HashiCorp & Veza:
Intelligent Access for Secrets Management

Plaintext secrets are vulnerable out in the wild. They can be phished or discovered hardcoded in your source. Weak or old secrets can be cracked. And with so many humans, automated processes and cloud platforms generating and using secrets, it's hard to know how many are out there. As migration to the cloud, adoption of microservices architecture and the proliferation of non-human identities drove an explosion in the number and scope of secrets, keys, and certificates used across the enterprise, practitioners coined the term "Secrets Sprawl" to cover the challenges of managing and protecting secrets.

Secrets Managers, like HashiCorp Vault, go a long way towards solving the problems of managing secrets themselves: storing them, integrating them into your business processes, and enforcing rotation policies. Augment HashiCorp Vault with the power of Veza's Access Graph, and together they can also address the access that those secrets provide, so that you can eliminate unneeded or risky access and apply the Principle of Least Privilege across all of your secrets.

HashiCorp Benefits

Eliminate Secrets Sprawl
Centralize all of your secrets in one place, so you can easily grant identity, and time-based access to the resources they protect.

Standardize best practices
Standardize adoption of security best practices across your stack, creating and enforcing org-wide policies for password strength, encryption standards, key expiration and rotation, certificate TTLs, and more.

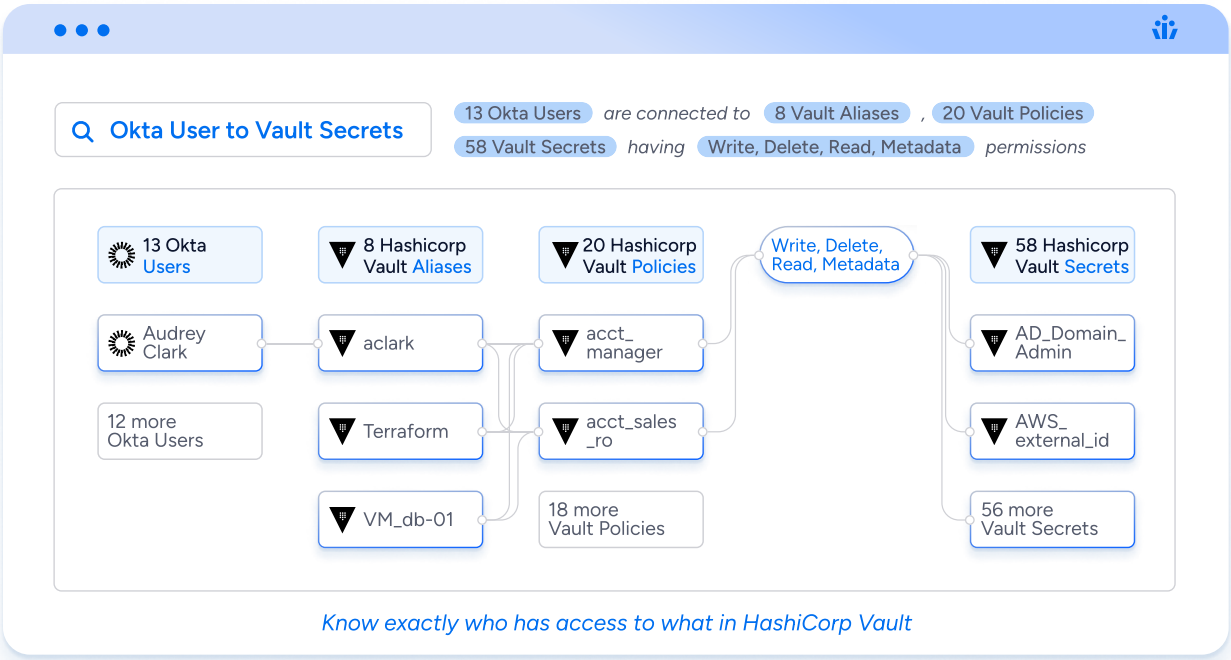
Secrets Integration
Easily and securely inject secrets into processes and environments, like Kubernetes and AWS services.

Rapid Response
Respond immediately to a detected incident or threat by revoking or restricting access to managed secrets, even if the attack vector or the source of the threat is not yet known.

HashiCorp + Veza Benefits

Veza's Identity Security platform answers the question of "Who has access to what" across all identities and systems in the enterprise. The granular visibility into access provided by Veza can turn HashiCorp Vault into a powerful tool for managing access risk and achieving least privilege.

