

Unifying Cloud Operations with HashiCorp

Beata Haber
Account Manager
HashiCorp (IBM)

Miguel Hernandez
Solutions Engineer
HashiCorp (IBM)

The explosion of cloud-native applications and the complexity of large, on-prem legacy systems have created formidable challenges

Innovation:

Businesses are challenged to minimize time to market and productionize AI



34% of CIOs report AI in production

Deployment:

Businesses are forced to cobble together solutions using a multitude of tools



30+ tools from up to 10 vendors

Management:

Businesses struggle to extract value from investments in technology



75% of enterprises fail to generate consistent ROI

Financial:

Businesses fail to manage spend using manual methods and waste budgets



35% average waste on cloud spend¹

Security:

Businesses face loss of reputation and escalating cost because of data breaches



\$4.88M average cost of data breach²

1Q2025:

IBM completes acquisition of HashiCorp

IBM completed the acquisition of HashiCorp, which includes its suite of products that provide enterprises with **extensive infrastructure lifecycle management and security capabilities** to enable organizations to automate their hybrid and multi-cloud environments.

"Combining IBM's portfolio and expertise with HashiCorp's capabilities and talent will create a **comprehensive hybrid cloud platform designed for the AI era.**"

Arvind Krishna, Chief Executive Officer, IBM
[Read the press release](#)



IBM TO BUY HASHICORP
ACQUISITION DETAILS

- IBM to pay \$35/share, implying value of \$6.4B
- A step forward in IBM's cloud computing ambitions
- IBM expects transaction to close by end of 2024

MONEY MOVERS **IBM CEO ON HASHICORP ACQUISITION**

CNBC

[Watch the video →](#)

HashiCorp is the
leading multi-cloud
infrastructure
automation
company

4500+

customers

918

≥\$100K ARR customers

\$583M

total revenue

2200

global employees

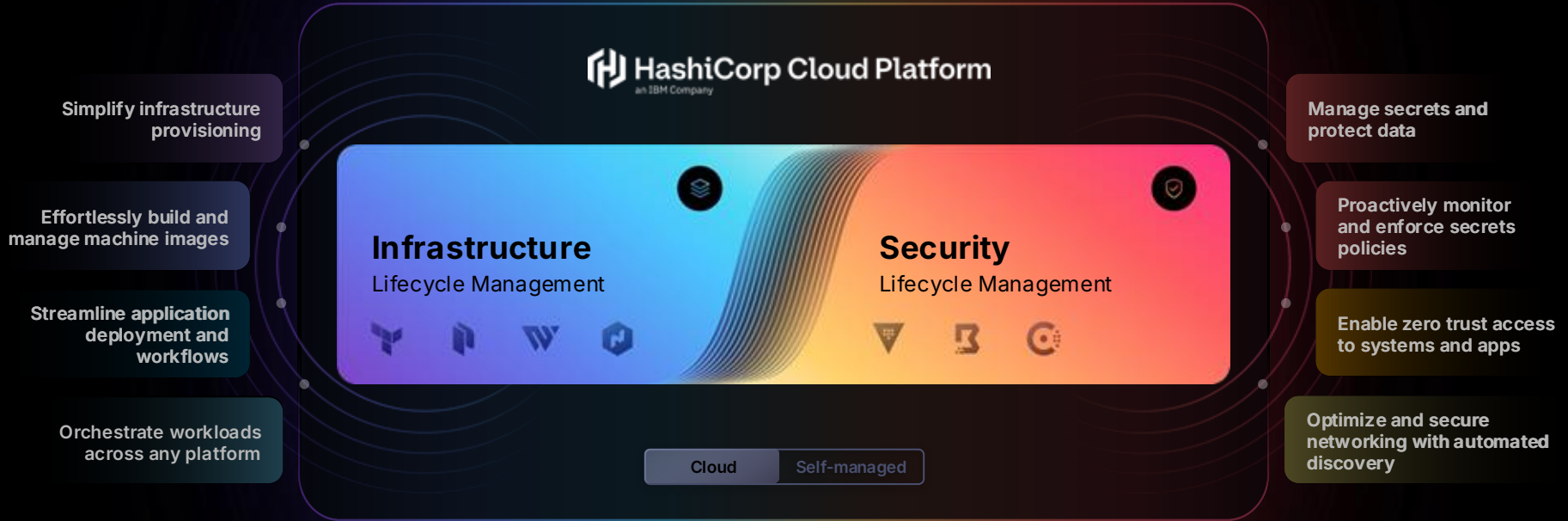
900+

ecosystem partners

450M

product downloads

Delivering a portfolio of hybrid solutions





Empowering every industry to do security right

Financial Services

KeyBank



SoftBank

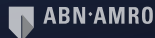
CREDICORP



Blackstone



wepay
a CHASE company



NORD/LB

S&P Global

Entertainment & TelCo

COMCAST



NBCUniversal



sky

pandora

RED|VENTURES



Manufacturing & Logistics



Lufthansa

AIRBUS

AirPlus
INTERNATIONAL

KPMG

WARE2GO

Software & Technology

Booking.com

Grab

priceline®

cielo



Shipt

SEAT
GEEK

Q2



Insurance & Health

PROGRESSIVE



GSK

AstraZeneca



ellume

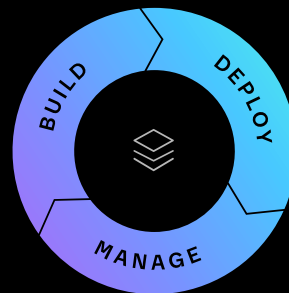
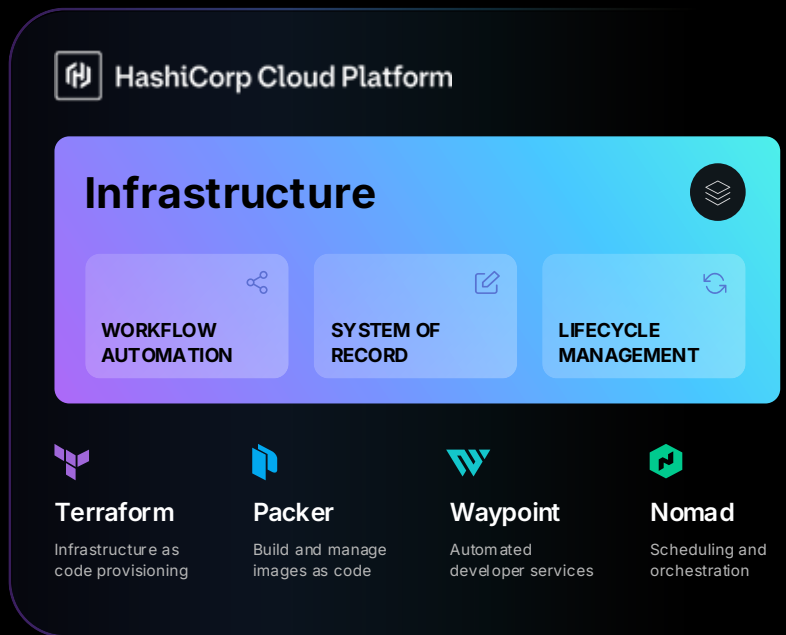
athenahealth

GoodRx

surescripts

Infrastructure Lifecycle Management

Maximize your infrastructure investments



Infrastructure as code to build, deploy and manage the lifecycle of infrastructure and applications.

1

INFRASTRUCTURE LIFECYCLE MANAGEMENT

Terraform

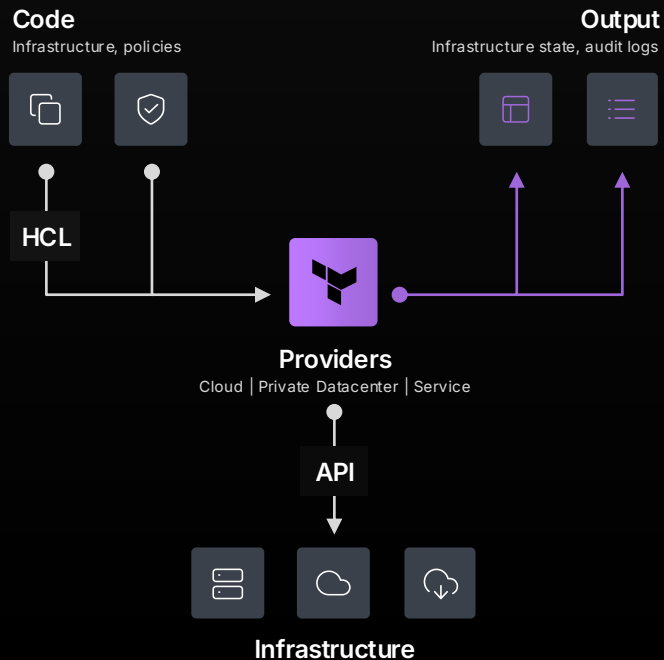
Standardize your infrastructure automation

Secure and optimize your infrastructure workflows to maximize your investments

Infrastructure as Code to define the desired configuration of resources

Infrastructure system of record for the state of resources across cloud providers

Lifecycle management for provisioning and policy automation and continuously optimize cloud resources



Empower your team with enterprise capabilities

Automation & optimization



RBAC
Remote State Storage
Registry
No Code Workflow
Roll-back/forward

Visibility & policy



Sentinel, OPA
Run Tasks
Workspace Mgmt
Drift Detection
Continuous Validation
Alerts
Audit Logs

Reliability & scale



Managed HA
Self-Managed HA
Self-Hosted Agents

Integrations & API



Okta
Splunk
HCP Packer
ServiceNow
Waypoint
...

