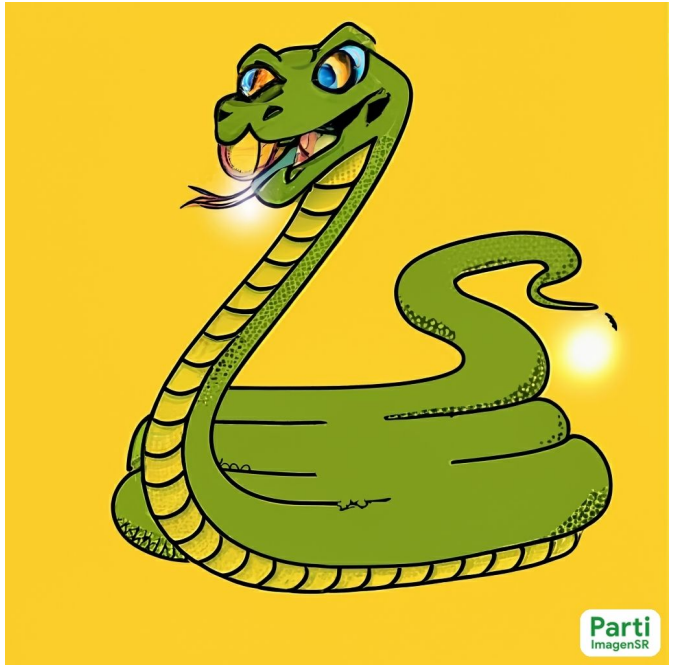


Geopolitisch

Die zunehmende globale Instabilität erfordert die Planung für disruptivere Szenarien.

Wie stelle ich die Überlebensfähigkeit im Falle einer erzwungenen Trennung sicher?

Vertrauensbildende Maßnahmen also? Oder doch besser Kontrolle?



Quelle: Vertrauen - Wie wir es gewinnen. (Prof. Dr. Niels Birnbaumer)

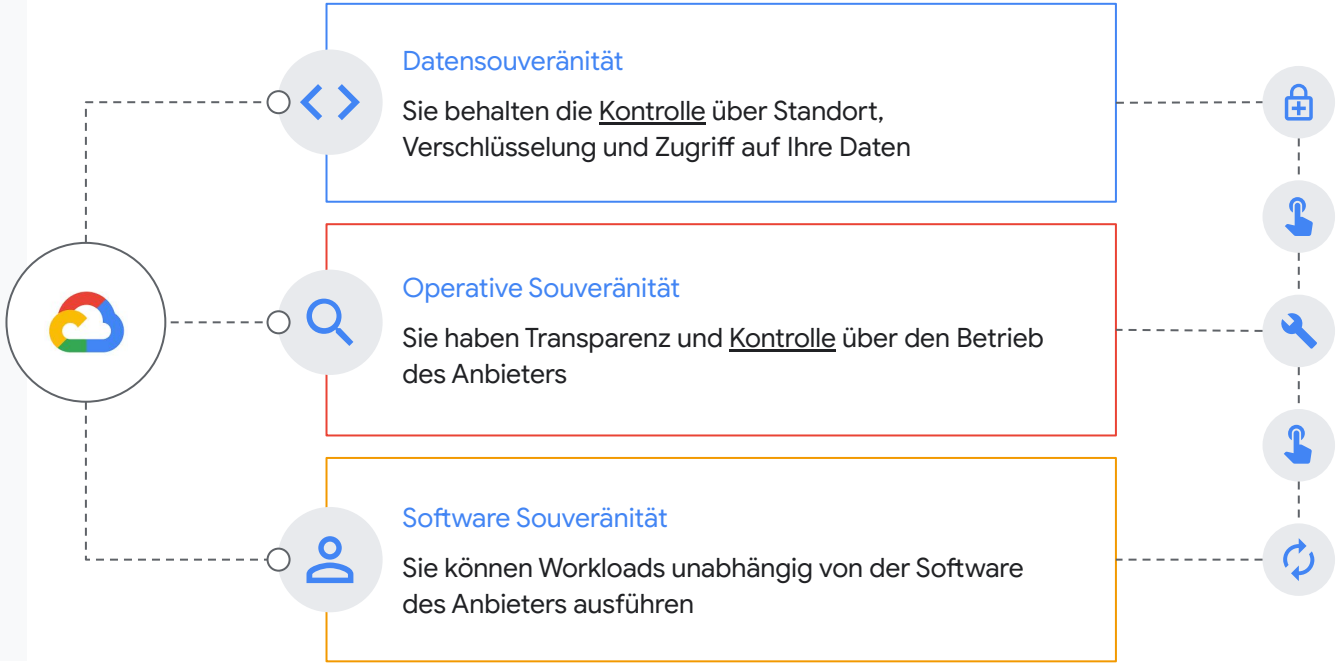
Wer anderen sein Vertrauen schenkt, macht sich verletzlich. Denn womöglich wird er verraten, belogen oder betrogen.

