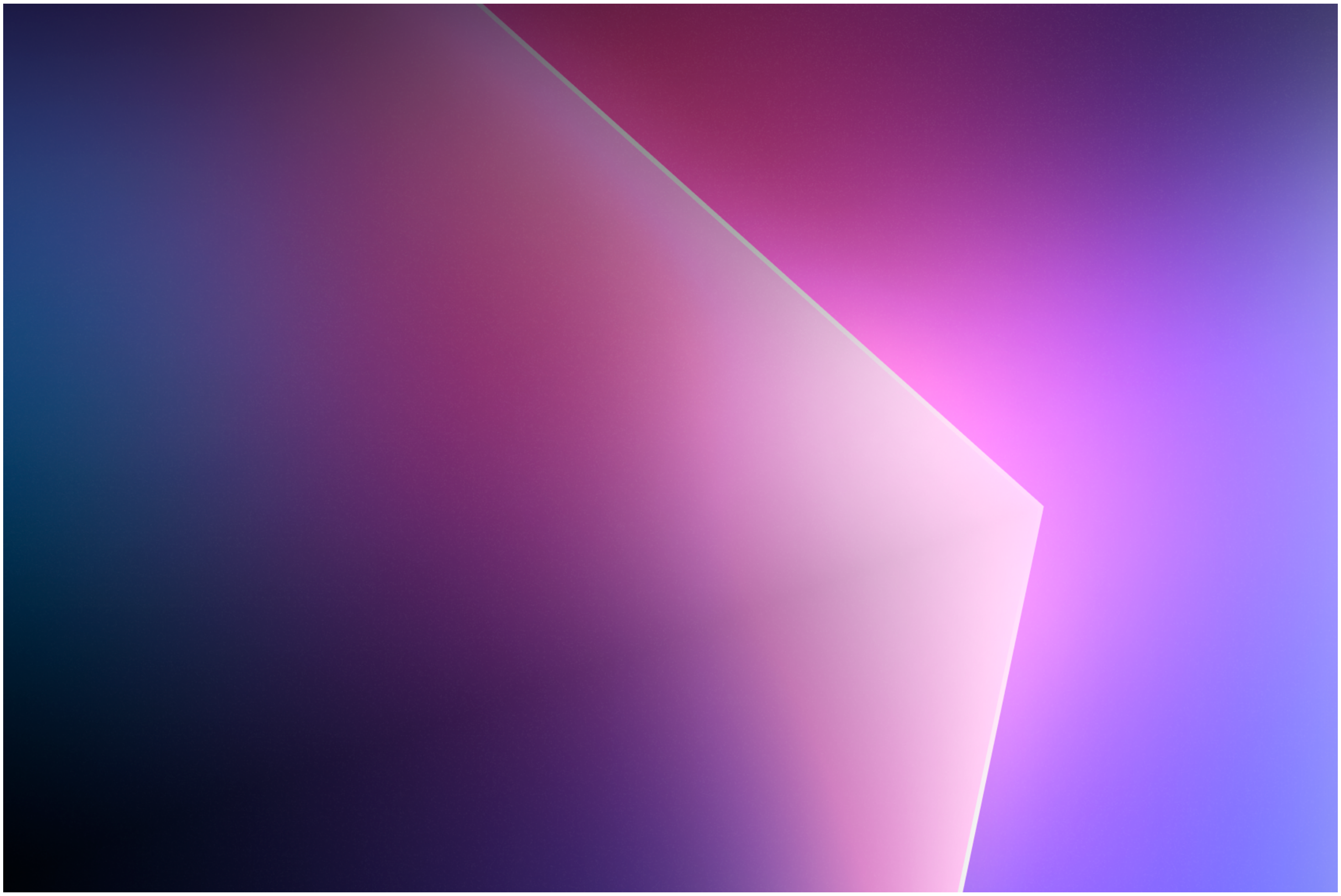


Empowering platform teams

How to do cloud right with The Infrastructure Cloud

HashiCorp
an IBM Company

Contents

Executive summary

Platform teams today are being asked to fix the cloud — without breaking it. As cloud adoption becomes nearly universal, measurable success remains elusive. Organizations continue to struggle with operational complexity, cost control, and security risk.

To overcome these challenges, streamlining cloud operations through standardized workflows and automation is essential. Equally critical is the emergence of platform teams as a strategic function to unify and scale these efforts across the organization.

This white paper introduces a best-practice framework for platform teams grounded in two core principles: streamlined workflows and a unified platform. It outlines how IBM's Infrastructure Cloud, delivered via the HashiCorp Cloud Platform (HCP), supports Infrastructure Lifecycle Management (ILM) and Security Lifecycle Management (SLM) to help organizations accelerate innovation, strengthen security, and optimize operations.

Finally, it explores the persistent challenges in adopting a centralized platform model — and the chaos that can result from a lack of clarity around how to build, operate, and scale platform teams effectively.

A platform team is a centralized group responsible for building and maintaining the internal developer platform—enabling standardization, automation, and governance across infrastructure and security workflows.

A new cloud operating model for organizations

In the early days of cloud adoption, speed was everything. Teams raced to deploy applications, often bypassing structure in favor of experimentation. The result? A fragmented landscape of tools, inconsistent processes, and mounting technical debt. Security misconfigurations became common. Costs spiraled. And platform teams — if they existed at all — were left to untangle the mess.

