



Cloud-Betriebsmodell: Das volle Potenzial freisetzen

Auf dem schnellsten Weg zu Mehrwert im modernen Multi-Cloud-Rechenzentrum



Executive Summary

Jetzt soll die Cloud zeigen, was sie leisten kann. Eine Unternehmens-IT, die im Zeitalter von Multi-Clouds im digitalen Wandel bestehen will, muss sich von ITIL-Gatekeeping zu DevOps-Spitzenleistungen mit verteilten Selfservice-Prozessen entwickeln.

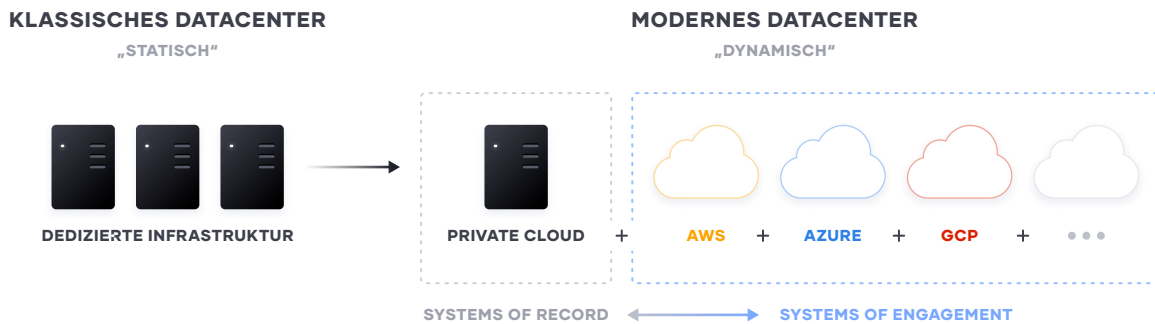
Für die meisten Unternehmen heißt digitale Transformation: schneller und skalierbar neuen Mehrwert und mehr Kundenwert schaffen. Für die Unternehmens-IT bedeutet das einen Wandel von der Kostenoptimierung zur Geschwindigkeitsoptimierung. Die Cloud ist ein unverzichtbarer Bestandteil dieser Entwicklung, da sie die schnelle Bereitstellung von On-Demand-Diensten ermöglicht und schier grenzenlos skalierbar ist.

Um den Cloud-Mehrwert so schnell wie möglich freizusetzen, müssen sich Unternehmen umsehen, wie sie die Anwendungsbereitstellung über alle Cloud-Ebenen hinweg am besten organisieren: indem sie auf Cloud-Operating-Modelle umstellen und Mitarbeiter, Prozesse und Tools darauf abstimmen.

In diesem Whitepaper sehen wir uns das Cloud-Betriebsmodell genauer an und stellen Lösungen für IT-Teams vor, mit denen sie dieses Modell in den Bereichen Infrastruktur, Sicherheit, Networking und Anwendungsbereitstellung erfolgreich umsetzen.

Umstieg auf Multi-Cloud-Rechenzentren

Der Wechsel zu Cloud- und Multi-Cloud-Umgebungen ist nichts weniger als ein Generationenwechsel in der IT. Es ist der Wechsel von dedizierten Servern im eigenen Rechenzentrum zu einem Pool von Rechenleistung, die auf Abruf verfügbar ist. Die meisten Unternehmen haben mit einem einzigen Cloud-Anbieter begonnen. Die meisten der Global-2000-Organisationen werden aber mehr als eine Cloud-Umgebung nutzen, ob strategisch oder durch Zusammenschlüsse und Übernahmen.



Die Cloud bietet neue Chancen, Geschwindigkeit und Volumen zu optimieren, und zwar bei den Anwendungen, die Kunden und Nutzer direkt handhaben (den sogenannten „Systems of Engagement“). Diese neuen Apps sind für die Kunden das primäre Mittel der geschäftlichen Interaktion – und sie sind bestens für die Cloud-Bereitstellung geeignet, weil sie ...

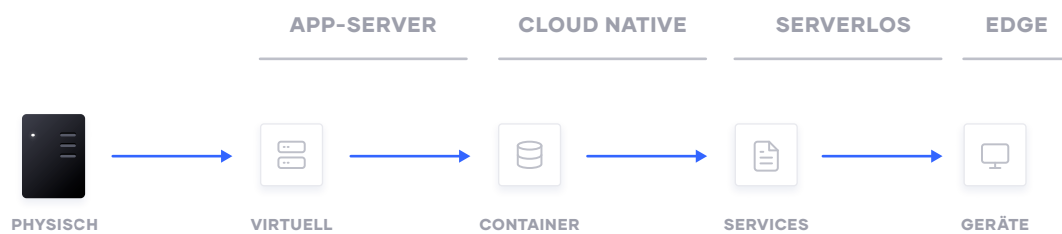
- ... dynamisch genutzt werden und oft kurzfristig um ganze Größenordnungen angepasst werden müssen;
- ... eine schnelle Erstellung und Iterierung erfordern. Viele Workloads sind naturgemäß nur kurzlebig, d. h. sie bieten ein spezielles Erlebnis rund um ein Event oder eine Kampagne.

In der Regel müssen diese Dialogsysteme jedoch an vorhandene Informationsspeicher angebunden werden (die sogenannten „Systems of Record“): an Datenbanken und interne Anwendungen, die oft weiterhin im bestehenden Rechenzentrum liegen. Im Endeffekt arbeiten Unternehmen mit einem Hybrid – einem Mix aus öffentlichen und privaten Cloud-Umgebungen.

Die Herausforderung besteht dann in der konsistenten Übertragung der Anwendungen in die Cloud und der möglichst reibungslosen Zusammenarbeit der einzelnen Entwicklerteams.



Erschwerend kommt hinzu, dass sich die grundlegenden Vorgehensweisen ändern: von der Kontrolle virtueller Maschinen in einer eigenständigen Umgebung zur Manipulation von Cloud-Ressourcen in einer gemeinsamen Umgebung. Unternehmen haben dann konkurrierende Betriebsmodelle, um während der Entwicklung der neuen Cloud-Infrastruktur den Status quo beizubehalten.







Erfolgreiches Cloud Computing erfordert Workflows, die das Unternehmen über mehrere Cloud-Anbieter hinweg skalierbar wiederverwenden kann. Dies setzt Folgendes voraus:

- konsistente Anweisungen zum Provisioning;
- Identitäten für Sicherheit und Netzwerkverbindungen;
- Privilegien und Rechte für Bereitstellung und Ausführung.

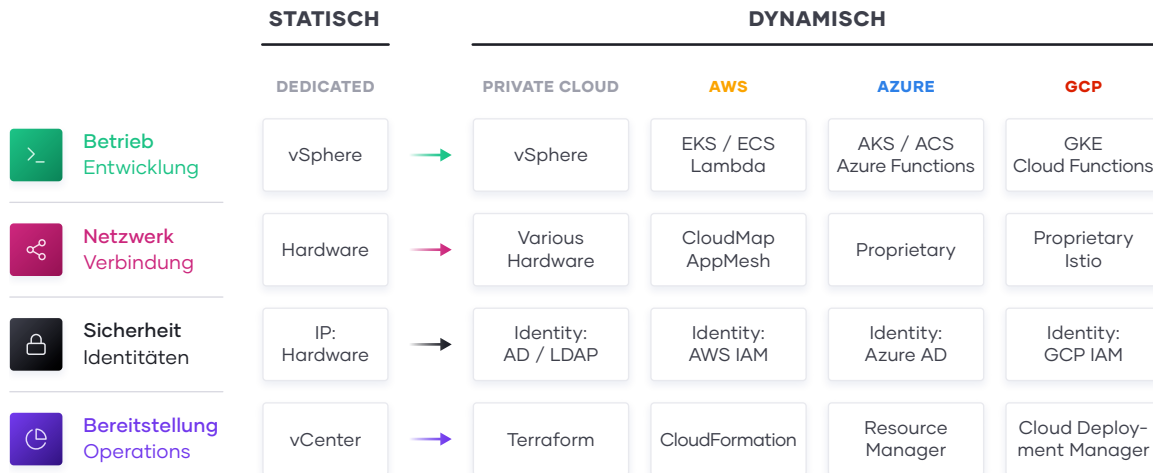
Das Cloud-Betriebsmodell und seine Logik

Die wichtigste Änderung beim Wechsel zur Cloud ist der Wandel von einer „statischen“ zu einer „dynamischen“ Infrastruktur – von der Konfiguration und Verwaltung eines fixen IT-Bestands hin zu Bereitstellung, Absicherung, Verknüpfung und Betrieb von dynamischen On-Demand-Ressourcen.

