HashiCorp | Tencent Cloud

Unlocking the Cloud Operating Model with Tencent Cloud

Achieving the fastest path to value in a modern, hybrid cloud datacenter

Table of Contents

Executive Summary

To thrive in an era of hybrid cloud architectures driven by digital transformation, enterprise IT must evolve from ITIL-based gatekeeping to enabling shared self-service processes for DevOps excellence.

For most enterprises, digital transformation means delivering new business and customer value more quickly, and at a very large scale. The implication for enterprise IT, then, is a shift from cost optimization to speed optimization. The cloud is a critical part of this shift, as it's required in order to rapidly deploy on-demand services at unlimited scale.

To unlock the fastest path to value in the cloud, enterprises must industrialize the application delivery process across each layer of the cloud: embracing the cloud operating model and tuning people, processes, and tools to take advantage of it.

This white paper lays out the benefits of implementing the cloud operating model with HashiCorp and offers guidance on how to successfully deploy it on Tencent Cloud.

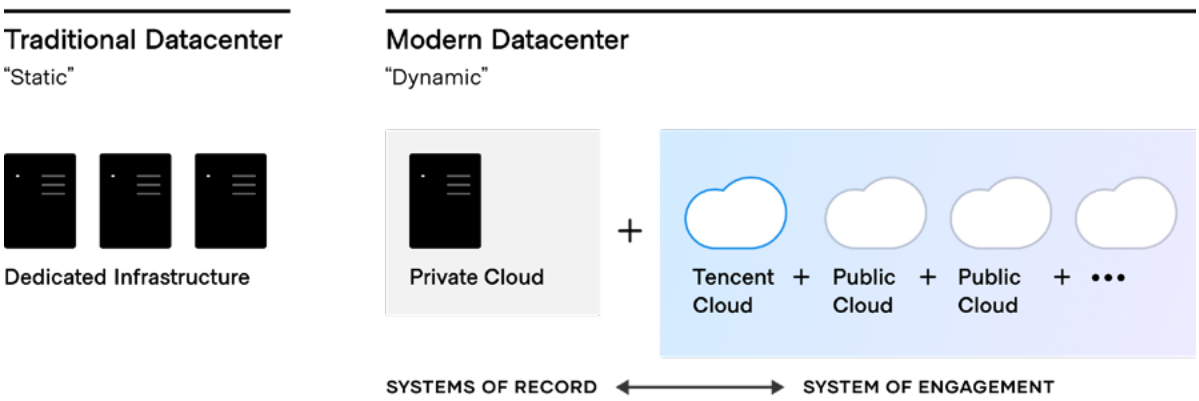
China Connect

Tencent Cloud is a secure, reliable and high-performance cloud compute service provided by Tencent, the largest Internet company in China. Organizations of all sizes and across all industries choose Tencent Cloud for four key reasons:

- **Competence.** Opportunities and challenges abound in China. Tencent Cloud offers local expertise and industry-leading cloud services to empower your business success in China.
- **Connectivity.** Tencent Cloud currently operates 70 availability zones spread across 27 regions globally, providing businesses with fast and secure networks to facilitate global and cross-border connectivity.
- **Consultancy.** Tencent Cloud provides end-to-end technical consulting services to facilitate your implementation of mandated technical standards under the local regulatory environment.
- **C2B2C Success.** With years of experience integrating its cloud solutions across the Weixin ecosystem, Tencent Cloud offers businesses valuable local market knowledge and expertise.

Transitioning to a Hybrid Cloud Datacenter

The transition to cloud and hybrid cloud environments is a generational transition for IT. This transition means shifting from largely dedicated servers in a private datacenter to a pool of compute capacity available on demand. While most enterprises began with one cloud provider, there are good reasons to use services from others. Inevitably, most Global 2000 organizations will use more than one cloud provider. In fact, 90% of large enterprises are already hybrid cloud, according to the 2021 HashiCorp State of Cloud Strategy Survey.



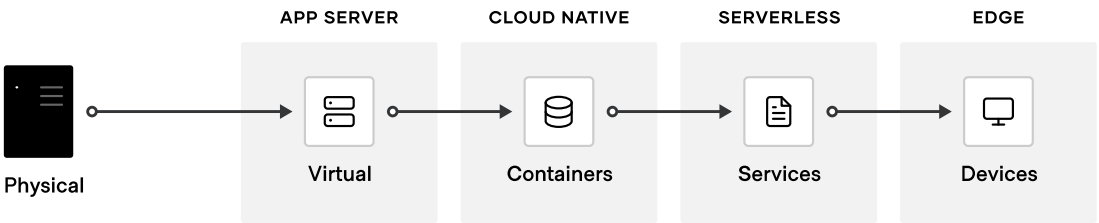
The cloud presents an opportunity for speed and scale optimization of new "systems of engagement" — the applications built to engage customers and users. These new apps are the primary interface for customers to engage with a business, and are ideally suited for delivery via the cloud, as they tend to:

- Have dynamic usage characteristics, needing to quickly scale loads up and down by orders of magnitude.
- Support fast development and iteration. Many of these new systems are central to how the organization engages its customers, so development teams need to quickly release enhancements in response to competitors and user feedback.

For most enterprises though, these systems of engagement must connect to existing "systems of record" — the organization's core business databases and internal applications, which often continue to reside on infrastructure in existing datacenters. As a result, enterprises often end up with a hybrid model — a mix of multiple public and private clouds and on-premises environments.

The challenge for most enterprises, then, is how to use the cloud to consistently deliver these applications while ensuring the least possible friction across the various development teams.

Compounding this challenge, the underlying primitives have changed from manipulating virtual machines in a self-contained environment to working with a variety of cloud resources in a shared environment. Enterprises must deal with competing operational models as they work to maintain their existing estate while also developing the new cloud infrastructure.



For cloud computing to deliver on its promises, enterprises need consistent workflows that can be reused at scale across multiple cloud providers. This requires:

- Consistent instruction sets for provisioning
- Identity for security and network connections
- Privileges and rights that support enterprise role-based access controls (RBACs)

Implications of the Cloud Operating Model

The essential implication of the transition to the cloud is the shift from "static" infrastructure to "dynamic" infrastructure: from a focus on configuration and management of a static fleet of IT resources to provisioning, securing, connecting, and running dynamic resources on demand.

