



Automating application delivery in the cloud operating model

Accelerating digital transformation in a modern, multi-cloud datacenter with F5 and HashiCorp



Executive summary

To realize the benefits of digital transformation and thrive in an era of multi-cloud architecture, driven by digital transformation, Enterprise IT must simplify operations with consistency at every layer of the cloud operating stack.

For most enterprises, digital transformation is a journey to move business from relying on mostly manual processes to embracing orchestrated, digital workflows that involve multiple business functions. From marketing to IT, from product development to customer service, digital transformation enables business to deliver new value more quickly, and at scale. The implication for Enterprise IT is a shift from managing isolated systems to operating integrated services. The cloud and cloud-native applications are an inevitable part of this shift as both present the opportunity to rapidly deploy on-demand applications with effortless scale.

These applications were not designed or developed with functions such as scale, security, and availability in mind. Such operational functions – application services – are inserted into the path between the application and its end user during deployment. They provide critical business functions required to ensure a fast, secure user experience.

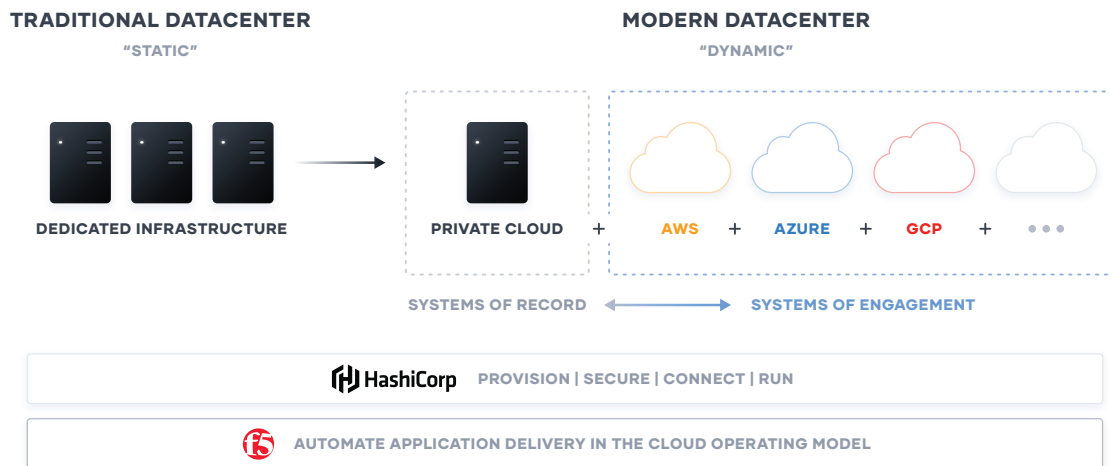
The application services that deliver and secure applications are a heterogeneous mix of commercial, cloud-based, and open source solutions. Each adds complexity with distinct operational consoles, APIs, and policies.

To unlock the fastest path to value of the cloud, enterprises must consider how to simplify this complexity by embracing the cloud operating model, and tuning people, process, and tools to it. In part, this entails embracing cloud and platform independent application services, infrastructure, and tools. Doing so reduces complexity along with tool sprawl, and helps organizations avoid being locked-in by cloud.

In this paper, we examine how F5 and HashiCorp combine to simplify multi-cloud complexity and accelerate Enterprise IT's digital transformation.

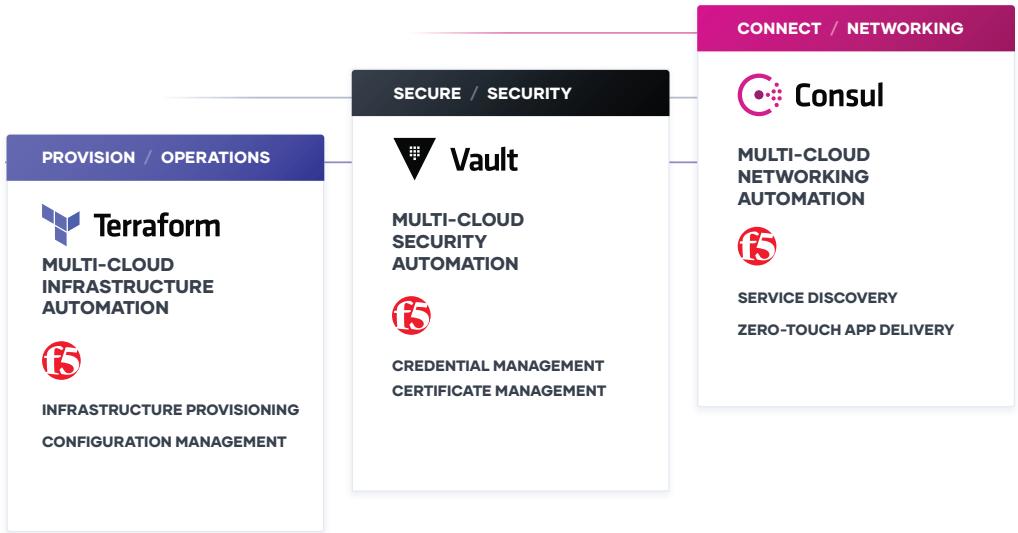
Transitioning to a multi-cloud datacenter