	STATISCH	DYNAMISCH
 Betrieb	Dedizierte Infrastruktur	Scheduling über alle Ressourcen
 Netzwerk	Host-basiert Statische IP	Service-basiert Dynamische IP
 Sicherheit	High trust IP-basiert	Low trust Identitätsbasiert
 Bereitstellung	Dedizierte Server Homogen	Kapazitäten nach Bedarf Heterogen

Konkret hat das nach und nach die folgenden Änderungen am Betriebsmodell zur Folge:

- **Bereitstellung:** Auf Infrastrukturebene wird aus dem Betrieb auf dedizierten Servern mit beschränktem Umfang eine dynamische Umgebung, in der Unternehmen problemlos auf steigenden oder sinkenden Bedarf durch Hoch- bzw. Herunterskalieren tausender Server reagieren können. Mit der Zunahme von Architekturen und Diensten steigt dann auch die Zahl der Rechenknoten signifikant an.
- **Sicherheit:** Auf dieser Ebene wird aus einer „High Trust“-Welt mit starken Perimetern und Firewalls eine „Low-Trust“- oder „Zero-Trust“-Umgebung ohne klare oder gar statische Perimeter. Dadurch ändert sich das grundlegende Sicherheitsverständnis von einem IP-basierten zu einem identitätsbasierten Ressourcenzugriff. Dieser Wandel wirkt hochgradig disruptiv auf traditionelle Sicherheitskonzepte.
- **Netzwerk:** Auf der Networking-Ebene schwindet die Abhängigkeit von physischen Standorten und IP-Adressen für Dienste und Anwendungen. Zum Zuge kommt stattdessen eine **dynamische Service Registry für Discovery**, Segmentierung und Composition. Das IT-Team im Unternehmen hat dann nicht mehr dieselbe Kontrolle über das Netzwerk oder die physischen Standorte von Rechenressourcen und muss nun über dienstebasierte Konnektivität nachdenken.
- **Betrieb:** Auf Laufzeitebene werden nicht mehr Artefakte auf einem statischen Anwendungsserver gestartet, sondern ein Scheduler regelt die Anwendungsbereitstellung in einem Infrastruktur-Pool, der auf Abruf bereitsteht. Außerdem bestehen neue Anwendungen nun aus einzelnen Services, die dynamisch bereitgestellt und unterschiedlich gepackt sind, von virtuellen Maschinen bis zu Containern.



Um diesen Herausforderungen zu begegnen, müssen sich die IT-Teams mit den folgenden Fragen beschäftigen:

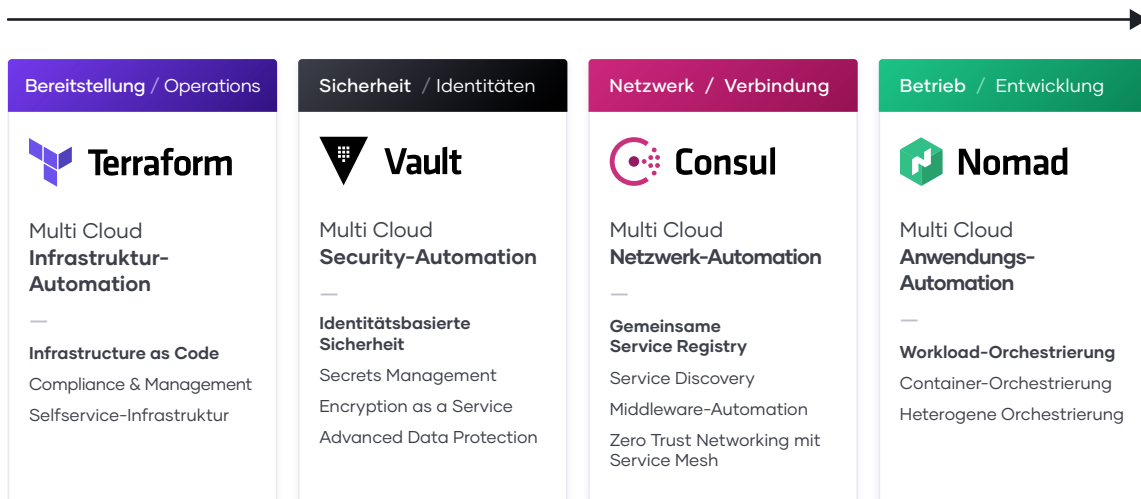
- **Mitarbeiter:** Wie können wir ein Team auf die Multi-Cloud-Realität vorbereiten, sodass die Leute ihre Fähigkeiten unabhängig von der Zielumgebung konsistent anwenden können?
- **Prozesse:** Wie platzieren wir zentrale IT-Dienste, die per Selfservice für Geschwindigkeit sorgen – im Gegensatz zu einem ticketbasierten Gatekeeper-Kontrollsystem –, und zwar so, dass wir dabei Compliance und Governance wahren?
- **Tools:** Wie setzen wir den Mehrwert, den unsere Cloud-Anbieter möglich machen können, am besten frei, und zwar speziell im Hinblick auf Kunden- und Geschäftsnutzen?

Das Potenzial der Cloud freisetzen

Da sich das Cloud-Betriebsmodell auf die Teams sowohl bei Infrastruktur, Sicherheit und Netzwerken als auch bei Anwendungen auswirkt, zeigt sich ein wiederkehrendes Muster beim Aufbau zentraler Shared Services – Centers of Excellence –, wenn Unternehmen eine dynamische Infrastruktur aufbauen, um die Anwendungsbereitstellung auf allen Ebenen erfolgreich zu meistern.

Generell gilt: Die IT-Geschwindigkeit wächst mit der Anzahl der von den Teams bereitgestellten Shared Services des Cloud-Betriebsmodells. Je größer die Cloud-Reife einer Organisation ist, desto höher ist ihre Geschwindigkeit.

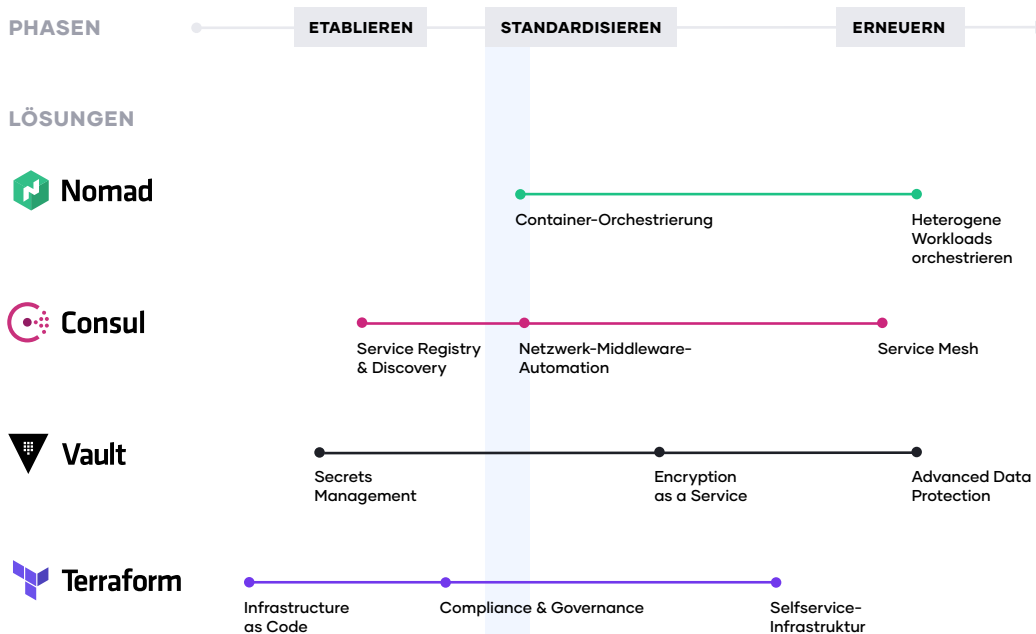
JEDE LÖSUNG DES HASHICORP-STACKS STEIGERT DIE REIFE UND GESCHWINDIGKEIT UNSERER KUNDEN