Es vergeht kaum ein Tag, an dem nicht irgendeine Institution, eine Partei oder eine Firma, die Konsumprodukte herstellt, darum wirbt, ja geradezu fleht, ihr Vertrauen zu schenken.

Der Vertrauende gibt Kontrolle ab, er hat keinen Einfluss auf das, was passiert. Er kann nur annehmen, dass alles in seinem Sinne geschieht. Vertrauen ist also ein riskantes Gefühl. Sein Gegenspieler ist die Angst. Denn auch die kann sich entfalten, wenn wir nicht die volle Kontrolle haben.

Die viel zitierte digitale Souveränität. Was hat es damit auf sich?

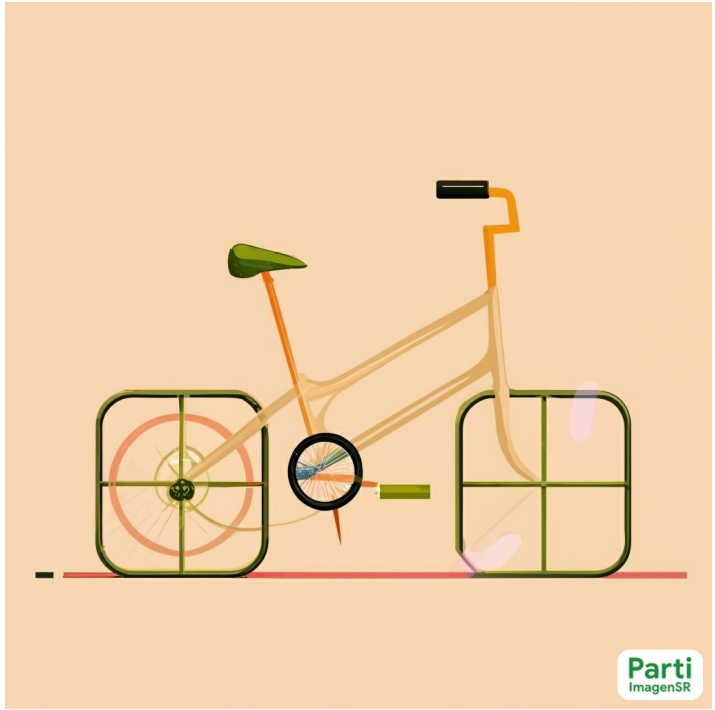
Unsere Vision von Souveränität geht über den Datenschutz hinaus.



Agenda

1. Die Grundsäulen digitaler Souveränität aus Sicht eines globalen Hyperscalers
2. “Quadratur des Kreises” - regulatorische Konformität vs. Innovationsfähigkeit, ein Widerspruch?
3. Souveräne hybride Clouds - Das Google Lösungsportfolio für souveräne Cloud Transformation

Gibt es die eine souveräne Cloud, die jede regulatorische Anforderung erfüllt und die volle Innovationskraft bietet?



Google gibt (die) Kontrolle an Kunden und Partner ab.

