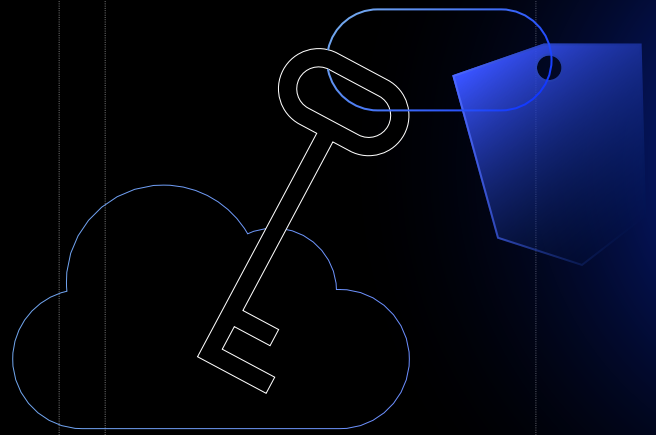
Case Study

SOFTSERVE TEAMS WITH HASHICORP VAULT TO STRENGTHEN SECURITY

SoftServe deploys HashiCorp Vault to strengthen client security and tighten their best practices



HashiCorp

softserve

OVERVIEW

It's no secret that security is a critical consideration for any platform, for both the visitor and the owner. It can be challenging for the platform owner to identify the right technology partner who is experienced in security implementations, and for that partner to select the correct tool to ensure that security.

Recently, a SoftServe client was ready to add 100 new microservice structures to enhance their offering and, therefore, decided to tighten their security best practices for their customers.

The company also wanted a more secure and flexible option for managing secrets in a Kubernetes infrastructure than their existing secrets management tool allowed. A "secret" is any data that requires tightly controlled access, such as API encryption keys, passwords, and certificates.

Recognizing the scope of the project, they looked for a reliable partner with extensive expertise specifically within the digital security domain. They chose SoftServe, which has been planning and executing complex security projects with distributed product development teams since 1993.

CHALLENGES

Our client's major challenge was to ensure the new security protocols and best practices were implemented smoothly, and that the authentication information mechanisms were scalable and maintainable.

SoftServe selected HashiCorp Vault, an identity-based secrets and encryption management system, as one of its key tools for the project. HashiCorp is a California-based, international software provider of open-source tools and proprietary products that allow developers and security professionals to run and connect cloud-computing infrastructure.

Vault works by validating and authorizing users, machines, and apps before providing them access to secrets or stored sensitive data. It allows users to integrate with different authentication methods, which may be more flexible than AWS Secrets Manager. It can also be used to manage other types of secrets such as certificates and Secure Socket Shell (SSH) credentials.

Integrating HashiCorp Vault into a business's infrastructure provides several benefits, including:

01

The ability to securely store and manage sensitive information, such as passwords and encryption keys, reducing the risk of data breaches and unauthorized access to sensitive data.

02

Can be configured to meet various compliance requirements, such as HIPAA, PCI-DSS, and SOC 2, making it easier for businesses to comply with regulations and industry standards.

03

Can be integrated with other tools, such as Ansible and Terraform, to automate the process of provisioning and revoking access to sensitive information, reducing the need for manual intervention, and increasing efficiency.

04

Provides users with detailed audit logs and access control capabilities, allowing businesses to monitor and track access to sensitive information, and to quickly detect and respond to any suspicious activity.

05

Supports high-availability mode, which makes it more reliable and less prone to outages.

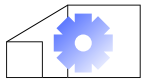
06

Can be used to store and manage any kind of secrets like API keys, database credentials, and SSH keys.

PLANNING

A dedicated team from SoftServe met with our client to develop a series of business and technical goals.

BUSINESS GOALS:



Expand the client's technical team's security expertise.

Quickly resolve any task or request issues.

Deliver a smooth and efficient project implementation.

TECHNICAL GOALS:

- Securely store and manage sensitive information, such as financial data, confidential documents, and customer information.
- Control access to sensitive information by setting granular permissions and policies.
- Automate the process of rotating and revoking access to secrets and credentials.
- Audit and track access to sensitive information to detect and prevent unauthorized access.
- Integrate with existing infrastructure and tools, such as cloud providers, Kubernetes, and CI/CD pipelines.
- Simplify the process of encrypting and decrypting data in transit and at rest.
- Help meet compliance requirements by providing a secure, auditable, and compliant environment for sensitive information.
- Streamline the process of managing and sharing secrets with third-party services and tools.
- Enable secure, programmatic access to secrets and credentials using APIs.
- Store and manage secrets for different environments such as development, staging, and production.

SOLUTION

We crafted a solution to meet our client's desire to securely manage and control access to sensitive information that included:

INCREASED SECURITY
By using Vault to securely store and manage sensitive information, our client could reduce the risk of data breaches and unauthorized access to their sensitive information.

COMPLIANCE
Vault could help our client meet compliance requirements by providing a secure, auditable, and compliant environment for sensitive information.