One enterprise we spoke with described their environment as "a cloud of clouds" — each team had its own tooling, its own way of provisioning infrastructure, and its own interpretation of security policy. Developers were agile, but operations were overwhelmed. Tickets piled up. Visibility was low. And ROI? Elusive.

Fast forward to today, and the picture is beginning to shift. Platform teams are emerging as the connective tissue across cloud operations. By standardizing workflows and consolidating tooling, they're enabling self-service without sacrificing control. They're reducing toil, improving security posture, and aligning infrastructure with business outcomes.

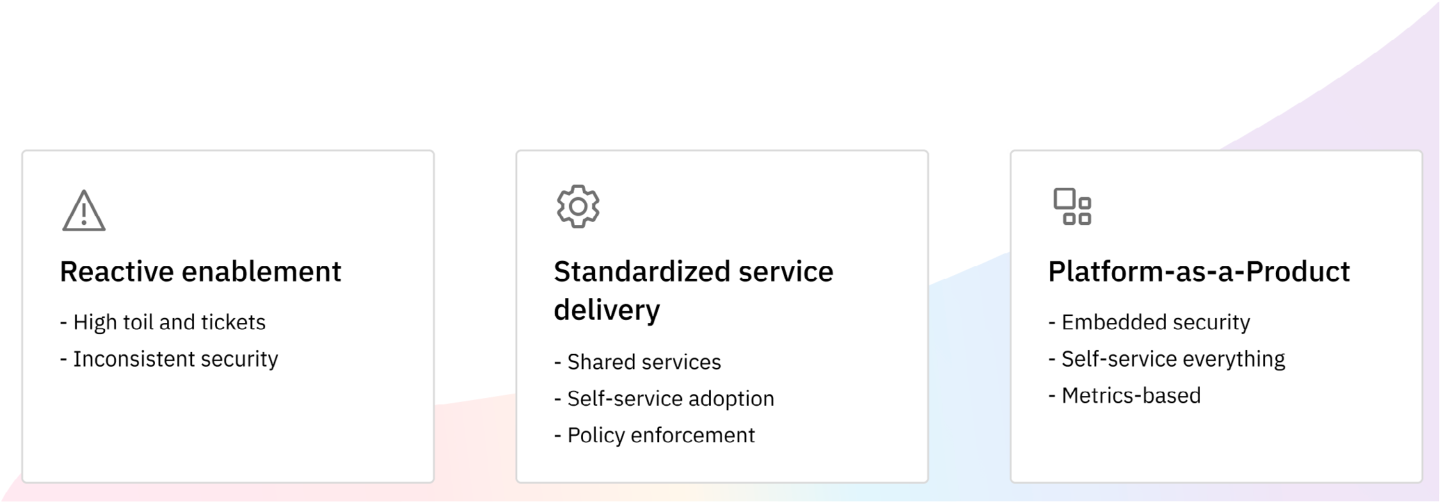
Still, the gap between adoption and value remains. According to PwC's 2024 Cloud and AI Business Survey:

78% of enterprises have adopted cloud services

12% of the 78% of enterprises that adopted cloud services reported full ROI

75% of those organizations reported rising inefficiencies and misconfigurations remain as the leading cause of security breaches

To close this gap, organizations need a new operating model — one grounded in standardization, automation, and lifecycle management. Platform teams are key to this transformation, but only if they're empowered with the right tools, clarity of ownership, and a unified approach to managing infrastructure and security at scale.



Reactive enablement

- High toil and tickets
- Inconsistent security

Standardized service delivery

- Shared services
- Self-service adoption
- Policy enforcement

Platform-as-a-Product

- Embedded security
- Self-service everything
- Metrics-based

Unlocking ROI through platform engineering: A persona perspective

Meet Jane, a lead platform engineer at a global enterprise.

When she joined, every team had their own way of doing things — different tools, different pipelines, different definitions of 'secure.' Developers wanted speed. Security wanted control. And they were stuck in the middle, trying to make it all work.

Platform engineering isn't just a trend — it's a product-driven response to the chaos left behind by early cloud adoption. As Jane and the others on her team can attest, they are not just building tools anymore. They're building products that their developers depend on every day.

With developers demanding faster, self-service access to infrastructure and security teams pushing for consistency and control, platform engineers like Jane are now the connective tissue. They're tasked with delivering sustainable velocity, governance, and cost control across sprawling hybrid and multi-cloud environments.

80% of large software organizations will implement platform teams by 2026, according to Gartner.[1]

This signals a major evolution: from ad hoc tooling and shadow IT to intentional platforms that treat infrastructure and security as curated, scalable, and reusable products. But it's not easy.

Platform engineers feel they are often building in the dark, as there's no universal blueprint. They are constantly balancing short-term developer needs with long-term architecture and security goals.

At their best, platform teams operate like internal product teams. They aren't just building tools — they're shipping products — delivering standardized infrastructure, reusable services, and consistent workflows that accelerate delivery and embed security by default. But this requires more than just technical skills. It demands a product mindset, organizational support, and a commitment to shared outcomes.

