Akeyless vs HashiCorp Vault: Secrets Management at Scale and Why Akeyless Costs Less

How Akeyless saves money with smart architecture

Agenda

1. Why secrets management matters
2. Challenges with Vault
3. How Akeyless solves these challenges
4. Deep dive into architecture differences
5. Demo walkthrough

Why Secrets Management?

Keeps passwords, keys, and credentials safe

Essential for companies to protect data and systems

Helps avoid breaches and costly downtime

The Challenge with HashiCorp Vault

- High licensing fees and hardware costs
- Complex to set up and manage
- Requires clusters in every geographic region
- Not all Secrets are replicated

Introducing Akeyless

Cloud-native, true SaaS secrets management

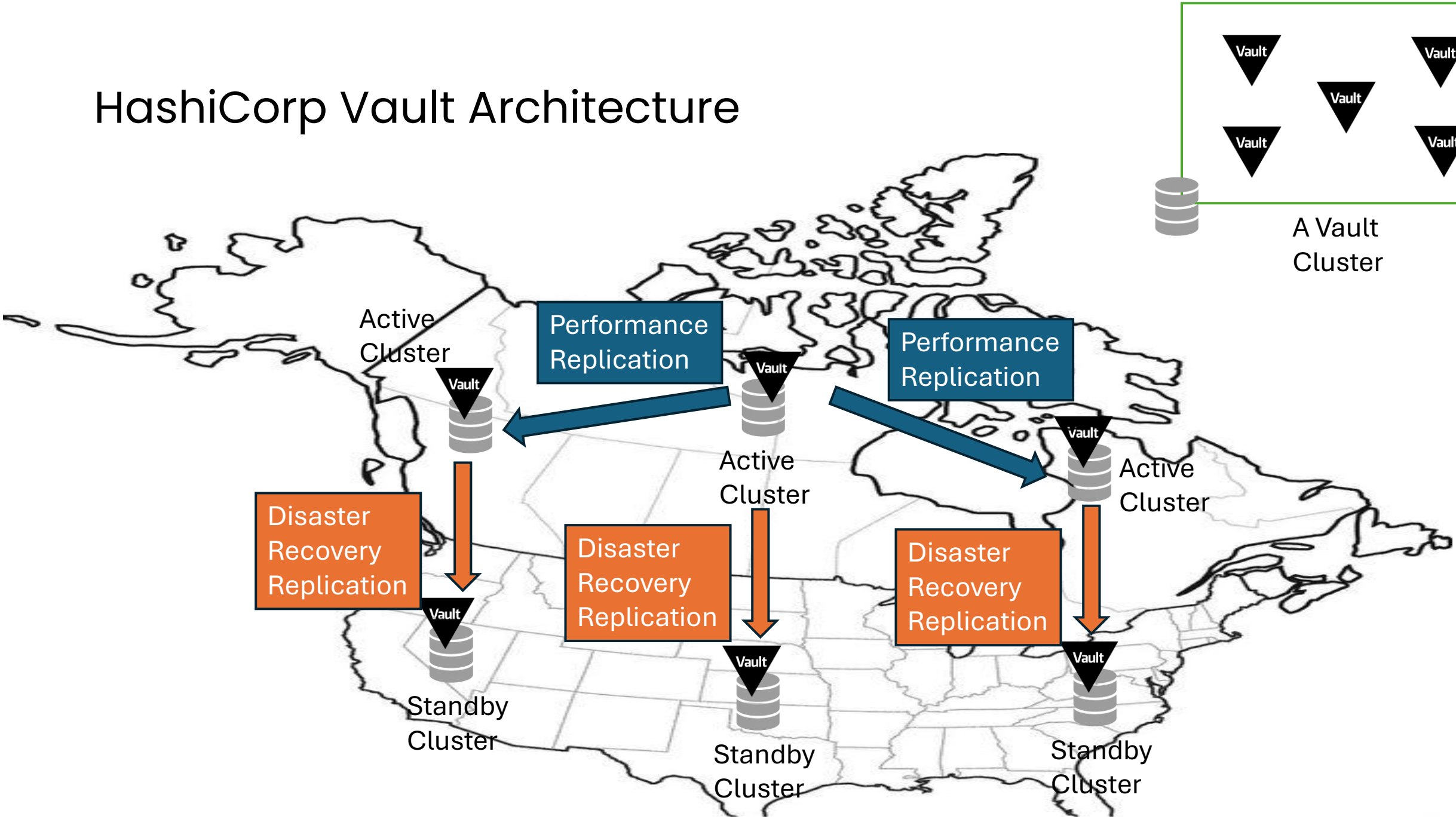
Easy deployment and zero maintenance

Pay-as-you-go pricing model

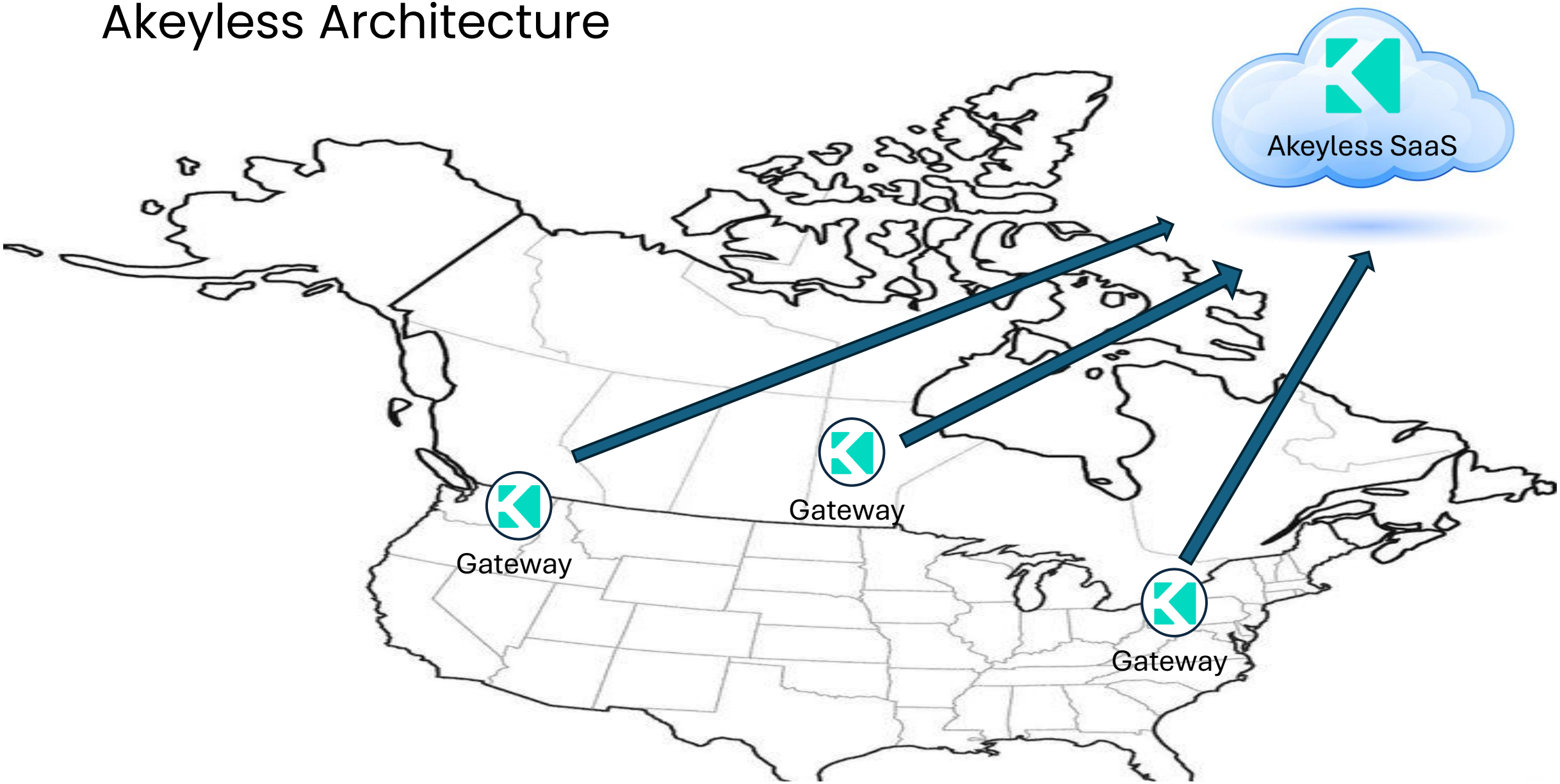
Architecture Comparison – HashiCorp Vault vs. Akeyless

HASHICORP VAULT	AKEYLESS
Requires a full cluster in every region	Uses stateless gateways at the edge of each private network
High hardware costs and licensing fees per cluster	Gateways connect to the SaaS backend via outbound communication
Complex to manage across regions	Easier to set up and far less costly

HashiCorp Vault Architecture



Akeyless Architecture



Distributed Fragments Cryptography (DFC)

Cimpress Case Study Overview

Global company with 12,000+ employees and $2B+ revenue

Central security team of 30 experts

Switched from Vault to Akeyless for cost and usability reasons

Akeyless Benefits for Cimpress

70% Cost Reduction: Lower licensing, hardware, and maintenance expenses

270% Higher Adoption: Easy onboarding and integration

Reliable & Scalable: Consistent performance across global teams

Demo

- Dashboard Tour
- Secrets Management Example with a Dynamic Secret
- Gateway in Action – Showing the Architecture