	Static		Dynamic
Run	Dedicated Infrastructure	→	Scheduled across the fleet
Connect	Host-based, Static IP	→	Service-based, Dynamic IP
Secure	High trust, IP-based	→	Low trust, Identity-based
Provision	Dedicated servers, Homogeneous	→	Capacity on-demand, Hetergeneous

This implies a number of changes in approach at each layer of the stack:

- **Provision:** The infrastructure layer transitions from running dedicated servers at limited scale to a dynamic environment where organizations can easily adjust to increased demand by spinning up thousands of servers and scaling them down when not in use. As architectures and services become more distributed, the sheer volume of compute nodes increases significantly.
- **Secure:** The security layer transitions from a fundamentally "high trust" world enforced by a strong perimeter and firewall to a "low trust" or "zero trust" environment with no clear or static perimeter. As a result, the foundational assumption for security shifts from being IP-based to identity-based access to resources. This shift is highly disruptive to traditional security models.
- **Connect:** The networking layer transitions from being heavily dependent on the physical location and IP address of services and applications to using a dynamic registry of services for discovery, segmentation, and composition. An enterprise IT team does not have the same control over the network, or the physical locations of compute resources, and must think about service-based connectivity.

- **Run:** The runtime layer shifts from deploying artifacts to a static application server to deploying applications with a scheduler atop a pool of infrastructure provisioned on demand. In addition, new applications become collections of dynamically provisioned services and packaged in multiple ways: from virtual machines to containers.

	Static		Dynamic	
	DEDICATED		PRIVATE CLOUD	TENCENT CLOUD
Run Deployment	vSphere	→	vSphere	TKE, SCF
Connect Networking	Hardware	→	Various Hardware	TSF
Secure Security	IP: Hardware	→	Identity: AD/LDAP	Identity: CAM
Provision Operations	vCenter	→	Terraform	Terraform

Additionally, each cloud provider has its own solution to these challenges. For enterprise IT teams, these shifts in approach are compounded by the realities of running on hybrid cloud infrastructures and the varying tools each technology provides. To address these challenges, teams must ask key questions around three core questions:

- **People:** How can we enable teams to thrive in a hybrid cloud reality, where skills must be applied consistently regardless of the target environment?
- **Process:** How do we position central IT services as a self-service enabler of speed instead of a ticket-based gatekeeper of control, while retaining compliance and governance?
- **Tools:** How do we best unlock the value of the available capabilities of the cloud providers to boost customer and business value?

Unlocking the Cloud Operating Model on Tencent Cloud

The implications of the cloud operating model impact enterprise teams across infrastructure, security, networking, and applications. In response, enterprises are establishing central shared services — centers of excellence — to deliver the dynamic infrastructure necessary at each layer for successful application delivery.

Tencent Cloud and HashiCorp tools work together to help IT and business units align on a clear strategy and plan to guide cloud implementation activities. As teams deliver on each shared service for the cloud operating model, IT velocity increases. The greater cloud maturity an organization has, the faster its velocity.

Expanding use of the HashiCorp Stack increases maturity and velocity for our customers

Provision / Operations

Terraform

Hybrid Cloud
Infrastructure Automation

- Infrastructure as code
- Compliance & management
- Self service infrastructure

Secure / Security

Vault

Hybrid Cloud
Security Automation

- Identity-based security
- Secrets management
- Encryption as a service
- Advanced data protection

Connect / Networking

Consul

Hybrid Cloud
Networking Automation

- Common service registry
- Service discovery
- Network middleware automation
- Zero trust networking with service mesh

Run / Deployment

Nomad

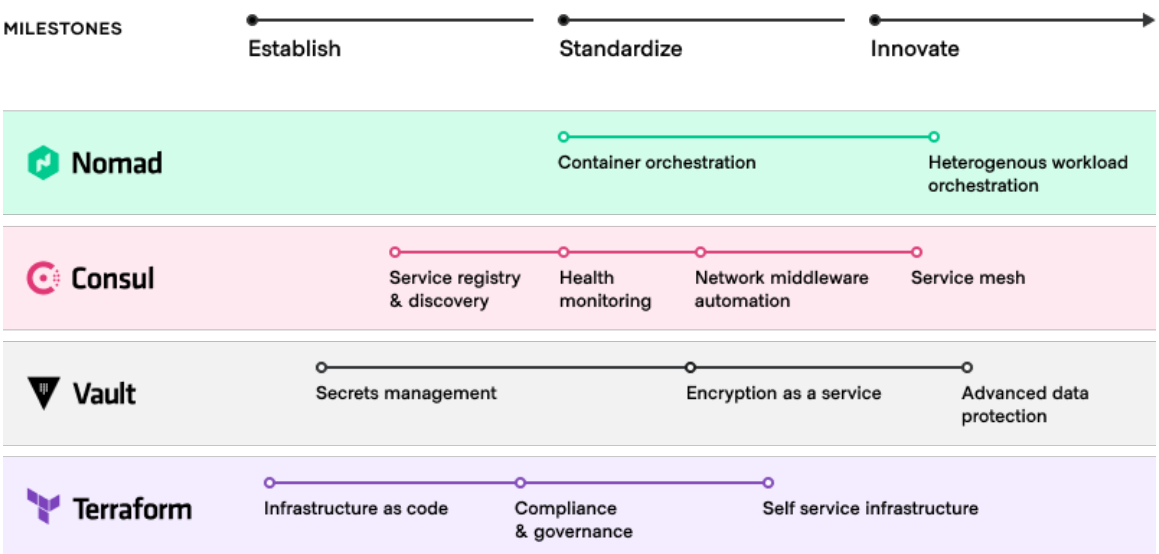
Hybrid Cloud
Application Automation

- Workload orchestration
- Container orchestration
- Hetergeneous orchestration

The typical journey to unlock the cloud operating model includes three major milestones:

- **Establish the cloud essentials:** At the beginning of the cloud journey, the immediate requirements are provisioning the cloud infrastructure — typically by adopting infrastructure as code and ensuring it is secure by implementing a secrets-management solution. These are the bare necessities to build a scalable, dynamic, and futureproof cloud architecture.
- **Standardize on a set of shared services:** As cloud consumption grows, enterprises need to implement and standardize on a set of shared services to take full advantage of the cloud's benefits. This can introduce challenges around governance and compliance, as setting access-control rules and tracking requirements become increasingly important.
- **Innovate using a common logical architecture:** Fully embracing the cloud and depending on cloud services and applications as the primary systems of engagement creates a need for a common logical architecture. This requires a control plane that connects with the extended ecosystem of cloud solutions and provides advanced security and orchestration across multiple services and clouds.