Wählen und kombinieren Sie unterschiedliche Souveränitäts-Level für Ihre Workloads

		Technische Features (features)	Typischer Use Case
Assured Workloads (durch Kunde) (verfügbar) PL, BE, DE, NL, I, FR, ES, FI, CA, USA, JP, ISR	Auf GCP	Data Residency Controls Lokales support Personal Access Transparency Controls External Key Management & Key Access Justification	**Alle Workloads**, die zusätzliche Datenschutzmaßnahmen und Aufenthaltskontrollen erfordern
Sovereign Controls (durch T-Systems) (verfügbar in ausgewählten Märkten wie DE und FR)	Auf GCP	Managed External Key Management & Key Access Justification Optional Partner services (e.g, BYOID)	**Ähnlich wie AW** und zusätzlicher Datenschutz als gemanagter Service (vom Partner)
Trusted Partner Cloud (Geplant in DE und FR für Ende 2024)	Separiert	Dedizierte, separierte Infrastruktur. Betrieb und Support durch Partner. Nationale Zertifizierungen.	Kritische Workloads, die besonderen Vorschriften wie dem Sozial-gesetzbuch oder VSnfD unterliegen.
Hosted Cloud (T-Systems oder Kunde) (verfügbar)	Air Gapped	Cloud native Workloads Betrieb durch Partner oder Kunden. Komplett isolierter (air-gapped) Stack	Geheimdienste, Verteidigung, öffentlicher Sektor mit **“air-gapped” Anforderungen.**

Welche souveräne Cloud für welche Workloads?

Public Cloud (Google)

Kern-Controls in der Public Cloud: Zugriffskontrolle, Verschlüsselung, Datenresidenz

Sovereign Controls (Partner)
Assured Workloads (Kunde)

Sovereignty Controls über externe Verschlüsselung, Service deployment location und zusätzliche Partner Services (Logs Reviews, BYOID)

Sovereign Trusted Partner Cloud

Operative Souveränität. Betrieb des Cloud Clusters durch lokale Partner für behördliche VSnfD Anforderungen oder Sozialdaten.

Distributed Cloud (Kunde oder Partner)

Google Distributed Cloud Hosted (Google or partner operated)
Bietet survivability und “air gapped” Betrieb

Google Cloud

Assured Workloads und Sovereign Controls im Detail

Google Cloud

Assured Workloads (Google) und Sovereign Controls durch T-Systems basieren auf derselben Technologie

Google Cloud Platform

Standard Google Cloud Org

Ergänzende Angebote für digitale Souveränität

Assured Workloads durch Google

Kunden gemanagte Datensouveränität

- Kein zusätzlicher Papierkram bzw. Beteiligung Dritter
- Flexibilität in der Auswahl der Region und Kontrollen
- Externes Schlüsselmanagement in der Verantwortung des Kunden

Sovereign Controls durch T-Systems

Partner gemanagte Datensouveränität

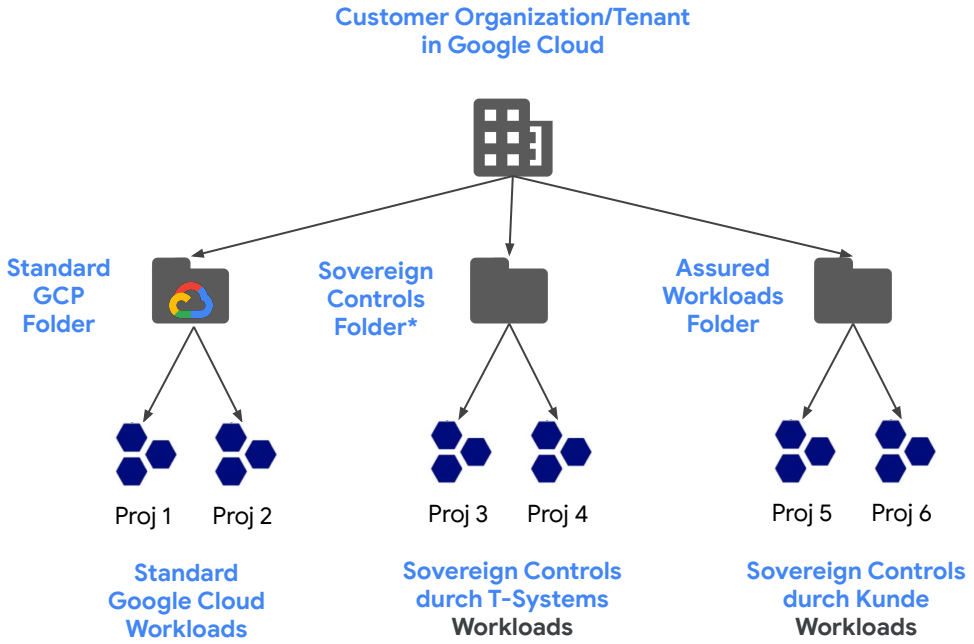
- Vom Partner verwaltete externe Schlüsselinfrastruktur
- Erweiterte, durch Partner gemanagte Kontrollen für eine komfortable Erfüllung von regulatorischen Auflagen.

