armanino

System and Organization Controls (SOC) 3

Report on Controls Relevant to the Security, Availability, and Confidentiality Trust Services Categories

December 1, 2021 to November 30, 2022

REPORT PREPARED FOR

HashiCorp

TABLE OF CONTENTS

armanino

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of

HashiCorp, Inc.

San Francisco, California

Scope

We have examined HashiCorp, Inc.'s ("HashiCorp" or the "Company") accompanying assertion titled "Management's Assertion" (assertion) that the controls within HashiCorp's cloud infrastructure automation platform were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved based on trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service Organization's Responsibilities

HashiCorp is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved. HashiCorp has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HashiCorp is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HashiCorp's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Service Auditor's Independence

We are required to be independent of HashiCorp and to meet our other ethical responsibilities in accordance with the relevant ethical requirements relating to our examination.

Opinion

In our opinion, management's assertion that the controls within HashiCorp's cloud infrastructure automation platform were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

ARMANINO LLP

Armanino LLP

San Francisco, California

January 27, 2023

MANAGEMENT'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within HashiCorp, Inc.'s ("HashiCorp" or the "Company") cloud infrastructure automation platform (system) throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that HashiCorp's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section III "Description of the System" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). HashiCorp's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Description of the System."

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE HASHICORP CLOUD INFRASTRUCTURE AUTOMATION PLATFORM

Overview of Operations

Company Overview

Founded in 2012, HashiCorp, Inc. ("HashiCorp" or the "Company") is a cloud infrastructure automation company that enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. Each product is aimed at specific stages in the lifecycle of a software application, with a focus on automation. Many have a plugin-oriented architecture in order to provide integration with third-party technologies and services.

HashiCorp is headquartered in San Francisco, but is a remote-first company, and as a result, HashiCorp employees are distributed across the globe, including the United States, Canada, Australia, Bulgaria, France, Japan, Netherlands, UK, Sweden, and Germany, among others.

Services Provided

HashiCorp's suite of products consist of software that can be installed on-premises, and cloud-hosted Software-as-a-Service (SaaS) products. HashiCorp Cloud Platform (HCP) is a fully managed platform offering HashiCorp products as a service to automate infrastructure on any cloud.

HCP products are deployed, operated and maintained by HashiCorp on behalf of its customers. SaaS offerings include products such as Terraform Cloud (TFC), HCP Vault on AWS, and HCP Consul on AWS. On-premises software is provided by HashiCorp to customers for deployment and operation within their own computing environment(s), whether in private data centers or in cloud environments, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure; HashiCorp's Cloud Platform products are deployed, operated and maintained by HashiCorp on behalf of its customers.

The HashiCorp suite of products addresses the challenges of provisioning, securing, connecting, and running cloud infrastructure: providing consistent workflows and automation appropriate to multi-cloud infrastructure, security, and network management.

The on-premises HashiCorp software products - collectively referred to as "On-Premises Products" - in scope are further described below:

- Provision: (Terraform): Automate provisioning, compliance and management of cloud infrastructure using a common workflow. Terraform Enterprise provides collaboration, governance, and self-service workflows on top of the infrastructure as code provisioning from open source. Terraform Enterprise provides workspaces, modules, and other powerful constructs for teams working together to build infrastructure. Operators can package infrastructure as code into reusable modules enabling developers to quickly provision in a self-service fashion. Likewise, policy-as-code and logging enable organizations to secure, govern, and audit their entire deployment.
- Secure (Vault): Manage secrets and protect sensitive data based on user and workload identity. Vault tightly controls access to secrets and encryption keys by authenticating against trusted sources of identity such as Active Directory, LDAP, Kubernetes, CloudFoundry, and cloud platforms. Vault enables fine grained authorization of which users and applications are permitted access to secrets and keys.
- Connect (Consul): Accelerate application delivery by automating the network, including physical devices, virtual appliances, and distributed service mesh.

Overview of Operations (continued)

Services Provided (continued)

- Run (Nomad): Deploy any application and iterate safely with progressive delivery, failover strategies, and integrated security and network.

The HashiCorp SaaS offerings in scope are:

- Terraform Cloud: Terraform Cloud is an application that helps teams use Terraform together. It manages Terraform runs in a consistent and reliable environment and includes easy access to shared state and secret data, access controls for approving changes to infrastructure, a private registry for sharing Terraform modules, detailed policy controls for governing the contents of Terraform configurations.
- HCP Vault on AWS: HCP Vault allows organizations to get up and running quickly, providing immediate access to Vault's best-in-class secrets management and encryption capabilities, with the platform providing the resilience and operational excellence so you do not have to manage Vault yourself.
- HCP Consul on AWS: HCP Consul is a fully managed service mesh to discover and securely connect services in AWS. This provides an easy path to adopt service mesh for both individuals and organizations while reducing the operational burden of running it in production. HCP Consul is offered in both an on-demand and annual subscription offering.

