HashiCorp
an IBM Company

WHITE PAPER

Infrastructure Lifecycle Management with the HashiCorp Cloud Platform

Do cloud right with a unified platform to build, deploy, and manage your infrastructure.

Executive summary

Over the last decade, most organizations have adopted the cloud to run some or all of their applications. Still, only 10% realize the business impact they thought they would — cutting costs, improving resilience, and driving new revenue. Why does it seem like organizations often get cloud wrong?

At HashiCorp, we have the opportunity to work with all types of organizations and individuals in our community, showing us a range of issues facing developers and IT operations. We talk with dozens of individual users every day and hundreds of companies every single week to discuss their ongoing development and operational challenges. At the majority of companies adopting cloud infrastructure, we see three stages of maturity:

- **Stage 1 - Adopting:** Organizations provision and manage cloud resources directly through infrastructure as code and multiple teams work on a common code base to encourage the reuse of common patterns. This reduces the need for development teams to reinvent existing processes and eliminates manual errors.
- **Stage 2 - Standardizing:** Organizations create, test, and validate standard images and reusable modules of infrastructure code and publish them to internal libraries to ensure consistency and ease patches and updates. They also use policy as code to enforce security and regulatory requirements before provisioning resources.
- **Stage 3 - Scaling:** Organizations enable self-service with an internal developer platform (IDP) to provide development teams with preconfigured templates and workflows to automate the creation of their application environments. They also consistently monitor their environments, automatically remediate issues as they arise, and effectively manage resource decommissioning.

This white paper explores the infrastructure challenges organizations face that keep them from realizing the full benefits of their cloud investments. It lays out a blueprint for successful Infrastructure Lifecycle Management (ILM) with The Infrastructure Cloud, an integrated portfolio of products powered by the HashiCorp Cloud Platform (HCP) that automates the building, deployment, and management of the infrastructure supporting critical applications.

For a high-level overview of The Infrastructure Cloud and how it can help your organization, please see the Infrastructure Cloud white paper.

Table of Contents

Three pitfalls of early cloud adoption

Migrating to cloud infrastructure outsources the task of running a datacenter to the experts at Amazon, Microsoft, Google, etc. The cloud provides an environment where developers can create and deploy applications rapidly. These are all good things, but when speed and convenience are the only two concerns in cloud migration, organizations often encounter three pitfalls:

Inefficiency from IT decentralization

When teams are given cloud access and very little guidance or guardrails, IT becomes decentralized, fragmented, and hard to scale. While teams may see velocity gains early on, in this "wild west" environment, productivity gains eventually taper off and the organization does not achieve the promised business value.

Greater risk from a lack of embedded security

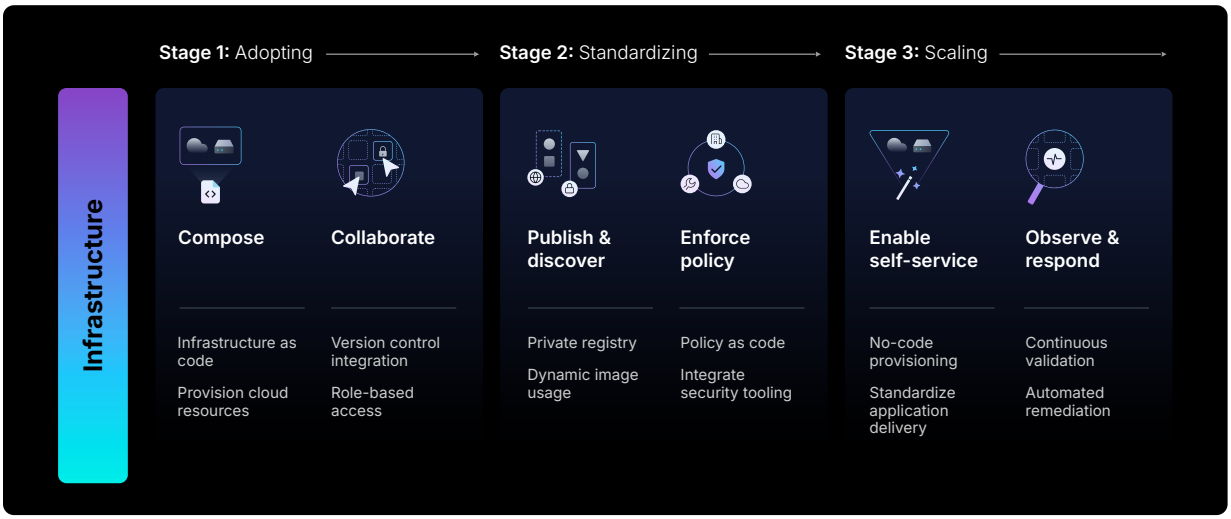
If there aren't enough shared best practices, guardrails, tools, or workflows across an organization, security also becomes extremely difficult and tedious to manage. Early in cloud adoptions, organizations often end up with weaker security controls across their teams compared to on-premises, in-house infrastructure approaches. Without embedded guardrails and standardized approaches, security can become an afterthought, exposing the organization to major risks. Security in the cloud is not the same as security in the datacenter.

