HashiCorp

The Infrastructure Cloud

Do cloud right with a unified platform for your entire digital estate

WHITE PAPER

Contents

Introduction

Over the last decade, most organizations have adopted 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. Organizations seem to struggle with the new way of doing things. Why does it seem like organizations often get the cloud wrong?

This white paper explores the challenges organizations face in realizing the full benefits of their cloud investments and lays out a blueprint for doing cloud right — an approach already used by thousands of cloud-mature organizations. That blueprint is enabled by The Infrastructure Cloud from HashiCorp, a unified platform to manage the lifecycle of your cloud infrastructure and security resources to help run your most critical applications.

According to **PwC's 2023 Cloud Business Survey**, *78% of companies have adopted cloud in most or all parts of their business, but only 10% consider themselves to be truly cloud-powered.*

Why it's hard to do cloud right

The cloud provides an environment where developers can create and deploy applications to cloud infrastructure instantaneously by discovering and using the tools and cloud services that best fit their applications. But focusing on application delivery alone causes many organizations to struggle with their cloud program due to lack of visibility and control over cloud infrastructure and security.

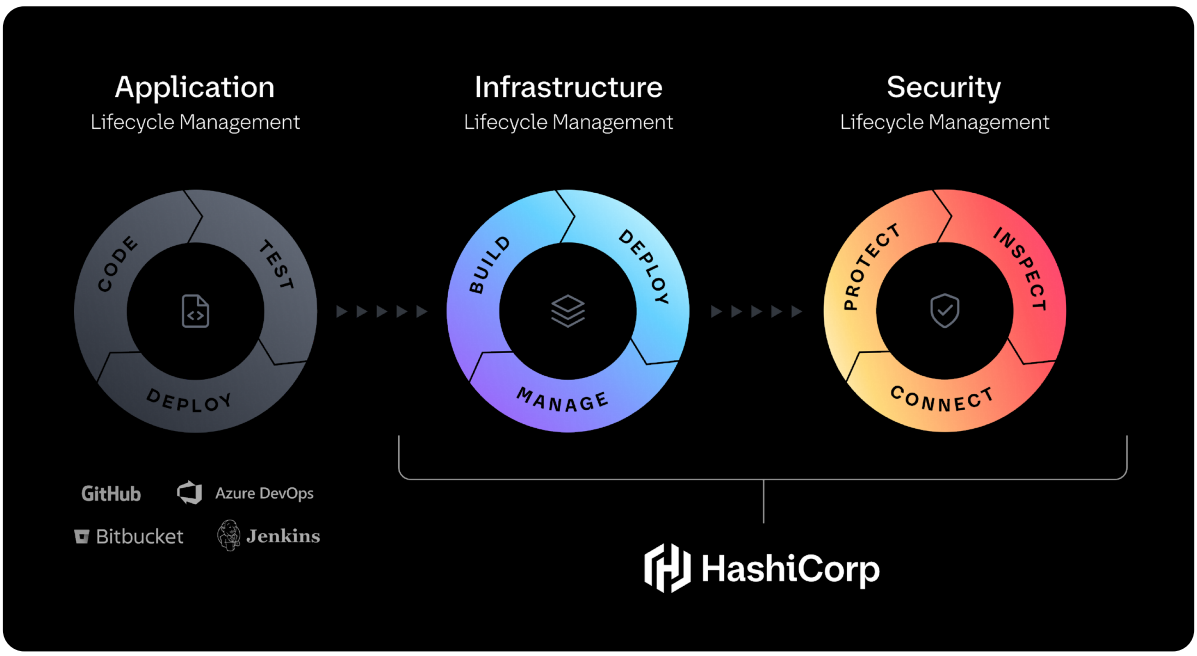
Building a cloud program that looks at the application value chain from end to end brings solutions for application delivery and infrastructure and security lifecycles that are based on systems of record, data that informs decisions, controls for governance, and processes for risk inspection.

Enterprises must embrace these processes for each part of the application value chain.

According to the 2023 HashiCorp State of Cloud Strategy Survey, 94% of organizations are wasting money in the cloud and estimate they overspend by up to 33%. When it comes to risk, IBM estimates the global average cost of a data breach at $4.5M, not including the cost to an organization's reputation.