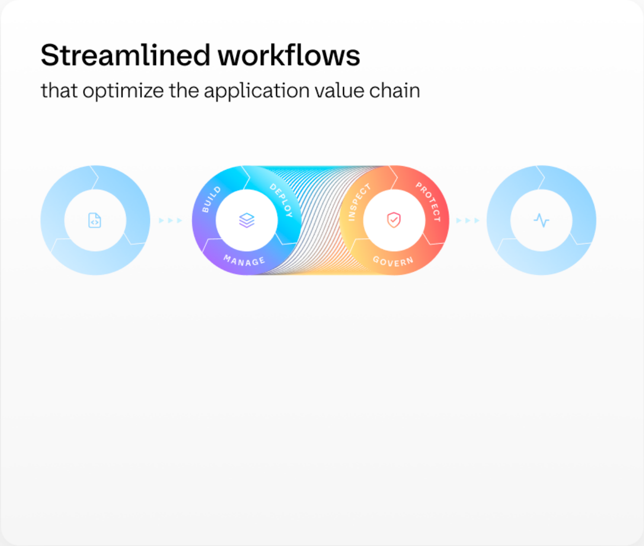
Engineers like Jane and others would agree that done right, platform engineering can bridge silos, reduce toil, and lay the foundation for scalable cloud success.

[1] Gartner®. https://www.gartner.com/en/infrastructure-and-it-operations-leaders/topics/platform-engineering

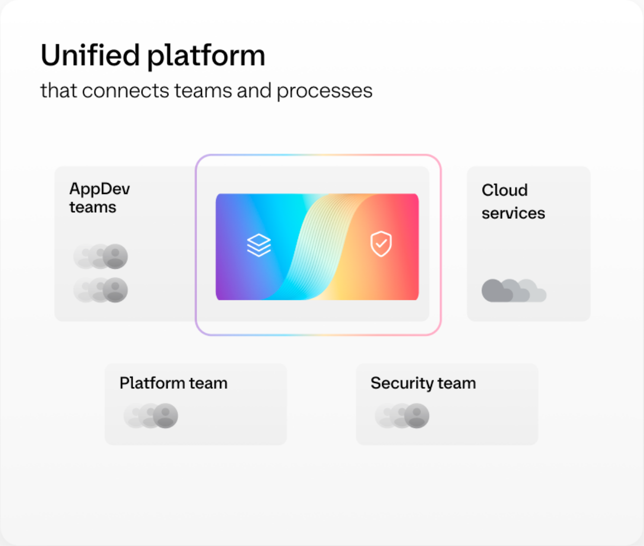
A unified approach to the application value chain

This evolution in platform team responsibility demands more than just tactical fixes–it calls for a broader, integrated strategy. To mature beyond initial cloud challenges, teams must shift from fragmented, reactive patterns to managing the full application value chain holistically. That means going beyond application lifecycles to also own and streamline the infrastructure and security lifecycles that support them. This requires:

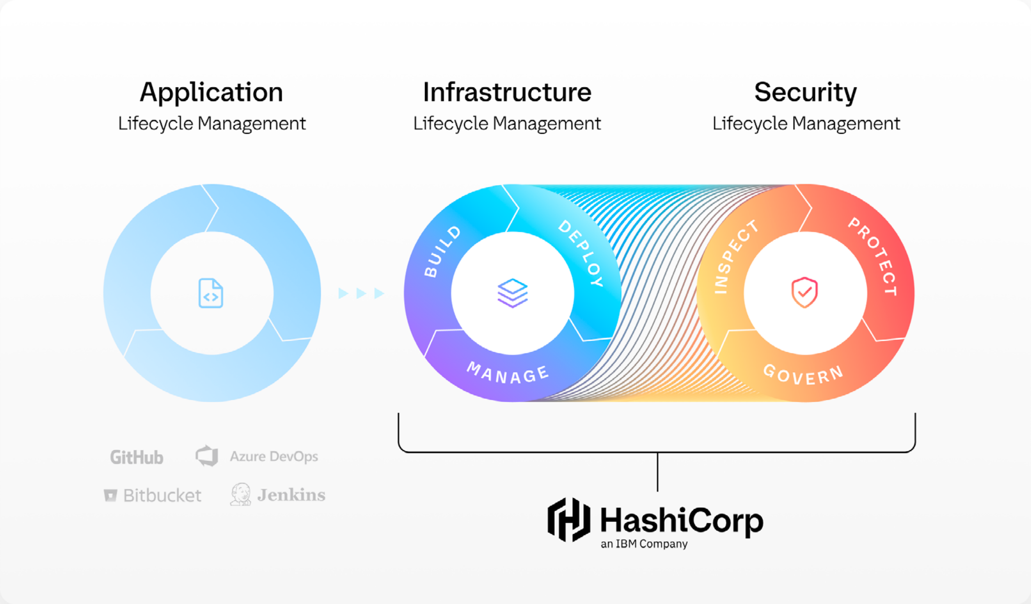
- **Streamlined workflow:** Automating provisioning, governance, access, and security across teams.



Streamlined workflows
that optimize the application value chain



Unified platform
that connects teams and processes



- **A unified platform:** Centralizing visibility and control across hybrid and multi-cloud environments.

Together, ILM and SLM form the backbone of HashiCorp's Infrastructure Cloud, our unique approach to enabling platform teams to manage infrastructure and security lifecycles as one cohesive system. Delivered through the HashiCorp Cloud Platform (HCP), this unified platform gives platform teams the automation, policy enforcement, and self-service capabilities they need to move from reactive management to proactive leadership. It's how HashiCorp helps platform teams do cloud right by standardizing the application value chain and equipping them to deliver speed, security, and scalability at enterprise scale.