The following HashiCorp departments are included as part of the scope of this document:

- Engineering: responsible for developing the source code of the products, maintaining the code, and assisting customers with troubleshooting when necessary.
- Cloud: responsible for deploying, managing, and monitoring HCP.
- Support: responsible for providing technical support for customers.
- Security: responsible for defining and executing HashiCorp's security and compliance activities.
- IT: responsible for managing and supporting corporate assets, such as laptops and SaaS applications used by HashiCorp personnel.
- Legal: Responsible for overall corporate governance and compliance, including negotiating contracts with customers and service providers to ensure they adhere to applicable regulations and standards, and addressing any non-compliance issues should they arise.

People (HR): Develop/maintain org charts and communicate key areas of authority, responsibility, and line of reporting. Maintain job descriptions with defined skills, responsibilities and knowledge required for a particular job. Ensure employees acknowledge in writing that they have read and understood the security policies, code of conduct, and other relevant enterprise policies and standards.

Risk Assessment

HashiCorp maintains a risk management process to identify, assess, prioritize, and address risks. The HashiCorp security team is responsible for performing risk assessments. A risk owner is identified and documented for each identified risk. Internal, external, and fraud risks are considered.

The assessment process includes scoring the risk, identifying already implemented mitigations and, where there are no active mitigations, identifying potential mitigations. Every risk for which mitigations aren't currently implemented or mitigations are incomplete must be remediated or accepted by the risk owner. Remediations are prioritized based on importance and available resources. Risk assessment results are communicated to all relevant stakeholders. Risk owners are made aware of identified risks and all context and background around mitigations and risk acceptance.

Risk assessments are reviewed at least quarterly, or as major changes are made, whichever comes first.

CONTROL ACTIVITIES

Policies and Procedures

Relevant policies, standards, and procedures are updated by their respective owners and made available to HashiCorp employees through the HashiCorp intranet. HashiCorp maintains a formal security policy. The HashiCorp security policy is version and change controlled, and changes are approved by authorized personnel prior to being made. Information security topics addressed by the HashiCorp security policy include, but are not limited to:

- Software development
- Vulnerability management
- Logging and monitoring
- Asset management
- Physical security
- Data classification
- Risk management
- Access management
- Vendor security risk management

Network Security Overview

Cloud Products (Terraform Cloud, HCP Consul on AWS, HCP Vault on AWS)

All sensitive data transmitted and processed within the production network are encrypted in transit and at rest. Servers and network components are secured with access control mechanisms and protected by hardened industry standard network configurations. All security services are monitored and updated in a timely manner to address emerging vulnerabilities.

On-Premises Products

On-premises products are deployed by customers within environments under their control. Network security is the responsibility of the customer. HashiCorp provides guidelines on data security that customers may use to secure their deployments. It is the responsibility of the customer to implement any guidelines appropriate to their deployment.

Network Security Overview (continued)

Remote Access

Cloud Products (Terraform Cloud, HCP Consul on AWS, HCP Vault on AWS)

Remote access to the production environment and instances is restricted using an internal cloud authentication broker tool developed and maintained by the security team.

On-Premises Products

On-premises products are deployed by customers within environments under their control. HashiCorp does not have remote access to customer environments.

Endpoint Protection

Cloud Products (Terraform Cloud, HCP Consul on AWS, HCP Vault on AWS)

All production hosts have system-level monitoring and alerting for malicious activity. Alerts are sent to the security team for triage.

Employee Workstations

Endpoint protection and monitoring software is deployed to all employee workstations. HashiCorp uses a managed endpoint security, detection, and response solution, Crowdstrike Falcon Complete. Endpoint agents monitor and alert for malicious activity. Alerts are reviewed and triaged, and confirmed incidents remediated by the Falcon Complete and security teams.

Secure Baseline Configurations

Cloud Products (Terraform Cloud, HCP Consul on AWS, HCP Vault on AWS)

Production infrastructure is configured in accordance with industry best practice. A secure base image is created for use by production hosts. HashiCorp defines and manages its infrastructure configurations as code. Changes to infrastructure configurations are subject to the controls discussed under *Change Management*.