Google Cloud

Sovereign Controls sind ein Ordner in der Landingzone eines Kunden

Souveräne Workloads werden in vorhandenen Organisationen innerhalb eines souveränen Ordners bereitgestellt: Alle Projekte in diesem souveränen Ordner “erben” die entsprechenden Sovereign-Controls.

Kunden können souveräne Workloads ohne zusätzlichen Verwaltungsaufwand bereitstellen.



Bei Assured Workloads werden dem Kunden erweiterte Kontrollmechanismen auf der Google Cloud übergeben.

Assured Workloads integriert erweiterte Kontrollen in bestehende Produkte und Dienste

Kontrolle über die Daten Residenz	*Datenresidenzkontrollen für globale APIs und Regionalisierung "at rest" und "in transit". Die Region kann hier frei gewählt werden.*
Datenzugriffskontrolle	*Datenzugriffspfade werden zugeordnet und Zugriffskontrollen werden eingerichtet, um sie basierend auf der vom Kunden gewählten Compliance einzuschränken.*
Schlüsselmanagement	*Kunden haben die Möglichkeit, ihre Schlüssel in oder außerhalb von Google Cloud zu verwalten, um ihren Sicherheits- und Compliance-Anforderungen gerecht zu werden.*
Zugriffskontrolle und -transparenz	*Der administrative Zugriff auf Kundendaten und Workloads wird protokolliert, geprüft und nur unter vordefinierten Supportbedingungen gestattet*
Begrenzung auf konforme Services	*Entwickler können ausschließlich konforme Produkte und Dienste verwenden*

Die technische Realisierung wird durch vertragliche Verpflichtungen und Transparenz ergänzt

Google Cloud

Sovereign Controls von T-Systems bieten gemanagten Schutz für die Plattformkontrollen von Google Cloud

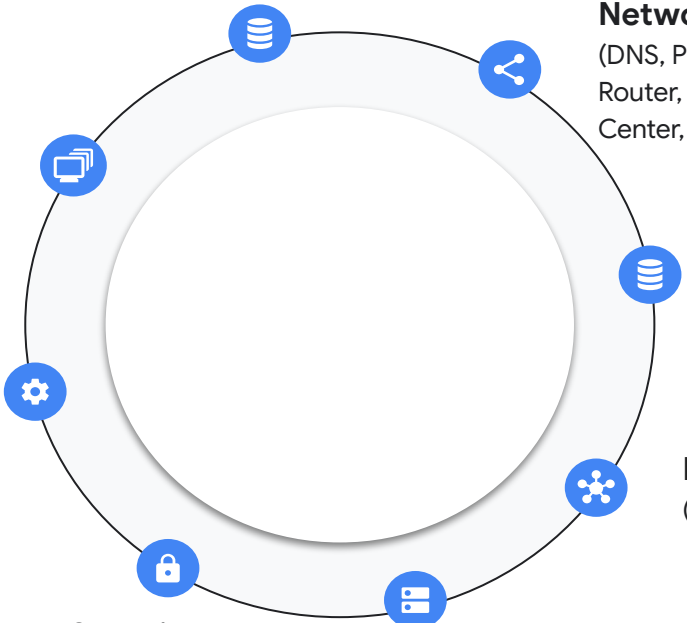
Sovereign Controls durch T-Systems auf Google Cloud

Kontrolle über die Daten Residenz	*Kundendaten werden "at rest" in der deutschen Region von Google Cloud gespeichert und dürfen nicht außerhalb des Landes übertragen werden*
Localer Support	*Personalzugang und Kundensupport sind auf EU-Personen mit Sitz in der EU beschränkt*
Externe Verschlüsselung	*Schlüssel zur Verschlüsselung der Kundendaten werden von T-Systems gespeichert und verwaltet*
Zugriffskontrolle und -transparenz	*Der administrative Zugriff auf Kundendaten und Workloads wird protokolliert, geprüft und nur unter vordefinierten Bedingungen gestattet*
Identity Management	*Kundenidentitäten werden von T-Systems verwaltet*
Security operations center	*T-Systems bietet eine zusätzliche Überwachung des Cloud-Betriebs*

