

# Accelerate seamless hybrid cloud automation

Enable scalable hybrid cloud automation

**Establish a unified automation foundation for hybrid delivery built for scale, control, and speed.**

52%

of organizations say hybrid/multi-cloud complexity is a top priority<sup>1</sup>

78%

of enterprises feel infrastructure isn't prepared for AI-driven workloads<sup>2</sup>

62%

of companies lost time to market due to fragmented cloud tools and missing automation<sup>3</sup>

Large enterprises operating across hybrid and multi-cloud environments struggle to deliver at speed because automation is fragmented across provisioning, security, configuration, and connectivity, creating drift, manual handoffs, and slow release cycles that compound as containerized and AI workloads scale.

The only scalable path forward is a unified, policy-driven automation foundation that standardizes how hybrid cloud environments are built, secured, and operated end to end.

## Streamline workflows across environments

Eliminate fragmented delivery with reusable, policy-driven workflows built to scale across hybrid and multi-cloud.

- **Repeatable provisioning at scale:** Terraform provides shared workflows and policy guardrails, so teams can provision and govern infrastructure consistently across environments, eliminating rework and enabling faster self-service delivery.
- **Consistent, compliant hybrid environments:** Terraform, Packer, and Ansible align reusable modules, golden images, and repeatable configuration patterns to reduce drift and rework.
- **Secure-by-default delivery workflows:** Vault, Vault Radar, and Boundary automate secrets management, secure access, and exposure scanning across hybrid cloud, eliminating risky static credentials and slow approval bottlenecks so teams can ship faster with less risk.
- **End-to-end infrastructure and application lifecycle automation:** Ansible and OpenShift extend automation beyond provisioning into configuration and runtime operations, while Consul ensures services remain securely connected as they scale.

## Accelerate delivery of AI-ready, cloud native applications

Unlock faster innovation by using a unified automation foundation across infrastructure, security, configuration, and connectivity, so AI workloads move from pilot to production without operational bottlenecks.

- **Fully automated hybrid execution:** Terraform and Ansible automate delivery, Vault embeds secure access, OpenShift standardizes runtime, and Consul connects services, enabling one repeatable hybrid workflow.
- **Policy-driven automation for AI workloads:** By using Terraform, Vault, Ansible, and OpenShift to enforce guardrails, apply trusted configuration, and issue dynamically rotated secrets across provisioning and runtime, teams ship AI workloads faster with security built-in.
- **Faster AI iteration with repeatable release paths:** Terraform, Ansible, and OpenShift enable consistent AI environments and repeatable rollout workflows, reducing rebuilds and accelerating model and service updates across hybrid cloud.

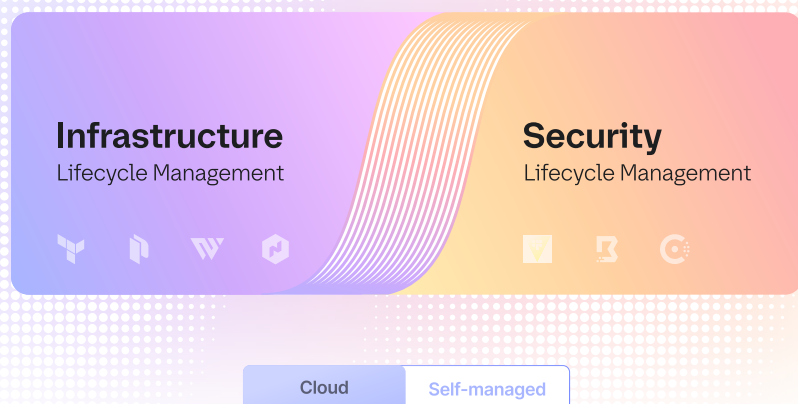
1. HashiCorp 2025 Cloud Complexity Report.  
2. Economist Impact report, Databricks.  
3. Predictions 2024: Cloud Computing, Forrester, October 30, 2023.

## Hybrid cloud done right

Together, HashiCorp and Red Hat solutions provide the automation foundation enterprises need to replace fragmented delivery with consistent, scalable operations. By aligning provisioning, configuration, security, and connectivity, teams move faster, reduce risk, and deliver AI-ready applications with built-in governance.

This foundation doesn't just accelerate delivery — it prepares organizations to operationalize AI confidently as hybrid environments become more complex.

### HashiCorp Cloud Platform



**Replace fragmented processes with one repeatable way to deliver, secure, and connect workloads across your hybrid cloud — at the speed AI demands.**

To learn more, contact your account representative or visit [www.hashicorp.com/en/infrastructure-cloud](https://www.hashicorp.com/en/infrastructure-cloud) to get started today.

### Deutsche Bank

**“You are able to write the Terraform IaC to create cloud resources, as well as contribute to the policy and standards that are published to our trusted private module registry. That’s a paradigm shift.”**

## 3000

developers enabled to consume cloud resources autonomously

[View study](#)



**“Using automation and Terraform heavily for onboarding our customers in various parts of their journey helped us accelerate software delivery.”**

## 20%

of dev team efforts saved

[View study](#)

### FIVERTY

**“Developers don’t have to wait for a central team to provision the infrastructure for them, which previously took hours or sometimes days. Now, teams use pre-configured modules and the magic happens.”**

## 80%

faster pull request approvals

[View study](#)

© Copyright IBM Corporation 2026

IBM, the IBM logo, HashiCorp, and Terraform are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/trademark](https://ibm.com/trademark).

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.

It is the user's responsibility to verify the operation of any non-IBM products or programs with IBM products and programs. IBM is not responsible for non-IBM products and programs.

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.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