Understanding the entire application value chain

The application value chain has three distinct segments, each requiring end-to-end lifecycle management:

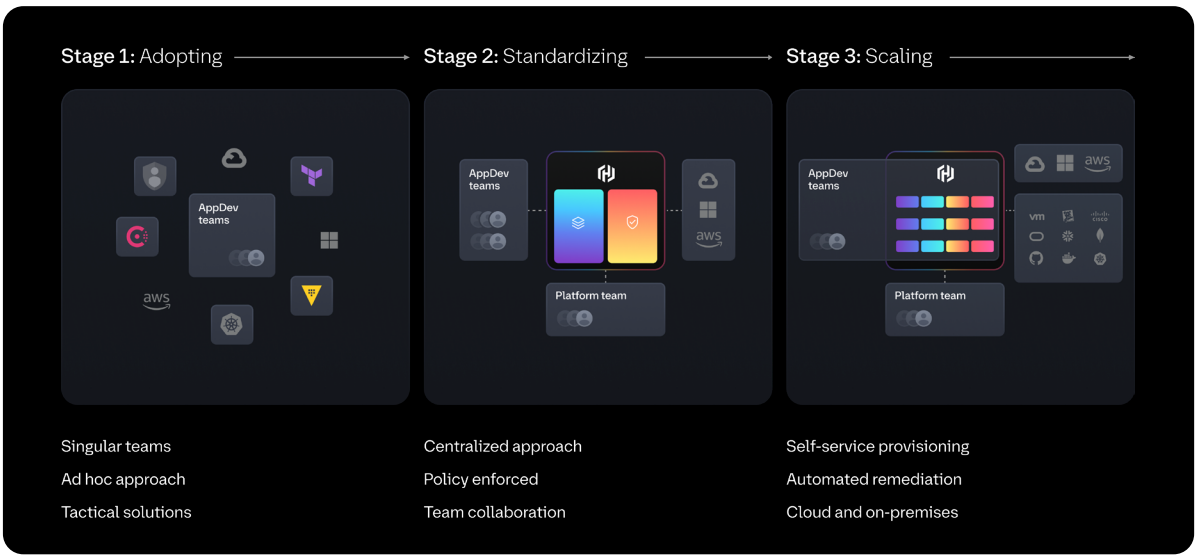


- **Application Lifecycle Management (ALM):** The most well-known part of the value chain addresses delivery of applications. Here, application developers have the workflows, systems, and capabilities to code, test, and deploy applications to cloud infrastructure.
- **Infrastructure Lifecycle Management (ILM):** This part of the value chain covers using infrastructure as code to build, deploy, and manage the infrastructure that underpins cloud applications. Here, the operations team has the tools in place to address cloud infrastructure from Day 1 to Day N, when it is eventually destroyed after it is no longer needed.
- **Security Lifecycle Management (SLM):** The third part of the value chain is about using identity-based access controls to manage the security lifecycle of secrets, user access, and services. Here, the operations and security teams have the functionality in place to inspect their security posture, protect sensitive elements, and securely connect machines, users, and services.

ALM is well-understood, and the arrival of infrastructure as code means the same general process can be applied to ILM and SLM, which are equally important to delivering a complete application value chain in the cloud.

Unless organizations address ILM and SLM, they face increased risks, higher costs, and failure to meet their business objectives.

A maturity-based blueprint for cloud success



Doing cloud right requires a holistic approach 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. That work has revealed a consistent three-stage blueprint for success:

- **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 applications and services as quickly as possible. However, this approach lacks a common platform, limits cross-team collaboration, and doesn't offer centralized enforcement of cost control or security/governance policies.
- **Stage 2 - Standardizing:** As cloud usage increases, organizations typically incorporate a programmatic approach to cloud consumption, focusing on gaining control of their cloud estate. A centralized platform team presents infrastructure and security as common shared services across the organization, which accelerates developer productivity by removing the manual tasks associated with deploying cloud resources or accessing secrets.
- **Stage 3 - Scaling:** As an organization's cloud journey matures, the platform team extends its workflows and best practices across the entire digital estate, including multiple cloud providers, SaaS applications, and on-premises datacenters. The team offers the organization increasingly sophisticated capabilities, from auto-remediation of configuration issues to true self-service provisioning.

This blueprint gives organizations a maturity model to benchmark where they stand in their cloud journey, and can suggest the next steps towards cloud maturity.

Infrastructure Lifecycle Management at each stage of cloud maturity

Well-architected Infrastructure Lifecycle Management is the foundation for successful cloud adoption. To work efficiently with multiple cloud providers, services, and third-party applications, a successful cloud program uses golden patterns — presented as infrastructure as code — across all teams. This abstracts complexities away from core development teams while ensuring they always use the approved approach, with governance policies already baked in. The result? Lower risk, less complexity, and accelerated productivity. Many organizations report this approach reduces time spent provisioning infrastructure by up to 90% and gets products to market up to five times faster.