Example enterprise journey to unlock a Cloud Operating Model

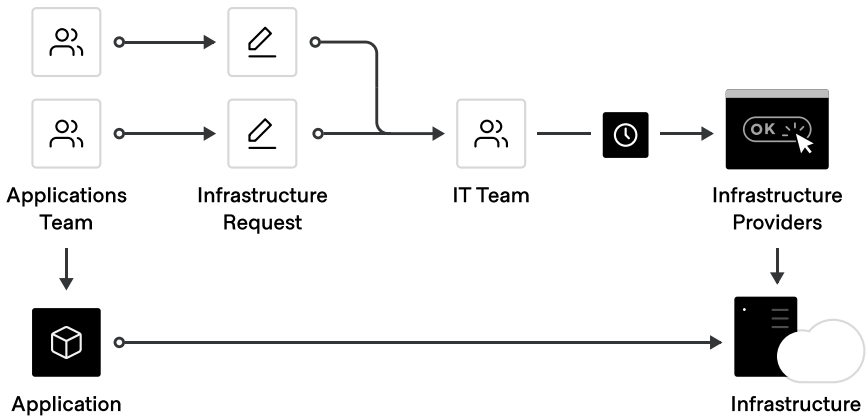


Hybrid Cloud Infrastructure Provisioning with HashiCorp Terraform

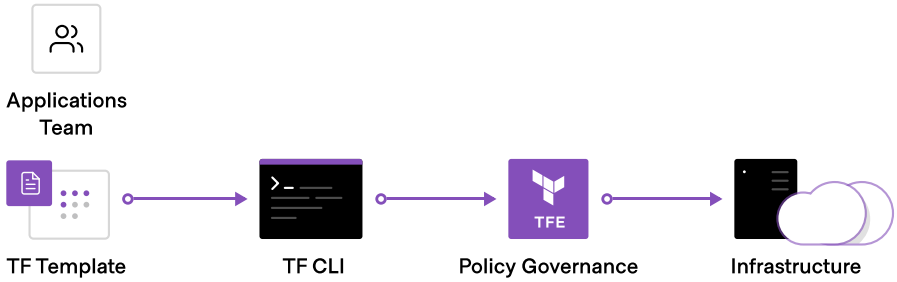
The foundation for adopting the cloud is infrastructure provisioning. HashiCorp Terraform is the world's most widely used cloud provisioning product. It can be used to provision infrastructure for any application using an ever-growing array of providers for popular platforms and technologies.

To create shared services for infrastructure provisioning, IT teams should start by implementing reproducible infrastructure as code practices, and then layering on compliance and governance workflows to ensure appropriate controls.

Before Terraform



After Terraform

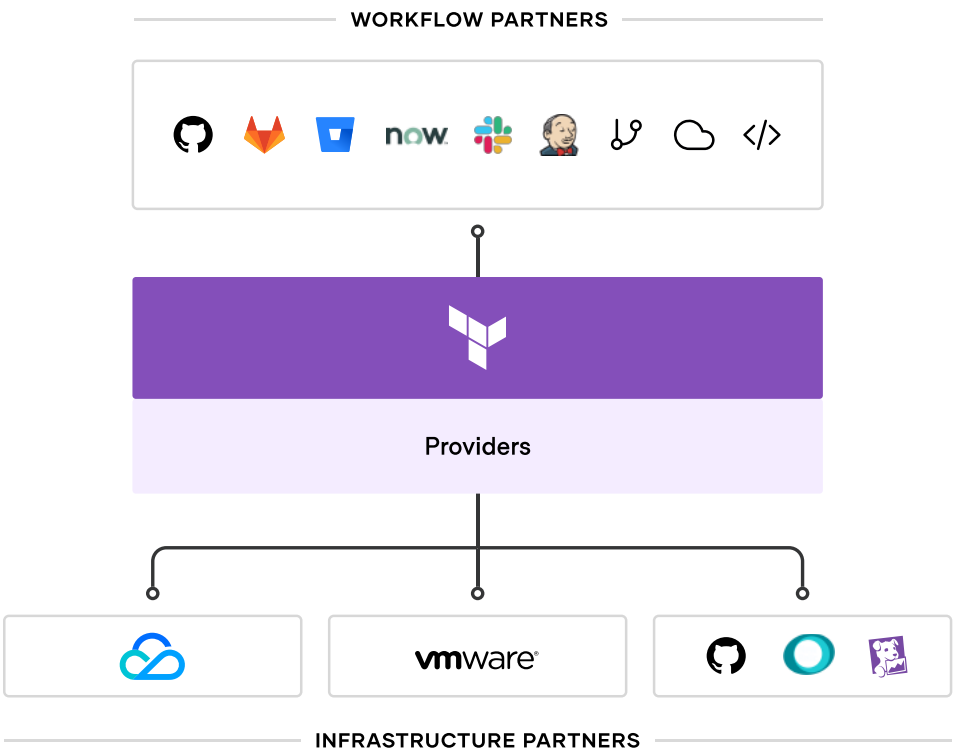


Reproducible Infrastructure as Code

The first goal of a shared service for infrastructure provisioning is to enable the delivery of reproducible infrastructure as code, providing DevOps teams a way to plan and provision resources inside CI/CD workflows using familiar tools.

DevOps teams can create Terraform templates that express the configuration of services from one or more cloud platforms. Terraform integrates with all major configuration-management tools to allow fine-grained provisioning following the provisioning of the underlying resources. Finally, templates can be extended with services from many other software providers, monitoring agents, application performance monitoring (APM) systems, security tooling, DNSs, content delivery networks, and more. Once defined, the templates can be provisioned as required in an automated way. That makes Terraform the *lingua franca* and common workflow for teams provisioning resources across Tencent Cloud, private clouds, and other infrastructure.

For self-service IT, decoupling the template-creation process and the provisioning process greatly reduces the time taken for any application to go live, since developers using pre-approved templates no longer need to wait for operations approval.