Benefits of consolidation:

- **Single system of record:** Central repository for infrastructure and security workflows
- **Automated policy enforcement:** Preemptive governance at scale
- **Developer self-service:** Empowerment with controls

But a platform is only as effective as the team that operates it. That's why the role of the platform team has become both more strategic and more transformative.

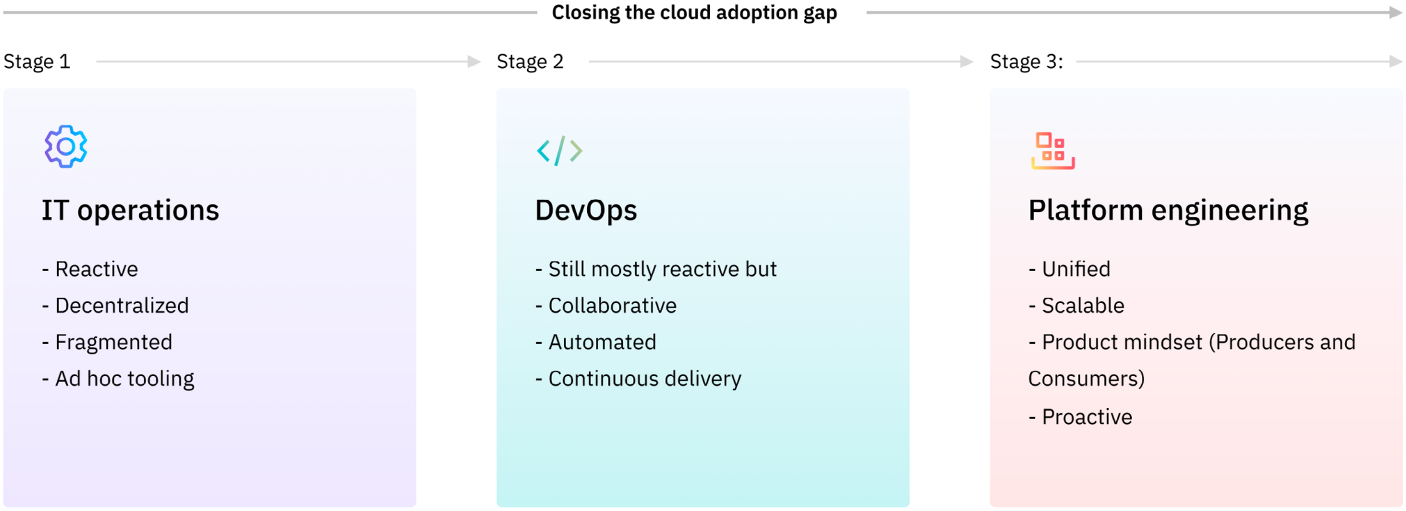
Platform management: From reactive ops to platform-as-a-product

As we will see further in this chapter, in order to achieve success with the application value chain, it is important for organizations to consider the entire lifecycle of the platform and that starts with the transition from a reactive operations team to a platform as a product team. So before we dive further into this transition, here are -

5 traits of a platform-as-a-product mindset

1. User-centered design: Every decision starts with understanding developer needs, pain points, and workflows.
2. Clear product ownership: Success metrics, roadmaps, and priorities are owned and managed like any external-facing product.
3. Consistent feedback loops: Regular input from users drives iteration and informs platform evolution.
4. Reliability as a feature: Uptime, security, and performance are part of the user experience, not just backend concerns.
5. Adoption-driven success metrics: Usage, satisfaction, and enablement are how impact is measured, not just shipped features.

Evolutionary path to platform team empowerment



Closing the cloud adoption gap

Stage 1

IT operations

- Reactive
- Decentralized
- Fragmented
- Ad hoc tooling

Stage 2

DevOps

- Still mostly reactive but
- Collaborative
- Automated
- Continuous delivery

Stage 3:

Platform engineering

- Unified
- Scalable
- Product mindset (Producers and Consumers)
- Proactive

“If no one’s using it, it doesn’t matter how powerful it is.”

And when it comes to the transition itself, as described in the previous sections, organizations need to evolve from a reactive and siloed approach to a more proactive, standardized and unified mode to help them be successful with cloud adoption and thrive in an era of hybrid and multi-cloud architectures.

Among other things, it also emphasizes the use of a shared service model to organize and deliver technology services, resources, or capabilities to different parts of an organization. This approach allows different teams or business units within the organization to leverage the same set of services, reducing redundancy and promoting consistency.

There are two roles in this model - Producers and Consumers

Producers ensure that the shared services are readily accessible and efficiently utilized by the Consumers, empowering them to leverage the benefits of the platform effectively. This is usually the platform team.

Consumers play a crucial role in leveraging the shared services to meet their specific needs and requirements while adhering to the guidelines and standards set by the producers. Consumers refer to any team within the organization that uses the shared services provided by the platform team (producers). This is usually the application development (AppDev) team, but could also extend to SecOps and other operations teams.

The unified control plane for platform teams

A centralized platform team is responsible for delivering core infrastructure and services as standardized, shared resources that can be easily consumed by users across the organization.