Here's how Infrastructure Lifecycle Management looks at each stage of the cloud journey:

Stage 1: Adopting

- **Compose:** ILM lets organizations provision and manage cloud resources directly through declarative infrastructure as code for even the largest distributed applications. This increases efficiency and eliminates manual errors.
- **Collaborate:** Multiple teams work on a common code base to encourage reuse of common patterns and boost productivity. This reduces the need for development teams to reinvent existing processes.

Stage 2: Standardizing

- **Publish and discover:** At this stage, ILM enables organizations to create, test, and validate standard images and reusable modules of code. They can then publish these to internal libraries to ensure consistency and ease patches and updates.
- **Enforce policy:** ILM helps organizations convert policy into code that enforces it before provisioning resources. This incorporates FinOps best practices along with security guidelines and regulatory requirements.

Stage 3: Scaling

- **Enable self-service:** As organizations become more cloud mature, they can create an internal developer platform (IDP) and provide development teams with preconfigured templates and workflows to automate creation of their application environments.
- **Observe and respond:** Finally, ILM relies on a system of record to consistently monitor the environment and automatically remediate issues as they arise.

DHCS

Customer spotlight:
California Department of Health Care Services (DHCS)

Developed modernized cloud infrastructure to support hundreds of applications by replacing diverse legacy technology tools with a single automation platform from HashiCorp.

Automated the provisioning of resources and reduced the time and effort required to deploy and manage infrastructure by as much as 70%.

Security Lifecycle Management at each stage of cloud maturity

SLM helps strengthen security by automating global secrets rotation, enforcing the necessary policies for each environment, and enabling just-in-time authorization for machines, services, and

people. Centralization also simplifies aggregating the data and demonstrating the policies required for security audits.

Here's how SLM looks at each stage of the cloud journey:

Stage 1: Adopting

- **Manage all secrets:** SLM lets organizations discover secrets and unify their management across platforms. They can automate the regular rotation of secrets to reduce risk while minimizing manual effort.
- **Enforce policy:** At this stage, organizations can convert authorization policies into code and establish a least-privileged approach to who has access, what they are able to do, and when they can do it.

ManTech.

Customer spotlight:
ManTech

This provider of technology solutions to the federal government accelerated security setup and service delivery from several months to 2-3 weeks.

Reduced the number of human touchpoints and interventions across security workflows to lower the risk of security incidents or other reputation-harming occurrences

Stage 2: Standardizing

- **Ensure continuity:** An SLM approach lets organizations actively manage sensitive data and avoid outages caused by expired credentials.
- **Automate and observe:** Organizations can leverage just-in-time dynamic credentials for privileged access. They can also record privileged sessions to troubleshoot issues and continuously scan for new unmanaged secrets.

Stage 3: Scaling

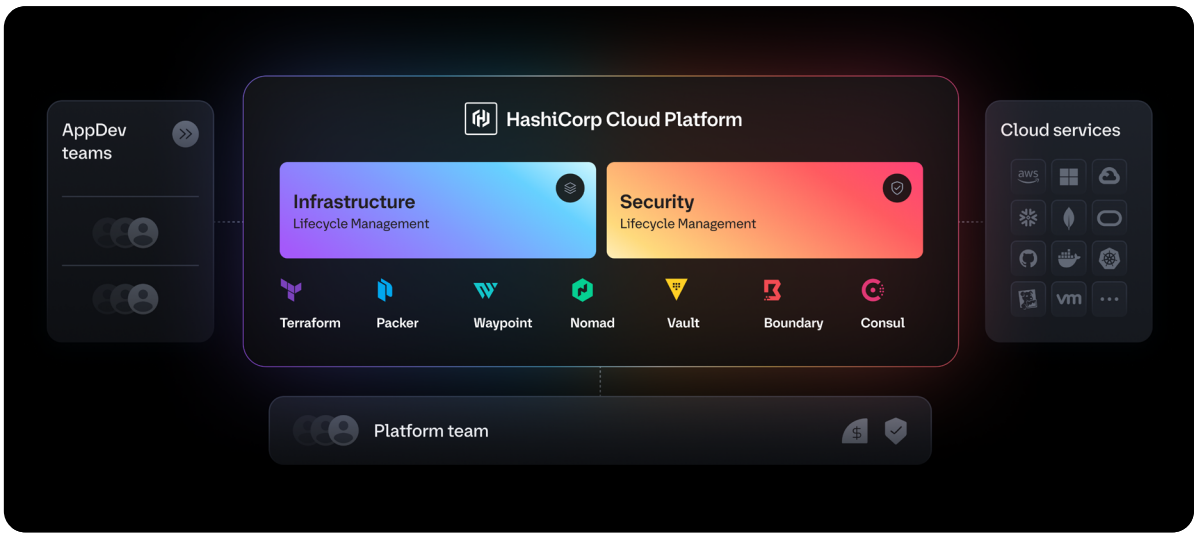
- **Remediate:** At this stage, organizations further minimize risk by automatically rotating and revoking credentials as needed.
- **Encrypt seamlessly:** SLM also brings a unified approach to encryption policy and technology, both at rest and in transit, which bolsters security with minimal manual overhead.

