HashiCorp

System and Organization Controls (SOC) 3

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

June 1, 2020 to November 30, 2020

armanino

Prepared by ArmaninoLLP's
Risk Assurance & Advisory Practice Group

TABLE OF CONTENTS

armanino

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of

HashiCorp Inc.,

San Francisco, California

Scope

We have examined HashiCorp's ("Company" or "HashiCorp") accompanying description of its on-premise systems Terraform Enterprise, Vault Enterprise, Consul Enterprise, Nomad Enterprise and cloud-hosted Software-as-a-Service (SaaS) systems Terraform Cloud and Consul Service on Azure found in Section III titled Management's Description of Controls throughout the period June 1, 2020 to November 30, 2020 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2020 to November 30, 2020, 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 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 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, in all material respects. 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 controls were not effective to achieve HashiCorp's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HashiCorp's service commitments and system requirements based 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 the effectiveness of 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that the controls within HashiCorp's platform were effective throughout the period June 1, 2020 to November 30, 2020, 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]

San Ramon, California

December 22, 2020

MANAGEMENT'S ASSERTION REGARDING THE DESIGN AND EFFECTIVENESS OF ITS CONTROLS OVER HASHICORP'S PLATFORM BASED ON THE TRUST SERVICES CATEGORIES FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY

We are responsible for designing, implementing, operating, and maintaining effective controls within HashiCorp Inc.'s platform (system) throughout the period June 1, 2020 to November 30, 2020, to provide reasonable assurance that HashiCorp's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in Management's Description of Controls 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 June 1, 2020 to November 30, 2020, 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 Management's Description of Controls.

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 June 1, 2020 to November 30, 2020, to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved based on the applicable trust services criteria.

Talha Tariq

CSO

HashiCorp, Inc.

December 22, 2020

MANAGEMENT'S DESCRIPTION OF CONTROLS

Company Overview

Founded in 2012, HashiCorp ("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.

Products Overview

HashiCorp's suite of products consist of software that can be installed on-premises, and cloud-hosted Software-as-a-Service (SaaS) products, such as **HashiCorp Consul Service on Azure** (HCS) and **Terraform Cloud** (TFC). 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 Enterprise): 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 Enterprise): 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.

Products Overview (continued)

- Connect (Consul Enterprise): Accelerate application delivery by automating the network, including physical devices, virtual appliances, and distributed service mesh.
- Run (Nomad Enterprise): 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.

- Consul Service on Azure: Allows the provision of HashiCorp-managed Consul clusters directly through the Microsoft Azure Marketplace. Fully managed by HashiCorp, from provisioning and management to upgrades, Consul on Azure allows customers to automatically leverage the latest security best practices to discover services and securely route traffic across multiple AKS or Azure Compute environments. Consul Service on Azure is made up of the control and data planes. The control plane is responsible for orchestrating the entire lifecycle of a Consul cluster including monitoring, patching and remediation. The data plane refers to the Consul components deployed within a managed VPC which are dedicated to a single customer. Customer data is contained within the data plane and is not shared with other customers.

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 HashiCorp's Cloud Products.
- 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

The HashiCorp Leadership Team (HLT) and the Board of Directors are responsible for overseeing internal controls.

Policies and Procedures

Relevant policies, standards, and procedures are updated by their respective owners and made available to HashiCorp employees through the HashiCorp wiki. Information security standards include, but are not limited to:

- HashiCorp Security Policy
- Software Development Standard
- Vulnerability Management Standard
- Logging and Monitoring Standard
- Asset Management Standard
- Physical Security Standard
- Data Classification Standard
- Risk Management Standard
- Access Management Standard
- Vendor Security Risk Management Standard

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.

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
- Virus/malware scanning of code repositories
- Vulnerability scans

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.

Product Security (continued)

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

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. A quarterly vulnerability scan is performed against Terraform Cloud by an independent third party.

Vulnerability fixes are included in new product releases, and communicated via product changelogs, security bulletins, and Common Vulnerabilities and Exposures (CVE) entries.

Availability and Confidentiality

Data Backup

Terraform Cloud

Backups of production database instances are automatically initiated every 24 hours days using the AWS managed instance backup and retained for 7 days. Backup data is encrypted as described in *Data Encryption*. Logs of the backups are produced by AWS and available through the AWS console. Outages and backup failures are monitored and responded to by AWS. HashiCorp is notified in the event of any AWS service outage.

Consul Service on Azure

Backups of production database instances are automatically initiated every 24 hours using the AWS managed instance backup and retained for 30 days. Control plane Consul backups are initiated once every 10 minutes and the 30 most recent backups are retained. Data plane Consul backups are initiated once every 24 hours and retained for 30 days. Data plane Terraform state files are stored within S3 and retained as long as the deployed resource exists. Backup data is encrypted as described in *Data Encryption*. Outages and backup failures are monitored and responded to.

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 client has decided to terminate its relationship with HashiCorp, all client data is archived and stored for the length of time indicated in the Enterprise License Agreement and Terms of Use. All contractual and legal matters relating to client termination are overseen by the Legal team.

Availability and Confidentiality (continued)

Consul Service on Azure

Consul Service on Azure is offered through the Azure Marketplace. When a client has decided to discontinue use of Consul Service on Azure, HashiCorp terminates all customer objects.

On-Premises Products

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

Disaster Recovery

Terraform Cloud

Because the HashiCorp Terraform Cloud infrastructure is cloud-hosted via AWS, a disaster event occurring at the HashiCorp San Francisco office would not impact production systems. If there was a major disaster or outage that destroyed or severely compromised the infrastructure within the AWS hosted regions, HashiCorp maintains a 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.

Consul Service on Azure

Because the Consul Service on Azure infrastructure is cloud-hosted via AWS and Azure, a disaster event occurring at the HashiCorp San Francisco office would not impact production systems. If there was a major disaster or outage that destroyed or severely compromised the infrastructure within the AWS or Azure hosted availability zones, HashiCorp maintains a recovery plan that allows Consul Service on Azure to run in alternative availability zones in the event of a loss of the services in the primary availability zones.

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.