Beyond providing these standardized resources, the platform team also:

Defines and implements best practices:
- They establish and disseminate best practices for how users interact with the organization’s infrastructure and services.
- These best practices are then integrated into automated workflows and training programs, ensuring consistent and efficient usage.

Facilitates cross-functional integration:
- They act as a central point of collaboration for other organizational teams, such as security, compliance, and finance.
- This ensures that critical requirements and policies from these departments are incorporated into relevant workflows and infrastructure designs.

Provides centralized monitoring and reporting:
- They offer a unified system for tracking, reporting, and auditing the usage of infrastructure and services.
- This system provides valuable insights into adoption patterns, performance, and potential risks, enabling informed decision making and proactive risk management.

In essence, the platform team streamlines access to essential resources, promotes consistent practices, and ensures alignment with organizational policies, for all its consumers–ultimately enhancing efficiency and reducing risk for the organization.

Platform-managed service workflow example

Managing network connectivity with a unified control plane
Organizations require robust solutions to manage secure network connectivity between services across diverse environments, including on-premises and multi-cloud deployments. These solutions often encompass service discovery, service mesh functionality, traffic management, and automated network infrastructure updates.

Implementing these capabilities within a cohesive framework typically involves collaboration among various teams, each with distinct responsibilities. The following is a list of coordination efforts that might be necessary:

Platform setup and maintenance

- Establish core networking infrastructure for the platform.
- Implement access controls with defined policies and roles.
- Set up monitoring systems for both the platform and connected services.
- Manage underlying infrastructure and perform platform administration.
- Leverage platform APIs to automate tasks and streamline workflows.

Service registration and utilization

- Register application services to enable discovery and connectivity.
- Design and implement health checks to ensure service availability and reliability.

Patterns and best practices

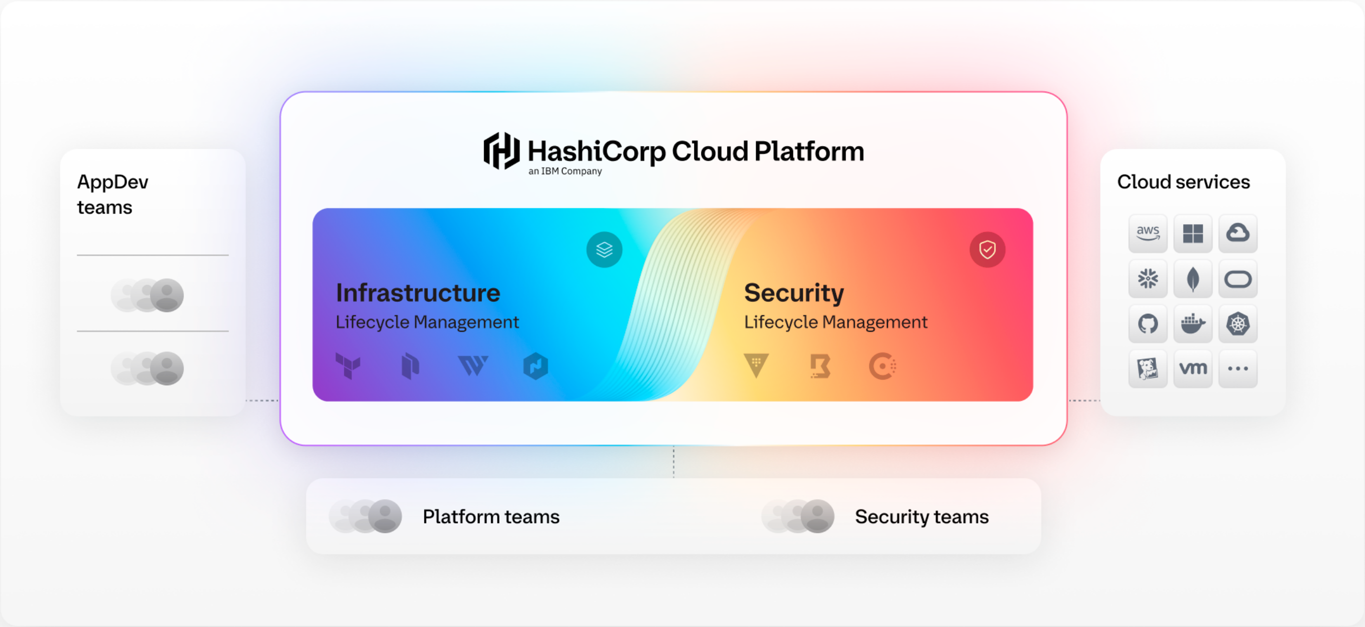
Let’s explore some of the common patterns of platform management and the best practices that organizations can and should implement to be successful in their hybrid cloud journey.

A pattern for a platform engineering team
Platform management, as shown in the diagram below, is a strategy that combines infrastructure and security management into a unified platform with a common control plane. This platform, operated by a **dedicated platform team, delivers essential services to DevSecOps teams to deploy cloud services.**

Key elements of this approach include:

- **Integration of ILM and SLM**: It provides a common control plane to unify infrastructure and security management, breaking down silos.
- **Infrastructure as code (IaC)**: As a leading strategy for a common control plane, it starts with IaC principles for provisioning and image management, enabling standardization, automation and consistency.
- **Automated services**: It provides automated developer services, scheduling, and orchestration to improve efficiency.
- **Security-centric approach**: It prioritizes security through identity-based secrets management, secure remote access, and service-based networking for enhanced connectivity and management.