Compliance and Management

Most teams also need to enforce policies covering the type of infrastructure created, how it is used, and which teams get to use it. HashiCorp's Sentinel policy as code framework provides compliance and governance without requiring a shift in the overall team workflow. Sentinel is also defined as code, enabling collaboration and comprehension for DevSecOps.

Without policy as code, organizations typically resort to ticket-based review processes to approve changes. This can make developers wait weeks or longer to provision infrastructure. Policy as code solves this by splitting the definition of the policy from the execution of the policy.

Centralized teams codify policies enforcing security, compliance, and operational best practices across all cloud provisioning. Automated enforcement of policies ensures changes are in compliance without creating a manual review bottleneck.

HashiCorp Terraform and Tencent Cloud

HashiCorp and Tencent Cloud have worked closely to integrate Terraform over the past few years. Customers can use the Terraform CLI to automatically deploy and version the configuration files to Tencent Cloud within an hour, and environments are reproducible. There is no risk from patching, because you can test exact infrastructure templates. Engineers can focus on problem-solving and building rather than submitting and waiting on provisioning requests. Further, teams can deploy the same code to multiple regions, environments, and cloud providers in a consistent, safe manner.

Additional Benefits of Terraform on Tencent Cloud

- **Strong community:** Feedback from the community continues to drive improvements in using Terraform with Tencent Cloud. Comments are tracked in GitHub. This approach provides a single, familiar view where Terraform users can see the status and impact of their changes. The use of GitHub also enables continuous integration and testing for infrastructure changes. Explore more on the Github repository for the Terraform Provider for Tencent Cloud.
- **Enterprise-ready:** Streamline operations and provision any infrastructure more securely and efficiently with Terraform Enterprise. Centralize infrastructure deployment within one workflow and provision, govern, and audit any environment.

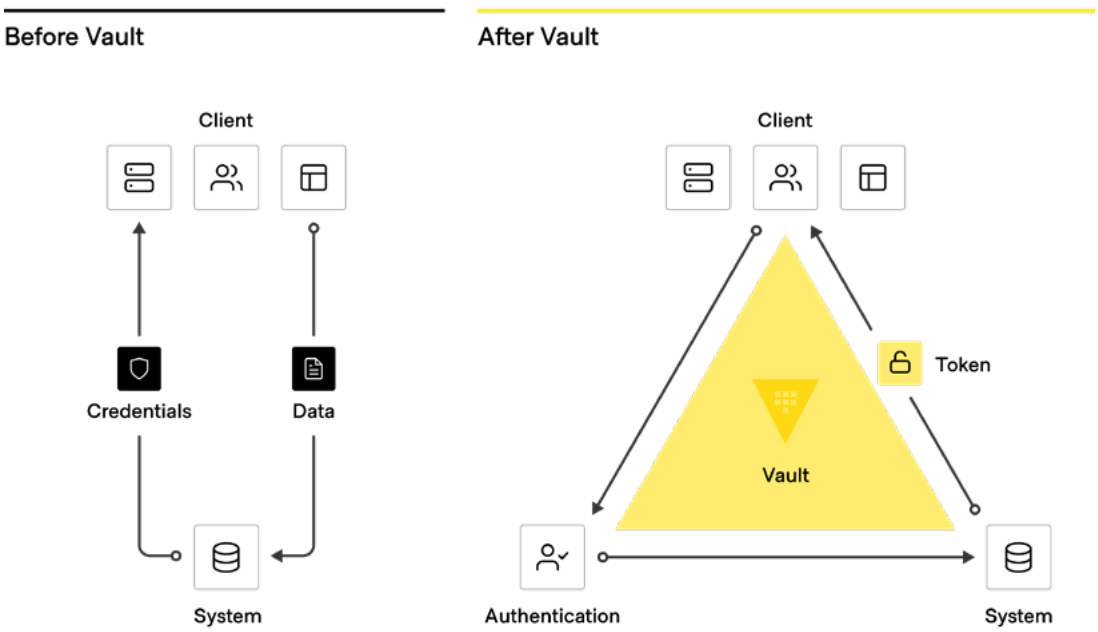
Hybrid Cloud Security with HashiCorp Vault

Dynamic cloud infrastructure means a shift from host-based identity to application-based identity, with low- or zero trust networks spanning multiple clouds without a clear network perimeter.

The traditional security world assumed high trust internal networks, which resulted in a hard shell and a soft interior. The modern zero trust approach works to harden the inside as well. This requires that applications be explicitly authenticated, authorized to fetch secrets and perform sensitive operations, and tightly audited.

HashiCorp Vault enables teams to securely store and tightly control access to tokens, passwords, certificates, and encryption keys for protecting machines and applications. This provides a comprehensive secrets management solution. Beyond that, Vault helps protect data at rest and data in transit. Vault exposes a high-level cryptography API for developers to secure sensitive data without exposing encryption keys. Vault also can act like a certificate authority, to provide dynamic short lived certificates to secure communications with SSL/TLS. Lastly, Vault enables the brokering of identity between different platforms, such as Tencent Cloud CAM, Active Directory in on-premises deployments, and other IAM services to allow applications to work across platform boundaries.

Vault is widely used across many industries — including stock exchanges, large financial organizations, and hotel chains — to provide security in the cloud operating model.



To achieve shared services for security, IT teams should enable centralized secrets management services, and then use those services to deliver more sophisticated Encryption-as-a-Service use cases such as certificate and key rotations and encryption of data in transit and at rest.

HashiCorp Vault Integrations on Tencent Cloud

Tencent Cloud has integrated Vault secrets engines and auth methods. Secrets engines are components that store, generate, or encrypt data. Secrets engines are very flexible, so it is easiest to think about them in terms of their function. Secrets engines are provided with some set of data, they take some action on that data, and they return a result. Auth methods are the components in Vault that perform authentication and are responsible for assigning identity and a set of policies to a user. In all cases, Vault will enforce authentication as part of the request processing.

Tencent Cloud CAM credentials can be used to authenticate systems and applications, which resolves the need to distribute initial access credentials. Moreover, Vault can dynamically generate and configure policies and role assignments. This provides users and applications outside of the cloud an easy method for generating flexible time- and permission-bound access into Tencent Cloud APIs.