Governance, risk, & compliance



SOC Compliance
24x7 Support

BETTER TOGETHER

Why HCP Packer



HCP Packer

Publish image metadata

Promote versions via channels

View ancestry and history

Revoke and roll back



HCP Terraform

Discover image artifacts
(Data source)

Provision infrastructure

Validate image status (Run tasks, drift
detection, continuous validation)

2

INFRASTRUCTURE LIFECYCLE MANAGEMENT

Packer





Use IaC to create and manage images in any environment from a central location.

Speed

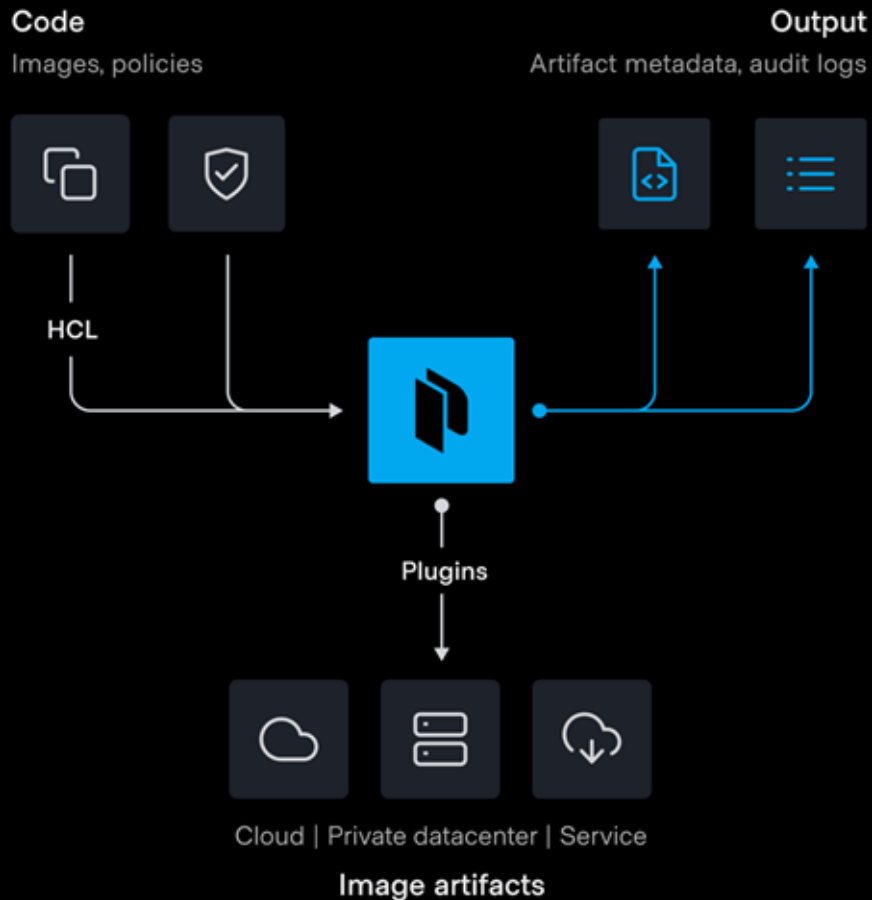
Standardize image creation and consumption to increase developer productivity.

Risk

Secure your images before deployment and continuously monitor health over time.

Cost

Retire long-lived unneeded images driving up cloud spend.



Empower your team with enterprise capabilities

Unified Workflow Management



HCL
Artifact Registry
Builder Plugins

Visibility & Optimization



Codify Security and Compliance
Standardize Versions
Image Revocation
Image Validation
Audit Logs

Reliability & scale



Golden Image Promotion
Image Ancestry
Inherited Revocation
Channel Assignment History

Integrations & API



Terraform
Okta
Plug-in Ecosystem
API Extensibility
Webhooks

Governance, risk, & compliance



SOC Compliance
24x7 Support

3

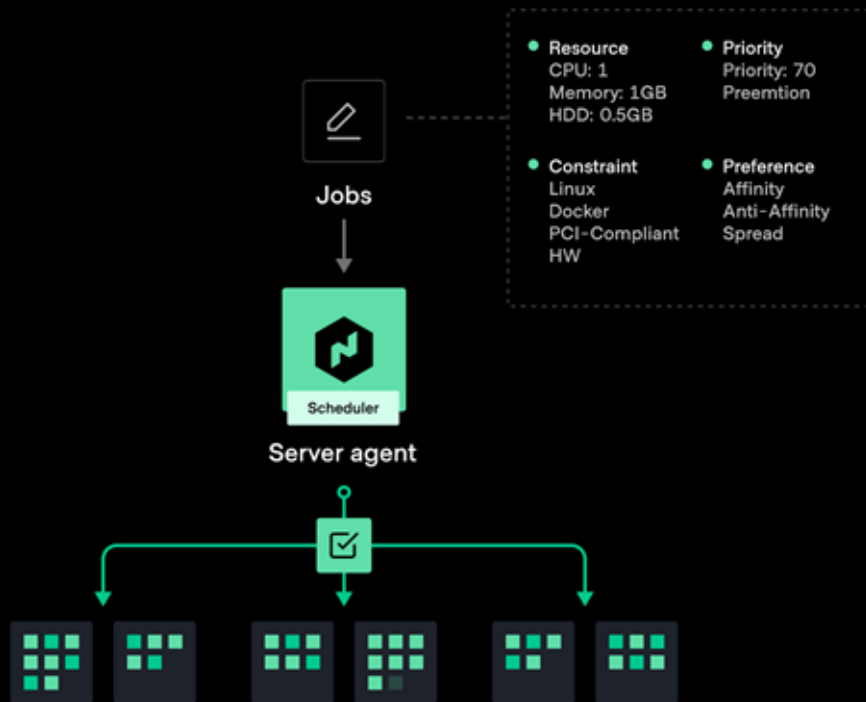
INFRASTRUCTURE LIFECYCLE MANAGEMENT

Nomad



How Nomad works

- A Nomad server forms the control plane for scheduling
- A Nomad client runs on the node and registers with the servers, watching for any work to be assigned and executing tasks
- A Nomad job runs on the client node and defines what applications to run, how many, and where





The standard for compute orchestration to **schedule**,
deploy, and **manage** workloads across any infrastructure

Deployment as Code

Application

Container

Binaries

VM

Java JARs

...

Cloud

AWS

Azure

GCP

...

Hashicorp

Terraform

Vault

Consul

Waypoint

...



