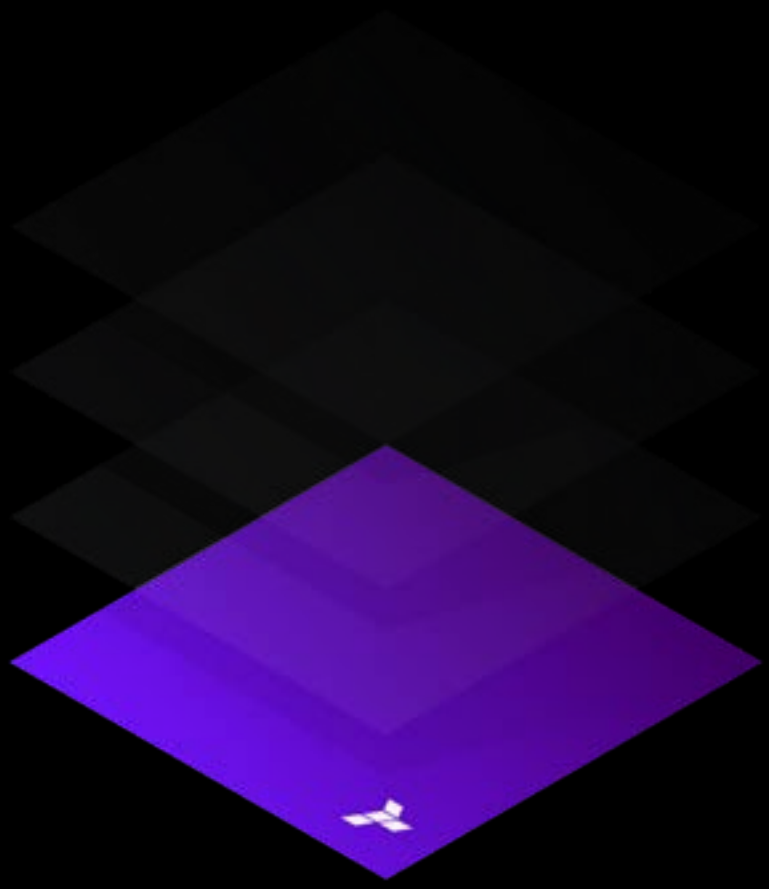
HashiCorp Terraform Cloud

Terraform Cloud Security & Compliance White Paper



HashiCorp

HashiCorp Terraform Cloud has established itself as the best way for practitioners, teams, and organizations to securely and reliably provision, manage and store the state of their infrastructures with over 5,000 new users each month, 500,000 runs each month, and over two million stored and managed infrastructure states.

Terraform Cloud is offered as a software as a service (SaaS) application and all of the infrastructure configuration data within, is hosted in the United States. Security, Privacy & Customer Trust is HashiCorp's top priority. This brief will cover aspects of data security, compliance levels, and service reliability with regards to Terraform Cloud.

Security Overview

Terraform Cloud was designed using core Information Security principles:

- **Confidentiality**: Prevent disclosure of information to unauthorized individuals
- **Integrity**: Maintain & assure the accuracy and consistency of data
- **Availability**: Ensure the information and service is available when needed

HashiCorp is committed to achieving these principles and the trust of our customers.

Security Program

HashiCorp has a dedicated Security, Privacy & Compliance program that coordinates security policy, program assessments and verification efforts to ensure customer and company information assets are adequately protected.

Security Team & Culture

HashiCorp has created a vibrant and inclusive security culture for all employees. Everyone at HashiCorp including our leadership is committed to our Customer Trust and Security as the highest priority. Our Security team is led by a Chief Security Officer with a cross functional team of security experts and dedicated teams focused on Product & Cloud Security, Threat Detection & Response, Risk & Compliance, Vulnerability Research and Enterprise Security. All employees receive regular security and awareness trainings that cover key security threats and their obligations to protect security, confidentiality and privacy of customer data.

Data Security & Privacy

Terraform Cloud places the security of the data it manages in the utmost regard. There are two main categories of data stored in Terraform Cloud, account and infrastructure. Account-based data includes information related to Terraform Cloud organizations, teams, and accounts such as authentication mechanisms, SSH keys, and version control system (VCS) related information and optionally payment information if a customer upgrades a paid tier. Infrastructure-based data includes information such as infrastructure configuration state files, logs, and variables. The data within the Terraform Cloud SaaS application is stored in either blob storage or PostgreSQL databases. Account data and Customer state files are encrypted at rest. More details can be found on the Terraform Cloud Data Security page.

It is not recommended for customers to store any personal data in Terraform Cloud. Consumers are encouraged to evaluate what data is being uploaded in their Terraform Cloud environment. HashiCorp strives to follow privacy by design principles, minimize personal data collection and does not sell Personal Data. Our Privacy Policy outlines the data elements we collect, process and store and can be reviewed here.

Network Security

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. Security services are monitored and updated in a timely manner to address emerging vulnerabilities.

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

Security Controls

Customers may use additional controls and integrations to further secure their Terraform Cloud Organizations. We recommend that wherever possible user authentication is managed via a Single Sign On (SSO) integration to ensure access control is consistently managed across enterprise systems. All access events are logged to an audit log, persisted for upto 14 days, and made available via an API for operational visibility or integration into other systems for analysis. User permissions can be managed via granular Role Based Access Controls (RBAC). Strict governance controls may be implemented to ensure only compliant changes are made to infrastructure through the use of the HashiCorp Sentinel Policy as Code framework.

Compliance

HashiCorp follows many regulatory and compliance standards. Terraform Cloud has achieved SOC 2 Type 1 compliance through the American Institute of CPAs (AICPA). This means Terraform Cloud has put in place and follows the procedures and security policies necessary to reduce risks, and that their processes can be requested and audited.

HashiCorp also meets applicable privacy requirements through a Data Protection Agreement (DPA) through agreements with controller-to-processor Standard Contractual Clauses approved by the European Commission. We have a security agreement and a DPA that is tailored to HashiCorp's business model. More information about and can be found here.

Third-Party Assessments & 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. External security assessments can be requested by prospects and customers under an NDA.

Vulnerability Reporting

We deeply appreciate any effort to discover and disclose security vulnerabilities responsibly. If you would like to report a vulnerability in one of our products, or have any security concerns with HashiCorp software, please e-mail security@hashicorp.com. Detailed process and our PGP key can be found here.

Reliability

The production infrastructure used by HashiCorp for Terraform Cloud has been engineered on the principles of high availability, security and confidentiality. To ensure availability of production infrastructure and customer-facing applications, HashiCorp maintains a Business Continuity and Disaster Recovery Plan. HashiCorp maintains a publicly available status page for Terraform Cloud's availability, which can be found here. The Terraform Cloud Business tier includes a service level agreement (SLA) to maximize reliability. Additional details about the SLA can be found in the HashiCorp Cloud SLA.


HashiCorp