Patch Management

Cloud Products (Terraform Cloud, HCP Consul on AWS, HCP Vault on AWS)

Production hosts use a secure base image as described in *Secure Baseline Configurations*. The secure base image is patched on a weekly basis and made available for use in production environments. HashiCorp infrastructure is immutable. When infrastructure is rotated, it uses the latest available, patched image.

Identity and Access Management

HashiCorp maintains an access control policy requiring access to HashiCorp information and resources must be provided according to the principles of least privilege.

Identity Management & Multi-Factor Authentication

Whenever possible, applications and systems use Okta single sign-on (SSO) or federated authentication over local accounts and passwords. HashiCorp services protected by Okta services are automatically configured to require multi-factor authentication.

Applications and systems containing restricted, or customer data must be protected by multi-factor authentication or Okta. Exceptions must be approved by the security team.

Network Security Overview (continued)

Identity and Access Management (continued)

Access Reviews

Access to each system and application are reviewed regularly by the owner. The frequency of the review will be determined by the criticality of the data. Access to production cloud infrastructure is reviewed at least quarterly. Other access is reviewed in accordance with risk, but no less frequently than annually. If any unnecessary access accounts are found, appropriate remediation action is taken.

System Passwords

Users are required to enter a user ID and password to access any HashiCorp system or application. Complexity standards for passwords have been established to enforce control. Password length for the HashiCorp workforce identity and access management platform must be 14 characters or more, which is the minimum to access production systems. Use of publicly available identification information as a password and the re-use of old passwords is prohibited. All system default passwords are changed.

When use of the HashiCorp workforce identity and access management platform is not possible, HashiCorp encourages the use of a password manager to generate and manage strong passwords which must be a minimum length of 8 characters or more.

Security & Incident Management

HashiCorp maintains a security incident response plan (SIRP) defining the protocols for assessing and responding to security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The incident process encompasses six phases: preparation, detection, containment, investigation, remediation, and recovery.

Security events are detected using security tools or notification by an inside or outside party. Incidents are reviewed by the security team. When a security event is confirmed as an incident, relevant stakeholders are notified and investigation begins, where the security team determines the priority, scope, and root cause of the incident. During the containment phase, the affected host or system is identified, isolated, or otherwise mitigated, and when affected parties are notified and investigative status established. Remediation is the post--Incident repair of affected systems, communication, and instruction to affected parties, and analysis that confirms the threat has been contained. Recovery then analyzes the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of “lessons learned” into future response activities and training.

System Development Life Cycle

HashiCorp’s software development practices are aligned with the HashiCorp security policy. The secure development model includes key steps such as analysis and design, development practices, testing and quality assurance, build and release, and software and maintenance. The standard ensures appropriate reviews and approvals are made by appropriate personnel prior to updates being made to production or build releases.

Terraform Cloud

Production and staging environments are kept strictly separate. No production data is used in staging environments or testing on local developer machines.

HCP Vault and HCP Consul

Production and staging environments are kept strictly separate. No production data is used in staging environments or testing on local developer machines.

Network Security Overview (continued)

Change Management Policy

Software source code is stored on GitHub, where a subset is publicly available as open-source software (OSS). Access to non-OSS source code and associated management platforms is restricted to authorized individuals.

All code changes are reviewed by at least one member of the HashiCorp engineering team, with small frequent iterations encouraged. During this review process, engineering team members provide comments and feedback to ensure submitted changes address the requirements outlined in the design specifications, as well as maintaining quality and security standards.

Changes are approved prior to incorporation into existing on-premises products and services. Approvals are not required for minor changes which do not impact the Terraform Cloud, HCP Consul, and HCP Consul on AWS production environment. All change requests and associated approvals are recorded and available to audit by engineering leadership and the security team. Additionally, significant changes are captured in release announcements.

Product Security

The Product Security team contributes to the security of all products and services across HashiCorp. Product security works cross-functionally to improve security in product design, release management, and development and performs internal security testing. Product security also engages and coordinates third-party penetration testing.

Security Testing

A range of automated and manual, scheduled and ad-hoc product security testing activities are conducted, including:

- Code review
- Static code analysis
- Dynamic testing
- Fuzzing
- Vulnerability scans
- Virus/malware scanning of code repositories

Third-Party Assessment & Penetration Testing

HashiCorp engages an independent third-party to conduct annual security assessments, including penetration testing activities, of on-premises products and cloud services.

