HashiCorp Vault

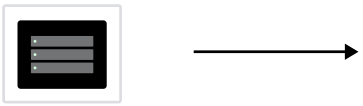
アイデンティティベースのシークレット管理の標準化

シークレットへのアクセスを管理して機密データを保護する、セキュリティ自動化のスタンダード

アイデンティティベースのセキュリティがクラウドと共に進

アイデンティティベースのセキュリティとは、従来の静的なセキュリティモデルから、動的な IP アドレスを使用した明確な境界のない環境に対応するセキュリティモデルへの移行を意味します。それに伴い、安全なネットワーク境界や信頼できるネットワークの確保よりも、インフラおよびアプリケーションサービスの保護が重視されるようになっています。

静的



ネットワーク境界が明確で本質的に信頼性の高いネットワークが整備されたデータセンター

従来のアプローチ

- 信頼性の高いネットワーク
- 明確なネットワーク境界
- IP アドレスごとに適用されるセキュリティ

動的

明確なネットワーク境界のない複数のクラウドとプライベートデータセンター

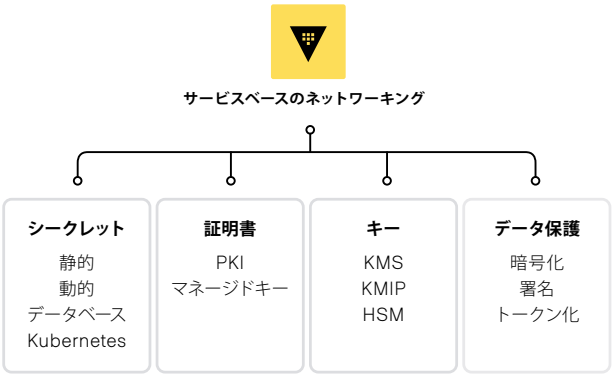
Vault のアプローチ

- パブリッククラウドにおける信頼性の低いネットワーク
- クラウド間の曖昧なネットワーク境界
- アプリケーションアイデンティティごとに適用されるセキュリティ

HashiCorp Vault

UI、CLI、HTTP API を使用してトークン、パスワード、証明書、暗号化キーなどの機密データを保護および保管し、それらに対するアクセスを厳重に管理します。

- 静的および動的シークレットの一元的な保管、利用、配布を実現
- Kubernetes 機能とのネイティブ統合によりシークレット管理機能の強化
- サービスアカウントのローテーションを自動化
- 暗号化鍵を一元管理しデータを保護



数兆個以上
年間で管理されるシークレットの数

2 億 5,000 万回以上
ダウンロード

70% 以上
米国上位 20 行の銀行

メリット

50% 節約できる時間

データ漏洩のリスクを低減

Vault で一元管理および保護された暗号化キーを使い、転送中と保管中の機密データを暗号化します。すべて単一のワークフローと API を通じて行われます。

100 万台以上 サポートされるエッジデバイス

侵害のリスクを低減

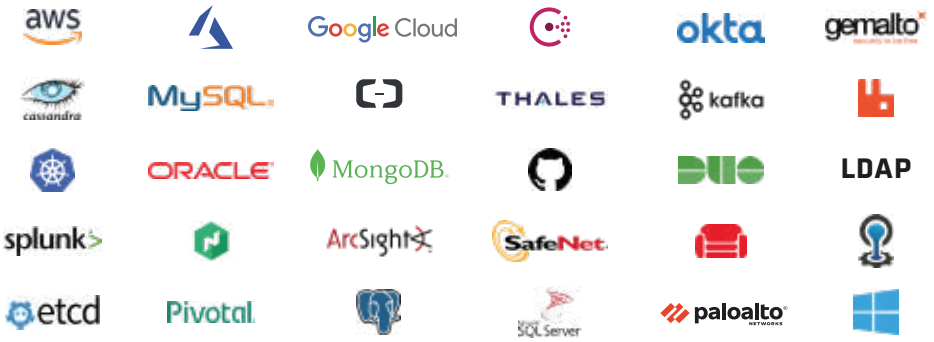
Vault でシークレットを一元管理し、信頼性の高いアイデンティティに基づいてアクセスを厳密に制御することで、ハードコードされた静的なクレデンシャルを取り除きます。

0% 予期せぬダウンタイム

生産性を向上

開発チームはアプリケーションデリバリプロセス中に自動的にシークレットを使用でき、単一の API を使ってプログラムにより機密データを保護できます。

サポート対象のテクノロジーとアイデンティティ



導入企業

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

機能の比較

		HCP Secrets	HCP Dedicated	Enterprise
導入 サービスレジストリとサービスディスカバリ	安全な保管		✓	✓
	Vault Agent		✓	✓
	詳細な監査ログ		✓	✓
	名前空間		✓	✓
	HCP Secrets	✓	✓	✓
標準化 安全なネットワーキング	クレデンシャルのリースと破棄		✓	✓
	安全なプラグイン		✓	✓
	エンティティおよびエンティティグループ		✓	✓
	クラスタ管理用 UI		✓	✓
	制御グループ			✓
	多要素認証		✓	✓
	パフォーマンスのレプリケーション		✓	✓
	ディザスターリカバリー（DR）		(SLA)	✓
	動的シークレット		✓	✓
	Secrets Sync	✓	✓	✓
拡張 ガバナンス、ライアンス、信頼性	ACL の管理およびテンプレート化		✓	✓
	Encryption as a Service コンプ		✓	✓
	PKI 証明書の管理		✓	✓
	AWS KMS での自動 Unseal		✓	✓
	GCP Cloud KMS での自動 Unseal			✓
	Azure Key Vault での自動 Unseal		✓	✓
	Sentinel の Policy as Code 管理		✓	✓
	HMS での自動 Unseal		✓	✓
	FIPS 140-2 および暗号化のコンプライアンス			✓
	ACME PKI		✓	✓