Wenn Kunden ein Cloud-Betriebsmodell umsetzen, sind typischerweise drei Phasen zu beobachten:

1. **Cloud Essentials etablieren** - Wenn Sie sich auf den Weg Richtung Cloud machen, ist die erste Voraussetzung die Bereitstellung der Cloud-Infrastruktur. Normalerweise geschieht dies durch den Wechsel zu Infrastructure as Code, wobei eine Secrets-Management-Lösung die Sicherheit gewährleistet. Das sind die unverzichtbaren Grundlagen, die Ihnen erst den Aufbau einer zukunftssicheren, skalierbaren und wirklich dynamischen Cloud-Architektur ermöglichen.
2. **Shared Services standardisieren** - Sobald die Cloud-Nutzung zunimmt, müssen Sie ein Shared-Services-Set implementieren und standardisieren, um das Potenzial der Cloud auszuschöpfen. Dies bringt neue Herausforderungen in Bezug auf Governance und Compliance mit sich: Zugriffskontrollregeln und Tracking-Voraussetzungen werden jetzt immer wichtiger.
3. **Mit einer gemeinsamen logischen Architektur erneuern** - Wenn Sie komplett auf die Cloud umsteigen und auf Cloud-Dienste und -Anwendungen als primäres System of Engagement setzen, braucht es eine gemeinsame logische Architektur. Dies setzt eine Steuerebene voraus, die mit dem wachsenden Ökosystem von Cloud-Lösungen verbunden ist und inhärent fortschrittliche Sicherheit und Orchestrierung über Dienste und unterschiedliche Cloud-Umgebungen hinweg bietet.

EXEMPLARISCHE ENTERPRISE JOURNEY AUF DEM WEG ZUM CLOUD-BETRIEBSMODELL



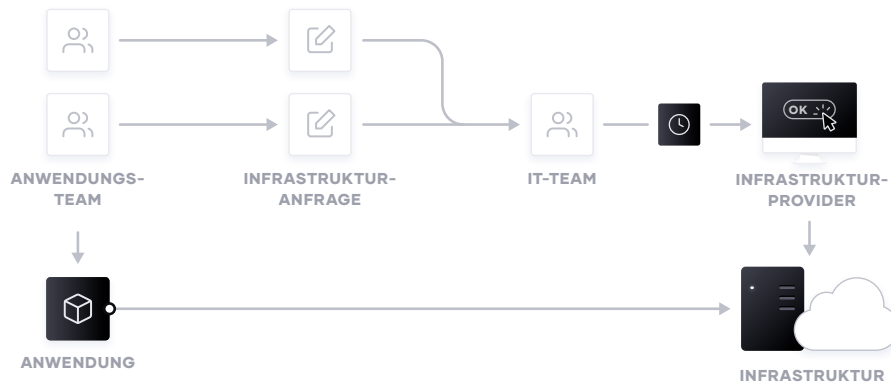
Im Folgenden wird dieser Weg, den Organisationen erfolgreich beschreiten, Schritt für Schritt erklärt:

Schritt 1: Bereitstellung der Multi-Cloud-Infrastruktur

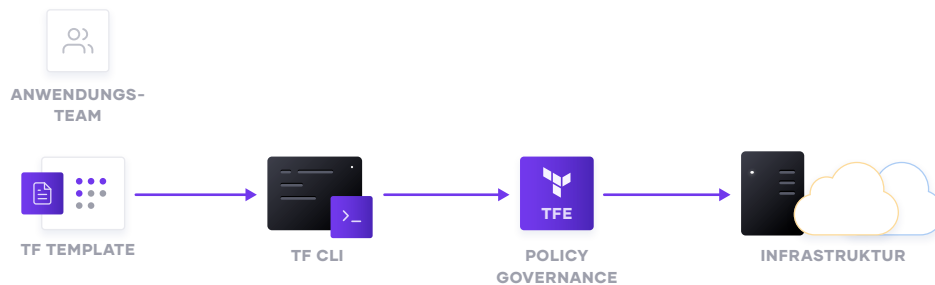
Die Infrastruktur-Bereitstellung ist die Basis der Cloud-Nutzung. HashiCorp Terraform ist das weltweit am meisten verwendete Produkt zur Cloud-Bereitstellung. Terraform schafft die Infrastruktur für jegliche Anwendungen, mit einer breiten Palette von Anbietern für alle Zielplattformen.

Um Shared Services bei der Infrastrukturbereitstellung zu etablieren, sollten IT-Teams mit der Implementierung einer reproduzierbaren Infrastruktur als Code Practices beginnen und anschließend Compliance- und Governance-Workflows einbinden, sodass für angemessene Kontrolle gesorgt ist.

OHNE TERRAFORM



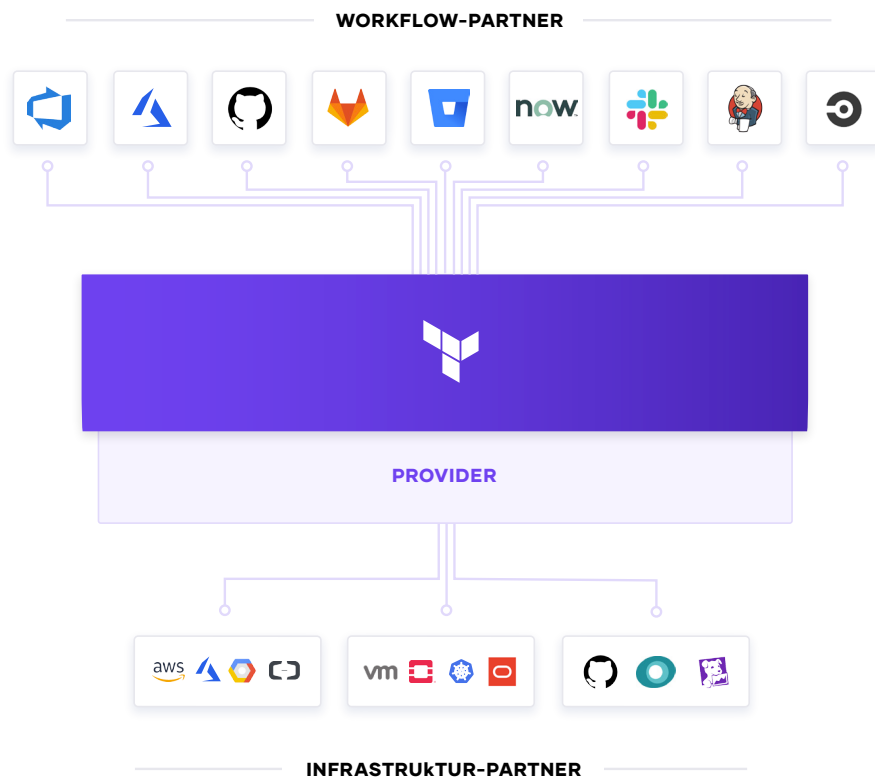
MIT TERRAFORM



Reproduzierbare Infrastructure as Code

Das erste Ziel von Shared Services für die Infrastrukturbereitstellung besteht darin, reproduzierbare Infrastructure as Code zu ermöglichen. So können DevOps-Teams im Rahmen von CI/CD-Workflows Ressourcen planen und bereitstellen, indem sie durchgängig vertraute Tools verwenden.

DevOps-Teams können Terraform-Templates erstellen, welche die Konfigurationen von Diensten einer oder mehrerer Cloud-Plattformen enthalten. Terraform arbeitet mit allen wichtigen Konfigurationsmanagement-Tools zusammen, sodass eine feingranulare Bereitstellung möglich wird, je nach Bereitstellung der Basisressourcen. Außerdem lässt sich Terraform um Dienste vieler Drittanbieter erweitern, etwa um Überwachungstools, APM-Systeme (Application Performance Monitoring), Sicherheitstools, DNS, Content Delivery Networks etc. Einmal definierte Vorlagen können nach Bedarf automatisiert bereitgestellt werden. So wird Terraform zur Lingua franca und zum übergreifenden Workflow für Teams, die Ressourcen über Public und Private Clouds hinweg bereitstellen.