While most enterprises began with only one cloud provider, research indicates a majority now (51%) operate applications in multiple cloud environments. The challenges arising from this reality range from inconsistent security to siloed operations created by the distinct operational models of each cloud environment. These challenges are exacerbated by an increasingly multi-generational application portfolio spanning architectures from monoliths to microservices.



The [HashiCorp Cloud Operating Model](#) is a blueprint for how organizations migrate to, and address the challenges of, a multi-cloud reality, to take advantage of a computing model that scales dynamically, on demand. No single vendor can address all the people and process challenges. This is where partnerships are needed to surface solutions collaboratively. Enterprises should plan and build workflows for consistent automation at every layer infrastructure, security, networking, and runtime.

Details of the process and challenges can be seen in HashiCorp's [Unlocking the Cloud Operating Model](#) white paper, but here we instead drill down into the layers of securing and scaling applications with application services in multi-cloud environments. Managing the application service lifecycle is critical to ensure consistent and secure deployments across multiple clouds, to deliver on the Cloud Operating Model.



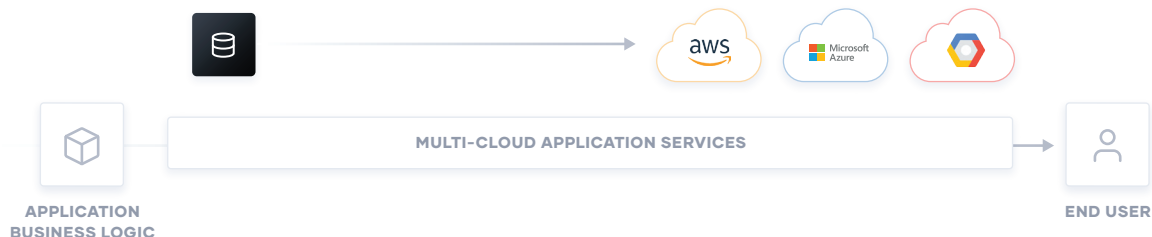
Simplifying multi-cloud complexity

The cloud presents an opportunity for organizations to expand their digital capabilities – applications – business needs to engage users and customers. These applications have become the new, digital face of a business and their ability to provide an exceptional experience is critical to success. The digital customer experience is based primarily on two characteristics: availability and performance. Failure to meet customer expectations with respect to these characteristics can be disastrous, with PWC noting that **32% of customers** will abandon a business after just one bad experience.





For most enterprises, the need to meet availability and performance expectations is realized with application services. The confusing array of options with which to ensure scale and speed across public and private cloud environments leaves most enterprises operating with a mismatched set of application services. **Our research** showed that 69% of organizations use ten or more application services to address security, scale, and performance needs.

For most organizations, each of these application services are managed separately with its own tools. This results in siloed teams and high operational complexity. These siloed tools and teams also result in limited visibility across the application delivery chain. Hence there is no holistic view of the business impact.

The challenge for most enterprises then is how to deploy and operate a consistent set of application services in a multi-cloud environment while reducing friction across various operational teams.



The HashiCorp Cloud Operating Model provides insight into the changes required for both applications and infrastructure to operate in this multi-cloud reality.

	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 Heterogeneous

HashiCorp and F5 automate application services

Terraform and F5 integrations provide the foundation for quickly and consistently provisioning application infrastructure and services in a multi-cloud model. Standardizing on application services enables a common operating model that addresses challenges associated with people, process, and tools in a multi-cloud reality:

- **People.** How can we enable a team for a multi-cloud reality, where skills can be applied consistently regardless of target environment?
- **Process.** How do we position central IT services as a self-service enabler of speed, versus 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 in pursuit of better customer and business value?

The answers to these questions are more complex in a multi-cloud reality. The introduction of new tools, operating models, and environments increases the burden on teams responsible for deploying and operating application services. This burden is made more challenging by the reality that multiple teams across IT - often operating in siloed structures - are all responsible for these services.

