Integration with HashiCorp Vault

Sonrai’s unique integration with HashiCorp Vault allows customers using Vault in AWS, Azure, and GCP environments to understand identities and workloads that have access to Vault secrets, what those secrets protect, and when they are used.

1. Authentication
2. Request Secret
3. Return Secret
4. Workload Uses Secret

Increased Visibility Into Vault Secrets
- When used in a public cloud workload
- When part of a cloud trust relationship
- When part of a cloud IAM/RBAC interaction

Answers Important Vault Questions
- Who/how an identity authenticates into Vault
- Identities that can access a secret?
- When secrets are used?
- What Vault IAM secrets protect?

Multi-cloud Vault Support
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Assess Vault Policy Change Risk
- Monitor access policy changes to a secret
- Baseline Vault IAM trust relationships
- Learn risky Vault policy changes before use

Want to see Sonrai and HashiCorp Vault in action?
Request a Demo son raisecurity.com/demo