Für eine Selfservice-IT erspart die Abkopplung der Vorlagenerstellung von der Bereitstellung enorm viel Zeit bis zum Go Live einer Anwendung, weil die Entwickler nicht länger auf eine Betriebsgenehmigung zu warten brauchen, solange sie eine bereits genehmigte Vorlage verwenden.

Compliance und Management

Die meisten Teams müssen außerdem Richtlinien durchsetzen, die den Infrastrukturtyp betreffen, die Art der Nutzung und die zugelassenen Teams. Die Sentinel-Richtlinie von HashiCorp sichert als Code-Framework Compliance und Governance, ohne dass eine Änderung des gesamten Team-Workflows nötig wäre. Außerdem ist die Richtlinie selbst als Code definiert und ermöglicht DevSecOps damit Kollaboration und Transparenz.

Wo eine solche Richtlinie nicht als Code vorliegt, greifen die Organisationen auf einen ticketbasierten Review-Prozess zurück, um Änderungen zu genehmigen. Die Folge ist, dass Entwickler wochenlang warten müssen, um Infrastruktur bereitzustellen, wodurch diese Methode zum Engpass wird. Policy as Code ermöglicht die Lösung dieses Problems durch Trennung der Richtliniendefinition von der Umsetzung.

Zentralisierte Teams kodifizieren Richtlinien und setzen auf diese Weise Sicherheit, Compliance und betriebliche Best Practices über die gesamte Cloud-Bereitstellung hinweg um. Die automatisierte Umsetzung von Richtlinien stellt die Konformität von Änderungen sicher und vermeidet Engpässe in Form von manuellen Prüfungen.

Schritt 2: Multi-Cloud-Sicherheit

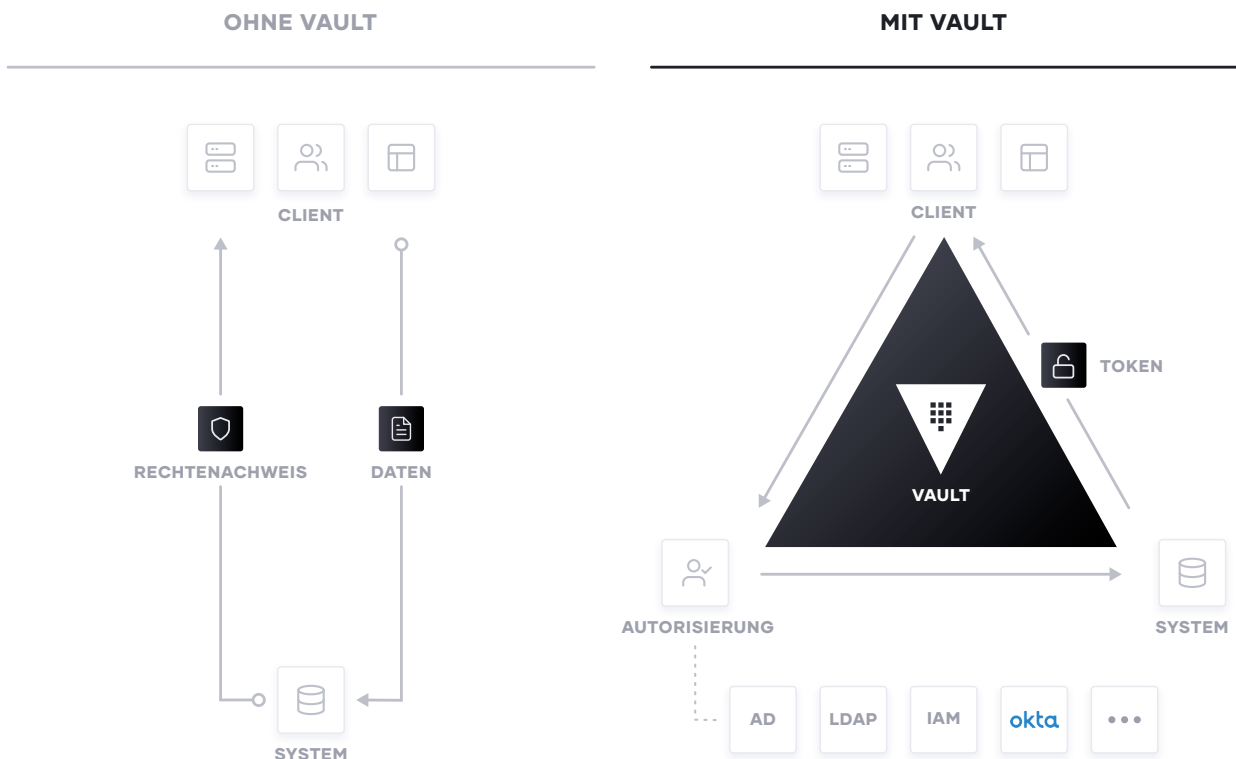
Dynamische Cloud-Infrastruktur bedeutet einen Wechsel von hostbasierten zu anwendungsbasierten Identitäten, mit Low- und Zero-Trust-Netzwerken über mehrere Clouds hinweg und ohne klare Netzwerkperimeter.

Im traditionellen Sicherheitsdenken setzen wir hochgradig vertrauenswürdige interne Netzwerke voraus, mit einer „harten Schale“ und einem „weichen Kern“. Beim modernen Zero-Trust-Ansatz arbeiten wir daran, auch den Kern zu härten. Das erfordert, dass Anwendungen explizit authentifiziert sein müssen, zum Abrufen vertraulicher Informationen und zur Durchführung sensibler Operationen autorisiert sowie streng überwacht sein müssen.

Mit HashiCorp Vault können Teams ihre Tokens, Passwörter, Zertifikate und Verschlüsselungen zum Schutz von Maschinen und Anwendungen sicher speichern und den Zugriff darauf streng kontrollieren. Im Ergebnis ist das ein voll ausgebautes Secrets-Management-System. Darüber hinaus schützt Vault sowohl Data at Rest als auch in Transit. Vault stellt eine High-Level-Kryptografie-API zur Verfügung, damit Entwickler ohne Offenlegung der Schlüssel sensible Daten sichern können. Vault kann auch als Zertifizierungsstelle fungieren und dynamische, temporäre Zertifikate zur Sicherung der Kommunikation per SSL/TLS bereitstellen. Des Weiteren ermöglicht Vault den Identitätsabgleich zwischen unterschiedlichen Plattformen, etwa zwischen dem lokalen Active Directory und AWS IAM, sodass Anwendungen auch plattformübergreifend funktionieren.

Vault ist weithin im Einsatz: Bei Börsen, großen Finanzinstituten, bei Hotelketten und allem, was dazwischen liegt, sorgt die Lösung für Sicherheit im Cloud-Betriebsmodell.

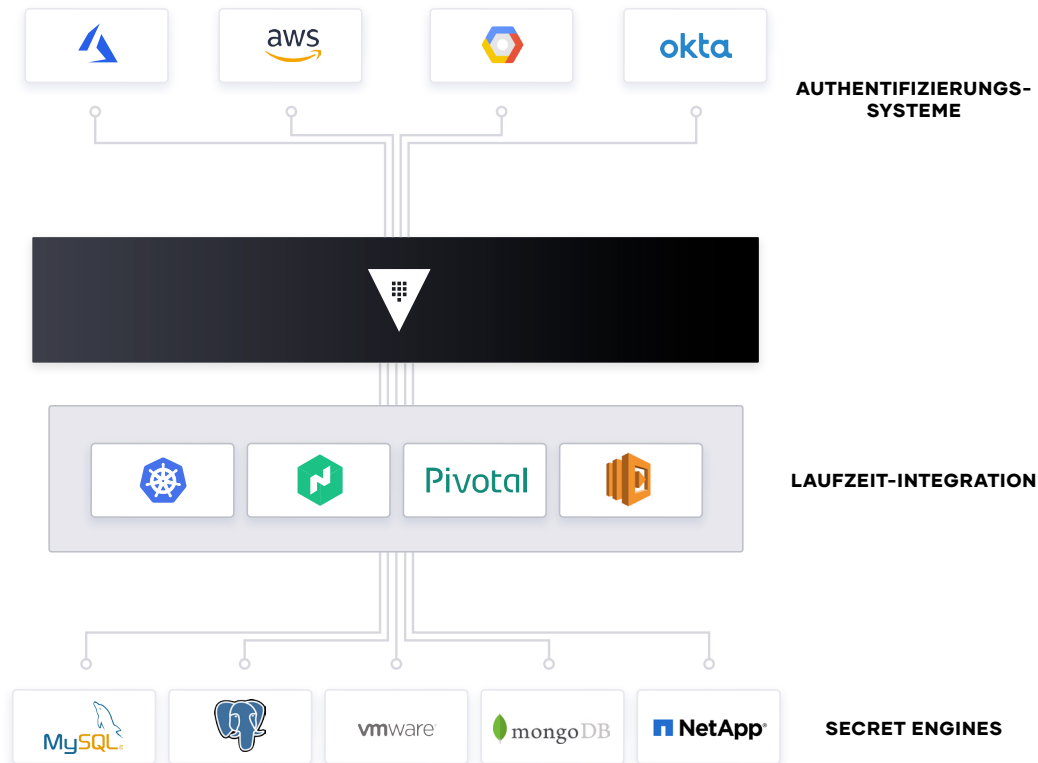
Um Shared Services in Sachen Sicherheit zu erreichen, sollten IT-Teams zentralisierte Secrets-Management-Systeme ermöglichen und diese Dienste dann dazu nutzen, noch genauere Encryption-as-a-Service-Anwendungsfälle wie Zertifikat- und Schlüsselrotationen zu bilden und ihre Daten bei Speicherung und Übertragung zu verschlüsseln.