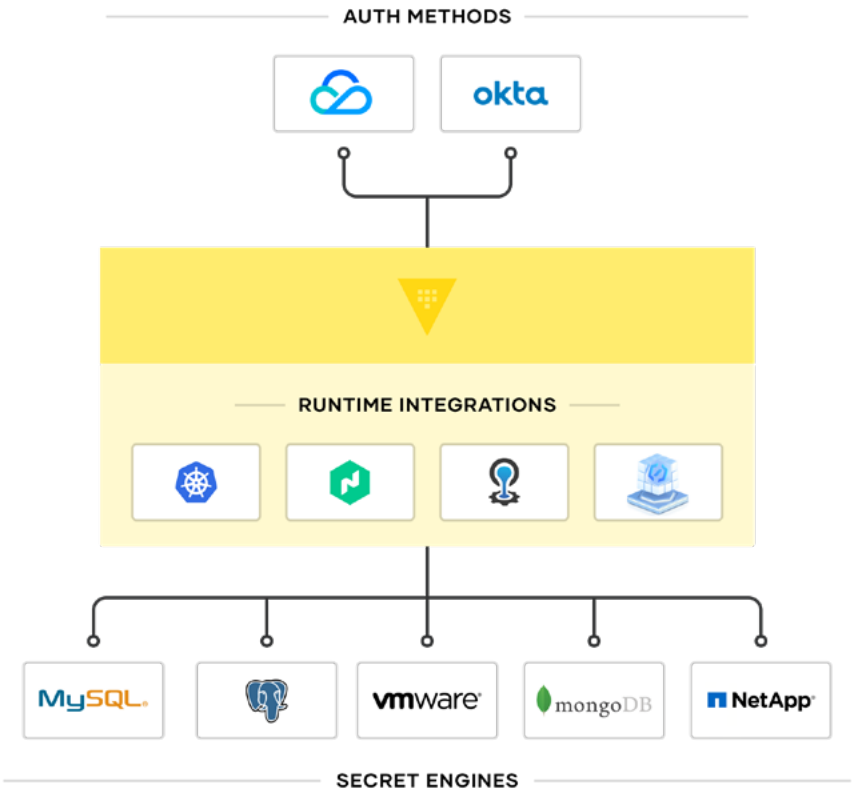
Using the Vault Tencent Cloud secrets engines plugin and auth methods plugin, customers can leverage all of the Vault features described below to automate their secrets management. Get more information on Vault Tencent Cloud plugins at vaultproject.io/docs/plugin-portal.

Secrets Management

The first step in cloud security is typically secrets management: the central storage, access control, and distribution of dynamic secrets. Instead of depending on static IP addresses, it's crucial to integrate with identity-based access systems such as Tencent Cloud CAM to authenticate and access services and resources.

Vault uses policies to codify how applications authenticate, which credentials they are authorized to use, and how auditing should be performed. It can integrate with an array of trusted identity providers such as cloud identity and access management (IAM) platforms, Kubernetes, Active Directory, and other Security Assertion Markup Language (SAML) based systems for authentication. Vault then centrally manages and enforces access to secrets and systems based on trusted sources of application and user identity.

Enterprise IT teams should build shared services that enable the request of secrets for any system through a consistent, audited, and secured workflow.



Encryption-as-a-Service

Additionally, enterprises need to encrypt application data at rest and in transit. Vault can provide Encryption-as-a-Service to provide a consistent API for key management and cryptography. This allows developers to perform a single integration and then protect data across multiple environments.

Using Vault as a basis for encryption as a service solves difficult security-team problems, such as certificate and key rotation. Vault enables centralized key management to simplify encrypting data in transit and at rest across clouds and datacenters. This helps reduce costs around expensive hardware security modules (HSM) and increases productivity with consistent security workflows and cryptographic standards across the organization.

While many organizations mandate developers to encrypt data, they often don't often explain the "how," which forces developers to build custom solutions without an adequate understanding of cryptography. Vault offers developers a simple, easy to use API, while giving central security teams the policy controls and lifecycle management APIs they need.

Advanced Data Protection

Organizations moving to the cloud or spanning hybrid environments must typically still maintain and support on-premises services and applications that need to perform cryptographic operations, such as data encryption for storage at rest. Development teams do not necessarily want to implement the logic around managing these cryptographic keys, and thus seek to delegate the task of key management to external providers. Advanced data protection allows organizations to securely connect, control, and integrate advanced encryption keys, operations, and management between infrastructure and Vault Enterprise, including automatically protecting data in MySQL, MongoDB, PostgreSQL, and other databases using transparent data encryption (TDE).

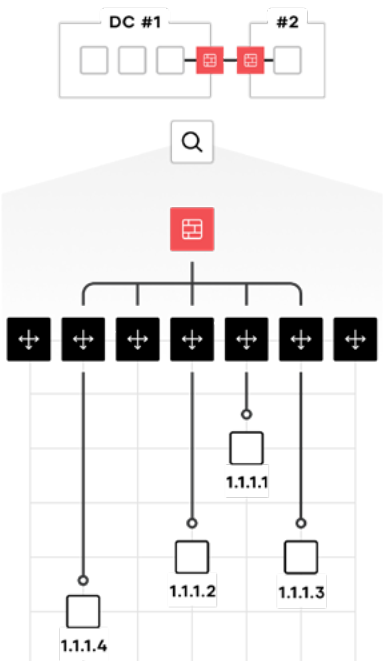
Organizations with high security requirements for data compliance (PCI DSS, HIPAA, etc.) often adopt more sophisticated technologies that can cryptographically protect anonymity for personally identifiable information (PII). Advanced data protection provides functionality for data tokenization, such as data masking, to protect sensitive data such as credit cards, sensitive personal information, bank numbers, and so on.