*planned

T-Systems | Google Cloud

Cloud Services mit Sovereign Controls



Analytics
(Big Query, Dataflow, Dataproc)

Networking
(DNS, Private network, Interconnect, NAT, Router, Load balancing, Network Connectivity Center, VPC, VPN, Identity-Aware Proxy)

Compute
(Compute Engine)

Storage
Cloud Storage, Persistent Disk

Operations
(Composer, Pubsub, Logging)

Kubernetes
(Kubernetes Engine)

Security
(Key management, IAM, audit logging, EKM, HSM)

Databases
(BigTable, Spanner, SQL)

Sovereign Controls unterstützt die beliebtesten Google Cloud Features und es werden stetig mehr ...

Sovereign Controls bieten Kontrollen für die beliebtesten Google Cloud-Dienste

Sovereign Controls auf Google Cloud

Verfügbare Services

- Artifact Registry
- BigQuery
- BigTable
- Cloud Composer
- Cloud console
- Cloud DNS
- Cloud IAM
- Cloud IAP
- Cloud Interconnect
- Cloud Load Balancing
- Cloud Logging
- Cloud NAT
- Cloud Router
- Cloud Spanner
- Cloud SQL
- Cloud Storage
- Compute Engine
- Dataflow
- Dataproc
- Key Management
- Kubernetes Engine
- Network Connectivity Center
- Persistent Disk
- Pub/Sub
- VPC-SC
- VPN

Service Roadmap

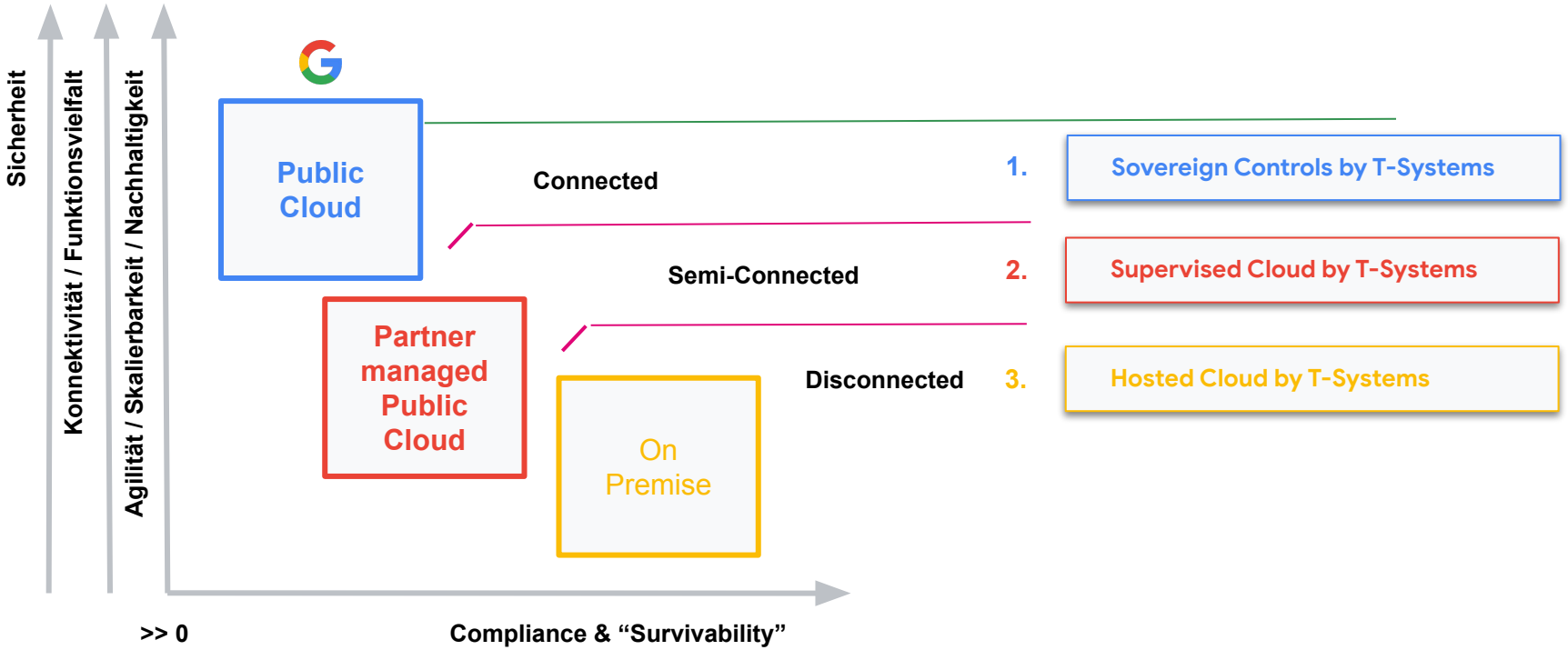
- Apigee
- Backup for GKE
- Cloud Armor
- Cloud Filestore
- Cloud Memorystore
- Cloud Monitoring
- Cloud Run
- Secret Manager
- Security Command Center
- Vertex AI
- ...und viele mehr