Secrets Management

Der erste Schritt in Sachen Cloud-Sicherheit ist normalerweise das Secrets Management: die zentrale Speicherung, Zugriffskontrolle und Verteilung dynamischer Geheimnisse. Sobald man sich von statischen IP-Adressen verabschiedet, ist es absolut wichtig, dass zur Authentifizierung und für den Zugriff auf Dienste und Ressourcen identitätsbasierte Zugriffssysteme wie AWS IAM und Azure AAD integrierbar sind.

Vault verwendet Richtlinien, um festzulegen, wie Anwendungen authentifizieren, welche Zugangsdaten sie verwenden dürfen und wie Revisionen vorgenommen werden sollten. Vault arbeitet mit einer Reihe Trusted-Identity-Anbieter zusammen, darunter Cloud-IAM-Plattformen (Identity and Access Management), Kubernetes, Active Directory und andere SAML-basierte Authentifizierungssysteme. Vault übernimmt dann die zentrale Verwaltung und Kontrolle des Zugriffs auf Geheimnisse und Systeme auf der Basis vertrauenswürdiger Anwendungen und Nutzeridentitäten.



IT-Teams wird empfohlen, einen Shared Service zu etablieren, der Zugriffsanforderungen für beliebige Systeme über einen konsistenten, geprüften und sicheren Workflow ermöglicht.

Encryption as a Service

Zusätzlich müssen Unternehmen ihre Daten verschlüsseln. Vault kann Encryption as a Service anbieten und stellt eine einheitliche API für Schlüsselverwaltung und Kryptografie bereit. So genügt eine einzige Integration, um Daten über mehrere Umgebungen hinweg zu schützen.

Vault als Basis für Encryption as a Service löst außerdem einige größere Security-Probleme, darunter das der Zertifikats- und Schlüsselrotation. Vault bietet eine zentrale Schlüsselverwaltung und ermöglicht die Verschlüsselung von Data at Rest und in Transit über Clouds und Rechenzentren hinweg. Das spart Kosten für teure HSMs (Hardware Security Modules) und steigert mit durchgängigen Sicherheitsworkflows und Kryptografiestandards in der gesamten Organisation die Produktivität.

Da viele Organisationen ihre Entwickler zwar zur Verschlüsselung berechtigen, aber keine Methode vorgeben, konzipieren Entwickler eigene Lösungen – oft ohne tiefere Kryptografiekenntnisse. Vault bietet dagegen eine einfache, anwenderfreundliche API und gibt zentralen Sicherheitsteams zugleich die nötigen Richtlinienkontrollen und Lifecycle-Management-APIs an die Hand.

Advanced Data Protection

Organisation, die in die Cloud ziehen oder hybride Umgebungen nutzen, unterhalten und pflegen nach wie vor lokale Dienste und Anwendungen, die kryptografische Operationen durchführen müssen (zum Beispiel die Verschlüsselung gespeicherter Daten). Diese Dienste möchten nicht unbedingt die Verwaltungslogik der kryptografischen Schlüssel implementieren und lagern die Schlüsselverwaltung deshalb lieber an externe Anbieter aus. Advanced Data Protection erlaubt es Organisationen dagegen, fortschrittliche Verschlüsselung inklusive Verfahren und Management zwischen Infrastruktur und Vault Enterprise zu integrieren, einschließlich automatischem Schutz der Daten in MySQL, MongoDB, PostgreSQL und anderen Datenbanken, die transparente Datenverschlüsselung (TDE) nutzen.

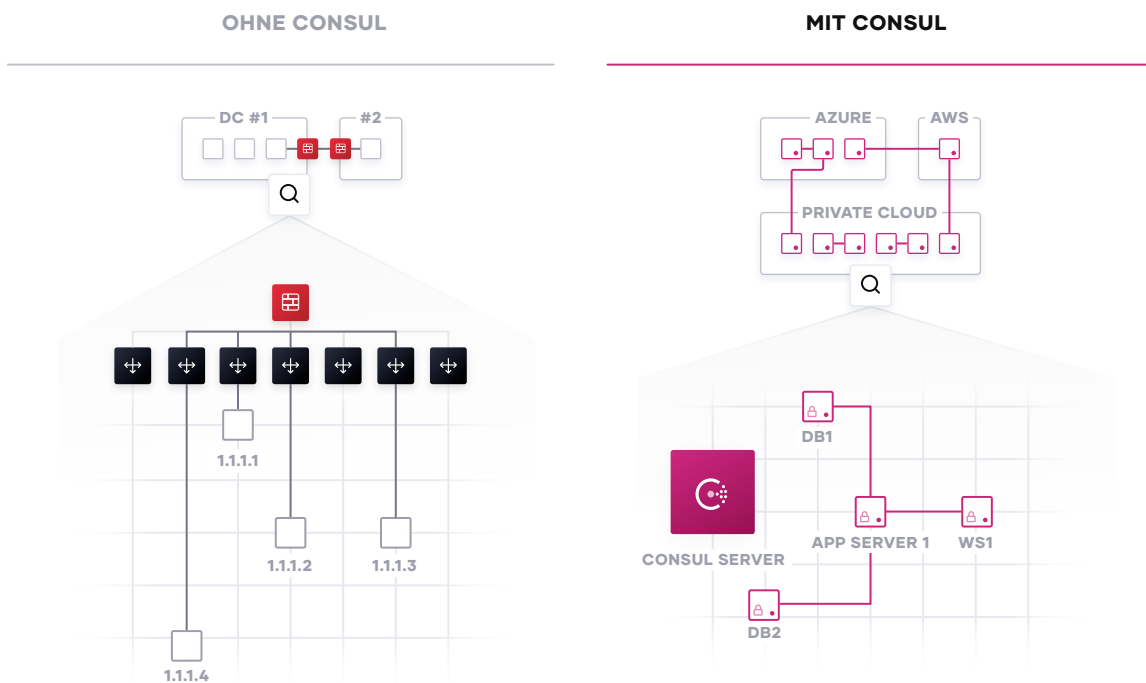
Für Organisationen mit hohen Sicherheitsanforderungen an Compliance (PCI-DSS, HIPAA etc.), Datenschutz und die kryptografisch gesicherte Anonymität personenbezogener Daten bietet Advanced Data Protection Funktionen zur Tokenisierung, zum Beispiel durch Verfremdung, um Kreditkartendaten, persönliche Informationen, Bankverbindungen und andere sensible Daten zu schützen.

Schritt 3: Multi-Cloud-Service-Vernetzung

Networking in der Cloud birgt meist die größten Schwierigkeiten beim Umstieg. Die Kombination dynamischer IP-Adressen, ein spürbarer Anstieg im East-West-Traffic beim Umstieg auf Microservices und das Fehlen klarer Netzwerkperimeter ist eine immense Herausforderung.