The result is a workflow that starts and stops as it crosses team boundaries and may stall when manual approvals are required to complete a given deployment task. To simplify deployment processes, organizations should strive to create a centralized workflow that enables each team to operate independently but are all aligned in the way they provision and update the application services infrastructure. This is where Terraform and BIG-IP can help.

Provision: HashiCorp Terraform and F5 BIG-IP

Using BIG-IP and Terraform, customers will be able to deploy platform and cloud independent infrastructure and application services. This enables organizations to accelerate their digital transformation journey by expanding and scaling their digital capabilities without suffering the slow down of siloed operational teams and tools.

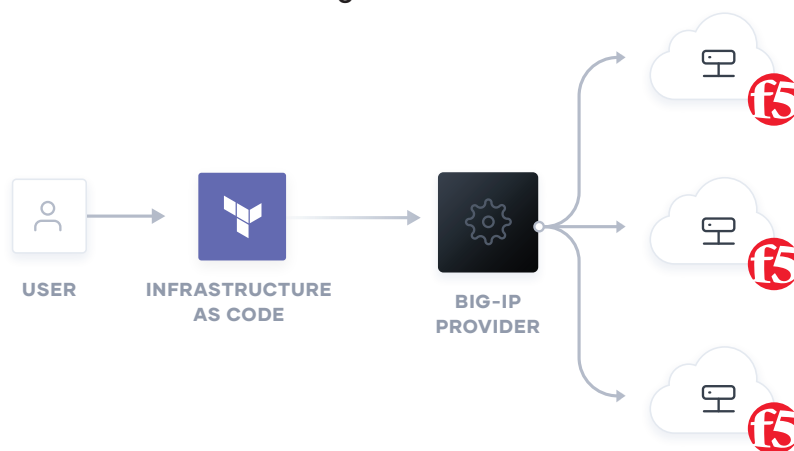
Terraform is the world's most widely used cloud provisioning product and can be used to provision infrastructure for any application using an array of providers for any target platform. To achieve shared services for infrastructure provisioning, IT teams should start by implementing reproducible infrastructure as code practices, and then layering compliance and governance workflows to ensure appropriate controls.

F5 BIG-IP is a platform for delivering application services that enable the scale, security, and performance of applications anywhere. Load balancing, access control, web application firewall, and encryption offload are among the application services that can be deployed and managed on a BIG-IP.

F5 integrations with Terraform enables customers to:

- Provision and manage F5 BIG-IP in large-scale, multi-cloud architectures
- Rapidly spin up and tear down infrastructure based on demand
- View configuration changes that are about to be applied – before applying them
- Enable policy and governance to match the speed of delivery with compliance to manage risk in a self-service environment

Terraform automates BIG-IP management



Deploy and manage F5 BIG-IP configurations as code using Terraform

Additionally, by using the BIG-IP provider Terraform can be used to automate BIG-IP configuration. The BIG-IP provider is enabled with integrations into the F5 automation toolchain supporting stateful configuration management.

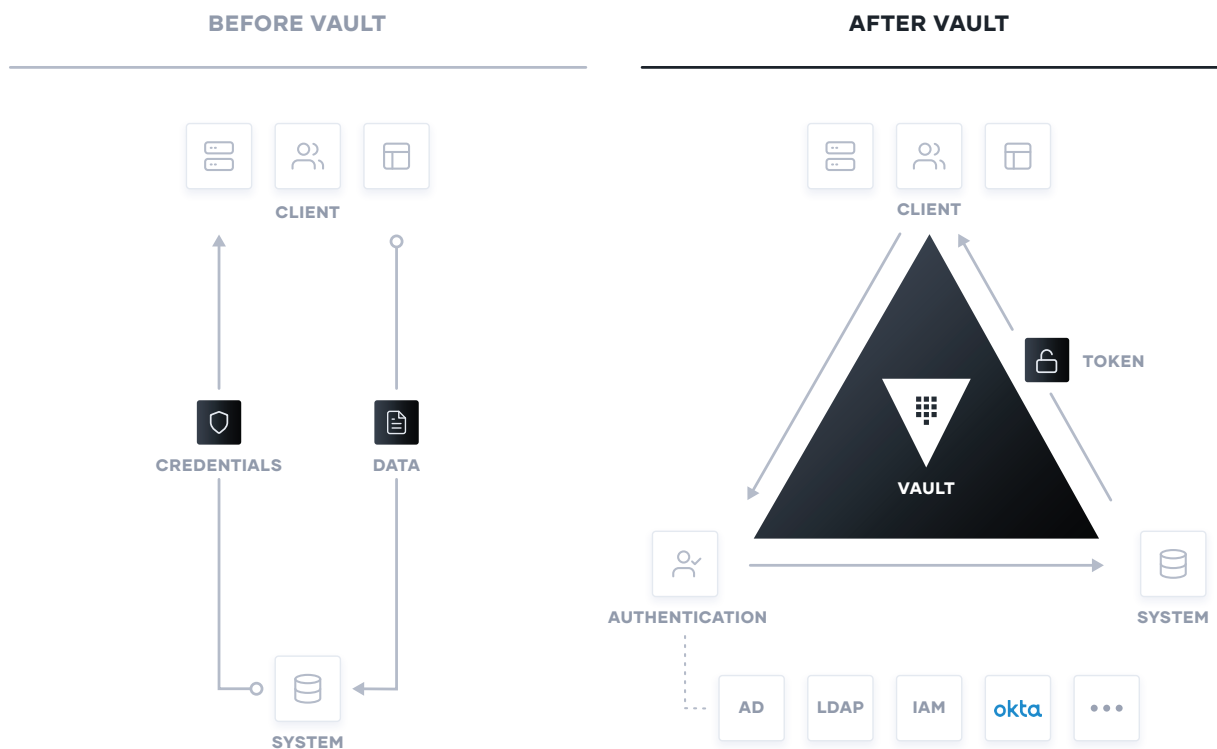
This capability enables teams to:

- Manage the entire application as code (infrastructure and application services)
- Scale application services and resources on-demand

Secure: HashiCorp Vault and F5

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, integrating with identity-based access systems such as AWS IAM and Azure AAD to authenticate and access services and resources is crucial.

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 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.



Infrastructure in any environment requires credentials to manage and operate. Vault can generate dynamic user credentials and certificate passphrases for BIG-IP, which can then be integrated into the BIG-IP provisioning process via Terraform. This eliminates the risky practice of hardcoding passwords in repositories and improves security practices across a multi-cloud environment.

Additionally, the key and certificate management capabilities of Vault provide an answer to a significant pain point for customers, that of renewing certificates. With security top of mind and best practices urging more frequent certificate rotations, customers are stressed by the need to manually renew and deploy new certificates. Vault can connect with certificate authorities (CA) and renew expiring certificates. With F5 and Vault, customers will be able to automate certificate management and reduce the risk of failing to renew certificates.

Connect: HashiCorp Consul and F5/NGINX

Based on our research, nearly 15% of the enterprise application portfolio today is built using microservices. Nearly one in five (19%) of customers indicate a preference for deploying application services in a containerized environment.

The adoption of modern application architectures is driven, in part, by the need for speed, efficacy, and scale across multiple cloud properties. But they are not islands and are often connected to and integrated with traditional applications that reside on-premises. This reality leaves operators struggling with very different networking models. The need for solutions that bridge this gap continues to be important to organizations as they embark on efforts to embrace cloud computing.

Consul enables cloud networking automation with a central shared registry to discover, connect and secure services across any runtime platform and cloud. F5's NGINX Application Platform is a suite of products that together form the core of what organizations need to create applications with performance, reliability, security, and scale.

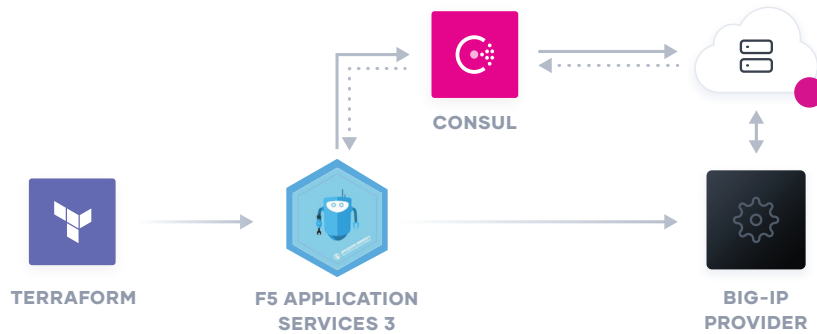
F5 and NGINX integrate with Consul to support the dynamic, service-based infrastructure of the Cloud Operating Model. Both solutions can act as an ingress and egress proxy in the Consul connect model.

Through its [AS3 extension](#), BIG-IP does service discovery with Consul. This capability greatly simplifies networking tasks by employing automation.

The dynamic nature of modern environments places consideration pressure to frequently update resource pools and networking attributes to ensure availability and connectivity. Neither cloud nor container-based environments eliminate the need for networking. Both environments still rely on standard IP-based networking constructs to route and forward traffic to and from an application. Without this capability, there is no connectivity. Both cloud and container-based environments offer the ability to automate those networking tasks, thereby enabling connectivity and, more importantly, the automation of that connectivity.