Meet The Infrastructure Cloud

The Infrastructure Cloud is best realized using HashiCorp Cloud Platform (HCP), which provides a programmatic approach to the lifecycle management of cloud infrastructure and security.

Drive value using the HashiCorp Cloud Platform

HCP is a unified SaaS platform that provides solutions for Infrastructure Lifecycle Management and Security Lifecycle Management, speeding time to value while lowering operational overhead and optimizing costs.



Key HCP benefits include:

- **Streamlined onboarding and management:** Get started in minutes and avoid lengthy provisioning and configuration workflows. Eliminate the cost and overhead of actively managing underlying infrastructure.
- **Well-integrated multi-product workflows:** Begin with simple use cases in infrastructure provisioning or secrets management, and naturally extend to more complex use cases such as image management within infrastructure provisioning workflows or privileged access management.
- **No infrastructure costs for ILM and SLM solutions:** Services run and managed by HashiCorp let organizations offload the cost of the infrastructure needed to run a platform of central services.

- **Latest upgrades automatically applied:** HCP customers always have access to the latest features and functionality without requiring system-wide upgrades that can disrupt team workflows.
- **Scalability:** HCP systems are designed to scale with customer needs and deliver performance to match changing business requirements.
- **High availability and disaster recovery:** With multiple clusters supporting each service, HCP assures availability and prompt recovery of data.
- **Geographic distribution:** Located in both North America and in Europe, our datacenters are positioned to give organizations the geographic coverage they require.
- **Common central services:** With HCP's shared platform, all products use a single, common identity for each user and provide a single interface for billing.

Infrastructure Lifecycle Management products

HashiCorp has been solving infrastructure problems for more than a decade, starting with cloud infrastructure provisioning and expanding into solutions for image management and multi-tenant compute orchestration. Our ILM solutions use infrastructure as code workflows and offer a system of record for managed resources as well as the ability to manage the entire infrastructure lifecycle. HCP products for ILM include Terraform, Packer, Waypoint, and Nomad:

- **HCP Terraform for infrastructure as code provisioning:** Uses a single workflow to let organizations provision their cloud, private datacenter, and SaaS infrastructure and continuously manage infrastructure throughout its lifecycle.
- **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.
- **HCP Waypoint for creating an internal developer platform:** Enables platform teams to deliver golden patterns and workflows to manage applications at scale in any environment — abstracting away the need for developers to deeply understand specific infrastructure and security practices. Currently in beta, HCP Waypoint is scheduled to be generally available in 2024.
- **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.

Security Lifecycle Management products

HashiCorp has been solving security challenges since 2015, starting with secrets management and expanding to include solutions for certificate and key management, data protection and encryption, privileged access management, and service networking. Our SLM solutions use identity-based security workflows and offer a system of record for sensitive information (credentials, certificates, keys, customer data) as well as the ability to manage the entire lifecycle of sensitive information. HCP products for SLM include Vault, Boundary, and Consul:

- **HCP Vault for secrets management:** Provides an identity-based approach to security that automatically authenticates and authorizes access to secrets and other sensitive data.
- **HCP Boundary for remote user access:** Built for the cloud, Boundary's modern approach to privileged access management uses identity-driven controls to secure user access across dynamic environments.
- **HCP Consul for service networking:** Offers an identity-based approach to service networking for service discovery, secure communication, and network automation across multiple cloud and runtime environments.

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 relating to significant changes in how applications are deployed, secured, and managed.

The Infrastructure Cloud from HashiCorp is a key to successful cloud adoption. It's built on more than a decade of industry-leading cloud infrastructure automation experience and counts many of the world's largest organizations as customers. HashiCorp's offerings meet you wherever you stand on your cloud journey.

The Infrastructure Cloud, delivered via the HashiCorp Cloud Platform, can solve your ILM and SLM challenges and maximize the value of your cloud investment now and in the future, while responsibly managing costs and mitigating risks. It's what you need to enable your platform teams and your cloud program to do cloud right.

www.hashicorp.com/infrastructurecloud

About HashiCorp

HashiCorp is The Infrastructure Cloud™ company, helping organizations automate multi-cloud and hybrid environments with Infrastructure Lifecycle Management and Security Lifecycle Management. 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