HashiCorp Consul stellt ein Multi-Cloud-Service-Netzwerk bereit, um die Vielzahl der Dienste zu verbinden und abzusichern. Consul ist ein weit verbreitetes Produkt, wobei viele Kunden deutlich mehr als 100.000 Knoten betreiben.

Networking Services sollten zentral bereitgestellt werden, sodass IT-Teams die Service Registry und die Service Discovery stellen. Eine allgemeine Registry ist sozusagen die Landkarte, die zeigt, welche Dienste gerade laufen, wo sie laufen und wie es um ihre Gesundheit bestellt ist. Die Registry kann programmatisch abgefragt werden, um Service Discovery zu ermöglichen oder zum Zweck der Netzwerkautomatisierung von API-Gateways, Load-Balancern, Firewalls und anderen kritischen Middleware-Komponenten. Diese Komponenten können bei einem Service-Mesh-Ansatz auch aus dem Netzwerk ausgegliedert werden. Dann laufen Proxies im Hintergrund, um die entsprechende Funktionalität zu gewährleisten. Service Meshs können die Netzwerktopologie drastisch vereinfachen, besonders bei Multi-Cloud- und Multi-Rechenzentren-Topologien.



Service Discovery

Der Ausgangspunkt beim Networking im Cloud-Betriebsmodell ist normalerweise eine gemeinsame Service Registry, die als Echtzeitverzeichnis anzeigt, welche Dienste aktuell laufen, wo sie laufen und ob sie in Ordnung sind. Traditionelle Networking-Ansätze brauchen Load Balancer und virtuelle IPs, um mit solchen Abstraktionen einen Dienst mit statischer IP zu adressieren. Wer den Netzwerkstandort der Dienste nachverfolgen will, braucht dazu Tabellenblätter, Load-Balancer-Dashboards oder Konfigurationsdateien – alles separate Quellen, die manuelle, keineswegs optimale Prozesse erfordern.

Bei Consul ist jeder Dienst programmatisch registriert. Es gibt DNS-Schnittstellen und APIs, damit sich alle Dienste gegenseitig erkennen können. Der integrierte Status-Check überwacht den Zustand jeder Instanz. So kann das IT-Team nach der Verfügbarkeit der Instanzen priorisieren und Consul kann Routing-Traffic zu geschwächten Instanzen unterbinden.

Consul kann zusammen mit anderen Diensten integriert werden, zum Beispiel mit traditionellen Load Balancern, die bestehenden North-South-Traffic verwalten, oder verteilten Anwendungsplattformen wie Kubernetes, um konsistente Registry- und Discovery-Services für Multi-Rechenzentren-, Cloud- und Plattformumgebungen anzubieten.

Netzwerk-Middleware-Automatisierung

Der nächste Schritt besteht darin, die Komplexität des laufenden Betriebs bei vorhandener Networking-Middleware durch Automation zu reduzieren. Die bisherigen manuellen, Ticket-basierten Prozesse zur Rekonfiguration von Load Balancern und Firewalls bei jeder Änderung an Netzwerkstandorten oder Dienstkonfigurationen kann Consul automatisieren. Dies wird dadurch erreicht, dass Netzwerk-Middleware-Geräten gestattet wird, die Änderungen von der Service Registry zu abonnieren. Dadurch erreicht man eine hochdynamische Infrastruktur, die wesentlich höher skaliert als statische Ansätze.

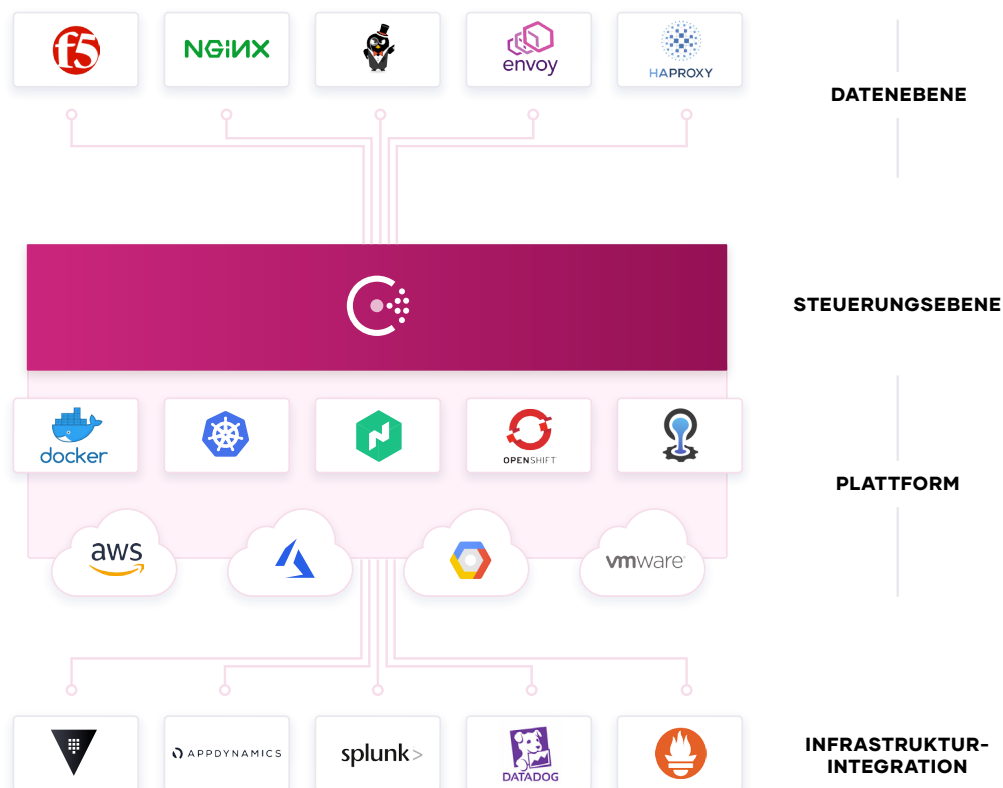
Dies entkoppelt außerdem den Workflow zwischen Teams, da die operativen Teams mit Consul Anwendungen unabhängig bereitstellen und veröffentlichen, während NetOps-Teams Consul abonnieren, um die Downstream-Automatisierung zu handhaben.

Zero Trust Networking mit Service Mesh

Wenn Organisationen mit Microservices oder Cloud-nativen Anwendungen skalieren, wird die zugrunde liegende Infrastruktur rasch größer und dynamischer und der East-West-Traffic steigt sprunghaft an. Dies führt dann oft zu einem starkem Zuwachs an teurer Netzwerk-Middleware mit Single Points of Failure und signifikanten Overhead-Kosten für die IT-Teams.

Consul bietet stattdessen ein verteiltes Service Mesh, das Routing, Autorisierung und andere Networking-Funktionen an die Endpunkte verlagert, statt sie durch Middleware zu zwingen. Das vereinfacht die Netzwerktopologie und ihre Verwaltung, man braucht keine teure Middleware auf den East-West-Traffic-Pfaden mehr, und die Service-to-Service-Kommunikation wird sehr viel zuverlässiger und skalierbarer.

Consul ist eine API-getriebene Steuerungsebene mit Sidecar Proxies (zum Beispiel Envoy, HAProxy oder NGINX). Diese Proxies bilden die verteilte Datenebene. Gemeinsam ermöglichen diese beiden Schichten ein Zero-Trust-Netzwerkmodell, das Service-to-Service-Kommunikation mit automatischer TLS-Verschlüsselung und identitätsbasierter Autorisierung leistet. NetOps und SecOps können Sicherheitsrichtlinien mit logischen Diensten statt über IP-Adressen definieren.