HashiCorp conducts internal and external assessments to ensure controls are effectively designed, implemented, and operating. Internally, control reviews, gaps analysis, and assessment exercises are performed on an ongoing basis to continuously monitor the design and operating effectiveness of controls. Externally, HashiCorp engages independent third-party firms to achieve certification against established frameworks such as SOC 2 and ISO 27001.

Management reviews and assesses results from continuous monitoring and certification activities. Control deficiencies are communicated internally, prioritized, and remediated.

Network Security Overview (continued)

Product Security (continued)

Vulnerability Management

HashiCorp identifies and remediates security vulnerabilities across all products. Vulnerabilities are identified through internal testing and external reports. The source and status of all vulnerabilities are tracked through an internal vulnerability response tracker.

Vulnerability fixes are included in new product releases, and communicated via product changelogs, security bulletins, and common vulnerabilities and exposures (CVE) entries.

Data Encryption

Terraform Cloud

Prior to storage, Terraform Cloud data is encrypted. All data is encrypted in transit.

HCP Vault and HCP Consul

Prior to storage, HCP Consul and HCP Vault data are encrypted. All data is encrypted in transit.

On-Premises Products

On-premises products are deployed by customers within environments under their control. Data encryption is the responsibility of the customer.

Data Backup

Cloud Products (Terraform Cloud, HCP Consul on AWS, HCP Vault on AWS)

Backups are taken of all important data. Backup data is encrypted as described in *Data Encryption* and replicated to multiple regions for redundancy. Since these replicated backups are on the same cloud infrastructure that hosts production infrastructure, HashiCorp can quickly recover from disaster. Outages and backup failures are monitored and responded to.

Terraform Cloud

Terraform Cloud is hosted in AWS within a region located in the United States. The backups of Terraform Cloud are stored in a region located in the United States and replicated to another geographic region also in the United States.

HCP Consul on AWS and HCP Vault on AWS

HashiCorp Cloud Platform has two distinct components: control plane and data plane.

The HCP control plane is hosted on AWS within a region located in the United. The backups of the control plane are stored in a region located in the United States and replicated to another region also in the United States. The HCP data plane is also hosted in a public cloud provider, and in regions chosen by the customer. Backups of the dataplane in any region are stored in a region located in the United States.

On-Premises Products

On-premises products are deployed by customers within environments under their control. Data backup is the responsibility of the customer.

Data Retention

Terraform Cloud

When a customer deletes an organization or workspace, the objects associated with the organization or workspace are deleted. Backups are retained.

Network Security Overview (continued)

Data Retention (continued)

HCP Vault on AWS

When a customer deletes a cluster, the data associated with that cluster is marked for deletion. A 30-day deletion hold is implemented to mitigate accidental or unauthorized cluster deletions. After 30 days, deletion is initiated and completed within 4 days.

HCP Consul on AWS

When a customer deletes a cluster, the data associated with that cluster is immediately deleted. Backups are retained.

Disaster Recovery

Because the infrastructure of HashiCorp cloud products is cloud-hosted via AWS, a disaster event occurring at the HashiCorp San Francisco office would not impact production systems. However, HashiCorp maintains a business continuity plan (BCP) to respond to disruptions or outages of systems critical to developing, operating, and providing customer support of HCP services. A business impact analysis (BIA) is performed for those critical systems, which includes defining a recovery time objective (RTO) and workaround procedure. Both the BCP and BIA are reviewed annually. A BCP tabletop is performed annually.

Terraform Cloud

If there was a major disaster or outage that destroyed or severely compromised the infrastructure within the AWS hosted regions, HashiCorp maintains a disaster recovery plan that allows Terraform Cloud to run in an alternate AWS region in the event of a loss of the services in the primary region. The disaster recovery plan is tested at least twice annually.

HCP Vault and HCP Consul

If there was a major disaster or outage that destroyed or severely compromised the infrastructure within the AWS hosted availability zones, HashiCorp maintains a disaster recovery plan that allows HCP Consul and HCP Vault to run in alternative availability zones in the event of a loss of the services in the primary availability zones. The disaster recovery plan is tested at least annually.

On-Premises Products

On-premises products are deployed by customers within environments under their control. Disaster recovery primarily is the responsibility of the customer. For outages impacting the development, delivery, and support of on-premises products, HashiCorp has created and maintains a business continuity plan (BCP). The BCP identifies critical systems, defines a recovery time objective (RTO) and workaround procedures, and defines recovery activities for major functions, including customer support. A business impact analysis (BIA) is performed for those critical systems, which includes defining a recovery time objective (RTO) and workaround procedure. Both the BCP and BIA are reviewed annually. A BCP tabletop is performed annually.