Enabling platform team capabilities

Unified Workflow Management



Containerized, Non-Containerized

Deployment

Nomad Pack Templating

Service/Batch Scheduling

Namespace Resource Quotas

Visibility & Optimization



Web UI

Resource Monitoring

Event Stream

Audit Logging

Reliability & scale



Autoscaling

Dynamic Application Sizing

Advanced Scheduling

Edge Computing

Job Failure Handling

Federation for Multi-Region Deployments

Automatic updates

Enhanced Read Scalability

Integrations & API



Device Plugins & GPU Support

Container Storage Interface Plugins

Consul and Vault Feature Integrations

Service Discovery

Governance, risk, & compliance



Redundancy Zones

24x7 Support

Automated Backups

Security Lifecycle Management

Reduce risk with Security Lifecycle Management

 HashiCorp Cloud Platform
an IBM Company

Security Lifecycle Management



Vault

Machine identity
management

• Vault Radar

Secret discovery
and remediation



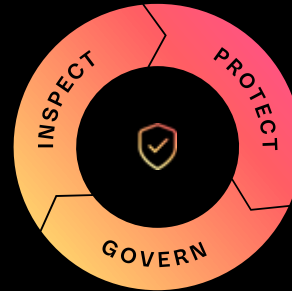
Boundary

Secure remote
access



Consul

Service-based
networking



Identity-based
secure access to
machines, people,
and services

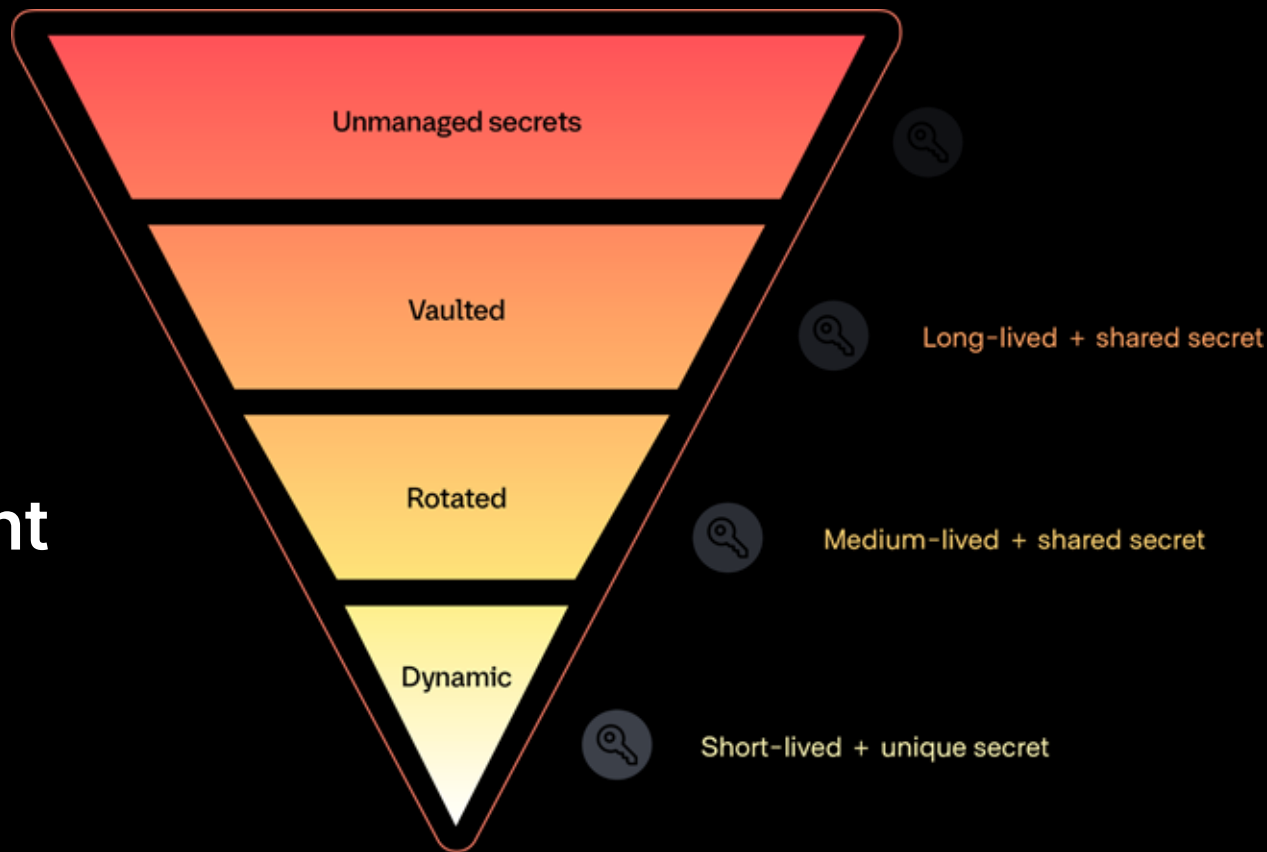
1

SECURITY LIFECYCLE MANAGEMENT

Vault

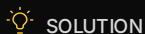


Security Lifecycle Management



Secure application identities & protect sensitive data

Secure based on least-privileged access



SOLUTION

Grant the minimum level of identity-based access required for machines across your organization.

Centralize & automate secrets lifecycle



SOLUTION

Automate complex secrets management tasks with centralized security policy from one platform.

Scale security without sacrificing control



SOLUTION

Scale security and across your hybrid estate while meeting strict compliance regulations.

Secure credentials across use cases



Secrets lifecycle management

Static

Dynamic

Databases

Kubernetes

Cloud credentials



Certificate management

PKI

Managed Keys

SSH



Key management

KMS

KMIP

HSM



Data protection

Encryption

Signatures

Tokenization

Data masking

FPE



Vault's Enterprise benefits

Resiliency



Disaster Recovery
Automatic Snapshots

Scalability



Performance
Replication
Performance Standby
Nodes

RBAC



Namespaces
Policy-as-code with
Sentinel
Control Groups

Compliance



HSM integrations
FIPS 140-2
PCI DSS
DORA
NIS2
ISO
...

Governance, risk, & compliance



SOC Compliance
Auditing
24x7 Support

2

SECURITY LIFECYCLE MANAGEMENT

Vault Radar





HCP Vault Radar

Discover unmanaged secrets

HCP Vault Radar leverages 300+ algorithms to discover sensitive data in Git-supported version control and collaboration platforms.

Scan diverse data sources

HCP Vault Radar integrates with common tools including Git-supported VCS, JIRA, and Confluence.

Remediate leaked secrets

HCP Vault Radar offers customizable remediation guidance based on secret type.

Securing sensitive data

Once sensitive data is identified, HCP Vault Radar provides functionality to secure data in Vault.



Dev



Production



CI

01

SECURITY LIFECYCLE MANAGEMENT

Boundary



Standardize secure remote access

Secure access management

Enforce least-privilege access while also handling credentials on behalf of end users, resulting in just-in-time access to resources.

Simplified and streamlined user experience

VPN-like user experience without requiring new tools or processes. Credentials are provided on demand or injected for a passwordless experience.

Enforce compliance

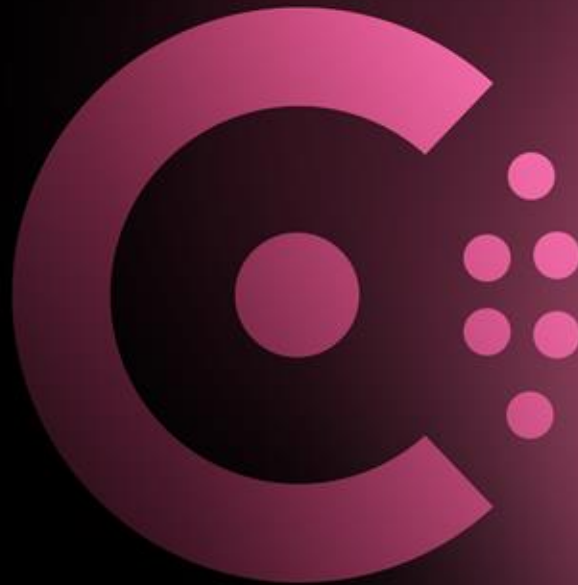
Track user connections, log activity, and record end user SSH sessions. Deter malicious behavior internally and facilitate remediation in the event of a breach.



3

SECURITY LIFECYCLE MANAGEMENT

Consul



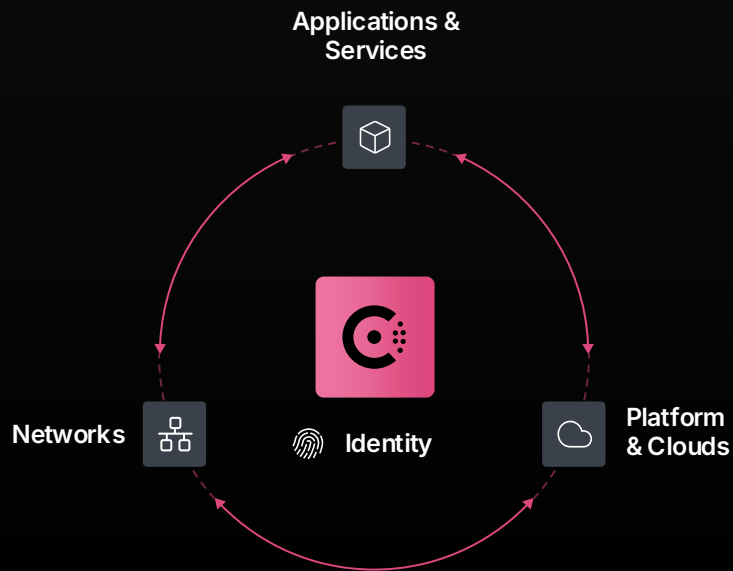
Consul is a Services Networking Platform

Discover and securely connect any service across any runtime

Multi-Platform Service Discovery to create a source of truth and foundation for tracking and routing services

Global Service Mesh & API Gateway to secure service to service connectivity and centralize traffic mgt

Networking Infrastructure Automation to reduce manual ticketing for dynamic IPs and reduce misconfigurations



Scale with enterprise-grade functionality

Automation & optimization



Service Discovery
Health Checks
Consul-Terraform
Sync
Layer 7 Traffic mgmt

Visibility & policy



Layer 7 Observability
Cluster Observability
Mutual TLS
Terminating Gateways
API Gateway ...

Reliability & scale



Cluster Peering
Automated Upgrades
& Backups
Redundancy Zones
Multi-runtime support
Admin Partitions ...

Integrations & API



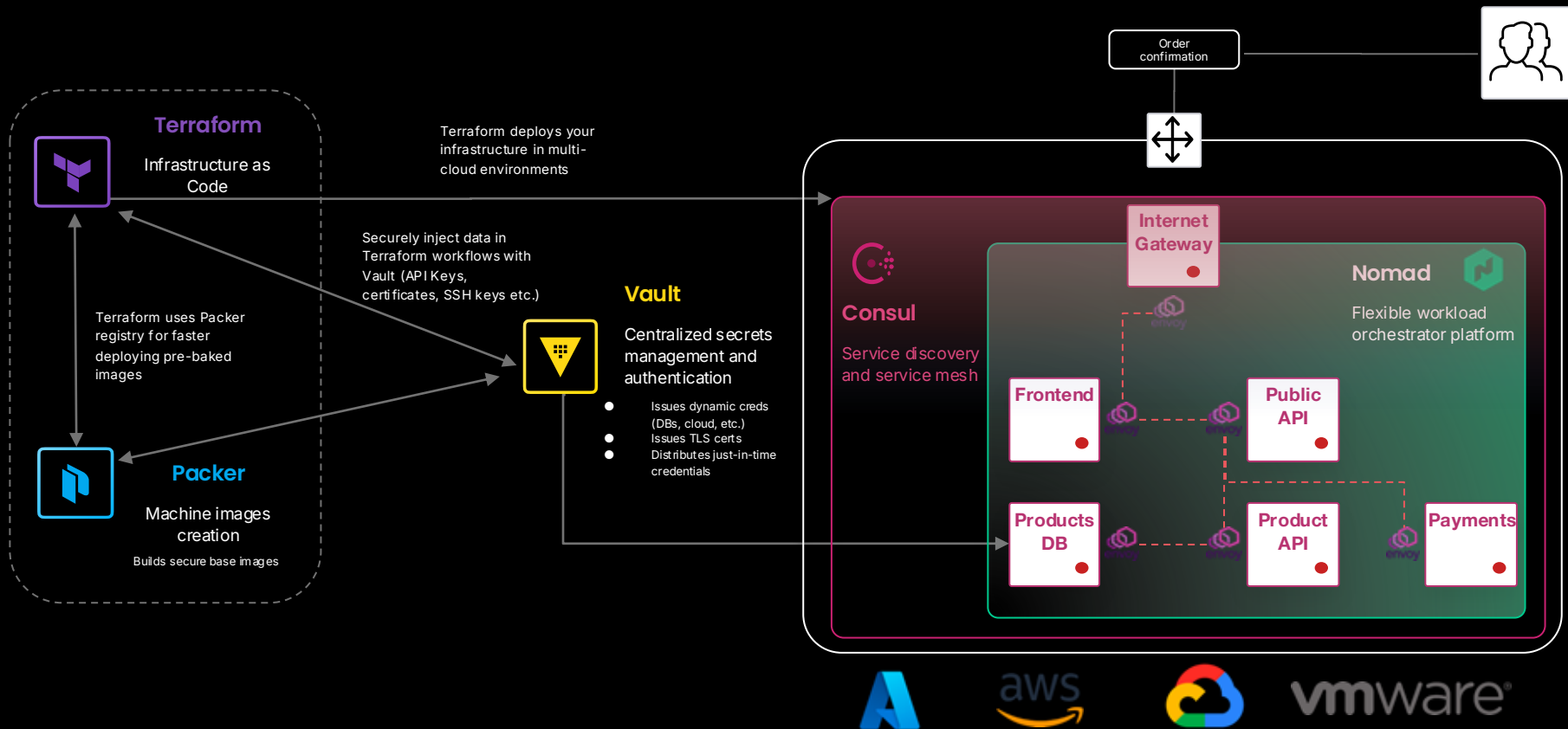
Datadog
Splunk
Grafana
Prometheus
Vault
Terraform ...