Higher cloud costs from unchecked usage

As the number of tools and services used rises, managing infrastructure across this growing footprint becomes increasingly difficult. Organizations often end up provisioning more infrastructure than what is needed for their workloads, or they lose visibility at scale, leaving unneeded infrastructure deployed and running up their cloud spend.

A maturity based-blueprint for cloud infrastructure success

Addressing the aforementioned challenges requires a modern, holistic approach to infrastructure management across people, processes, and tools. Over the last decade, HashiCorp has helped thousands of customers mature their use of the cloud and deliver on



their business objectives. This work has revealed a consistent three-stage maturity blueprint for organizations to incrementally derive greater business value from the cloud:

- **Stage 1 - Adopting:** Cloud usage is defined by individual teams engaging with cloud providers in silos, tools are discovered by individual developers, and the business focuses on delivering the infrastructure needed to support applications and services as quickly as possible. Having teams adopt **infrastructure as code** (IaC) is a step in the right direction at this stage, however, with a lack of a common platform, cross-team collaboration is limited and it is difficult, if not impossible, to consistently enforce cost control or security/governance policies across the entire organization.
- **Stage 2 - Standardizing:** As cloud usage increases, organizations begin to incorporate a programmatic approach to cloud consumption, focusing on gaining control of their cloud estate. A centralized **platform team** presents infrastructure as a common shared service and uses **policy-as-code** to enforce best practices across the organization. This accelerates developer productivity by automating many of the manual tasks associated with deploying cloud resources. Developers no longer need to have extensive skills in configuring infrastructure because the platform team is providing self-service infrastructure code templates (i.e. modules).
- **Stage 3 - Scaling:** As an organization's cloud journey matures, the platform team extends and unifies its workflows and best practices across the entire digital estate, including multiple cloud providers, SaaS applications, and on-premises datacenters. The platform team offers the organization increasingly sophisticated capabilities, from auto-remediation of configuration issues, org-wide auditing, automated infrastructure and security compliance, and full self-service provisioning.

This blueprint gives organizations a maturity model to benchmark where they stand in their cloud journey and suggests the next steps toward modernizing their approach to cloud infrastructure.

Infrastructure Lifecycle Management with the HashiCorp Cloud Platform

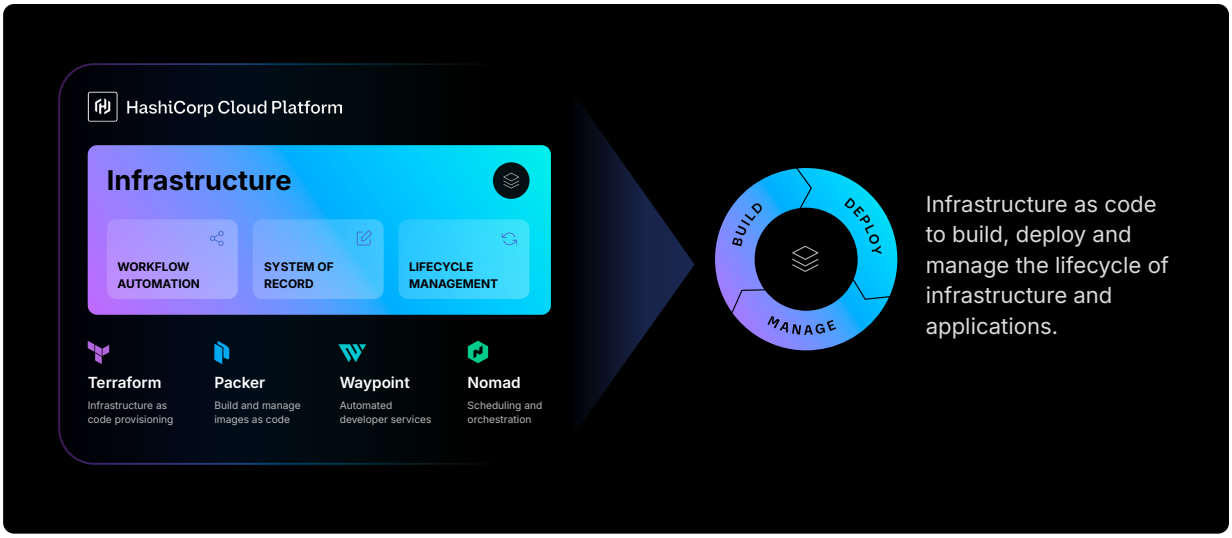
As we've worked closely with thousands of the world's largest organizations to understand their infrastructure challenges, we have seen two common themes emerge across all stages of maturity:

1. Well-architected Infrastructure Lifecycle Management is the foundation for successful cloud adoption.
2. To work efficiently with multiple cloud providers, services, and third-party applications, a successful cloud program uses golden patterns — presented as IaC — to consistently build, deploy, and manage infrastructure across all teams.

HashiCorp's **Infrastructure Lifecycle Management (ILM)** portfolio, delivered via the **HashiCorp Cloud Platform (HCP)**, is designed to address the challenges faced in each stage of the infrastructure lifecycle — Day 0 (build), Day 1 (deploy), and Day 2+ (manage). It offers turnkey tools and workflows needed to consistently deliver the infrastructure underpinning cloud applications from initial provisioning to maintenance, and eventual decommissioning. With HCP, platform teams are able to abstract complexities away from core development teams while ensuring they always use the approved approach by baking governance policies into deployment workflows.

The result? Lower risk, less complexity, lower net costs, and accelerated productivity.

The ILM portfolio includes **HCP Terraform**, **HCP Packer**, and **HCP Waypoint**, as well as **HashiCorp Nomad**. These solutions use infrastructure as code workflows to offer a system of record for managed resources and the ability to manage the entire infrastructure lifecycle. Each of these products addresses a specific challenge, but together they form a comprehensive workflow for addressing infrastructure needs at all stages of application deployment.



- **HCP Terraform** for infrastructure as code provisioning: Uses a single workflow to provision multi-cloud, private datacenter, and SaaS infrastructure while continuously tracking and validating infrastructure throughout its lifecycle to prevent issues such as configuration drift. It provides a central internal registry to manage and distribute golden infrastructure modules at scale.
- **HCP Packer** for image building and management: Lets organizations use a single workflow to build cloud and private datacenter images and continuously manage the lifecycle of images in provisioning pipelines. It provides a central image registry to track, revoke, and distribute golden images at scale.
- **HCP Waypoint** for creating an internal developer platform: Enables platform teams to deliver golden patterns and workflows to manage complex deployment sequences at a high level in any environment — abstracting away the need for developers to deeply understand specific infrastructure and security practices.
- **HashiCorp Nomad** for multi-tenant compute orchestration: Brings modern application scheduling to any type of software. Manages containers, binaries, and virtual machines efficiently in the cloud, on-premises, and across edge environments.

The remainder of this white paper will examine the three stages of cloud maturity: adopting, standardizing, and scaling. Each stage has its own set of milestones that the HashiCorp ILM portfolio can help you reach, enabling your organization to establish a successful cloud program and realize its promised business value.

Stage 1 - Adopting

The adopting stage is the period when organizations gain familiarity with the cloud and provision their first resources. At this stage, the approach is still very ad hoc as teams across the organization take different approaches and use different tools. This variability of approach leads to inconsistent infrastructure security and performance across teams. The adopting stage highlights the need for a consistent, collaborative approach to cloud infrastructure composition.

Compose

Successful cloud provisioning starts with a systematic and repeatable approach to creating the infrastructure needed to support cloud applications. Many modern organizations **use infrastructure as code** to codify infrastructure and the underlying system images. Once codified, infrastructure can be easily versioned, reused, and provisioned across cloud environments. Most **use the HashiCorp Configuration Language (HCL)**, native to HashiCorp Terraform, as their preferred IaC language for its simplified, human-readable nature.

Organizations typically start their cloud journey with their infrastructure resources not defined as IaC. For this reason, we encourage them to **convert their existing infrastructure into code with resource importing**. Importing resources makes managing, rebuilding, and collaborating on infrastructure significantly faster and easier. As more teams adopt IaC, the organization as a whole can start to take advantage of Terraform's infrastructure management capabilities and standardize its provisioning practices.

