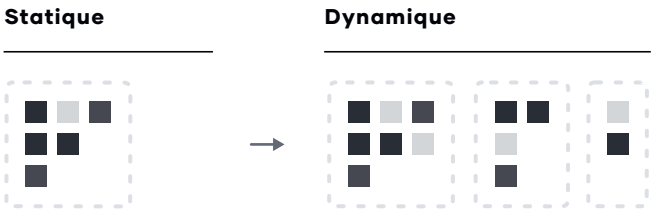
Vault

Automatisation de la sécurité cloud

Gérer les secrets et protéger les données sensibles dans les clouds publics et privés

Les défis de la sécurité de l'infrastructure

L'adoption du cloud signifie que les organisations passent d'une infrastructure statique vers un provisionnement et un management des infrastructures dynamiques : volume et distribution infinies de services, environnements ephémères et immutables, et capacité à déployer sur plusieurs environnements cibles.



Datacenters avec des réseaux intrinsèquement fiables avec des périmètres réseau clairs.

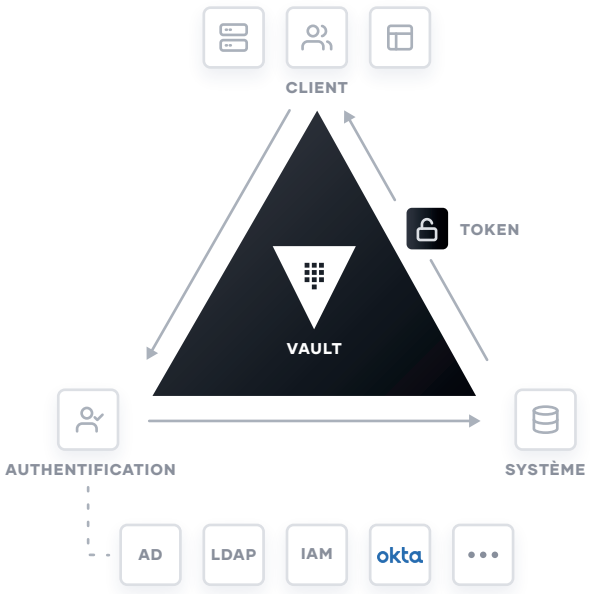
Plusieurs clouds et datacenters privés sans périmètre réseau clair.

HashiCorp Vault

Vault vous permet de sécuriser, stocker et contrôler étroitement l'accès aux tokens, mots de passe, certificats, clés de chiffrement et autres données sensibles à l'aide d'une interface utilisateur, d'une CLI ou d'une API HTTP.

Vous pouvez augmenter la productivité, contrôler les coûts en réduisant les systèmes, licences et frais généraux en gérant de manière centralisée toutes les opérations relatives aux secrets. Vault peut également aider à réduire le risque de violation en éliminant les identifiants statiques et écrits en dur en centralisant les secrets.

- **Identification des identités** pour l'authentification et accès à différents clouds, application de politiques et automatisation facile.
- **Un workflow unique** qui s'intègre à l'infrastructure existante, réduit les coûts et fournit un audit unifié.
- **Communauté open source solide**, extensible et ouverte, vaste écosystème de partenaires et moteurs de secrets multi-cloud complets.



Solutions et avantages

Réduisez le risque de fuite de données

Chiffrez les données sensibles en transit et au repos en utilisant des clés de chiffrement gérées et sécurisées en central au sein de Vault, le tout via un workflow et une API uniques.

Réduisez votre surface d'attaque

Éliminez les identifiants statiques et écrits en dur en centralisant les secrets dans Vault et en contrôlant étroitement l'accès en fonction des identités approuvées.

Augmentez la productivité

Permettez aux équipes de développement de consommer automatiquement des secrets dans le cycle de déploiement applicatif et de protéger les données sensibles par le biais d'une seule API.

Intégrations

- Authentifier et accéder à différents clouds, systèmes et terminaux en utilisant des identités fiables
- Maintenir les données d'application sécurisées grâce à la gestion centralisée des clés et aux API simples pour chiffrer/déchiffrer les données
- Stockage centralisé, accès et distribution de secrets dynamiques tels que les tokens, mots de passe, certificats et clés de chiffrement
- Fournit un support unifié entre des environnements hétérogènes. Intègre les workflows et les technologies que vous utilisez déjà

Approuvé par

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

Offres

	Open Source Ingénieur système	Entreprise Organisations
	Secrets dynamiques ✓	**Toutes les fonctions Open Source** ✓
	Stockage des secrets ✓	Reprise après sinistre ✓
	Plug-ins sécurisés ✓	Namespaces ✓
	Journaux d'audit détaillés ✓	Réplication ✓
	Location et révocation des secrets ✓	Filtres de réplication ✓
	ACL Templates ✓	Répliques en lecture ✓
	Agent Vault ✓	Groupes de contrôle ✓
	Workflow Init & Unseal ✓	HSM Auto-unseal ✓
	Rotation des clés ✓	Authentification multi-facteurs ✓
	Interface utilisateur avec gestion de cluster ✓	Intégration Sentinel ✓
	Entités et groupes d'identités ✓	FIPS 140-2 et Seal Wrap ✓
	Politiques de contrôle d'accès ✓	Support de KMIP ✓
	Plug-ins d'identité ✓	Transformation ✓
	Chiffrement as a Service ✓	
	Transit backend ✓	
	Rotation des clés de chiffrement ✓	
	Entités et groupes d'identités ✓	
	Politiques de contrôle d'accès ✓	
	Plug-ins d'identité ✓	
	AWS KMS Auto-unseal ✓	
	Azure Key Vault Auto-unseal ✓	
	GCP Cloud KMS Auto-unseal ✓	
	Stockage intégré ✓	

HashiCorp

www.hashicorp.com