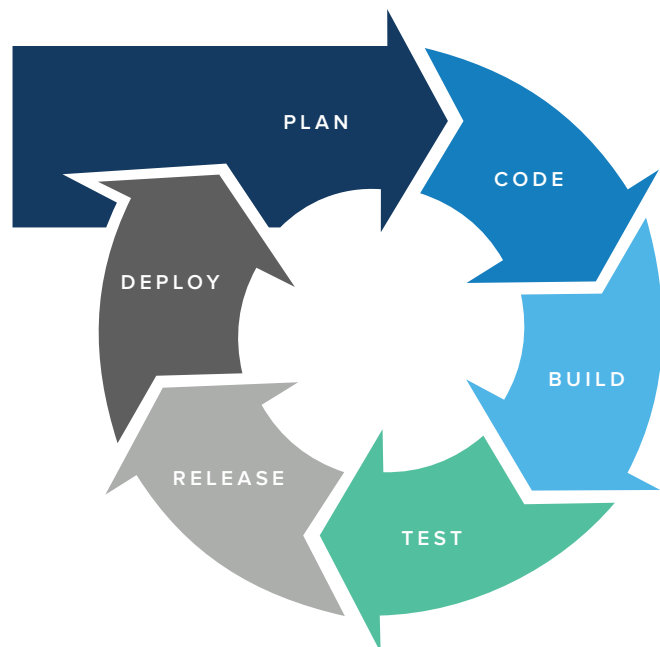# Okta + HashiCorp

Integrate Strong Identity into the Modern Development Pipeline

Development and operations teams are under constant pressure to create and deploy software in fast-paced continuous integration and continuous delivery (CI/CD) environments. Meeting these accelerated timelines means automating as many manual tasks as possible, and DevOps teams are turning to efficient "infrastructure as code" practices to power their efforts. But moving quickly in automated environments can expand the enterprise's attack surface and introduce new security vulnerabilities. To help companies adopt more efficient processes while keeping enterprise assets secure, Okta + HashiCorp have teamed up to provide powerful joint solutions that let developers and operations teams safely automate workflows across the software development lifecycle, without putting the enterprise at risk.

Shift-left security while adding automation efficiencies for developers

Okta's Advanced Server Access (ASA) works with HashiCorp to help teams securely automate time-consuming, risky manual processes. Okta's ASA enables a modern, dynamic development environment by baking strong, identity-based security right into the infrastructure layer. The combination of ASA + HashiCorp's Terraform lets teams securely and automatically spin up and spin down elastic cloud infrastructure. Additionally, the combination of Okta Identity Cloud + HashiCorp's Vault securely stores and simplifies team member access to tokens, passwords, certificates and encryption keys. Together, Okta and HashiCorp help companies confidently adopt Zero Trust security best practices, authenticating and authorizing every infrastructure access attempt, while simultaneously providing development teams with new tools to increase productivity.

Together, Okta + HashiCorp let you:

- Bake strong identity-based server access controls right into development workflows, to ensure end-to-end security and auditable access trails

- Secure the dev environment so teams can automate repetitive processes, like quickly and efficiently spinning up and down dynamic cloud environments

- Accelerate workflows for software development and deployment while simultaneously extending Zero Trust security principles to the infrastructure layer

—

How Okta + HashiCorp work together

The Okta + HashiCorp partnership safely reduces the time it takes teams to create, access, and deploy software within the cloud, while supporting the Zero Trust security architecture. Security can sometimes be an afterthought in today's dynamic, high-velocity development environments. But Okta's Advanced Server Access (ASA) lets enterprises inject identity and access controls directly into automated infrastructure. Okta and HashiCorp work together to extend Okta's strong identity management and security, including authentication and automated lifecycle management, to the infrastructure layer, and simultaneously protect ephemeral cloud environments and support agile development workflows.

Using Okta to manage Terraform, and vice versa

Busy teams creating and destroying elastic infrastructure on the fly want the freedom to control settings through code, but security and IT teams sometimes prefer the centralized control of the familiar Admin UI experience. Okta and HashiCorp's Terraform support both approaches. Developers can, for example, configure Okta groups through Terraform, and can use ASA to automate cloud server configurations that draw users, groups, and permissions from Okta. API connections between Okta and Terraform ensure that settings changed in Terraform are automatically reflected in the Okta Admin dashboard, and changes made in Okta that (intentionally or unintentionally) change a setting managed in Terraform are flagged by Terraform the next time it's run, so unwanted configuration changes can be quickly caught and reversed.

Making stored passwords and other secrets easily and securely accessible to development teams

Organizations sometimes have use cases that require developers to use credentials, like database passwords. These keys-to-the-kingdom can be high-value targets for credential thieves. For cases like these, Okta integrates directly with HashiCorp's Vault so developers' "secrets" can be securely encrypted and stored, safe from threat actors but easily accessed by authenticated parties through a seamless Okta Single Sign-On (SSO) and Multi-Factor Authentication (MFA) workflow.

With Okta + HashiCorp, enterprises can...

- Confidently support an agile, efficient, infrastructure-as-code environment

- Keep security teams happy by baking in strong identity-based security in from the start

- Enable developers and operations teams to securely spin up and down cloud infrastructure on demand

- Minimize reliance on static keys, while safely securing necessary passwords

- Extend Zero Trust access controls to infrastructure while taking full advantage of flexible cloud architecture efficiencies

---

For more information on this integration, go to
okta.com/partners/hashicorp

If you have questions, please contact our sales team at okta.com/contact-sales

---