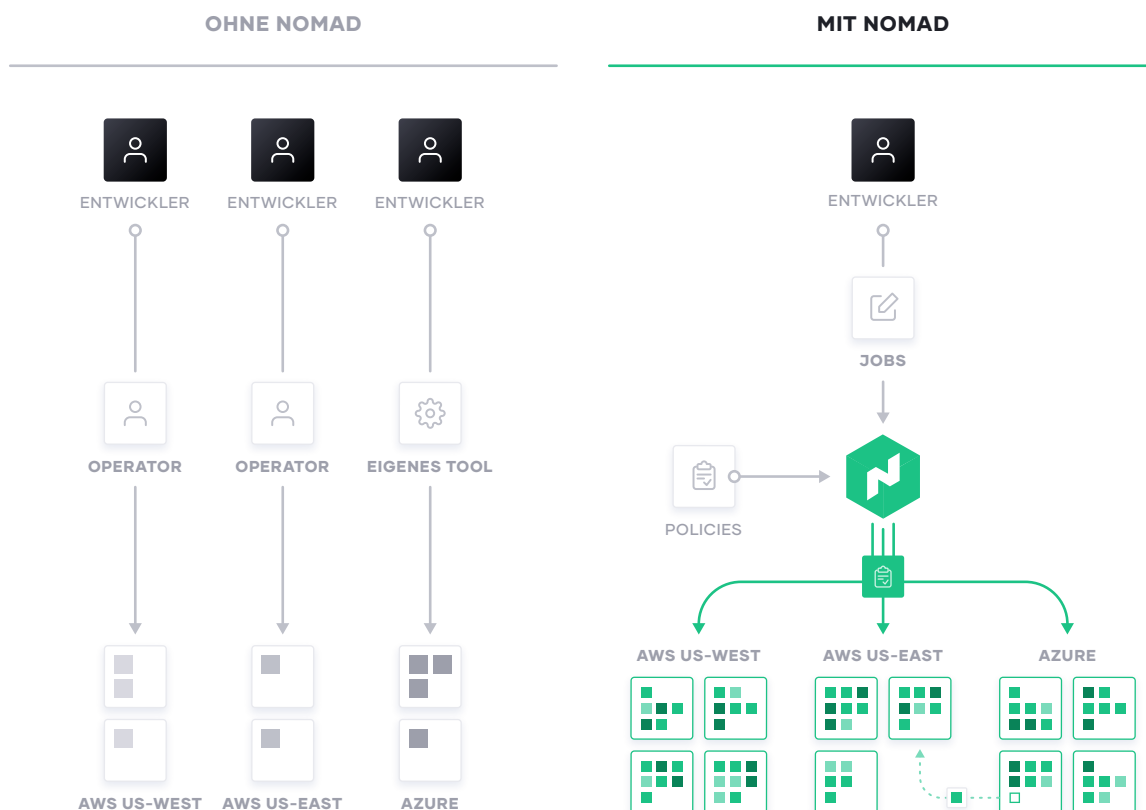


Consul ermöglicht eine feingranulare Dienstesegmentierung, um die Service-to-Service-Kommunikation mit automatischer TLS-Verschlüsselung und identitätsbasierter Autorisierung abzusichern. Consul arbeitet auch mit Vault zusammen, das für zentralisiertes PKI- und Zertifikatsmanagement sorgt. Dienste konfiguriert man über das API eines Key/Value-Speichers, mit dessen Hilfe man Dienste während der Laufzeit in Umgebungen jeder Art leicht konfigurieren kann.

Schritt 4: Multi-Cloud-Anwendungsbereitstellung

Abschließend werden laufend neue Apps ausgerollt, zugleich müssen aber die Legacy-Apps flexibler verwaltet werden. HashiCorp Nomad bietet einen flexiblen Orchestrator, der beide Arten für beliebige Workloads deployen und verwalten kann, von Dauerdiensten über schnelle Batches bis zu Systemagenten.

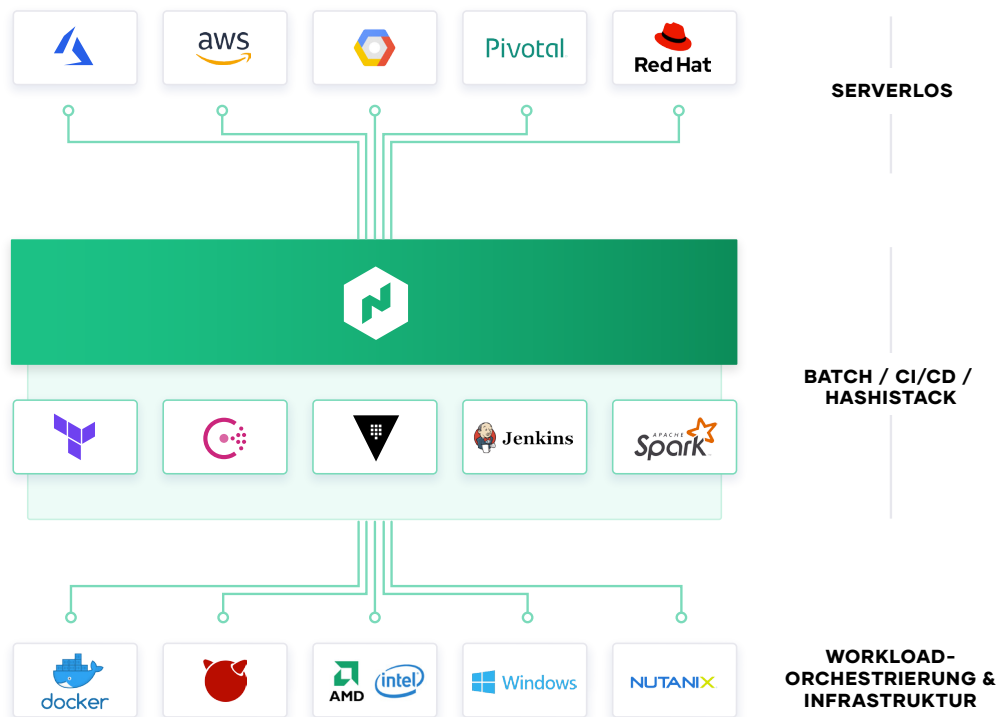
Damit Shared Services möglich werden, sollten IT-Teams Nomad gemeinsam mit Terraform, Vault und Consul nutzen. Das schafft eine konsistente Anwendungsbereitstellung, die den Anforderungen an Compliance, Sicherheit und Networking gerecht wird, inklusive Workload-Orchestrierung und Scheduling.



Gemischte Workloads orchestrieren

Viele neue Workloads werden als Container-Packages entwickelt, die für Kubernetes oder andere Container-Plattformen gedacht sind. Viele Legacy-Workloads gelangen aber gar nicht auf diese Plattformen, ebenso wenig zukünftige serverlose (Serverless) Anwendungen. Nomad bietet stattdessen einen durchgängigen Prozess für alle Workloads, von virtuellen Maschinen über Standalone-Binaries bis zu Containern – und gibt diesen Workloads noch genuine Orchestrierungsvorteile mit, beispielsweise Release-Automatisierung, Multiple-Upgrade-Strategien, Bin Packing und Widerstandsfähigkeit.

Für moderne Anwendungen – normalerweise Container – bietet Nomad denselben konsistenten, skalierbaren Workflow in jeder Umgebung. Nomad ist auf Einfachheit und Effektivität in Sachen Orchestrierung und Scheduling ausgerichtet und umgeht damit die Komplexität von Plattformen wie Kubernetes, die Spezialwissen allein für den Betrieb und Support von Container-Workloads erfordern.



Nomad lässt sich in bestehende CI-/CD-Workflows integrieren, sodass eine schnelle, automatische Anwendungsbereitstellung sowohl für Legacy- als auch für moderne Workloads machbar ist.

High Performance Computing

Nomad ist für das Scheduling von Anwendungen mit geringer Latenz in sehr großen Clustern ausgelegt. Das ist wichtig für Kunden mit großen Batch-Jobs, aber ebenso im High Performance Computing (HPC). In der Million Container Challenge war Nomad in der Lage, das Scheduling für eine Million Redis-Instanzen auf 5.000 Maschinen in drei Rechenzentren vorzunehmen, und das in weniger als fünf Minuten. Es gibt etliche große Nomad-Umgebungen, die sogar in noch größerem Maßstab operieren.

Dank Nomad können HPC-Anwendungen einfach über eine API Kapazitäten dynamisch an sich ziehen, woraus sich eine effiziente Ressourcenteilung für Datenanalyseanwendungen wie Spark ergibt. Das Scheduling mit geringer Latenz gewährleistet rechtzeitig verfügbare Ergebnisse und hält die Menge ungenutzter und damit vergeudeter Ressourcen gering.