In essence, platform management aims to streamline cloud operations and enhance security through automation and a unified platform, empowering development and operations teams.



Best practices for platform management

For a successful implementation, platform teams must follow these best practices:

Foundational practices

- **Understand your customers** - Know your developers' needs and build a pragmatic service catalog around them.
- **Define and measure reliability early** - Set expectations around reliability based on user outcomes to build trust.
- **Build in security and compliance** - Integrate these from the start using automation and reference architectures.
- **Create a formal platform team structure** - Define roles like platform team lead and cloud engineers with clear responsibilities.

Operational excellence

- **Use a maturity model to guide investments** - Understand where you are in the cloud journey and plan accordingly.
- **Continuously reduce toil and increase automation** - Automate everything possible and unify operations through a control plane.
- **Optimize costs with showbacks and chargebacks** - Use tagging and reporting to drive cost transparency and reduce waste.
- **Evaluate platform success** - Track metrics like stability, usage, developer satisfaction, and business impact.
- **Align goals to business outcomes** - Regularly engage with leadership to ensure platform priorities support the organization's strategy.

Adoption and enablement

- **Provide a delightful developer experience** - Offer self-service, sensible defaults, and prescriptive guidance.
- **Enable self-led education** - Build a portal with documentation and learning resources.
- **Build internal communities through advocacy** - Promote platform usage via town halls, feedback loops, and community events.

Following the best practices in this white paper can help you move away from a reactive workflow to a more proactive workflow. Below, let's look at an example of the typical interactions across an organization. They may be generally similar in motion, but a key distinction is where they start, i.e. whether it is proactive or reactive.

Platform pro tip

Don't skip the "marketing" part.

Even the best platform will struggle with adoption if developers don't know it exists or how to use it. Treat internal advocacy like product marketing—clear messaging, regular updates, and feedback loops are key.

Reactive workflow

SecOps monitors threats
SecOps identifies a threat vector and reports it to Security.

Security creates policy
Policies are created in response. If using IaC, enforcement is continuous; otherwise, policies are manually handed off.

Dev teams implement policy
Policies are encoded and launched into developer portals or infrastructure tooling.

AppDev teams deliver apps
Teams incorporate new policies as one-offs, while still managing compliance and security concerns.

Additional interactions
Workflows may extend to secret management, auditing, secure access, etc., often as isolated tasks.

Proactive workflow (Best practices-based)

Architecture establishes patterns
Architecture defines forward-thinking patterns for efficient software delivery.

Security creates policy
Security reviews and applies policies to recommended architectural patterns.

Platform engineering implements policy
Policies are encoded and integrated into the IDP or infrastructure tooling.

AppDev teams deliver apps
Teams focus on delivering business value, with security embedded in the platform.

Platform teams evolve best practices
Continuously refine patterns to address new threats and drive innovation.

Proactive platform engineering workflow example

HashiCorp empowers your platform teams to provide agile application delivery mechanisms and automates across your entire hybrid estate, so you can get to market faster and more efficiently than your competitors.

The image at the end of this page explains how HashiCorp's cloud platform can help unify DevSecOps and Platform teams with automated security and workflow governance, and can help the teams work at a high velocity to deliver applications rapidly. To see some of the key elements of these, let's look at another story of AcmeCorp and how they transformed.

AcmeCorp is growing fast, but their application delivery pipeline is slowing them down. Developers are waiting on infrastructure. Security is chasing secrets in code. Ops is buried in tickets. Everyone's frustrated.

Then, they make a shift.

They empower their platform team with HashiCorp's Infrastructure Cloud. Suddenly, things start to change.

After the shift: How AcmeCorp transformed:

Infrastructure provisioning is automated
- Developers no longer wait days for environments.
- With IaC and automation, infrastructure is provisioned in minutes—securely and consistently.

Standardized registries across environments
- Teams reuse modules and templates across clouds, reducing duplication and increasing reliability.

Guardrails are built-in
- Every deployment is wrapped in automated policies—no more manual reviews or risky shortcuts.
- Teams extend compliance with the platform's built-in audit logging capabilities.

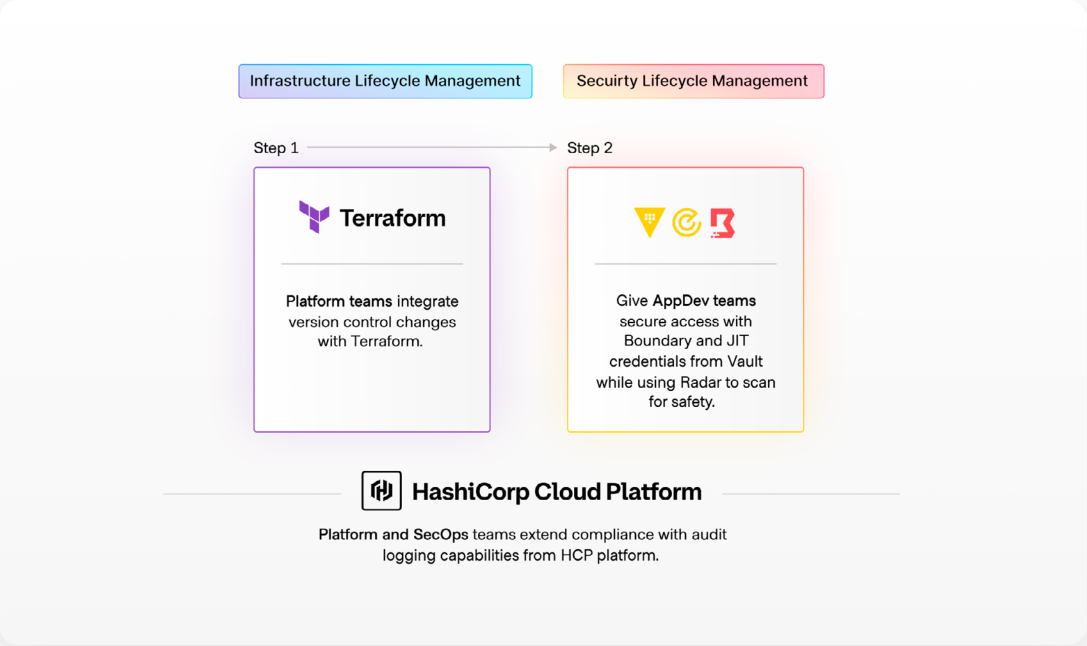
Developers get one-click access to everything
- From secrets to services, everything is accessible through a unified, self-service portal with automated workflows.