By employing Terraform and AS3, BIG-IP configurations are automatically updated to reflect the current state of an environment at both the network and application layers. Using information polled from Consul, AS3 automatically adds or removes BIG-IP pool members as needed without manual intervention, further simplifying day 2 operations and improving operator productivity.

This capability also enables organizations to offer self-service capabilities directly to developers. By automating the operation of connectivity and availability within modern application environments, developers need not request operator intervention to provision and operate infrastructure. Automation enables self-service, which improves productivity for both operators - who can focus on other critical tasks - and developers, who can move with speed to deliver new features and capabilities to the business.

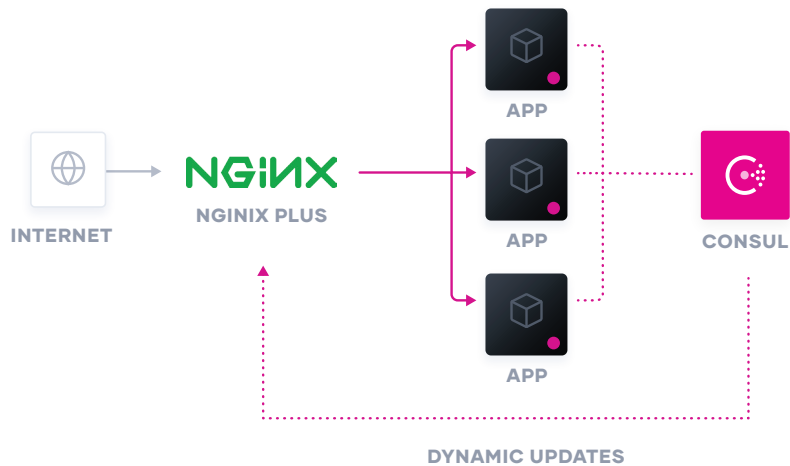


Accelerate application delivery by automating networking related tasks. Enable end to end automation.

This capability is also [available for NGINX Plus](#).

Automated management of pool members for both BIG-IP and NGINX Plus:

- Enables organizations to expand application footprints across multiple clouds without sacrificing security or performance
- Eliminates error prone manual steps and IT tickets, reducing friction between teams competing for valuable operational attention



Realizing consistency with multi-cloud application services

As companies progress on their digital transformation journey and begin to expand their digital capabilities across applications and cloud properties, they will encounter challenges to consistent operation and management of the application services that deliver and secure those capabilities.

Application services present an opportunity to standardize to realize the consistency of operation, management, and ultimately, capabilities. Through standardization on multi-cloud application services, organizations will benefit by reducing tool sprawl, optimizing processes, and enabling people to break down silos and provide self-service IT. Self-service IT for all components of the cloud operating model is paramount to enabling organizations to choose speed when delivering new capabilities to their customers.

Conclusion

A common cloud operating model is an inevitable shift for enterprises aiming to maximize their digital transformation efforts. F5 and HashiCorp provide solutions for each layer of the cloud to enable enterprises to make this shift to the cloud operating model.

Enterprise IT needs to evolve away from ITIL-based control points with its focus on cost optimization, toward becoming self-service enablers focused on speed optimization. It can do this by delivering shared services across each layer of the cloud designed to assist teams deliver new business and customer value at speed.

Unlocking the fastest path to value in a modern multi-cloud data center through adopting a common cloud operating model means shifting characteristics of Enterprise IT:

- **People: Shifting to multi-cloud skills**
 - Reuse skills from internal data center management and single cloud vendors and apply them consistently in any environment.
 - Embrace DevSecOps and other agile practices to continuously deliver increasingly ephemeral and distributed systems.
- **Process: Shifting to self-service IT**
 - Position Central IT as an enabling shared service focused on application delivery velocity: shipping software every more rapidly with minimal risk.
 - Establish centers of excellence across each layer of the cloud for self-service delivery of capabilities.
- **Tools: Shifting to dynamic environments**
 - Use tools that support the increasing ephemerality and distribution of infrastructure and applications and that support the critical workflows rather than being tied to specific technologies.
 - Provide policy and governance tooling to match the speed of delivery with compliance to manage risk in a self-service environment.

Addressing all three characteristics can be achieved by adopting cloud and platform independent tools, infrastructure, and application services. Reducing the number of languages, frameworks, and policies people need to learn, use, and maintain will provide a means to avoid being locked into a cloud and enable greater consistency and predictability in application deployments everywhere.

With thanks to Lori Mac Vittie