When starting to provision resources spanning multiple environments and cloud providers (AWS, Google Cloud, Microsoft Azure, etc.), integrating new tooling with existing tools can be a massive challenge. HashiCorp can help simplify these efforts by letting you **use the provider plugin ecosystem to integrate thousands of existing technologies** with IaC provisioning. With over 4,000 providers, and growing, this ecosystem enables a smooth integration of the peripheral technologies you are already using, helping you get up to speed faster and realize value sooner. Critically, this agility is possible without sacrificing security. Terraform offers built-in dynamic credential management to **securely authenticate to providers across cloud environments**.

Collaborate

The other piece of a successful adopting stage focuses on enabling collaboration across individuals, teams, and whole organizations. Shifting to the cloud can seem daunting when organizations do so in isolation without help. But you don't have to write all your infrastructure code from scratch — Terraform has a vast community of experts that publish open-source **infrastructure configurations in the Terraform public registry**. This allows teams around the world with varying skill levels to harness the code written by experts to avoid reinventing well-established configurations. With more than 17,000 pre-written modules, and growing, the registry provides a trusted and comprehensive infrastructure foundation to get you started.

Leaders also need to make sure that internal teams are not operating in isolation, which can lead to inconsistent cloud infrastructure approaches and outcomes. Promoting consistency requires a common platform to access, review, and version infrastructure. Organizations can **integrate IaC workflows with a version control system (VCS)** like GitHub or GitLab to enable teams to work on a common code base. This helps encourage the reuse of best practices and patterns, boosting productivity and setting the foundation for infrastructure as a shared service across the entire organization.

As teams begin collaborating, to mitigate security risks, it is crucial to understand and define the specific access needed for different users. HCP's role-based access control (RBAC) functionality helps organizations effectively **manage teams and customize permissions**. This helps practice the principle of least privilege by ensuring that different users have access to only the resources and capabilities needed for their roles.

With resources consolidated under a single control pane, organizations can then focus on grouping their infrastructure logically to separate workloads. They can **organize resources with workspaces** and projects in HCP Terraform that provide isolation between infrastructure layers to help orchestrate complex deployments and reduce the potential impact of changes. These groupings provide teams with specific environments to work in and allow admins to grant permissions based on roles and organizational requirements. Similarly, HCP Packer helps **organize image artifacts with channels**.

Through the steps above, organizations can set a solid foundation for infrastructure composition and effective collaboration. With these cloud workflows successfully taking shape, organizations progress to Stage 2, which focuses on standardizing infrastructure consumption across the organization.

Stage 2 - Standardizing

Organizations entering the second stage, standardizing, have gained some familiarity with how to provision and use cloud resources. Individuals have begun to collaborate and share best practices, and teams may follow some processes when spinning up new infrastructure. However, they soon discover that without guardrails in place, security and compliance issues start to emerge and cloud spend balloons. This stage highlights the need to establish a shared, standardized approach to infrastructure provisioning and a means to effectively enforce it across the organization.

Publish and discover

Standardizing infrastructure provisioning starts with establishing consistent processes to create, test, and validate reusable modules of code and images, then making them easily discoverable so they can be consumed throughout the organization.

HCP Terraform lets users **test modules to ensure quality** before they are published. Tests allow authors to consistently validate the functionality of their configuration in a safe environment as they run against specific, short-lived resources. This prevents the risk of disrupting your existing infrastructure or state while helping ensure that your configurations will function as expected.

Once modules are tested and ready for use, you can then **publish standardized infrastructure modules in an internal private registry**. The private registry helps you share Terraform providers and Terraform modules across your organization. It includes support for versioning and provides a searchable list of modules available for reuse. Organizations can **gain further visibility into valuable infrastructure information with built-in explorer views**. These views provide insight into their entire infrastructure estate including workspaces, module and provider usage, Terraform versions, and health status.

With HCP Packer, you can also standardize golden images in a central artifact registry. Platform teams can define which images are approved for consumption to ensure that only the images with the latest security and organizational requirements are being used throughout the organization's provisioning pipelines.

Enforce policy

Rapid provisioning opens up tremendous possibilities, but organizations need to ensure they have effective policy guardrails in place to mitigate risk and unneeded cloud spend. Historically, these security, compliance, and cost policies required manual validation and enforcement, creating weeks-long bottlenecks in the deployment process.