CI/CD pipelines are fully integrated
- Secrets are scanned and rotated automatically. If a key leaks, the system catches it before it hits production.

Platform pro tip

Don't just automate—productize.

Treat your internal platform like a product. Market it. Support it. Evolve it. That's how you drive adoption and deliver real business value.


Infrastructure Lifecycle Management
Secuirty Lifecycle Management
Step 1
Step 2
Terraform
Platform teams integrate version control changes with Terraform.
Give AppDev teams secure access with Boundary and JIT credentials from Vault while using Radar to scan for safety.
HashiCorp Cloud Platform
Platform and SecOps teams extend compliance with audit logging capabilities from HCP platform.

Platform management with HashiCorp Cloud Platform (HCP)

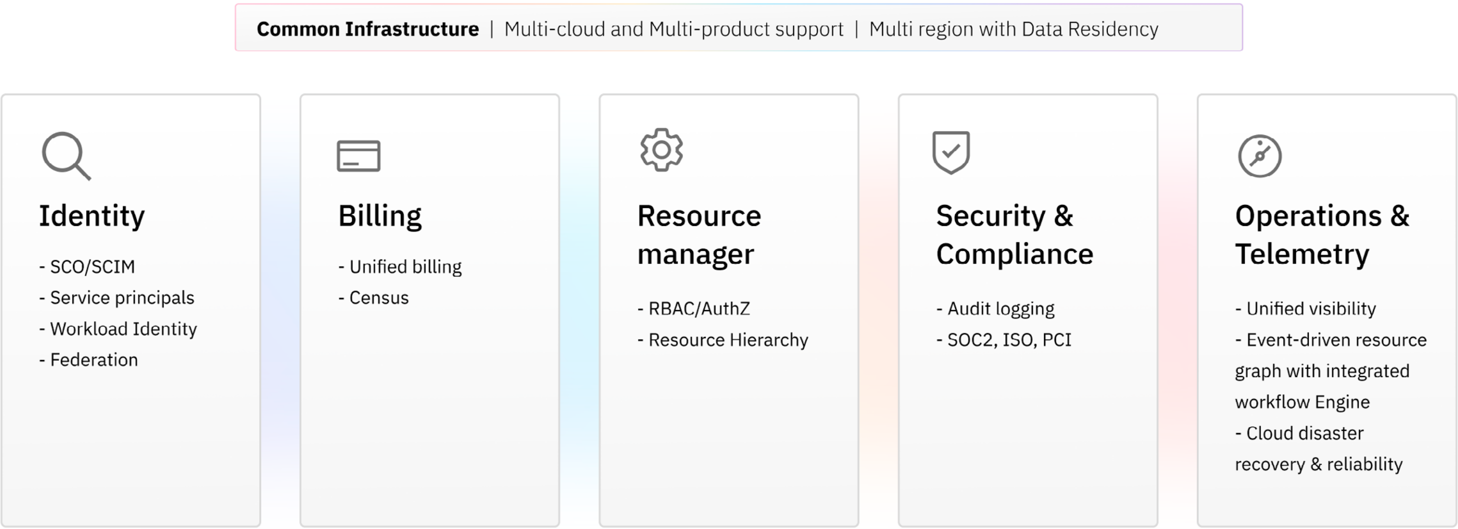
HashiCorp offers a comprehensive unified platform and a common control plane for ILM and SLM, facilitating consistent workflows across diverse runtime environments. This standardized and automated approach provides a central system of record for cloud operations.

The Infrastructure Cloud unifies infrastructure and security management across hybrid, multi-cloud, and on-premises environments. By providing a single system of record, it centralizes workflows, governance, and automation, aligning teams through a shared platform. Organizations can access the Infrastructure Cloud through HashiCorp's on-premises commercial software and as a SaaS solution via HCP.

Key characteristics: Platform management through a common control plane

Although these are the key characteristics of a unified platform, this should be treated as a readiness checklist that every platform team should aim to support, from a feature and functionality standpoint, on their platform.