Governance, risk, & compliance



24x7 Support
Audit Logs

HashiCorp Portfolio



INFRASTRUCTURE LIFECYCLE MANAGEMENT

Terraform

Cloud growth brings new infrastructure challenges



4,700+

Providers



18,500+

Modules



25+

Run task partners



Google Cloud



Bitbucket



Alibaba Cloud

GitLab

openstack.



Vault

okta

paloalto

splunk>



circleci

servicenow.

Nomad



450M+

Downloads



38K+

Certified users



2,500+

Customers



 BARCLAYS

pandora

Booking.com



SEAT
GEEK



 co-operators



AstraZeneca 

Foot Locker



SAP Ariba 

ROBLOX

wepay
a CHASE company

cruise

 athenahealth

Q2



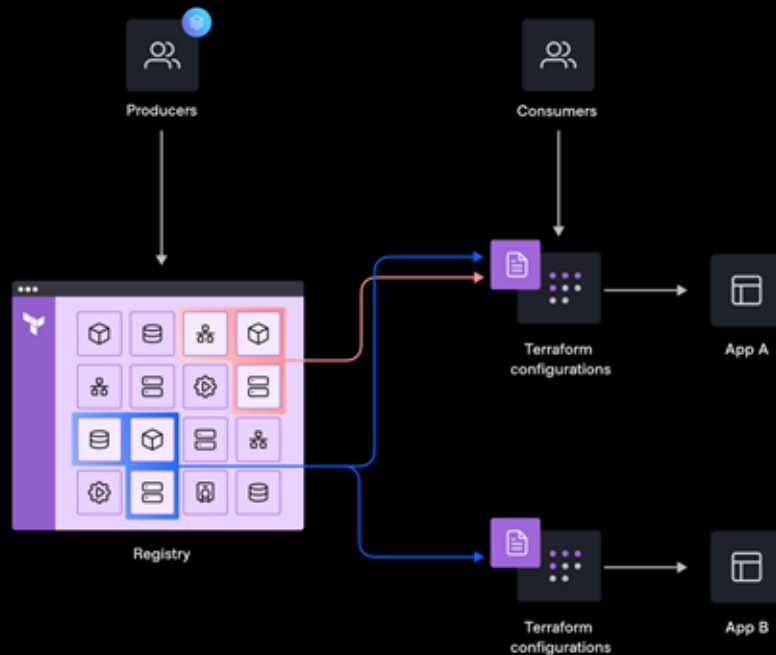
Use vetted infrastructure components

Compose, collaborate, reuse

Promote best practices across your organization with reusable, pre-approved modules and manage the module lifecycle from end to end.

Standardize the provisioning process

Help teams collaborate smoothly and securely with a unified, standardized workflow.



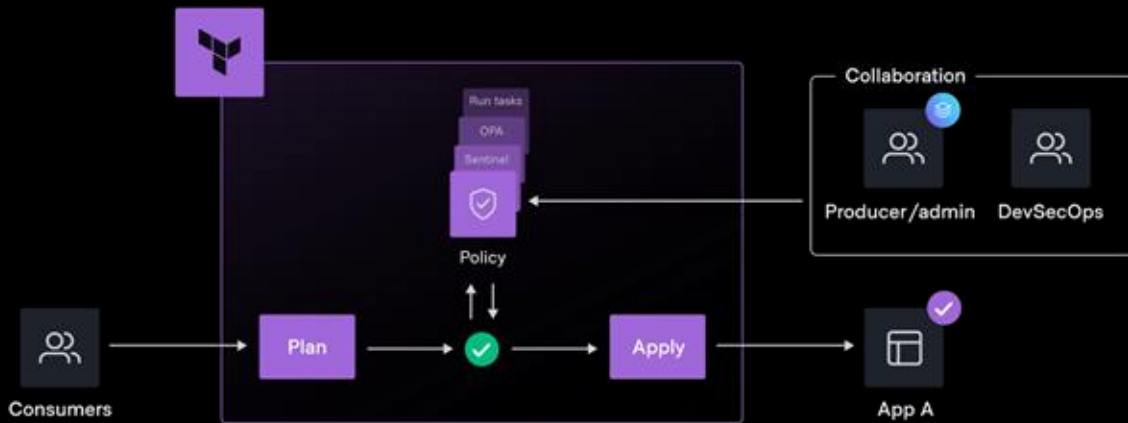
Enforce guardrails automatically

Ensure security

Limit risk and maintain efficiency with automated policy enforcement for compliance when provisioning.

Integrate third-party services

Leverage run tasks that cover security and code scanning, cost control, and regulatory compliance checks for enhanced validation.



Manage the infrastructure lifecycle at scale

Detect and alert

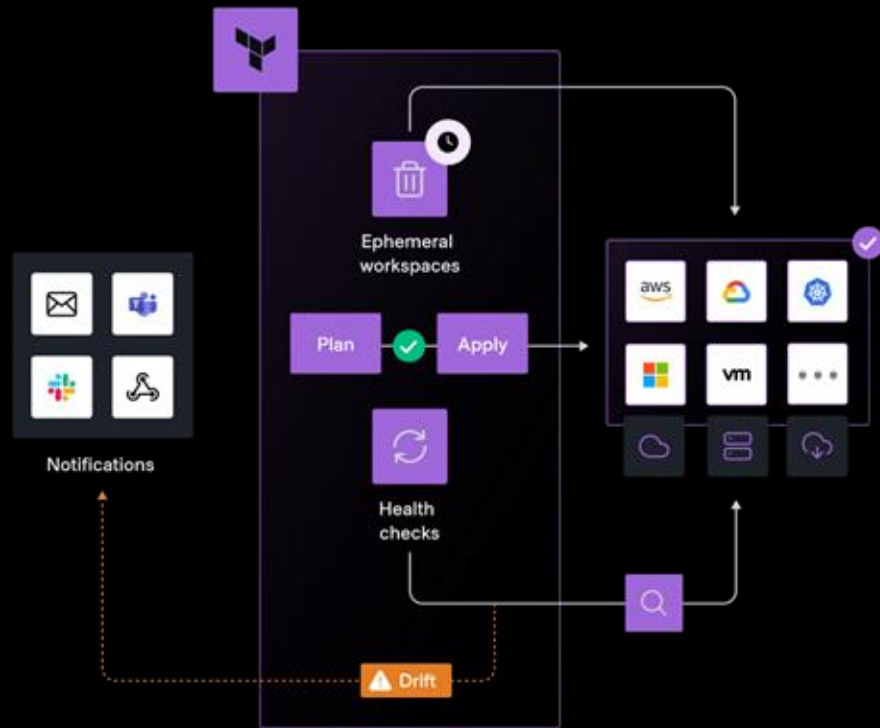
Get alerted when unexpected infrastructure changes happen thanks to continuous visibility that limits costs and security risks.

Validate deployed workloads

Monitor if workloads are operating as expected to respond to image revocation, close security gaps, control budgets, deal with certificate expiration, and more.

Ephemeral workspaces

Enable automatic destruction of resources without manual cleanup, reduce infrastructure costs, and streamline workspace management.



Your biggest risks come after deployment

DAY 0

Monitor all workspace data

Optimize IT operations with a consolidated view.

? THINGS TO CONSIDER

Are you able to keep infrastructure up to date across teams?

DAY 1

Enforce policies and guardrails

Achieve faster deployments with built-in security.

? THINGS TO CONSIDER

Do you still use manual, ticket-based reviews for security and compliance?

DAY 2

Enable self-service

Increase velocity by sharing infrastructure components with self-service workflows.

? THINGS TO CONSIDER

Do your developers rely on a platform team to provision resources?

DAY N

Auto-destroy resources

Eliminate temporary and inactive resources to save costs.

? THINGS TO CONSIDER

Do you have unused or forgotten infrastructure that wastes your budget?



Workspaces

A workspace is a collection of everything Terraform needs to run: configuration, variable values, and state data.