Hybrid Cloud Service Networking with HashiCorp Consul

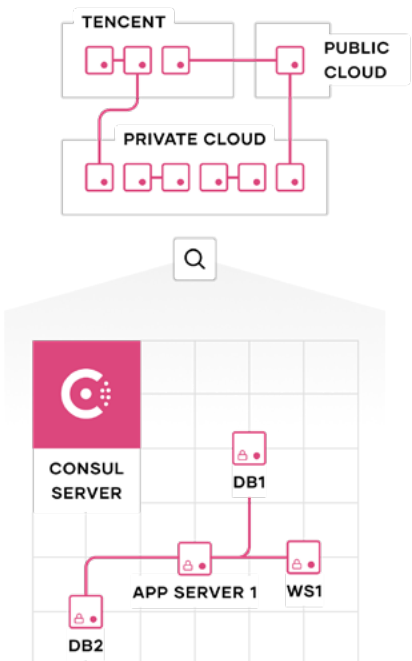
Networking in the cloud is often one of the most difficult aspects of adopting the cloud operating model. The combination of dynamic IP addresses, a significant growth in east-west traffic in microservices architectures , and the lack of a clear network perimeter is a formidable challenge. HashiCorp Consul provides a hybrid cloud service networking layer to connect and secure services. Consul is widely deployed at scale, with many customers running more than 100,000 nodes in their environments.

Networking services should be provided centrally, where a single IT team provides service registry and service discovery capabilities to development teams. A common registry provides a "map" of what services are running, where they are, and their current health status. The registry can be queried programmatically to enable service discovery or drive network automation of API gateways, load balancers, firewalls, and other critical middleware components. These middleware components can be moved out of the network using a service mesh approach, where proxies run on the edge to provide equivalent functionality. Service mesh approaches can simplify the network topology, especially for hybrid cloud and multi-datacenter topologies.

Before Consul



After Consul



Service Discovery

The starting point for networking in the cloud operating model is typically a common service registry, which provides a real-time directory of what services are running, where they are, and their current health status. Traditional approaches to networking rely on load balancers and virtual IPs to provide naming abstractions to represent a service with a static IP. Tracking the network location of services is often done with spreadsheets, load-balancer dashboards, or configuration files, all of which are disjointed manual processes prone to error.

Consul programmatically registers each service and provides DNS and API interfaces to enable any service to be discovered by other services. The integrated health check monitors each service instance's health status so the IT team can triage the availability of each instance.

What's more, Consul can help prevent routing traffic to unhealthy service instances.

Consul can integrate with other services that manage existing north-south traffic, such as traditional load balancers, and distributed application platforms such as Kubernetes, to provide a consistent registry and discovery service across multi-datacenter, hybrid cloud, and multi-platform environments.

Network Middleware Automation

The next step is to reduce the operational complexity of existing networking middleware through network automation. Instead of a manual, ticket-based process to reconfigure load balancers and firewalls every time there is a change in service network locations or configurations, Consul can automate these network operations. This is achieved by enabling network middleware devices to subscribe to service changes from the service registry, enabling highly dynamic infrastructure that can scale to significantly larger deployments than static-based approaches.

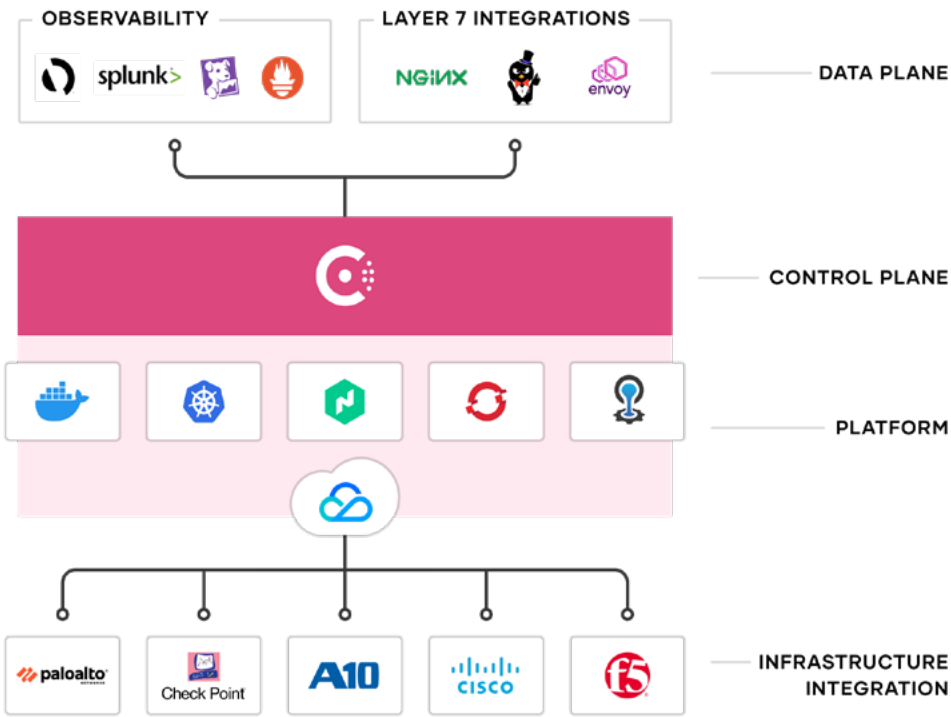
This decouples the workflow between teams, as operators can independently deploy applications and publish to Consul, while NetOps teams can subscribe to Consul to handle the downstream automation.

Zero Trust Networking with Service Mesh

As organizations scale with microservices-based and cloud-native applications, the underlying infrastructure becomes larger and more dynamic, leading to an explosion of east-west traffic. This can bring a proliferation of expensive network middleware that carry single points of failure and significant operational overhead.

Consul provides a distributed service mesh that pushes routing, authorization, and other networking functionalities to the endpoints in the network, rather than imposing them through middleware. This makes the network topology simpler and easier to manage, removes the need for expensive middleware within east-west traffic paths, and makes service-to-service communication much more reliable and scalable.

Consul is an API-driven control plane that integrates with sidecar proxies alongside each service instance (proxies such as Envoy, HAProxy, and NGINX). These proxies provide the distributed data plane. Together, these two planes enable a zero trust network model that secures service-to-service communication with automatic TLS encryption and identity-based authorization. Network operation and security teams can define the security policies with logical services rather than IP addresses.