Similar to infrastructure as code, policy as code can be used to reduce manual errors, enable scaling, and avoid bottlenecks. HCP Terraform helps users **write policy as code with HashiCorp Sentinel or Open Policy Agent (OPA)** to define custom policies that are automatically enforced in the provisioning workflow. For example, policies might validate that an end user is consuming approved modules rather than creating custom code, or a policy might ensure the infrastructure is tagged for visibility or that storage buckets are encrypted and not publicly accessible.

Terraform users can also **take inspiration from pre-written policy sets created by trusted experts** in the policy libraries section of the official Terraform Registry. This automatic policy integration into your provisioning workflows can be customized with different enforcement levels such as advisory, to warn users when a policy fails, soft mandatory for policies that can be overridden by an authorized user, and hard mandatory, which blocks the provisioning process until policy failures are resolved. Users can also **use run tasks to directly integrate third-party tools** into the steps of your Terraform provisioning process — **more than 20 partners** support additional workflows such as code scanning, cost control, and regulatory compliance.

Even with a standardized provisioning process and policy guardrails in place, infrastructure settings can still be undone or circumvented. This can open your infrastructure up to the possibility of configuration drift, or unexpected changes that violate the processes organizations have standardized on. To minimize outages, unnecessary costs, and emergent security holes, teams should have a system in place to monitor this drift. Organizations can try to build this into their processes, or they can use HCP Terraform to **manage resource drift with drift detection**. Drift detection notifies admins if your infrastructure has changed, enabling you to take the appropriate action to ensure stable security and reliability.

With a consistent approach to how infrastructure is consumed and embedded policies to meet security and compliance needs, organizations are ready to scale their cloud workflows across the entire organization.

Stage 3 - Scaling

As organizations mature to the third stage, scaling, the platform team focuses on extending its workflows and best practices across the entire digital estate, regardless of whether environments are on-premises or cloud-based. Platform teams will begin to offer the organization increasingly sophisticated capabilities, from health monitoring and lifecycle management capabilities to more turnkey levels of self-service provisioning. With the foundational cloud workflows established, organizations can shift focus to ensuring their standardized infrastructure approach remains persistent at scale and over time, and they can focus on further accelerating developer productivity.

Enable self-service

While HCL and premade Terraform modules simplify the use of IaC, not all users will be well-versed in the specifics of infrastructure configuration and Terraform usage. As organizations scale, they need a simplified, self-service model so developers with limited infrastructure knowledge can efficiently deploy the resources they need. For an even faster developer experience, organizations can **use no-code provisioning to make self-service even simpler**. No-code provisioning lets users deploy infrastructure in a push-button, self-service fashion without having to write Terraform configuration. Organizations can also **integrate with self-service platforms** that their developers are already familiar with such as ServiceNow and AWS Service Catalog, or CI/CD tooling like GitHub Actions.

Platform teams can also **set up an internal development platform (IDP) with HCP Waypoint** to expand their self-service capabilities. An IDP is a middle interface layer that sits between developers and platform teams to separate their differing concerns. The goal is to package and provide a set of golden patterns and workflows for developers so they can focus on the application lifecycle, while the platform teams own the pieces that underpin the infrastructure. With Waypoint, platform teams can define standard workflows for various actions such as building an application environment, deploying to production, and performing a rollback, which developers can execute from a simple user interface. Specifically how these applications are provisioned can be defined using standardized templates with Terraform modules.

Mature users can also modernize their application workflows by establishing a consistent approach to scheduling for any type of software. Users can **schedule and orchestrate applications with HashiCorp Nomad** to manage containers, binaries, and virtual machines

across cloud, edge, and on-premises environments from a single location. By efficiently scheduling work across large clusters, companies can scale applications to any size while minimizing overhead.

Observe and respond

Finally, ILM relies on a system of record to provide full visibility, enable consistent monitoring of environments, and remediate issues as they arise. Platform teams need to ensure that once their infrastructure is in a healthy state, it stays that way. Effectively monitoring your infrastructure on Day 2 and beyond is crucial to reducing the risk of costly outages by detecting failures or misconfigurations before they become a problem.

HCP Terraform helps organizations **continuously monitor infrastructure health over time** with health checks that verify whether custom conditions in workspace configurations continue to pass after provisioning. These checks give customers flexible options to validate their infrastructure uptime, health, and security — all in one place without requiring additional tools.