Workspaces offer powerful decomposition for monolithic configurations to match your organization and application structures.

Community

- Workspaces are independent state files

Cloud and Enterprise

- Remote, persistent shared resources
- Flexible permissions for role-based access
- Version control system (VCS) integration

Create a new Workspace

Workspaces determine how Terraform Cloud organizes infrastructure. A workspace contains your Terraform configuration (infrastructure as code), shared variable values, your current and historical Terraform state, and run logs. [Learn more](#) about workspaces in Terraform Cloud.

1 Choose Type

2 Connect to VCS

3 Choose a repository

4 Configure settings

Connect to a version control provider

Choose the version control provider that hosts the Terraform configuration for this workspace.



GitHub



Azure DevOps Services
Azure DevOps



Bitbucket Cloud
Bitbucket Cloud



GitLab.com
GitLab.com

[Connect to a different VCS](#)

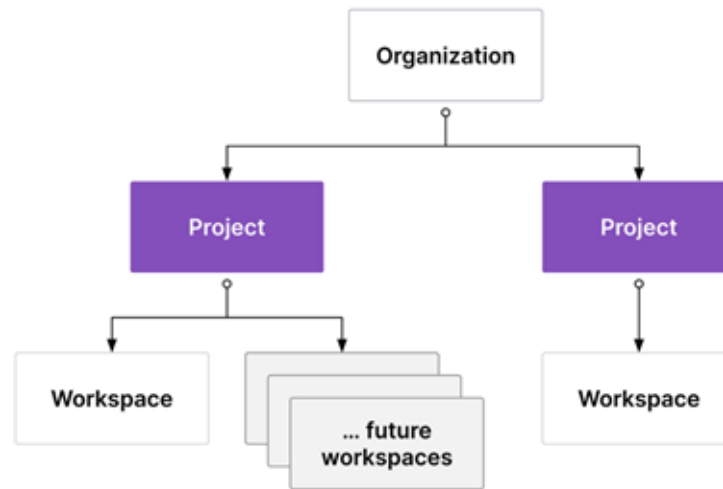




Projects

Organize and govern workspaces

- Group workspaces in an organization based on usage and ownership patterns
- Apply team permissions to achieve least privilege without the management overhead of per-workspace assignment
- Project-scoped variable sets and policy sets to apply consistent guardrails to new and existing workspaces
- Combine with dynamic provider credentials for per-project authentication scope
- Enable self-service with support in no-code provisioning, ServiceNow, and HCP Waypoint workflows

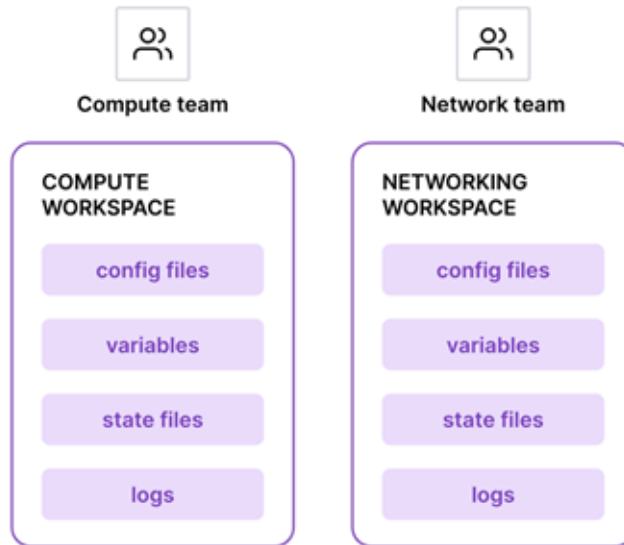




Workspaces

Use workspaces to:

- Organize and decompose monolithic infrastructure into micro-infrastructures
- Match the organization of your application or teams with your infrastructure
- Limit the blast radius of infrastructure changes





Variable sets

Reuse shared variables

Make common input variables available to multiple workspaces without duplicating effort.

Scope assignments to:

- Entire organization
- Projects
- Individual workspaces

Override values at the workspace level for additional flexibility, or mark a variable set as “prioritized” to prevent overrides.

Key	Value	Category
AWS_SECRET_ACCESS_KEY AWS Secret Access Key SENSITIVE	Sensitive - write only	env
AWS_ACCESS_KEY_ID AWS Access Key ID SENSITIVE	Sensitive - write only	env





Infrastructure state

Secure state management

State is Terraform's understanding of the world, providing mapping between configurations and real-world infrastructure.

Remote state management with HCP Terraform and Terraform Enterprise provides encrypted state storage, versioning, and role-based access to state files.

	Triggered via UI #sv-561B13Qnn5dJQPWg danbarr triggered from Terraform 2 months ago #run-9XTRtphsuFaLwINp 31e7582
	Merge pull request #6 from danbarr/fix-security #sv-VWxucMVgaCyP75Ks danbarr triggered from Terraform 3 months ago #run-hK3c46PH4a8UJgG 31e7582
	Triggered via UI #sv-6RGgKVAw9t18UFFz danbarr triggered from Terraform 3 months ago #run-CwFuq1JfK7CncKJf 9e19be4
	Triggered via UI #sv-qzhbv4QTZkb8qwgT danbarr triggered from Terraform 3 months ago #run-yCG82CBNDfMidzGF 9e19be4
	Revert drift and refresh base image #sv-sn37B2nu1dQC8Y5q danbarr triggered from Terraform 3 months ago #run-VMcHfQc5mHvWFf5E 9e19be4
	Merge pull request #4 from danbarr/hashicafe #sv-J29EoJbJtYWhCjtb danbarr triggered from Terraform 3 months ago #run-yqEne9j96Kg9dNHD 9e19be4
	Deploy prod #sv-gQz4YzCjrie5SZVN danbarr triggered from Terraform 3 months ago #run-YLYX9gPcZVEWJZGZ 9e19be4



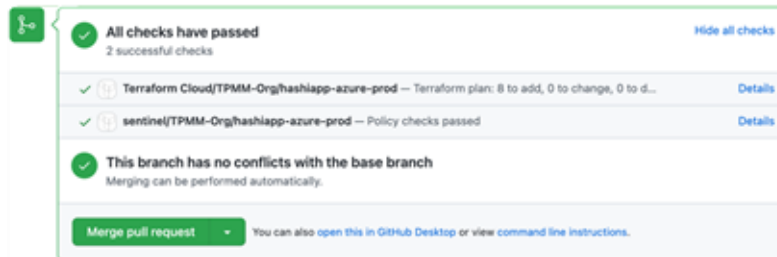
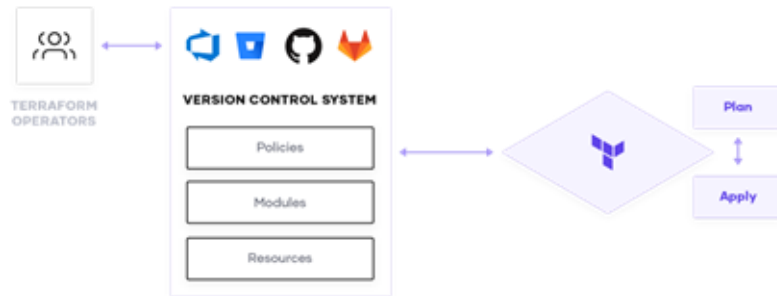


VCS connection

VCS-driven workflow

Terraform connects to the major VCS providers allowing for automated versioning and execution of configurations.

- Integrate with existing VCS workflows
- Automatically trigger runs and policy checks upon pull requests and merges
- Automatically publish new module and policy set versions when merged/tagged in Git
- Support for cloud and self-hosted versions of Azure DevOps, Bitbucket, GitHub, and GitLab





Remote operations

Consistent runtime environment

HCP Terraform and Terraform Enterprise allow users to trigger runs remotely, while automatically coordinating runs by multiple users.

- Execution modes:
 - UI or VCS via pull request/merge
 - CLI with the `cloud` backend
 - API call in CI/CD pipeline
- Runs execute in disposable single-use agents
- Automatic state locking prevents conflicting changes
- Run history and state versioning empowers collaboration

✓ Applied **Update default instance size and image**

 danbarr triggered a run from GitHub a few seconds ago

Run ID	run-SK82qsZWTw5Psv8U	
Configuration	From GitHub by  danbarr	Branch main Repo danbarr/tf-azure-webapp
Commit	9b8bf0a : Update default instance size and image	
Trigger	File change detected in VCS	
Execution Mode	Remote	

✓ **Plan finished** 2 minutes ago

Started 11 minutes ago > Finished 11 minutes ago

+ 1 to create



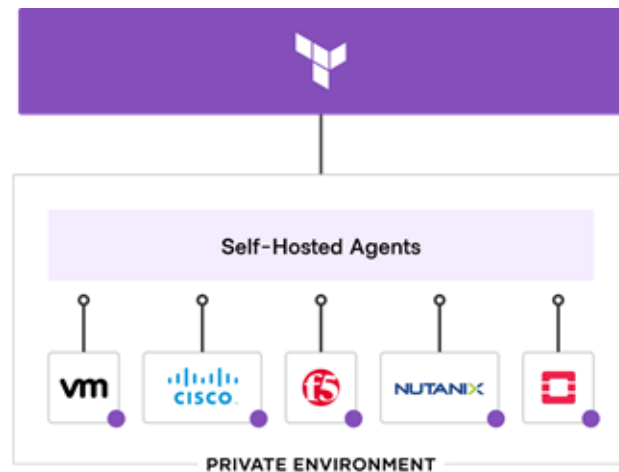


Remote operations

Self-hosted agents

HCP Terraform agents can be self-hosted in a private network or on-premises environment. This allows Terraform to securely interact with APIs that are not reachable from the public internet.