Platform management simplified



Common Infrastructure | Multi-cloud and Multi-product support | Multi region with Data Residency

Identity

- SCO/SCIM
- Service principals
- Workload Identity
- Federation

Billing

- Unified billing
- Census

Resource manager

- RBAC/AuthZ
- Resource Hierarchy

Security & Compliance

- Audit logging
- SOC2, ISO, PCI

Operations & Telemetry

- Unified visibility
- Event-driven resource graph with integrated workflow Engine
- Cloud disaster recovery & reliability

A list of those characteristics is as follows:

Standardization of operations and telemetry:
Implement standardized operational procedures and telemetry data collection across all cloud resources to ensure consistency and facilitate effective monitoring and management.

Unified visibility through event-driven resource graph with integrated workflow engine:
Establish a centralized and dynamic view of all cloud resources utilizing an event-driven resource graph, complemented by an integrated workflow engine to streamline operational tasks and provide comprehensive insights.

Robust cloud disaster recovery and reliability:
Ensure business continuity and minimize downtime through the implementation of comprehensive cloud disaster recovery strategies and the establishment of highly reliable infrastructure.

Comprehensive identity management (RBAC/AuthZ, Resource Hierarchy):
Implement a robust identity management system encompassing Role-Based Access Control (RBAC), authorization mechanisms (AuthZ), and a well-defined resource hierarchy to enforce security policies and control access to cloud resources.

Comprehensive audit logging:
Maintain a detailed and comprehensive audit log of all activities and changes within the cloud environment to support security investigations, compliance requirements, and operational transparency.

Adherence to industry compliance standards (PCI, SOC2, ISO, etc.):
Ensure adherence to relevant industry compliance standards, including but not limited to PCI DSS, SOC 2, and ISO 27001, to meet regulatory obligations and maintain customer trust.

Unified billing for all platform services:
Implement a unified billing system, leveraging census data and other appropriate mechanisms, to provide a consolidated and transparent view of costs for all services utilized on the platform.

Efficient resource management through SCO/SCIM:
Employ System for Cross-domain Identity Management (SCIM) and potentially other Service Catalog Operations (SCO) to facilitate efficient provisioning, de-provisioning, and management of resources and identities across the cloud environment.

Leveraging service principals for secure automation:
Utilize service principals to enable secure and automated interactions between applications and services, minimizing the need for human intervention and enhancing security.

Implementation of workload identity federation:
Implement workload identity federation to provide a secure and scalable approach for applications running in the cloud to access other cloud resources without the need for long-lived credentials.

Common infrastructure support across multi-cloud and multi-product environments:
Establish a common underlying infrastructure that provides consistent support for diverse cloud platforms and a wide range of products and services, promoting interoperability and reducing complexity.

Multi-region deployment with defined data residency:
Implement a multi-region deployment strategy with clearly defined data residency policies to meet regulatory requirements, improve application performance, and enhance resilience.

HCP provides a common control plane

Finally, as a summary to bring all the previous details together, here are some salient points on the value proposition in terms of an organization’s business needs and pain points for doing cloud right:

Accelerated delivery and innovation
Platform teams enable rapid, high-velocity application delivery through automation, developer self-service, and seamless hybrid/multi-cloud workflows—boosting productivity and accelerating innovation across the organization.

To explore how platform engineering drives developer velocity, refer to our white paper on delivering innovation at scale.

Strengthened security and governance
A unified platform approach enhances security and compliance through centralized risk management, automated policy enforcement, and identity-based controls—enabling proactive threat mitigation and zero trust practices across all environments.

To learn how unified workflows strengthen cloud security, refer to our paper The next generation of cloud security.

Optimized cloud operations and ROI
Platform engineering streamlines cloud operations through automation, proactive cost management, and standardized development practices—boosting resilience, enhancing visibility, and maximizing ROI across the organization.

To learn how platform teams improve cloud efficiency and cost control, refer to our paper on optimizing cloud operations.

Cloud success starts with the right team

Cloud success doesn't come from having more tools—it comes from having the right strategy.

Platform teams sit at the center of this strategy. By unifying infrastructure and security lifecycles, standardizing workflows, and enabling self-service with guardrails, they shift the organization from reactive to resilient.

> "The best platforms don't just deliver tools - they deliver trust."

With IBM's Infrastructure Cloud, platform teams have a proven blueprint and the tools to deliver it—empowering speed, reducing risk, and driving cost-efficiency at scale.

Start your platform transformation today

Building a high-performing platform team doesn't happen overnight. But every great transformation starts with a few focused steps. Here's where to start:

Your blueprint to do cloud right:

Adopt a product mindset

- Adopt a product mindset to drive greater value, user satisfaction, and long-term platform success.

Refer back to this white paper for a deeper dive into how this mindset shift can transform your platform strategy.

Evaluate and identify gaps

- Evaluate your team's maturity and identify critical gaps in your infrastructure and security workflows.

Engage your HashiCorp sales and support teams to further discuss how to assess your current state and uncover opportunities for improvement.

Optimize and streamline

- Optimize team performance and accelerate business outcomes by aligning roles and streamlining scalable, automated workflows.

Engage your HashiCorp sales and support teams to further discuss how to structure your team and unify your workflows for maximum impact.

20%

increase in operational efficiency

HARVARD BUSINESS REVIEW

View study

15%

reduction in security incidents

FORRESTER

View study

407%

ROI over three years, with a payback period of under seven months

IDC

View study

Produced in the
United States of America
August 2025

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.