IMPROVED EFFICIENCY
By automating the process of rotating and revoking access to secrets and credentials, our client could streamline their workflow and increase their organization's efficiency.

BETTER VISIBILITY
Vault's audit and tracking features would allow our client to detect and prevent unauthorized access to sensitive information, which provides better visibility and control over their data.

INTEGRATION
HashiCorp Vault integrates with existing infrastructure and tools, such as cloud providers, Kubernetes, and CI/CD pipelines, allowing our client to easily manage secrets across different environments, improving their overall workflow.

IMPROVED COLLABORATION
Our client could share secrets and credentials with third-party services and tools, making it easier for teams to collaborate effectively.

EASY ACCESS
HashiCorp Vault enables secure, programmatic access to secrets and credentials using APIs, making it easier for our client to access sensitive information.

COST-EFFICIENCY
By using Vault to manage and control access to sensitive information, our client could reduce the costs associated with managing and securing data, such as hiring additional security staff and data breach costs.

Overall, using HashiCorp Vault to securely manage and control access to sensitive information improves our client's digital security, efficiency, compliance, and workflow, ultimately leading to more streamlined and cost-effective operations.

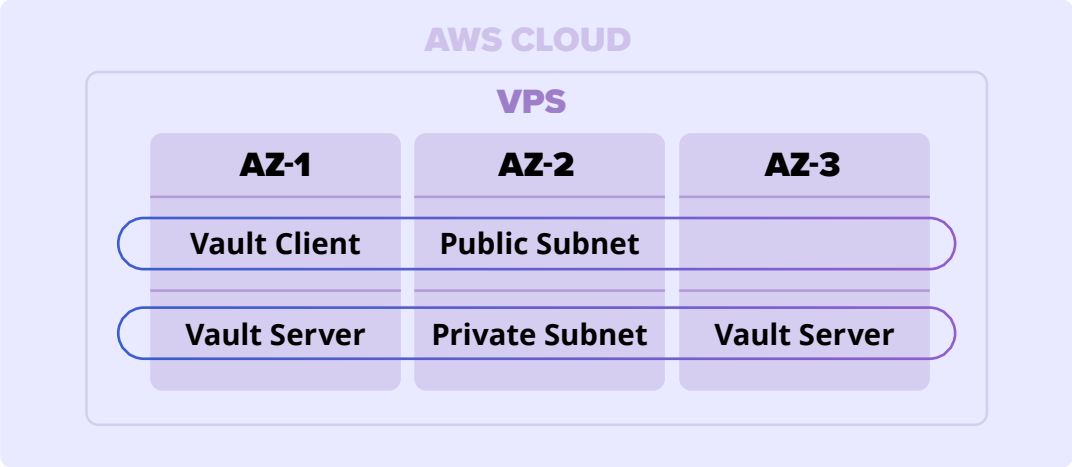
PROJECT

The SoftServe team created the project system design to increase security, speed up time to market, and achieve client satisfaction. The team performed the integration according to HashiCorp's best practices and recommendations.

SoftServe began by investigating our client's existing cloud infrastructure, which consisted of a few hundred microservices hosted in a managed Kubernetes cluster provisioned in AWS EC2 instances and integrated with RDS, S3, and AWS Secrets Manager. Following this review, SoftServe proposed a solution for a secure authentication mechanism.

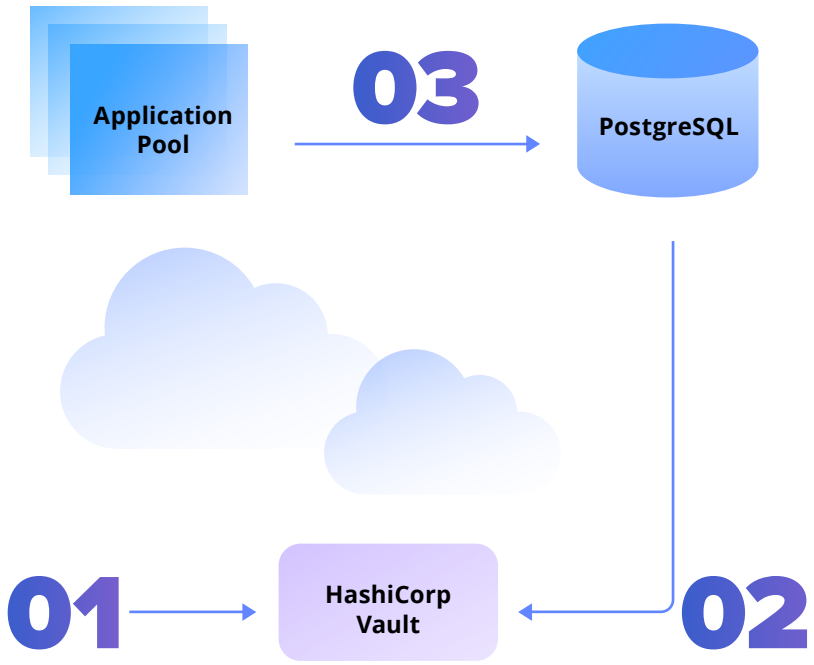
Next came the process of installing and configuring HashiCorp Vault. This included setting up a dedicated server for Vault and configuring it to authenticate with Kubernetes. Then, Kubernetes authentication was set up, including the creation of a Kubernetes service account, and configuring it to authenticate with Vault.