T-Systems | Google Cloud

Agenda

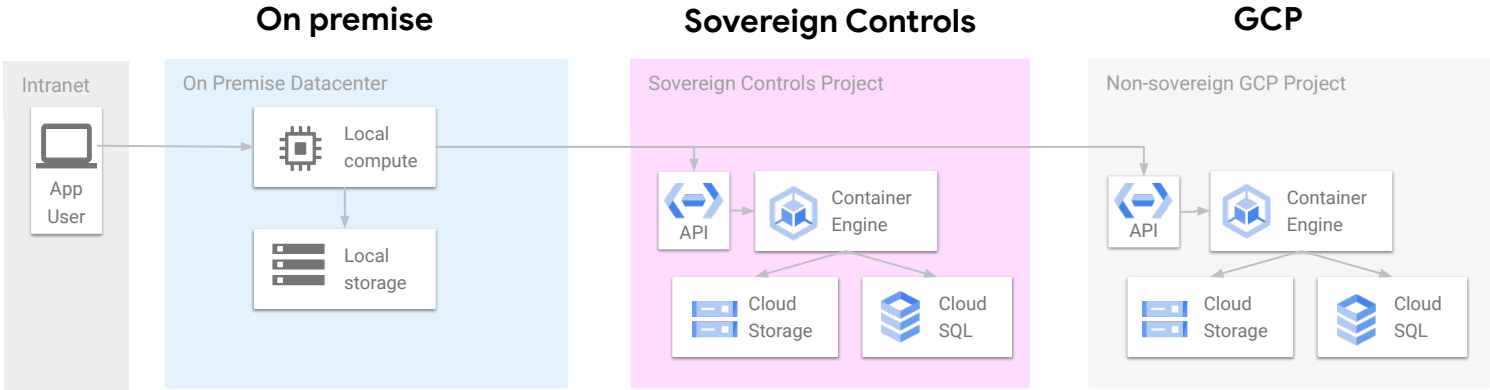
1. Die Grundsäulen digitaler Souveränität aus Sicht eines globalen Hyperscalers
2. “Quadratur des Kreises” - regulatorische Konformität vs. Innovationsfähigkeit, ein Widerspruch?
3. Souveräne hybride Clouds - Das Google Lösungsportfolio für souveräne Cloud Transformation

Hybride souveräne Cloudlösungen



Design von hybriden Souveränen Workloads

Für souveräne Workloads können Komponenten je nach Sensitivität auf mehreren Plattformen bereitgestellt werden

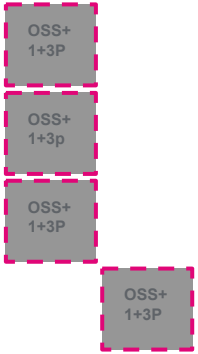


Umfang	Komponenten, die hochsensible Daten verarbeiten und speichern	Sensible Daten sind in der Cloud nur in Sovereign Controls erlaubt	Nicht sensible Daten (z. B. als intern, aber nicht vertraulich eingestuft).
Feature	Erfüllung höchster Souveränitätsanforderungen	Datensouveränität, Skalierbarkeit und verwaltete Dienste der Cloud	Bester Preis und Skalierbarkeit Datenresidenz für Schlüsseldienste möglich