Access Visibility

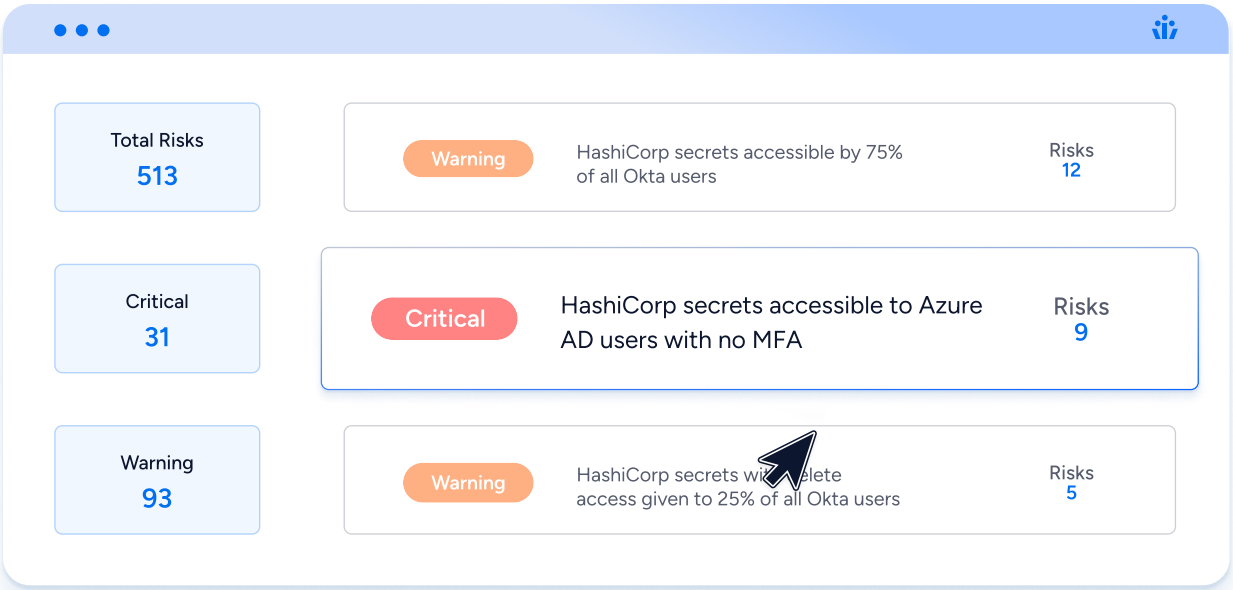


Know exactly who has access to what in HashiCorp Vault

With Veza's Access Graph, you can visualize all identities that can access any secret in HashiCorp Vault: including vault-native identities, federated identities from your Identity Providers (IdPs) and non-human identities (NHIs). You can also see how they get that access: via entities, aliases, groups, and policies. Flip this idea around, and you can get a full picture of the access for any identity to secrets in HashiCorp Vault.

- ☑ Ensure that your provisioning actions actually give an identity the access it needs, and no more.
- ☑ Protect critical data by always knowing who can access your most sensitive secrets.
- ☑ With Veza's visibility into all IdPs, apps (including custom apps) and on-prem and cloud data systems, find local accounts, certificates and other credentials not currently managed through HashiCorp Vault and migrate them.
- ☑ Understand HashiCorp Vault secrets in the context of your entire stack - for example, understand the access a single user gains through multiple IdP identities, and combine access data from HashiCorp Vault and other secrets managers, in AWS, Azure, etc.

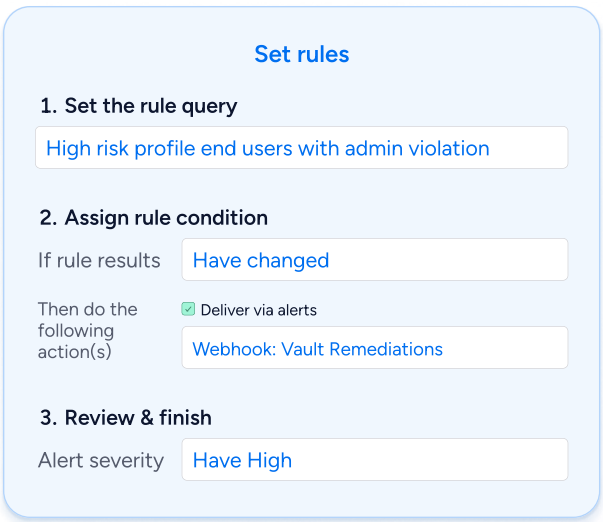
Access Intelligence

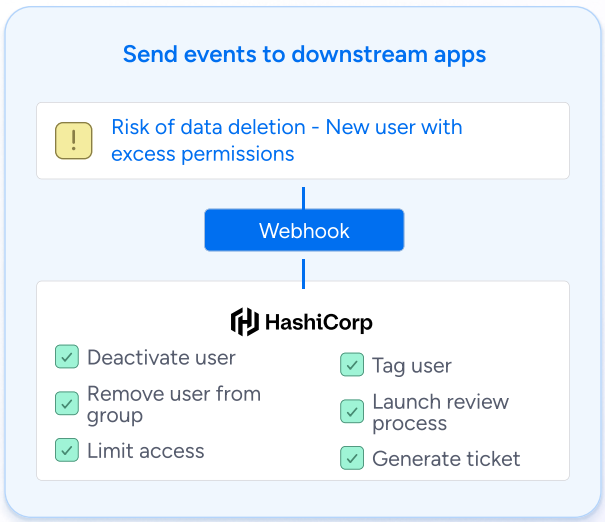


Beyond showing access for individual entities or secrets, Veza analyzes all access to secrets by all identities, human and non-human, to provide both out-of-the-box and custom intelligence. Use Access Intelligence to find anomalies and risks, like:

- Unneeded access to secrets
- Secrets assigned to a high proportion of identities
- "High blast radius" identities with access to a high proportion of secrets
- Secrets assigned to identities that are dormant, inactive, or vulnerable (for eg. no MFA)
- Federated and local identities with the ability to delete secrets in HashiCorp Vault
- Unused HashiCorp Vault licenses (entities with no secret access)

Risk Management and Remediation

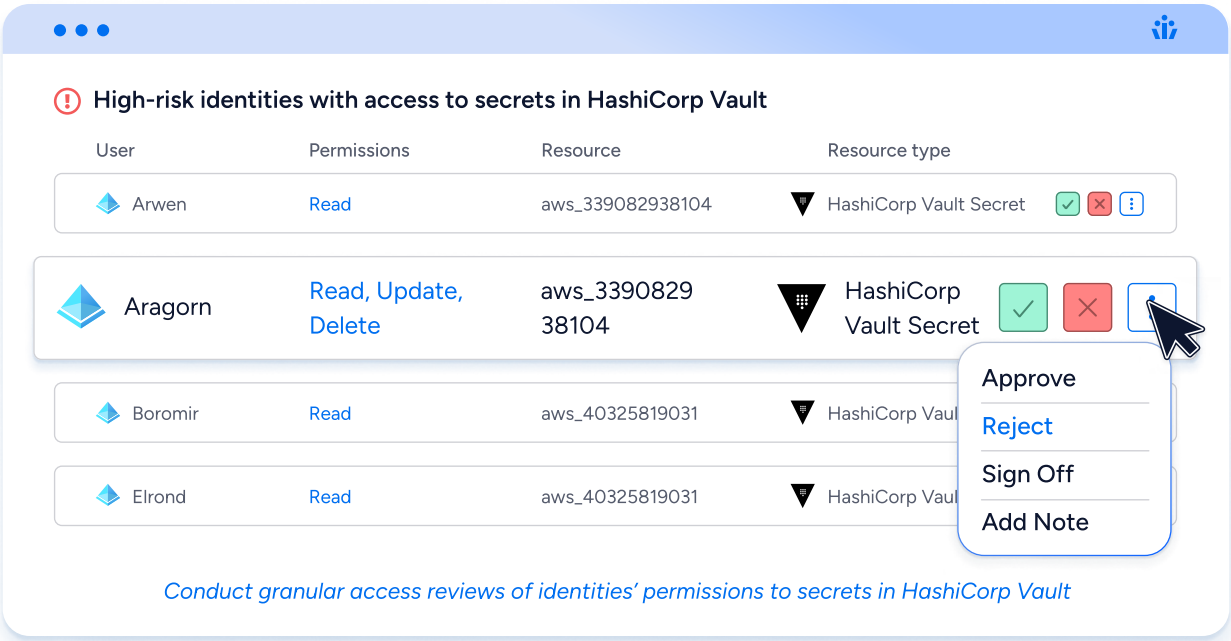




Veza continually monitors for changes to the state of access across your entire stack, including HashiCorp Vault secrets. A suite of integrations for alerts and remediation allows you to detect and fix risks before they can be exploited by an attacker.

- Alert your security and governance teams when new identities gain access to critical secrets.
- Automatically initiate workflows in ITSM tools like ServiceNow or Jira when risky access is detected.
- Create custom webhooks to automatically take action in HashiCorp Vault. For example, deactivate an entity, remove an entity from a group, or launch a review process.

Compliance



Conduct granular access reviews of identities' permissions to secrets in HashiCorp Vault

Base your compliance on the same granular detail of access provided by the Access Graph, slash manual compliance processes and spreadsheets, and give decision makers the context they need to make the right call.

- Compile, schedule, and assign quarterly or annual access reviews and certifications for all identities and secrets instantly.
- Conduct rapid reviews to remove access for at-risk identities.
- Automate follow-up actions through webhooks or ITSM tools to ensure that unapproved access is actually removed.

Get Started

To learn more about how Veza can help you eliminate risk and apply least privilege in HashiCorp Vault, visit veza.com/schedule-demo today.