HASHICORP VAULT ON AMAZON EKS



- Enabled AWS KMS auto-unseal
- Enabled Cluster HA
- Enabled Raft storage for HA
- Enabled Vault audit to AWS CloudWatch
- Enabled SSL at Vault UI endpoint

SoftServe's team then created and stored secrets in HashiCorp Vault, such as database credentials, API keys, and other sensitive information. Secrets were injected into Kubernetes pods, including the configuration of the Kubernetes pods to authenticate with Vault and retrieve secrets at runtime. This action can be performed by using a Sidecar container or Kubernetes-Vault-monitoring and logging to track access to secrets, and to detect and respond to any potential security incidents. It was also necessary to set up the periodic rotation and revocation of secrets when necessary.



Finally, it was important to test the entire project integration to ensure that everything worked as expected. These tests included creating test pods, injecting test secrets, and verifying that the pods could retrieve the secrets at runtime.

During the integration, SoftServe and HashiCorp worked together to integrate HashiCorp Vault in the AWS Kubernetes service by:

Managing secrets in a secure and scalable way, such as with database credentials, API keys, and other sensitive information.

Securely storing secrets in Kubernetes can be challenging, as they can be easily exposed through misconfigurations or compromised pods. HashiCorp Vault provides a secure way to store and manage secrets but integrating it with Kubernetes was a complex challenge.

Another challenge lay in **authentication and authorization**, ensuring that only authorized users and applications have access to the secrets stored in Kubernetes. With HashiCorp Vault, we make sure that only authenticated and authorized users can access secrets.

Our client's previous sectors management solution was unreliable and had scalability performance issues. HashiCorp Vault has built-in availability and a performance replica to ensure a high service level objective (SLO). Its audit and logging feature also provides a detailed view for auditing purposes and ensures compliance with requirements.

TECH STACK

- HashiCorp Vault
- AWS
- Kubernetes
- AWS CloudWatch

THE RESULTS

SoftServe chose HashiCorp Vault because the solution covers these best practices:

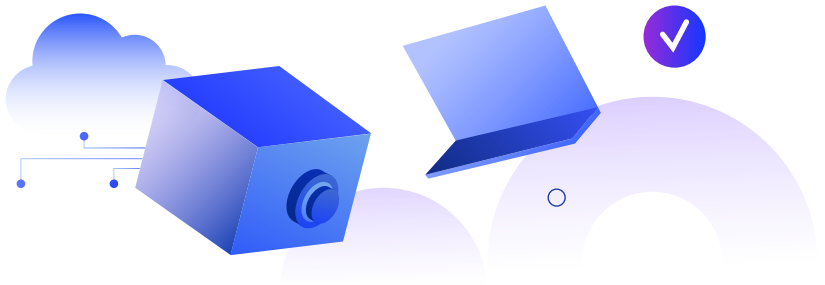
- Scalability and high performance
- An automated secrets rotation
- A standard and uniform method for secret management minimizes the effort needed to onboard new services to the system
- Integration with AWS IAM right out of the box

Integrating Vault in Kubernetes hosting on AWS provides significant benefits for security and compliance and ensures that costs are managed efficiently.

By integrating HashiCorp Vault into its existing production infrastructure on AWS Kubernetes, our client improved the security of its sensitive information and complied with industry regulations. Our client also automated the process of provisioning and revoking access to sensitive information, which reduced the need for manual intervention and increased efficiency.

HashiCorp Vault's high-availability mode ensures that our client's sensitive information is always available and can be recovered easily in case of a disaster. The audit logs and access control capabilities provided by Vault helped our client quickly detect and respond to any suspicious activity, further increasing the security of its sensitive information.

The integration of HashiCorp Vault into our client's existing production infrastructure on AWS Kubernetes has significantly improved the security and compliance of the company's sensitive information, while also increasing efficiency and availability.



Want to learn more about how SoftServe can help you strengthen and improve your organization's platform security and best practices using HashiCorp Vault?
LET'S TALK!

About SoftServe

We are advisors, engineers, and designers who deliver innovation, quality, and speed — elevating and accelerating our clients' digital journeys.

Our approach is built on a foundation of empathetic, human-focused experience design that ensures value and continuity from concept to release.

Visit our website, blog, LinkedIn, Facebook, and Twitter pages.

info@softserveinc.com
www.softserveinc.com

NORTH AMERICAN HQ

201 W 5th Street, Suite 1550
Austin, TX 78701
+1 866 687 3588 (USA)
+1 647 948 7638 (Canada)

BERLIN

Kurfürstendamm 11
Berlin 10719
+49 30 300 149 314 0
Toll free: 0 800 18 90 559

EUROPEAN HQ

30 Cannon Street
London EC4 6XH
United Kingdom
+44 333 006 4341

softserve