Organizations scaling their cloud program often see an accumulation of resources that are no longer relevant or in use, particularly in testing and development environments. These unused or forgotten resources may be outdated, contain security vulnerabilities, and drive up unneeded cloud spend. To prevent this, organizations can **automatically destroy infrastructure resources** in HCP Terraform. Once a predefined date or inactivity period is reached, Terraform will automatically apply a destroy plan on the workspace. Similarly, HCP Packer lets you **schedule revocation for artifacts** at the image level. When a golden image version has reached its end of life and is revoked, these deprecation workflows are streamlined with built-in automation such as inherited revocation and channel rollback.

When these infrastructure events occur, organizations can **use HCP notifications to inform users and external systems of important infrastructure events**. With notifications, relevant stakeholders can stay informed through their preferred communication platforms such as Slack, Microsoft Teams, and email. Notifications can also trigger webhooks to extend the workflow with custom automation. That could include initiating functional tests via HCP Terraform after publishing a new image version to HCP Packer, deleting the image or template in the cloud provider when the corresponding artifact version is deleted, and sending notifications to stakeholders when these events occur.

These monitoring and lifecycle management capabilities let organizations effectively scale their cloud program across the entire company while ensuring security and cost standards continue to be met over time.

Conclusion

While the cloud promises dramatic advances in how organizations innovate, respond to market trends, and connect with their customers and employees, it also requires a new cloud operating model to address significant changes in how infrastructure is built, deployed, and managed.

Infrastructure Lifecycle Management is a key to successful cloud adoption. Built on over a decade of industry-leading cloud infrastructure automation experience with many of the world's largest organizations, HashiCorp's ILM offerings meet you wherever you are on your cloud journey.

image or template in the cloud provider when the corresponding artifact version is deleted, and sending notifications to stakeholders when these events occur.

By taking advantage of these monitoring and lifecycle management capabilities, organizations can effectively scale their cloud program across the entire organization while ensuring security and cost standards continue to be met over time.

Resources

To help you get started, we've collected the associated documentation for each stage of cloud maturity:

Stage 1: Adopting

Compose: Organizations provision and manage cloud resources directly through infrastructure as code, increasing efficiency and eliminating manual errors.

- Use infrastructure as code (IaC)
- Use the HashiCorp Configuration Language (HCL)
- Convert existing infrastructure into code with resource importing
- Use the provider plugin ecosystem to integrate existing technologies
- Securely authenticate to providers across cloud environments

Collaborate: Multiple teams working on a common code base to encourage the reuse of common patterns, reducing the need for development teams to reinvent existing processes.

- Leverage common infrastructure configurations in the Terraform public registry
- Integrate your IaC workflows with a version control system (VCS)
- Manage teams and customize permissions
- Organize resources with workspaces
- Organize image artifacts with channels

Stage 2: Standardizing

Publish and discover: Organizations create, test, and validate standard images and reusable modules of code and publish them to internal libraries to ensure consistency and ease patches and updates.

- Test modules to ensure quality
- Standardize infrastructure modules in an internal private registry
- Standardize golden images in a central artifact registry
- Gain visibility into valuable infrastructure information with built-in explorer views

Enforce policy: Organizations use policy as code to enforce security and regulatory requirements before provisioning resources.

- Write policy as code with HashiCorp Sentinel or Open Policy Agent (OPA)
- Take inspiration from pre-written policy sets created by trusted experts
- Leverage run tasks to directly integrate third-party tools
- Manage resource drift with drift detection

Stage 3: Scaling

Enable self-service: Organizations create an internal developer platform (IDP) and provide development teams with preconfigured templates and workflows to automate the creation of their application environments.

- Use no code provisioning to make self-service even simpler
- Integrate with self-service platforms
- Set up an internal development platform (IDP) with HashiCorp Waypoint
- Schedule and orchestrate applications with Nomad

Observe and respond: Organizations have a system of record to consistently monitor the environment and automatically remediate issues as they arise.

- Continuously monitor infrastructure health over time
- Automatically destroy infrastructure resources
- Schedule revocation for artifacts
- Use HCP notifications to notify users and external systems of important infrastructure events

About HashiCorp

HashiCorp is The Infrastructure Cloud™ Company, helping organizations automate multi-cloud and hybrid environments with Infrastructure Lifecycle Management (ILM) and Security Lifecycle Management (SLM). HashiCorp offers The Infrastructure Cloud on the HashiCorp Cloud Platform (HCP) for managed cloud services, as well as self-hosted enterprise offerings and community source-available products. The company is headquartered in San Francisco, California.

For more information visit hashicorp.com