armanino

System & Organization Controls (SOC) 3

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

December 1, 2020 to November 30, 2021

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, 2020 to November 30, 2021, 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*).

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, 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.

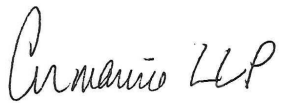
Inherent Limitations

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 cloud infrastructure automation platform were effective throughout the period December 1, 2020 to November 30, 2021, 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 17, 2021

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, 2020 to November 30, 2021, 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 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 December 1, 2020 to November 30, 2021, 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 December 1, 2020 to November 30, 2021, to provide reasonable assurance that HashiCorp's service commitments and system requirements were achieved based on the applicable trust services criteria.

MANAGEMENT'S DESCRIPTION OF CONTROLS

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.

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.

SaaS offerings include products such as **Terraform Cloud** (TFC) and **HashiCorp Consul Service on Azure** (HCS). 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.

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.

Products Overview (continued)

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

- 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 Azure Kubernetes Service (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 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.

Products Overview (continued)

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 intranet. Policies and standards are version and change controlled, and changes are approved by authorized personnel prior to being made. 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

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 annually or as major changes are made, whichever comes first.

Network Security

Terraform Cloud

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.

Consul Service on Azure

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.

Remote Access

Terraform Cloud

Remote access to the production environment and instances are restricted using an internal cloud authentication broker tool developed and maintained by the Security Team.

Remote Access (continued)

Consul Service on Azure

Remote access to the production environment and instances are 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 Management & Protection

Terraform Cloud

All production hosts have system-level monitoring and alerting for malicious activity. Alerts are sent to the Security team for triage. Production hosts use a hardened base that establishes a secure configuration baseline. The base image is updated and patched weekly. Newly deployed hosts use the updated and patched hardened base image.

Endpoint Management & Protection (continued)

Consul Service on Azure

Control plane instances have system-level monitoring and alerting for malicious activity. Alerts are sent to the Security team for triage. Data plane instances are not monitored as they are within the tenancy of the customer.

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 HashiCorp Security teams. Secure baseline configurations are established and employee workstations are configured against those baselines using endpoint configuration tooling.

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.

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. User access lists for applications, secured folders, root accounts and databases are reviewed by the system owners in collaboration with the IT and Security teams on a regular basis. 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. When use of Okta is not possible, HashiCorp encourages the use of 1Password to generate strong passwords and manage passwords. Passwords must be a minimum length of 8 characters or more. Use of publicly available identification information as a password and the re-use of old passwords is prohibited. All system default passwords are changed.

Section III – Management's Description of Controls

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 Software Development Standard. 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.

System Development Life Cycle (continued)

Consul Service on Azure

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

Change Management

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 software development 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.

Change Management (continued)

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 Vault, HCP Consul, or HCS 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.

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.

Consul Service on Azure

Prior to storage, Consul Service on Azure data is 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

Terraform Cloud

Backups of production database instances are automatically initiated every 24 hours 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

When a client has decided to discontinue use of HCP Consul or HCP Vault, HashiCorp terminates all customer objects.

Disaster Recovery

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 recovery plan that allows Terraform Cloud to run in an alternate AWS region in the event of a loss of the

Disaster Recovery (continued)

services in the primary region. The Terraform Cloud disaster recovery plan has a stated Recovery Time Objective (RTO) of 8 hours and Recovery Point Objective (RPO) of 30 minutes.

Because the Terraform Cloud infrastructure 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 tested annually.

Consul Service on Azure

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.

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. 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 tested 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.