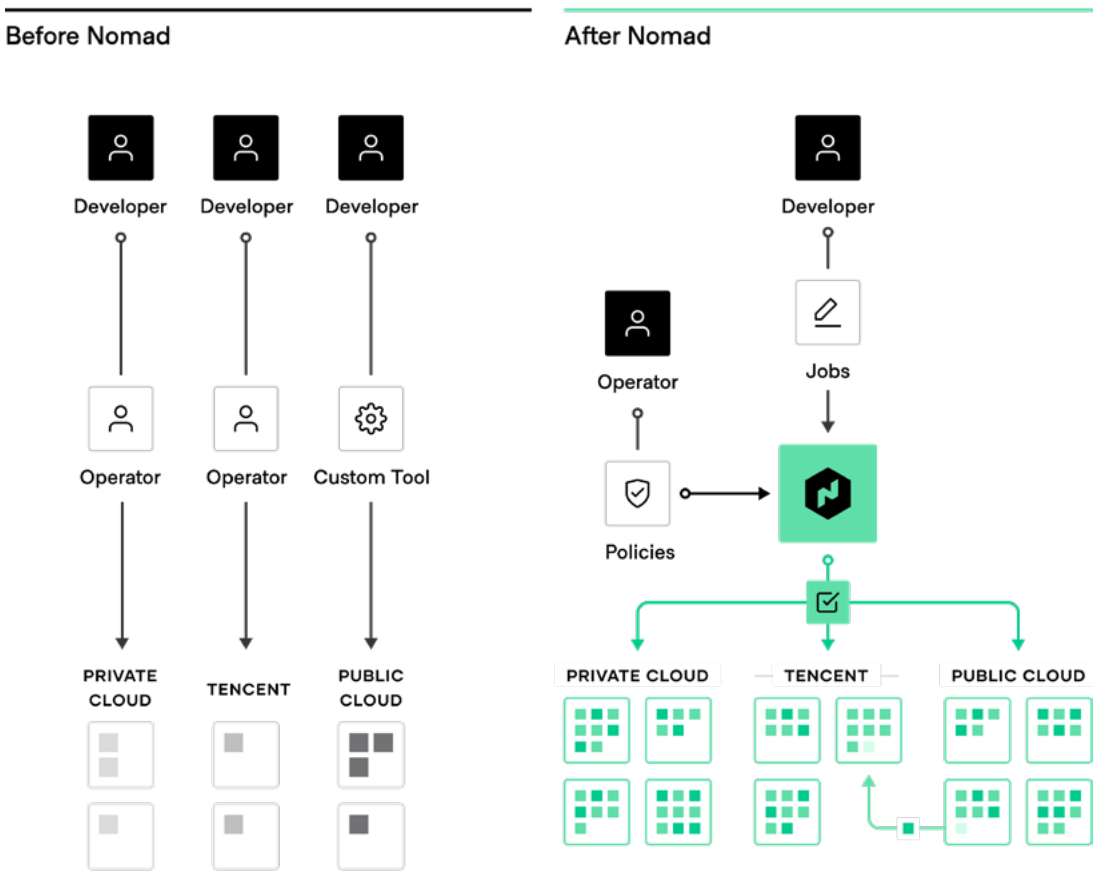


Consul enables fine-grained service segmentation to secure service-to-service communication with automatic TLS encryption and identity-based authorization. Consul can be integrated with Vault for centralized PKI and certificate management. Service configuration is achieved through an API-driven key-value store that can be used to easily configure services at runtime in any environment.

Hybrid Cloud Application Delivery with HashiCorp Nomad

Finally, at the application layer, new apps are increasingly distributed while legacy apps still need to be managed more flexibly. HashiCorp Nomad is a flexible orchestrator. Nomad can deploy and manage both legacy and modern applications for all types of workloads: from long-running services to short-lived batch jobs to system agents.

To get the benefits of shared services for application delivery, IT teams should use Nomad in concert with Terraform, Vault, and Consul. This combination enables the consistent delivery of applications on cloud infrastructure, while meeting necessary compliance, security, and networking requirements.

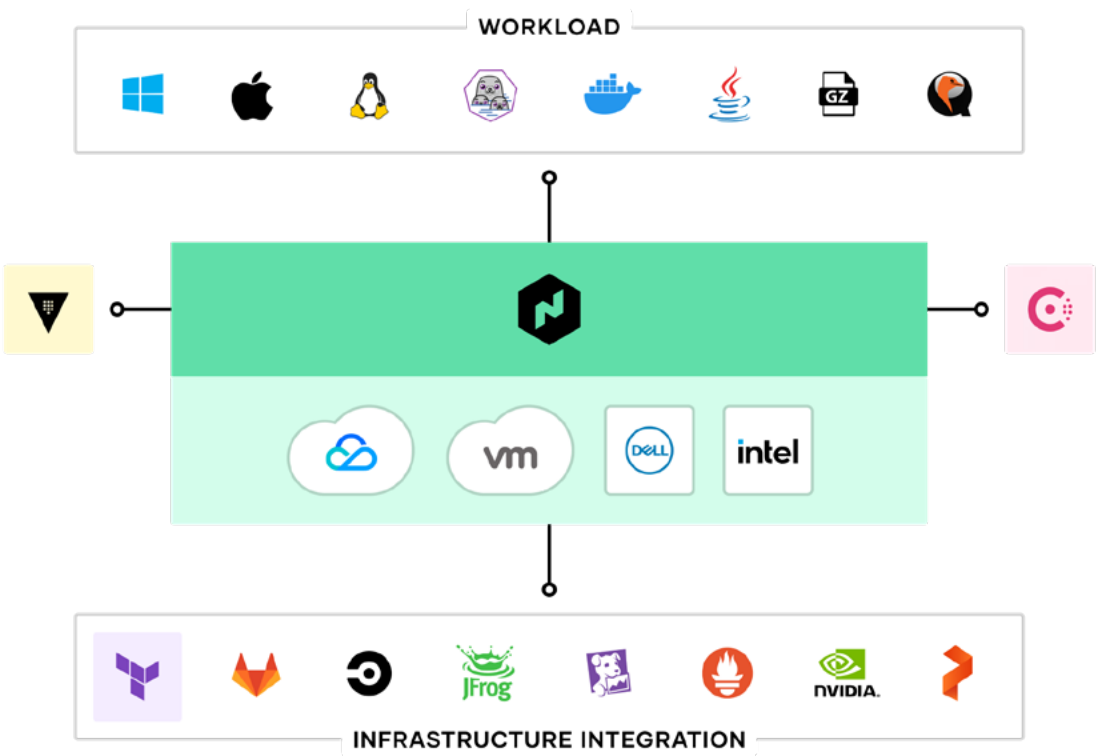


Mixed Workload Orchestration

Today, many new workloads are developed with container packaging to be deployed to Kubernetes or other container-management platforms. But many legacy workloads will not be moved onto those platforms, nor will future serverless applications. Nomad provides a consistent process for deployment of all workloads from virtual machines through standalone binaries and containers. It provides core orchestration benefits across all those workloads, such as release automation, multiple upgrade strategies, bin packing, and resilience.