Google Cloud

Hybrid Sovereign Digital Applications

(Kern) Funktional



OSS*-basierter Anwendungskern, der vollständig „getrennt“ betrieben wird und in der „**Hosted Cloud by TSI**“ gehostet wird (möglicherweise erweitert durch Google (1P) + Lösungen von Drittanbietern (3P) (z. B. DBs)). Kontinuierlicher Betrieb im Falle eines „Black Swan“-Ereignisses.

Fortgeschritten

Erweiterte Anwendungen mit **OSS- und Google Cloud Native-basierten** Komponenten, die auf „**Sovereign Controls by TSI**“ betrieben werden (z. B. Effizienz-steigerungen, erweiterte Analysen). Einige vollständig portable (Kern-)Funktionsdienste können hier auch betrieben werden (Warm- oder Hot-Standby), um von den elastischen Skalierungsmodellen und der Sicherheit der Public Cloud zu profitieren.

‘State of the Art’

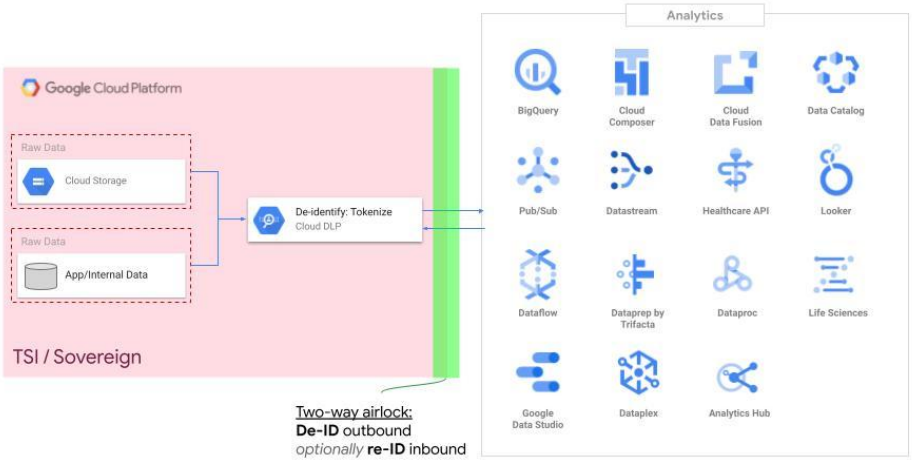
Hinzufügen weiterer innovativer Google Cloud-Dienste. Diese könnten beispielsweise dazu beitragen, das Benutzererlebnis zu verbessern, **würden jedoch die Kernfunktionalitäten der Anwendung nicht beeinträchtigen.**

* OSS = Open Source Software

Google Cloud

Data Loss Prevention für hybride Use Cases

Beispiel für eine hybride Architektur/ Lösung



1. Aufnahme personenbezogener Daten (PII), die Bilder enthalten, in einen sicheren, souveränen Google Cloud Storage (GCS)-Bucket
2. Verwendung des Data Loss Prevention (DLP)-Dienstes für diese Bilddaten, um personenbezogene Daten (PII) zu entfernen
3. Nutzung der weiteren Analyse dieser anonymisierten Bilder in nachgelagerten Analysediensten der Google Cloud Plattform.

Erweiterte souveräne Use Cases

Industrie	Use Case
Banken / Versicherungen	Kfz-Versicherungsansprüche – Fotos des Schadens werden an die Versicherungsgesellschaft gesendet und ein ML-Modell schätzt die Schadenskosten.
Transport / Logistik	Beschädigte Pakete, Frachtcontainer und beschädigte Waren werden mithilfe eines ML-Modells identifiziert und an einen speziellen Prozess weitergeleitet.
Medizin	Gefährliche Unregelmäßigkeiten werden in medialen Bildern erkannt (z. B. Krebs und andere Krankheiten)
…	…

Hybride architekturen können den Funktionsumfang souveräner Umgebungen entscheidend erweitern.

Vielen Dank!