No inbound network access is required, agents only make outbound connections to the HCP Terraform or Terraform Enterprise control plane.



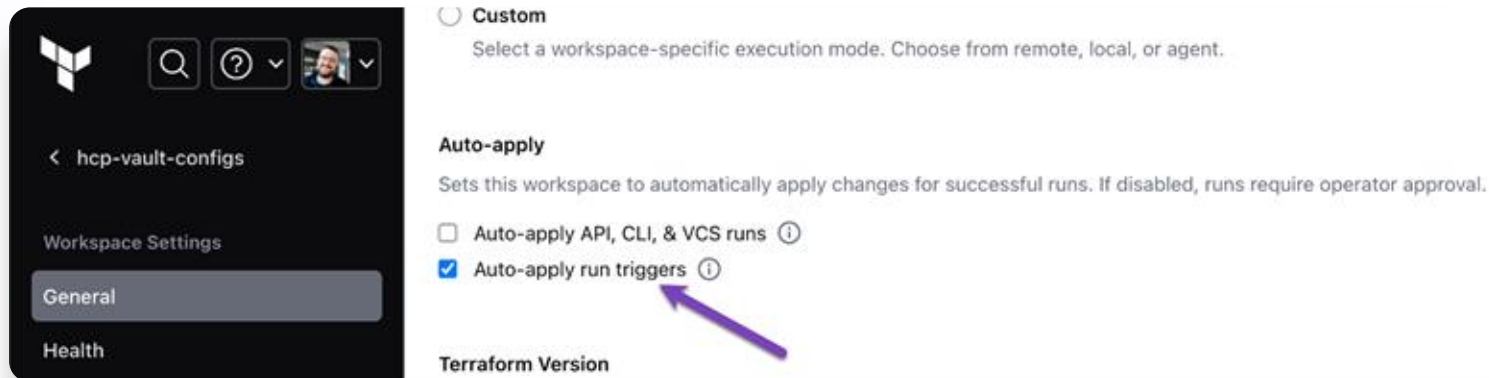


Run triggers | Auto-apply

Chain applies across workspaces

Previously, run triggers would not auto-apply the downstream workspace, even if that workspace had auto-apply enabled.

Workspace setting to auto-apply runs started by a run trigger.





Team management

Custom permissions

Choose from predefined access levels or customize permissions for teams at the organization, project, and workspace level.

Granular permissions include:

- View, execute, and approve runs
- Download Sentinel mocks
- Access to variables and state versions
- Approve policy overrides
- Manage organization and workspace settings

The screenshot shows the 'Add team access' interface. At the top, it says 'Grant a team permissions on this project.' Below this, a note states: 'Standard permission groups (Admin, Maintain, Write, Read) contain additional permissions not shown below. [Learn more about project permissions](#).' The interface is divided into two main sections: 'Team' and 'Custom Permissions'. In the 'Team' section, there is a 'Select team' dropdown menu. Below it, under 'Permission groups', there are five options: 'Read' (Can view everything in the project), 'Write' (Can update everything in the project), 'Maintain' (Full control of everything in the project, but not the project itself), 'Admin' (Full control of the project), and 'Custom' (Create a custom permission set for this team). The 'Write' option is currently selected and highlighted with a blue border. At the bottom of the 'Team' section are 'Assign permissions' and 'Cancel' buttons. The 'Custom Permissions' section on the right is titled 'Create a custom permission set for the selected team'. It contains three sub-sections: 'Project access' with options 'Read' (selected), 'Update', and 'Delete'; 'Create workspaces', 'Delete workspaces', and 'Move workspaces' (all unchecked); and 'Team management' with options 'None' (selected), 'Read', and 'Manage'.





Policy as code

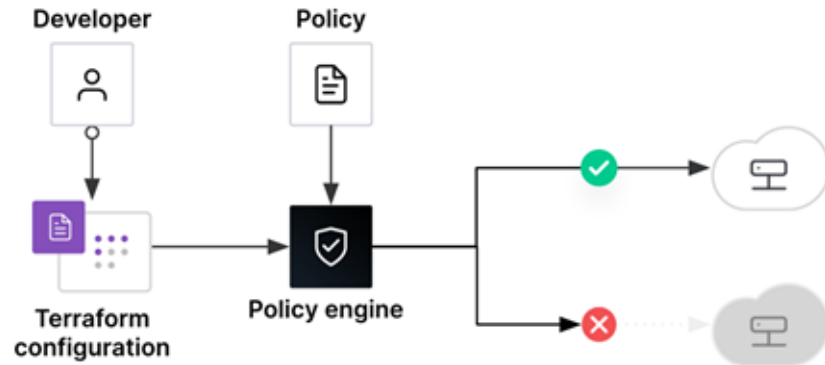
Codify governance

Automate reviews and approvals to help teams move faster without increasing risk

- Codify policies to create automated guardrails
- Policy checks built into the provisioning workflow
- Use policy to enforce best practices, security measures, or compliance requirements

Implementations:

- Community-driven scanning and policy tools
- Commercial offerings
- HashiCorp Sentinel





Policy as code | Sentinel

Sentinel policy as code framework

Automate reviews and approvals to accelerate teams without increasing risk

- Codify policies to create automated guardrails
- Policy checks built into the provisioning workflow
- Use policy to enforce best practices, security measures, or compliance requirements

Granular enforcement levels:

- Advisory: warning when a policy fails
- Soft mandatory: explicit override is required to proceed
- Hard mandatory: block provisioning when a policy fails

```
import "tfrun"
import "tfplan/v2" as tfplan

desired_vm_size = "Standard_D2"
workspace_name = tfrun.workspace.name

configured_vm_size =
  tfplan.module([]).resources.`
    azurerm_virtual_machine.catapp[0].appli
    ed.vm_size

main = rule {
  desired_vm_size == configured_vm_size
}
```





Run tasks

Extend the Terraform workflow with external services

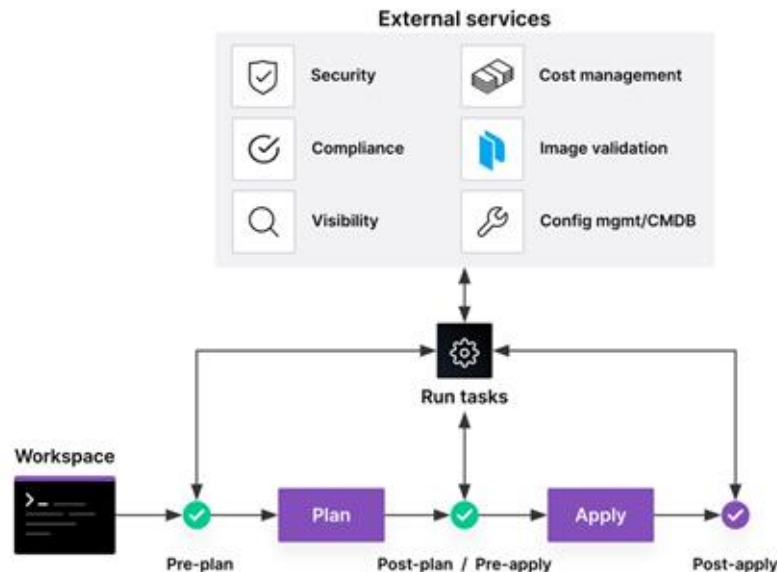
Integrate third-party partner and custom services during pre-plan, post-plan, pre-apply, and post-apply.

Enables extended capabilities for:

- Security
- Regulatory compliance
- Cost management
- Visibility

Customize enforcement level (advisory or mandatory) per-workspace or org-wide.

Discover integrations in the Terraform Registry.



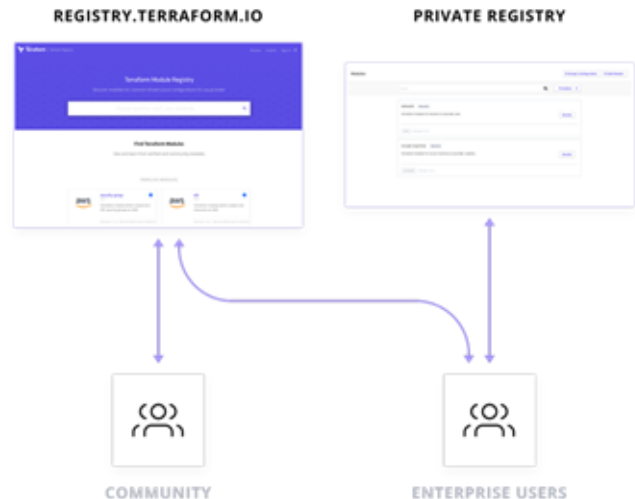


Private registry

Systematic approach to testing

The private registry, part of HCP Terraform and Terraform Enterprise, offers organizations a secure repository to store and share modules and custom providers.

- Modules can be authored with best practices and operational efficiency built in, e.g. tagging resources, secure-by-default configurations, etc.
- Providers and modules from the public registry can be added to offer a curated selection of approved components
- Automatic publishing and versioning via VCS integration





No-code provisioning

Predefined input values

No-code module publishers can specify acceptable values for required input variables.