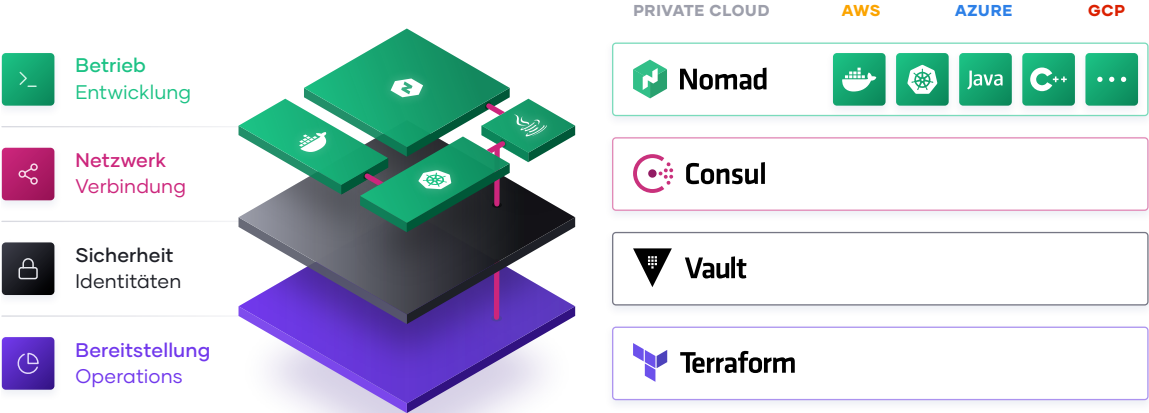
Multi-Datacenter-Workload-Orchestrierung

Nomad ist by design regionenübergreifend für Multi-Clouds konzipiert und verarbeitet mit einem konsistenten Workflow Lasten aller Art. Wenn Teams weltweite Anwendungen in mehreren Rechenzentren oder über Cloud-Grenzen hinweg ausrollen, leistet Nomad die nötige Orchestrierung und das Scheduling, unterstützt von den Ressourcen und Richtlinien für Infrastruktur, Sicherheit und Networking. Das oberste Ziel: die erfolgreiche Bereitstellung der Anwendung.

Schritt 5: Effizienz in der Anwendungsbereitstellung

Letztlich stellen die Shared Services bei Infrastruktur, Sicherheit, Networking und Anwendungs-
laufzeit eine hocheffiziente Form der Anwendungsbereitstellung in industriellem Maßstab dar. Man
macht sich dabei die dynamischen Vorteile jeder der Cloud-Ebenen zunutze.

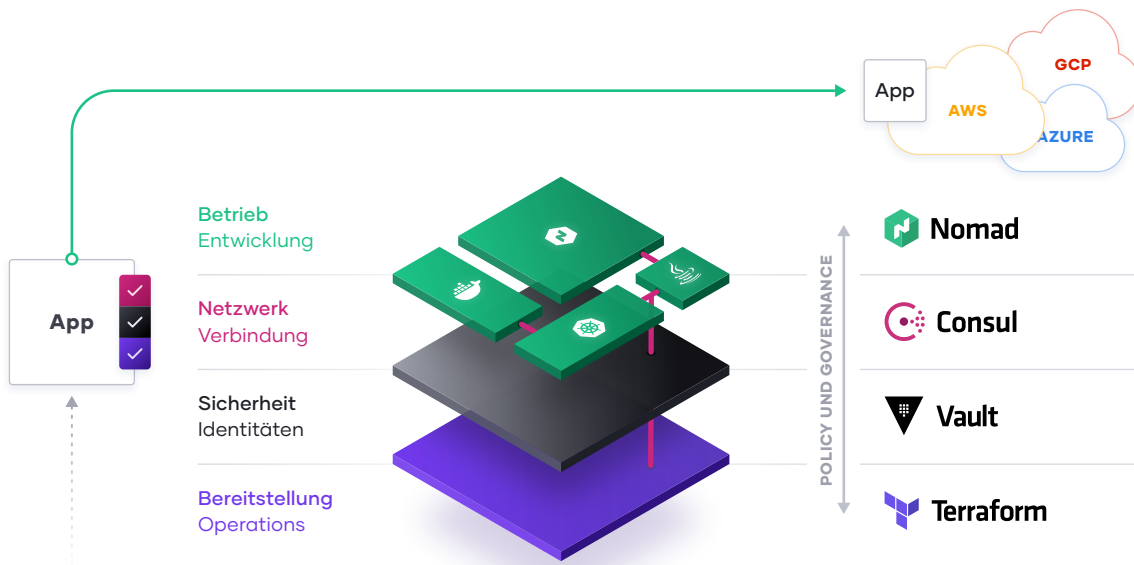
Das Cloud-Betriebsmodell ermöglicht eine vollständig regelkonforme und regulierte Selfservice-IT,
mit der Teams ihre Anwendungen noch schneller bereitstellen können.



Fazit

Ein allgemeines Cloud-Betriebsmodell ist der unvermeidliche Schritt für Unternehmen, die aus dem digitalen Wandel das meiste herausholen wollen. Die Tool-Suite von HashiCorp ist dazu gedacht, für jede Cloud-Ebene Lösungen zu liefern, damit Ihnen der Wechsel zum Cloud-Betriebsmodell gelingt.

Die Unternehmens-IT muss sich von ITIL-Kontrollpunkten mit Fokus auf Kostenoptimierung weiterentwickeln, in Richtung eines Selfservice-Enablers mit Fokus auf Geschwindigkeitsoptimierung. Dies gelingt durch Bereitstellung von Shared Services auf jeder Cloud-Ebene, die Ihre Teams dabei unterstützen, zügig neuen geschäftlichen Mehrwert und Kundenwert zu schaffen.



Den schnellsten Weg zu neuem Mehrwert zu erschließen, bedeutet in einem modernen Multi-Cloud-Rechenzentrum mit Einführung eines gemeinsamen Cloud-Betriebsmodells, dass sich der Charakter der Unternehmens-IT grundlegend wandelt:

- **Mitarbeiter: Wechsel zu Multi-Cloud-Skills**
 - Fertigkeiten, die im internen Rechenzentrumsmanagement und mit einzelnen Cloud-Anbietern gewonnen werden, können durchgängig in beliebigen Umgebungen eingesetzt werden.
 - Die Einführung von DevSecOps und anderer agiler Praktiken führt dazu, dass Sie immer kurzlebiger und verteilte Systeme effizient bedienen.

- **Prozesse: Wechsel zu Selfservice-IT**
 - Eine zentral positionierte IT als Shared-Service-Enabler ist auf Geschwindigkeit in der Anwendungsbereitstellung ausgerichtet: Software immer noch schneller ausliefern, und das bei minimalem Risiko.
 - Centers of Excellence auf allen Cloud-Ebenen stellen Fähigkeiten in Form von Selfservice-Angeboten bereit.

- **Tools: Wechsel zu dynamischen Umgebungen**
 - Geeignete Tools werden der zunehmenden Flüchtigkeit und Verteilung von Infrastruktur und Anwendungen gerecht, sie unterstützen die kritischen Workflows, anstatt an spezielle Technologien gebunden zu sein.
 - Passende Richtlinien- und Governance-Tools sorgen dafür, dass Risikomanagement und Compliance mit der neuen Bereitstellungsgeschwindigkeit mithalten können.

Über HashiCorp

HashiCorp ist der führende Anbieter für Multi-Cloud-Infrastruktur-Automatisierungssoftware. Die Software-Suite von HashiCorp ermöglicht Organisationen konsistente Workflows, um beliebige Infrastrukturen für Anwendungen aller Art bereitzustellen, abzusichern, zu vernetzen und zu betreiben. Die Open-Source-Tools Vagrant, Packer, Terraform, Vault, Consul und Nomad von HashiCorp werden jedes Jahr millionenfach heruntergeladen und sind unter den Global 2000 weit verbreitet. Die Enterprise-Versionen verbessern die Open-Source-Tools noch mit Features für Collaboration, Betriebsabläufe, Governance und Multi-Datacenter-Funktionalität. Der Hauptsitz des Unternehmens befindet sich in San Francisco. HashiCorp wird durch Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP und Bessemer Venture Partners unterstützt. Weitere Informationen finden Sie unter www.hashicorp.com oder wenn Sie HashiCorp auf Twitter folgen: [@HashiCorp](https://twitter.com/HashiCorp).