For modern applications — typically built in containers — Nomad provides the same consistent workflow at scale in any environment. Nomad is focused on simplicity and effectiveness at orchestration and scheduling, and avoids the complexity of platforms such as Kubernetes that require specialist skills to operate and solve only for container workloads.

Nomad integrates into existing CI/CD workflows to provide fast, automatic application deployments for legacy and modern workloads.



High Performance Computing

Nomad is designed to schedule applications with low latency across very large clusters. This is critical for customers with large batch jobs, as is common with high performance computing (HPC) workloads. In the 2 Million Container Challenge, Nomad was able to schedule one million instances of Redis across 5,000 machines in three datacenters, in less than 5 minutes. Several large Nomad deployments run at even larger scales.

Nomad makes it easy for high-performance applications to use an API to consume capacity dynamically, enabling efficient sharing of resources for data analytics applications like Spark. The low latency scheduling ensures results are available quickly and minimizes wasted idle resources.

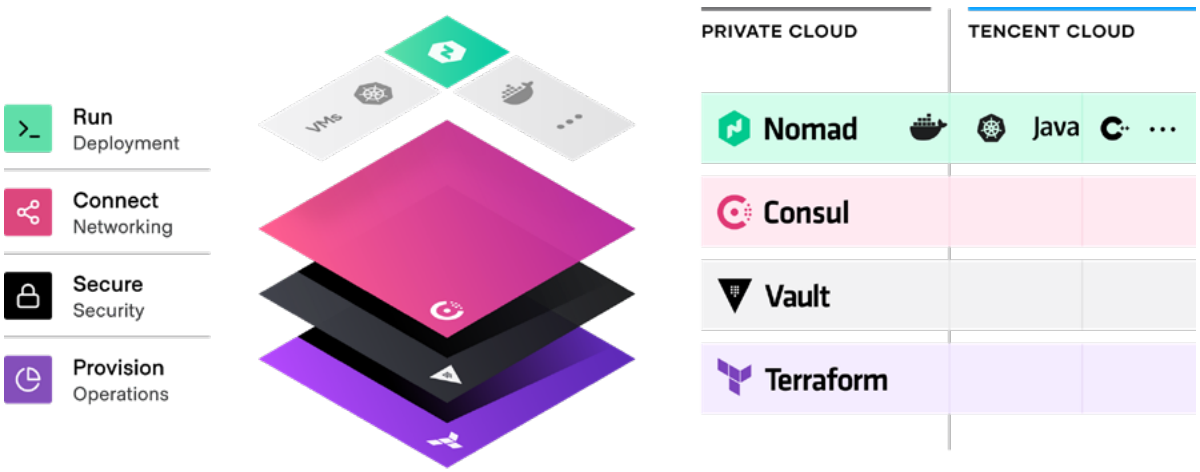
Multi-Datacenter Workload Orchestration

Nomad is multi-region and hybrid cloud by design, with a consistent workflow for deploying any workload. As teams roll out global applications in multiple datacenters or across cloud boundaries, Nomad provides orchestration and scheduling. The product is supported by infrastructure, security, and networking resources, to help ensure the application is successfully deployed.

Industrialized Application Delivery Process

Ultimately, these shared services across infrastructure, security, networking, and application runtime present an industrialized process for application delivery, while taking advantage of the dynamic nature of each layer of the cloud.

Embracing the cloud operating model enables self-service IT that is fully compliant and governed, and enables teams to deliver applications at increasing speed.



Conclusion

In conclusion, the transition to Tencent Cloud, and hybrid-cloud environments is a generational and inevitable transition for IT. Each organization has its own unique and special journey. This is not an easy challenge, but the outcome can be transformational. Organizations that successfully complete the transformation can deliver new business and customer value more rapidly and at a large scale. They can also save on operational costs by running their infrastructure on demand around the world.

To successfully execute this transition, it is important to understand the current static state, the target dynamic state, have a thorough migration plan, and adopt the right tools. Leveraging the cloud operating model with HashiCorp and Tencent Cloud can help simplify the complexity of transformation, accelerate the migration process, and establish new self-service IT processes using the right tools designed for a new, dynamic environment.

About HashiCorp and Tencent Cloud

HashiCorp and Tencent Cloud have a long-standing relationship driven by the companies and the community built around their tools. Organizations of all sizes trust HashiCorp tools to provision, secure, run, and connect applications running in Tencent Cloud. Tencent Cloud proactively integrated and built communities with HashiCorp tools and committed to continuously integrating its products with HashiCorp services. This partnership drives Tencent Cloud and HashiCorp to innovate newer and better cloud implementation methods for enterprise organizations.

About Tencent

Tencent Cloud is one of the leading cloud providers in the world with a focus on helping global enterprises succeed in China. With an extensive presence across China, global engagement teams based around the world, and decades of experience deeply rooted in delivering optimal digital engagement to its massive user base, Tencent Cloud offers a powerful and robust cloud solution specifically designed to address the unique challenges faced by enterprises as they expand into China.

Tencent Cloud is part of a rich digital ecosystem that includes some of China's top social, messaging, mobile payment, gaming, digital literature, music streaming, and video platforms. With over a billion users, Tencent is a global technology leader and the largest technology company in Asia.

Go to market faster in China with the leading China native cloud solution that provides less complexity and more certainty for success.

About HashiCorp

HashiCorp is a leader in hybrid cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows and a standardized approach to automating the critical process involved in delivering applications in the cloud: infrastructure provisioning, security, networking, and application deployment. HashiCorp's open source tools Vagrant™, Packer™, Terraform®, Vault™, Consul®, Nomad™, Boundary, and Waypoint™ were downloaded approximately 100 million times during the fiscal year ended January 31, 2021. Enterprise and managed service versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-datacenter functionality. The company is headquartered in San Francisco, though 90% of HashiCorp employees work remotely, strategically distributed around the globe.

HashiCorp