- Reduces the risk of failed deployments due to typos or invalid input
- Examples:
 - Cloud regions
 - Instance sizes
 - Metadata values

New workspace from module
Module: HashiCafe-inc/nocode-webserver/aws

1 Configure module inputs 2 Configure workspace settings

prefix
This prefix will be included in the name of most resources.
hashicafe

env
Select one of the provided options
✓ dev
test
prod

The region where the resources are created.
us-east-2

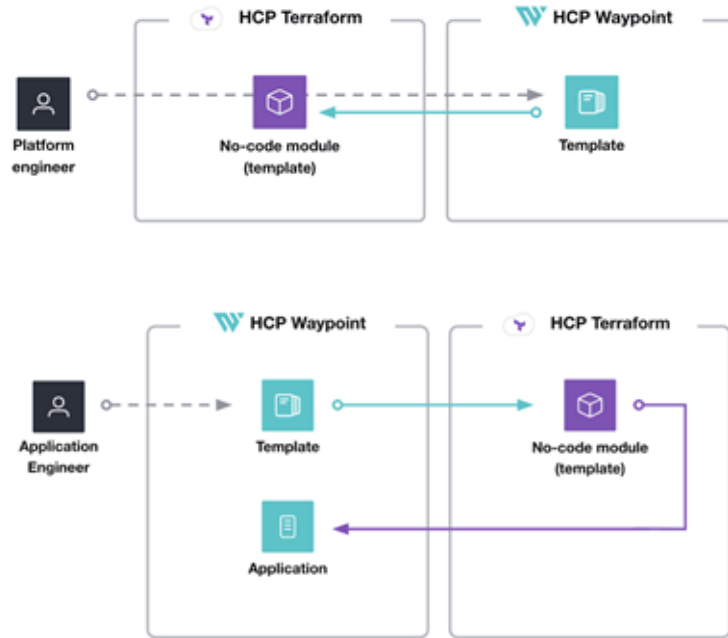
Cancel Next: Workspace settings



HCP Waypoint

HCP Waypoint is now generally available with templates to enable enterprise platform teams to abstract and standardize application scaffolding in one place.

- **Templates** abstract and standardize application scaffolding like infrastructure, dependencies, application workflows, and access control in one place
- **Terraform no-code modules** underpin templates and allow developers to create their applications without worrying about the infrastructure details
- **Template upgrade workflow** pushes upgrades to Waypoint applications when the Waypoint template is updated, including updates to the underlying Terraform module version





Drift detection

Detect and alert when unexpected infrastructure changes occur

- Assessment runs are preemptively performed
- Supports all resources provisioned by Terraform
- Customizable notifications via email, Slack, or Microsoft Teams
- Optionally receive alerts via webhooks for custom responses
- Enable per-workspace or org-wide

The screenshot displays the 'Projects & workspaces' dashboard in the HashiCorp Terraform Cloud console. At the top, there's a header with 'HashiCorp-inc / Projects & workspaces' and a 'New' button. Below this, the 'Workspaces' section is active, showing a search bar and filters for Tags, Status, and Health (1). A dropdown menu is open for the 'Health' filter, showing options: 'Drift' (selected), 'Health error', and 'Check failed'. The main table lists three workspaces:

Workspace Name	Run Status	Repo	Health
hashicorp-db-dev Health warning Database	✓ Applied		
hashicorp-shared-networking Health warning Shared-Services	✓ Applied	danbar/tf-aws-demo-vpc	3 days ago
hashicorp-web-prod Health warning ECommerce-Frontend	✓ Applied	danbar/tf-aws-webapp	2 hours ago

At the bottom, a 'Health' summary card shows '2 minutes ago' and a 'View Details' link. It includes a progress bar and a table of resource counts:

Drifted resources	Not drifted
3	10





Continuous validation

Customizable alerts

Codify assertions to verify the health of resources via custom conditions and checks.

Use cases include:

- Image revocation (with HCP Packer)
- Certificate expiration
- Service health
- Application functional validation

Enable per-workspace or org-wide

Continuous validation

 Ready [Start health assessment](#)

Last successfully checked a few seconds ago. Next assessment in an hour.

Your infrastructure does not satisfy the assertions defined in your configuration. Learn more about [continuous validation](#).

Failed 1 Passed 4 Unknown 0 All 5



ASSERTION	STATUS	MESSAGE
aws_instance.hashicorp	 Passed	Assertion passed
check_dns_health	 Passed	Assertion passed
▼ check_web_health	 Failed 2	2 assertions failed
	 Failed	The image referenced in the Packer bucket is more than 30 days old.
	 Failed	http://ec2-3-129-173-35-us-east-2.compute.amazonaws.com returned an unhealthy status code
data.aws_subnets.default	 Passed	Assertion passed





Notifications

Customizable alerts

Configure email, Slack, Teams, or webhook notifications for workspace events:

- Health events: drift detected or health assessment failed
- Run events: created, needs attention, completed, errored, and more

Create a Notification

Notifications allow you to send messages to other applications based on run and workspace events.

Destination



Webhook
POST messages to any
URL



Email
Send messages to users
via email



Slack
Send messages to a Slack
channel



Microsoft Teams
Send messages to a
Microsoft Teams channel

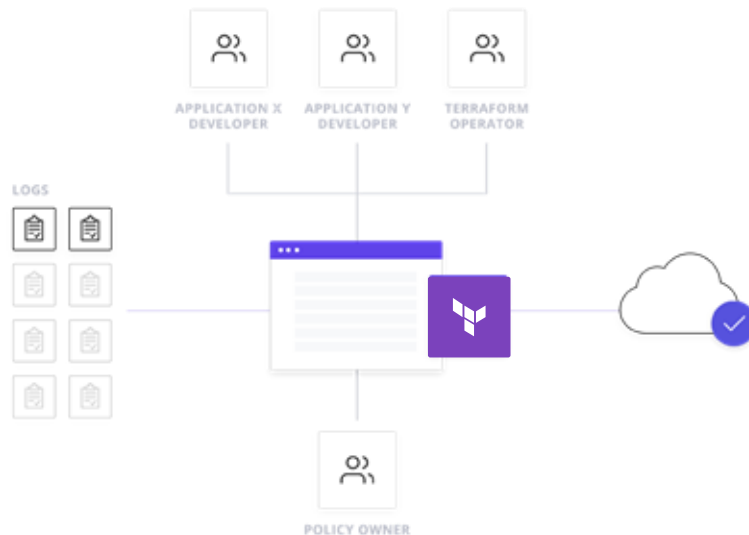




Audit logs

Terraform audit logs provide a stream of events related to activities in an organization.

- Track operations and identity across the organization to gain insight into past and present configurations
- Trace the actor, action, and affected resource
- Events include settings, configuration changes, executions, and environment updates





Audit logs | Splunk integration

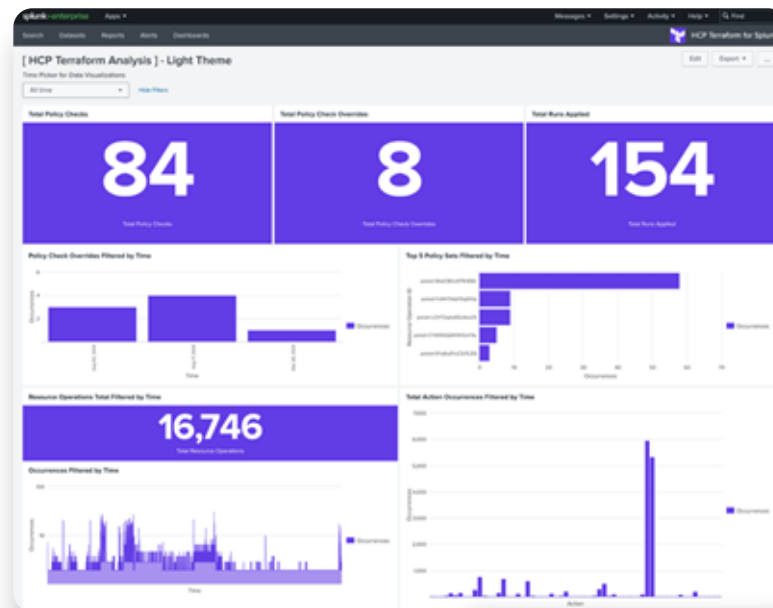
HCP Terraform auditing with Splunk

Official Splunk app polls the audit trails API endpoint

Pull audit logs from HCP Terraform without complicated network or firewall configurations

Splunk app includes dashboards to easily query and visualize events

Enable long-term retention of audit events





Ephemeral workspaces

Automatic resource destruction

Set a time-to-live for a workspace to auto-initiate a destroy run.

Schedule a one-time destruction, or recurring based on inactivity.

Configure reminder and completion notifications.

Use cases include:

- Development sandboxes
- Automated test pipelines
- Demo or classroom lab environments

Automatically destroy

Set a date and time to automatically destroy infrastructure in this workspace.



Auto destroy settings

☒ Destroy at specific time ☐ Destroy if inactive Beta

Terraform Cloud will automatically destroy the resources in this workspace at the specified time.

Timeframe

Custom

Date

11/08/2023, 01:28 PM

Timezone (Local)

GMT-08:00 (Pacific Standard Time)

Auto destroy will run in

Confirm auto destroy

Manually destroy

Queuing a destroy plan will destroy infrastructure managed by Terraform Cloud. Run `terraform destroy -out=destroy.tfplan` locally.

Queue destroy plan

Calendar interface showing the date selection process. The calendar is for November 2023. The date 11/08/2023 is selected. The time 01:28 PM is selected. The timezone is GMT-08:00 (Pacific Standard Time).





Terraform CE to HCP migration

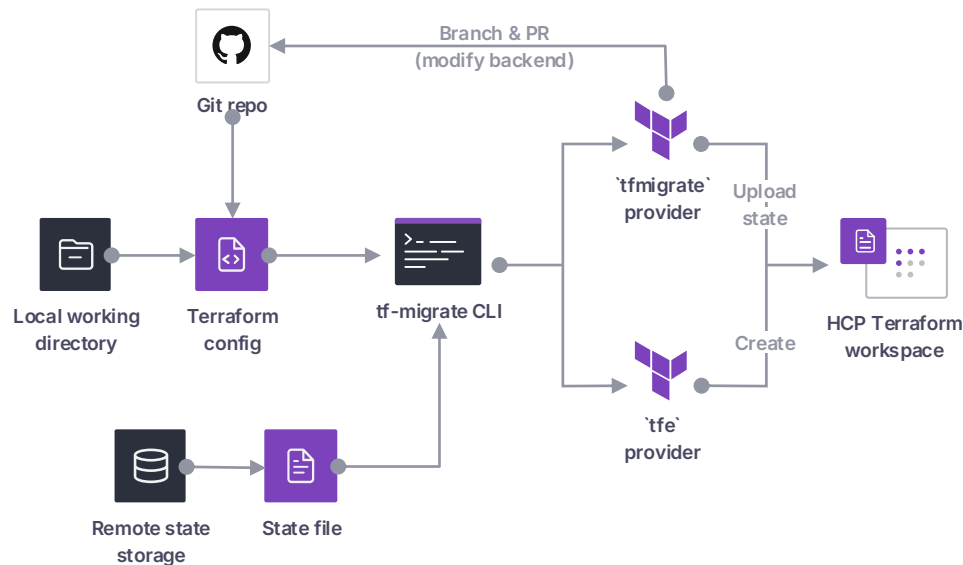
Automated migration

The Terraform CE to HCP Migrator (tf-migrate) facilitates migration of common DIY workflows from Community Edition to HCP Terraform or Terraform Enterprise.

Automates the following aspects of migration:

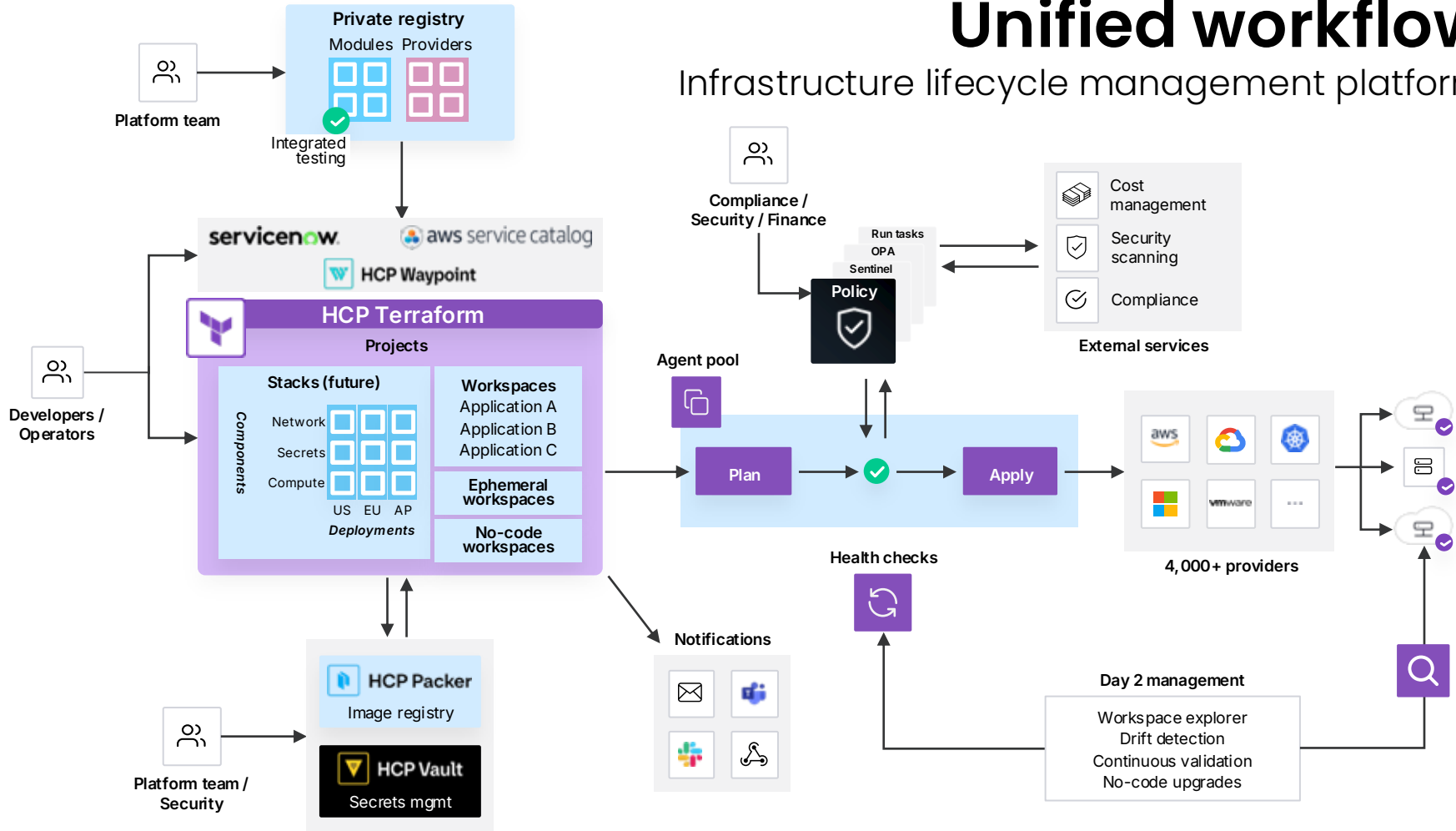
- Workspace setup
- State migration
- Backend changes

Workspace config is generated using the `tfe` provider which can be used for ongoing workspace management.



Unified workflow

Infrastructure lifecycle management platform



Enabling Platform Team Capabilities

Terraform Community

Use infrastructure as code to provision resources

CLI only

DIY approach

Unknown usage within Teams

No support

Terraform Enterprise



Automate

Automate Pipelines and Infrastructure as code

Leverage providers and pre-approved, reusable modules

Connect to VCS for source code collaboration



Secure

Enforce security and compliance standards with RBAC and policies

Standardize workflows and enable self-service

Integrate with industry leading operation tools

Protect secrets & state files



Manage

Gain usage and health visibility across the entire organization

Validate the health of deployed resources with Terraform drift detection & continuous validation

Auto-destroy temporary resources

24x7 Support

Solutions for cloud success



Infrastructure automation

Rapidly provision development environments and CI/CD pipelines.

Accelerate innovation and efficiency



Secure provisioning and authentication

Enforce secure and compliant workflows

Multi-cloud risk mitigation



Image management

Secure and centrally manage all of your images

Multi-cloud risk mitigation



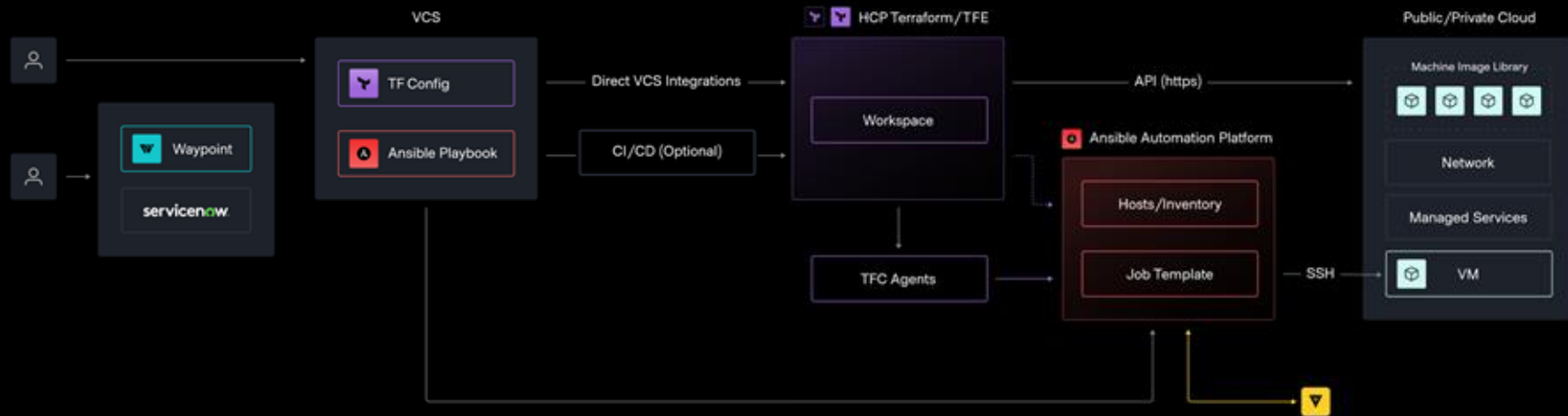
Self-service infrastructure

Empower teams by making infrastructure easily accessible and at scale

Accelerate innovation and efficiency and Optimize cloud operations and ROI

STREAMLINED WORKFLOW TO PROVISION AND CONFIGURE INFRASTRUCTURE ACROSS ANY CLOUD

Integration architecture — Terraform, Vault and Ansible



HCP Terraform and Terraform Enterprise

HCP TERRAFORM (Cloud)	TERRAFORM ENTERPRISE
- Includes HCP Waypoint - Includes The Explorer - Includes Terraform Stacks - SaaS - Priced by Resources Under Managed	- Operational burden - Flexibility in terms of deployment and architecture - Priced by Workspaces



Thank you

